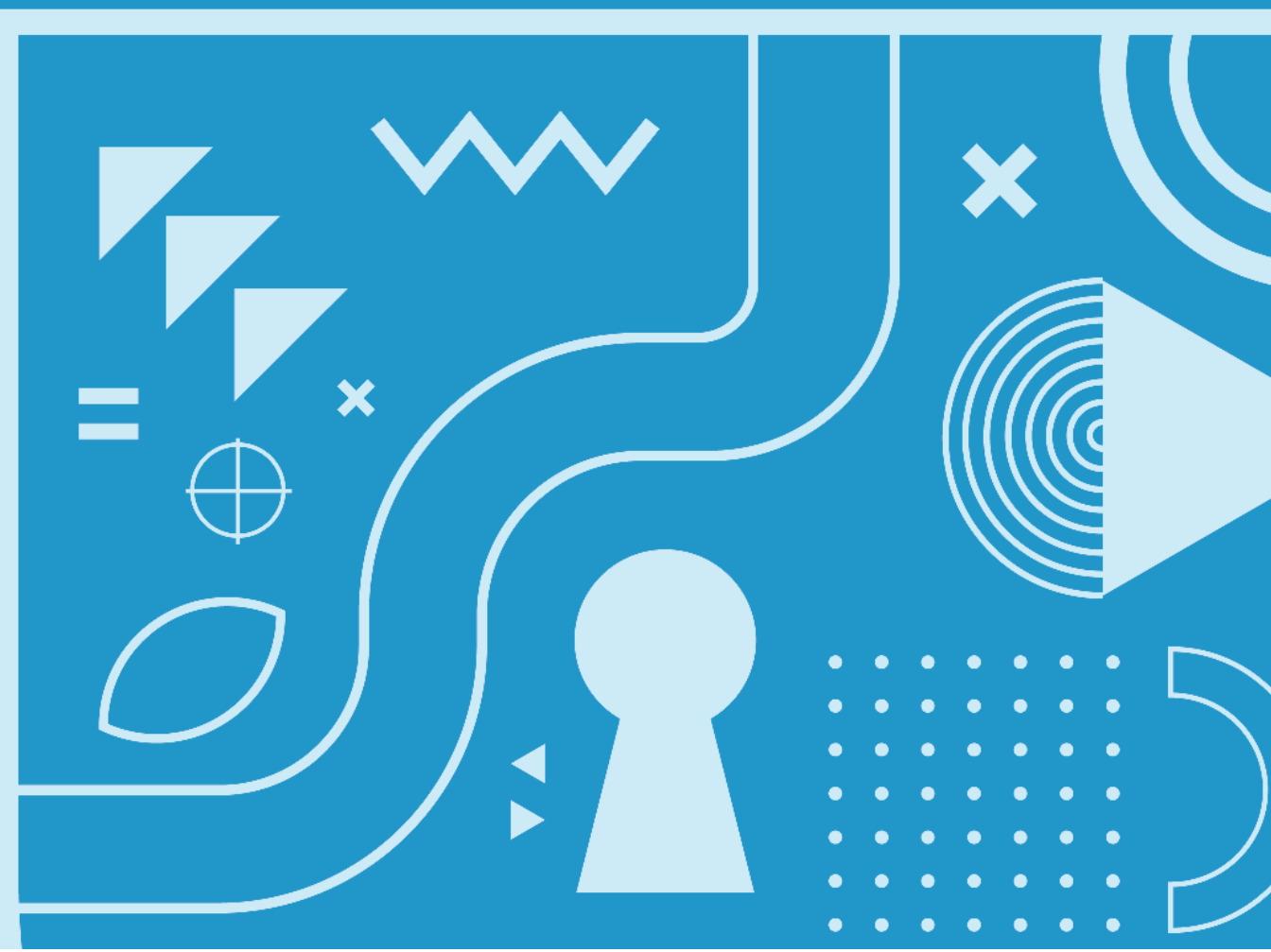
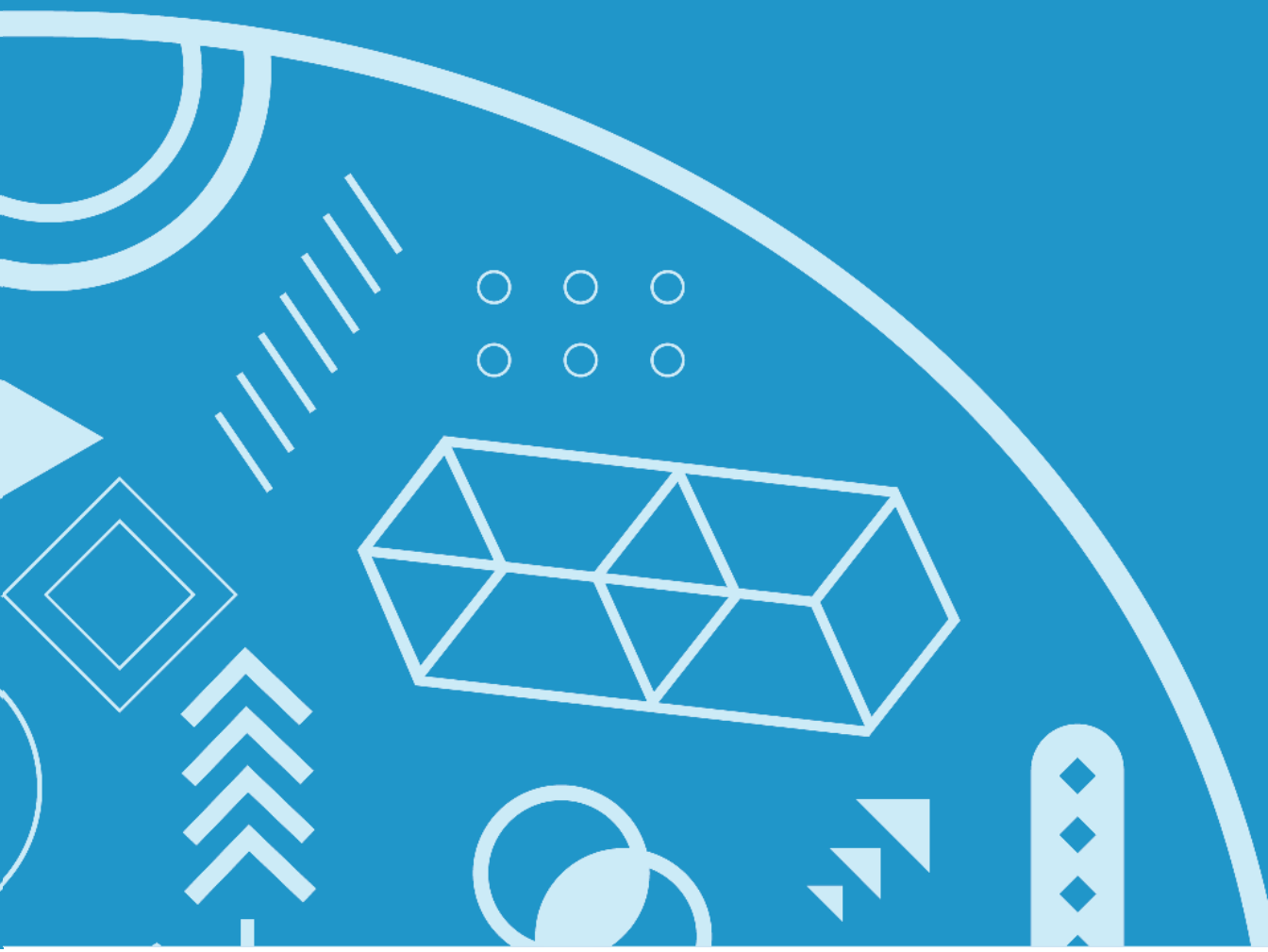


NATIONAL PRIVACY COMMISSION

THE 2024 COMPENDIUM OF NPC ISSUANCES

CIRCULARS





NPC Circular 2024-01

Date : **26 January 2024**

Subject : **AMENDMENTS TO CERTAIN PROVISIONS OF THE 2021 RULES OF PROCEDURE OF THE NATIONAL PRIVACY COMMISSION**

Pursuant to the authority vested in the National Privacy Commission (NPC) through Section 7(b) of Republic Act No. 10173, otherwise known as the "Data Privacy Act of 2012" (DPA), to receive complaints and institute investigations on matters affecting any personal information, the following amendments are hereby prescribed and promulgated, repealing for this purpose certain provisions of the 2021 Rules of Procedure of the NPC dated 28 January 2021.

SECTION 1. Rule I, Sections 4 and 5 of the 2021 NPC Rules of Procedure are hereby amended and renumbered to read as follows:

"**SECTION 4.** ***Definition of Terms.*** – The terms defined in the DPA, and its rules, are adopted accordingly in this Circular.

a. **AFFIRMATIVE DEFENSES** – shall refer to any defense by the respondent which, if found to be credible, will negate liability under the DPA, even if it is proven that the respondent in fact committed the alleged acts.

b. **BREACH INVESTIGATION** – shall refer to an investigation conducted by the NPC with respect to a data breach notification prompted by the applicable rules promulgated by the Commission.

c. **COMMISSION** – shall refer to the Privacy Commissioner and the two (2) Deputy Privacy Commissioners.

d. **COMPLAINT INVESTIGATION** – shall refer to an investigation conducted by the NPC with respect to a formal complaint filed by a data subject or his or her representative for violation of the DPA.

e. **COMPLIANCE CHECK** – shall refer to the systematic and impartial evaluation of a personal information controller (PIC) or personal information processor (PIP), in whole or in any part, process, or aspect thereof, to determine whether activities that involve the processing of personal data are carried out in accordance with the standards mandated by the DPA, IRR, and NPC issuances. It is an examination that includes Privacy Sweeps, Documents Submission, and On-Site Visits, which intends to determine whether a PIC or PIP is able to demonstrate organizational commitment, program controls, and review mechanisms intended to assure privacy and personal data protection in data processing systems.

f. **COURIER** – shall refer to any private mail carrier accredited by the Supreme Court, the NPC, or by international conventions of which the Philippines is a signatory.

g. **DIGITAL SIGNATURE** – shall refer to an electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer's public key; and (2) whether the initial electronic document had been altered after the transformation was made.[1]

h. **DOCUMENTS SUBMISSION** – shall refer to a mode of Compliance Check where the NPC may require the submission of documents and additional information from a PIC or PIP that has undergone a Privacy Sweep to, among others, clarify certain findings arising therefrom and to determine the level of compliance of the PIC or PIP with respect to its obligations under the DPA, IRR, and NPC issuances.

i. **ELECTRONICALLY-STORED INFORMATION** – shall refer to any information that is received, recorded, transmitted, stored, processed, retrieved, or produced electronically. It shall include any printout or output that accurately reflects the electronically stored information.[2]

j. **EVALUATING OFFICER** – shall refer to a member of the Compliance and Monitoring Division (CMD), a special committee, or task force (or respective members thereof) that may or may not include members from the CMD, created by order of the Commission to evaluate documents and information submitted to the CMD pertaining to compliance requirements and personal data breach notifications.

k. **HEARING OFFICER** – shall refer to a member of the Complaints and Investigation Division (CID), a special committee, or task force (or respective members thereof) that may or may not include members from the CID, created by order of the Commission to conduct hearings.

l. **INVESTIGATING OFFICER** – shall refer to a member of the CID, a special committee, or task force (or respective members thereof) that may or may not include members from the CID, created by order of the Commission to conduct investigations, hearings, and prepare related reports.

m. **JURIDICAL PERSON** – shall refer to: (1) the State and its political subdivisions, (2) corporations, institutions, and entities that are created by law for public interest or purpose, and (3) corporations, partnerships, and associations for private interest or purpose to which the law grants a juridical personality, separate and distinct from that of each shareholder, partner, or member.[3]

---

[1] Rules on Electronic Evidence, A.M. No. 01-7-01-SC, Rule 2, § 1(e) [July 17, 2001].
[2] *Id.* Rule 2, § 1(h).
[3] An Act to Ordain and Institute the Civil Code of the Philippines, [CIVIL CODE OF THE PHILIPPINES], Republic Act No. 386, Art. 44 (1949).

n. **MEDIATION** – shall refer to the voluntary process in which a Mediation Officer facilitates communication and negotiation and assists the parties in reaching a voluntary agreement regarding a dispute.

o. **MEDIATION OFFICER –** shall refer to a member of the Legal Division (LD), a special committee, or task force (or respective members thereof) that may or may not include members from the LD, created by order of the Commission to conduct mediation.

p. **MEDIATION SUPPORT OFFICER** – shall refer to a member of the LD, a designated person, special committee, or task force (or respective members thereof) that may or may not include members from the LD, created by order of the Commission to provide support to Mediation Officers.

q. **NPC** – shall refer to the National Privacy Commission created under the DPA.

r. **ON-SITE VISIT** – shall refer to a mode of Compliance Check if there are persistent or substantial findings of non-compliance of the PIC or PIP with the obligations indicated in the DPA, IRR, and NPC issuances.

s. **PARTIES IN INTEREST –** shall refer to a real party in interest who stands to be benefited or injured by the judgment in the suit, or the party entitled to the avails of the suit. Unless otherwise authorized by law or these Rules, every action must be prosecuted or defended in the name of the real party in interest.[4]

t. **PRELIMINARY MEDIATION CONFERENCE –** shall refer to the initial mediation conference after the parties mutually agree to enter into the mediation proceeding and the case is referred by the Investigating Officer to the Mediation Officer.

u. **PRIVACY SWEEP –** shall refer to the initial mode of Compliance Check where the NPC shall review a PIC or PIP's compliance with respect to its obligations under the DPA, IRR, and NPC issuances, based on publicly available or accessible information, such as, but not limited to websites, mobile applications, raffle coupons, brochures, and privacy notices.

v. **PRIVATE CAUCUS –** shall refer to a private meeting with either party called by the Mediation Officer, with the consent of both parties, to discuss issues in private and to arrive at a mutually satisfactory agreement beneficial to all parties.

w. **PUBLIC AUTHORITY** – shall refer to any government entity created by the Constitution or law.

x. **RULES** – shall refer to the 2021 NPC Rules of Procedure, including its amendments, unless otherwise stated.

---

4 2019 Amendments to the 1997 Rules of Civil Procedure (A.M. No. 19-10-20-SC), [RULES OF COURT], Rule 3, § 2 (May 1, 2020).

y. ***SUA SPONTE* INVESTIGATION** – shall refer to an investigation initiated by the NPC on its own for possible violation of the DPA."

"SECTION 5. *Enforcement Powers.* – The Commission may use its enforcement powers under the DPA in the course of investigations to order cooperation of the subject of the inquiries or other interested individuals or entities, including public authorities, or to compel appropriate action to protect the interests of data subjects."

SECTION 2. Rule II, Section 1 of the 2021 NPC Rules of Procedure is hereby amended to read as follows:

"**SECTION 1. *Who may file complaints.*** – Subject to Rule X of these Rules, data subjects who are affected by a privacy violation or data breach may file complaints for violations of the DPA: *Provided*, that a representative may file on behalf of a data subject if he or she is authorized by a special power of attorney. In the case of a minor or a person alleged to be incompetent, the pertinent provisions of the Rules of Court and its amendments shall apply. It is sufficient that proof establishing the relationship with the complainant be presented to the NPC as an attachment to the complaint. In case the minor or a person alleged to be incompetent is represented by the father or mother, the birth certificate shall be considered sufficient proof, while for the guardian, the court order designating the person as guardian shall be sufficient.

One or more data subjects may be represented by a single juridical person: *Provided*, that the juridical person filing the complaint must be authorized by a special power of attorney to appear and act on behalf of the data subjects: *Provided further*, the person representing the juridical person acting as the representative of one or more data subjects must be authorized to appear and act on behalf of the juridical person by a Board Resolution contained in a duly notarized Secretary's Certificate or its equivalent in case of government agencies[5].

In cases where the complainant is a non-resident citizen who has no authorized representative in the Philippines or is unable to appoint such a representative, such person may submit a complaint in accordance with these Rules: *Provided*, that the complaint must be notarized by the Philippine Embassy or Consulate, or with an apostille certificate from the country of origin."

SECTION 3. Rule III, Section 6 of the 2021 NPC Rules of Procedure is hereby amended to read as follows:

"**SECTION 6. *Service of judgments, orders, or resolutions of the NPC.*** – At the discretion of the Commission, judgments, orders, or resolutions shall be served either personally, by registered mail, by courier, by sending through user accounts and auto- generated notification of electronic systems implemented by the NPC, or by electronic mail. When a complaint, pleading, or any other submission is filed or submitted through electronic mail, the NPC may serve its judgments, orders, or resolutions by electronic mail through the same electronic mail address used in the filing of the complaint or pleading, or submission of document, unless otherwise indicated in the

[5] This includes a department, bureau, office, instrumentality, government-owned or controlled corporation, local government, state university and college, or a distinct unit in it.

complaint, pleading, motion, or other submissions of parties. When the NPC has opted to serve a judgment, order, or resolution by electronic mail, it shall no longer serve its issuances in the same case or matter by any other mode of service, unless circumstances warrant otherwise.

For judgments, orders, or resolutions served by electronic mail, electronic service is considered complete at the time of electronic transmission of the document, or when available, at the time that the electronic notification of service of document is sent.

For matters coursed through the electronic systems implemented by the NPC, the service of judgments, orders, or resolutions is deemed completed at the time it is successfully uploaded to the system."

SECTION 4. Rule IV of the 2021 NPC Rules of Procedure is hereby amended and renumbered to read as follows:

"RULE IV – PRE-INVESTIGATION PHASE

SECTION 1. ***Outright dismissal, when allowed.*** – Within thirty (30) calendar days from receipt of the complaint, the Investigating Officer may give the complaint due course or dismiss the complaint without prejudice, on any of the following grounds:

1. The complaint is insufficient in form or does not comply with Section 3, Rule II of these Rules;

2. The complainant does not give the respondent an opportunity to address the complaint, unless failure to do so is justified;

3. The complaint does not pertain to a violation of the DPA or does not involve a privacy violation or data breach;

4. There is insufficient information to substantiate the allegations in the complaint; or

5. The parties, other than the responsible officers of juridical persons, cannot be identified or traced despite diligence to determine them.

SECTION 2. ***Amendment of complaint, when allowed.*** – The complainant may substantially amend the complaint once as a matter of right at any time before the respondent has filed a comment, in which case the respondent shall be provided a copy and granted a fresh period to submit his or her comment. Substantial amendments after the respondent has filed a comment may only be done upon motion and with leave of the Investigating Officer.

SECTION 3. ***Permissive joinder of parties***. – All persons in whom or against whom any right to relief in respect to or arising out of the same transaction or series of transactions is alleged to exist, whether jointly, severally, or in the alternative, may, except as otherwise provided in these Rules, join as complainants or be joined as respondents in one complaint, where any question of law or fact common to all such complainants or to all such respondents may arise in the action; but the NPC may make such orders as may be just to prevent any complainant or respondent from being

embarrassed or put to expense in connection with any proceedings in which the party may have no interest.

SECTION 4. ***Compulsory joinder of indispensable parties.*** – Parties in interest without whom no final determination can be had of an action shall be joined either as complainants or respondents.

SECTION 5. ***Necessary party***. – A necessary party is one who is not indispensable but who ought to be joined as a party if complete relief is to be accorded as to those already parties, or for a complete determination or settlement of the claim subject of the action.[6]

SECTION 6. ***Non-joinder of necessary parties to be pleaded***. – Whenever in any complaint or pleading in which a claim is asserted a necessary party is not joined, the pleader shall set forth the party's name, if known, and shall state why the party is omitted. Should the NPC find the reason for the omission unmeritorious, it may order the inclusion of the omitted necessary party if jurisdiction over the person may be obtained.

The failure to comply with the order for a necessary party's inclusion, without
justifiable cause, shall be deemed a waiver of the claim against such party.

The non-inclusion of a necessary party does not prevent the NPC from proceeding with its investigation, and any decision rendered therein shall be without prejudice to the rights of such necessary party.

SECTION 7. ***Misjoinder and non-joinder of parties.*** – Neither misjoinder nor non-joinder of parties is ground for dismissal of a complaint. Parties may be dropped or added by order of the NPC by motion of any party or on its own initiative at any stage of the action and on such terms as are just. Any claim against a misjoined party may be severed and proceeded with separately.

SECTION 8. ***Entity without juridical personality as respondent***. – When two or more persons not organized as an entity with juridical personality enter into a transaction, they may be sued under the name by which they are generally or commonly known. In the answer of such respondent, the names and addresses of the persons composing the entity must be accurately stated. The address to be used shall be the last known address of the respondent.

SECTION 9. ***Submission of comment.*** – Upon finding that the complaint may be given due course, the respondent shall be required to file a verified comment within fifteen
(15) calendar days from receipt of the order. A copy of the complaint, together with its supporting evidence, shall be attached to the order to comment.

A complaint may be submitted for resolution if the respondent does not file a comment within the period provided.

In case the respondent is a minor or a person alleged to be incompetent, the pertinent provisions of the Rules of Court and its amendments shall apply. It is sufficient that proof establishing the relationship with the respondent be presented to the NPC as an

6 RULES OF COURT, Rule 3, § 8.

attachment to the comment. In case the minor or a person alleged to be incompetent is represented by the father or mother, the birth certificate shall be considered sufficient proof, while for the guardian, the court order designating the person as guardian shall be sufficient.

In case the respondent is a juridical person, the representative filing the comment must be authorized to appear and act on behalf of the juridical person by a Board Resolution contained in a duly notarized Secretary's Certificate, or its equivalent for a government agency[7].

SECTION 10. ***Content of the comment.*** – The respondent shall raise all of his or her defenses in the comment. No motions to dismiss shall be entertained: *Provided*, the Investigating Officer, in his or her discretion, may treat a motion to dismiss as the respondent's comment.

SECTION 11. ***Change of physical address or electronic mail address***. – A party who changes physical address or electronic mail address while the complaint is pending must promptly file, within five (5) calendar days from such change, a notice of change of physical address or electronic mail address with the NPC and serve the notice on all other parties. Service through the physical address or electronic mail address of a party, on record, shall be presumed valid, unless such party notifies the NPC of any change.

SECTION 12. ***Prohibited pleadings and motions.*** – The following pleadings and motions shall not be allowed in the complaint proceedings:

1. motions to dismiss the complaint;
2. motions for a bill of particulars;
3. motions to declare respondent in default;
4. dilatory motions for postponement;
5. replies or rejoinders, except if the preceding pleading incorporates an actionable document;
6. third-party complaints;
7. interventions; and
8. appeals or motions for reconsideration from any interlocutory order of the Investigating Officer.

SECTION 13. ***Affirmative defenses.*** – In lieu of a motion to dismiss, the respondent may raise in the comment affirmative defenses such as but not limited to:

1. The NPC has no jurisdiction over the subject matter;

[7] This includes a department, bureau, office, instrumentality, government-owned or controlled corporation, local government, state university and college, or a distinct unit in it.

2. The action is barred by a prior judgment;

3. There is another action pending between the same parties for the same cause;

4. The complainant has no legal capacity to sue;

5. That the pleading asserting the claim states no cause of action or is found to be frivolous, vexatious, or made in bad faith;

6. The action has otherwise prescribed under the statute of limitations; or

7. That the claim or demand set forth in the complaint has been paid, waived, abandoned, or otherwise extinguished.

SECTION 14. ***Authority of the Investigating Officer to rule on motions.*** – The Investigating Officer may directly rule on motions that do not fully dispose of the case on the merits. No appeal or motion for reconsideration may be taken for any interlocutory order made by the Investigating Officer but these may be included as an issue once the case has reached the Commission for adjudication under Rule VIII of these Rules."

SECTION 5. Rule VI of the 2021 NPC Rules of Procedure is hereby amended and renumbered to read as follows:

"RULE VI – ALTERNATIVE DISPUTE RESOLUTION

SECTION 1. ***Willingness to mediate***. – During the preliminary conference or at any stage of the proceedings but before endorsement of the case for decision by the Legal and Enforcement Office (LEO) Director or the Commission, as the case may be, the parties, by mutual agreement, may signify their interest to explore the possibility of settling issues by mediation.

SECTION 2. ***Application for mediation.*** **–** The parties shall jointly file with the Investigating Officer an Application for Mediation manifesting their earnest commitment to engage in a meaningful settlement process and their willingness to abide by these Rules and the orders issued by the assigned Mediation Officer.

Parties may apply for mediation through their representatives, *provided* that the latter are duly authorized in accordance with Section 8 of this Rule. Otherwise, no order to mediate shall be issued by the Investigating Officer until and unless such requirements have been completed and substantiated.

No application for mediation shall be approved without payment of the mediation fee.

SECTION 3. ***Mediation fees***. – The mediation fee, in an amount prescribed by the Commission in a separate issuance, shall be paid by the parties upon the filing of the Application for Mediation.

Parties may be exempted from the payment of the mediation fee under the same grounds as Section 4, Rule II of these Rules.

SECTION 4. *Order to mediate, when issued.* – The Investigating Officer shall issue an Order to Mediate, which shall state the following: (a) the approval of the Application for Mediation; (b) the suspension of the complaint proceedings for up to ninety (90) calendar days pending the mediation proceedings; (c) the name of the assigned or designated Mediation Officer who shall preside over the mediation proceedings; and
(d) the date, time, and place when the parties shall appear before the Mediation Officer for the Preliminary Mediation Conference. Copies of the Order to Mediate shall be furnished to the Mediation Officer and the parties.

SECTION 5. *Conduct of Mediation Officers.* – All Mediation Officers and Mediation Support Officers shall be bound by the NPC Mediation Code of Conduct.

SECTION 6. *Preliminary Mediation Conference.* – The Mediation Officer shall receive the appearances of the parties and inform them of the mediation process and the manner by which the proceedings will be conducted. The Mediation Officer shall reiterate the benefits of an early settlement of the dispute and endeavor to achieve the fairest and most expeditious settlement possible.

Each party shall be allowed to make a brief statement of their respective position and preferred outcome. The Mediation Officer shall assist the parties in exploring common grounds for settlement while respecting party autonomy throughout the process.

When necessary, the parties shall agree on the schedule of the next mediation conference and the Mediation Officer shall issue an order therefor.

SECTION 7. *Separate caucuses and subsequent conferences.* – The Mediation Officer may, with the consent of both parties, hold separate caucuses with each party to enable a determination of their respective real interest in the dispute: *Provided*, that each party shall be afforded equal time and opportunity to ventilate such interest and motivation. The Mediation Officer may call such conferences or caucuses as may be necessary to facilitate settlement.

The Mediation Officer shall hold in confidence any matter disclosed during the separate caucuses and shall exercise reasonable prudence and discretion in the safeguarding of such information.

SECTION 8. *Personal appearance by the parties.* – Individual parties are required to personally appear during mediation conferences. Representatives may appear on behalf of individual parties: *Provided*, that they are authorized by a special power of attorney to appear, offer, negotiate, accept, decide, and enter into a mediated settlement agreement without additional consent or authority from the principal. If the party is a juridical person, the representative must be authorized by a Board Resolution contained in a duly notarized Secretary's Certificate, or any equivalent written authority to offer, negotiate, accept, decide, and enter into a mediated settlement agreement.

No representative shall be allowed to appear in mediation on behalf of a party without proper authorization as verified by the Mediation Officer.

The parties shall inform the LD about changes in representation through a written statement or manifestation along with the corresponding written authority to offer,

negotiate, accept, decide, and enter into a mediated settlement agreement submitted to the Mediation Officer prior to the next scheduled mediation conference. The mediation shall not proceed until and unless the representatives are duly authorized in accordance with this Section.

SECTION 9. ***Failure of parties to appear, effect.*** – If any of the parties fail to appear without justifiable reason for two (2) consecutive mediation conferences at any stage of the proceedings, the Mediation Officer may order its termination and refer the same for the resumption of complaint proceedings: *Provided*, in case of doubt that the party's absence is justified, the Mediation Officer may order for another caucus or conference. The Mediation Officer may require the non-appearing party to explain why said party should not be required to pay treble costs incurred by the appearing party, including attorney's fees, in attending the mediation conferences or caucuses, and be henceforth permanently prohibited from requesting mediation at any other stage of the complaint proceedings before the NPC.

SECTION 10. ***Presence of lawyers in mediation.*** – Lawyers who act as counsels, upon the discretion of the Mediation Officer, may attend the mediation conferences in the role of an adviser and consultant to their clients and shall cooperate with the Mediation Officer towards securing a settlement of the dispute. They shall help their clients comprehend the mediation process and its benefits and assist in the preparation of a mediated settlement agreement and its eventual enforcement.

Lawyers who act as duly authorized representatives of juridical persons may directly attend the mediation conference with all its concomitant rights and obligations.

SECTION 11. ***Venue.*** – Mediation proceedings may either be conducted via videoconferencing technology for the remote appearance and testimony of parties, as provided under Rule XIII, Section 7 hereof, or within the NPC premises, as agreed by both parties. Upon request of both parties, the Mediation Officer may authorize the conduct of a mediation conference at any other venue, provided that all related expenses, including transportation, food, and accommodation, shall be borne by both parties. If a change of venue is requested by one party, it must be with the other's conformity, and they shall agree on the terms of handling the expenses.

SECTION 12. ***Mediation period and extension.*** – The Mediation Officer shall endeavor to achieve a mediated settlement of the dispute within sixty (60) calendar days from the Preliminary Mediation Conference.

Upon reasonable ground to believe that settlement may yet be achieved beyond the initial mediation period of sixty (60) calendar days, the Mediation Officer may extend the mediation period for another thirty (30) calendar days for good cause shown. In all instances, the mediation period shall not exceed ninety (90) calendar days.

SECTION 13. ***Mediated Settlement Agreement.*** – A mediated settlement agreement following successful mediation shall be jointly prepared and executed by the parties or their representatives, with the assistance of their respective counsels, if any. Only the parties or their authorized representatives shall have the authority to confirm the provisions of the mediated settlement agreement and execute the agreement. The execution of a mediated settlement agreement shall terminate the mediation proceedings. The Mediation Officer shall certify that the contents of the agreement

have been explained, understood, and mutually agreed upon by the parties, and that the provisions are not contrary to law, public policy, morals, or good customs.

SECTION 14. *Confirmation Conference.* – The Mediation Officer shall require the parties to attend a confirmation conference prior to the endorsement of their mediated settlement agreement to the Commission. The parties shall present to the Mediation Officer the signed mediated settlement agreement, as well as the evidence of compliance with the stipulation in the agreement, if applicable.

In case of failure of any of the parties to appear for two (2) consecutive confirmation conferences, the Mediation Officer may resolve to submit the parties' mediated settlement agreement to the Commission for confirmation: *Provided,* that the appearing party has agreed to proceed, that the parties have fully complied with all the obligations arising from the provisions of the mediated settlement agreement, that the parties have submitted all the necessary documents, and the LD has duly notified the non-appearing party. In such cases, the non-appearing party's right to amend, object, or revoke specific provisions in the mediated settlement agreement shall be deemed waived.

When the agreement involves future obligations or obligations susceptible to partial fulfillment beyond the mediation period, the party responsible shall submit proof of compliance to the Enforcement Division (EnD).

SECTION 15. *Confirmation by the Commission.* – The Mediation Officer shall issue a resolution submitting the signed mediated settlement agreement to the Commission within thirty (30) calendar days from the date of the confirmation conference. The Commission shall issue a resolution confirming the mediated settlement agreement within thirty (30) calendar days from submission of the resolution and mediated settlement agreement. Copies of the resolution issued by the Commission shall be furnished to the parties, the Investigating Officer, and the Mediation Officer.

SECTION 16. *Effect of confirmed Mediated Settlement Agreement.* – A confirmed mediated settlement agreement shall have the effect of a decision or judgment on the complaint but without prejudice to Rule X of these Rules and shall be enforced in accordance with the NPC's rules and issuances.

SECTION 17. *Failure to reach settlement.* – If the parties are unable to arrive at a settlement of their dispute, or it becomes apparent that a settlement, given the disparity of the respective positions of the parties, is not likely or achievable within the sixty (60) calendar day mediation period or the reasonable extension of such period under Section 12 of this Rule, the Mediation Officer may declare the mediation unsuccessful and terminate the proceedings by issuing a Notice of Non-Settlement of Dispute and furnishing copies to the Investigating Officer and the parties.

Parties may be allowed to re-apply for mediation despite a prior failure to reach settlement, unless otherwise permanently prohibited in accordance with Section 9 of this Rule: *Provided,* that the application is filed before the endorsement of the case for decision by the Commission: *Provided further,* that the application is done in compliance with this Rule.

SECTION 18. ***Resumption of complaint proceedings.*** – Upon receipt of the Notice of Non-Settlement of Dispute issued by the Mediation Officer, the Investigating Officer shall issue an order lifting the suspension of the complaint proceedings, which shall resume as a matter of course. Copies of the order, including the notice of the next hearing date of the complaint proceedings, shall be furnished to all the parties.

SECTION 19. ***Confidentiality of proceedings.*** – The mediation conferences shall be held in private. Persons other than the parties, their representatives, counsel, and the Mediation Officer may attend only with the consent of the parties and upon approval by the Mediation Officer. Anyone present during a mediation conference shall not disclose any information obtained during the conference to any other person, nor utter the same through other means.

The mediation proceedings and all related incidents shall be kept strictly confidential, and all admissions or statements shall be inadmissible for any purpose in any proceeding, unless otherwise specifically provided by law. However, evidence or information that is otherwise admissible or subject to discovery does not become inadmissible or protected from discovery solely by reason of its use in mediation.

No transcript or minutes of the mediation proceedings shall be taken, and the personal notes of the Mediation Officer, if any, shall likewise be inadmissible nor cognizable in any court, tribunal, or body for whatever purpose and shall be securely destroyed upon termination of the mediation proceedings.

SECTION 6. Rule VII, Section 3 of the 2021 NPC Rules of Procedure is hereby amended to read as follows:

"SECTION 3. ***Fact-Finding Report.*** – Within thirty (30) calendar days from the last day of the reglementary period to file memoranda, the Investigating Officer shall submit to the Commission a Fact-Finding Report, including the results of the investigation, the evidence gathered, and recommendations. Within ten (10) calendar days from submission of the Fact-Finding Report to the Commission, both parties shall be furnished with a notice that the case has been submitted for decision to the Commission.

For cases recommended for outright dismissal under Rule IV, Section 1 of these Rules, the Investigating Officer shall submit to the LEO Director a Fact-Finding Report, including the basis and recommendation for outright dismissal of the complaint."

SECTION 7. Rule VIII of the 2021 NPC Rules of Procedure is hereby amended and renumbered to read as follows:

"RULE VIII – DECISION

SECTION 1. ***Action on the recommendations of the Investigating Officer.*** – The Commission shall review the evidence presented, including the Fact-Finding Report and evidence on record. On the basis of the review, the Commission may: (1) promulgate a decision; (2) issue interlocutory orders on matters affecting personal data; or (3) order the conduct of a clarificatory hearing or the submission of additional documents, if in its discretion, additional information is needed to make a decision.

No motion for clarificatory hearing shall be entertained. In case the Commission finds that a clarificatory hearing is necessary, the following shall be observed:

a. The parties shall be notified of the scheduled clarificatory hearing at least five
(5) calendar days before the schedule;

b. The Commission may require additional information and compel attendance of any person involved in the complaint;

c. The parties shall not directly question the individuals called to testify but may submit their questions to the Commission for its consideration;

d. The Commission may require the parties to submit their respective memoranda containing their arguments on the facts and issues for resolution.

SECTION 2. ***Additional issues to be raised before the Commission.*** – Upon motion, both parties may raise as an issue during adjudication any interlocutory order or decision issued by the Investigating Officer, Evaluating Officer, special committee, or task force, as the case may be. The Commission, in its discretion, may resolve the issues separately or jointly with the merits of the case.

Once a given case has reached the Commission for adjudication, the Investigating Officer, Evaluating Officer, special committee, or task force shall transmit to the Commission any pleadings, motions, and other submissions erroneously filed subsequent to the endorsement of the main case to the Commission. Subject to the discretion of the Commission, these pleadings, motions, and other submissions may form part of the main case.

SECTION 3. ***Decision for Cases Dismissed Outright.*** – The LEO Director shall review the evidence presented, including the Fact-Finding Report and the evidence on record. Based on the review, the LEO Director may: (1) promulgate a decision dismissing the case outright based on the grounds in Rule IV, Section 1 of these Rules; or (2) remand the complaint for investigation and require the respondent to file a verified comment to the complaint and appear for preliminary conference. *Provided*, the dismissal shall be without prejudice to the refiling with the NPC in accordance with the Rules, or filing of appropriate civil, criminal, or administrative cases against the respondent before any other forum or tribunal, if any.

SECTION 4. ***Decision for Cases where Complainant files an Affidavit of Desistance.*** – The LEO Director shall review the evidence presented, including the Fact-Finding Report, evidence on record, and any other supporting documents. Based on the review, the LEO Director shall promulgate a decision. The dismissal shall be with prejudice to the refiling with the NPC, but without prejudice to the filing of appropriate civil, criminal, or administrative cases against the respondent before any other forum or tribunal, if any.

SECTION 5. ***Refiling of complaint or motion for reconsideration on the decision issued by the Legal and Enforcement Office.*** – The complainant may refile the complaint with the NPC or file with the LEO a motion for reconsideration of the decision dismissing the case outright. Otherwise, the decision of the LEO Director shall become final and executory within fifteen (15) calendar days from notice thereof

with proof of service on the adverse party. If the complainant files a motion for reconsideration, the motion for reconsideration shall be endorsed to the Commission for its resolution within fifteen (15) calendar days from the LEO Director's receipt of such motion.

SECTION 6. ***Rendition of decision.*** – The decision of the Commission shall resolve the issues on the basis of all the evidence on record and its own consideration of the law. The decision may include enforcement orders on the following:

a. an award of indemnity on matters affecting personal data protection, or rights of the data subject, where the indemnity amount to be awarded shall be determined based on the provisions of the Civil Code;

b. a permanent ban on the processing of personal data;

c. a recommendation to the Department of Justice for the prosecution and imposition of penalties specified in the DPA;

d. an order to conduct a *sua sponte* investigation under Rule X such as in cases when the responsible officer of a juridical entity must be determined for recommendation to the Department of Justice for prosecution;

e. an order to compel or petition any entity, government agency, or instrumentality to abide by its orders or take action on a matter affecting data privacy;

f. an imposition of fines for violations of the DPA or NPC issuances; or

g. any other order to enforce compliance with the DPA.

SECTION 7. ***Motion for reconsideration on the decision issued by the Commission.*** **–** The decision of the Commission shall become final and executory fifteen (15) calendar days from notice thereof with proof of service to the adverse party. One motion for reconsideration may be filed, which shall suspend the running of the period. Any appeal from the decision shall be to the proper courts, in accordance with law and the rules.

SECTION 8. ***Entry of judgments and final orders.*** — If no appeal or motion for reconsideration is filed within the time provided in these Rules, the judgment shall attain finality, and an entry of judgment shall be issued to the parties. The date when the judgment becomes executory shall be deemed as the date of its entry. The entry of judgment shall contain the dispositive portion of the judgment with a certificate that such judgment has become final and executory."

SECTION 8. Rule X of the 2021 NPC Rules of Procedure is hereby amended and renumbered to read as follows:

"RULE X – *SUA SPONTE* INVESTIGATION

SECTION 1. ***Commencement.***– The NPC, through the CID or a special committee or task force assigned for such purpose, may initiate an investigation on the circumstances surrounding a possible data privacy violation or data breach in cases of, but not exclusive to, matters that arose from pending cases before the NPC, including those that have resulted in a confirmed mediated settlement agreement, reports from the daily news, trends or academic studies, information gathered from corroborated and substantiated anonymous tips, or reports from other offices of the NPC or government agencies.

SECTION 2. ***Temporary and permanent ban on processing of personal data.*** – A temporary or permanent ban on processing of personal data may be imposed on the subject of a *sua sponte* investigation in order to protect national security or public interest, or if it is necessary to preserve and protect the rights of data subjects, in accordance with Rule IX of these Rules.

SECTION 3. ***Assignment of Investigating Officer or special committee or task force.*** – The Commission may, when it deems proper, assign an Investigating Officer or create a special committee or task force which shall be specifically assigned to conduct the investigation.

SECTION 4. ***Conduct of sua sponte investigation.*** **–** The Investigating Officer or special committee or task force shall investigate the circumstances surrounding the privacy violation or data breach, subject to due process requirements under the law. Investigations may include on-site examination of systems and procedures. In the course of the investigation, the parties subject of the investigation may be required to furnish additional information, document, or evidence, or to produce additional witnesses, or to appear for an investigation hearing or clarificatory conference before the Investigating Officer, special committee, or taskforce, or the Commission, in accordance with Rule VIII, Section 1.

SECTION 5. ***Request for case files during the conduct of a sua sponte investigation.*** – Within fifteen (15) calendar days upon receipt of a request for case files by the parties- in-interest subject of the investigation, or their representative, legal heirs and assigns, or successors-in-interest, the CID shall release the requested case files to the requesting party. The representative shall be authorized by a special power of attorney. In case a party is a juridical person, the representative shall be authorized to appear and act on behalf of the juridical person by a Board Resolution contained in a duly notarized Secretary's Certificate or its equivalent for a government agency[8].

The requested case files may be in the form of a physical copy or an electronic copy. For physical copies, the same be in the form of a copy only or a certified true copy, at the option and cost of the requesting party. For electronic copies, the same be issued to the requesting party and duly protected by a password.

The requested case files shall include documents and communications between the requesting party and the NPC, together with its attachments. Documents that are internal in nature, such as, but not limited to, Technical Reports, Minutes of the

8 This includes a department, bureau, office, instrumentality, government-owned or controlled corporation, local government, state university and college, or a distinct unit in it.

Meeting, and Memorandum within the NPC, shall be excluded. Third-party reports and submissions shall also be excluded.

SECTION 6. ***Sua Sponte Fact-Finding Report.*** – Within thirty (30) calendar days from the termination of the investigation, the Investigating Officer or special committee or task force shall submit to the Commission a Fact-Finding Report, which shall include the results of the investigation, the evidence gathered, and any recommendations. In a *sua sponte* investigation, the Fact-Finding Report serves as the complaint, with the CID as the nominal complainant.

SECTION 7. ***Order to comment.*** – Upon receipt by the Commission of the Fact-Finding Report, the respondent identified after the conduct of the preceding investigation shall be provided a copy of the Fact-Finding Report and its annexes and given an opportunity to submit a comment or other pleadings, if necessary. In cases where the respondent or respondents fail without justification to submit a comment or appear before the NPC when so ordered, the Commission shall render its decision on the basis of available information under Rule VIII of these Rules.

SECTION 8. ***Existence of a complaint during sua sponte investigation and vice versa, effect.*** – If, during the proceedings of a *sua sponte* investigation, a formal complaint relating to the same act or omission for violation of the DPA is filed against the respondent, the complaint proceedings shall follow the normal procedure under these Rules: *Provided*, that the complaint proceedings shall not suspend the *sua sponte* proceedings, or vice versa: *Provided further*, that discovery and mediation proceedings under Rule V shall be available to the parties of the complaint proceedings: *Provided finally*, that a mediated settlement agreement shall only terminate the complaint proceedings but not the *sua sponte* investigation.

The preceding paragraph shall likewise apply if the complaint proceedings occurred first, and the NPC wishes to initiate a *sua sponte* investigation thereafter."

SECTION 9. Rule XI of the 2021 NPC Rules of Procedure is hereby amended to read as follows:

"RULE XI – BREACH INVESTIGATION

SECTION 1. ***Procedure for data breach notification.*** **–** The procedure for data breach notification and other requirements shall be governed by the DPA, its IRR, and NPC issuances pertaining to data breach management. These Rules shall apply in a suppletory character.

SECTION 2. ***Receipt of data breach notifications.*** – The CMD shall be the initial recipient of data breach notifications and shall immediately assign an Evaluating Officer to review the data breach notification.

SECTION 3. ***Preliminary requests that shall be resolved by CMD.*** **–** Upon receipt of the data breach notification, the Evaluating Officer shall recommend to resolve preliminary requests from the PIC or PIP for (a) extensions to notify data subjects or

(b) extensions to file full breach report. The preliminary requests for extensions granted by the CMD shall be for a period of twenty (20) calendar days counted from the date of the request.

SECTION 4. *Preliminary requests and related Motions that must be endorsed to the Commission.* – The CMD shall endorse to the Commission the following requests from the PIC or PIP:

a. On notification of data subjects:
    i Request for exemption;
    ii Request for postponement;
    iii Request for extension beyond twenty (20) calendar days; or
    iv Request for use of alternative modes of notification.

b. On submission of full report:
    i Request for extension beyond twenty (20) calendar days; or
    ii Subsequent request for extension.

c. Other preliminary requests not covered by the preceding Section.

d. Motion for Reconsideration filed by the PIC or PIP on their preliminary request and other related pleadings.

The Commission may delegate to the CMD the resolution of Section 4 (a)(iii) and (b) as deemed necessary.

SECTION 5. *Initial breach notification evaluation and monitoring.* – The Evaluating Officer shall review the completeness of the data breach notification and determine the other documents needed to assess the PIC or PIP's breach management. The PIC or PIP may be directed to submit additional documents through an order.

Further, the CMD shall monitor the compliance of the PIC or PIP with the periods provided in the NPC issuances on data breach and the subsequent extensions allowed under the preceding sections.

In case of non-compliance, the CMD may apply for a Cease-and-Desist Order in accordance with the NPC issuances pertaining to the matter.

SECTION 6. *Final breach notification evaluation.* – Upon receipt of all the documents required to assess the PIC or PIP's breach management, the Evaluating Officer shall prepare a Breach Notification Evaluation Report based on information available on record.

The report may contain a recommendation of a possible violation of the DPA arising from the breach matter and a recommendation for the imposition of administrative fines on other infractions.

Upon the finding of a possible data privacy violation that requires further investigation, the CMD shall endorse the Final Breach Notification Evaluation Report to the Commission for the resolution of the breach case while endorsing the matter to the CID for further investigation for a possible data privacy violation.

SECTION 7. *Conduct of breach investigation.* – Upon receipt of the Final Breach Notification Evaluation Report, an Investigating Officer shall determine if there is a

necessity to conduct an on-site or technical investigation. The Investigating Officer shall request proper authority from the NPC before conducting any on-site or technical investigation. The Investigating Officer may also request assistance from the technical personnel of the NPC. In the course of the investigation, the complainant and respondent may be required to furnish additional information, document, or evidence, or to produce additional witnesses.

SECTION 8. ***Fact-Finding Report*** – The Investigating Officer shall submit to the Commission a Fact-Finding Report within thirty (30) calendar days from the termination of the on-site or technical investigation or receipt of the Final Breach Notification Evaluation Report, whichever is applicable.

SECTION 9. ***Order to comment.*** – Upon receipt by the Commission of the Fact-Finding Report, the respondent identified after the conduct of the preceding investigation shall be provided with a copy of the Fact- Finding Report and its annexes and given an opportunity to submit a comment or other pleadings, if necessary. In cases where the respondent fails without justification to submit a comment or other pleadings, or appear before the NPC when so ordered, the Commission shall render its decision on the basis of available information under Rule VIII of these Rules.

SECTION 10. ***Failure to submit breach notification.*** – Should the NPC receive information that a possible data breach occurred but the PIC or PIP did not submit any notification to the NPC, the CID may use this information to initiate a *sua sponte* investigation under Rule X.

During the *sua sponte* investigation, if a breach notification is submitted by the PIC or PIP, the CID shall continue with its *sua sponte* investigation on violations of the DPA and NPC issuances for possible recommendations for prosecution with the Department of Justice or imposition of administrative fines. The CMD shall, for its part, evaluate the breach matter submitted and recommend the imposition of administrative fines, if warranted.

SECTION 11. ***Post-breach monitoring and compliance.*** **–** The CMD shall monitor compliance of PICs or PIPs with the orders and resolutions issued by the Commission during its evaluation of the data breach matter.

The EnD shall ensure the enforcement and monitoring of compliance of all other judgments, resolutions, decisions, or orders issued by the Commission.

SECTION 10. This Rule has been included to read as follows:

"**RULE XII – COMPLIANCE CHECKS**

SECTION 1. ***Procedure for Compliance Checks.*** **–** The procedure for Compliance Checks and other requirements shall be governed by the DPA, its IRR, and NPC issuances pertaining to Compliance Checks. These Rules shall apply in a suppletory character.

SECTION 2. ***Conduct of Privacy Sweep.*** – The CMD shall conduct a Privacy Sweep of all publicly available or accessible information, including, but not limited to

websites, mobile applications, raffle coupons, brochures, privacy notices, social media pages or accounts, and physical or digital forms of a PIC or PIP.

SECTION 3. ***On-the-spot Privacy Sweep.*** – The CMD may also conduct on-the-spot Privacy Sweep on the premises, pop-up stores, kiosks, or stalls of a PIC or PIP where personal data is processed. The Privacy Sweep shall be limited to public areas and publicly available or accessible information. The CMD may verify the PIC or PIP's compliance by examining all physical or digital forms, including, but not limited to data processing systems, logbooks, raffle coupons, brochures, and posters used in the PIC or PIP's operations.

SECTION 4. ***Issuance of Warning Letter or Notice of Documents Submission.*** –

a. Warning Letter: when applicable – The CMD shall issue a Warning Letter in the following instances:
   i. If after a Privacy Sweep, the CMD discovers data privacy issues involving a PIC or PIP who has not yet registered or whose registration has expired in accordance with the relevant NPC Circular on Registration; or
   ii. If the CMD determines that the risk to the rights and freedoms of a data subject is present, and requires the PIC or PIP's urgent and immediate action.

b. Notice of Documents Submission: when applicable – The CMD shall issue a Notice of Document Submission in the following instances:
   i. If after a Privacy Sweep, the CMD discovers that the PIC or PIP has failed to demonstrate substantial compliance with the DPA, its IRR, and other NPC issuances;
   ii. If the CMD requires additional information to fully determine the PIC or PIP's level of compliance; or
   iii. If the CMD requires further verification to determine if the PIC or PIP has embedded data privacy policies and data protection measures in its operations.

SECTION 5. ***Review and assessment of documents submitted by the PIC or PIP.*** **–** The Evaluating Officer shall review the sufficiency of the documents submitted by the PIC or PIP and determine other documents necessary to assess the PIC or PIP's compliance. The PIC or PIP may be directed to submit additional documents.

The CMD shall monitor all compliance of the PIC or PIP, including the submission within the periods provided in the NPC's issuances on compliance checks and the subsequent extensions allowed under Section 6 of this Rule.

SECTION 6. ***Request for extension that shall be resolved by CMD.*** **–** If the PIC or the PIP requests for additional time to comply with the Warning Letter, Notice of Documents Submission, Deficiency Report, or other orders issued by the CMD, the CMD may grant the request: *Provided,* that the PIC or PIP shall submit a formal letter with a justification for the extension, signed by the Data Protection Officer (DPO) or head of the organization, requesting for additional time which shall not exceed a cumulative period of thirty (30) calendar days counted from the date of the initial request. In case of refusal of the request for extension, the CMD shall send the denial of the request for extension and order the PIC or PIP to submit the same immediately.

SECTION 7. ***Failure of the PIC or PIP to comply with the Warning Letter.*** **–** If the PIC or PIP fails to comply within seven (7) calendar days from receipt of the Warning Letter, the CMD shall order the PIC or PIP to show valid cause why it should not be subject to the NPC's issuance on administrative fines and other actions that the Commission may deem proper to ensure compliance with the law.

SECTION 8. ***Failure of the PIC or PIP to comply with the Notice of Documents Submission.*** **–** If the PIC or PIP fails to comply within fifteen (15) calendar days from receipt of the Notice of Documents Submission, the CMD shall order the PIC or PIP to show valid cause why it should not be subject to the NPC's issuance on administrative fines and other actions the Commission may deem proper to ensure compliance with the law.

SECTION 9. ***Show cause order for non-compliance with the mandatory registration requirement of the NPC.*** – If based on the findings in the Privacy Sweep conducted by the CMD, the PIC or PIP is subject to mandatory registration but has failed to register, the CMD shall issue a show cause order for non-registration directing the PIC or PIP to register its DPO and Data Processing Systems within five (5) calendar days from receipt of the order. Non-compliance with the show cause order may subject the PIC or PIP to administrative fines and other actions the Commission may deem proper to ensure compliance with the law.

SECTION 10. ***Conduct of On-Site Visit (OSV).*** **–** The CMD shall conduct an OSV to the PIC or PIP's principal place of business or where personal data is processed in cases where there are persistent issues[9] or substantial findings of ~~non-compliance with the obligations indicated in the DPA and NPC issuances.~~

Authorized personnel of the NPC shall conduct a focused inspection on the relevant issues within the premises of a PIC or PIP that may include presentation of documents or records, visits to selected departments or units wherein processing of personal information are undertaken, taking of photos and videos for monitoring purposes, and interviews of relevant personnel tasked to handle personal information processed by the PIC or PIP subject to the Compliance Check.

The CMD may, in its discretion, directly conduct an OSV if it determines that the totality of circumstances warrant such action, taking into account the succeeding provision.

SECTION 11. ***Considerations for the conduct of Compliance Checks.*** – A PIC or PIP may be subject to a Compliance Check based on any of the following considerations:

a) Level of risk to the rights and freedoms of data subjects posed by personal data processing by a PIC or PIP;
b) Reports received by the NPC against the PIC or PIP, or its sector;
c) Non-registration of a PIC or PIP that is subject to the mandatory registration requirement as provided under NPC Circular on Registration of Data Processing System;
d) Unsecured or publicly available personal data found on the premises and on the internet that may be traced to a PIC or PIP;

---

[9] Persistent issues pertain to the inadequate implementation of security measures to address the heightened risk to the rights and freedoms of data subjects.

e) Other considerations that indicate non-compliance with the DPA, IRR, or NPC issuances; and

f) When, in the discretion of the CMD, there is an urgent need to ensure the protection of voluminous personal data records and the same can only be done by actual physical inspection of said records within the PIC's or PIP's office premises.

In cases where the CID is investigating or commencing an investigation against a PIC or PIP undergoing or scheduled for a Compliance Check, the Compliance Check shall be held in abeyance and the investigation shall be given precedence until such investigation has been concluded or submitted further for adjudication.

SECTION 12. *Service of orders.* – The CMD shall send an order to a PIC or PIP on the conduct of a Compliance Check through the electronic mail address used at the time it registered with the NPC. Such order shall be deemed received on the next business day: *Provided,* for unregistered organizations, the order shall be sent to any publicly available email address that may be found on websites or other social media pages or accounts and it shall be addressed to the head of the organization.

A PIC or PIP shall take the necessary steps to ensure that its registered e-mail address is working and able to receive the order promptly.

SECTION 13. *Notice of On-Site Visit.* – A notice of OSV shall be issued by the CMD to the PIC or PIP at least five (5) days before such visit. The notice shall include a list of required documents to be submitted by the PIC or PIP at least three (3) days prior to the OSV.

The CMD shall present the physical copy of the notice and provide the list of authorized personnel of the NPC to conduct the OSV. The authorized NPC personnel shall wear their identification cards at all times.

SECTION 14. *Issuance of Deficiency Report.* – The CMD shall issue a Deficiency Report based on the determination from the OSV that there are existing gaps in the PIC or PIP's compliance with the DPA, its IRR, and NPC issuances.

SECTION 15. ***Issuance of Notice of Deficiencies***. – If the PIC or PIP fails to address the issues raised in a Deficiency Report or is determined to be non-compliant with the DPA, its IRR, and other issuances of the NPC after being subjected to any of the modes of Compliance Checks, the CMD shall issue the Notice of Deficiencies indicating the period of time within which to correct the identified deficiencies, which shall not be less than ten (10) days from receipt of the Notice.

SECTION 16. Issuance of Compliance Order. – The Commission shall issue a Compliance Order in any of the following instances:

a) After the lapse of the period provided in the Notice of Deficiencies and no action was taken by the PIC or PIP to correct the identified deficiencies;

b) After the lapse of the period provided in the Notice of Deficiencies and such identified deficiencies persist.

If the persistence of the deficiencies is due to the considerable period of time or resources needed to implement the necessary remediation measures, the timeline to complete such measures, as approved by the Commission, shall be embodied in a Compliance Order;

c) In the course of the conduct of an OSV, the PIC or PIP refuses or fails to provide access to premises, records or prevents the conduct of the inspection; or

d) In the course of the conduct of the on-the-spot Privacy Sweep, the PIC or PIP refuses or prevents the conduct of the inspection on otherwise publicly available areas or information.

Compliance Orders shall state the deficiencies remaining or actions to be taken, the period within which to undertake the corrections ordered by the Commission, and the period to report such actions.

SECTION 17. *Issuance of other orders.* – The Commission, through the CMD, may issue pertinent orders in connection with the conduct or furtherance of a Compliance Check or the assessment of any PIC or PIP's compliance with any orders in relation thereto.

SECTION 18. *Refusal to undergo Compliance Check.* – A PIC or PIP who, without good reason and despite due notice, refuses or prevents the CMD from performing a Compliance Check may be subject to appropriate penalties and sanctions as may be allowed by law. In case of refusal, the following provisions shall govern:

A. *Action to be taken upon refusal or failure to comply with documents submission.* Refusal or failure to submit the requested documents or policies within the period stated in the notice or order shall subject a PIC or PIP to an OSV from the CMD, enforcement actions, and imposition of fines in accordance with the NPC's issuance on administrative fines and other actions the Commission may deem proper to ensure compliance with the law.

B. *Action to be taken upon refusal or failure to provide access to premises or records during an OSV and on-the-spot Privacy Sweep.* Refusal or failure to provide access to premises or records during an OSV and on-the-spot Privacy Sweep shall subject a PIC or PIP to a Compliance Order, enforcement actions, and imposition of fines in accordance with the NPC's issuance on administrative fines and other actions the Commission may deem proper to ensure compliance with the law.

C. *Failure or refusal to provide an explanation to Compliance Orders.* Refusal or failure to submit an explanation to the order cited in the preceding paragraphs, or if the explanation does not present a compelling reason to justify such refusal or failure, may subject a PIC or PIP to contempt proceedings, as may be permitted by law, before the appropriate court, or such other actions as may be available to the Commission.

SECTION 19. *Certificate of No Significant Findings.* – The CMD shall issue a Certificate of No Significant Findings to a PIC or PIP that has undergone document

submission or an OSV, where no substantial deficiencies were found, or the deficiencies identified in the Deficiency Report or Notice of Deficiencies have already been addressed to the satisfaction of the NPC.

The issuance of this certificate is without prejudice to any other recommendation being made by the CMD for the improvement of the PIC or PIP's compliance with the DPA, IRR, and NPC issuances. The issuance of this certificate does not bar an investigation for any possible liability arising from complaints and/or personal data breaches filed before the NPC."

SECTION 11. Rule XII of the 2021 NPC Rules of Procedure is hereby amended and renumbered to read as follows:

"RULE XIII – MISCELLANEOUS PROVISIONS

SECTION 1. ***Transitory provision.*** – These Rules shall apply to all complaints filed after its effectivity. It shall also apply to pending proceedings, except to the extent that their application would not be feasible or would work injustice.

SECTION 2. ***Procedure for Cease-and-Desist Orders.*** **–** Procedure for the issuance of Cease-and-Desist Orders shall be governed by NPC issuances pertaining to the matter.

SECTION 3. ***Procedure for breach notification.*** **–** Procedure for data breach notification to the Commission shall be governed by the NPC issuances pertaining to the matter.

SECTION 4. ***Request for case files.*** **–** Copies of the case files may be requested by any party to the complaint or their authorized representative, lawful heirs, and assigns, in accordance with Section 17 of the DPA, or successors-in-interest, by filling-out the request form before the General Records Unit of the NPC. The request for case files may be in the form of a physical copy or an electronic copy, at the option and cost of the requesting party. *Provided*, that the representative is authorized by a special power of attorney. *Provided further*, that in case where a party is a juridical person, the representative is authorized by a Board Resolution contained in a duly notarized Secretary's Certificate or its equivalent for a government agency[10]. *Provided finally*, that in case where the files are requested by the heirs, assigns, or successors-in-interest, proof of authority or relationship must be presented.

SECTION 5. ***Procedure for requests for advisory opinion.*** **–** Procedure for requests for advisory opinion shall be governed by NPC issuances pertaining to the matter.

SECTION 6. ***Procedure for enforcement of administrative fines.*** – Procedure for the enforcement of administrative fines shall be governed by NPC issuances pertaining to the matter.

SECTION 7. ***Procedure for videoconferencing technology***. - Procedure for the use of videoconferencing technology for the remote appearance and testimony of parties before the NPC shall be governed by NPC issuances pertaining to the matter.

---

[10] This includes a department, bureau, office, instrumentality, government-owned or controlled corporation, local government, state university and college, or a distinct unit in it.

Notwithstanding any provision of these Rules, the conduct of preliminary conferences, summary hearings, mediation conferences, investigations, clarificatory hearings, and all other hearings may be conducted through videoconferencing technology at the discretion of the concerned division or Commission.

SECTION 8. *Repealing clause.* – NPC Circulars No. 2016-04 and 2018-03 are hereby repealed. All other issuances by the Commission which are contrary to the provisions of these Rules are also hereby repealed or amended accordingly.

SECTION 9. *Amendments.* – These Rules or any of its portion may be amended or supplemented by the Commission.

SECTION 10. *Application of Rules of Court.* – The Rules of Court shall apply in a suppletory character and whenever practicable and convenient.

SECTION 11. *Effectivity.* – These Rules shall take effect fifteen (15) days after publication in a newspaper of general circulation."

SECTION 12. *Repealing Clause.* – The Rules not included herein and amended accordingly shall remain in force and full effect. If any part of this issuance is declared unconstitutional or invalid, such provision/s thereof not so declared shall remain valid and subsisting.

SECTION 13. *Effectivity*. – These amendments shall take effect fifteen (15) days after its publication in a newspaper of general circulation.

Approved:

SGD.
ATTY. JOHN HENRY D. NAGA
Privacy Commissioner

SGD.
ATTY. LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD.
ATTY. NERISSA N. DE JESUS
Deputy Privacy Commissioner

NPC Circular No. 2024 – 02

DATE : 9 August 2024

SUBJECT : CLOSED-CIRCUIT TELEVISION (CCTV) SYSTEMS

WHEREAS, the National Privacy Commission (NPC) previously issued NPC Advisory No. 2020-04, or the Guidelines on the Use of Closed-Circuit Television (CCTV) Systems, which provides guidance to all personal information controllers (PICs) and personal information processors (PIPs) on the use of CCTV systems operating in public and semi-public areas;

WHEREAS, CCTV systems process personal and sensitive personal information (collectively, personal data);

WHEREAS, there is a need to provide an updated policy framework on the use of CCTV systems as the technology for such systems is continuously evolving, and the use of the same has become accepted and even mandated in certain instances;

WHEREAS, these guidelines are necessary to address emerging privacy risks, and enable PICs and PIPs to properly manage personal data processing through CCTV systems;

WHEREAS, PICs and PIPs must ensure that the use of CCTV systems adheres to the general principles of privacy and upholds data subjects' rights and freedoms;

WHEREFORE, in consideration of the foregoing premises, the NPC hereby issues this Circular on CCTV systems.

SECTION 1. ***Scope.*** — This Circular shall apply to all PICs and PIPs engaged in the processing of personal data through CCTV systems, except when CCTV systems are used for any of the following purposes:

A. *Personal, family, or household affairs.* This Circular shall not apply to the use of CCTV systems for purely personal, family, or household affairs as defined herein.

   Where CCTV systems capture images of individuals beyond the boundaries of a private and non-commercial residence or establishment, particularly where it monitors a public space, such use cannot be considered purely for personal, family, or household use. As such, the owner of the CCTV systems is a PIC and subject to the corresponding obligations under the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and all relevant issuances of the NPC.

B. *Lawful surveillance*. This Circular shall not apply to law enforcement, intelligence, and investigative agencies and other government agencies conducting lawful surveillance

in accordance with their respective mandates. Nonetheless, they shall be subject to the applicable requirements of the Philippine Constitution and other laws and regulations regulating surveillance activities.

SECTION 2. ***Definition of Terms.*** — The definition of terms used in the DPA and its IRR, as amended, and other NPC issuances are adopted herein. In addition, whenever used in this Circular, the following terms are defined as follows:

A. "Commission" refers to the Privacy Commissioner and the two (2) Deputy Privacy Commissioners, acting as a collegial body;

B. "Closed-Circuit Television" or "CCTV" refers to closed-circuit television or camera surveillance systems in a fixed or stationary location that can capture images of individuals or other information relating to individuals;

C. "Masking" refers to the process of obscuring or hiding parts of a video or image from being viewed, like blurring or covering faces, body parts, or other objects that will reveal personal data;

D. "NPC" refers to the National Privacy Commission created under the DPA;

E. "Personal, family, or household affairs" refers to the uses that are limited to those with no connection to any professional activity and not intended for profit or commercial gain. For purposes of this Circular, this includes the use of CCTV for home security purposes within the premises and boundaries of a private and non-commercial residence or establishment. Nevertheless, the totality of the circumstances surrounding the processing will be considered in determining whether the specific processing activity falls under the exception in Section 1 (A) of this Circular.

   The following factors may be considered in determining whether a specific processing activity falls outside the scope of the personal, family, or household affairs exception:

   1. Dissemination of personal data to an indefinite number of people;
   2. Processing may have an adverse impact on the rights and freedoms of the involved data subjects; or
   3. Processing of personal data about data subjects who have no personal, family, or household relationship with the person engaged in the processing.[1]

F. "Public authority" refers to any government entity created by the Philippine Constitution or law;

G. "Public space" refers to streets and alleys, public parks, schools, buildings, malls, bars, restaurants, transportation terminals, public markets, spaces used as evacuation centers, government offices, public utility vehicles as well as private vehicles covered

[1] See: National Privacy Commission, KEC v. JMP [NPC 19-764] (November 11, 2021) and ARTICLE 29 DATA PROTECTION WORKING PARTY Statement of the Working Party on current discussions regarding the data protection reform package, Annex 2 Proposals for Amendments regarding exemption for personal or household activities (2013).

by app-based transport network services and other recreational spaces such as, but not limited to, cinema halls, theaters and spas;[2]

H. "Semi-public space" refers to any indoor or outdoor space that, even if privately owned, is open or accessible to the public during its operating hours;

I. "Video analytics" refers to any technology that processes a digital video signal using a special algorithm to perform a security-related function. The common types of video analytics are fixed algorithm analytics, artificial intelligence learning algorithms, and facial recognition systems.[3]

SECTION 3. ***General principles.*** — PICs and its PIPs engaged in the processing of personal data through CCTV systems are mandated to ensure that reasonable and appropriate safeguards are in place for the protection of personal data, taking into account the rights of the data subject. For this purpose, PICs and its PIPs shall adhere to the following principles:

A. *Transparency*. PICs shall provide appropriate CCTV notices to inform data subjects of the existence and purpose of CCTV systems in operation. Given that CCTV notices are a specific kind of privacy notice, the requirements for privacy notices as stated in NPC Circular No. 2023-04 or the Guidelines on Consent shall apply. In addition, PICs shall ensure that CCTV notices adhere to the following:

1. Information about the use of CCTV systems shall be made available to the data subjects in the most appropriate format and in clear, plain, and concise language.
2. These CCTV notices shall be readily visible and prominently displayed within the appropriate premises, such as but not limited to, points of entry or other conspicuous areas.
3. The nature, scope, and extent of surveillance, purpose, capabilities of the CCTV systems, and other necessary information shall be provided to the data subjects in accordance with their right to be informed under the DPA.

B. *Legitimate purpose.* PICs shall ensure that the purpose of processing is not contrary to law, morals, or public policy, and that such purpose is clearly determined, specified, and declared to the data subject prior to the use of the CCTV systems.[4]

C. *Proportionality and Data Minimization.* PICs shall ensure that the use of CCTV systems remains necessary and proportional to the specified and declared legitimate purpose. PICs and its PIPs shall regularly review its use of CCTV systems to determine if the purpose of the processing could not reasonably be fulfilled by any other less intrusive means, and if the personal data processed is limited to that which is adequate, relevant, suitable, necessary, and not excessive in relation to the purpose.

D. *Fairness and Lawfulness*. The processing of personal data using CCTV systems shall be neither manipulative, oppressive, nor discriminatory. PICs shall ensure that the means

[2] An Act Defining Gender-Based Sexual Harassment in Streets, Public Spaces, Online, Workplaces, and Educational or Training Institutions, Providing Protective Measures and Prescribing Penalties Therefor [Safe Spaces Act] (2019) Republic Act No. 11313 (2019).
[3] See: Science Direct, Video Analytics, citing Electronics Elements, Thomas L. Norman CPP, PSP, CSC, in Effective Physical Security (Fifth Edition), 2017, available at https://www.sciencedirect.com/topics/computer-science/video-analytics (last accessed 31 March 2023).
[4] National Privacy Commission, MLF v. MYTAXI.PH CORPORATION (GRAB PHILIPPINES) [NPC 19-142] (March 21, 2022).

and method of the processing shall be in accordance with law, morals, public policy, and good customs.

E. *Accountability*. PICs shall be responsible for personal data processed using CCTV systems and shall use contractual or other reasonable means to ensure proper safeguards are in place when the processing is subcontracted to PIPs. PICs shall demonstrate compliance by adhering to the general principles of privacy, implementing safeguards, keeping appropriate records, upholding data subject rights and their other obligations under the DPA, IRR, and relevant issuances of the NPC.

SECTION 4. ***Lawful basis.*** — PICs shall identify the most appropriate lawful basis for processing under the DPA and the same should be provided when required by the Commission.

A. PICs shall determine the more appropriate lawful basis other than the consent of the data subject for the processing of their personal data through the use of CCTV systems. PICs must consider that the purpose of using CCTV systems will vary and consent may not be the most suitable lawful basis in the context of specific processing activities, such as those involving open surveillance in public and semi-public places.

B. The processing of CCTV footage including sensitive personal information shall be based on the most appropriate lawful basis under Section 13 of the DPA.

SECTION 5. ***Safeguards***. — PICs and its PIPs shall implement reasonable and appropriate security measures, including privacy by design principles, to protect personal data processed against accidental, unlawful, or unauthorized use,[5] to minimize privacy intrusion, and to comply with the requirements under the DPA, its IRR, and relevant issuances of the NPC.

A. *Policies*. PICs and its PIPs shall establish policies that govern the operation of CCTV systems, which include:

1. Information on the legitimate purpose;
2. Information on the lawful basis for processing;
3. Regular conduct of privacy impact assessments (PIAs) and regular review of the use of the CCTV systems;
4. CCTV notice and placement thereof;
5. Operational details of the CCTV systems, such as but not limited to, procurement, installation, operation, control, monitoring, maintenance, incident response and reporting;
6. Designation of authorized personnel who shall be responsible for handling access requests, monitoring live feeds, and the day-to-day operation of the CCTV systems;
7. Subject to Sections 6 to 8 of this Circular, the policy shall provide procedures for the following:
    a. Requests for access to CCTV footages, whether for viewing or providing a recording or copy thereof;
    b. Handling inquiries and complaints, if any; and

[5] Data Privacy Act of 2012, § 20 (2012).

c. Managing personal data breaches and security incidents involving the CCTV systems;

8. Documented retention policy containing the retention period of CCTV footage and manner of disposal or destruction when the retention period has lapsed. The documented retention policy shall be included in the CCTV policy;
9. Security measures to be implemented for the protection of CCTV footage against any accidental, unauthorized, or unlawful processing, including access (e.g. copying or viewing), alteration, destruction, or disclosure, and the conduct of regular evaluation and audit of such security measures; and
10. Process for the regular review and assessment of the policy document, audits to determine if the policy is being implemented and complied with, and policy revision and updates.

B. *Deployment and operation*. PICs and its PIPs shall be subject to the following parameters upon the implementation of CCTV systems:

1. *Location and placement*. To ensure that CCTV systems capture footage in a manner consistent with the DPA and to avoid unreasonable intrusions on the data subjects' privacy, the PIC and its PIPs shall thoroughly consider the location and angles of the cameras.
   a. CCTVs shall only be used to monitor the intended spaces, taking into consideration the purpose for such monitoring;
   b. Should the CCTV systems have zoom and rotation capabilities, PICs and PIPs shall ensure that such functionalities will not result in surveillance of private spaces (*e.g.*, private backyards, through windows of private residences); and
   c. Use of CCTVs in areas where individuals have a heightened expectation of privacy (*e.g.*, fitting rooms, rest rooms, toilets, lactation or breastfeeding rooms,) is strictly prohibited.

2. *Quality and integrity of data*. To sufficiently fulfill the intended purposes for installation, PICs shall ensure that the data captured and recorded by CCTV systems be of appropriate and suitable quality. PICs and its PIPs shall implement reasonable and appropriate safeguards to ensure and maintain the integrity and accuracy of the footage recorded and stored, including any associated metadata (*e.g.*, time, date, and location) that may facilitate access requests for CCTV footage.

3. *Storage*. Footage recorded by CCTV systems shall be stored in a secure manner, whereby its confidentiality, integrity, and availability are ensured. The recorded footage shall be encrypted pursuant to the applicable issuances of the NPC.
   a. Without prejudice to the exercise of the right to access of data subjects and third-party access requests, access to the area where the CCTV footage is stored shall be restricted to authorized personnel only;
   b. Access logs for the CCTV footage, including access requests, reproductions, and transfers, shall be updated on a regular basis as determined by the PIC; and
   c. PICs and PIPs shall restrict monitoring of live CCTV feeds to authorized personnel only. It shall identify and state in its CCTV policy the personnel authorized to monitor such live feeds.

4. *Retention.* While there is no specific retention period for CCTV footage, CCTV footage shall be retained only for as long as necessary to fulfill the purpose for which the CCTV footage was obtained.
    a. Retention periods shall not be determined based solely on the storage capacity of CCTV systems.
    b. The retention period shall be clearly documented and form part of the CCTV policy.
    c. CCTV footage shall be destroyed once it is no longer needed for its declared and specified purpose.

5. *Video analytics.* The same requirements shall apply when processing personal data derived from CCTV systems that utilize video analytics. PICs shall utilize PIAs to assess and minimize potential privacy risks.

6. *Assistance of PIPs.* In accordance with Sections 43 and 44 of the IRR, PICs should put in place contractual or other reasonable means to ensure the cooperation and assistance of PIPs they have engaged to process personal data on their behalf.

SECTION 6. ***Data subject request for access.*** — Any person whose personal data is recorded on CCTV systems has a right to reasonable access to the same pursuant to Section 16 of the DPA and Section 34 of the IRR.

A. PICs and PIPs shall establish policies allowing for access, and shall consider the following:

    1. Use of a simple and accessible process for submitting requests for access, which includes viewing and obtaining a copy of CCTV footage;
    2. Verification of the identity of the data subject requesting for access through the presentation of supporting documentation, such as IDs or other similar documents: *provided*, that the information required shall only be to the extent necessary to confirm such identity;
    3. For persons requesting access for and on behalf of another, PICs and its PIPs may request evidence of proper authorization and other supporting documents to validate the authority and identity of the representative as well as to confirm the identity of the requesting party;
    4. Purpose and manner of the request for access, which should not be contrary to law, morals, or public policy; and
    5. Sufficient details on the requested footage such as the specific date, approximate time, and location, to enable PICs and its PIPs to locate such footage.

B. Where images of persons other than the requesting data subject appear on the CCTV footage, such as a specific person sought to be identified as part of the request for identification of malefactors for the protection of lawful rights and interests, establishing legal claims, investigation, or law enforcement purposes, Section 12 (f) or 13 (f) of the DPA may apply as the basis for the disclosure.

SECTION 7. ***Third-party access request.*** — A third-party access request is a request to access CCTV footage made by a person other than the data subject involved in the footage or the latter's authorized representative. If a data subject involved in the footage or their authorized representative requests access to CCTV footage, the presence of another person's

image within the CCTV footage does not automatically classify such request as a third-party access request. Further, in handling third-party access requests, the same policies and procedures outlined in the previous section shall apply.

A. PICs shall decide on the merits of the request for disclosure based on the DPA, IRR, relevant issuances of the NPC, and other existing laws and regulations.

   1. Once a PIC has disclosed information to the requesting party, the latter becomes responsible for the copy they hold. It is the requesting party's responsibility to comply with the DPA, its IRR, and other related issuances of the NPC in relation to any processing of the personal data involved in the CCTV footage requested.
   2. The method for disclosing the requested information should be secure to ensure access only by the intended recipient.

B. Subject to the criteria provided for the lawful processing of personal data under Sections 12 and 13 of the DPA, CCTV footage may be disclosed in the following instances:

   1. *Law enforcement and criminal investigations.* With respect to requests for CCTV footage to be disclosed in relation to a criminal investigation, PICs and its PIPs shall cooperate on the appropriate disclosure of CCTV footage to the authorized law enforcement agencies in connection with the latter's constitutional or statutory functions (*e.g.*, criminal investigations, case build-up).
      a. Law enforcement officers shall provide the PIC to whom the request is made with a written statement, affirmative declaration, or equivalent to establish the lawfulness of the request.
      b. The request for CCTV footage shall be made following, and with strict adherence to, existing standard operating procedures in the conduct of an investigation and law enforcement operation as stated in the applicable rules and regulations of law enforcement agencies and other pertinent public authorities.

   2. *Court Order.* Requests for disclosure and use of CCTV footage and images by virtue of a lawful order of a court of competent authority are allowed, taking into consideration the rules on the issuance of subpoenas.

   3. *Administrative investigations.* The use of CCTV footage for purposes of an administrative investigation shall be allowed. The requesting party shall provide sufficient proof of the investigation being conducted or the pending complaint before an administrative body.

   4. *Request from the media.* PICs and its PIPs are not obliged to release CCTV footages to the media, unless there is a lawful basis for processing under Sections 12 or 13 of the DPA or processing under a special case, specifically Section 4 (d) of the DPA. Further, the disclosure should always be with due regard to the general principles of privacy, rights of data subjects, and codes of conduct and ethical standards of journalism.
      a. PICs and its PIPs are likewise proscribed from disclosing CCTV footages of identifiable individuals to the media for amusement or entertainment purposes, unless it is with the consent of the data subjects. It is incumbent upon

the media to prove that the requested CCTV footage shall not be used for amusement or entertainment purposes.

b. Law enforcement agencies may release CCTV footage to the media on a case- to-case basis taking into account the lawful basis for processing of personal data under Sections 12 and 13 of the DPA, or processing under a special case, considering the requirements of public order and safety, verification or confirmation of identity, and other relevant factors.

c. Where the media's request involves images of individuals other than the specific person sought to be identified for news reporting, the requesting media personnel or journalist must mask the images of those other individuals before making the footage public.

5. *Other third-party requests.* Third-party access requests for CCTV footage and images shall be evaluated with greater scrutiny to prevent violation of the privacy rights of the data subjects concerned.

   a. Upon determination of PICs that the requesting third party's needs outweigh those of the data subjects to whom the CCTV footage and images pertain, it may release information to such requesting third party.

   b. PICs must determine on a case-to-case basis if they will accede to such request taking into consideration the general principles of privacy, the rights and freedoms of the data subjects whose images are recorded by the CCTV systems, and a lawful basis for processing under Section 12 or Section 13 of the DPA.

SECTION 8. ***Response procedure.*** — The following shall be implemented:

A. When the requesting party informs the PIC in writing of its intention to view or obtain a copy of a particular CCTV footage, the PIC and its PIPs shall preserve the pertinent CCTV footage by taking the same out of the coverage of the established retention period as indicated in the documented retention policy until such time as any of the following occur:

   1. The access request is fulfilled;
   2. The access request is abandoned by the requesting party; or
   3. In cases where the requesting party files a complaint questioning the PIC's denial of the access request or the NPC conducts an investigation on the matter, and the Commission affirms the PIC's denial of the request.

   A request is deemed abandoned when the requesting party has not fulfilled the requirements in Section 6 or 7 of this Circular, as the case may be, within thirty (30) days from initially informing the PIC of the intention to either view or obtain a copy of the CCTV footage.

B. Upon fulfillment of the requirements in Sections 6 or 7 of this Circular, PICs and its PIPs shall allow access to the CCTV footage through viewing or providing a copy to the data subject or the third party, as the case may be, taking into consideration the stated purpose for the request.

   1. *Viewing.* The requesting party may be allowed a reasonable opportunity to view the requested footage, subject to the following conditions:

      a. CCTV footage shall be viewed in an authorized and secure area;

b. Only the requesting party and the authorized personnel of PICs and their PIPs shall be allowed to view such footage; and
c. Other security measures to ensure confidentiality of the footage to be viewed shall be implemented, such as signing of non-disclosure agreements or prohibiting the capture of the footage through mobile phones and other devices, where appropriate.

2. *Obtaining a copy of the CCTV footage.* The requesting party may be given copies of the CCTV footage subject to the following conditions:
   a. PICs and their PIPs shall ensure that the copying of footage is made in a secure manner that maintains the integrity of the footage and any associated metadata.
   b. In circumstances where there is technical difficulty in providing a copy of the footage in video format, PICs and their PIPs may provide still images as an alternative. Where still images are provided, it would be necessary to supply sufficient stills for the duration of the requested footage.
   c. PICs or their PIPs may charge the data subject or third party a reasonable fee to cover administrative costs for providing a copy of the footage. For this purpose, PICs or their PIPs shall not impose excessive fees in order to discourage such requests.

SECTION 9. ***Period for complying with the request.*** — Requests shall be acted upon without undue delay.

A. The period shall not exceed five (5) working days from receipt of the request when the request is for viewing only. The period shall not exceed fifteen (15) working days from the receipt of the request when the request involves obtaining a copy of the CCTV footage.

   The request is considered submitted at the time the requesting party complies with the requirements stated in Section 6 or 7 of this Circular, as the case may be.

B. If a request is complex or involves numerous footage, whether for viewing or obtaining a copy of the CCTV footage, the period to comply with such request may be extended for an additional period not exceeding fifteen (15) working days.

C. In case of an extension, PICs or its PIPs shall notify the data subject or the authorized representative in writing of the intended date of compliance and the reason for the extension.

SECTION 10. ***Denial of request.*** — Requests for access to CCTV footage may be denied upon appropriate evaluation.

A. The following are grounds for denial:

   1. Incomplete information regarding the requested CCTV footage, as stated in Section 6: *provided,* that the data subject, their authorized representative, or third party is first given a reasonable opportunity to amend the request and provide complete information;

2. The access request is frivolous or vexatious. The determination of what constitutes frivolous or vexatious may be made on the basis of the particular circumstances of the request;
3. The purpose for and manner of viewing or obtaining a copy of the footage is contrary to law, morals, or public policy;
4. The request to obtain a copy of the CCTV footage is disproportional to the purpose stated by the requesting party;
5. The burden or expense of providing access would be unreasonable or involve disproportionate effort on the part of the PIC or its PIP;
6. The footage has already been deleted by the time the PIC or its PIP received the request pursuant to its documented retention policy as stated in Section 5(A)(8) of this Circular; or
7. If disclosure of the footage could put an ongoing criminal investigation at risk as determined by the appropriate public authority. For this purpose, the PIC should provide written proof of this determination.

B. PICs can only deny a request after giving the data subject or third party a reasonable opportunity to amend the request. Should the PIC deny a request for CCTV access, it shall provide the requesting party with the reason for the denial within five (5) working days from receipt of the request: *provided*, that the denial shall not serve as a bar for future requests by the same data subject or third party which complies with Section 6(A)(5) of this Circular on the sufficiency of details on the requested footage.

The determination of the reasonableness of the denial of a request shall be made upon the initiation of an investigation by the NPC or upon the filing of a complaint, pursuant to the NPC's Rules of Procedure.

SECTION 11. ***Interpretation.*** — Any doubt in the interpretation of any provision of this Circular shall be interpreted in a manner mindful of the rights and interests of the data subject, and without prejudice to the application of other pertinent laws and regulations on the matter.

SECTION 12. ***Penalties.*** — The processing of personal data in violation of this Circular shall carry criminal, civil, and administrative liability pursuant to the provisions of the DPA, its IRR, and related issuances of the NPC.

SECTION 13. ***Transitory Provisions.*** — PICs and PIPs shall be given a period of sixty (60) calendar days from the effectivity of this Circular to comply with the requirements provided herein.

SECTION 14. ***Separability Clause.*** — If any portion or provision of this Circular is declared null and void, or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 15. ***Repealing Clause.*** — All other rules, regulations, and issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

SECTION 16. ***Effectivity***. — This Circular shall take effect fifteen (15) calendar days after its publication in the Official Gazette or a newspaper of general circulation.

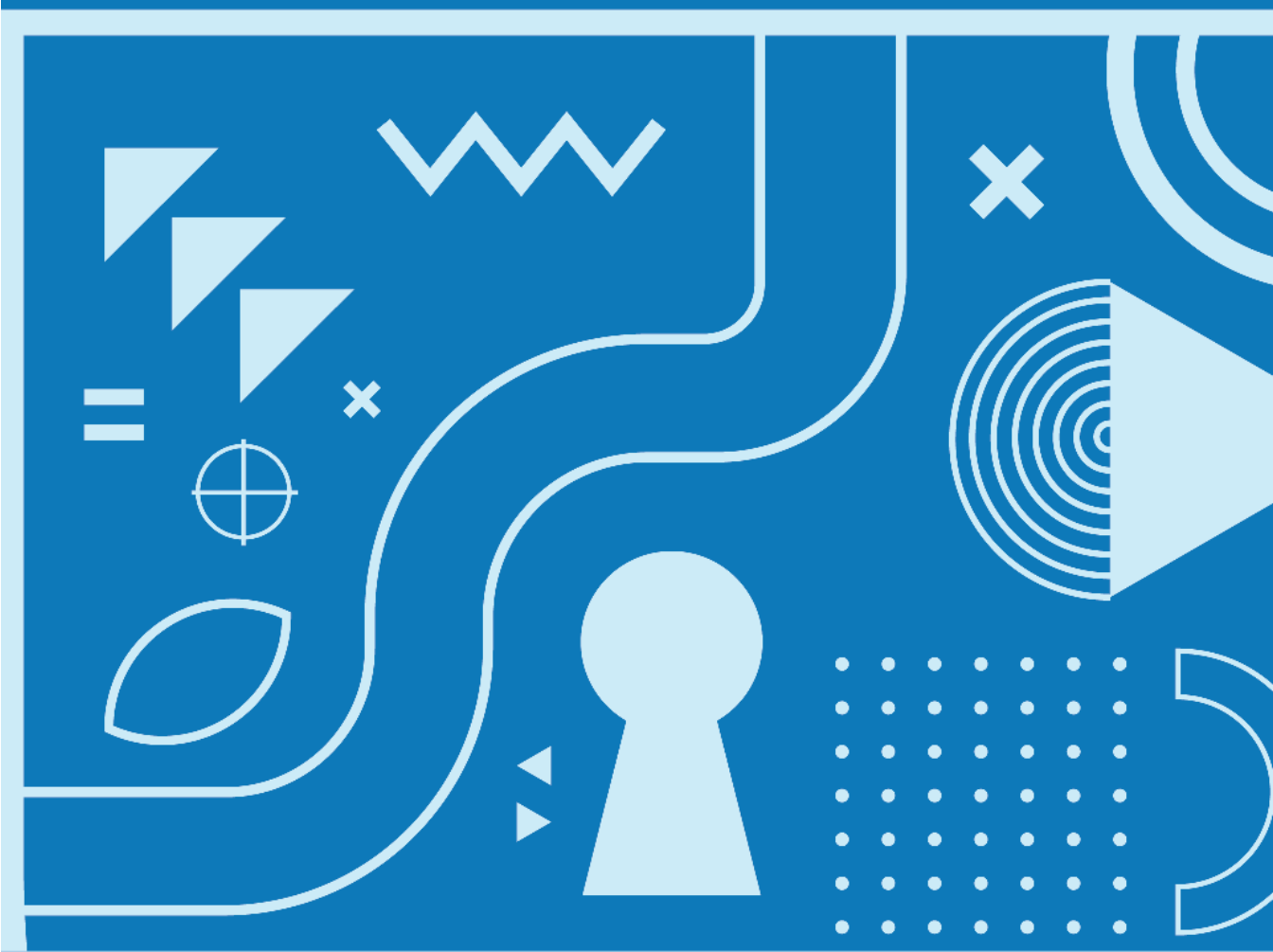
Approved:

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

ADVISORY





NPC Advisory No. 2024 - 01

DATE : **30 May 2024**

SUBJECT : **MODEL CONTRACTUAL CLAUSES FOR CROSS-BORDER TRANSFERS OF PERSONAL DATA**

WHEREAS, Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring the free flow of information to promote innovation and growth. The State also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected;

WHEREAS, the National Privacy Commission (NPC) is mandated to ensure proper and effective coordination with data privacy regulators in other countries and participate in international and regional initiatives for privacy and data privacy protection, such as the Global Privacy Assembly (GPA);

WHEREAS, the NPC is a member of the GPA Global Frameworks and Standards Working Group (GFSWG) that is tasked to advance the GPA's work towards supporting secure cross- border flows of personal data across jurisdictions;

WHEREAS, the GPA GFSWG published a detailed comparison of model contractual clauses from different jurisdictions and regional organizations, including the Association of Southeast Asian Nations, Council of Europe, European Union, Ibero-American Network, Argentina, New Zealand, and the United Kingdom;

WHEREAS, the NPC previously issued Advisory No. 2021-02 or Guidance for the Use of the Association of Southeast Asian Nations (ASEAN) Model Contract Clauses and ASEAN Data Management Framework;

WHEREAS, the ASEAN and European Commission published a comparative guide to model contractual clauses of the ASEAN and European Commission to facilitate cross-border transfers of personal data from the ASEAN to the European Union (EU), from EU to ASEAN or between EU and ASEAN, and within ASEAN;

WHEREAS, the NPC acknowledges the importance of these initiatives as the use of model contractual clauses is one of the more widely used mechanisms for cross-border transfers of personal data;

WHEREAS, the DPA is not a barrier to cross-border transfers of personal data;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Advisory on the availability of model contractual clauses for cross-border transfers of personal data.

SECTION 1. ***Purpose***. — This Advisory provides guidance to personal information controllers (PICs) and personal information processors (PIPs) on the availability of the various model contractual clauses for transfers of personal data across jurisdictions.

SECTION 2. ***Definition of Terms.*** — The terms used in the DPA and its Implementing Rules and Regulations (IRR), and other NPC issuances, as amended, are adopted herein.

SECTION 3. ***Model Contractual Clauses (MCCs).*** — MCCs are terms and conditions that PICs and PIPs may include in binding legal agreements that govern cross-border transfers of personal data. MCCs do not preclude PICs and PIPs from further negotiating legal agreements.

A. The GPA GFSWG published the Comparative Tables of Contractual Clauses document (Document).

1. The Document provides an overview of select MCCs and serves as a comparative guide for PICs and PIPs on these MCCs for cross-border transfers of personal data.

2. The Document provides a comparative analysis of the following MCCs for cross- border transfers of personal data:

    i. Model Contractual Clauses of the Association of Southeast Asian Nations (ASEAN MCCs);
    ii. Standard Contractual Clauses of the Council of Europe (CoE SCCs);
    iii. Standard Contractual Clauses of the European Commission (EU SCCs);
    iv. Model Contractual Clauses of the Ibero-American Data Protection Network (RIPD MCCs);
    v. Model Contract of International Data Transfer of the Agency for the Access to Public Information of Argentina (AR Clauses);
    vi. Model Contractual Clauses of the Office of the Privacy Commissioner of New Zealand (NZ MCCs); and
    vii. International Data Transfer Agreements of the Information Commissioner's Office in the United Kingdom (UK IDTA).

3. The Document, which is composed of two parts, is available on the GPA website through the following links:

    i. Contractual Clauses for transfers from Controllers to Controllers;[1] and
    ii. Contractual Clauses for transfers from Controllers to Processors.[2]

[1] Global Privacy Assembly, Working Group Reports, Global Frameworks and Standards WG Report GFSWG 2023- Annex B, available at https://globalprivacyassembly.org/wp-content/uploads/2023/10/1.1-GPA-Annual-Working-Group-Report- Annex-B-Controller-to-Controller-clause-comparison-tables-tracked-changes.pdf (last accessed: 18 December 2023).
[2] Global Privacy Assembly, Working Group Reports, Global Frameworks and Standards WG Report GFSWG 2023- Annex C, available at https://globalprivacyassembly.org/wp-content/uploads/2023/10/1.2-GPA-Annual-Working-Group-Report- Annex-C-Controller-to-Processor-clause-comparison-tables-tracked-changes.pdf (last accessed: 18 December 2023).

B. The ASEAN and the European Commission published a Joint Guide to ASEAN MCCs and EU SCCs (Joint Guide).

   1. The Joint Guide provides an overview and comparative analysis of the ASEAN MCCs and EU MCCs and best practices to operationalize safeguards under these MCCs for cross-border transfers of personal data from ASEAN to EU, from EU to ASEAN or between EU and ASEAN, and within ASEAN.

   2. The Document is available on the ASEAN website through the following link:

      i. Joint Guide to ASEAN MCCs and EU SCCs.[3]

SECTION 6. ***Voluntary adoption.*** — This guidance is intended for voluntary adoption and does not impose any additional rights or obligations.

A. The NPC does not require contractual parties to adopt the use of MCCs. It remains the PIC and PIP's obligation to refer to the MCCs and determine for themselves whether applicable laws may impose additional obligations on the parties. Nevertheless, the use of MCCs may aid PICs in upholding the accountability principle in cross-border transfers of personal data.

B. The NPC will not accept any requests for review of agreements or contracts to determine conformity with any model contractual clauses.

SECTION 7. ***Effects.*** — The Advisory does not amend the DPA, its IRR, and other relevant issuances of the NPC, and shall neither preclude, limit, nor constrain the NPC's exercise of its mandate.

SECTION 8. ***Interpretation.*** — Any doubt in the interpretation of any provision of this Advisory shall be liberally interpreted in a manner mindful of the rights and interests of the data subjects.

Approved:

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

[3] Association of Southeast Asian Nations and European Commission, Joint Guide to ASEAN MCCs and EU MCCs, available at https://asean.org/wp-content/uploads/2024/02/Joint-Guide-to-ASEAN-Model-Contractual-Clauses-and-EU- Standard-Contractual-Clauses.pdf (last accessed: 07 February 2024).

NPC Advisory No. 2024 - 02

DATE : **12 August 2024**

SUBJECT : **GUIDELINES ON PERSONAL DATA PROCESSING BASED ON SECTION 13 (F) OF THE DATA PRIVACY ACT OF 2012**

WHEREAS, Section 7 (g) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) empowers the National Privacy Commission (NPC) to publish, on a regular basis, a guide to all laws relating to data protection;

WHEREAS, Section 9 of the Implementing Rules and Regulations of the DPA (IRR) empowers the NPC to develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

WHEREAS, Section 13 (f) of the DPA provides that the processing of sensitive personal information and privileged information is lawful when it is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority;

WHEREAS, there is a need to clarify the application of Section 13 (f) of the DPA to enable personal information controllers (PICs) to properly rely on this provision as the basis for processing personal data;

WHEREAS, the intention of the DPA is not to grant blanket exemption to public authorities, but rather to strike a balance between the need for public authorities to process personal data pursuant to its functions and mandates and the need to safeguard the rights and interests of data subjects;

WHEREAS, the legislative intent in passing the DPA is to give full effect to all its provisions. The whole and every part of the statute must be considered in fixing the meaning of any parts and to produce a harmonious whole. A statute must be so construed as to harmonize and give effect to all its provisions whenever possible;[1]

WHEREAS, the DPA recognizes public authority's need to process information in specific situations pursuant to its constitutional or statutory mandate or functions, as discussed in Section 4 (e), Section 12 (e), Section 13 (b), and Section 13 (f) of the DPA;

WHEREAS, information necessary to carry out the functions of public authority following Section 4 (e) of the DPA may be processed without a lawful basis under Section 12 or 13 of the DPA;

[1] Francisco I. Chavez v. Judicial Bar and Council, G.R. No. 202242 (2012).

WHEREAS, the information referred to in Section 4 (e) of the DPA does not pertain to personal information. The doctrine of last antecedent states that a qualifying or relative word or clause, such as "which," "said," and "such," is to be construed as applying to the words, phrase, or clause next preceding or, as is frequently stated, to the next preceding antecedent, and not as extending to or including others more remote, unless a contrary intention appears.[2] Following the doctrine of last antecedent, the phrase "which includes the processing of personal data" relates to the immediately preceding phrase "functions of public authority" and not to the term "information";

WHEREAS, processing of personal data for the performance by the independent central monetary authority or law enforcement and regulatory agencies, for its constitutionally and statutorily mandated functions under Section 4 (e) can find lawful basis under Sections 12 (e), 13 (b), or 13 (f) of the DPA, as applicable;

WHEREAS, processing of personal data by the government or public authority in relation to its constitutional or statutory mandate can find lawful basis in Section 12 (e) or Section 13 (b) of the DPA;

WHEREAS, Section 12 (e) of the DPA pertains to the processing of personal information when necessary to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority, which necessarily includes processing of personal information for the fulfillment of its mandate;

WHEREAS, Section 13 (b) of the DPA allows the processing of sensitive personal information and privileged information when provided for by existing laws and regulations: *provided*, that such regulatory enactments guarantee the protection of the sensitive personal information and privileged information: *provided further*, that the consent of the data subjects are not required by law or regulation permitting the processing of sensitive personal information and privileged information;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Advisory on the Guidelines on Personal Data Processing based on Section 13 (f) of the DPA.

SECTION 1. ***Scope.*** — This Advisory applies to all natural or juridical persons relying on Section 13 (f) of the DPA as a lawful basis for processing personal data.

SECTION 2. ***Processing under Section 13 (f) of the DPA.*** — Processing on the basis of Section 13 (f) of the DPA requires that the processing is necessary, and the processing is for the protection of lawful rights and interests or the establishment, exercise, or defense of legal claims. Thus, processing under Section 13 (f) of the DPA is read as follows:

A. The processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings;

B. The processing is necessary for the establishment, exercise, or defense of legal claims; or

[2] Marvin L. San Juan v. People of the Philippines, G.R. No. 236628 (2023).

C. The processing entails providing to government or public authority personal data that is necessary for the protection of lawful rights and interests in court proceedings or the establishment, exercise, or defense of legal claims in relation to its constitutional or statutory mandate. Such instances may include providing information that supports the investigation of a law enforcement or regulatory agency.

SECTION 3. ***Processing under Section 13 (f) of the DPA as legitimate interest.*** — Processing under Section 13 (f) of the DPA may be considered legitimate interest under Section 12 (f) of the DPA, which is a lawful basis for processing personal information.

A. Processing personal information that is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings or necessary for the establishment, exercise, or defense of legal claims[3] may be considered as legitimate interest under Section 12 (f) of the DPA.[4] As such, Section 13 (f) in relation to Section 12 (f) of the DPA may be a lawful basis for processing personal information for this purpose.

B. The PIC must fulfill the requisites for processing based on legitimate interest in NPC Circular 2023-07 or the Guidelines on Legitimate Interest.[5]

SECTION 4. ***Necessary.*** — Determining the proper application of Section 2 of this Circular takes into consideration the necessity of the specific processing activity undertaken for the legitimate purpose of protecting lawful rights and interests of natural or legal persons in court proceedings, or establishing, exercising, or defending legal claims.[6]

The specific processing activity is necessary when it is adequate, relevant, suitable, and not excessive in relation to such legitimate purpose.[7] The specific processing activity must be within the limitations of the law.[8]

SECTION 5. ***Protection of Lawful Rights and Interests; Establishment, Exercise, or Defense of Legal Claims.*** —

A. Processing of personal data on the basis of Section 13 (f) of the DPA may be conducted during stages preparatory to a case. It does not require that there be an existing proceeding before an administrative agency, court, or other tribunal.
B. Processing of personal data on the basis of Section 13 (f) of the DPA need not result in the filing of an actual case.

---

[3] EA and TA v. EJ, EE and HC, NPC 17-018, 15 July 2019, at 8, *available at* https://privacy.gov.ph/wp- content/uploads/2024/06/NPC-17-018-2019.07.15-EA-and-TA-v-EJ-Decision-FinalP.pdf.
[4] KRL v. Trinity University of Asia, AA, MC, NCB, RG GV, GCT, RR, MR, PB, CID Case No. 17-K-003, 19 November 2019, at 6, *available at* https://www.privacy.gov.ph/wp-content/uploads/2020/10/CID-17-K-003-KRL-v-Trinity-Decision-PSD- 10Aug2020.pdf.
[5] *See* National Privacy Commission, Guidelines on Legitimate Interest, NPC Circular No. 2023-07 [NPC Circ. No. 2023-07] (13 December 2023).
[6] EA and TA v. EJ, EE and HC, NPC 17-018, 15 July 2019, at 8, *available at* https://privacy.gov.ph/wp- content/uploads/2024/06/NPC-17-018-2019.07.15-EA-and-TA-v-EJ-Decision-FinalP.pdf.
[7] National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule IV, § 18 (c) (2016); *See* Spouses MCD and JJD v. Victoria Milling Company, et al., NPC 19-758 & 19-1846, 30 June 2023, at 23, *available at* https://privacy.gov.ph/wp-content/uploads/2024/05/NPC-19-758-to-NPC-19-1846-2023.06.30-MCD-_-JJD-v- Victorias-Milling-Company-et-al-Decision-FinalP.pdf.
[8] Spouses MCD and JJD v. Victoria Milling Company, et al., NPC 19-758 & 19-1846, 30 June 2023, at 21, *available at* https://privacy.gov.ph/wp-content/uploads/2024/05/NPC-19-758-to-NPC-19-1846-2023.06.30-MCD-_-JJD-v-Victorias- Milling-Company-et-al-Decision-FinalP.pdf.

C. "Natural or legal persons" under Section 13 (f) of the DPA refers to persons whose lawful rights and interests are protected in court proceedings, including the parties and their witnesses.[9]

D. Legal claims that are established, exercised, or defended may refer to legal claims of persons other than those who processed the personal data.[10]

SECTION 6. ***Transparency; Right to be Informed.*** — Service of pleadings to the parties of a case is understood as the next practical opportunity to inform data subjects, in relation to Section 16 (a) and (b) of the DPA, of the nature, purpose, and extent of the processing of their personal data for the protection of lawful rights and interests or the establishment, exercise, or defense of legal claims.

Data subjects whose personal data is processed on the basis of Section 13 (f) of the DPA is informed of the specific processing activity when they are served with a copy of the pleading containing the personal data following the applicable rules of procedure on summons and service.

SECTION 7. ***Determination of merit of lawful rights and interests and legal claims; admissibility of evidence.*** — The Commission only determines whether the processing of personal data is necessary in relation to the lawful rights and interests sought to be protected or the legal claims that are sought to be established, exercised, or defended. The Commission does not rule on the admissibility of evidence, its materiality, relevance, or probative value to a particular case outside its jurisdiction,[11] or the propriety of the legal strategy employed by parties in legal proceedings.[12] The establishment, exercise, or defense of a legal claim under Section 13 (f) of the DPA as a lawful basis for processing personal data is independent of the existence of a cause of action.[13]

SECTION 8. ***Interpretation.*** — Any doubt in the interpretation of any provision of this Advisory shall be liberally interpreted in a manner mindful of the rights and interests of the data subjects.

Approved:

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

---

[9] JCB v. FRL, NPC 21-031, 03 March 2022, at 11, *available at* https://privacy.gov.ph/wp-content/uploads/2024/05/NPC-21- 031-2022.03.03-JCB-v.-FRL-Decision-FinalP.pdf.
[10] JCB v. FRL, NPC 21-031, 03 March 2022, at 11, *available at* https://privacy.gov.ph/wp-content/uploads/2024/05/NPC-21- 031-2022.03.03-JCB-v.-FRL-Decision-FinalP.pdf.
[11] RJC v. DL, NPC 22-012, 10 November 2022, at 8, *available at* https://privacy.gov.ph/wp-content/uploads/2023/08/NPC-22- 012-2022.11.10-RJC-v.-DL-Decision.pdf.
[12] RJC v. DL, NPC 22-012, 26 January 2023, at 11, *available at* https://privacy.gov.ph/wp-content/uploads/2023/07/NPC-22- 012-2023.01.26-RJC-v.-DL-Resolution-w-Sgd-Final.pdf.
[13] EA and TA v. EJ, EE and HC, NPC 17-018, 05 November 2020, at 3, available at https://privacy.gov.ph/wp- content/uploads/2024/08/NPC-17-018-2020.11.05-EA-_-TA-v.-EJ-EE-_-HC-Resolution.pdf.

NPC Advisory No. 2024 – 03

DATE : 17 December 2024

SUBJECT : GUIDELINES ON CHILD-ORIENTED TRANSPARENCY

WHEREAS, Section 7 (g) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) empowers the National Privacy Commission (NPC) to publish, on a regular basis, a guide to all laws relating to data protection;

WHEREAS, Section 9 of the Implementing Rules and Regulations of the DPA (IRR) empowers the NPC to develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

WHEREAS, Section 20 of the DPA provides that Personal Information Controllers (PIC) must implement reasonable and appropriate organizational, physical, and technical security measures intended for the protection of personal data. In determining the appropriate level of security, PICs must consider the risks represented by the processing, among other factors;

WHEREAS, a 'child' refers to a person below eighteen (18) years of age or those eighteen (18) or over but are unable to fully take care of themselves or protect themselves from abuse, neglect, cruelty, exploitation, or discrimination because of a physical or mental disability or condition;[1]

WHEREAS, children, as data subjects and rights holders, are entitled to meaningful access to information;[2]

WHEREAS, PICs or Personal Information Processors (PIP), when processing children's personal data, should ensure that children receive extra protection. Such processing should be context-specific and principles-based;

WHEREAS, the NPC recognizes the need to provide children with opportunities to create and interact within a protective environment;

WHEREAS, the principles of "best interests of the child"[3] and "evolving capacities"[4] are the primary considerations in all actions involving children. Recognizing children as rights

---

[1] *See* An Act Providing For Stronger Deterrence And Special Protection Against Child Abuse, Exploitation And Discrimination, And For Other Purposes [Special Protection of Children Against Abuse, Exploitation and Discrimination Act of 1992], Republic Act No. 7610 § 3 (a) (1992).

[2] *See* UN Committee on the Rights of the Child (UNCRC), General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2 March 2021).

[3] *See* Convention on the Rights of the Child art. 3(1), *adopted* 20 November 1989, 1577 U.N.T.S. 3.

[4] *See Id.* art. 5.

holders with varying degrees of maturity gives full effect to their best interests and evolving capacities;

WHEREAS, Section 16 of the DPA provides for the data subjects' right to be informed of processing of their personal data;

WHEREAS, Section 11 of the DPA provides that processing personal data should adhere to the general privacy principles;

WHEREAS, the Principle of Transparency requires PICs to provide data subjects with the necessary information on the nature, purpose, and extent of processing, including the risks and safeguards involved, the identity of the PIC, as well as data subject rights and how these can be exercised;

WHEREAS, the Principle of Transparency requires that any information and communication relating to the processing of personal data should be easy to access, concrete and definitive, understood by a member of its target audience, and presented in a simple manner using clear and plain language while retaining necessary technical terms;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Advisory on the Guidelines on Child-Oriented Transparency.

SECTION 1. ***Scope.*** — This Advisory applies to all PICs and PIPs engaged in the processing of children's personal data, whether in a digital or physical environment. It covers products or services specifically intended for children or likely to be accessed by children.

SECTION 2. ***Risk-Based Assessment.*** — The processing of children's personal data must adhere to the general privacy principles.[5] PICs shall ensure that, in accordance with the Principle of Transparency, children are aware of the nature, purpose, and extent of the processing of personal data. Consistent with the purpose of a Privacy Impact Assessment (PIA), PICs shall adopt a risk-based and child-oriented approach when informing children whose data they are processing, taking into account their age and the risks involved in the specific processing activity.

A. ***Privacy Impact Assessment (PIA).*** PICs must incorporate Child Privacy Impact Assessments (CPIA) as part of their PIAs before launching products or services intended or likely to be accessed by children and thereafter as may be necessary.[6] The PIA is a continuing requirement, regularly reviewed and updated to account for changes in products, services, processes, or regulations.[7] The factors that must be considered include, but are not limited to:

    1. Purpose of processing;
    2. Types of data to be processed (*e.g.*, collected, used, or disclosed);
    3. Sources of data;
    4. Systems to be used (*e.g.*, open or closed systems);

---

[5] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 11 (2012).

[6] *See* National Privacy Commission, Security of Personal Data in the Government and the Private Sector, Circular No. 06, Series of 2023 [NPC Circ. No. 23-06], (01 December 2023).

[7] *See Id.*

5. Data storage and disposal;
6. Data sharing;
7. Security measures implemented;
8. Effect or impact of the specific processing activity on children;
9. Age range of intended or likely users;
10. Process owner for the specific processing activity of the PIC or PIP;
11. Risk Identification; and
12. Involvement of Parents or Guardians

    The involvement of parents or guardians may be necessary in determining whether children may participate in the specific processing activity, particularly when there are heightened risks to children. PICs must determine the appropriate methods for securing and verifying this involvement based on the level of risk to children.

B. PICs should implement appropriate measures to address any risks identified in the PIA to ensure the protection of children's personal data taking into consideration the best interests of the child, and to promote the Principle of Transparency in processing activities.[8]

   In this regard, PICs may employ the following measures, among others:

   1. ***Age Assurance Mechanisms.*** PICs may implement age assurance mechanisms or solutions to determine the age range of their users as a tool to adopt age- appropriate practices when processing children's personal data. In determining the most suitable age assurance mechanism or solution for a specific processing activity, PICs should recognize that relying solely on users' self-declaration may be inadequate for high-risk processing activities.

      PICs must ensure that children understand the purpose of the age assurance process. The processing of personal data for age assurance must adhere to the general privacy principles and must have a lawful basis for processing.[9]

   2. ***Privacy Controls.*** PICs must adopt a risk-based approach to determine and implement appropriate and enhanced privacy controls when processing children's personal data, ensuring:

      a. **High Privacy Settings by Default**: Children's accounts must have privacy settings set to the highest level by default. This includes disabling geolocation services, setting profiles to private, and minimizing data sharing unless necessary for the specific purpose.[10]

      b. **Easy Access to Privacy Settings**: PICs must ensure that children are fully aware of the available privacy settings and how to adjust them. These settings should be clear, easy to access, and designed in a way that enables children to understand and control their privacy preferences while maintaining a minimum level of protection.

---

[8] Data Privacy Act of 2012, § 20 (f).
[9] *See Id.* §§ 11 – 13.
[10] *Id.* § 11.

SECTION 3. *Privacy Notice.* PICs shall ensure that children are aware of the nature, purpose, and extent of the processing of personal data.[11] PICs should consider the readability (*e.g.*, vocabulary, tone, or style), comprehension, and granularity of Privacy Notices while taking into consideration the best interests and evolving capacities of children.

PICs shall ensure that the Privacy Notice, including any information and communication relating to the processing of personal data, is readily accessible, taking into consideration user experience and user interface. PICs must clearly inform children how to access any information or communication relating to the processing of their personal data.

PICs may utilize a variety of alternative formats, such as videos, infographics, animations, and audio recordings, to deliver privacy-related information to children. PICs should design these formats to ensure that the Privacy Notices are presented in a manner that is simple and easily understandable, taking into consideration the age range of the intended or likely users.

A. ***Content.*** PICs should inform the children of the following:

    1. Specific and precise processing activities involving the personal data of the children;
    2. Purpose of processing;
    3. Appropriate lawful basis;
    4. Potential consequences and risks associated with the processing of the personal data of the children;
    5. Importance of privacy settings;
    6. Rights as data subjects and the manner and method of exercising these; and
    7. Revisions or updates to the Privacy Notice, if any.

B. ***Age-Appropriate Privacy Notice.*** PICs must ensure that any information or communication relating to the processing of children's personal data should be concrete and definitive, and understood by intended or likely users whose personal data are involved in the specific processing activity. [12] PICs shall present the information in a simple manner using clear and plain language while retaining necessary technical terms.[13] This ensures that children receive relevant privacy-related information in a language that is appropriate and easily comprehensible, taking into consideration the age range of the intended or likely users.

    In instances where the product, or service involves or contemplates children as data subjects, regardless of whether it is also intended for adults, PICs must provide child- friendly Privacy Notices in addition to standard versions.[14]

C. ***Just-in-time Privacy Notice.*** [15] PICs shall provide information on how children's personal data will be processed at the point in time when personal data is about to be processed. PICs shall ensure that the information presented is the minimum specific information relevant to the specific processing activity that will be undertaken;

---

[11] *Id.*
[12] *See* National Privacy Commission, Guidelines on Consent, Circular No. 04, Series of 2023 [NPC Circ. No. 23-04], § 3 (D)(3) (07 November 2023).
[13] *Id.*
[14] *See Id.* § 3.
[15] *See Id.* § 2 (E).

D. ***Layered Privacy Notice.***[16] PICs shall use Layered Privacy Notices that embody the minimum specific information for purposes of the Principle of Transparency. These should direct children to supplemental and detailed information relevant to the specific processing activity that will be undertaken. PICs shall ensure that the supplemental and detailed information presented to children is separate from that intended for adults and presented in a language that is appropriate and easily comprehensible for children;

E. ***Deceptive Design Patterns.***[17] PICs shall not use deceptive methods or any form of coercion, compulsion, threat, intimidation, or violence in the processing of the children's personal data.

PICs shall not use characters that children know and trust to influence them to provide more information than necessary for the specified and declared purpose. Further, PICs shall not use designs that nudge or steer children toward selecting options that compromise their privacy or are inconsistent with their best interests.

SECTION 4. ***Data Breach Notification.*** — In cases of data breaches that fall under mandatory breach notification according to issuances on data breach management, PICs shall notify the data subjects even if the data subjects are children.[18]

In cases where the affected data subjects are children, PICs shall notify both the children and their parents or guardians. When notifying children, PICs must use the appropriate language readily understandable to the children. [19]

PICs are not precluded from notifying children and their parents or guardians when the data breach does not fall under mandatory breach notification.

SECTION 5. ***Accountability.*** —PICs are responsible for the processing of children's personal data, including personal data that has been subcontracted or outsourced to their PIPs.[20] In all actions, PICs must place the best interests of the child as the primary consideration. As such, PICs must adopt a risk-based and context-specific approach when determining the most suitable age-assurance mechanism or solution, if any; when evaluating appropriate content for their data subjects and the manner of informing them of the specific processing activity; and when implementing appropriate and enhanced security measures, privacy controls, and safeguards.

SECTION 6. ***Interpretation.*** — Any doubt in the interpretation of any provision of this Advisory shall be liberally interpreted in a manner mindful of the rights and interests of children, recognizing them as rights holders and giving full effect to their best interests and evolving capacities.

---

[16] *See Id.* § 3 (D)(3)(c).

[17] *See Id.* § 7; National Privacy Commission, Guidelines on Deceptive Design Patterns, Advisory No. 01, Series of 2023 [NPC Adv. No. 23-01] (07 November 2023).

[18] *See* NPC Circ. No. 23-04, § 11.

[19] *See Id.* § 3 (D)(3).

[20] Data Privacy Act of 2012, § 21.

Approved:

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Advisory on Guidelines on Child-Oriented Transparency

Questions Raised During the Call for Public Input as of 17 December 2024

General Questions

Question	Answer
1. What is the purpose of the Advisory?	The Advisory is intended to be the first of many advisories that will be released on children's privacy to ensure that children are protected while they create and interact within a protective environment. The Advisory focuses on child-oriented transparency. It clarifies how the Principle of Transparency and existing obligations of Personal Information Controllers (PIC) and Personal Information Processors (PIP) apply when processing children's personal data.
2. Who is considered a "child" under the Advisory?	A 'child' refers to a person below eighteen (18) years of age or those eighteen (18) or over but are unable to fully take care of themselves or protect themselves from abuse, neglect, cruelty, exploitation, or discrimination because of a physical or mental disability or condition.
3. Why does the Advisory directly address children, even though they lack the legal capacity to act?	The NPC recognizes children as data subjects and rights holders. Their lack of legal capacity to act does not diminish the rights as data subjects under Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).
4. When does the Advisory apply? Does it apply only when the processing is done within the Philippines?	The Advisory applies when PICs and PIPs are engaged in the processing of children's personal data, whether in a digital or physical environment. It covers products or services specifically intended for children or likely to be accessed by children. The Advisory also applies when the processing is done outside the Philippines pursuant to the extraterritorial application of the DPA. As provided in Section 6 of the DPA and Section 4, Rule II of its Implementing Rules and Regulations (IRR), the DPA, its IRR, and issuances of the Commission apply to acts of processing personal data performed in and outside the Philippines in the following instances:

	1. The natural or juridical person involved in the processing of personal data is found or established in the Philippines; 2. The processing relates to personal data about a Philippine citizen or resident; 3. The entity has a link with the Philippines. As the Advisory provides guidelines on how the DPA and its IRR applies in relation to the processing of children's personal data, it will apply even when the processing is done outside the Philippines.
5. Does the lack of explicit guidance on parental consent mean that this Advisory does not apply if parental consent is obtained?	No. The Advisory applies regardless of the basis for processing. Section 1 does not limit the applicability of the Advisory to processing based on consent. In addition, this Advisory focuses on the Principle of Transparency.
6. Why isn't there a specific "age of digital consent" in the Advisory?	An advisory is not the proper issuance to establish an age of digital consent. Advisories provide guidance on understanding existing legal principles concerning specific issues related to safeguarding personal data. Establishing an age of digital consent will require legislative action through a law passed by Congress. This is because setting such an age would impact legal provisions related to a person's capacity to act, which are governed by the New Civil Code and related legislation.
7. What are the enforcement mechanisms and penalties for non-compliance with the Advisory?	Due to the nature of an advisory, this Advisory does not introduce new obligations or penalties. It is based on existing obligations under the DPA, its IRR, and other issuances of the Commission. Enforcement mechanisms established under the DPA, its IRR, and relevant issuances apply in relation to the Advisory.
8. Will a PIC be given a period to ensure compliance with the provisions of the Advisory?	No. The Advisory provides clarification on existing obligations imposed under the DPA, its IRR, and other issuances of the Commission. The Advisory only seeks to provide further guidance when processing children's personal data.

Risk-Based Assessment

Question	Answer
9. Who will conduct the risk-based assessment and determine the need for a Child Privacy Impact Assessment (CPIA)?	As provided in Section 2 (A) of the Advisory, PICs must incorporate Child Privacy Impact Assessments (CPIA) as part of their Privacy Impact Assessments (PIA) before launching products or services intended or likely to be accessed by children and thereafter as may be necessary.
10. Is there a prescribed form or procedure for the conduct of a CPIA?	No. There is no prescribed form for the CPIA. A CPIA forms part of the PIA, which is a continuing obligation on the part of PICs. Section 5 of NPC Circular 2023-06 (Security of Personal Data in the Government and the Private Sector) provides guidelines on the conduct of a PIA. Section 2 (A) of the Advisory further clarifies this requirement when PICs process personal data for products or services intended or likely to be accessed by children. As such, PICs may use any method, structure, or form, provided PICs comply with Section 5 of NPC Circular 2023-06 and take into consideration the factors listed under Section 2 (A) of the Advisory.
11. Is the list of factors provided under Section 2(A) exhaustive?	No. The factors enumerated under Section 2(A) of the Advisory is not exhaustive. PICs may consider other factors when conducting their CPIAs.
12. How often should a CPIA be conducted?	PICs should regularly conduct CPIAs if their products or services are intended or likely to be accessed by children. A CPIA forms part of the PIA, which is a continuing obligation on the part of PICs. Section 4 of NPC Circular 2023-06 (Security of Personal Data in the Government and the Private Sector) provides that it should be regularly reviewed and updated to account for changes in products, services, processes, or regulations. The degree of regularity, however, depends on the circumstances which PICs are in the best position to determine.
13. Does the inclusion of parental involvement in Section 2 (A)(12) mean parental consent is mandatory?	The Advisory focuses on child-oriented transparency. The factors enumerated under Section (A) only serve as a guide on what factors PICs may consider when conducting their CPIAs. This is to ensure that the CPIAs take into account the different risks that may arise with the processing of children's personal data.

14. Will the NPC release a list of expected tools or mechanisms for age assurance?	No. The NPC will not release a list of suggested age assurance mechanisms. PICs are in the best position to determine the need for age assurance mechanisms and the proper solutions to implement based on their purpose and risk-based assessment.
15. Can PICs rely solely on users' self-declaration for age verification?	While not expressly prohibited, PICs should recognize that relying solely on users' self-declaration may be inadequate for high-risk processing activities.

Privacy Notice

Question	Answer
16. Is there a prescribed form for the child-friendly privacy notice? Are there minimum standards that must be met?	No. There is no prescribed form for the child-friendly privacy notice. Following the Principle of Transparency, PICs shall ensure that children are aware of the nature, purpose, and extent of the processing of personal data. Section 3 of the Advisory further clarifies this requirement where the PICs' products or services are specifically intended for children or are likely to be accessed by children.
17. Can PICs opt to have a singular Privacy Notice for both adults and children?	No. A singular notice is not sufficient. The information presented in a standard version of the Privacy Notice may be too complicated for children. On the other hand, the information provided may not be detailed enough to give sufficient information to adults.
18. Can PICs employ age-tiered privacy notices?	PICs are in the best position to determine the suitability of employing age-tiered privacy notices based on their risk-based assessment of their processing activities Following its continuing obligation to conduct PIAs, PICs shall adopt a risk-based and child-oriented approach when informing children whose personal data they are processing, taking into account their age and the risks involved in the specific processing activity.

Data Breach Notification

Question	Answer
19. Is the PIC required to notify both the parent or guardian and the child?	Yes. By notifying both the parent or guardian and the child, the child is better equipped to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. Section 20 (f) of the DPA requires PICs to notify their affected data subjects of breaches in cases that fall under mandatory breach notification. NPC Circular 16-03 (Personal Data Breach Management) provides the procedure for breach notification. Section 4 of the Advisory further clarifies breach notification where the affected data subjects are children. It provides, "[i]n cases where the affected data subjects are children, PICs shall notify both the children and their parents or guardians."
20. Is there a prescribed form and language for data breach notifications?	Yes. Section 18 of NPC Circular 16-03 (Personal Data Breach Management) provides guidelines on the notification of affected data subjects, including contents and form. Section 4 of the Advisory further clarifies that when notifying children, PICs must use the appropriate language that is readily understandable to the children.

Accountability

Question	Answer
21. Who is accountable?	PICs are responsible for processing children's personal data, including personal data that has been subcontracted or outsourced to their PIPs, in accordance with the Principle of Accountability.

NPC Advisory No. 2024 – 04

DATE : **19 December 2024**

SUBJECT : **GUIDELINES ON THE APPLICATION OF REPUBLIC ACT NO. 10173 OR THE DATA PRIVACY ACT OF 2012 (DPA), ITS IMPLEMENTING RULES AND REGULATIONS, AND THE ISSUANCES OF THE COMMISSION TO ARTIFICIAL INTELLIGENCE SYSTEMS PROCESSING PERSONAL DATA**

WHEREAS, Section 7 (g) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) empowers the National Privacy Commission (NPC) to publish, on a regular basis, a guide to all laws relating to data protection;

WHEREAS, Section 9 of the Implementing Rules and Regulations of the DPA (IRR) empowers the NPC to develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

WHEREAS, Artificial Intelligence (AI) systems, which are dynamic and continuously evolving, are designed to perform tasks that require human intelligence, with or without human intervention, using techniques that enable machines to learn from data, perceive environments, process and adapt to new inputs, manipulate or generate output, and make decisions or predictions based on a set of defined objectives;[1]

WHEREAS, the DPA, its IRR, and the issuances of the Commission, which are principles- based and technology-neutral, apply to all forms of processing of personal information and sensitive personal information (collectively, personal data);

WHEREAS, the DPA, its IRR, and the issuances of the Commission apply when the processing of personal data is involved in the development or deployment of AI systems, including its training and testing;

WHEREAS, it is necessary to provide additional guidance regarding the application of the general privacy principles and specific key concepts in the DPA, its IRR, and the issuances of the Commission insofar as the AI systems involve the processing of personal data;

---

[1] *See* Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, at 36, *available at* https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea- 8c1f-01aa75ed71a1 (2019); OECD Council, *Recommendation on Artificial Intelligence*, OECD/LEGAL/0449, *available at* https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449 (2024); ISO/IEC JTC 1/SC 42, *Information Technology – Artificial Intelligence – Artificial Intelligence Concepts and Terminology*, ISO/IEC 22989:2022, § 3.1.4, *available at* https://www.iso.org/standard/74296.html (2022); National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, NIST AI 600-1 (2024), n. 1, *available at* https://doi.org/10.6028/NIST.AI.600-1.

WHEREFORE, in consideration of these premises, the NPC hereby issues this Advisory on the Guidelines on the Application of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and the issuances of the Commission to Artificial Intelligence Systems Processing Personal Data.

SECTION 1. ***Scope.*** — This Advisory applies when the processing of personal data is involved in the development or deployment of AI systems, including its training and testing.

SECTION 2. ***Application of the DPA.*** — The obligations of Personal Information Controllers (PIC), and their Personal Information Processors (PIP), under the DPA, its IRR, and the issuances of the Commission, including adhering to the general privacy principles, upholding the rights of the data subjects, determining the appropriate lawful basis for processing, and implementing security measures, apply insofar as AI systems involve the processing of personal data.

A. ***Transparency.*** PICs shall inform their data subjects of the nature, purpose, and extent of the processing of personal data when such processing is involved in the development or deployment of AI systems, including its training and testing.[2] PICs must be able to explain the purpose for such processing, the factors and inputs considered by such AI systems, the risks associated with the processing, the expected output of the AI systems, the impact of the AI systems on data subjects,[3] and any applicable dispute mechanisms available to their data subjects.[4] PICs shall ensure that any information on such processing is easy to access, concrete and definitive, understood by members of their target audience, and presented in a simple manner using clear and plain language while retaining necessary technical terms.[5]

B. ***Accountability.***[6] PICs shall be accountable for the processing of AI systems and for the outcomes and consequences of such processing when personal data is involved. This accountability is imposed on the specific PIC undertaking the development or deployment of the AI system, including its training and testing. When such processing is subcontracted or outsourced, PICs shall remain accountable for the actions of their PIPs.[7]

1. ***Demonstrable Measures.*** PICs and, in cases where the processing is subcontracted or outsourced, their PIPs, must be able to demonstrate that they have implemented effective policies and procedures to comply with the DPA, its IRR, and other issuances of the Commission. PICs must maintain the necessary documentation on

---

[2] *See* An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 11 (a) (2012).

[3] *Id.*

[4] *See id.* § 16 (a), (b), & (d).

[5] National Privacy Commission, Guidelines on Consent, Circular No. 04, Series of 2023 [NPC Circ. No. 23-04], § 3 (D)(3) (07 November 2023).

[6] *See* Data Privacy Act of 2012, § 21.

[7] *Id.*

these policies and procedures, including those for AI systems that involve the processing of personal data.

2. ***Governance Mechanisms.*** [8] PICs shall institute appropriate and effective governance mechanisms to ensure the responsible and ethical processing of personal data in the development or deployment of AI systems, including its training and testing.

   These include, but are not limited to, the conduct of Privacy Impact Assessments (PIA);[9] integration of privacy-by-design and privacy-by-default; implementation of common industry security standards; continuous monitoring of the AI systems' operations; creation of a dedicated AI ethics board; regular retraining and scrubbing of the AI systems; and mechanisms for humans to intervene in decision- making and review the output of AI systems.

   a. AI systems can involve automated decision-making, and the effects of such automated decisions can pose a significant risk to the rights and freedoms of data subjects. In such cases, as an additional safeguard, PICs shall implement mechanisms to allow for meaningful human intervention carried out by persons with the necessary competence and authority.

      PICs shall also implement mechanisms to allow their data subjects to question and contest automated decisions when the effect of such decisions poses a significant risk to the rights and freedoms of data subjects.[10]

   b. PICs shall also be responsible for regularly monitoring the proper implementation and effectiveness of these governance mechanisms.

C. ***Fairness.***[11] PICs shall ensure that personal data is processed in a manner that is neither manipulative nor unduly oppressive to data subjects. As such, PICs shall implement mechanisms to identify and monitor biases in the AI systems and to limit such biases and their impact on the data subjects. PICs must consider systemic bias, human bias, and statistical bias when assessing or auditing their AI systems.

   Consistent with the Principle of Fairness, PICs shall not utilize AI Washing, the practice where PICs overstate the involvement of AI systems to the detriment of their data subjects, and other deceptive practices.

D. ***Accuracy.***[12] PICs must maintain the accuracy of personal data to ensure the fairness of the output of the AI systems. PICs shall implement appropriate measures to ensure that personal data utilized in the AI systems is correct and kept up to date.

---

[8] *See generally Id.* §§ 20 & 21.
[9] *See* National Privacy Commission, Security of Personal Data in the Government and the Private Sector, Circular No. 06, Series of 2023 [NPC Circ. No. 23-06], (01 December 2023).
[10] *See* Data Privacy Act of 2012, § 16.
[11] *See* National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule IV, § 19 (b) (2016).
[12] *See Id.* rule IV, § 19 (c).

E. ***Data Minimization.***[13] PICs shall exclude, by default, any personal data that is unlikely to improve the development or deployment of AI systems, including its training and testing.

F. ***Lawful Basis for Processing.*** PICs shall determine the most appropriate lawful basis under Sections 12 and 13 of the DPA prior to the processing of personal data in the development or deployment of AI systems, including its training and testing.[14]

Publicly available personal data do not lose the protection afforded by the DPA, its IRR, and the issuances of the Commission simply because it has been made public or is publicly accessible.[15] When PICs process personal data that is publicly available, they shall determine the most appropriate lawful basis under the DPA and ensure that the processing adheres to the general privacy principles.

SECTION 3. *Rights of the Data Subject.* [16] — AI systems involving the processing of personal data can have implications on the exercise of data subject rights.

PICs should implement mechanisms, which may include Privacy-Enhancing Technologies (PET), to ensure the proper exercise of data subject rights while allowing for the responsible and ethical processing of personal data in the development or deployment of AI systems, including its training and testing.

A. PICs shall implement effective mechanisms or alternative measures to give effect particularly to the right to object, the right to rectification, and the right to erasure or blocking. In such cases, PICs shall communicate to their data subjects the scope and consequences of the exercise of these rights following the Principle of Transparency. When the request is not feasible, PICs shall inform their data subjects of such fact and their reasons. Nevertheless, PICs shall implement effective mechanisms or alternative measures to carry out, as far as possible, the intended effect of these rights.

B. PICs shall ensure that their data subjects may exercise data subject rights before, during, and after the development or deployment of AI systems, including its training and testing.

C. The fact that personal data has been incorporated into data sets does not automatically make the exercise of data subject rights unreasonable. PICs' inaction towards providing mechanisms that allow for the meaningful exercise of data subject rights negates any claim that fulfilling such requests is unreasonable.

---

[13] *See Id.* rule IV, § 19 (b).

[14] Data Privacy Act of 2012, §§ 12 & 13.

[15] EA and TA v. EJ, EE and HC, NPC 17-018, 15 July 2019, at 7, *available at* https://privacy.gov.ph/wp- content/uploads/2022/09/NPC-17-018-EA-and-TA-v-EJ-Decision-2019.07.15-.pdf.

[16] *See* National Privacy Commission, Data Subject Rights, Advisory No. 01, Series of 2021 [NPC Advisory No. 2021-01] (29 January 2021).

SECTION 4. ***Interpretation.*** — Any doubt in the interpretation of any provision of this Advisory shall be liberally interpreted in a manner mindful of the rights and interests of the data subjects.

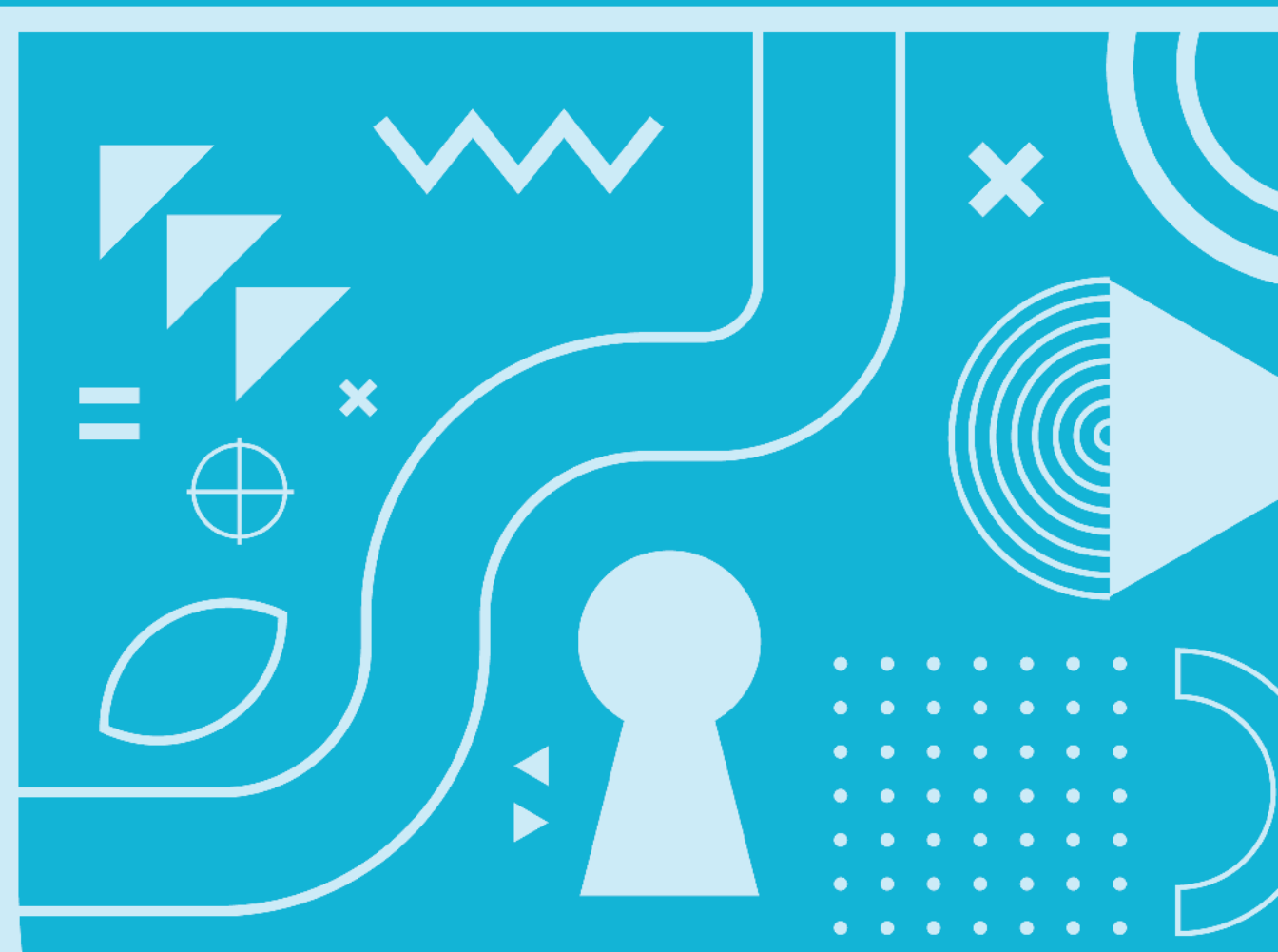
Approved:

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

ADVISORY OPINIONS





ADVISORY OPINION NO. 2024-001[1]

18 January 2024

[redacted]

Re: REQUEST FOR ACCESS TO PERSONAL DATA FOR AUDIT PURPOSES

Dear [redacted]:

We respond to your request for an Advisory Opinion regarding the Commission on Audit's (COA) request to access personal and sensitive personal information in relation to its performance audit.

You mention that the COA is conducting a performance audit on the COVID-19 National Vaccination Program, which is helmed by the Department of Health (DOH). As part of the audit process, the COA's audit team needs access to the COVID-19 Vaccination Information Management System (VIMS) to review the accuracy and reliability of data generated therefrom. The Epidemiology Bureau (EB) of the DOH maintains processing over the VIMS and serves as the primary source of information for the nationwide vaccination status posted on the DOH website.

However, the DOH expressed concerns about data privacy regarding the COA's request for access to the VIMS. The DOH reasoned that the local government units (LGUs) were solely responsible for collecting the data stored in the VIMS, while EB's role is limited to storing and managing the data in accordance with its mandate. Although the audit team had already conducted tests of the data against the source documents held by the LGUs, the conduct of a national-level review of the data from the VIMS will achieve a different audit objective.

You thus seek guidance on how to conduct the audit process in compliance with the Data Privacy Act of 2012 (DPA).

[1] Tags: processing; audit function; constitutional mandate.

NPC Advisory Opinion No. 2020-016; constitutional or statutory mandate.

We reiterate our stance in NPC Advisory Opinion No. 2020-016 in which we acknowledged the authority of the COA as an independent constitutional body and recognized its power, authority, and duty to examine, audit and settle all accounts and expenditures of the funds and properties of the Philippine government.[2] We also stated therein that:

> The DPA shall not be used to hamper, or interfere with, the performance of the duties and functions of duly constituted public authorities. Pursuant to the 1987 Constitution, the COA shall have exclusive authority, subject to certain limitations, to define the scope of its audit and examination, establish the techniques and methods required therefor, and promulgate accounting and auditing rules and regulations, including those for the prevention and disallowance of irregular, unnecessary, excessive, extravagant, or unconscionable expenditures or uses of government funds and properties.
>
> With this in mind, the COA in carrying out its mandate, enjoys the presumption of regularity in the performance of its duties. The determination of what methods to utilize in the collection or gathering of personal data in performing its auditing functions shall be left to the COA's sound discretion.

As such, the COA's intended access to the VIMS database to review its completeness, reliability, and overall performance falls within COA's constitutional mandate and, hence, the processing thereof is generally allowed.[3]

General data privacy principles; Security measures

Please note that although the COA has the authority to process personal data pursuant to its mandate, it still bears the responsibility of following other rules and regulations laid out in the DPA, its IRR, and any other guidelines set by the National Privacy Commission (NPC). This means that COA must process personal data lawfully and fairly, with strict adherence to the general data privacy principles. It is important to note that personal data collected must be proportionate, adequate and not excessive in relation to the original purposes for which they were collected,[4] which is particularly relevant in the given scenario.

The COA is also required to implement reasonable and appropriate physical, organizational and technical security measures to ensure the protection of the processed personal data. Furthermore, it is also required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents which may lead to security breaches.[5] This is particularly significant as the data being processed are classified as sensitive personal information. Additionally, COA must ensure that the audit is confined only to data related to the COVID-19 National Vaccination Program, as specified in the engagement letter addressed to the DOH.

---

[2] § 2(1), Article IX-D, The 1987 Philippine Constitution.
[3] § 4(e), Data Privacy Act of 2012.
[4] § 11(d), Data Privacy Act of 2012.
[5] § 20 (c) (4), Data Privacy Act of 2012.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2024-002[1]

19 January 2024

[redacted]

Re: REQUEST FOR COMMENTS/INSIGHTS REGARDING THE USE OF ARTIFICIAL INTELLIGENCE (AI) IN THE CIVIL SERVICE COMMISSION'S (CSC) CORRESPONDENCE

Dear [redacted]:

We provide this Advisory Opinion upon the referral of the Department of Information and Communications Technology (DICT) as regards your request for comments and insights on the data privacy implications in the use of artificial intelligence (AI) for the Civil Service Commission's (CSC) correspondence.

On the use of AI in the processing of personal information; general principles; data subject rights; privacy impact assessment

According to the Organization for Economic Co-operation and Development (OECD), "[a]n AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."[2]

We reiterate the discussion in our 18 August 2023 letter that, at present, we see no manifest conflict with the use of AI in relation to the provisions of the Data Privacy Act of 2012 (DPA).
[3] The DPA recognizes the policy of the State to ensure the free flow of information and to

[1] Tags: Artificial Intelligence, General Principles of Privacy, Data Subject Rights, Privacy Impact Assessment.
[2] Organization for Economic Co-operation and Development (OECD), AI terms & concepts, *available at:* https://oecd.ai/en/ai- principles [last accessed date: 15 January 2024].
[3] An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

promote innovation and growth, alongside its duty to protect the fundamental human rights of privacy and of communication.

Section 4 of the DPA states that the law applies to the processing of all types of personal information, save for some exceptions. The DPA does not distinguish as to the type of technology used in the processing of personal information. Hence, whether the processing uses AI technology or not, the processing must abide by the provisions of the DPA as with other means and methods of processing information.

In other words, personal information controllers (PICs) who are processing personal information using AI technology must adhere to the general principles of privacy, have a lawful basis for processing, implement reasonable appropriate security measures, and uphold data subject rights, among other obligations under the DPA. Consequently, PICs are accountable for the means and methods they use in processing personal information.

Specifically for the principle of transparency in relation to the right of data subjects to be informed and right to rectify, the CSC must provide adequate information to data subjects and have mechanisms in place to enable them to exercise their rights. Please refer to NPC Advisory No. 2021-01: Data Subject Rights for further information.

In addition, the CSC should assess whether the use of any AI technology is fair and proportional to the purpose of processing, considering the risks to the rights and freedoms of data subjects. This may be done by conducting a privacy impact assessment (PIA). For further guidance on PIAs, please see NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments.

On the use of AI to improve correspondences and communication

We acknowledge that using AI has its advantages such as improving human productivity. The OECD has also acknowledged its potential:

> "Artificial Intelligence (AI) is a general-purpose technology that has the potential to: improve the welfare and well-being of people, contribute to positive sustainable global economic activity, increase innovation and productivity, and help respond to key global challenges. It is deployed in many sectors ranging from production, finance and transport to healthcare and security."[4]

On this note, we do not see any apparent issues in using AI, such as Chat Generative Pre- Trained Transformer (ChatGPT), to improve CSC's correspondence. However, we emphasize that if personal information is processed using such AI, PICs must implement proper safeguards to ensure the protection of the rights of data subjects.

[4] Organization for Economic Co-operation and Development (OECD), Recommendation of the Council on Artificial Intelligence [OECD/Legal/0449], *available at:* https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#:~:text=The%20OECD's%20work%20on%20Artificial,respond%20to%20key%20global%20challenges. [last accessed date: 15 January 2024]

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

cc : [redacted]

ADVISORY OPINION NO. 2024-003[1]

02 April 2024

[redacted]

Re: RANDOM SURVEILLANCE OF TELECOMMUTING EMPLOYEES AND CONSENT TO THE RECORDING OF VIRTUAL MEETINGS.

Dear [redacted]:

We respond to your request for an Advisory Opinion on the data privacy implications of the employee monitoring policies that your company intends to implement.

You state that your company is a business process outsourcing solutions and information technology-enabled services provider. As such, your employees regularly process personal information of customers, such as their full name, credit card number, card verification number, address, and phone number.

Your company allows its employees to telecommute, or work remotely, using either company-issued equipment or their own device. To provide an additional level of security to prevent mishandling or unnecessary disclosure of confidential data to unauthorized third parties, your company is considering the adoption of certain policies that involve the requisition of web cameras with built-in microphones that will be turned on at random intervals to record short videos (including image and audio) of the subject employee and his/her immediate surroundings. Also, your company intends to record all work-related virtual meetings, conferences, trainings, and coaching sessions.

Thus, you ask whether the Data Privacy Act of 2012[2] (DPA): 1) permits the installation of a monitoring software to randomly record telecommuting employees and their immediate surroundings for purposes of data security; and 2) requires your company to secure the written consent of the employees every time a work-related virtual meetings, conferences, trainings, and coaching sessions (collectively, "virtual meetings") is held.

---

[1] Tags: Telecommuting, monitoring software, employee surveillance, contract, legitimate interest.
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

Reasonable expectation of privacy.

Generally, the factual circumstances of each case determine the reasonableness of the expectation of privacy. Similarly, customs, community norms, and practices may limit or extend an individual's reasonable expectation of privacy. The reasonableness of a person's expectation of privacy is, thus, determined on a case-to-case basis.[3]

Nevertheless, it is worth revisiting our discussion in NPC Advisory Opinion No. 2018-090[4] on the application of this concept in the workplace, *viz.*:

> (C)ourts have generally held that employees have a decreased expectation of privacy with respect to work devices, email accounts, and internet surfing activities. The same may be said for the contents therein, since there is an assumption that its use will be limited to work-related purposes.
>
> Yet, with the DPA now in place, the reasonable expectation test should be revisited and interpreted in the context of the law.
>
> By virtue of a legislation on data protection and privacy, the assumption is that individuals now have an expectation of privacy. As to the second element, data privacy is now more than a reasonable expectation – it is now enshrined in the DPA. The reasonable expectation of privacy test then should take into consideration the standards provided under the DPA.
>
> This means that employees must be aware of the nature, purpose, and extent of the processing of his or her personal data in the workplace. The processing of personal information of employees shall also be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. Lastly, the processing of such information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

Scope of the DPA; personal information; processing; lawful basis; general data privacy principles.

The DPA applies to the processing of personal and sensitive personal information (collectively, personal data) and to any juridical person involved in the processing of personal information.[5] Personal information is defined as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[6]

Processing refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[7]

---

[3] National Privacy Commission, NPC Advisory Opinion No. 2018-090 (28 November 2018).
[4] *Id.*
[5] Data Privacy Act of 2012, § 4.
[6] *Id.* § 3 (g).
[7] *Id.* § 3 (j).

The installation of a monitoring software is considered as processing under the DPA since it involves the collection and/or recording of the employees' personal data. As such, a lawful basis must be established for processing of personal data under either Sections 12 or 13 of the DPA.

In the scenario you provided, your company may rely on either Section 12 (b) or 12 (f) of the DPA. Section 12 (b) of the DPA allows processing for the fulfillment of a contract with the data subject. You may utilize this basis as long as the employment contract provides specific provisions allowing the installation of equipment/software for furtherance of employment, including enhancement of productivity of telecommuting employees to ensure that they adapt with flexible working arrangements, for the protection of the interest of the clients or customers, or the enforcement of company policies. In which case, the installation of monitoring software is justified as a necessary consequence of the employer-employee relationship.

On the other hand, Section 12 (f) of the DPA allows processing if it is necessary for the purposes of the legitimate interests pursued by the PIC. We acknowledge that employers have legitimate business interests, such as management of workplace productivity, service quality control or enforcement of company policies, employee safety, protection of business assets, intellectual property or other propriety rights, prevention of vicarious liability where the company assumes legal responsibility for the actions and behavior of employees, compliance with statutory or regulatory obligations that provide, or give reasonable cause, for the preventive monitoring of employees,[8] amongst others. However, they must ensure that the processing activity should be directly related to the legitimate interest being pursued.

Thus, while the processing of personal information based on the legitimate interests of the PIC is allowed under the DPA, an employer must still assess if the installation of a monitoring software will pass the three-part test of legitimate interest, namely:

1. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;
2. Necessity test - The processing of personal information must be necessary for the purposes of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test - The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PICs or third party, considering the likely impact of the processing on the data subjects.

The processing must also comply with the general data privacy principles of transparency, legitimate purpose, and proportionality. In NPC Advisory Opinion No. 2018-084, we stated that it is incumbent upon the employer to determine the purpose/s of computer monitoring which must not be contrary to law, morals, or public policy. Additionally, the principle of proportionality directs the employer to assess the proportionality of the information collected, and the ways and means of processing. This means that the employer shall process information that is adequate, relevant, suitable, necessary, and not excessive in relation to the

[8] Privacy Guidelines: Monitoring and Personal Data Privacy at Work (April 2016), available at https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf (last accessed Feb. 23, 2024).

declared and specified purpose. Since the monitoring of the employees' surroundings may result in the capturing of personal data of other individuals, the company should determine whether the data collected is proportional to the achievement and fulfillment of the purpose of monitoring and that it clearly aligns with the need and objectives of the organization.[9] Lastly, to ensure adherence to the principle of transparency, the employer should effectively communicate to the employees, through the issuance and dissemination of a policy, the conduct of employee monitoring, the specific purpose, scope and actual method of monitoring, security measures to protect personal data, as well as the procedure for redress in cases where the rights of the employee as a data subject are violated.

As to your query on written consent of the employees for virtual meetings, please note that consent may not be the most appropriate basis for such processing since employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the company-employee relationship.[10] Instead, your company may still rely on either Sections 12(b) or 12(f) of the DPA as long as the recording of virtual meetings is work-related. Consequently, you may dispense with the requirement of obtaining the consent of employees every time virtual meetings are recorded.

Privacy Impact Assessment.

Finally, we recommend the conduct of a Privacy Impact Assessment (PIA) prior to the establishment and use of the proposed monitoring software or whenever there is a significant change in the software or software to assess and mitigate risks on the rights and freedoms of data subjects.

A PIA is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or a personal information processor (PIP). It considers the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations.[11]

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

---

[9] *Id.*
[10] ARTICLE 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, available at https://ec.europa.eu/newsroom/article29/items/610169 (last accessed Feb.22, 2024).
[11] NPC Advisory No. 2017-03, Guidelines on Privacy Impact Assessment, 31 July 2017.

ADVISORY OPINION NO. 2024-004[1]

16 May 2024

[redacted]

Re: ACCESS TO INDIVIDUAL USER ACCOUNTS BY SERVICE PROVIDER

[redacted]:

We respond to your request for an Advisory Opinion on whether the Data Privacy Act of 2012 (DPA)[2] permits an arrangement wherein a service provider such as Smile Technology Pte. Ltd. (Smile) may process personal information and sensitive personal information (collectively, personal data) by accessing individual user accounts from government or financial sites through a separate digital platform.

You state that your client, Smile, is a foreign company that is building a digital platform which provides companies with a unified application programming interface (API) to access the employment and income data of its users. Known as the Smile API, it is a single API for employment and income data in Asia which is accessible through Smile's website or through an integrated widget in the employer or service providers' applications (Third Party Apps). Smile API intends to provide comprehensive and verified employment data to aid banks, financial technology companies (fintechs), recruitment agencies, and other service providers in making informed decisions when evaluating loan applications, credit limits, and job candidates (Applicants).

You further state that Smile shall obtain the consent of the Applicants before processing their personal data, including processing for the purpose of disclosure to third parties. During the account creation process, the Applicants are informed of the nature, purpose and extent of the processing. The Applicants shall then signify their consent by actively checking a tickbox to Smile's Terms and Conditions and Privacy Policy which are readily available through Smile's platforms.

---

[1] Tags: automated access; personal information processor; consent.
[2] An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, (2012).

Thereafter, the Applicants shall provide their login credentials and link their accounts to government websites (*e.g.*, Social Security System [SSS] and Philhealth) and other third party platforms via Smile API. Smile shall then use automated means to log in to these sites and extract the Applicants' personal data.

Smile intends to collect and process personal data from various sources such as employment documents, human resource (HR) and payroll systems, gig economy platforms, and social security systems. In addition, Smile will access the Applicants' respective government accounts to retrieve real-time personal data. The personal data that Smile will process are the following:

1. Name
2. Home address
3. Email address
4. Telephone number – work
5. Age
6. Date of birth
7. Marital status
8. Education
9. Photo
10. Offense committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings
11. Information issued by government agencies peculiar to an individual:
    a. Unique identifiers (e.g. Tax Identification Number (TIN), Unified Multipurpose Identification (UMID) number, driver's license number, passport number, Government System Insurance Service (GSIS)/SSS number, voter's registration number, etc.)
    b. Licenses or its denials, expiry, suspension or revocation
    c. Tax returns
    d. Social security contributions
12. Actual and estimated income
13. Profiling and credit scoring data
14. Job performance
15. Social media profiles (e.g. Applicant's account data, user ID, linked accounts, profile information and login credentials)

If the Applicants wish to withdraw their consent, they can easily do so by pressing the "Disconnect Access" button provided in the Smile platforms, including Third Party Apps. Once consent is withdrawn, Smile will delete the personal data from its system within ten (10) minutes.

Thus, you inquire if Smile's access and extraction of personal data to the Applicants' corresponding user accounts, and the subsequent disclosure to its clients and third parties, are compliant with the DPA, its Implementing Rules and Regulations (IRR) and other issuances of the National Privacy Commission (NPC).

Processing based on consent.

Since the dataset that Smile plans to process involves both personal information and sensitive personal information, the processing of the entire data should find lawful basis under Section

13 of the DPA. Specifically, Section 13 (a) allows processing based on consent prior to the processing of personal data.

Consent, as defined under the DPA, is any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal data about and/or relating to him or her.[3] The DPA also requires that consent shall be evidenced by written, electronic or recorded means.[4]

To lawfully process personal data based on consent, Smile needs to guarantee that the consent obtained from the Applicants meets the standards required under the DPA and NPC's issuances.

It is essential that the Applicants are fully informed about how their personal data will be processed. The Applicants should be provided with clear and detailed information regarding the processing of their personal data, as well as any potential consequences that might result from giving their consent. Obtaining consent must be done in an honest and straightforward manner. This means that the information presented to the Applicants while obtaining consent must be communicated in plain and simple language that is easily comprehensible by the intended audience. The Applicants must also be informed of specific processing activities, such as the sharing of personal data with third parties.

It is worth noting that the Applicants, as data subjects, must be given a genuine choice to decline or retract their consent when processing personal data. This implies that the process for refusing or withdrawing consent should be straightforward and free from complicated procedures and requirements at any given time. Further, Smile must ensure that its online portals, through which user consent is obtained, do not employ any design elements or techniques aimed at manipulating or deceiving users into taking any action related to the processing of their personal data.[5] These types of design elements, known as deceptive design patterns, should be avoided.[6]

Smile must also be able to provide another option for those Applicants who do not wish to use the Smile platforms in the processing of their personal data, but still want to pursue their respective transactions/applications with Smile's clients. In such case, these individuals should be informed about other options on how to proceed with their application. Failure to comply with the requirements in obtaining lawful consent may result in possible penalties that may subject Smile to administrative fines or penalties.

Consequently, Smile can process the personal data of the Applicants by accessing their individual user accounts and collecting personal data from external websites, as long as the requirements on obtaining consent are followed. Once lawful consent is obtained, and the Applicants are informed about the nature, extent, and purpose of the disclosure prior to the processing, the subsequent disclosure of the same to clients such as employers and third parties may also be allowed.

Personal information processor; Accountability

---

[3] Data Privacy Act of 2012, Section 3 (b).
[4] Ibid.
[5] National Privacy Commission, Guidelines on Deceptive Design Patterns, NPC Advisory No. 2023-01, Section 2 (A) (7 November 2023).
[6] *Id.* Section 3.tt

A personal information controller (PIC) is an organization that controls the collection, holding, processing or use of personal information.[7] On the other hand, a personal information processor (PIP) is a natural or juridical person to whom a PIC may outsource or instruct the processing of personal data about a data subject.[8]

If a digital platform provider, like Smile, provides employment and income information to assist its clients in making their hiring and loan decisions, then it will be considered as PIP for this specific service.

Be that as it may, Smile must also comply with the requirements provided by the DPA and other relevant rules and regulations similar to a PIC. In addition, a PIP is also bound to adhere to the terms and conditions agreed upon in its contract with the PIC.[9]

As a PIP, one of the basic requirements is for Smile to designate a data protection officer (DPO) in the Philippines and register its processing systems with the NPC. Even though Smile is a foreign corporation and its processing activities happen outside of the Philippines, it is still obligated to comply with the DPA since it processes the personal information of Philippine citizens and residents.[10] Moreover, Smile must also comply with NPC Circular No. 2022-04 on the registration of personal data processing systems, a copy of which is available at https://privacy.gov.ph/wp-content/uploads/2023/05/Circular-2022-04-2.pdf.

Smile should also perform regular privacy impact assessments (PIA) to identify and evaluate potential privacy risks. These assessments should suggest measures to address and reduce the impact of these risks on the individuals whose data is being processed.

We highly recommend that a written agreement be executed between Smile and its PICs to ensure accountability in its processing. This agreement should clearly outline the obligations and liabilities of all parties involved, including their responsibilities to the data subjects.

We emphasize that if Smile processes personal data for any purpose other than providing useful information to its PICs, then it becomes a PIC for that specific processing activity. Consequently, Smile shall assume the concomitant obligations of a PIC under the DPA.

Rights of the data subject; data portability; retention policy; right to object

The Applicants using the Smile API must be informed of their rights as data subjects and given the opportunity to exercise them. Considering that the processing of personal data is based on consent, we emphasize its significance on the rights to access, object and data portability.

The right to access and portability are interrelated. The right to access allows a data subject reasonable access to, upon demand, the following:

1. Contents of his or her personal information that were processed;

---

[7] *Id.* Section 3 (h).
[8] *Id.* Section 3 (i).
[9] Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" [Implementing Rules and Regulations of Data Privacy Act of 2012], Section 45 (2016).
[10] Data Privacy Act of 2012, Section 6 (b).

2. Sources from which personal information were obtained;
3. Names and addresses of recipients of the personal information;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal information to recipients;
6. Information on automated processes where the data will or likely to be made as the sole basis of any decision significantly affecting or will affect the data subject;
7. Date when his or her personal information concerning the data subject were last accessed and modified; and
8. The designation, name or identity and address of the personal information controller.[11]

The right to data portability gives individuals the ability to obtain a copy of their personal data that has been processed or is being processed by a PIC in a commonly used electronic format that can be further used by the individual.[12] This right is based on the principle that individuals have the right to maintain control over their personal data that is being processed by a PIC, either through consent or contract, for commercial purposes, or through automated means.[13]

Individuals also have the right to object to the processing of their personal data. In case there is a significant change in the information that was provided to the data subject in a consent form, privacy notice or any similar communication, the data subject should be notified and allowed to object or withdraw their consent for the processing of their personal data.[14] Once a person withdraws their consent, any processing of their data must stop immediately, unless there are other lawful bases to continue. If personal information has already been shared with third parties with the consent of the person, they must immediately be informed of the objection.

It is important to note that the Applicants for employment or loans are considered as data subjects not only of Smile but also of the entities who engaged Smile for this specific purpose, and the corresponding organizations from which their personal data will be obtained (e.g., SSS, GSIS, Philhealth, etc.). For instance, when an individual uses Smile's platforms to apply for a job at Company A, they become a data subject of Smile and Company A. They also remain as data subjects of the organizations that Smile can access through the Applicant's accounts. However, it is important to note that, as the Applicants are utilizing the Smile API, Smile must allow them to exercise their data subject rights, and that they must have a mechanism in which these rights may be exercised.

General data privacy principles; Security measures

Personal data should only be collected for specified and legitimate purposes, which must be declared beforehand, and processed in a way that is compatible with the declared and specific purpose.[15] It is also crucial to maintain accurate and relevant personal data at all times.[16] Personal data processed should be proportionate, adequate and not excessive, limited to what is necessary for the intended purpose.[17] Moreover, personal data collected must be retained

[11] *Id.* Section 16 (c).
[12] *Id.* Section 18.
[13] Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 36.
[14] *Id.* Section 34 (d).
[15] Data Privacy Act of 2012, Section 11 (a).
[16] *Id.* Section 11 (c).
[17] *Id.* Section 11 (d).

only for as long as necessary for the fulfillment of the purposes for which the data was obtained.[18]

Thus, Smile must ensure that the processing of personal data is limited to the purpose of assessing an individual's eligibility for employment or loan. It is also important for Smile to have a retention policy on the personal data within its custody. This includes the retention of personal data of persons whose applications were not successful or did not proceed.

PIPs, like Smile, must also implement reasonable and appropriate physical, organizational and technical security measures to ensure the protection of the personal data under its custody. Furthermore, Smile is also required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents which may lead to security breaches.[19] Smile may consider industry best practices in the implementation of security measures.

In terms of compliance with the DPA, it is important to note that this is an ongoing process that requires regular evaluation of the effectiveness of security measures against current and potential risks. Furthermore, it is important to emphasize that a PIP's main objective should not be solely focused on compliance. Compliance is achieved when personal data is protected, and the rights of data subjects are upheld through appropriate and reasonable security measures.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

[18] *Id.* Section 11 (e).
[19] Data Privacy Act of 2012, Section 20 (c) (4).

ADVISORY OPINION
NO. 2024-005[1]

21 May 2024

[redacted]

Re: USE OF ARTIFICIAL INTELLIGENCE (AI) IN CALL ANALYSIS AND MONITORING OF CALL CENTER EMPLOYEES

[redacted]:

You inform that you represent a U.S. based company engaged in the hospitality business (Company). The Company operates a business process outsourcing subsidiary in the Philippines that provide customer services to its customers.

The Company is currently reviewing an Artificial Intelligence (AI) program, to be administered by a third-party system provider, that will analyze call recordings and email exchanges between its call center employees and customers (the "tool"). The tool will analyze the call recordings and emails using behavior and sentiment analysis to autoscore call center employees and rank them against other employees to identify opportunities for employee coaching and development, among others.

You further inform that AI-based analytics are performed on the interaction and will process the following personal data: names, address, job title and other unique identifier that could identify an individual or device. The analytics provide insights and autoscores the interaction of the customer and the employees. The autoscoring and predictions are limited to the call center employees and there are no rankings, scorings, or predictions on the customer level at this time.

You also mention that objections by employees may be raised to the Company's privacy team. If the team determines that the Company's interests do not outweigh that of the employee's, the employee can be opted out of the analysis.

The Company intends to rely on legitimate interest as the lawful criterion for processing personal data in connection with the proposed activity.

[1] Tags: Artificial intelligence; legitimate interest; proportionality; right to object.

Thus, you seek advice on the following concerns:

1. Whether the Company could rely on legitimate interest as its legal basis for processing personal information in connection with this activity?
2. Whether the use of automated scoring/analysis to aid in measuring performance, identifying coaching, and learning opportunities is justified given the above-stated purpose/interest?
3. Whether the employees have the right to object to the processing and whether such right outweighs the legitimate interest of the Company?

Personal information; lawful criteria for processing

The Data Privacy Act of 2012 (DPA) applies to the processing of all types of personal information and sensitive personal information (collectively, personal data). Personal information is defined as any information whether recorded in a material form or not, from which the identity of the individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[2]

The names, address, and other unique identifiers such as one's voice or speech pattern are considered as personal information. The DPA allows the processing of personal information when it is necessary for the purpose of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[3]

Section 3(a) of NPC Circular No.2023-07[4] defines legitimate interest as any actual and real interest, benefit, or gain that a Personal Information Controller (PIC) or third party may have in or may derive from the processing of specific personal information.

In *MAF v. Shopee*,[5] the National Privacy Commission (NPC) provided the following conditions for processing based on legitimate interest, *viz.*:

> (1) the legitimate interest is established; (2) the processing is necessary to fulfill the legitimate interest that is established; and (3) the interest is legitimate and lawful, and it does not override the fundamental rights and freedoms of data subjects

In determining if legitimate interest is established, the following must be considered:

> 1. The purpose of the specific processing activity must be specific, such that it is clearly defined and not vague or overbroad.

---

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, (2012).
[3] *Id.*
[4] National Privacy Commission, Guidelines on Legitimate Interest, NPC Circular No. 2023 – 07, (13 December 2023).
[5] National Privacy Commission, MAF v. Shopee Philippines, Inc. [NPC 21-167] (Sept. 22, 2022).

2. The purpose of the specific processing activity must not be contrary to laws, morals, or public policy following the principle of legitimate purpose; and

3. The interest established must be declared to the data subject prior to the processing or at the next practical opportunity, following the principle of transparency and the right of the data subject to be informed.[6]

Applying the above conditions to this case, the use of automated scoring to evaluate employee performance can be considered as a legitimate interest since it directly contributes to the Company's goal of improving its services. By assessing and identifying areas of improvement of its employees, the Company can enhance overall performance which will ultimately benefit both the employees and the Company.

Adherence to data privacy principles; legitimate purpose, proportionality

To determine whether the processing is necessary to fulfill the legitimate interest that is established, the means or method chosen for the specific processing activity undertaken by the PIC or third party should be necessary and lawful. Thus, the means to fulfill the legitimate interest must be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose, in accordance with the principle of proportionality; and the means chosen to accomplish the legitimate interest is itself lawful. The PIC cannot violate any law in the process of accomplishing its legitimate interest.[7]

In this case, you state that the Company's aim is to identify trends across interactions, supply additional feedback to other areas of the business, help in targeted training based on identified trends, among others. Hence, the personal data processed should be strictly used only for such purposes to comply with the second condition provided in the *MAF* case. Further, to comply with the principle of proportionality, the data to be collected should only be for the declared specified purposes made known to the employees.

It is important for the Company to strike a balance between its processing activities and the rights of its data subjects. Additionally, even if a personal information controller has a legal basis for processing information, it is still required to follow the fundamental data privacy principles of proportionality, transparency, and legitimate purpose. The processing of personal information must be limited only to the extent that is necessary for the stated purpose and that there are no other means to achieve such legitimate purpose.

Lastly, the principle of proportionality dictates that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. We advise that the use of the AI tool should be used only to achieve the goals and objectives of the Company stated in its privacy policy. The Company should also make sure that their employees are properly informed of this policy before the tool is utilized by the Company. This could be established and disclosed to the employees through the Company's privacy notice and policies.

---

[6] §6 *Id.*
[7] §7 *Id.*

Right to object; limitations

The right to object to the processing of personal data applies in instances where processing is based on consent or legitimate interest. Nevertheless, it is still possible to continue processing personal data despite the objection where, for example, the same is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship.[8] We refer to NPC Advisory No. 2021-01 on Data Subject Rights which provides:

> SECTION 7. Right to Object. — The data subject shall have the right to object to the processing of his or her personal data where such processing is based on consent or legitimate interest.
>
> x x x
>
> C. When a data subject objects, the PIC shall cease the processing of personal data and comply with the objection, unless the processing falls under any other allowable instances pursuant to in Sections 12 or 13, other than consent and legitimate interest.
>
> Should there be other grounds to continue processing the personal data, the PIC shall have the burden of determining and proving the appropriate lawful basis or compelling reason to continue such processing. The PIC shall communicate and inform the data subject of said lawful basis or compelling reason to continue processing.

Thus, the determination of whether the legitimate interest of the Company outweighs those of the employees' objections, or if they can cite other grounds to continue processing personal data is a matter that should be decided upon by the PIC and not the NPC.

Please be advised that the foregoing was rendered based solely on the information you provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

---

[8] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34 (b) (2) (2016)

ADVISORY OPINION NO. 2024-006[1]

03 June 2024

[redacted]

Re: CONFLICT OF INTEREST IN APPOINTING A DATA PROTECTION OFFICER

Dear [redacted]

We respond to your request for an Advisory Opinion on whether a conflict of interest may arise in the appointment of certain officers of [redacted] as its Data Protection Officer (DPO).

You state that [redacted] is a real estate development company. [redacted]'s management intends to appoint a new DPO. The primary candidate for the position is the Head of its Regulatory and Compliance Group (HRCG) who is also in charge of the Records Management Unit (RMU) and the Registration and Titling Unit (RTU). You aver that the RMU focuses on secure document storage and safekeeping, while the RTU handles the registration and titling of sold properties. Both units do not participate in determining the purposes and methods of data collection; their roles are exclusively dedicated to document safekeeping and liaising with administrative bodies. Instead, it is the Sales, Customer Service, and Human Resources units that have the decision-making powers in the processing of personal data. The alternative candidate is the Head of Systems and Methods (HSM), who oversees the Information and Technology Group, in case there is a finding of conflict of interest in the appointment of the HRCG.

Thus, you seek guidance on the propriety of the appointment of [redacted]'s DPO candidates.

Data Protection Officer; autonomy; conflict of interest

Under National Privacy Commission (NPC) Advisory No. 2017-01, a DPO must have a sufficient level of autonomy to perform their responsibilities effectively. While absolute autonomy is not mandated, the DPO must execute their duties independently.

[1] Tags: Data Protection Officer; conflict of interest; autonomy.

It is in this context that the propriety of the appointment of a DPO candidate must be determined. Based on our assessment of the facts presented, both the HRCG and the HSM have sufficient autonomy to execute their current responsibilities concurrently with the DPO position. Thus, we see no legal hindrance in their appointment as a DPO.

We recognize, though, that there may be conflict of interest situations that may arise in the course of the performance of the DPO functions of either the HRCG or HSM. In which case, you may consider the guidelines from Article 29 of the Data Protection Working Party of the European Commission - Guidelines on DPOs,[2] to determine whether there would be potential conflict of interest:

- Identification of the position/s which would be incompatible with the function of DPO;
- Draft internal rules to avoid conflicts of interests;
- Provide an explanation about conflicts of interests;
- Declare that the DPO has no conflict of interests with regard to his/her function as a DPO, as a way of raising awareness of this requirement;
- Include safeguards in the internal rules of the organization and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interest.

Additionally, please note that registering a DPO is solely for the purpose of appointing an official contact for the NPC. Internally, an organization may appoint or designate more than one DPO or establish a data privacy structure that is best suitable for its needs. [redacted] is neither restricted nor prohibited from appointing more than one DPO under the DPA.

Please be advised that the foregoing was rendered based solely on the information you provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

[2] European Commission, Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2017, page 16, available at https://ec.europa.

ADVISORY OPINION
NO. 2024 - 007[1]

02 July 2024

[redacted]

Re: DISCLOSURE AND RELEASE OF INCIDENT REPORTS BY AN EDUCATIONAL INSTITUTION.

Dear [redacted]

We respond to your request for guidance on the release of incident reports containing personal information of individuals.

Specifically, you seek guidance on whether Calayan Educational Institution, Inc. (CEFI) may release incident reports under the following circumstances:

1. Sans any court order, is it permissible under the Data Privacy Act and other existing regulations to release incident reports to parties directly involved in the incidents, knowing that personal information of other individuals may be disclosed within these reports?

2. Sans any court order, is it permissible under the Data Privacy and other existing regulations to release incident reports to parties not directly involved in the incidents but mentioned in said reports, knowing that personal information of other individuals may be disclosed within these reports?

3. What should CEFI do to safeguard the right to privacy of individuals whose personal information is contained within incident reports when considering request for copies of or access to such reports?

4. What specific protocols or procedures should requesting parties follow or adhere to when seeking access to or copies of incident reports, particularly in cases where personal information of other individuals may be disclosed.

[1] Incident reports; court order; proportionality; law enforcement.

5. Can CEFI be held liable for refusing to release incident reports despite request from involved parties or those mentioned in the reports?

6. Can the Office of the Prosecutor and other government agencies such as the Department of Education (DepEd) and/ or the Commission on Higher Education (CHED) compel the production or release of reports or other documents containing personal and/or other confidential information in conducting investigations and/or in aid of cases/ complaints filed before them?

7. During investigations conducted by government agencies such as the DepEd and CHED of complaints filed by or against our institution, may our institution submit evidence containing personal and other confidential information in its defense?

Considering that the issues you present are interrelated, we shall address them jointly in the discussions below.

Lawful criteria for processing; Adherence to Data Privacy Principles

The disclosure or sharing of personal and sensitive personal information (collectively, personal data) is considered as processing under the Data Privacy Act of 2012 (DPA). An incident report is a document which contains sensitive personal information because it necessarily involves information concerning an infraction committed or alleged to have been committed by an individual.[2] In NPC Advisory Opinion 2020-013[3] we stated that processing of sensitive personal information shall be considered lawful when it fulfills any one of the criteria listed under Section 13 of the DPA.

In response to questions 1, 2, 6 and 7, in general, the processing of sensitive personal information is prohibited, unless it is necessary for the protection of lawful rights and interests of natural or juridical persons in proceedings, or for the establishment, exercise or defense of legal claims, or when provided to government or public authority in the exercise of their mandate.[4] Therefore, disclosure of sensitive personal information is permissible even without a court order if based upon the foregoing circumstances regardless if the disclosure is made to those directly involved, those merely mentioned, or to public authorities in the exercise of their mandate.

But as we stated in NPC Advisory Opinion 2018-071,[5] even if the DPA recognizes processing of personal data pursuant to the mandate of government agencies, the processing must still adhere to the principles of transparency, legitimate purpose, and proportionality. Personal information must be collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified, and legitimate purpose only. This means that the phrase, "necessary for law enforcement purposes" found in paragraph (e), Section 4 of the DPA is not a weapon that can be indiscriminately wielded by any agency that invokes it. The law enforcement agency must establish its mandate to enforce a particular law, and more importantly, that they are not unreasonably infringing on the rights of individuals guaranteed

[2] Data Privacy Act 2021, § 3 (l) (2).
[3] National Privacy Commission, NPC Advisory Opinion No. 2020-013 (21 February 2020).
[4] Ibid. § 13
[5] National Privacy Commission, NPC Advisory Opinion No. 2018--071 (5 October 2018).

by the Constitution. Failure to establish both grounds renders the processing unnecessary and contrary to law.[6]

We wish to emphasize that an incident report serves to paint a full picture of the truth behind what transpired, and ultimately to advance the lawful rights and interests of those involved. Thus, withholding necessary and vital information under the guise of protecting privacy rights would render its purpose nugatory.

Protocols in Data Protection

In response to questions 3, 4 and 5, the manner of exercising a data subject's right to access would vary from every Personal Information Controller (PIC). As such, there is no catch-all protocol to be followed. An educational institution such as CEFI, however, is required to draft organizational policies that will uphold the rights of the data subject including their right to access. PICs are empowered to establish such reasonable standards and guidelines for data protection and implementation which include the limitation of such rights. Among others, a PIC may limit the exercise of data subject rights when a legitimate purpose exists in justifying such limitation. An example of such limitation may include restriction of certain information through redaction. This limitation on the data subjects' rights is based on the principle of proportionality[7] which essentially provides that the processing of information should be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. You may check our website at privacy.gov.ph for additional resources and guidance on procedures and policies concerning a data subject's right to access. Moreover, a PIC should also keep in mind other governing laws from other regulators in crafting its protocols.

In all cases, however, the restrictions should be in proportion to the purpose of such limitation.[8] For instance, where a PIC denies or limits the exercise of data subject rights, the PIC should ensure that the data subject is clearly and fully informed of the reason for the limitation or denial.[9] CEFI as a PIC can be held liable for an unjustified refusal to release incident reports to concerned parties.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

---

[6] National Privacy Commission, NPC Advisory Opinion No. 2023-18 (29 September 2023).
[7] Data Privacy Act 2021, § 11
[8] National Privacy Commission, NPC Advisory Opinion No. 2021-001 (19 January 2021).
[9] Ibid.

ADVISORY OPINION NO. 2024-008[1]

09 July 2024

[redacted]

Re: DISCLOSURE OF PUBLIC DOCUMENTS RELATIVE TO A LOCAL GOVERNMENT UNIT'S PURCHASE OF REAL PROPERTIES.

Dear [redacted]

We respond to your request for an Advisory Opinion on the propriety of disclosing several documents relative to the purchase of two (2) real properties by the City of San Pedro, Laguna (the "LGU").

You state that you received a request from a citizen and taxpayer of the LGU asking for copies of the following documents:

1) Authority to enter into a Contract of Sale from the Sangguniang Panlungsod;
2) Determination of the Purchase Price from the Assessment Committee;
3) Notarized Deed of Sale between the City Government and the Owner-Sellers;
4) Certificate of availability of funds from the City Budget Officer;
5) Official voucher relative to the purchase and copies of checks issued in the names of the Owner-Sellers;
6) Certificate from National Agencies issued for this purpose; and
7) Other related documents submitted to the Commission on Audit.

Recognizing that some of the documents contain personal and sensitive personal information (collectively, "personal data"), you seek guidance from the National Privacy Commission (NPC) on the following concerns: (1) Whether the request may be granted even if the afore- mentioned documents contain personal and sensitive personal information; and (2) The manner and parameters in which the processing may be conducted, if allowed.

[1] Tags: Public documents, scope of the DPA, freedom of information.

Access to public documents; scope of the DPA; Freedom of Information.

The Data Privacy Act of 2012 (DPA)[2] acknowledges that certain public documents containing personal data are outside its scope, thus:

> SEC. 4. *Scope.* – This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: *Provided,* That the requirements of Section 5 are complied with.
>
> This Act does not apply to the following:
>
> (a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
>
> (1) The fact that the individual is or was an officer or employee of the government institution;
> (2) The title, business address and office telephone number of the individual;
> (3) The classification, salary range and responsibilities of the position held by the individual; and
> (4) The name of the individual on a document prepared by the individual in the course of employment with the government.[3] (emphasis supplied)

Furthermore, NPC Advisory No. 2017-02 provides for factors that must be considered by a government agency or office when resolving a request for access to public documents, *viz.*:

1. The information requested falls under matters of public concern;
2. The individual requesting for personal data has declared and specified the purpose of his or her request;
3. The declared and specified purpose is not contrary to law, morals, public policy; and
4. The personal data requested is necessary to the declared, specified, and legitimate purpose.[4]

Relative to requests for disclosure of public documents emanating from government agencies, Executive Order No. 02[5] recognizes the right of the people to have access to information, official records, and to documents and papers pertaining to official acts, transactions, or

---

[2] An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, (2012).

[3] Emphasis supplied.

[4] National Privacy Commission, NPC Advisory No. 2017-02 (3 April 2017).

[5] Office of the President, Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies to Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor, Executive Order No. 2 [EO No. 2] (July 23, 2016).

decisions, which are in the possession or under the custody of the government and relating to matters of public concern. Nevertheless, EO No. 2 clarifies that it is not without limitation as it recognizes certain exceptions in its application as enshrined in the Constitution, existing laws, or jurisprudence.

Based on the foregoing, the disclosure of documents to the requester relative to the purchase of real properties may be allowed pursuant to EO No. 2 since the information contained in these documents involve matters of public concern. Likewise, the personal data of public officers which are included in these documents can also be disclosed in light of Section 4 (a) of the DPA.

However, we note that while the requested documents may be disclosed, it must only be to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned.[6] Accordingly, there is a need to balance, on a case- to-case or per document basis, the right to information of the public and the right to data privacy of government personnel.

Thus, where the documents or forms contain personal data of the government officer or employee which is no longer of public concern, government agencies as personal information controllers (PICs) may redact such personal data prior to the release of such documents.[7]

Legitimate interest; general data privacy principles.

As to the personal data of private individuals which may be part of the data requested, you may rely on Section 12 (f) of the DPA. Such provision permits the processing of personal information when it is necessary for the purpose of the legitimate interests pursued by the PIC or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

Section 3(a) of NPC Circular No. 2023-074[8] defines legitimate interest as any actual and real interest, benefit, or gain that a personal information controller (PIC) or third party may have in or may derive from the processing of personal information. However, processing based on a legitimate interest may only be relied upon when it involves processing of personal information and not when it involves sensitive personal information.

Please note that the determination of whether legitimate interest is established rests upon the PIC. The case of *MAF vs. Shopee*[9] is highly instructive on this matter, *viz.*:

> In determining if legitimate interest is established, the following must be considered:
>
> (1) The purpose of the specific processing activity must be specific, such that it is clearly defined and not vague or overbroad;
> (2) The purpose of the specific processing activity must not be contrary to laws, morals, or public policy following the principle of legitimate purpose; and

[6] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (a)(1) (2016).
[7] National Privacy Commission, NPC Advisory Opinion No. 2019-026 (24 April 2019).
[8] National Privacy Commission, Guidelines on Legitimate Interest, NPC Circular No. 2023-07, (13 December 2023).
[9] National Privacy Commission, MAF v. Shopee Philippines, Inc. [NPC 21-167] (22 September 2022).

(3) The interest established must be declared to the data subject prior to the processing or at the next practical opportunity, following the principle of transparency and the right of the data subject to be informed.

The processing must also comply with the general data privacy principles of transparency, legitimate purpose, and proportionality. Particularly applicable to your concern is the principle of proportionality which requires PICs to assess the proportionality of the information processed, and the ways and means of processing. This means that that PIC shall only grant access to such information that is adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose.

Since the public documents requested may contain personal data of private individuals, the PIC shall determine whether the data requested is proportional to the purpose of the requester.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2024-009 [1]

23 July 2024

[redacted]

Re: Use of Personal Information in Election Proceedings

Dear [redacted]

We respond to your request for guidance on the proper use of personal information in the conduct of elections for sectoral representatives pursuant to the LPG Industry Regulation Act (LPG Act).[2]

You inform that the Department of Energy (DOE) and the Department of Trade and Industry (DTI) established a task force to regulate the safe operations of the Liquified Petroleum Gas industry, consistent with the LPG Act and Joint Department Circular No. (JDC) 2022-11-0002.[3] One of the duties of the task force is to issue the guidelines for the selection of Sectoral and Regional Program Implementation Task Force (RPITF) Representatives and Members of the National Program Policy Task Force (NPPTF).

Thus, the DOE drafted the guidelines for the composition, selection and voting of Sectoral Representatives and Members of the RPITF and NPPTF. The draft guidelines provide for the creation of an election committee in charge of the election of sectoral representatives. It also tasks the DOE to publish and provide the election committee with all the relevant personal information of individuals who wish to take part in the election, such as: 1. business name of LPG establishment; 2. name of the owner; 3. name of authorized representative; and 4. business address.

[1] Sec. 12 DPA, Personal Information, Fulfillment of Mandate, Publication.
[2] An Act Establishing The Regulatory Framework For The Safe Operations Of The Liquefied Petroleum Gas Industry, Delineating The Powers And Functions Of Various Government Agencies, Defining And Penalizing Certain Prohibited Acts, [LPG Industry Regulation Act, 2021] Republic Act 11592 (2021)
[3] Department of Energy, Joint Department Circular No. JDC2022-11-0002, "LPG Cylinder Exchange, Swapping, and Improvement Programs and Its Implementing Guidelines" (25 November 2022)

Hence, you seek guidance on how to properly process the foregoing data for the elections consistent with the Data Privacy Act.[4]

Scope of the DPA; Personal Information

The DPA applies to the processing of personal information.[5] Personal information is defined as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual[6]. Meanwhile, processing refers to any operation or any set of operations performed upon personal information including, but not limited to the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.[7]

Please note that personal information under the DPA refers to personal information of natural persons. Thus, the processing of a business name and business address of LPG establishments belonging to corporate entities is not considered as personal information under the DPA.[8] Conversely, when the information refers to natural persons such as that of the business owner or authorized representative of the LPG establishment, it is considered as personal information under the DPA and, as such, its processing is subject to its provisions.

Lawful Criteria for Processing; Fulfillment of Mandate; Proportionality Principle

Sec. 12 (e) of the DPA provides that a public authority's statutory mandate is one of the lawful criteria for the processing of personal information.[9] In this case, the lawful criteria by which the DOE can share and publish personal information is the LPG Industry Regulation Act[10] together with the DOE's general mandate of improving LPG programs under the JDC. Thus, in furtherance of its mandate, the DOE may share the personal information it has gathered to the election committee and publish the same to better facilitate the conduct of the elections.

In line with the proportionality principle of the DPA, sharing and publication of the foregoing personal information must be limited to the fulfilment of DOE's mandate. This means that the DOE may only share the necessary personal information only to facilitate the conduct of the elections.

It is worth mentioning that the election committee will also be considered as a personal information controller (PIC) under the DPA as it will be in possession of personal information of nominated individuals. As with the DOE, the use of personal information gathered should

[4] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

[5] Ibid. § 4

[6] Ibid. § 3 (g)

[7] Id. § 3 (j)

[8] National Privacy Commission, NPC Advisory Opinion No. 2020-052 (27 November 2020)

[9] Data Privacy Act of 2012, § 12 (e).

[10] LPG Industry Regulation Act (2021), § 5

be limited only to the declared and specified purpose/s which are for the composition, selection, and voting of sectoral representatives and members of the RPITF and NPPTF.

Hence, any other use of personal information not aligned with the abovementioned purposes would contravene the DPA.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN IV
Director IV, Privacy Policy Office

ADVISORY OPINION
NO. 2024 - 010[1]

30 September 2024

[redacted]

Re: DISCLOSURE OF COOPERATIVE MEMBER'S LOAN LEDGERS

Dear [redacted],

We respond to your request for an Advisory Opinion concerning various issues involving the disclosure of loan ledgers containing the personal data of cooperative members. Specifically, the following queries were posed:

> *Q1 (on DISCLOSURE): Can the Coop Office release/disclose the loan ledgers of Member A to Member B considering they also contain personal data (including financial) of Member A?*
>
> *Q2 (on AUTHORITY TO DISCLOSE): If YES to Q1, who shall authorize the disclosure, shall it be the Cooperative Chairman being the highest Coop officer?*
>
> > *Q2.1. What if the highest Coop Officer also considers NOT authorizing the disclosure of said loan ledgers?*
> > *Q2.2. Can we elevate it to the Coop General Assembly (being the highest decision- making body in a Cooperative) and they can be the one (as a GA) to decide whether to disclose the ledgers or not?*
>
> *Q3 (on CONSENT): Do we still need to get the consent of Member A about the Coop disclosing his loans ledgers (considering that he transferred his loan anyway to Member B)? Note: As for the consent, we already asked the consent of Member A about it and he signified that he will not provide consent.*
>
> *Q4: If NO to Q1, can the Coop issue a Statement of Account which also reflects the contents of the ledgers without other personal data and as long as it is Certified Correct by a Coop Officer?*

[1] Tags: Coop Loan ledger; Disclosure; Lawful processing.

Q5: If it's okay to ask, what other pertinent Philippine law/s apply to the stated situation? Note: Our Audit Committee hinted that a BSP ruling exempts the issuance of ledgers/info of a transferred loan from the DPA 2012. Will that said BSP ruling apply?

Considering that the issues raised are interrelated, we shall address them jointly below.

Personal Information; Sensitive Personal Information; Criteria for Lawful Processing

Personal information is defined under Republic Act (R.A) No. 10173, or the Data Privacy Act of 2012 (DPA),[2] as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual[3].

On the other hand, sensitive personal information refers to personal information:

> *(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;*
>
> *(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;*
>
> *(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and*
>
> *(4) Specifically established by an executive order or an act of Congress to be kept classified.*[4]

Meanwhile, processing is defined as any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data[5].

Thus, the disclosure of personal and sensitive personal information (collectively referred to as "personal data") from an individual or entity to another is considered processing under the DPA.

In this case, the loan ledgers and statements of account (SOA) are documents that contain personal data as they necessarily include information about [redacted] members such as their name, address, and contact details. We assume it also includes [redacted] members' financial records and transaction histories. Hence, the processing either of the loan ledgers or SOA

---

[2] An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

[3] *Id.*, §. 3(g)

[4] *Id.*, §. 3(l)

[5] *Id.*, §. 3(j)

should be based on any of the following lawful criteria for processing under Sections 12 and 13 of the DPA, *to wit*:

> *SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when **at least one** of the following conditions exists:*
>
> *(a) The data subject has given his or her consent;*
> *(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;*
> *(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;*
>
> *xxx*
>
> *(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.*
>
> *SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:*
>
> *(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;*
> *(b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;*
>
> *xxx*
>
> *(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;*
>
> *xxx*

Based on these provisions, lawful processing of personal data is not always anchored on consent, as there are other criteria which may be more appropriate that may be invoked by the personal information controller (PIC).

Thus, the disclosure of the loan ledgers and/or SOAs of [redacted] members to other members even without the member's consent is permissible if it is based on any of the circumstances cited under Sections 12 and 13.

Appointment of Data Protection Officer; Obligations of [redacted] as PIC

The decision to disclose personal data rests with [redacted] and its process owner.[6] If no process owner is identified, [redacted], through its Board or General Assembly and in consultation with its Data Protection Officer (DPO), may decide whether and how much personal data will be disclosed.[7]

Please note that NPC Circular 22-04[8] requires PICs to designate and register a DPO, who shall be responsible for ensuring compliance with the DPA, its IRR, NPC issuances, and other relevant laws. The DPO may be consulted and may be allowed to participate in meetings of senior and middle management to represent the interest of the members.

It is important to note that the registration and designation of a DPO is a legal requirement imposed upon PICs like [redacted]. For further guidance, you may check https://privacy.gov.ph/appointing-a-data-protection-officer/.

Rights of the Data Subjects

[redacted]'s Data Protection Officer (DPO) or its Board of Directors or General Assembly, whichever is applicable, must also consider the Rights of the Data Subject[9] when disclosing its members' personal data.

These rights are likewise recognized in the Cooperative Development Authority (CDA)'s Memorandum Circular No. 2023-14[10] or the CDA Implementing Rules and Regulations of the Financial Products and Services Consumer Protection Act (CDA FCPA IRR). It relevantly states that financial consumers have the right to expect that their financial transactions, as well as all personal information disclosed in the course of their transactions with CDA-Regulated Entities (CDAREs) are kept confidential and secured at all times. CDAREs are required to uphold privacy and protect the data of their financial consumers.

Data Privacy Principles; Appropriate Security Measures

As a PIC, [redacted] is mandated by the DPA to adhere to the data privacy principles of transparency, legitimate purpose, and proportionality[11]. The principle of transparency dictates that the data subject must be aware of the nature, purpose and the extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the PIC, his or her rights as a data subject, and how these can be exercised[12]. The principle of legitimate purpose mandates that the processing of personal data shall be compatible with a declared and specified purpose, which must not be contrary to law, morals,

---

[6] Data Privacy Act of 2012, §. 20(e).
[7] Data Privacy Act of 2012, §. 12.
[8] National Privacy Commission, NPC Circular 2022-04 (05 December 2022)
[9] Data Privacy Act of 2012, §. 16.
[10] Cooperative Development Authority, Memorandum Circular No. 2023-14 (11 July 2023)
[11] Data Privacy Act of 2012, §. 11.
[12] Implementing Rules and Regulations of the Data Privacy Act of 2012, Rule IV, § 18.

or public policy. Lastly, the principle of proportionality requires that the processing of personal information shall be adequate, suitable, necessary, and not excessive in relation to the purpose sought to be achieved by the PIC.

Hence, should the [redacted] disclose the information being requested, they must comply with the foregoing principles. Otherwise, it may not be considered as lawful processing under the DPA. Further, NPC Circular 2023-06[13] requires PICs to implement reasonable and appropriate organizational, physical, and technical security measures to ensure the protection of personal information against any accidental or unlawful destruction, alteration, or disclosure, and against any other unlawful processing. As a PIC, the [redacted] must consider the issues it may encounter in the improper disclosure of personal data. This also includes the requirement to conduct privacy impact assessments to identify and assess various privacy risks and propose measures intended to address and mitigate their effect on the data subjects. We emphasize that the DPA, its IRR, and other issuances of the NPC do not prohibit cooperatives from conducting their day-to-day activities and transactions

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

[13] National Privacy Commission, NPC Circular 2023-06 (01 December 2023)

ADVISORY OPINION NO. 2024-011[1]

12 November 2024

[redacted]

Re: REQUEST OF DEATH CERTIFICATES FOR THE PROCESSING OF INSURANCE CLAIMS

Dear [redacted]

We respond to your request for an Advisory Opinion on the propriety of releasing the death certificate of war veteran-pensioners (pensioners) either to [redacted] or [redacted] for the processing of insurance claims.

You inform that [redacted] grants loans to pensioners pursuant to its partnership with the [redacted] The loans are paid through the pensioners' monthly pension from [redacted] The pensioners are covered by life insurance that in the event of demise, the proceeds will be applied to the loans and the excess, if any, shall go to the pensioners' heirs. [redacted] a wholly owned subsidiary of [redacted] facilitates the processing of the insurance claims on behalf of [redacted] owns an insurance company currently servicing the insurance requirements of [redacted][2]

Upon the death of the pensioners, their heirs are entitled to claim burial and other death benefits from the [redacted] The process involves submission of the pensioners' death certificates which serve as proof of death. The death certificates are also supposed to be submitted to [redacted] for the processing of insurance claims to settle any outstanding loan of the pensioner. Most of the time, however, the heirs fail to submit a copy of the death certificate to [redacted] Accordingly, [redacted] requested for copies of the death certificates from the Philippine Statistics Office (PSA) and [redacted] but both offices denied the request citing the Data Privacy Act of 2012 (DPA).

Hence, this request for an Advisory Opinion.

---

[1] Tags: personal data; lawful criteria for processing, sensitive personal information, establishment or exercise of legal claims, legitimate interest, fulfillment of contractual obligations; general data privacy principles.

[2] [redacted] available at [redacted] (last accessed 09 October 2024).

Death Certificate; personal data

A death certificate is an official document setting forth particulars relating to a person's death.[3] It contains the following details relating to an individual, namely:

a) date and place of death,
b) full name,
c) age,
d) sex,
e) occupation or profession,
f) residence,
g) marriage status,
h) nationality of the deceased, and
i) proximate cause of death.[4]

Under the DPA, personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[5]

On the other hand, sensitive personal information (SPI) refers to personal information:

1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4) Specifically established by an executive order or an act of Congress to be kept classified.[6]

Based on the definitions above, a death certificate contains both personal and sensitive personal information (collectively referred to as "personal data"). As such, the processing of a death certificate requires the establishment of the applicable lawful basis provided for in Sections 12 and 13 of the DPA.

Lawful criteria for processing

[redacted]'s request for the death certificates of its deceased debtor-pensioners for the settlement of their financial obligations finds bases under Sections 12 (b) and 13 (f) of the DPA which respectively provides:

> *Section 12. Criteria for Lawful Processing of Personal Information* – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

[3] Philippine Statistics Authority, Death Certificate, available at https://psa.gov.ph/death-certificate (last accessed 04 September 2024).
[4] §6, Law on Registry of Civil Status, Act No. 3753 (1930).
[5] §3(g), Republic Act No. 10173.
[6] *Id.*, §3(L).

xxx

(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract.

xxx

Section 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

xxx

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

The provision of the insurance policy pertinently states:

> *Section 7. Amount of Claim Payment.* – In the event of a claim, *xxx* shall pay to [redacted] the amount which shall not exceed the outstanding loan balance at the time of the death of the insured/borrower.

Related to the above provision, the consent clause states:

> I/we hereby ***consent and authorize*** [redacted] ***to*** collect, use, ***process***, store, update, and disclose all of my information, personal and otherwise, ***relative to any loan***, products, services, facilities or channels that I/we may avail of now or in the future from the bank. *xxx*
>
> I/we hereby consent to the transfer, ***disclosure***, and communication of any information *xxx* ***from*** [redacted] ***to its*** branches, ***subsidiary,*** **agents** and representatives and third parties *xxx* selected by [redacted] (collectively referred to as the "Receiving and Disclosing Parties") for the following uses, including but not limited to: (i) the ***provision of any products and services***; *xxx* (viii) ***management of loan*** and (ix) disclosure and sharing of information under any applicable law, regulation, court, regulator or legal process. *(Emphasis supplied)*

In cases where the creditor obtained the insurance policy on the life of its debtors, the processing of the insurance claims usually involves the creditor securing and submitting the necessary proofs of death to the insurance company. In a case with a similar factual milieu,[7] the Supreme Court took cognizance of a provision in the mortgage redemption insurance policy[8] which states that the death benefit is payable to the creditor upon receipt and approval of the necessary proof of death. Similar to this case, we understand that [redacted] secured a policy on the life of its debtors as a form of security whereby the proceeds shall cover the pensioners' inability to repay the loan. Through the insurance policy, the pensioners consented to the processing of their personal information including the disclosure of the same to [redacted] for the provision of any products or services and/or management of loan. Given the consent provided by the debtor-pensioners, it appears that either [redacted] or its agent/subsidiary, [redacted] may request for the release of the debtor-pensioners' death certificate for purposes of the processing of the insurance claim.

As to the processing based on Section 13(f) of the DPA, please note that such criterion does not require a court order or an existing court proceeding for it to apply. It is enough that the

[7] Noda v. Social Security System, G.R. L-57834, 12 November 1981.
[8] The mortgage redemption insurance policy was procured by SSS on the life of its principal debtor.

processing is for the establishment of a legal claim. You may refer to NPC Advisory 2024-02 dated 12 August 2024[9] for the other requirements of processing based on Section 13(f).

General data privacy principles;
Reasonable and appropriate security measures

It should be stressed, however, that even if the processing is supported by one of the cited lawful criteria, the processing must strictly adhere to the data privacy principles of transparency, proportionality, and legitimate purpose as well as the implementation of appropriate security measures.

The principle of proportionality is of particular relevance to the present concern. Proportionality, as required under Section 11 of the DPA, requires that the personal data sought must be necessary for purposes for which it is to be used, that it must be adequate and not excessive in relation to the purposes for which they are collected and processed. It also requires that the personal data must be retained only for as long as necessary for the fulfillment of the purposes for which it was obtained. Further, personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

We note that the insurance policy only requires a satisfactory proof of death of the insured.[10] As such, if the insurer's requirement is only a confirmation of the fact of death, you may also consider as an alternative a certification to that effect from either the [redacted] or PSA, particularly in view of the PSA's Memorandum Circular (MC) No. 2019-15 dated 11 June 2019 restricting access to copies of civil registry documents, such as death certificates.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

[9] Guidelines on Personal Data Processing Based on Section 13(f) of the Data Privacy Act of 2012.
[10] §8, General Insuring Provisions, Group Credit Life Insurance Policy.

ADVISORY OPINION NO. 2024-012[1]

16 October 2024

[redacted]

Re: RIGHT TO INSPECT CORPORATE RECORDS VIS-À-VIS THE DATA PRIVACY ACT OF 2012.

Dear [redacted]

We respond to your request for an Advisory Opinion regarding the relation between the right of a stockholder to inspect corporate records under Section 73 of the Revised Corporation Code of the Philippines (RCC)[2] and the Data Privacy Act of 2012 (DPA).[3]

You state that your client, Tibiao Bakery Inc. (TBI), received a request from a law office representing certain stockholders to be furnished with a statement of account detailing the advances made by TBI to its officers and employees, including their names, dates, and amounts of the advances, and the relevant supporting board resolution.

In response, TBI allowed the examination of its books and records subject to the following conditions:

- The examination of books and records of TBI pertaining to the advances to its directors, officers, stockholders and employees is allowed subject to compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA)
- That the data subject should give his or her consent, specific to the purpose prior to the processing;
- That [redacted], in his capacity as administrator of the Estate of [redacted], has given his consent to examine the books and records of the corporation pertaining to the

[1] Tags: personal information, sensitive personal information, lawful processing, Corporation Code, inspection of corporate books and records, data subject rights
[2] An Act Providing for the Revised Corporation Code of the Philippines, [Revised Corporation Code of the Philippines], R.A. 11232 (2019)
[3] An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

advances of the late [redacted];

- That the examination shall be limited only to those who gave their consent; and
- That the undersigned is requested to submit a request for Advisory Opinion to the NPC.

On the agreed date of the examination, the law office argued that they were not required to obtain the consent of the other stockholders as their request is based on Section 73 of the RCC in relation to Sections 12(c) and 13(b) of the DPA. As such, they have an unqualified and absolute right to inspect corporate records.

Thus, TBI presents the following issues:

- Whether TBI must secure the prior consent of the data subjects who are the subject of the demand to inspect; or
- If TBI is allowed by law to favorably act on the demand to inspect even in the absence of the aforesaid prior consent, if it is obligated to provide the demanded "statement of account," notwithstanding the language of Section 73 of the Revised Corporation Code.

The right to inspect corporate records vis-a-vis the right to data privacy.

For a thorough understanding of the matter at hand, it is imperative to consider the provisions of the applicable laws and relevant jurisprudence regarding the concerns you raise.

Section 73 of the RCC recognizes the stockholders' right to inspect corporate records, *viz.*:

> SEC. 73. Books to be Kept; Stock Transfer Agent. -- Every corporation shall keep and carefully preserve at its principal office all information relating to the corporation including, but not limited to:
>
> xxx
>
> (d) A record of all business transactions;
>
> (e) A record of the resolutions of the board of directors or trustees and of the stockholders or members;
>
> xxx
>
> Corporate records, regardless of the form in which they are stored, shall be open to inspection by any director, trustee, stockholder or member of the corporation in person or by a representative at reasonable hours on business days, and a demand in writing may be made by such director, trustee or stockholder at their expense, for copies of such records or excerpts from said records. The inspecting or reproducing party shall remain bound by confidentiality rules under prevailing laws, such as the rules on trade secrets or processes under Republic Act No. 8293, otherwise known as the "Intellectual Property Code of the Philippines", as amended, Republic Act No. 10173, otherwise known as the "Data Privacy Act of 2012", Republic Act No. 8799, otherwise known as "The Securities Regulation Code", and the Rules of Court.
>
> xxx
>
> Any officer or agent of the corporation who shall refuse to allow the inspection and/or

> reproduction of records in accordance with the provisions of this Code shall be liable to such director, trustee, stockholder or member for damages, and in addition, shall be guilty of an offense which shall be punishable under Section 161 of this Code: Provided, That if such refusal is made pursuant to a resolution or order of the board of directors or trustees, the liability under this section for such action shall be imposed upon the directors or trustees who voted for such refusal: Provided, further, That it shall be a defense to any action under this section that the person demanding to examine and copy excerpts from the corporation's records and minutes has improperly used any information secured through any prior examination of the records or minutes of such corporation or of any other corporation, or was not acting in good faith or for a legitimate purpose in making the demand to examine or reproduce corporate records, or is a competitor, director, officer, controlling stockholder or otherwise represents the interests of a competitor.
>
> xxx

It can be drawn from the law and jurisprudence that the right to inspect is subject to the following conditions:

a. It can only be exercised for a purpose germane to his interest as a stockholder;[4]
b. It must be exercised in good faith, for specific and honest purpose, and not to gratify curiosity, or for speculative or vexatious purposes;[5]
c. It must be exercised during reasonable hours on business days;
d. Copies of corporate records or excerpts from said records must be at the expense of the requesting director, trustee, or stockholder; and
e. It is subject to other applicable laws.

This right is also subject to defenses, as in:

a. That the requesting stockholder has improperly used information before;
b. There is a lack of good faith in the request for inspection;[6]
c. There is a lack of legitimate purpose;
d. The requesting party is not a stockholder of record, or is a competitor, director, officer, controlling stockholder or otherwise represents the interests of a competitor;
e. There are trade secrets or other Intellectual Property Rights that are entitled to protection; and
f. Limitations provided by the Data Privacy Act of 2012.

In advocating for your position, you cited a portion of the ruling in *Gokongwei, Jr., v. Securities and Exchange Commission*,[7] *to wit*:

> In Grey v. Insular Lumber, this Court held that "the right to examine the books of the corporation must be exercised in good faith, for specific and honest purpose, and not to gratify curiosity, or for specific and honest purpose, and not to gratify curiosity, or for speculative or vexatious purposes. The weight of judicial opinion appears to be, that on application for mandamus to enforce the right, it is proper for the court to inquire into and consider the stockholder's good faith and his purpose and motives in seeking inspection. Thus, it was held that "the right given by statute is not absolute and may be refused when the information is not sought in good faith or is used to the detriment of the corporation.

[4] Gokongwei, Jr., v. Securities and Exchange Commission, G.R. No. L-45911 (April 11, 1979)
[5] M.E. Grey v. Insular Lumber Company, G.R. No. L-45144 (April 3, 1939)
[6] Terelay Investment and Development Corp. v. Cecilia Teresita J. Yulo, G.R. No. 160924, (August 5, 2015)
[7] *Ibid*, 6.

However, we wish to emphasize that the Supreme Court also ruled in the same case that:

> The stockholder's right of inspection of the corporation's books and records is **based upon their ownership of the assets and property of the corporation**. It is, therefore, an incident of ownership of the corporate property, whether this ownership or interest be termed an equitable ownership, a beneficial ownership, or a ownership. This right is predicated upon the necessity of self-protection. It is generally held by majority of the courts that where the right is granted by statute to the stockholder, **it is given to him as such and must be exercised by him with respect to his interest as a stockholder and for some purpose germane thereto or in the interest of the corporation**. In other words, the inspection has to be germane to the petitioner's interest as a stockholder, and has to be proper and lawful in character and not inimical to the interest of the corporation.
>
> xxx
>
> It appears to be the **general rule that stockholders are entitled to full information as to the management of the corporation and the manner of expenditure of its funds, and to inspection to obtain such information**, especially where it appears that the company is being mismanaged or that it is being managed for the personal benefit of officers or directors or certain of the stockholders to the exclusion of others.

Also, in the case of *Terelay Investment and Development Corporation, vs. Cecilia Teresita J. Yulo,*[8]
the Supreme Court held that:

> In general, however, officers and directors have no legal authority to close the office doors against shareholders for whom they are only agents, and withhold from them the right to inspect the books which furnishes the most effective method of gaining information which the law has provided, on mere doubt or suspicion as to the motives of the shareholder. **While there is some conflict of authority, when an inspection by a shareholder is contested, the burden is usually held to be upon the corporation to establish a probability that the applicant is attempting to gain inspection for a purpose not connected with his interests as a shareholder, or that his purpose is otherwise improper.** The burden is not upon the petitioner to show the propriety of his examination or that the refusal by the officers or directors was wrongful, except under statutory provisions.

Congruently, the DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.[9] It defines personal information as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[10] Meanwhile, sensitive personal information refers to personal information:

> (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
> (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

[8] *Ibid, 8.*
[9] Data Privacy Act of 2012, §. 16.
[10] Data Privacy Act of 2012, §. 3(g).

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.[11]

In the present case, the corporate records requested to be inspected contain both personal information and sensitive personal information (collectively referred to as "personal data"). Significantly, Section 12(c) and Section 13(b) state:

> SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> xxx
>
> (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
>
> ...
>
> SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> xxx
>
> (b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
>
> xxx

The DPA has the twin task of protecting the fundamental human right of privacy while ensuring the free flow of information.[12] It cannot conveniently be invoked to curtail the existing rights of the stockholders of a corporation, particularly to their right of inspection of corporate books and records, provided such activities are in accordance with prevailing laws and regulations.

Based on the foregoing, TBI may favorably act on the requesting stockholders' request to access its corporate records. But TBI has the prerogative to determine the propriety of the other party's request to access its corporate records and documents, since this right, while inherent, may be subject to limitations, defenses, and relevant laws like the DPA.

The allegations of bad faith and improper use of information cannot operate as a valid ground to refuse an inspection, if not sufficiently proven.[13] It must be established that the scope or manner of the request and the conditions under which it was made are so frivolous that the huge cost to the business will, in equity, be unfair to the other stockholders.[14]

---

[11] Data Privacy Act of 2012, §. 3(l).
[12] Data Privacy Act of 2012, §. 2.
[13] Sy Tiong Shiou et al v. Sy Chim, G.R. No. 174168 (March 30, 2009)
[14] Philippine Associated Smelting and Refining Corporation vs. Pablito O. Lim, et al, G.R. No. 172948 (October 05, 2016)

Consent; Data Privacy Principles; Duty of Confidentiality

As mentioned above, Sections 12(c) and Section 13(b) provide for the lawful basis for the processing of the corporate records in the present case. This necessarily means that the other stockholders need not consent to the inspection. Nevertheless, TBI, as a personal information controller (PIC) may limit the scope of the inspection or redact such information that is not relevant to the request consistent with the general privacy principles of transparency, legitimate purpose, and proportionality,[15] and in recognition of the rights of the data subjects affected.[16] In Advisory Opinion 2019-011,[17] we emphasized that:

> The data subject concerned has the right to be informed of the request for disclosure. Moreover, the corporation has the obligation to examine or inquire about the particular demand thereby disclosing only those personal information that are necessary, not excessive, relevant and adequate to fulfill the legitimate purpose of the demand, as required by Section 74 [now Section 73] of the Corporation Code.

TBI must also implement reasonable and appropriate organizational, physical and technical measures to ensure the confidentiality and security of personal data,[18] as mandated by the DPA and as supported by NPC Circular 23-06.[19]

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

---

[15] Data Privacy Act of 2012, §. 11.
[16] Data Privacy Act of 2012, § 16-18.
[17] National Privacy Commission, Advisory Opinion 2019-011 (14 January 2019)
[18] Data Privacy Act of 2012, §. 20.
[19] National Privacy Commission, NPC Circular 23-06 (01 December 2023)

ADVISORY OPINION NO. 2024-121

05 November 2024

[redacted]

Thru: [redacted]

Re: Requests for Member and Vessel Information by government agencies pursuant to a Senate investigation.

Dear [redacted]

We respond to your inquiry on whether the requests of the Philippine Coast Guard (PCG) and the Bureau of Immigration (BI) for information and access to records of the Manila Yacht Club (MYC) related to an ongoing Senate investigation violates the Data Privacy Act of 2012 (DPA).[2]

You state that the PCG sent a letter-request to MYC for the list of names of yachts that are MYC members as well as a list of other vessels that arrived and departed from the MYC in the month of July 2024. On the other hand, the BI also sent a letter requesting for a meeting to verify with your records the movement of yachts specifically those with declarations for international travel for the months of May, June, and July 2024. Both government agencies stated that the purpose of their request is for them to provide information in connection with an ongoing investigation of various Senate Committees on the alleged escape of a fugitive using a yacht. Besides the letter-request from the PCG and BI, there was neither a *subpoena* nor an official directive from any government entity that required the MYC to produce the information requested by the PCG and BI.

You state that MYC is willing to cooperate and have started the process of obtaining the consent of its members. However, your concern in granting the requests is that the MYC may be constrained to disclose, among others, the following documents which contain personal data:

1. The signed and executed membership forms of your members;
2. The logbook of security personnel;

---

[1] Tags: Vessels, scope of the DPA, personal information, processing for fulfillment of statutory and constitutional mandate.
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the private Sector, Creating for this Purpose a National Privacy Commission, and for other Purposes [Data Privacy Act of 2012], Republic Act No.10173 (2012).

3. Member's guest list declarations, including the attached government issued IDs of theirs guests;
4. The logbook of MYC's dispatcher records.

You state further that these records also contain the following information which you view as protected by the DPA:

i. The names of your members;
ii. The names and personal details of your member's guests (contained in the government issued IDs presented to the MYC);
iii. Member's official signature;
iv. Names of the vessels of members and other details which when put together with other information available to the public may directly and certainly identify MYC members;
v. Member's use of their vessels, specifically the locations visited and frequented;
vi. Member's phone numbers, email address, residence and business address;
vii. Government issued IDs such as passports, driver's license.

Thus, you seek guidance on the following:

1. Whether the names of the MYC member's vessels are considered as personal information under the DPA; and
2. Whether granting the requests of the PCG and/or the BI for other information and/or examination of records may be deemed a violation of Section 32 of the DPA?

Considering that the issues you present are interrelated, we shall discuss them jointly.

Personal information; processing by a public authority.

The DPA defines personal information as any information from which the identity of an individual is apparent or can be reasonably and directly ascertained, or when put together with other information would directly and certainly identify an individual.[3] Meanwhile, sensitive personal information (SPI) are those personal information specifically classified under Section 3(l) of the DPA as sensitive. Both terms are jointly referred to as personal data.

Thus, whether the name of the vessel of an MYC member, or information on yacht movement, constitutes personal information would depend on the context of the disclosure.

The name of a vessel or the movement of yachts for a particular period, by itself, may not be considered as personal information. Hence, there would be no data privacy concern to speak off in that instance. However, if the vessel's name can be linked to an individual, or if the processing would result in the disclosure of other personal data that would lead to the identification of an individual, such disclosure can qualify as processing of personal data. In which case, the proper basis/bases under the DPA must be established.

Besides the member's individual consent, the disclosure of personal data of MYC members to law enforcement authorities (LEA) may be justified under the circumstances based on Section 12 (e) and Section 13 (b) and (f) of the DPA, *viz.*:

[3] Id., §3(g)

For personal information -

(e) The processing is necessary to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate;

xx

x For sensitive personal

information -

(b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

xxx

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

(Underscoring supplied).

Compliance with procedural rules; proportionality.

It must be emphasized that the existence of lawful bases does not grant LEAs absolute and unrestricted right to access and process personal data. The LEAs must still comply with the principles of transparency, legitimate purpose, and proportionality. Moreover, they must comply with procedural rules prescribed by law to ensure that individual rights are respected and upheld.

After all, the DPA is anchored on Section 3, Article III of the 1987 Constitution, which provides:

1. The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.
2. Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.

The DPA reinforces the constitutional safeguard to the right to privacy in that, while LEAs such as the PCG and BI may obtain personal data from MYC, such processing must still comply with the applicable legal requirements to ensure that requests for information are legally justified, specific, proportional and carried out through the appropriate channels.

We note that under Republic Act No. 9993, or the Philippine Coast Guard Law of 2009, the PCG's primary mandate involves maritime safety, law enforcement, search and rescue, marine environmental protection, and national security within Philippine waters. Under Section 3 (I) of RA 9993, one of the mandates of the PCG is to assist in the enforcement of laws on fisheries, immigration, tariff and customs, forestry, firearms and explosives, human

trafficking, dangerous drugs and controlled chemicals, transnational crimes and other applicable laws within the maritime jurisdiction of the Philippines.

On the other hand, under Commonwealth Act No. 613, or the Philippine Immigration Act of 1940, the BI is principally responsible for the administration and enforcement of immigration, citizenship, and alien admission and registration laws. Section 37(a) of CA 613 authorizes the Commissioner of Immigration (or a designated officer) to issue *subpoenas* for witnesses and documents relevant to cases involving deportation, exclusion, and other immigration-related issues.

From the foregoing, it appears that disclosing to the PCG and the BI the personal data of MYC members through a mere letter-request could potentially expose all the parties to liability not only for violation of the DPA but also of their respective mandates and internal processes. Nevertheless, both the PCG and BI may still pursue their investigation with MYC if the BI would issue a *subpoena* to be served and enforced jointly with the PCG. Alternatively, since it is only the BI that has the express power to *subpoena,* the PCG may separately conduct its investigation by requesting the Senate to issue a *subpoena* to the MYC.

Requiring the presentation of a *subpoena* instead of a mere letter-request ensures that the LEAs comply with the principle of proportionality under the DPA and to avoid questions on the admissibility of the evidence they may obtain. Additionally, a *subpoena* also serves as a safeguard to the data privacy rights of the other members of the MYC who have no connection to the investigation.

As we have stated in previous Advisory Opinions, the DPA is not meant to prevent LEAs from processing personal data when necessary to fulfill their mandates. Rather, the DPA serves to ensure that an individual's right to informational privacy is respected while promoting the fair, secure, and lawful processing of personal data.

Please be advised that the foregoing was rendered based solely on the information you provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2024-014[1]

25 November 2024

[redacted]

Re: DISCLOSURE OF INDIVIDUALS' NAMES IN RELATION TO THE REGISTRATION AND USE OF FAKE NATIONAL IDENTIFICATION CARDS

Dear [redacted]

We respond to your request for an Advisory Opinion on the propriety of disclosing the names of individuals in connection with their registration with the Philippine Statistics Authority (PSA) for the issuance of national identification cards (national IDs), including the reported use of fake national IDs.

We understand that the PSA intends to publicly post the names of hundreds of thousands of applicants and/or registered persons whose national IDs were undelivered due to change of address, including those with errors in the capture of their biometric information during registration. The PSA, pursuant to its mandate to deliver the national IDs, communicated with the applicants/registered persons through their registered mobile numbers, conducted house-to-house visits, and even sought assistance from the respective barangay officials. However, considering that the mobile number is merely optional in the application form, most of the concerned applicants/registered persons did not list down one in their forms. Thus, the PSA is proposing to post the names of these applicants/registered persons on its website and registration centers to complete their registration for the issuance of their national IDs and for the undelivered national IDs to be claimed.

Furthermore, the PSA also inquired as to whether providing the relying parties with a list of individuals who were reported to have presented fake national IDs during transactions with various government agencies and/or financial institutions is in accordance with the provisions of Republic Act No. 10173, also known as the Data Privacy Act of 2012[2] (DPA).

---

[1] Tags: mandate; processing of personal information; general data privacy principles; personal data protection.
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes.

We note that a relying party[3] refers to a service provider who relies on any PhilSys-enabled service, such as authentication or any other process that identifies and verifies the identity of their customers. Thereafter, a registered relying party submits to the PSA the PhilSys Number (PSN)[4] of an individual for authentication. In addition, the relying party is obliged to conform with the standards and guidelines set by the PSA, in consultation with DICT to ensure the security, efficiency, and integrity of the authentication process.[5]

Under the IRR of the Republic Act No. 11055,[6] also known as the Philippine Identification System Act (PhilSys Act), the presentation of the national ID shall constitute as sufficient proof thereof, subject to proper authentication.[7] Aside from the PSA, the general public and all relying parties may check and verify the authenticity of a national ID through the PhilSys Check, an offline identity authentication tool in the form of a website. However, any entity requesting authentication via PhilSys Check must obtain the cardholder's consent.[8]

Processing of personal information; publication of names of individuals

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.[9]

Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[10] Under the DPA, names that directly identify an individual are considered as personal information.

Accordingly, the intended posting and/or disclosure of names constitutes processing,[11] which should comply with the provisions of the DPA, particularly on the general data privacy principles. Further, the processing of such information shall be done within the limits of the PSA's mandate.

As stated in your letter-request, the PSA intends to publicly-post the names of approximately 197,470 applicants who were reported to have errors in their captured biometric information, particularly iris scan and fingerprints. The purpose of which is to recapture their biometric information. Otherwise, the PSA cannot generate a PSN for the said individuals with issues in their captured biometric information.

Section 8(D) of the Implementing Rules and Regulations (IRR) of the PhilSys Act provides: "*xxx*

D. Registration Process

---

[3] §4(q), IRR of R.A. No. 11055.

[4] Section 7(a), Republic Act No. 11055 – *Philippine Identification System Components* – The PhilSys shall have the following key components: (a) *PhilSys Number (PSN)*. - The PSN is a randomly generated, unique, and permanent identification number that will be assigned to every citizen or resident alien upon birth or registration by the PSA *xxx*.

[5] §12, 2nd par., IRR of R.A. 11055.

[6] An Act Establishing the Philippine Identification System.

[7] §12, IRR of R.A. 11055.

[8] Philippine Statistics Authority, PhilSys Check, available at https://philsys.gov.ph/philsys-check/ (last accessed 2 October 2024).

[9] §4, Republic Act No. 10173.

[10] §3(g), Republic Act No. 10173.

[11] §3(j), Republic Act No. 10173.

> *xxx*
> If the biometric and demographic information of the applicant are found to be unique, a PSN will be generated for the applicant. Otherwise, further verification shall be conducted by the PSA. **In the event that the applicant cannot be issued a PSN, he or she will be notified accordingly**.
>
> Registration in the PhilSys is deemed successful and complete upon confirmation of registration by the PSA and the issuance of the PSN. *xxx" (Emphasis supplied)*

Considering the above provision and on account of the PSA's extensive efforts to contact the applicants through various means, the intended disclosure is allowed for the PSA to effectively carry out its mandate.

Secondly, the PSA has already logged 328,739 cases of undelivered national IDs tagged as return-to-sender due to change of address by the intended recipients. Thus, the PSA is contemplating to post the names of the said registered persons on its website and at the respective registration centers.

We emphasize that the PhilSys Act provides stringent safeguards for adequate protection of registered individuals' personal data, specifically under Section 17 of the Act.[12] The said provision establishes a general rule that no person may disclose, collect, record, convey, disseminate, publish, or use any information of registered persons with the PhilSys. This includes restrictions on giving access to or copies of such information to third parties or entities, including law enforcement agencies, national security agencies, or units of the AFP.

By way of exception, the personal data of persons registered with the PhilSys can be disclosed if the latter has given prior consent thereto. The consent, however, must be specific to the particular purpose for which the information is being collected for processing. Another exception is the existence of compelling interest of public health or safety. This exception, however, requires an order from a competent court, establishment of significant harm to the public, and notification to the affected parties.

Section 17 of the PhilSys Act explicitly prohibits the disclosure of personal data of individuals registered with the PhilSys, allowing exceptions only under specific circumstances to prevent unauthorized access and/or disclosure of personal data. Given these constraints, the PSA may instead consider publishing general notices or advisories about the undelivered/unclaimed national IDs with corresponding instructions on how to claim the same and/or the need to update their information with the PSA. The PSA may also consider using a secure online portal where applicants/registered persons may check the status of their national IDs.

---

[12]"*Section 17. Protection Against Unlawful Disclosure of Information/Records.* - No person may disclose, collect, record, convey, disseminate, publish, or use any information of registered persons with the PhilSys, give access thereto or give copies thereof to third parties or entities, including law enforcement agencies, national security agencies, or units of the Armed Forces of the Philippines (AFP), except in either of the following circumstances:
(a) When the registered person has given his or her consent, specific to the purpose prior to the processing; and
(b) When the compelling interest of public health or safety so requires, relevant information may be disclosed upon order of a competent court, provided that the risk of significant harm to the public is established and that the owner of the information is notified within seventy-two (72) hours of the fact of such disclosure. *xxx*."

Adherence to general data privacy principles; reasonable and appropriate security measures

Lastly, the PSA intends to disclose to relying parties a list of persons reported to have presented fake national IDs in transactions with various government agencies and/or financial institutions.

It is worth noting that under the PhilSys Act, it is the policy of the State to establish a single national identification system to promote seamless delivery of service, reduce corruption and curtail bureaucratic red tape, avert fraudulent transactions and misrepresentations, strengthen financial inclusion, and to promote ease of doing business.[13] Notably, the PSA is mandated to act on matters affecting the integrity and security of the PhilSys, which includes taking proactive measures against the use of fake, falsified, or altered national IDs.

As such, the disclosure of personal information to registered relying parties is allowed to avert fraudulent transactions and misrepresentations or for customer due diligence purposes, among others. However, the PSA must ensure that any disclosure of personal data aligns with the provisions of the DPA, particularly adherence to the general data privacy principles of transparency, legitimate purpose, and proportionality, including the implementation of appropriate and reasonable security measures. Thus, the disclosure to relying parties should be limited only to the name of the individual/s appearing on the face of the national ID that is determined to be fake or counterfeit. This guarantees that the disclosure does not go beyond what is necessary to achieve the legitimate purpose of preventing fraud and ensuring the integrity of the PhilSys.

The PSA may also consider enhancing the implementation of appropriate security measures to easily detect the presence of counterfeit national IDs, thereby upholding the integrity of the national ID system.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
VIDA ZORA G. BOCAR
OIC-Director IV, Privacy Policy Office[14]

[13] §2, R.A. No. 11055.
[14] Per PCSO No. 100, s. 2024

ADVISORY OPINION
NO. 2024-0015[1]

07 November 2024

[redacted]

Re: REQUEST TO OBTAIN A COPY OF PERSONAL DATA FOR AUDIT PURPOSES

Dear [redacted]

We respond to your request for an Advisory Opinion on whether the [redacted] Registrar (Registrar) may comply with the request of the Commission on Audit (COA) for a list of deceased persons without violating Republic Act No. 10173, or the Data Privacy Act of 2012 (DPA).[2]

You state in your letter that the COA requested the Registrar for a list of deceased persons containing personal information and sensitive personal information (collectively called personal data). Specifically, the COA asked the Registrar for a list containing the complete names and dates of birth of persons who died or were issued death certificates from January 2020 to December 2023. The COA's request is in connection with its audit of Social Security System (SSS) pension fund payments. You also state that although the Registrar possesses the requested information, you hesitate from providing COA with the requested personal data since you posit that the consent of the deceased's nearest surviving next of kin is necessary under the circumstances. Furthermore, COA's request covers all deceased persons in Victorias City regardless of whether they are SSS members or not. Considering that the Registrar has no means to validate who among the deceased individuals were SSS members, you are concerned that even the personal data of non-SSS members may be disclosed to COA in the process.

Thus, you seek guidance as to whether you may legally accede to the COA's request.

---

[1] Tags: processing; personal data; audit function; mandate
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes.

Personal and sensitive personal information

Personal and sensitive personal information are defined under Section 3 of the DPA, as follows:

> (g) *Personal information* refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
>
> *xxx*
>
> (l) *Sensitive personal information* refers to personal information:
>
> (1) About an individual's *xxx* age *xxx*;

It is clear that the name of a deceased individual is considered personal information. On the other hand, the complete date of birth qualifies as sensitive personal information as it can be used to ascertain an individual's age.

Therefore, the processing of such information should be anchored on *any* of the criteria for lawful processing outlined in Sections 12 and 13 of the DPA for personal and sensitive personal information, respectively. It is worthy to note, however, that Section 4(e) of the DPA establishes a special case when the processing is in the performance of an agency's constitutional or statutory function or mandate.

Constitutional or statutory mandate of the Commission on Audit.

Under the 1987 Constitution,[3] the COA is considered as the guardian of public funds, vesting it with broad powers over all accounts pertaining to government revenue and expenditures and the uses of public funds and property including the exclusive authority to define the scope of its audit and examination, establish the techniques and methods for such review, and promulgate accounting and auditing rules and regulations.[4] Section 11, Chapter 4, Subtitle B, Title I, Book V of Executive Order No. 292, otherwise known as the Administrative Code of 1987, mirrors this constitutional mandate of COA.

Additionally, Section 3, Rule IV of the 2009 Revised Rules of Procedure of the Commission on Audit provides for the responsibility of the auditor to obtain sufficient evidence to support his/her findings as well as to safeguard the same.[5]

We reiterate our stance in *NPC Advisory Opinion No. 2020-016* in which we acknowledged the authority of the COA as an independent constitutional body and recognized its power, authority, and duty to examine, audit and settle all accounts and expenditures of the funds and properties of the Philippine government. We also stated therein that the DPA should not be interpreted to hamper, or interfere with, the performance of the duties and functions of duly constituted authorities. Further, the COA, in carrying out its mandate, enjoys the presumption of regularity in the performance of its duties. The determination of what

---

[3] Section 2, Article IX-D of the 1987 Constitution

[4] Yap v. Commission on Audit, G.R. No. 158562, 23 April 2010.

[5] Commission on Audit, Issuances, Revised Rules of Procedure, available at https://www.coa.gov.ph/issuances/2009-revised- rules-of-procedures-of-the-commission-on-audit/ (last accessed 11 October 2024).

methods to utilize in the collection or gathering of personal data in performing its auditing functions shall be left to the COA's sound discretion.

We emphasize that the DPA, its IRR, and related NPC issuances should be read in conjunction with existing laws. The DPA has the twin task of protecting the right to privacy while ensuring the free flow of information and should not be used as an excuse for non-compliance with other existing laws, rules and regulations.[6] The 1987 Constitution explicitly grants the COA with enough latitude to determine, prevent and disallow irregular, unnecessary, excessive, extravagant or unconscionable expenditures of government funds.[7]

Accordingly, the COA must be provided with the necessary information to effectively carry out its audit function and examine government expenditures.

Principle of Proportionality.

There is a legal presumption granted to COA that it will lawfully process personal data pursuant to its mandate, and that the processing shall be limited to achieving the specific purpose, function, or activity. Nevertheless, COA remains subject to the requirements under the DPA, its IRR, and NPC issuances. This includes implementing security measures to secure and protect personal data mandated under *NPC Circular No. 2023-06.*[8] Significantly, maintaining compliance with the law requires strict adherence to the data privacy principles outlined in the DPA, one of which is the principle of proportionality, *to wit*:

> *Section 11. General Data Privacy Principles.* The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.
>
> Personal information must be:
>
> *xxx*
>
> (c) Accurate, **relevant** and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;
>
> (d) **Adequate and not excessive in relation to the purposes for which they are collected and processed**;
>
> *(Emphasis supplied).*

The principle of proportionality was further elaborated in Section 18 of the Implementing Rules and Regulations (IRR) of the DPA:

> *Section 18. Principles of Transparency, Legitimate Purpose and Proportionality.* The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.
>
> *xxx*

---

[6] See: National Privacy Commission, Advisory Opinion No. 2018-035 (20 July 2018).
[7] Sanchez v. Commission on Audit, G.R. No. 127545, 23 April 2008.
[8] Security of Personal Data in the Government and the Private Sector.

> c. Proportionality. The processing of information shall be adequate, relevant, **suit- able, necessary**, and not excessive in relation to a declared and specified purpose. **Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.**
>
> *(Emphasis supplied).*

Thus, it is essential to ensure that the information to be disclosed for audit purposes should only be limited to what is necessary to achieve the objectives of the audit. Consequently, we suggest that the Registrar coordinate with the COA to seek guidance on the personal data needed for the audit, particularly since the latter's request appears to be too extensive and disproportionate for its purpose.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

ADVISORY OPINION
NO. 2024 - 016[1]

11 December 2024

[redacted]

Re: DISCLOSURE OF PERSONAL DATA PURSUANT TO A MISSION ORDER BY THE BUREAU OF INTERNAL REVENUE

Dear [redacted]

We respond to your inquiry on whether the disclosure of documents and information pursuant to a Bureau of Internal Revenue Mission Order (MO) violates the Data Privacy Act of 2012 (DPA).[2]

You inform that the [redacted] is the subject of the BIR's Tax Compliance Verification Drive (TCVD). Armed with an MO, the BIR revenue officers stated that the TCVD is aimed at determining whether taxes are being properly remitted for the lease of residential units at the [redacted]. Hence, they verbally requested the [redacted] 's Property Management Office (PMO) for the following information:

- A list of residential units currently being leased out;
- Name of unit owner/s whose unit/s is/are being leased out;
- Contact number of unit owner/s whose unit/s is/are being leased out;
- Copies of notarized lease contracts.

You are concerned about the general nature of the MO and the request of the revenue officers, specifically on the fact that:

1. The MO is directed only to the [redacted] and does not list any other taxpayer/s.
2. The request was merely made verbally despite the sensitivity of the information being requested which includes the personal information of unit owners.
3. The ambiguity surrounding the specific transactions subject of the TCVD which the MO also failed to identify.

---

[1] Tags: scope of the DPA, personal information, special cases, public authority.
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the private Sector, Creating for this Purpose a National Privacy Commission, and for other Purposes [Data Privacy Act of 2012], Republic Act No.10173 (2012).

Hence, you inquire whether providing the requested information to the BIR would violate the DPA. In addition, you also seek guidance on the following:

1. The types of information and documents you are permitted to provide pursuant to the MO without violating the DPA; and

2. The specific form or documentation from the BIR that should outline the requested information and documents, as well as the activity or transaction for which the TCVD will be conducted.

Regulatory mandate; processing of personal information by a public authority.

The DPA and its Implementing Rules and Regulations (IRR) excludes certain types of information that are being processed by a public authority, *viz.*:

> SECTION 5. Special Cases: The Act and these Rules do not apply to the following specified information, limited to the minimum required for collection, access, use, disclosure, or other processing necessary for the relevant purpose, function, or activity:
>
> x x x
>
> d. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this Act shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);
>
> Provided, that the non-applicability of the Act or these Rules do not extend to personal information controllers or personal information processors, who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity.

Hence, information required by a public authority in the exercise of its regulatory function pursuant to its constitutional or statutory mandate falls outside the DPA's scope. However, as we have previously stated in Advisory Opinion No. 2020-015[3], this exemption must be interpreted strictly such that:

1. It applies solely to the minimum necessary collection, access, use, disclosure, or other processing related to the specific purpose, function, or activity. Any processing for

[3] National Privacy Commission, Re: Collection of Personal Data by the Bureau of Internal Revenue for Tax Compliance Purposes, NPC Advisory Opinion No. 2020-015 (Feb. 24, 2020).

regulatory purposes must comply with constitutional or statutory mandates and adhere strictly to all required substantive and procedural processes.

2. Only the specified information is exempt from the DPA's provisions. The public authority remains obligated as a personal information controller (PIC) under the DPA to implement security measures for personal data protection, respect data subject rights, and follow data privacy principles.

The BIR is a public authority primarily tasked to ensure compliance with the NIRC, as amended, and other relevant tax laws and issuances. The MO itself cites Section 6(c) of the NIRC, which provides:

> SECTION 6. Power of the Commissioner to Make Assessments and Prescribe Additional Requirements for Tax Administration and Enforcement. –
>
> (C) Authority to Conduct Inventory-taking, Surveillance and to Prescribe Presumptive Gross Sales and Receipts. - **The Commissioner may, at any time during the taxable year, order inventory-taking of goods of any taxpayer as a basis for determining his internal revenue tax liabilities, or may place the business operations of any person, natural or juridical, under observation or surveillance if there is reason to believe that such person is not declaring his correct income, sales or receipts for internal revenue tax purposes**. The findings may be used as the basis for assessing the taxes for the other months or quarters of the same or different taxable years and such assessment shall be deemed prima facie correct. cd
>
> When it is found that a person has failed to issue receipts and invoices in violation of the requirements of Sections 113 and 237 of this Code, or when there is reason to believe that the books of accounts or other records do not correctly reflect the declarations made or to be made in a return required to be filed under the provisions of this Code, the Commissioner, after taking into account the sales, receipts, income or other taxable base of other persons engaged in similar businesses under similar situations or circumstances or after considering other relevant information, may prescribe a minimum amount of such gross receipts, sales and taxable base, and such amount so prescribed shall be prima facie correct for purposes of determining the internal revenue tax liabilities of such person.

It is clear that the BIR Commissioner has the legal authority to examine the business activities of any individual or entity. Moreover, the DPA itself limits the rights of data subjects where the processing of personal data is for the purpose of investigations in relation to any tax liabilities.[4]

We note that Section V. 1.2 of Revenue Memorandum Order (RMO) 9-2006 prescribes the guidelines and procedures in the conduct of a TCVD. Under Section V. 1.2, the Revenue District Office shall:

3. Gather data/information for evaluation of all taxable persons/entities from the following:

    a. List of registered taxpayers from RDO records;

[4] Id., §19

b. List of persons who have secured Mayor's Permit for the current year from the Office of the Mayor;
c. List of big landowners of the town from the Assessor's Office/Registry of Deeds;
d. List of professionals who have secure Professional Tax Receipts (PTRs) from the Municipal Treasurer;
e. List of persons engaged in business in the barangays from the Barangay Captains;
f. List of stores/tenants and location map of each stores/tenants from building owners/administrators; and
g. Such other data as may be gathered thru the MOA between the BIR and Bureau of Local Government Finance (BLGF) dated May 25, 1995

In line with the above RMO, the BIR is thus authorized to request related taxpayers' information in connection with the conduct of a TCVD.

General data privacy principles;
Proportionality

While the DPA does not prohibit the BIR from processing personal data pursuant to its mandate, it must nevertheless comply with the general data privacy principles under the DPA. In this regard, the verbal request of the BIR for data relative to the TCVD appear to lack specificity as to their relevance and necessity for the stated tax compliance objectives. This absence of a clear, well-defined purpose raises concerns about whether the BIR is acting within the bounds of proportionality.

Considering that the MO did not indicate that there is a need to examine the tenants or unit owners' information as part of the TCVD, these broad requests for information risk being excessive and potentially intrusive, as they may go beyond what is reasonably necessary to achieve the intended tax compliance objectives. In this case, the BIR should have stated the need to obtain the contact numbers of unit owners whose units are being leased out and copies of notarized lease contracts. These pieces of information pertain specifically to the data subjects and not to the [redacted], which was the only listed taxpayer in the MO. Therefore, their data privacy rights must be respected and safeguarded.

Non-compliance with these principles could not only compromise individual privacy but also expose the BIR to potential violations of the DPA. Therefore, while the BIR's TCVD aims to enhance tax compliance, it is imperative that its implementation conform to the principles of legitimate purpose and proportionality. To support the objectives of the TCVD while upholding data privacy principles, the BIR may consider reevaluating its data collection practices to ensure that each piece of requested information is necessary and proportionate to achieve its tax compliance objectives. For instance, the BIR could provide a clear justification for specific data requests, such as contact numbers of unit owners and copies of notarized lease contracts, to establish their relevance to the TCVD's objectives. This approach would help balance regulatory requirements *vis-a-vis* the data privacy rights of the individuals concerned.

To determine the type of information and documents you may disclose pursuant to the MO, we suggest that if any part of the request is unclear or seems unjustified, you should seek clarification from the BIR. This can be done by requesting for clarification not as a challenge

to the investigation but as a means to ensure accurate and complete compliance with the BIR's request. This could include asking for guidance on specific document requirements or the scope of the data being sought.

To address your inquiry about the specific form or document that the BIR should provide to outline the requested information and documents, as well as the activity or transaction for which the TCVD will be conducted, it is important to note that NPC does not have the authority or jurisdiction to impose what documents or requests the BIR should provide in response to such inquiries. The BIR is responsible for establishing the regulations, formats, and templates concerning tax compliance and information requests. Therefore, consulting directly with the BIR will ensure compliance with the requirements of a TCVD and the DPA. In doing so, it is crucial to consider the principle of proportionality. The BIR should ensure that each piece of requested information is necessary and proportionate to achieve the intended tax compliance objectives. If any part of the request seems unclear or seems to involve excessive data collection, you may request clarification from the BIR on how each item relates to the tax compliance verification process. Moreover, when personal data of third parties such as tenants or property owners is involved, their data privacy rights must be respected. The BIR may also consider providing clear justifications for the relevance of certain information to ensure that only the necessary data is being gathered; thus, maintaining a balance between regulatory mandate and privacy protection.

Please be advised that the foregoing was rendered based solely on the information you provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2024- 017[1]

18 December 2024

[redacted]

Re: PUBLICATION OF FORMER EMPLOYEES' PERSONAL DATA

Dear [redacted]

We respond to your request for an Advisory Opinion on whether your client's intended action of publicizing its former employees' names, photographs, offenses or infractions committed, pending criminal cases, if applicable, and their severance from employment could be justified under Section 12(f) of the Data Privacy Act of 2012 (DPA).[2]

You state that your client is a large construction company, and it has encountered various instances of unethical and unlawful conduct by its employees.[3] Necessarily, such conduct has affected the company's integrity and reputation.

To address and mitigate unlawful practices, safeguard the interests and goodwill of the company, and inform the public to prevent former employees from engaging or committing other similar misconduct, your client expressed its intention to publish in newspapers of general circulation the identity, photographs, offenses, pending criminal cases, and employment severance details of the employees involved.

Thus, you seek guidance if the disclosure of the mentioned personal data through publication can be justified under Section 12(f) of the DPA.

---

[1] Tags: lawful processing of sensitive personal information; due process; data privacy principles; publication of employee data; data subject rights

[2] An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

[3] E.g. Bribery, kickbacks, theft, misappropriation of company assets, and allegations of sexual harassment, among others.

Personal data; Secs. 12, 13 of the DPA.

Oftentimes, when an employee is separated from employment, employers find it necessary to notify their clients that such employee is no longer connected with them. This common practice is recognized by the NPC. However, to ensure the protection of personal data, we must consider the circumstances surrounding the present matter.

As stated in your letter, your client intends to publish notices to forewarn the public against transacting with the employees involved and to prevent the possibility of such employees misrepresenting their association with the company, considering that some of them were charged in court by the company.

The DPA defines personal information as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[4] On the other hand, the DPA classifies the following as sensitive personal information, *viz.*:

x x x

> (2) About an individual's health, education, genetic or sexual life of a person, or to **any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings**;[5]
>
> (Emphasis supplied).

x x x

Further, processing is defined under the DPA as any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[6]

Applying the foregoing to your present concern, the employees' names, photographs and the fact of their severance from the company is considered as personal information, while offenses, pending criminal cases, and employment severance details are considered sensitive personal information under the DPA.

As regards the personal information intended to be published, we stated in Advisory Opinion No. 2019-024[7] that:

> It has been the common practice for companies to publish notices in newspapers and other media that a certain person appearing in the photograph used to be their employee, but is now no longer connected with the company, and a warning that transactions with the said person on behalf of the company will no longer be honored. The above is still allowed under the DPA. The basis for processing may be Section 12(f) which provides for the processing that is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties

[4] Id., Sec. 3(g)
[5] Id., Sec. 3(l)
[6] Id., Sec. 3(j)
[7] National Privacy Commission (NPC) Advisory Opinion No. 2019-024 (07 May 2019)

> to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution. Legitimate interest refers to matters that are desired by or important to a PIC, which must not be contrary to law, morals or public policy. This includes business, financial or other reasonable purpose.

On the other hand, NPC Circular 2023-07[8] provides that in the determination of legitimate interest, the following must be considered:

> SECTION 3. General Considerations. — Section 12(f) of the DPA permits the processing of personal information when the processing is necessary for the legitimate interests pursued by the PIC or a third party to whom the personal information is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject that require protection under the Philippine Constitution.
>
> A. Legitimate interest refers to any actual and real interest, benefit, or gain that a PIC or third party may have in or may derive from the processing of specific personal information.
> B. Processing based on a legitimate interest may only be relied on for the processing of personal information. It cannot be relied upon when the processing involves sensitive personal information and privileged information.
> C. The third party in Section 12(f) of the DPA refers to any natural or juridical person to whom personal information is disclosed and who is not the PIC, the personal information processor (PIP), or the data subject of the specific processing activity.
> D. The fundamental rights and freedoms of data subjects protected under the Philippine Constitution and the effect and impact of the specific processing activity on such rights and freedoms shall be assessed and weighed against the legitimate interest of the PIC or third party through a legitimate interest assessment.

Indeed, your client's interest in preventing former employees from engaging in fraudulent activities may well be considered as a legitimate interest contemplated by the DPA. This is particularly important to ensure that customers only engage with authorized employees, especially if these former employees transact with the public. Therefore, the publication of severance from employment is justified, provided that such processing will not have unwarranted impacts on the rights and freedoms of data subjects—in this case, the former employees.

However, there appears to be no applicable lawful criteria to publish sensitive personal information[9] of these former employees, which include infractions committed and potential and/or pending cases. Disclosing their offenses and cases may be excessive to the primary purpose of the public notices, which is to forewarn the public against transacting with these individuals and to prevent the possibility of these employees misrepresenting their association with the company. To post case details before a final judgment has been rendered by the court may subject these former employees to public ridicule and prejudice. Furthermore, the publication may also be violative of an individual's right to due process, which is a basic right guaranteed and protected by the 1987 Philippine Constitution, alongside the right to privacy.

With this, we suggest informing your client to reevaluate its proposed public notice mechanisms. The publication of severance of employment alone may be sufficient to inform

[8] NPC Circular 2023-07 (13 December 2023)
[9] DPA, Sec. 3(l)

the public, and to include additional information such as pending criminal action/s could be considered intrusive and violative of Section 13 of the DPA.

General data protection principles; proportionality

It must be emphasized that even if there exists a legal basis for processing, the DPA prohibits excessive processing of personal data. As such, the Personal Information Controller (*i.e.*, your client) is still required to comply with the general data privacy principles of transparency, legitimate purpose, and proportionality.[10]

Notably, the principle of proportionality dictates that the processing of personal data shall be adequate, relevant, suitable necessary and not excessive in relation to a declared specified purpose. Thus, disclosure of personal data through public notices should be limited to its declared, specified, and legitimate purpose. Since the primary intent is to warn the public to prevent transactions with the former employees in the name of the company, the publication of severance of employment may already be sufficient and proportionate to achieve the purpose sought.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

[10] Id , Sec. 11.

ADVISORY OPINION NO. 2024-018[1]

20 December 2024

[redacted]

Re: REQUEST FOR SHARING OF REAL-TIME TRAFFIC SITUTATION VIA LIVE STREAMING FOR THE TOLLWAY SURVEILLANCE MONITORING INFORMATION SYSTEM (TSMIS) PROJECT

Dear [redacted]

We respond to your request for an Advisory Opinion on the data privacy implications of the Toll Regulatory Board (TRB)'s request for access to the Closed-Circuit Television (CCTV) Systems video maintained by the toll road operators.

In your letter, you state that you requested toll road operators to share their CCTV footage showing real-time traffic flow in order to implement the TRB's Tollway Surveillance Monitoring Information System (TSMIS) Project.

However, one of the toll road operators (hereafter, the "Operator") declined the request reasoning that the DPA generally requires the consent of motorists before publishing images or data captured by their tollway CCTV systems. The Operator also cites Section 18 of the DPA's Implementing Rules and Regulations (IRR) which mandates that if alternative means are available to comply with data protection requirements without releasing personal data, those means should be prioritized.

The Operator further stated that they are already providing real-time traffic updates through TV and radio networks, as well as publishing updates on their Twitter account and their tollways app. Consequently, they believe that the requested "live feed" from their CCTV systems is unnecessary. Furthermore, they expressed their concern that live streaming of traffic from their CCTV systems via the proposed software (Discord, Skype, or Zoom) may lead to unauthorized processing and cybersecurity risks, as they do not have control over these software and any individuals with access to the stream could record or download the

[1] Tags: CCTV footage, special case, public authority, statutory mandate.

footage.

In response, TRB argues that:

1. TRB's request falls under Section 4(e) of the DPA and Section 5(d) of its IRR as a Special Case, since, by law, it has jurisdiction and power to regulate the operation and maintenance of toll facilities which includes the installation of CCTVs.

2. TRB will neither collect nor process personal information or personally identifiable information. TRB is merely requesting the toll operators to share real-time CCTV footage of traffic situations on the toll expressways, not the personal or identifiable information of motorists using the tollways.

3. TRB's access to CCTV footage. Furthermore, TRB will not take control of the CCTV cameras or monitors but will only have access to live footage of traffic conditions on the toll expressways. The toll operators will maintain control over the footage, ensuring that no personal or identifiable information of motorists is included in the shared streams.

4. TRB will utilize a secure software platform, such as Discord or any other software recommended by the toll operators to prevent any data security incidents. As additional safeguards, TRB will:
    (i) Limit access to the software to authorized personnel only;
    (ii) Share only snippets, screenshots, or short clips of the footage with toll expressway users for real-time traffic information;
    (iii) Establish a retention period for the shared footage.

5. Necessity and proportionality of the request: The request to share real-time traffic footage via live stream is both necessary and proportionate to the legitimate interests pursued by TRB as a regulatory agency. Firstly, it ensures the proper maintenance of tollway facilities by allowing real-time monitoring of their operations. Secondly, it aids in analyzing traffic patterns, responding to emergencies, and managing traffic incidents on the toll expressways. Lastly, it provides a convenient way to offer toll expressway users real-time footage of traffic conditions.

6. Impact of denying TRB's request: Finally, the denial of TRB's access to the toll operators' CCTV footage due to perceived risks to data privacy and security could set a negative precedent for regulatory agencies like TRB. Such a decision could be used by regulated entities as a basis to refuse compliance with their obligations under the Concession Agreements or Supplemental Toll Operation Agreement (STOA).

Hence, your present request.

Personal information; processing; CCTV.

The Data Privacy Act of 2012 (DPA)[2] defines personal information as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put

[2] An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

together with other information would directly and certainly identify an individual.[3]

Meanwhile, processing is defined as any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.[4]

On the other hand, NPC Circular No. 2024 – 02[5] defines Closed-Circuit Television or "CCTV" as referring to closed-circuit television or camera surveillance systems in a fixed or stationary location that can capture images of individuals or other information relating to individuals.

Based on your statements, the screenshots of submitted CCTV footage from tollways reveal, at best, only vehicle plate numbers. The nature of tollways, where vehicles are moving at high speeds, makes it difficult to immediately identify an individual based solely on CCTV footage without employing high technology applications like automated license plate recognition (ALPR), facial recognition, and integrated data analytics that enhance the ability to identify vehicles and individuals.

Applying the definition provided by the DPA, plate numbers, on their own or without additional information that could directly and certainly identify an individual, cannot be considered personal information. Thus, without access to other databases, plate numbers only identify a vehicle and not the user or its owner.

Scope of the DPA; public authority; limitations on data subjects' rights.

Generally, the DPA applies to the processing of all types of personal information and to any natural and juridical person involved in the processing of personal information. However, the DPA and its IRR provide a list of specified information which do not fall within its scope. Particularly, Section 5(d) of the IRR states that:

> *Section 5. Special Cases. The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:*
>
> *xxx*
>
> *d. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law.*
>
> *xxx*
>
> *Provided, that the non-applicability if the Act or these Rules do not extend to personal information controllers or personal information processors who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function or activity.*

[3] Id., Sec. 3(g)
[4] Id., Sec. 3(j)
[5] National Privacy Commission, NPC Circular No. 2024-02 (9 August 2024)

However, for this exemption to apply, the following must be established:

1. *The information is necessary in order to carry out the law enforcement or regulatory function of a public authority;*
2. *The processing is for the fulfillment of a constitutional or statutory mandate;*
3. *There is strict adherence to all due process requirements;*
4. *Applies only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned; and*
5. *Only the specified information falls outside the scope of the DPA. The public authority, considered as a personal information controller under the DPA, must still comply with the other requirements of the DPA such as the implementation of reasonable and appropriate physical, organizational and technical security measures, uphold the rights of data subjects and adhere to the data privacy principles of transparency, legitimate purpose, and proportionality.*[6]

Presidential Decree No. 1112[7] vests the TRB with the jurisdiction to regulate the operation and maintenance of toll facilities. As such, the CCTV footage that the TRB requests qualifies as information that is necessary for TRB to carry out its regulatory function. In other words, TRB's processing of CCTV footage is permitted under the DPA as this is necessarily included in its mandate to determine and decide the kind, type and nature of public improvements that will be constructed and/or operated on toll facilities, including the establishment, operation and maintenance of Service Facilities throughout the tollways.

Further, the TRB's request may also find support under Section 7 of NPC Circular No. 2024 – 02, *to wit*:

> SECTION 7. Third-party access request. — A third-party access request is a request to access CCTV footage made by a person other than the data subject involved in the footage or the latter's authorized representative. If a data subject involved in the footage or their authorized representative requests access to CCTV footage, the presence of another person's image within the CCTV footage does not automatically classify such request as a third-party access request. Further, in handling third-party access requests, the same policies and procedures outlined in the previous section shall apply.
>
> x x x
>
> B. Subject to the criteria provided for the lawful processing of personal data under Sections 12 and 13 of the DPA, CCTV footage may be disclosed in the following instances:
>
> x x x
>
> 5. Other third-party requests. Third-party access requests for CCTV footage and images shall be evaluated with greater scrutiny to prevent violation of the privacy rights of the data subjects concerned.
>
> a) Upon determination of PICs that the requesting third party's needs outweigh those of the data subjects to whom the CCTV footage and images pertain, it may release information to such requesting third party.
> b) PICs must determine on a case-to-case basis if they will accede to such request taking into consideration the general principles of privacy, the rights and freedoms of the data subjects whose images are recorded by the CCTV systems, and a lawful basis for processing under Section 12 or Section 13 of

[6] National Privacy Commission, NPC Advisory Opinion 2021-028 (16 July 2021)
[7] Authorizing The Establishment Of Toll Facilities On Public Improvements, Creating A Board For The Regulation Thereof And For Other Purposes [Toll Operation Decree], Presidential Decree No. 1112

the DPA.

Based on the foregoing, the Operator should consider TRB's regulatory function as an appropriate lawful basis under the DPA in allowing viewing access to live CCTV footage in its toll facilities.

Data privacy principles; security measures; accountability of the PIC.

It must be emphasized that even if the TRB's request to the Operator may be considered as a special case, this only means that it need not establish a lawful criteria for its processing of personal data under Sections 12 of the DPA. The TRB, as a Personal Information Controller (PIC), is still subject to the other requirements under the DPA, its IRR, and issuances of the NPC. Moreover, the TRB must also adhere to the general data privacy principles of transparency, legitimate purpose, proportionality[8], and accountability.

The principle of proportionality states that the processing of personal data shall be adequate, relevant, suitable necessary, and not excessive in relation to a declared specified purpose. It also states that personal data shall only be processed if the purpose of the processing cannot be reasonably fulfilled by any other means. Thus, TRB's access to CCTV footage should be limited to its specified purpose and to specific requested footage.

On the other hand, the principle of legitimate purpose supposes that the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. In this regard, the TRB should ensure that the access to real-time footage serves its mandate to respond to tollway concerns, emergencies, and to aid in the management of traffic in tollways. The TRB, in collaboration with other toll operators, should establish comprehensive guidelines governing the sharing and access to these footage, ensuring compliance with the data privacy principles.

Meanwhile, the principle of transparency requires that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject and how these can be exercised. Thus, the TRB must provide the appropriate privacy notices to apprise data subjects that it will take CCTV recordings. A privacy notice is a statement made to a data subject that describes how an organization collects, uses, retains, and discloses personal information. A privacy notice may be referred to as a privacy statement, a fair processing statement, or, sometimes, a privacy policy[9].

Lastly, the principle of accountability requires PICs to be responsible for personal data processed using CCTV systems and shall use contractual or other reasonable means to ensure proper safeguards are in place when the processing is subcontracted to Personal Information Processors (PIPs)[10]. The TRB may ensure compliance by adhering to the general principles of privacy, implementing safeguards, keeping appropriate records, upholding data subject rights and their other obligations under the DPA, IRR, and relevant issuances of the NPC.

In the present case, we suggest that the TRB and tollway operators post privacy notices in conspicuous areas where CCTVs are operated, like toll gates, which must cite the lawful

[8] Section 18, Implementing Rules and Regulations of the Data Privacy Act of 2012.
[9] National Privacy Commission, NPC Advisory Opinion 2022-015 (23 June 2022)
[10] Sec. (3), NPC Circular 2024-02

criteria upon which the processing is based, as well as to duly inform affected data subjects.

Finally, by virtue of NPC Circular 2023-06[11], TRB should ensure the implementation of organizational, physical, and technical security measures when it receives the requested footage and information, and have mechanisms in place to enable the free exercise of data subject rights, where appropriate. We recommend that the TRB ensure that it has proper guidelines in processing CCTV footage, especially those containing personal information, taking into consideration the above discussions.

We advise that TRB adopt a more secure platform for accessing CCTV footage from toll operators. The TRB should collaborate with these toll operators to determine appropriate platforms for access and ensure that access is strictly limited to a designated personnel to prevent potential cybersecurity risks and unauthorized access.

Furthermore, we recommend implementing "view-only" access controls to minimize the risk of any accidental, unauthorized, or unlawful processing. Once viewing access is granted to the TRB, it is crucial that the use of the footage be strictly limited to its intended purpose of resolving the concerns, and emergencies, and aiding in the management of traffic in tollways.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished to us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

[11] National Privacy Commission, NPC Circular No. 2023-06 (01 December 2023)

ADVISORY OPINION NO. 2024-019[1]

26 December 2024

[redacted]

Re: INSPECTION OF CORPORATE RECORDS BY THE U.S. SECURITIES AND EXCHANGE COMMISSION VIS-À-VIS THE DATA PRIVACY ACT OF 2012

Dear [redacted], *et. al*:

We respond to your request for an Advisory Opinion on whether the records processed by your client, [redacted] (Company), are exempted from the application of the Data Privacy Act of 2012 (DPA);[2] and whether the DPA would pose any impediment to the United States Securities and Exchange Commission (U.S. SEC) ability to examine and access the Company's records.

You also seek clarification on whether the National Privacy Commission (NPC) can issue a letter of assurance to the U.S. SEC stating that: 1) NPC shall allow the U.S. SEC direct access to its records in accordance with the exemption stated in Section 4 of the DPA; and 2) the DPA shall not operate as a restriction in preventing the U.S. SEC from exercising its authority to review and examine relevant records kept and processed by the Company.

As background, you state that the Company is a business process outsourcing corporation duly organized under Philippine laws providing services to offshore clients. The Company is registered with both the Philippine Economic Zone Authority (PEZA) and the Board of Investments (BOI) as an export enterprise.

The Company's affiliate company, [redacted], entered into a contract with the Bank of [redacted] for the purpose of providing business processing services. The services involves mutual fund transactions for the clients of the Bank, including performance of procedures relating to subscription, redemptions, switching, know-yourclient (KYC) procedures, processing of account opening forms, risk disclosures, and distribution of dividends, among others. The Bank's target mutual fund clients are United

[1] Foreign jurisdiction; special cases; legitimate purpose; lawful processing.
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, (2012).

States citizens and residents, but all data processing services will be performed by the Company in the Philippines.

In the performance of the services above, the Bank will collect the data and the same will be passed to the Company for processing. The data are personal and sensitive personal information, specifically: names, birthdates, home addresses, social security numbers, national ID information, and account/banking information.

To process the Bank customers' data under its contract, the Bank is required under United States laws to deal only with registered transfer agents. Thus, the Company filed an application to obtain a transfer agent registration from the U.S. SEC. Briefly, a transfer agent registration allows an entity to record changes of ownership, maintain the issuer's security holder records, cancel and issue certificates, and distribute dividends.

The Company's transfer agent application is currently pending before the U.S. SEC, and the latter requested the former to produce a written assurance issued by its local authorities to the effect that the Company, as a matter of law, can provide the U.S. SEC with prompt direct access to its books and records (which includes personal data of its clients and employees) and to submit to onsite inspection and examination by the U.S. SEC once registered.

From the foregoing, this Advisory Opinion seeks to address issues:

1. Whether the U.S. SEC may be granted access to records processed by the Company in light of Section 4 of the DPA, particularly on the extraterritorial application of the DPA; and

2. Whether the DPA poses any impediment to the U.S. SEC's authority to examine and access the Company's records. This considers the balance between the DPA's provisions on data protection and the U.S. SEC's mandate as a regulatory agency to conduct examinations and investigations involving personal data.

Scope of the DPA; special cases; foreign jurisdiction.

The DPA and its Implementing Rules and Regulations (IRR) exclude from its scope the personal and sensitive personal information of foreigners originally collected in foreign jurisdictions and subsequently processed in the Philippines. Section 4(g) of the DPA explicitly states:

> *Section 4. Scope* – [...] This act does not apply to the following:
>
> xxx
>
> (g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

Similarly, the IRR provides a parallel provision in Section 5(f):

> *Section 5. Special Cases* – The Act and these Rules shall not apply to the following

> specified information, only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned:
>
> f. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption. In the absence of proof, the applicable law shall be presumed to be the Act and these Rules:
>
> *Provided*, that the non-applicability of the Act or these Rules do not extend to personal information controllers or personal information processors, who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity.

The DPA and its IRR provide an exemption from the coverage of the DPA for personal data processed in the Philippines when the following conditions are met: 1) the personal information is collected from residents of foreign jurisdictions; 2) the collection complies with the data privacy laws of those foreign jurisdictions; and 3) the personal information is being processed within the Philippines.

In this case, you mentioned that the Company will process personal data that: 1) is obtained by its client, the Bank, from residents of a foreign jurisdiction (specifically, the United States of America); 2) such data has been collected in compliance with the data privacy laws of that jurisdiction; and 3) such data is transferred to the Company in the Philippines strictly for processing purposes.

While the Company's current situation qualifies for an exemption under the DPA, it is important to emphasize that the exemptions cited under the DPA and its IRR is not absolute. As stated in Section 5 of the IRR, personal information controllers (PICs) and personal information processors (PIPs) are permitted to process personal data in special cases; however, such processing must be strictly limited to what is necessary to achieve the specific purpose, function, or activity.

In other words, PICs and PIPs remain accountable for ensuring compliance with the DPA's requirement on the implementation of robust organizational, physical, and technical security measures to protect personal data and to uphold the data privacy principles.

For example, a government agency with a statutory mandate may process personal data without the necessity of obtaining the data subject's consent or presenting any other lawful criteria for processing.[5] However, this processing must be strictly limited to what is essential to fulfill the agency's mandate. The agency is required to collect only the data necessary to perform its functions, use it solely for the intended purpose, and disclose only the information required for co-regulation or public disclosure. Additionally, the agency must ensure that robust security measures are in place to protect the personal data it processes.

[5] National Privacy Commission, NPC Advisory Opinion No. 2017-020 (18 July 2017).

In the same vein, the U.S. SEC's review of relevant records in the Company's custody qualifies as a special case of lawful processing under Section 4(g) of the DPA, in relation to Section 5 of the IRR. The processing conducted by the U.S. SEC serves the specific purpose of fulfilling regulatory requirements under the U.S. Securities and Exchange Act. Such processing complies with the requirement to be strictly limited to what is necessary to achieve the specified purpose. Further, as a government agency, the U.S. SEC is presumed to implement adequate safeguards to protect the personal data in its custody, thereby fulfilling the requirement to establish robust security measures for data protection.

At the same time, the personal data processed in the Philippines by the Company, acting as a PIP, remains protected under the DPA. The U.S. SEC may be granted direct access to the Company's records and conduct inspections. However, such access is subject to the Company's strict adherence to the DPA's principles of transparency, legitimate purpose, proportionality, and accountability.

Principle of Comity and Reciprocity; request for letter of assurance; lawful processing.

While Philippine corporations are primarily governed by local laws, their participation in international markets often necessitates compliance with additional regulatory requirements imposed by foreign entities, such as the U.S. SEC. These requirements are generally upheld in the Philippines under the principle of comity, where such additional regulatory requirements imposed by foreign entities are often complied with, provided they do not conflict with Philippine laws. Comity, in this context, is neither an absolute obligation nor a mere act of goodwill. Rather, it represents the mutual respect one nation extends to the laws and actions of another, balancing international duty, practical considerations, and the protection of its own citizens' rights.[7]

Similarly, the principle of reciprocity also finds application in the present concern. Reciprocity refers to the mutual exchange of rights or obligations between nations, fostering cooperation and ensuring equitable treatment. It is a cornerstone of international relations, particularlyin areas such as trade, finance, and regulatory compliance, where mutual respect for legal frameworks is crucial.[8]

The Philippines adheres to both the principles of comity and reciprocity and is committed to fostering international cooperation and conformity to global standards, all while ensuring compliance with its own legal requirements including those related to privacy and data protection.

In this context, the letter of assurance requested by the U.S. SEC from the NPC may not be appropriate given that the issuance of the same goes beyond the NPC's function. Instead, this Advisory Opinion serves the same purpose as it clarifies that the DPA should not be interpreted as a hindrance to the U.S. SEC's regulatory functions, particularly in the examination of books and records containing personal data processed by the Company.

In sum, the NPC will recognize the U.S. SEC's inspection of the Company's records as constituting lawful processing under the DPA, provided that the data privacy principles of

[7] Sison v. The Board of Accountancy and Ferguzon, G.R. No. L-2529, December 31, 1949.
[8] *Sison*, G.R. No. L-2529, *id.*

transparency, legitimate purpose, proportionality, and accountability are upheld.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

DECISIONS





MCD,

Complainant,

-versus-

VICTORIAS MILLING COMPANY, MOC, EVR, GEK, AND SC,

Respondent.

x----------x

NPC 19-758

For: Violation of the Data Privacy Act of 2012

JJD,

Complainant,

-versus-

VICTORIAS MILLING COMPANY, MOC, EVR, GEK, AND SC,

Respondent.

x----------x

NPC 19-1846

For: Violation of the Data Privacy Act of 2012

DECISION

AGUIRRE, *D.P.C.*;

Before this Commission are the consolidated cases filed by Spouses MCD and JJD (collectively, Complainants) against Victorias Milling Company (VMC), MOC, EVR, GEK, and SC (Respondents) for alleged violations of Section 25 (Unauthorized Processing), Section 26 (Access due to Negligence), Section 28 (Processing for Unauthorized Purposes), Section 29 (Unauthorized Access or Intentional Breach), Section 31 (Malicious Disclosure), Section 32 (Unauthorized Disclosure), and Section 33 (Combination or Series of Acts) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

Complainants were employees of VMC.[1] MCD narrated that during his employment as Head of the Asset Management Department from January 2016 to May 2018, VMC required him to submit a Disclosure Statement of all his financial interests and that of the members of his family up to the second degree of consanguinity or affinity.[2] This included a declaration of "the sugarcane farms [he] owned, leased, or managed, and the businesses that [he] and [his] family members may have an interest in that deals with VMC."[3] JJD, as the Administrative Assistant of the Asset Protection and Safety Department, was also required to submit a Disclosure Statement with the same contents.[4]

Complainants explained that "the Disclosure Statement is a highly sensitive document which contained [their] private matters which could not be disclosed or published without [their] knowledge and consent."[5] He further stated that the submission of the Disclosure Statement does not give VMC the right to process their personal data contained in the document.[6]

In January 2018, Complainants claimed that Respondents conducted field investigations, verifications, inspections, interviews, and inquiries to validate the sugarcane farms that they declared in their Disclosure Statements.[7] Complainants alleged that GEK, one of the respondents, surreptitiously took and carried away the sugarcane that they already harvested.[8] They also contended that GEK submitted to VMC her observations and findings that two haciendas located in the municipality of E.B. Magalona were not declared in the Disclosure Statements of the Complainants.[9] They further alleged that GEK discovered that Complainants are "in the business of

---

[1] Complaint-Affidavit of MCD y C, 27 June 2019, at 1, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).
[2] *Id.*
[3] *Id.*
[4] Complaint-Affidavit of JJD y J, 27 June 2019, at 1, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).
[5] Complaint-Affidavit of MCD y C, 27 June 2019, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).
[6] *Id. at 3; Id.*
[7] *Id. at 2; Id.*
[8] *Id.*
[9] *Id.*

financing the farming activities of certain sugarcane planters who bring their produce to VMC for milling."[10]

As a result, Complainants received Notices to Explain directing them to explain the alleged violations of the VMC Employee Code of Conduct and Discipline and other VMC Policy and Procedures.[11] As stated in the Notices, Complainants, as VMC employees, held "positions that can exert influence on other VMC employees and workers to [their] benefit and advantage, hence at the least, [their] disclosures became imperative as [their] personal business transactions could have run in conflict with [their positions]."[12]

In their Written Explanations, Complainants stated that when they submitted their Disclosure Statements in October 2017, the two haciendas were no longer leased nor operated by them.[13] They explained that the contracts of lease for both farms had already expired in 2013.[14] MCD also explained that financing the farming activities of sugarcane planters, buying standing and cut sugarcanes, and delivering them to VMC for milling does not amount to a conflict of interest.[15] In his Complaint-Affidavit, MCD added that as far as he knows, VMC does not engage in buying standing sugarcanes.[16]

Despite their explanations, Complainants received Notices of Suspension from VMC, suspending them for seven (7) days for "blatant disregard or any deviation from established control and other VMC Policies and Procedures."[17] They were also not allowed to mill their sugarcanes with VMC.[18]

---

[10] *Id.* Annex C; *Id.* Annex C;
[11] Complaint-Affidavit of MCD y C, 27 June 2019, at 3, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).
[12] *Id.* Annex C; *Id.* Annex C.
[13] *Id.* Annex D; *Id.* Annex D.
[14] *Id.* at 3; *Id.* at 3.
[15] Explanation of MCD Complaint-Affidavit of MCD y C, 27 June 2019, Annex D, *in* Sps. MCD- JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).
[16] Complaint-Affidavit of MCD y C, 27 June 2019, at 3, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).
[17] *Id.* at 4; *Id.* at 4.
[18] *Id.*

Because of this, MCD requested a grievance conference.[19] In his Request for Grievance, MCD argued that it was not clear in the Notice of Suspension what specific policies and procedures were disregarded by him that would merit his suspension.[20] He further argued that the Disclosure Statement "does not even state the corresponding sanction in case of incomplete or erroneous statement."[21] Finally, he argued that the investigation in relation to his Disclosure Statement was performed without his knowledge and consent.[22]

Complainants explained that despite the valid grounds they alleged, VMC disregarded their explanations and decided to suspend them and disallow them from milling sugar until further notice.[23] Because of this, Complainants claimed that they were "forced to render [their] voluntary resignation from employment."[24]

Due to the incident, Complainants filed their respective Complaint- Affidavits dated 27 June 2019, against Respondents for violations of the DPA.[25]

Complainants alleged that VMC violated the DPA when Respondents conducted an investigation and validation of the sugarcane farms that they stated in their Disclosure Statements without their knowledge and consent.[26] They prayed for the Commission to find Respondents guilty of violations of the DPA.[27] They also claimed that they are entitled to moral damages, exemplary damages, and attorney's fees.[28]

---

[19] Request for Grievance dated 17 February 2018, Complaint-Affidavit of MCD y C, 27 June 2019, Annex F, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] Complaint-Affidavit of MCD y C, 27 June 2019, at 4, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).
[24] Complaint-Affidavit of MCD y C, 27 June 2019, at 4, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 3-4, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).
[25] *Id.*
[26] *Id.*
[27] *Id.* at 5; *Id.* at 4-5.
[28] *Id.*

On 18 December 2020, the National Privacy Commission (NPC), through its Complaints and Investigation Division (CID), consolidated the two (2) cases and directed the parties to Confer for Discovery.[29]

On 11 March 2021, Respondents filed their Entry of Appearance.[30]

On 23 March 2021, only Complainants, through their representative, appeared for the discovery conference, while Respondents failed to appear.[31] Complainants manifested that they are not willing to reset the discovery conference.[32] Thus, in view of Complainants' manifestation and the effectivity of NPC Circular 2021-01 (2021 NPC Rules of Procedure),the CID ordered Respondents to file their verified comment within fifteen (15) days from receipt of the Order.[33]

On 30 September 2021, the CID issued an Order stating that it has not received a verified comment from Respondents.[34] As a result, to give due course to the cause of both parties, it gave Respondents a final period of fifteen (15) days from receipt of the Order to file its verified comment to the complaint.[35]

On 18 October 2021, Respondents filed their Consolidated Comment.[36]

In their Consolidated Comment, Respondents explained that in the course of its business operations, it collects, uses, and processes the personal data of its employees, consultants, visitors, clients, and other stakeholders.[37]

---

[29] Order to Confer for Discovery, 10 February 2021, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[30] Entry of Appearance dated 01 March 2021, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[31] Order to File Verified Comment, 23 March 2021, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[32] *Id.*
[33] *Id.*
[34] Order (To File Verified Comment and Appear Virtually for Preliminary Conference), 27 September 2021, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[35] *Id.*
[36] Consolidated Comment, 18 October 2021, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[37] *Id.*

Respondents claimed that VMC believes in the importance of good corporate governance as part of sound strategic management.[38] Therefore, they undertake the necessary efforts to create awareness and ensure compliance with the same, which includes the creation of the Manual on Corporate Governance.[39]

Further, Respondents explained that VMC, as a publicly listed corporation, must comply with the Securities and Exchange Commission Code of Corporate Governance for Publicly Listed Companies under SEC Memorandum Circular 19 Series of 2016 which provides for "the adoption of programs that mitigate corrupt practices such as but not limited to bribery, fraud, extortion, collusion, conflict of interest and money laundering."[40]

Respondents stated that as part of its compliance with the SEC's Memorandum Circular 19 Series of 2016, guided by its Manual on Corporate Governance and pursuant to good corporate governance, it required all of its employees and consultants to execute the VMC Disclosure Statement yearly or as often as required.[41] The disclosure was designed "to prevent and address any actual or potential conflict of interest that may adversely affect the interest of the company and its stakeholders, such as personal dealings between employees, consultants and VMC."[42]

Through its Disclosure Statements, Respondents explained that it collects from each employee and consultant his or her name, position, VMC ID number, other positions held outside VMC, names of family members related to any director, officer, employee, or consultant of VMC group, relationships, and signature.[43]

Respondents then narrated that in early 2018, VMC conducted a validation of the information contained in the submitted Disclosure

---

[38] *Id.*
[39] *Id.*
[40] *Id.* at 3.
[41] *Id.* at 2.
[42] Consolidated Comment, 18 October 2021, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[43] *Id.* at 3.

Statements.[44] It then discovered that "there were certain sugarcane farms and financing activities linked to Complainants that were not divulged in their Disclosure Statements."[45] Hence, in accordance with its company procedures and the Labor Code of the Philippines, it initiated its internal administrative process which resulted in the suspension of Complainants.[46]

Respondents alleged that during the entire process of investigation, assessment, and action about Complainants, they complied with the DPA and other applicable laws.[47] They explained that "to maintain the confidentiality of personal data, only authorized personnel whose functions included participation in the conduct of internal administrative proceedings under the Labor Code (i.e., HR, Legal, Audit) were given access to information which includes the other respondents."[48] They further alleged that the individual respondents only carried out their tasks by virtue of their positions as officers or employees of VMC.[49]

> For her part, Ms. GEK has authority to access personal information in relation to the Disclosure Statement as Head of the Transformation Department and Internal Audit being that she is responsible in auditing information/processes and providing reports thereon that could adversely affect the business of VMC, one of which is the violation of the company's policy on conflict of interest. For their part, Ms. MOC, Ms. EVR and Ms. SC have authority to access personal information being signatories of the Notice to Explain and other necessary processes by the company.[50]

They claimed that prior to the effectivity of Complainants' resignation, they had amicable discussions and considered their demands.[51] After negotiation, both Complainants received a sum of money, that is One Million Five Hundred Thousand Pesos (Php 1,500,000.00) for MCD and Five Hundred Thousand Pesos (Php

---

[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.* at 4.
[48] Consolidated Comment, 18 October 2021, at 4, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[49] *Id.* at 3.
[50] *Id.* at 19.
[51] *Id.* at 4.

500,000.00) for JJD.[52] On 26 April 2018, Complainants also executed a Release, Waiver and Quitclaim on account of the received settlement.[53]

On 28 June 2019, the Respondents disclosed that VMC filed before the Regional Trial Court of Silay a complaint for breach of contract against Complainants.[54] It was after the filing of the aforementioned complaint that the Respondents discovered the present case filed before the Commission.[55]

Respondents argued that the complaint should be dismissed on the grounds that Complainants are guilty of forum shopping, that the claim or demand set forth in the complaint has been paid, waived, abandoned, or otherwise extinguished, and that the complaint lacks merit.[56]

Respondents contended that the information contained in the Disclosure Agreement only pertained to personal information as defined under the DPA and their processing was based on contracts under Section 12 (b), compliance with a legal obligation under Section 12 (c), and legitimate interest under Section 12 (f) of the DPA.[57]

They explained that the processing of personal data was based on a contract.[58] Further, they stated that at the time of processing, an employment relationship existed between them and Complainants which is governed by an employment contract.[59] This allows them to process certain information that are necessary and related to the fulfilment of the contract:

> *Processing of personal data based on contract*

---

[52] *Id.*
[53] *Id.*
[54] Consolidated Comment, 18 October 2021, at 4-5, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[55] *Id. at 6.*
[56] *Id.*
[57] *Id.* at 13.
[58] *Id.* at 14.
[59] *Id.*

> It is of no issue that there is an employment relationship between Complainants and VMC at the time when the processing of the personal information was done. Such relationship is governed by the contract entered into by the parties. In an employment relationship, certain information are processed which are necessary and is related to the fulfillment of the contract between the parties. Such information includes personal data which is needed to benefit the employee like those data needed to process salary as well as those for the benefit of the employer, VMC in this case, needed to protect its interest such as disclosures of information involving conflict of interest. When the Complainants entered into a contract with the respondent VMC, they were made aware that certain information will be collected and processed by the company, failure of which may result in the severance of their employment contract.[60]

They further stated that as a Personal Information Controller (PIC), VMC has a legal obligation to process personal data to comply with the law, especially since it is a publicly listed company subject to compliance with regulatory requirements, particularly SEC Memorandum Circular 19 Series of 2016:

> *Processing of personal data based on legal obligation*
>
> VMC, being a publicly listed company, is subject to certain legal obligations set out by its regulators. Regulatory requirements also qualify as a legal obligation.
>
> In relation to the Disclosure Statement which is the subject of this present case, the pertinent issuance of the Securities and Exchange Commission, i.e., SEC Memorandum Circular No. 19, Series of 2016 applies. The said memorandum requires that the Company must adopt programs that mitigate corrupt practices such as but not limited to bribery, fraud, extortion, collusion, conflict of interest and money laundering. As previously stated, the VMC Disclosure Statement is part of VMC's compliance to the said SEC-mandated Code of Corporate Governance for Publicly-Listed Companies which is designed to prevent and address any actual or potential conflict of interest that may adversely affect the interest of the company and its stakeholders

---

[60] Consolidated Comment, 18 October 2021, at 14, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

such as personal dealings between employees, consultants and VMC.[61]

They also stated that VMC has a legitimate interest in processing Complainants' personal information, being a publicly listed company with a responsibility towards its investors.[62] Also, part of its good corporate governance initiatives is "to ensure that all possible conflicts of interest of its employees and consultants are addressed."[63] They explained that VMC processes personal information in relation to the Disclosure Statement to protect its legitimate interest of preventing fraud and violations of its policies which may affect the business:

> *Processing of personal data based on legitimate interest*
>
> In this case, the processing of the personal information contained in the Disclosure Statement is necessary for the purposes of the legitimate interest of VMC. VMC as a publicly listed company has a responsibility towards its investors. It holds its shareholders' best interests as a priority and is committed in maintaining stockholder confidence and optimism at all times. Part of its good corporate governance initiatives is to ensure that all possible conflict interest of its employees and consultants are addressed. Hence, it has mandated all those connected to the company to submit their Disclosure Statements.
>
> . . .
>
> In this case, the processing of the personal information contained in the Disclosure Statement is based on the legitimate interest of the organization to prevent fraud and violation of its policies which may affect the business.[64]

Respondents argued that assuming the Disclosure Statements contained sensitive personal information, they still have lawful basis in processing the information because it is necessary for the protection of its lawful rights and interest pursuant to Section 13 (f) of the DPA.[65]

---

[61] *Id.*
[62] *Id.* at 15.
[63] *Id.*
[64] *Id.* at 15.
[65] *Id.* at 16-17.

> The act of Complainants in withholding information which VMC requires from all its employees and consultants gave rise for VMC to process the information in order to protect its lawful rights and interest and implement company policies.[66]

Respondents added that there was a need to assess whether Complainants can reasonably expect their data to be processed in such manner.[67] They argued that because of the employment contract entered into between the parties and VMC's legitimate interest, Complainants have a lesser expectation of privacy in relation to the disclosures made by Complainants to VMC and its authorized persons.[68]

Respondents also contended that Complainants failed to particularly identify which information was processed and how the individual respondents were able to unlawfully access or disclose their information as they were performing such in their official capacity:[69]

> Aside from mentioning Ms. GEK performing her function to validate the contents of the Disclosure Statement, Ms. EVR and Ms. SC as issuer and signatory of the Notice to Explain, Complainants did not give any material information which can substantiate their allegation that respondents MOC, EVR, GEK and SC unlawfully processed, used or disclosed their personal data.[70]

Finally, Respondents alleged that "the allegations lack the necessary information to establish [Complainants'] claims and that indeed the crime alleged has been committed."[71]

In relation to Sections 25, 28, and 32, Respondents stated that they have clearly explained that there was lawful basis in the processing of the information based on contract, legitimate interest and/or protection of lawful rights and interests, or the establishment,

---

[66] Consolidated Comment, 18 October 2021, at 17, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[67] *Id.*
[68] *Id.* at 18.
[69] *Id.* at 19.
[70] *Id.*
[71] *Id.* at 20.

exercise, or defense of legal claims.[72] Therefore, the allegations that Respondents committed unauthorized processing, processing personal data for unauthorized purpose/s, and unauthorized disclosure must not prosper.[73]

As to Sections 26, 29, and 31, Respondents contended that the allegations do not provide for the acts or facts that result in a violation of these sections.[74] They argued further that the imputation that Respondents maliciously and fraudulently conducted the investigation to validate Complainants' sugarcane farms is not within the purview of Sections 26, 29, and 31 of the DPA.[75] There was no allegation of disclosure of unwarranted or false information with malice or bad faith on the part of Respondents.[76]

Respondents thus averred that they did not violate Sections 25, 26, 28, 29, 31, 32, and 33 of the DPA and prayed for the dismissal of the complaint with prejudice for failure to substantiate and prove the allegations.[77]

During the 26 October 2021 preliminary conference, only Respondents appeared.[78] The CID noted the receipt of Complainants' Urgent Motion for Postponement and the preliminary conference was reset for the last time.[79]

On 16 November 2021, during the Preliminary Conference, Complainants manifested that they are requesting for the minutes or records of the grievance proceedings held on 01 March 2018. Respondent's counsel, however, raised the relevance which the document may serve as the same had nothing to do with the allegations in the complaint.[80] Complainants, through counsel,

---

[72] Consolidated Comment, 18 October 2021, at 20, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.* at 2.
[78] Order, 26 October 2021, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846
(NPC 2021).
[79] Fact-Finding Report, 29 December 2022, at 3, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).
[80] Order (After the Preliminary Conference on 16 November 2021), 16 November 2021, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

answered that the minutes of the grievance proceedings will show the basis of Complainants' suspension and that some of Complainants' vital records were violated.[81] Respondents opposed the production of the document considering that the grievance proceedings tackled a different matter and is not connected with data privacy.[82] As a result, the CID ordered Respondents to submit a Comment/Opposition to the Discovery of the Document.[83]

During the Preliminary Conference, both parties, however, manifested that they are willing to undergo mediation proceedings.[84] Therefore, the proceedings were suspended. [85]

On 19 and 20 November 2021, Respondents[86] and Complainants[87] respectively, signed and submitted their Applications for Mediation.

On 05 January 2022, the CID issued an Order to Mediate and for the parties to appear for a preliminary mediation conference.[88] The CID, however, ordered the termination of the mediation proceedings due to the parties' repeated delays in rescheduling the preliminary mediation conference for more than two (2) months.[89]

On 10 March 2022, the Mediation Officer issued a Notice of Non- Settlement to the parties.[90] On 15 March 2022, the CID lifted the suspension of the complaints proceedings and ordered the parties to file their memoranda.[91] The CID also ordered Respondents to submit their Comment/Opposition to the Discovery of the Document. [92]

---

[81] *Id.*
[82] *Id.*
[83] *Id.* at 2.
[84] *Id.*
[85] *Id.*
[86] Application for Mediation, 19 November 2021, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[87] *Id.*
[88] Order to Mediate, 05 January 2022, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).
[89] Notice of Non-Settlement of Dispute, 10 March 2022, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).
[90] *Id.*
[91] Order (for Resumption of Complaints Proceedings, Requiring Respondents to Submit their Comment/Opposition to the Discovery of the Document, and Requiring the Parties to Submit their Simultaneous Memoranda), 15 March 2022, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).
[92] *Id.*

On 30 March 2022, Respondents submitted their Comment/Opposition to the Discovery of the Document dated 30 March 2021.[93] Respondents argued that the disclosure of the internal documents and communications, specifically the minutes of the grievance meeting, was "irrelevant, protected by a form of privilege, and must be excluded for legitimate reasons such as but not limited to internal policies, labor relations policy, dispute resolution rules, among others."[94]

> The fact in issue in the instant case is the alleged violation sometime on or before 23 January 2018 and the Disclosure Statements. The minutes of the grievance meeting was on 18 March 2018 in relation to work suspension. Thus, the request has no bearing on the allegations in the complaint. [95]

On 01 April 2022, the CID noted the Respondents' Comment/Opposition to the Discovery of the Document.[96]

On 18 April 2022, Respondents filed their Memorandum.[97] They reiterated that aside from the bare allegations of Complainants, nothing in the complaint "provided any detail as to who among the Respondents processed personal data, what kind of personal data, and how could they have used [the] personal data."[98] Further, they restated their arguments that there was lawful processing based on contract, legal obligation, legitimate interest, and protection of lawful rights and interest [99]

On 11 August 2022, Complainants filed their Memorandum.[100] They maintained that the acts of Respondents in "processing, validating, spying, [and] publishing the contents of the Disclosure Statements of

---

[93] Comment/Opposition to Discovery of Document, 30 March 2022, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

[94] *Id.*at 2.

[95] *Id.*at 3.

[96] Order (Noting the Comment/Opposition to Discovery of Document filed by Respondents), 01 April 2022, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

[97] Memorandum for the Respondents, 18 April 2022, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

[98] *Id.* at 16.

[99] *Id.* at 20-22,

[100] Memorandum for Complainant, 20 July 2022, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

the complainants is a gross violation of the [DPA]" because the submission of their Disclosure Statements do not give Respondents absolute authority to process its contents.[101] Complainants further alleged that Respondents conducted their investigations and inquiries with bias because "they came up with an unverified report that is grossly erroneous, having no factual basis but hearsays and assumptions, full of malice and ill-intent."[102]

Issues

I. Whether there is substantial evidence to find Respondents liable for a violation of the DPA;

II. Whether Respondents' act of processing the contents of the Disclosure Statements is a violation of the DPA.

Discussion

The Commission dismisses the case for lack of substantial evidence.

Complainants failed to substantiate their allegations on how the Respondents violated the DPA. Other than the general statements made in their complaints and Memorandum, the Complainants neither specified the personal data that was unlawfully processed nor alleged the Respondents' specific acts that amount to a violation of the DPA.

Nevertheless, Respondents' acts of processing the contents of Complainants' Disclosure Statements was pursuant to its legitimate interest and did not go beyond what Complainants can reasonably expect upon submission of their Disclosure Statements.

I. There is no substantial evidence to find Respondents liable for a violation of the DPA.

---

[101] *Id.*
[102] Memorandum for the Respondents, 18 April 2022, at 7, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

Respondents, who are VMC and its officers and employees, cannot be held liable for a violation of the DPA based on the allegations of and evidence submitted by Complainants.

Complainants claimed that Respondents violated Sections 25, 26, 28,
29, 31, 32, and 33 of the DPA by processing their personal data without their authority and consent.[103] To substantiate their complaint, Complainants submitted their Disclosure Statements,[104] a copy of the blotter report that records the incident where Respondent GEK surreptitiously took and carried away their sugarcane for milling,[105] the Notices to Explain issued by Respondents to MCD and JJD,[106] the written Explanations of MCD and JJD,[107] the Notices of Suspension,[108] the Request for Grievance submitted by MCD,[109] the Letter giving VMC the opportunity to reply before filing a complaint with the NPC,[110] the Certification from Negros Del Norte Planters Association that JJD informed them about the expiration of the lease of one of the undisclosed haciendas,[111] and the Letter from VMC stating that they are referring the matter to their legal counsel.[112]

Section 1 of Rule 131 of the 2019 Amendments to the Revised Rules on Evidence provides:

> Section 1. *Burden of proof and burden of evidence*. **Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim** or defense by the amount of evidence required by law. Burden of proof never shifts.

---

[103] Complaint-Affidavit of MCD y C, 27 June 2019, at 5, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 5, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

[104] *Id.* Annex A; *Id.* Annex A.

[105] *Id.* Annex B; *Id.* Annex B.

[106] *Id.* Annex C; *Id.* Annex C.

[107] *Id.* Annex D; *Id.* Annex D.

[108] *Id.* Annex E *Id.* Annex E.

[109] Complaint-Affidavit of MCD y C, 27 June 2019, Annex F, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

[110] Complaint-Affidavit of MCD y C, 27 June 2019, Annex G, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of MCD y C, 27 June 2019, Annex F *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

[111] Complaint-Affidavit of MCD y C, 27 June 2019, Annex F *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

[112] Complaint-Affidavit of MCD y C, 27 June 2019, Annex H, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of MCD y C, 27 June 2019, Annex G *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

> Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a prima facie case. Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case.[113]

Section 6 of Rule 133 of the 2019 Amendments to the Revised Rules on Evidence provides:

> Section 6. *Substantial Evidence*. In cases filed before administrative or quasi-judicial bodies, a fact may be deemed established if it is supported by substantial evidence, or that amount of relevant evidence which a reasonable mind might accept as adequate to justify a conclusion.[114]

In this case, Complainants, had the burden of proof in alleging a violation of the DPA. Complainants, however, did not discharge this burden as they failed to support their allegations with substantial evidence.

In *BSA Tower Condominium Corporation v. Reyes,*[115] the Supreme Court held that:

> The basic rule is that mere allegation is not evidence and is not equivalent to proof. Likewise, charges based on mere suspicion and speculation cannot be given credence. [116]

As correctly stated by Respondents, nothing in the complaint "provided any detail as to who among the Respondents processed personal data, what kind of personal data, and how could they have used [the] personal data."[117]

In their submissions, Complainants only mentioned that Respondent GEK validated the contents of the Disclosure Statements by

---

[113] 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. No. 19-08-15-SC, rule 131, §1 (1 May 2020). Emphasis supplied.
[114] *Id.* rule 133, §6.
[115] BSA Tower Condominium Corp. v. Reyes II, A.C. No. 11944 (2018).
[116] *Id.*
[117] Memorandum for the Respondents, 18 April 2022, at 20-22, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

conducting a field investigation.[118] They failed to prove how Respondents MOC, EVR and SC, as issuers and signatories of the Notice to Explain, unlawfully processed their information.

Further, they failed to particularly identify which information Respondents processed and how Respondents unlawfully accessed or disclosed Complainants' personal data. They neither specified nor discussed the provisions of the DPA that Respondents supposedly violated.

In sum, Complainants failed to discharge their burden and to submit substantial evidence to support their claim against Respondents. Thus, the case must be dismissed for lack of substantial evidence.

II. Respondents' act of processing and validating the contents of Complainants' Disclosure Statements was pursuant to its legitimate interest.

While it has been established earlier that Complainants failed to identify which information Respondents processed, a perusal of the records shows that the personal data in the Disclosure Statements only involves personal information.

Section 3 (g) of the DPA defines personal information:

> Section 3. *Definition of Terms.* Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:
>
> . . .
>
> (g) Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[119]

---

[118] Complaint-Affidavit of MCD y C, 27 June 2019, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

[119] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy

The Disclosure Statements included the names, positions, I.D. numbers, employment information, personal relationships, and financial interests of the employees and consultants of VMC.[120] The employees and consultants' names clearly fall under the definition of personal information. Further, these information, when put together, can directly and certainly identify the members of VMC. Thus, they are considered personal information under the DPA.

Nevertheless, Respondents processed the personal information involved according to a lawful criterion under Section 12 (f) of the DPA. Section 12 (f) of the DPA allows for the processing of personal information when it is necessary for the purposes of the legitimate interests pursued by the PIC:

> Section 12. *Criteria for Lawful Processing of Personal Information*. The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> . . .
>
> (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[121]

Processing based on legitimate interest requires the fulfillment of the following conditions: (1) the legitimate interest is established; (2) the means to fulfill the legitimate interest is both necessary and lawful; and (3) the interest is legitimate and lawful and it does not override fundamental rights and freedoms of data subjects.[122]

Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (g) (2012).

[120] Complaint-Affidavit of MCD y C, 27 June 2019, Annex A, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, Annex A, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

[121] Data Privacy Act of 2012, § 12 (f).

[122] MAF v. Shopee, NPC 21-167, 22 September 2022, at 9, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-21-167-2022.09.22-MAF-v.-Shopee-Decision-Final.pdf (last accessed 05 July 2023).

In this case, Respondents have clearly established that the processing and validating of the Disclosure Statements were done pursuant to the VMC's legitimate interest of preventing and addressing any actual or potential conflict of interest that may adversely affect the interest of the company in its stakeholders, such as dealings between employees, consultants and VMC.[123]

A. Respondents established their legitimate interest in processing Complainants' Disclosure Statements.

The first requisite of processing based on Section 12 (f) of the DPA is that the legitimate interest is established.[124] This focuses on what the PIC seeks to accomplish with the specific processing activity. To determine whether this has been established, the PIC must comply with the general privacy principles of (1) legitimate purpose and (2) transparency.

Section 11 of the DPA discusses legitimate purpose as follows:

> Section 11. *General Data Privacy Principles.* The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, **legitimate purpose** and proportionality.
>
> Personal information must, be:
>
> (a) **Collected for specified and legitimate purposes** determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;
>
> ...
>
> (e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or **for legitimate business purposes, or as provided by law**[.][125]

---

[123] Consolidated Comment, 18 October 2021, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

[124] MAF v. Shopee, NPC 21-167, at 9.

[125] Data Privacy Act of 2012, § 11 (a)(e). Emphasis supplied.

Elaborating on this, Section 18 of the Implementing Rules and Regulations of the DPA (IRR) provides:

> Section 18. *Principles of Transparency, Legitimate Purpose and Proportionality.* The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.
>
> . . .
>
> b. Legitimate purpose. The processing of information shall be compatible with a declared and **specified purpose which must not be contrary to law, morals, or public policy.**[126]

The legitimate purpose principle requires that: (1) the purpose of processing must be specified; and (2) that purpose must not be contrary to law, morals, or public policy.[127]

The first element requires that there should be a specific purpose, such that the purpose of processing is clearly defined and not vague or overbroad. While this does not require an exhaustive enumeration of each and every purpose, the purpose must be specific enough for the data subject to understand the purpose of processing. The second element requires the purpose to be within the limitations of the law, which should be understood to include the entire body of laws, rules, and regulations.[128] Additionally, the purpose of processing should not go against prevailing morals or run counter to public policy.[129]

Both elements of legitimate purpose are satisfied in this case. The processing of Complainants' information was done pursuant to a legitimate purpose, which was to comply with existing regulations and to ensure that there were no deviations from the company's policies that could be detrimental to the business of VMC. Further,

---

[126] National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule IV, § 18 (a)(b) (2016) Emphasis supplied.
[127] *See* Data Privacy Act of 2012, § 11; Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 18 (a)(b).
[128] MLF v. MyTaxi.PH Corp., NPC 19-142, 31 March 2022, at 8, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-19-142-MLF-v.-Grab-Philippines 2022.03.31.-Decision.pdf (last accessed 24 August 2023).

such purpose is not contrary to any law, rule, or regulation or against morals and policy.

VMC, as a publicly listed corporation, has a responsibility towards its investors and must comply with the Securities and Exchange Commission Code of Corporate Governance for Publicly Listed Companies under SEC Memorandum Circular 19 Series of 2016.[130] The SEC Memorandum Circular requires such corporations "to establish corporate disclosure policies and procedures that are practical and in accordance with best practices and regulatory expectations."[131] This includes the adoption of anti-corruption programs to mitigate corrupt policies which include conflict of interest.[132]

Further, VMC has legitimate business interest to prevent and address conflicts of interest that may adversely affect the company and its stakeholders.[133] VMC, in compliance with the SEC Circular and pursuant to good corporate governance, required all of its employees and consultants to execute the Disclosure Statements. Clearly, Respondents have a real and present interest in the processing of the Disclosure Statements of its employees.

Further, the transparency principle requires that the claimed interest is declared to the data subject.[134] The PIC should inform the data subject of the nature, purpose, and extent of the processing, using clear and plain language that is easy to access and understand.[135]

In this case, Respondents clearly and adequately communicated to the employees, including Complainants, VMC's legitimate interest in processing Complainants' information through the provisions found in the Disclosure Statements. As stated in the Disclosure Statements, the disclosure is done "in accordance with the VMC Group policy on

---

[130] Consolidated Comment, 18 October 2021, at 3, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[131] Securities and Exchange Commission, Code of Corporate Governance for Publicly-Listed Companies, Principle 8 (2016).
[132] *Id.* Recommendation 15.2.
[133] Consolidated Comment, 18 October 2021, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).
[134] Data Privacy Act of 2012, § 11 (a).
[135] Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 18 (a).

good corporate governance to ensure transparency in (the) working relations with all parties."[136] Further, the Disclosure Statements stated who are covered and what would amount to a conflict of interest.[137]

> **1. Coverage**
> This statement is to be accomplished by employees and consultants of Victorias Milling Company, Inc. (VMC) and its subsidiaries (the VMC Group).
>
> **2. Definition of Terms**
>
> ...
>
> **Conflict of Interest –** any personal or financial interest, actual or apparent, that is in conflict with VMC Group duties and responsibilities.
>
> Areas wherein conflict of interest may arise:
> 1. Dealings with/as suppliers, contractors, business partners, consultants, or third parties
> 2. Dealings with directors, employees, consultants, and prospective employees and consultants
>
> ...
>
> 3. In accordance with the VMC Group policy on good corporate governance to ensure transparency in my working relations with all parties, I hereby declare and disclose the following: [138]

Thus, Respondent established their legitimate interest and satisfied the first requisite of processing based on Section 12 (f) of the DPA. They have communicated their specific purpose in processing Complainants' Disclosure Statements and such purpose is not contrary to law, morals, or public policy.

B. The means that Respondents used to fulfill its legitimate interest were both necessary and lawful.

The second requisite of processing based on Section 12 (f) of the DPA is that the means to fulfill the legitimate interest is both necessary and lawful.[139] For this requisite, the PIC must evaluate how it is

---

[136] Complaint-Affidavit of MCD y C, 27 June 2019, Annex F, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).
[137] *Id.*
[138] *Id.*
[139] MAF v. Shopee, NPC 21-167, at 9.

accomplishing its legitimate interest as previously established. The PIC must show that the means or the specific processing activity undertaken is (1) necessary and (2) lawful.[140]

As the Commission previously held, the qualifier "necessary" refers to the general privacy principle of proportionality.[141] Following this principle, the processing must be adequate, relevant, suitable, and necessary, such that it is not excessive in relation to the declared and specified purpose.[142]

Section 11 of the DPA provides:

> Section 11. *General Data Privacy Principles.* The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and **proportionality.**
>
> Personal information must, be:
>
> . . .
>
> (c) Accurate, **relevant and, where necessary for purposes for which it is to be used the processing of personal information**, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;
>
> (d) **Adequate and not excessive in relation to the purposes for which they are collected and processed**[.][143]

Section 18 of the Implementing Rules and Regulations of the DPA (IRR) elaborates on proportionality:

> Section 18. *Principles of Transparency, Legitimate Purpose and Proportionality.* The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and **proportionality**.

---

[140] *See* Data Privacy Act of 2012, § 11 (b)(c)(d).
[141] EA and TA v. EJ, EE, and HC, NPC 17-018, 15 July 2019, at 10, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-17-018-EA-and-TA-v-EJ-Decision- 2019.07.15-.pdf, (last accessed 24 August 2023).
[142] Data Privacy Act of 2012, § 11 (c)(d).
[143] *Id.* § 11 (b)(c)(d). Emphasis supplied.

. . .

> c. Proportionality. The processing of information shall be **adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.** Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[144]

Given this, processing is deemed proportional when (1) processing is adequate, relevant, and necessary to the declared and specified purpose; and (2) the means by which processing is performed is the least intrusive means available.[145]

In *Philippine Stock Exchange Inc. v. Secretary of Finance*, the Supreme Court explained "necessary" to mean that "the personal data sought by the State must be acquired through 'narrowly tailored' means, which are only necessary to accomplish the regulatory agencies' given mandate."[146] As applied in this case, the PIC must adopt means that are only necessary to accomplish its legitimate interest to prevent abuses.

In this case, Respondents' act of validating the VMC employees' Disclosure Statements was necessary to verify the accuracy of the entries and detect discrepancies in the Disclosure Statements. Respondents conducted field investigations, verifications, inspections, interviews, and inquiries simply to verify the entries of Complainants on their Disclosure Statements.[147] By doing so, Respondents can ensure that all possible conflicts of interests of the VMC employees and consultants are addressed. Further, as stated by Respondents, the validation was done with utmost confidentiality as "only authorized personnel whose functions included participation in the conduct of internal administrative proceedings under the Labor Code were given access" to Complainants' information.[148]

---

[144] Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 18 (c). Emphasis supplied.

[145] MAF v. Shopee, NPC 21-167, at 14.

[146] Philippine Stock Exchange v. Secretary of Finance, G.R. No. 213860 (2022).

[147] Complaint-Affidavit of MCD y C, 27 June 2019, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

[148] Consolidated Comment, 18 October 2021, at 4, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

Specifically, GEK, as the Head of the Transformation Department and Internal Audit, is responsible for auditing information and providing reports thereon that could adversely affect the business of VMC.[149] Thus, it was necessary for her to process the information in the Disclosure Statements.

The second element is also present as the means chosen by Respondents were lawful. For this element, it requires that the means chosen to accomplish the legitimate interest is itself lawful.[150] The PIC cannot violate any law in the process of accomplishing its legitimate interest. Considering that the determination of lawfulness goes into the means chosen to accomplish the legitimate interest, it is different from the lawfulness of the purpose under the general privacy principle of legitimate purpose (i.e. purpose must not be contrary to law, morals, and public policy). Section 11 of the DPA provides:

> Section 11. *General Data Privacy Principles.* The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.
>
> Personal information must, be:
>
> . . .
>
> (b) Processed fairly and **lawfully;**

Respondents' adopted means for validating the information in the Disclosure Statements were lawful. The field investigation and the inquiries done by Respondents did not violate any existing law or regulation, company policy, or contractual agreement between VMC and Complainants.

C. Respondents' interest is legitimate and lawful and it does not override fundamental rights and freedoms of data subjects.

---

[149] *Id.* at 19.
[150] *See* Data Privacy Act of 2012, § 11 (b).

The third requisite is that the interest is legitimate and lawful and it does not override fundamental rights and freedoms of data subjects. [151] This requisite focuses on the effect of accomplishing the legitimate interest such that it does not override the fundamental rights and freedoms of the data subjects.

A determination of the effect of accomplishing legitimate interest requires an analysis of the totality of the three (3) requisites. Given that the legitimate interest of the PIC has been established (first requisite) and the PIC's means to fulfill that legitimate interest is both necessary and lawful (second requisite), it must now be determined whether the processing undertaken does not override the Complainants' fundamental rights and freedoms (third requisite).

In determining the effect of the PIC's legitimate interest on the data subject, aside from the categories of personal information that is processed, the Commission considers the general privacy principle of fairness and the reasonable expectation of the data subjects with regard to the processing of their personal information.

Section 11 (b) of the DPA states that the personal information must be processed fairly.[152]

> Section 11. *General Data Privacy Principles.* – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.
>
> Personal information must, be:
>
> . . .
>
> (b) Processed **fairly** and lawfully[.][153]

Section 19 of the Implementing Rules and Regulations of the DPA (IRR) elaborates on fairness:

---

[151] MAF v. Shopee, NPC 21-167, at 9.
[152] Data Privacy Act of 2012, § 11 (b).
[153] *Id.* Emphasis supplied.

> Section 19. *General principles in collection, processing and retention.* The processing of personal data shall adhere to the following general principles in the collection, processing, and retention of personal data:
>
> . . .
>
> b. Personal data shall be processed **fairly** and lawfully.
>
> 1. Processing shall uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent, and allow the data subject sufficient information to know the nature and extent of processing.
> 2. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.
> 3. Processing must be in a manner compatible with declared, specified, and legitimate purpose.
> 4. Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
> 5. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.[154]

As discussed, Respondents processed Complainants' personal data in compliance with the SEC Circular and pursuant to good corporate governance.[155] The validation of the Disclosure Statements did not go beyond what can be reasonably expected by Complainants, as employees, when they submitted their Disclosure Statements to VMC. It is not unreasonable to expect that these Disclosure Statements would be subject to verification and validation as a necessary consequence.

The interest of Respondents to comply with regulatory requirements and protect its business from conflicts of interest that may adversely affect the company is legitimate and does not override the fundamental rights and freedoms of the data subjects, including

---

[154] Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 19(b). Emphasis supplied.
[155] Consolidated Comment, 18 October 2021, at 2, *in* Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

Complainants. This legitimate interest does not, in any way, disregard the fundamental rights and freedoms of Complainants.

In sum, for processing based on Section 12 (f) of the DPA to apply, the PIC must comply with three (3) requisites.[156] The first requisite focuses on what the PIC is accomplishing and the legitimate purpose that has been communicated to the data subject. The second requisite refers to how the PIC is accomplishing the legitimate interest, such as the means chosen or the specific processing activity undertaken, which should be necessary and lawful. Finally, the third requisite considers the effect of accomplishing the legitimate interest, such that it does not override the fundamental rights and freedoms of the data subjects.

In this case, Respondents complied with all three requisites for processing based on legitimate interest. Respondents have clearly established the legitimate interest in processing the Disclosure Statements. The investigations and interviews lawfully conducted were necessary to verify the accuracy of the entries in the Disclosure Statements. Further, their acts did not go beyond what could be reasonably expected by Complainants, as employees, when they submitted their Disclosure Statements. Thus, even if Complainants had presented substantial evidence to support their claims, Respondents would still have lawful basis under Section 12 (f) of the DPA when they processed Complainants' personal information.

Given the foregoing, the Commission cannot find Respondents liable for violating Section 25 (Unauthorized Processing), Section 26 (Access due to Negligence), Section 28 (Processing for Unauthorized Purposes), Section 29 (Unauthorized Access or Intentional Breach), Section 31 (Malicious Disclosure), Section 32 (Unauthorized Disclosure), and Section 33 (Combination or Series of Acts) of the DPA.

WHEREFORE, premises considered, this Commission resolves that the case filed by Spouses MCD and JJD against Victorias Milling Company, MOC, EVR, GEK, and SC is **DISMISSED** for lack of substantial evidence.

---

[156] MAF v. Shopee, NPC 21-167, at 9.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases before any other forum or tribunal, if any.

SO ORDERED.

City of Pasay, Philippines.
30 June 2023.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

JOHN HENRY D. NAGA
Privacy Commissioner

(on official leave)
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

D-S & I LAW OFFICES
Counsel for Complainants

KAB
Counsel for Respondents

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

MAG

Complainant,

-versus-

NPC 20-283

For: Violation of the Data Privacy Act of 2012

BANK OF THE PHILIPPINE ISLANDS

Respondent.

x----------x

DECISION

AGUIRRE, *D.P.C.*;

Before this Commission is a Complaint filed by MAG against the Bank of the Philippine Islands (BPI) for alleged violation of the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 06 February 2020, MAG received a call from a man claiming to be an officer of BPI.[1] She alleged that the man was looking for a "MAG."[2] MAG asked her if she was doing an online transaction with either Shopee or Lazada within the last twenty (20) minutes to which MAG immediately said no.[3] After this, he narrated that the man told her that there was an unauthorized transaction happening as they speak and that he will try to stop the purchases, but he will be needing some information and assistance from her.[4]

---

[1] Complaints-Assisted Form, 22 September 2020, Annex C, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2020).
[2] *Id.*
[3] *Id.*
[4] *Id.*

The man called again and asked for MAG's credit card details such as her credit card number, the expiry date, and the security code, which she gave, trusting that the man was an authorized BPI representative.[5] She also gave him the One Time Passwords (OTP) that she received via SMS.[6]

MAG stated that she did not realize that she was giving him approval to make online purchases.[7] Further, she alleged that the man assured her that the online purchases and credit card itself were cancelled and that a card replacement can be secured through the nearest BPI branch.[8]

After the fraudulent call, MAG immediately accessed her BPI online application and checked her available credit limit.[9] She was shocked and devastated to learn about the decrease in her available credit limit.[10] MAG stated that she knew she had no outstanding balance in that BPI credit card and the amount of her available credit limit.[11]

Realizing she was defrauded, on the same day, MAG called the BPI hotline and reported the incident.[12] She also requested that her credit card be cancelled.[13]

The BPI customer representative informed her that no transaction has been posted yet but it will be best to get in touch with the merchants, Shopee and Lazada, to cancel the unauthorized transactions.[14]

MAG also alleged that she has reached out to Shopee and Lazada's respective customer services and reported to them the fraudulent transactions.[15] They, however, could no longer cancel the transactions because the goods were already delivered.[16]

---

[5] *Id.*
[6] *Id.*
[7] Complaints-Assisted Form, 22 September 2020, at Annex C, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2020).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Complaints-Assisted Form, 22 September 2020, at Annex C, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2020).
[14] *Id.*
[15] *Id.*
[16] *Id.* Annex D-E.

The following morning, MAG visited the office of BPI Credit Card in Makati City to report the incident with the hope that the transactions can still be reversed.[17] She alleged that she was entertained by several bank officers from the BPI Fraud Division and it was Ms. LM who received her complaint. [18]

Thereafter, MAG received her BPI Statement of Account through email and the four (4) alleged unauthorized online purchases were already reflected.[19]

MAG explained that prior to the call, she inquired with BPI's Hotline and talked to a bank officer seeking assistance on how to manage her bills and for the cancellation of her expired credit card.[20] She narrated that the bank officer told her that she will be receiving a call from another bank officer in the coming days.[21] She further explained that she received a call a few days later from a BPI bank officer who explained her possible payment options.[22] MAG, however, could not decide which payment scheme to choose and told the bank officer that she would call the BPI Hotline once she has made up her mind.[23] Thus, MAG contends that when the alleged fraudster called her and identified himself as a bank officer from BPI, she thought the call was legitimate.[24]

On 22 September 2020, MAG filed a complaint against BPI before the National Privacy Commission (NPC).[25] She alleged that BPI violated Section 32 (Unauthorized Disclosure) of the DPA and prayed for the payment of damages, imposition of fines, and for BPI to write off the billed transactions on her credit card.[26]

---

[17] *Id.* Annex C.
[18] *Id.*
[19] Complaints-Assisted Form, 22 September 2020, at Annex C, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2020).
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] Complaints-Assisted Form, 22 September 2020, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2020).
[26] *Id.* at 5-6

On 07 December 2020, the NPC, through its Complaints and Investigation Division (CID), directed the parties to Confer for Discovery.[27]

On 25 December 2020 and 20 January 2021, MAG and BPI, respectively, consented to the conduct of the proceedings through e- hearing.[28]

On 18 March 2021, the CID issued an Order cancelling and resetting the discovery conference to 06 April 2021 due to the self-quarantine measures being observed by the presiding officer.[29]

On 05 April 2021, the CID issued another Order cancelling the discovery conference set on 06 April 2021 following the extension of the Enhanced Community Quarantine imposed in the National Capital Region and nearby provinces.[30]

In view of the effectivity of NPC Circular 21-01 (2021 Rules of Procedure of the NPC), the CID ordered the BPI to file its verified comment.[31]

On 12 May 2021, the parties were ordered to appear virtually before the CID for preliminary conferences on 26 May 2021 and 09 June 2021.[32]

During the 26 May 2021 preliminary conference, none of the parties appeared.[33] The CID, however, granted the request of BPI's counsel dated 24 May 2021 that the conference be reset to a later date.[34]

---

[27] Order to Confer for Discovery, 07 December 2020, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2020).
[28] Consent to E-Hearing (Complainant), 25 December 2020, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2020); Consent to E-Hearing (Respondent), 20 January 2021, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[29] Order, 18 March 2021, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[30] Order to File Verified Comment, 05 April 2021, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[31] *Id.*
[32] Order to Appear for Preliminary Conference, 12 May 2021, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[33] Order, 26 May 2021, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[34] *Id.*

On 10 June 2021, during the Preliminary Conference, MAG manifested that she is seeking the discovery of the incident report or any pertinent document relevant to the present complaint as a result of BPI's investigation after the filing of the dispute.[35] BPI, on the other hand, sought the discovery of the (1) call logs or other proofs of communication with the alleged BPI officer, (2) complaints or disputes filed with Lazada and Shopee, and (3) result, resolution or decision of the complaints or disputes filed.[36] BPI's counsel also manifested that it did not receive a copy of the Order to File Verified Comment dated 05 April 2021.[37]

Both parties also manifested their willingness to undergo mediation proceedings.[38] The parties stated that the documents that they requested from each other would be necessary and significant during the mediation proceedings.[39] Thus, the CID ordered the parties to submit the documents and to fill out their applications for Mediation.[40] BPI was also furnished a copy of the Order to File Verified Comment.[41]

On 18 June 2021, MAG and BPI signed and submitted their Applications for Mediation.[42]

On the same date, MAG submitted the requested documents after the discovery proceedings namely: (1) call logs, (2) email correspondence with Shopee, and (3) email correspondence with Lazada.[43]

On 21 June 2021, the CID issued an Order to Mediate and for the parties to appear for a preliminary mediation conference.[44]

---

[35] Order, 10 June 2021, at 1, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[36] *Id.*
[37] *Id.*
[38] *Id.* at 2.
[39] *Id.*
[40] *Id.*
[41] Order, 10 June 2021, at 1, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[42] Application for Mediation (Complainant), 13 June 2021, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021). Application for Mediation (Respondent), *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[43] Email from Complainant, 18 June 2021, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[44] Order to Mediate, 21 June 2021, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).

On 15 September 2021, BPI filed its Comment.[45]

In its Comment, BPI argued that MAG failed to substantiate her claim that she was subject of a vishing[46] attack.[47] BPI explained that MAG anchored her accusations on the alleged call she received from a person who represented himself as a "BPI agent."[48]

BPI claimed that other than her bare allegations, MAG "manifestly failed to adduce any evidence to support her claim that she indeed received a call from a fraudster."[49] BPI argued that it cannot be faulted for denying MAG's claim for reversal because BPI "has in its favor the disputable presumption that the subject transactions were fair and regular and that the ordinary course of business has been followed."[50] Further, the transactions cannot be reversed as they were properly authenticated.[51] BPI stressed that once a transaction has been authenticated, the bank immediately transmits payment to the merchant.[52] Thus, a reversal would already result in the bank's assumption of the financial obligation.[53]

BPI added that aside from the absence of any evidence to prove the alleged fraudulent call, even the identity of the alleged fraudster remained a mystery.[54] Thus, on this ground alone, the complaint merits outright dismissal under Section 12 (d) of NPC Circular 21-01 (2021 NPC Rules of Procedure).[55]

---

[45] Comment, dated 03 September 2021, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[46] Vishing or voice phishing is a fraudulent practice where verbal communication technology (e.g. VOIP or telephone) is used by an unauthorized entity pretending to be a reputable company. The aim is to manipulate individuals into revealing financial or personal information, or into providing unlawful access to their corporate networks. European Cybercrime Center, Vishing: The Voice Phishing Scam, *available at* https://www.europol.europa.eu/cms/sites/default/files/documents/vishing_final_version.pdf (last accessed 22 September 2023).
[47] Comment, dated 03 September 2021, at 5, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[48] *Id.*
[49] *Id.*at 6.
[50] *Id.*
[51] *Id.*
[52] *Id. at 7.*
[53] Comment, dated 03 September 2021, at 7, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[54] *Id.*
[55] *Id.* at 7-8.

Further, BPI stated that MAG's claim that BPI made disclosures to the alleged fraudster is based solely on surmises and conjectures.[56] BPI argued that MAG failed to adduce any evidence to show that the personal information possessed by the alleged fraudster came from BPI.[57] BPI averred that "the instant charge is based solely on the [C]omplainant's hasty conclusion that simply because she just recently communicated with BPI, any information possessed by the alleged fraudster must have come from the bank without any justification or substantiation."[58]

BPI argued that MAG's name and mobile number could have been obtained from other sources and through other illegal means, such as phishing, mail theft, social engineering, malware.[59]

In addition to these, BPI also stressed that it implements a multi-factor authentication process to verify online credit card transactions, such that online transactions can only be executed by providing certain information and performing the necessary confirmation.[60]

> It should be remembered that credit card transactions made online can only be executed if the transactions can be verified by providing the following information and performing the necessary confirmation, to wit:
>
> a. The 16 digit credit card number;
> b. The 3 digit CVC (Card Verification Code)/CVV (Card Verification Value) printed in the back of the credit card;
> c. The expiry date of the credit card; and
> d. Authentication of each transaction via a One-Time Password (OTP) sent to the credit card owner's registered mobile number. [61]

BPI stated that "unless knowingly or unknowingly disclosed by the complainant, no third party would know the complainant's credit card details, especially her 3-digit CVC."[62] Further, each online transaction

---

[56] *Id.* at 8.
[57] *Id.*
[58] *Id.*
[59] Comment, dated 03 September 2021, at 8, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[60] *Id.* at 9.
[61] *Id.*
[62] *Id.* at 10.

must be authenticated through an OTP sent to the credit card owner's
registered mobile number.[63]

BPI emphasized that in this case, it was MAG, as she herself admitted, who gave her credit card information and OTP to the alleged fraudster.[64]

Finally, BPI explained that it regularly sends advisories to its clients instructing them to safeguard their financial information.[65] These advisories contain security reminders and guidelines on the proper and responsible use of credit cards.[66]

Thus, BPI averred that it did not violate Section 32 of the DPA and prayed for the dismissal of the complaint for lack of merit.

On 20 December 2021, the Mediation Officer issued a Notice of Non- Settlement to the parties.[67] On 20 December 2021, the CID lifted the suspension of the complaint proceedings and ordered the parties to file their respective memoranda.[68]

On 17 January 2022, MAG filed her Memorandum.[69]

In her Memorandum, MAG stated that BPI, as a Personal Information Controller (PIC), has several obligations to its data subjects including implementing reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data.[70]

MAG alleged that BPI was negligent in holding and storing personal information of its data subjects because how else would the alleged fraudster know that she is a BPI credit card holder and all her other

---

[63] *Id.*
[64] *Id.*
[65] Comment, dated 03 September 2021, at 11, *in* MAG v. Bank of the Philippine Islands, NPC 20- 283 (NPC 2021).
[66] *Id.* at 8.
[67] Notice of Non-Settlement of Dispute, dated 18 August 2021, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[68] Order for Resumption of Complaints Proceedings and to Submit Memoranda, 20 December 2021,
in MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[69] Memorandum for the Complainant, 17 January 2022, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2022).
[70] *Id.* at 5

personal information.[71] She stated that there is clearly a breach of confidentiality and privacy on the part of BPI.[72] She further alleged that "all surrounding circumstances also give doubt as to the security measures practiced and applied by BPI with regard to the protection of the personal information of their Data Subjects."[73] MAG stated that when she filed a dispute with BPI, she was only "given an option on how to pay the unauthorized purchases, no more no less."[74]

Thus, according to MAG, BPI should be accountable for the negligence in holding and storing her personal information.[75] She prayed that BPI be held liable under Section 26 (b) of the DPA.[76] She further prayed for the reversal of the credit card charges, moral damages, and exemplary damages.[77]

To substantiate her allegations, she submitted the (1) printed screenshot of the call log,[78] (2) printed screenshots of the BPI OTP,[79] (3) email thread between BPI and her,[80] (4) email thread between Shopee and her,[81] (5) email thread between Lazada and her,[82] (6) BPI Statement of Account,[83] (7) BPI Cardholders' Statement of Disputed Item,[84] and
(8) NPC Complaints Assisted Form.[85]

On 27 January 2022, BPI filed its Memorandum.[86]

BPI stated that there is a "pre-existing contract between the parties whereby Complainant is extended credit through the use of her BPI

---

[71] *Id.*
[72] *Id.* at 6.
[73] *Id.*
[74] *Id.*
[75] Memorandum for the Complainant, at 6-7, 17 January 2022, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2022).
[76] *Id.*
[77] *Id.* at 6-7.
[78] *Id.* Annex A.
[79] *Id.* Annex B.
[80] *Id.* Annex C.
[81] Memorandum for the Complainant, 17 January 2022, Annex D, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2022).
[82] *Id.* Annex E.
[83] *Id.* Annex F.
[84] *Id.* Annex G.
[85] *Id.* Annex H.
[86] Memorandum for the Respondent, 27 January 2022, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2022).

Mastercard, while BPI is given the contractual right to collect and demand payment for the credit extended as they fall due."[87] Thus, BPI has the right to process the personal information of MAG to the extent necessary to fulfil the subject contract.[88]

BPI stated further that MAG, as the cardholder, consented to the processing of information necessary to the fulfilment of the relevant contracts, and to comply with relevant government regulations.[89] This was evidenced by the stipulation on terms and conditions for the use of a BPI Credit card.[90]

Further, MAG's allegation that BPI committed unauthorized processing is without any basis.[91] BPI denied any participation in the commission of the fraudulent act and stressed that it was MAG herself who disclosed the relevant OTP and other information to the alleged fraudster.[92]

BPI also reiterated its arguments in its Comment that MAG has manifestly failed to substantiate her claim that she was subject of a vishing attack and that BPI made disclosures to the alleged fraudster.[93] BPI also restated that it implements a multi-factor authentication process to verify online credit card transactions and regularly sends advisories to its clients reminding them to safeguard their financial information.[94]

To support its defenses, BPI attached the following to its Memorandum: (1) Letter dated 12 March 2020 to prove that BPI promptly responded to MAG's complaint,[95] (2) Advisories made by BPI through various means of communication,[96] and (3) BPI Credit Card Terms and Conditions.[97]

---

[87] *Id.* at 3.
[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] Memorandum for the Respondent, 27 January 2022, at 4, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2022).
[93] *Id.* at 7-11.
[94] *Id.* at 11-13.
[95] *Id.* Exhibit 1.
[96] *Id.* Exhibit 2.
[97] *Id.* Exhibit 3.

Issue

Whether there is substantial evidence to find BPI liable for a violation of Section 26 (Accessing Due to Negligence) and Section 32 (Unauthorized Disclosure) of the DPA.

Discussion

The Commission dismisses the case for lack of substantial evidence.

BPI cannot be held liable for a violation of the DPA based on the allegations of and evidence submitted by MAG.

In her Memorandum, MAG claims that the alleged fraudster gained access to her personal information because BPI was negligent in holding and storing her personal information.[98] To substantiate her complaint, she submitted the printed screenshot of the call log,[99] printed screenshots of the BPI OTP,[100] an email thread between BPI and her,[101] an email thread between Shopee and her,[102] an email thread between Lazada and her,[103] her BPI Statement of Account,[104] and the BPI Cardholders' Statement of Disputed Item.[105] She also attached a Certification of Authenticity stating that the evidence submitted consists of screenshots and photo reproductions of the original non- documentary evidence.[106]

In this case, MAG, as the complainant, had the burden of proof in alleging a violation of the DPA. She, however, did not discharge this as she failed to support her allegations with substantial evidence.

---

[98] Memorandum for the Complainant, 17 January 2022, at 5, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2022).
[99] *Id.* Annex A.
[100] *Id.* Annex B.
[101] *Id.* Annex C.
[102] *Id.* Annex D.
[103] *Id.* Annex E.
[104] Memorandum for the Complainant, 17 January 2022, Annex F, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2022).
[105] *Id.* Annex G.
[106] *Id.* at 10.

Section 1 of Rule 131 of the 2019 Amendments to the Revised Rules on Evidence provides:

> Section 1. *Burden of proof and burden of evidence.* **Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim** or defense by the amount of evidence required by law. Burden of proof never shifts.
>
> Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a prima facie case. Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case.[107]

Section 6 of Rule 133 of the 2019 Amendments to the Revised Rules on Evidence provides:

> Section 6. *Substantial Evidence*. In cases filed before administrative or quasi-judicial bodies, a fact may be deemed established if it is supported by substantial evidence, or that amount of relevant evidence which a reasonable mind might accept as adequate to justify a conclusion.[108]

In *BSA Tower Condominium Corporation v. Reyes,*[109] the Supreme Court held that:

> The basic rule is that mere allegation is not evidence and is not equivalent to proof. Likewise, charges based on mere suspicion and speculation cannot be given credence. [110]

Based on MAG's narration, the alleged fraudster knew only of her full name and mobile number.[111] As correctly stated by BPI, the alleged fraudster, however, could have obtained such information from other sources and through other illegal means.[112] There was no evidence to show that the information came from BPI. Further, while MAG submitted a Certification of Authenticity with her evidence, this does

---

[107] 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. No. 19-08-15-SC, Rule 131, § 1 (01 May 2020). Emphasis supplied.
[108] *Id.* Rule 133, § 6.
[109] BSA Tower Condominium Corp. v. Reyes II, A.C. No. 11944 (2018).
[110] *Id.*
[111] Complaints-Assisted Form, 22 September 2020, at Annex C, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2020).
[112] Comment, dated 03 September 2021, at 8, *in* MAGv. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).

not create a connection between the fraudulent activity and BPI's
alleged involvement.

As admitted in her complaint, MAG's own actions directly resulted in the disputed transactions.[113] The fact that the alleged fraudster knew her personal information does not automatically mean that there was a breach or negligence on the part of BPI.

Based on MAG's assertions, it cannot be said that BPI was remiss in its obligation to implement security measures under the DPA. As explained in BPI's Comment and Memorandum, BPI implements a multi-factor authentication process to verify online credit card transactions, such that online transactions can only be executed by providing certain information and performing the necessary confirmation.[114] To reiterate, it was MAG herself who disclosed her credit card information and OTP to the alleged fraudster.[115]

The Commission reminds data subjects that they should endeavor to protect their personal data, including bank account numbers, log-in credentials, credit card details, and OTPs sent through email links, text messages, or phone calls, to avoid possible risk or harm. As the Commission has previously held, the security of personal information is a joint obligation of both the data subjects and the data controller or processor.[116] The implementation of reasonable security measures does not mean that the measure is foolproof and immune from any contributory negligence on the part of the data subject.[117]

In sum, MAG's admissions and the lack of substantial evidence to support her allegations cannot give rise to the conclusion that BPI failed to implement security measures and that this supposed failure resulted in the unauthorized transactions.

---

[113] Complaints-Assisted Form, 22 September 2020, at Annex C, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2020).
[114] Comment, dated 03 September 2021, at 9, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2021).
[115] Complaints-Assisted Form, 22 September 2020, at Annex C, *in* MAG v. Bank of the Philippine Islands, NPC 20-283 (NPC 2020).
[116] EDF v. BPI, NPC 21-016, 17 Match 2022, at 10, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-21-016-2022.03.17-EDF-v.-BPI-Decision-1.pdf (last accessed on 21 September 2023).
[117] *Id.*

Given the foregoing, the Commission cannot find BPI liable for violating Section 26 (Accessing Due to Negligence) and Section 32 (Unauthorized Disclosure) of the DPA.

As to MAG's prayer on the reversal of the unauthorized transactions, such is beyond the jurisdiction of the Commission,

WHEREFORE, premises considered, this Commission resolves that the case filed by MAG against Bank of the Philippine Islands is **DISMISSED** for lack of substantial evidence.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases before any other forum or tribunal, if any.

SO ORDERED.

City of Pasay, Philippines.
17 August 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

MAG
Complainant

BANK OF THE PHILIPPINE ISLANDS BPI
LEGAL AFFAIRS AND DISPUTE
RESOLUTION DIVISION
Attn: CDP
and BDN
Respondent

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

FGP,

Complainant,

-versus-

NPC Case No. 18-038
(formerly CID Case No. 18-E-038) *For: Violation of the Data Privacy Act of 2012*

MAERSK GLOBAL SERVICE CENTRES, PHILIPPINES, LTD.

Respondent.

x----------x

DECISION

***AGUIRRE*, D.P.C.:**

Before this Commission is a complaint for a violation of the data subject's rights to access and rectification.

Complainant FGP was an employee of Respondent Maersk Global Service Centres, Philippines, Ltd. from 29 March 2010 to 30 April 2014. As a requirement of Complainant's current employer, Reed Elseview Shared Services, Inc. (RESSPI), he consented to a background check to be done by Human Capital Asia, Inc. This background check involves, among others, verification of his records from his previous employments.

On 8 March 2018, Complainant was informed by the Human Resources representative of RESSPI that they received a report from Human Capital Asia, Inc. The report indicated that an e-mail was sent to Respondent to verify employment details, and Respondent claimed that they had no records with Complaimant's name in their HR database. [1]

On 13 March 2018, Complainant sent an e-mail to Respondent to confirm the fact that Human Capital Asia, Inc. contacted them as well

---

[1] Records, pp. 50-69.

as the contents of the report. Respondent replied on 19 March 2018 and confirmed the same.

On 20 March 2018, Complainant sent another e-mail to Respondent and attached proof of his past employment with them, such as his Employee IDs, certificate of employment, and Bureau of Internal Revenue (BIR) 2316 forms for his years of employment with them.[2]

Complainant stated that he demanded for the following from Respondent, via e-mail:

a. An explanation as to why they have no records with my name in their database despite the fact that I was indeed their former employee;
b. That they inform the Background Investigator that I was their former employee;
c. That they provide me two certificates of employment;
d. That they provide me the name and designation of their Personal Information Controller.[3]

Complainant did not receive any feedback or reply from Respondent despite his follow-up e-mails on 22 and 27 March 2018,[4] prompting him to file this complaint with the National Privacy Commission (NPC) for Respondent's violation of his rights as a Data Subject, particularly his Right to Access, Right to Rectification, and, if appropriate, the Right to Damages.[5]

The parties were ordered to appear for Discovery Conference on 18 July 2018.[6] Complainant and Respondent, through counsel, appeared. Both parties manifested that they were willing to enter into an amicable settlement. They were given fifteen (15) days from 18 July, or until 02 August 2018, to file their Compromise Agreement. Respondent was given ten (10) days from then or until 12 August 2018 to file their Responsive Comment in case the parties fail to reach a settlement. Complainant will then have ten (10) days from receipt to file his Reply.[7]

Complainant, however, sent an e-mail to the investigating officer on 06 August 2018, stating that he decided not to enter into an amicable

---

[2] *Ibid.*
[3] *Ibid.*
[4] *Id.*, at 67-69.
[5] *Supra at* Note 1.
[6] Records at pp. 94-95.
[7] *Id.*, at 49.

settlement with Respondent. He also informed the investigating officer that he would like to proceed with the complaint.[8]

After two (2) motions for extension of time to file its Responsive Comment, Respondent submitted its Comment on 07 September 2018.

Arguments of the Parties

In their Comment, Respondent asserts that the Complaint should be dismissed on the ground of Complainant's failure to file the same within the proper reglementary period, citing NPC Circular No. 16-04 or the NPC Rules of Procedure ("Rules"):

> Section 4. Exhaustion of remedies. No complaint shall be entertained unless:
>
> xxx
>
> c. The complaint is filed within six (6) months from the occurrence of the claimed privacy violation or personal data breach, or thirty (30) days from the last communiqué with the personal information controller or concerned entity, whichever is earlier.[9]

Respondent points out that Complainant's last communication with them was through an e-mail on 27 March 2018 and that records of this case readily show that Complainant only filed his complaint on 24 May 2018. They state:

> 7. Thus, Complainant filed the instant Complaint 58 days- already more than 30 days – after his last communication with Respondent Maersk. Clearly, Complainant was in violation of Section 4(c) of Rule II of the NPC Rules and his Complaint should not be entertained by this Honorable Office.
>
> xxx
>
> 9. Notably, this Honorable Office may waive this requirement for the filing period of the Complaint, but ONLY IF:
>
> (1) Good cause is shown by the complainant; or
> (2) The complaint involves a serious violation of the Data Privacy Act.
>
> In either instance, this Honorable office must take into account "the risk of harm to the affected data subject."

---

[8] Id., at 44.
[9] Section 4, Rule II, NPC Circular 16-04. Dated 15 December 2016.

> 10. None of these exceptions are present in the case at bar.
>
> 11. Complainant failed to allege, let alone show, any good cause why his Complaint should be considered by this Honorable Office, notwithstanding his belated filing thereof.
>
> xxx
>
> 13. In any event, it must be taken into account that the risk of harm to the Complainant is minimal, if none at all.
>
> 13.1 Complainant admits that he is presently employed by Reed Elsevier Shared Services (Philippines), Inc. ("Reed"), the company who requested for a background check of his past employment with Respondent Maersk.[10]

Respondent also disputes Complainant's Right to Damages by stating:

> 13.2. Signficantly, Complainant admits that there are no damages to him arising from Respondent Maersk's alleged violation of the Data Privacy Act. While he states that he will claim damages if any are found after the filing of his Complaint, the fact that he has been unable to identify any damages to him strongly shows that there (sic) the risk of harm to him is minimal, if none at all.
>
> 13.3. Lastly, it is respectfully manifested that Respondent Maersk had already confirmed with Reed the Complainant's past employment. Respondent Maerks had even verified as correct all the employment details declared by the Complainant. This may explain why he had been employed by Reed.

In Complainant's Reply, he argues that the lapse of the thirty (30)-day reglementary period should not be a cause for the dismissal of his complaint :

> 4. On 24 April, the Complainant attempted to send the complaint to this Honorable Office using the Complaints-assisted Online Form provided in the official website of the Commission;
>
> xxx
>
> 6. Due to this technical issue, the Complainant has resorted to producing and sending to this Honorable Office, via e-mail, a sworn and duly notarized Complaint-Affidavit, which took

---

[10] *Id.*, 30-34.

> additional time and effort, as compared to simply sending the complaint in the Online Form.
>
> xxx
>
> 8. Based on the facts presented,
>
> a. The online complaint form is a valid means to send a complaint to The Commission, and
>
> b. Had there been no technical issue, the complaint would have been filed the latest on 24 April 2018, which is 28 days after my last communication with the Respondent. [11]

Complainant also addresses the issue of damages that may be awarded to him, stating:

> 11. While the Complainant continues to confirm that there are no known damages resulting from Respondent's violation of the Complainant's rights as a data subject at the date of the submission of his Reply, the same Act does not require damages or harm on a data subject for the rights of the data subject to be violated.
>
> xxx
>
> 12. Without even any damage or harm resulting from the Respondent's violations of the rights of the Complainant, the evidences presented on (sic) the Complaint already established that the Complaint is valid under the following criteria as per Section 3 of the same act:
>
> a. That the Complainant is a data subject of the Respondent, and
>
> b. The Respondent commited violations of the Complainant's rights as the Respondent's data subject.
>
> xxx
>
> 21. Had the Complainant fail (sic) to keep any documents as proof of his employment with the Respondent, the employment of the Complainant may have been terminated, as per company policy, resulting from his failure to prove his employment with Respondent.[12]

---

[11] *Id.*, 14-26.
[12] *Ibid.*

Issues

1. Whether the Complaint may be dismissed for being filed beyond the thirty (30)-day period as provided under Section 4(c) of the NPC Rules of Procedure.
2. Whether Respondent committed acts in violation of Complainant's rights to access and rectification under the Data Privacy Act (DPA).

Discussion

The Complaint should not be dismissed.

The Rules provide that no complaint shall be entertained unless it is filed within six (6) months from the occurrence of the claimed privacy violation or personal data breach, or thirty (30) days from the last communication with the personal information controller or concerned entity, whichever is earlier.[13]

This rule was intended to prevent a deluge of vexatious complaints from those who waited for a long period of time to pass before deciding to lodge a complaint with the NPC, unduly clogging its dockets. Notably, however, the same Section provides that the Commission has the discretion to waive such period for filing upon good cause shown, or if the complaint involves a serious violation or breach of the DPA, taking into account the risk of harm to Complainant.

The Supreme Court also provides the following:

> The Court has allowed some meritorious cases to proceed despite inherent procedural defects and lapses. This is in keeping with the principle that rules of procedure are mere tools designed to facilitate the attainment of justice and that strict and rigid application of rules which would result in technicalities that tend to frustrate rather than promote substantial justice must always be avoided. It is a far better and more prudent cause of action for the court to excuse a technical lapse and afford the parties a review of the case to attain the ends of justice, rather than dispose of the case on technicality and cause grave injustice to the parties, giving a false impression of speedy disposal of cases while actually resulting in more delay, if not a miscarriage of justice.[14]

---

[13] Section 4, NPC Circular 16-04. Dated 15 December 2016.
[14] PNB v. Court of Appeals, G.R. No. 218901, 15 February 2017.

In this case, the allegations and evidence presented by the Complainant sufficiently warrants the waiver of the thirty (30)-day requirement from the last communication with the personal information controller within which to file the complaint. The Commission is convinced that the case involves a possible serious violation of the data subject's rights to access and rectification.

The Rules speak of "risk of harm" and do not require an actual harm or damage to Complainant. As pointed out by Complainant, his lack of employment record could have resulted in his inability to provide previous work experience, which could have jeopardized his current employment. The fact that Complainant was able to keep and provide other proof of employment, such as his company IDs, BIR forms, and past certificates of employment, is extraneous to this case and speaks more to the diligence of Complainant rather than the absence of any risk of harm caused by the actions of Respondent. Respondent's continuing inaccurate record may cause further repurcussions in the future, should Complainant seek employment elsewhere.

Hence, contrary to what Respondent alleges, the violation of Complainant's rights was not "minimal" such that the Commission's discretion to waive the period requirement should be curtailed.

Respondent committed acts in violation of Complainant's right to access under the DPA.

The DPA provides that every data subject has the right to reasonable access, upon demand, of his or her personal data and certain information about the processing, which the controllers must provide.[15] This includes the following information:

> (1) Contents of his or her personal information that were processed;
> (2) Sources from which personal information were obtained;
> (3) Names and addresses of recipients of the personal information;
> (4) Manner by which such data were processed;
> (5) Reasons for the disclosure of the personal information to recipients;

[15] See R.A. 10173, Section 16(c).

> (6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
> (7) Date when his or her personal information concerning the data subject were last accessed and modified; and
> (8) The designation, or name or identity and address of the personal information controller;[16]

In his e-mail dated 20 March 2018,[17] Complainant requested information regarding the fact of his employment with Respondent, specifically the following:

1. An explanation as to why they have no records of his employment, whereas in fact [he] was indeed a former employee of Maersk Global Service Centres, Philippines Ltd.
2. Two (2) Certificates of Employment; and
3. The name and designation of their Personal Information Controller.

Despite follow-up e-mails by Complainant, Respondent failed to provide the requested information. While Respondent sent correspondence to Human Capital Asia, Inc. belatedly on 18 April 2018 to clarify Complainant's employment information, Respondent has not responded to the request of Complainant as of the time the instant Complaint was filed on 27 March 2018.

Respondent did not violate Complainant's right to rectification.

The DPA likewise provides that every data subject has the right to rectification, defined as their right to:

> Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: *Provided,* That the third parties who have previously received such processed personal information shall he

[16] *Ibid.*
[17] Records, p. 67.

> informed of its inaccuracy and its rectification upon reasonable request of the data subject.[18]

While the provision states that the information must be corrected "immediately and accordingly," the Commission looks at the circumstances surrounding the request. This may include, among others, the volume of information involved and the time that has lapsed since the time the information was processed. Hence, there is no uniform timeframe for all the personal information controllers to comply with the obligation to correct inaccurate information,[19] as long as there is no undue or excessive delay.[20]

The records of this case show that Complainant was informed on 08 March 2018 that Respondent did not have his employment information in their HR database. Respondent confirmed this to Complainant on 19 March 2018. After Complainant's request on 20 March 2018 for Respondent to inform Human Capital Asia, Inc. of the correct information regarding his previous employment, Respondent rectified the matter with Human Capital Asia, Inc. through an e-mail sent on 18 April 2018.

The Commission finds that the e-mail to Human Capital Asia, Inc. twenty nine (29) days after receiving Complainant's request is considered reasonable under the circumstances and complies with the requirement that "the third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon reasonable request of the data subject."

Complainant is entitled to damages.

The DPA provides that every data subject has the right to be indemnified for "any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information."[21] Indeed, it is part of the Commission's mandate to award indemnity on matters affecting any personal information.[22]

Despite Respondent's verification of Complainant's records with Human Capital Asia, Inc., the fact remains that Respondent stored and disclosed inaccurate information about Complainant. This is contrary

---

[18] R.A. 10173, Section 16(d).
[19] NPC Advisory Opinion 2018-018. Dated 21 April 2017.
[20] *See,* EU General Data Protection Regulation, Article 16.
[21] R.A. 10173, Section 16(f).
[22] R.A. 10173, Sec. 7(b).

to Respondent's obligations to observe the general data privacy principles under the DPA, which require that personal information must be, among others:

> (c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date xxx [23]

Respondent's failure to provide the requested information to Complainant[24] also indicates a lack of mechanism for data subjects to exercise their right to access under the DPA.[25]

Contrary to Respondent's assertion that the risk of harm is "minimal, if none at all," Complainant faced a real risk of negative consequences from an inconsistency between his declared information and the background check. It is worth noting that the DPA does not require actual or monetary damages for data subjects to exercise the right to damages. As provided in the law, the consequences of processing inaccurate information is enough for the right to arise.[26]

The DPA provides that restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.[27] The relevant provision in this Code states:

> Art. 2221. Nominal damages are adjudicated in order that a right of the plaintiff, which has been violated or invaded by the defendant, may be vindicated or recognized, and not for the purpose of indemnifying the plaintiff for any loss suffered by him.

The DPA gives individuals the right to receive indemnfication from personal information controllers and personal information processors for both material and non-material damages.[28] The Supreme Court has also clarified that no actual present loss is required to warrant the award of nominal damages, thus:

> Nominal damages are recoverable where a legal right is technically violated and must be vindicated against an invasion that has produced no actual present loss of any kind or where there has been a breach of contract and no

---

[23] *Id*, at Sec. 11(c).
[24] *Supra* at Note 17.
[25] *Supra* at Note 16.
[26] *Supra* at Note 21.
[27] R.A. 10173, Sec. 37.
[28] *See,* Handbook on European Data Protection Law, p. 246.

> substantial injury or actual damages whatsoever have been or can be shown.[29]

Pursuant to the New Civil Code and the aforementioned findings of a failure to process personal information that is accurate, relevant and up to date,[30] as well as a failure to provide a mechanism for data subjects to access their personal information upon reasonable request,[31] the Commission finds that the award of nominal damages to Complainant is warranted.

WHEREFORE, all these premises considered, this Commission resolves to **AWARD** Complainant FGP damages in the amount of P5,000.00 for Respondent Maersk Global Service Centres, Philippines, Ltd.'s violation of his right to access. Respondent is hereby **ORDERED** to submit its compliance within fifteen (15) days from receipt of this Decision.

SO ORDERED.

Pasay City, 21 May 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

---

[29] Seven Brothers Shipping Corporation v. DMC-Construction Resources, Inc. G.R. No. 193914. November 26 2014.
[30] *Supra* at Note 23.
[31] *Supra* at Note 25.

COPY FURNISHED:

FGP
Complainant

ROMULO MABANTA BUENAVENTURA SAYOC & DELOS ANGELES
Counsel for Respondent Maersk

COMPLAINTS AND INVESTIGATION DIVISION
GENERAL RECORDS UNIT
ENFORCEMENT DIVISION
National Privacy Commission

JCR
Complainant,

-versus-

NPC Case No. 17 - K - 001
For: Violation of the provisions of the Data Privacy Act of 2012

GLOBE TELECOM, INC.
Respondent.
x----------x

DECISION

AGUIRRE, *D.P.C.:*

Before this Commission is a Complaint filed by Complainant JCR against Respondent Globe Telecom, Inc. for supposed violations of
R.A. 10173 ("Data Privacy Act").

The Facts

The facts of this case are not disputed.

On 03 November 2017, Complainant accidentally left her phone containing her Globe Subscriber Identity Module ("SIM") card in a taxi on her way to Makati. Her mobile number with Respondent served as her principal means of communication since its issuance. The next day, she went to Respondent's store in Greenbelt 3, Makati to request the deactivation of her lost SIM card and the issuance of a new SIM card with the same mobile number. An employee of Respondent named MCK assisted Complainant. She was given a blank inactive SIM card but they were unable to process the request. Complainant left her sister's mobile number so Respondent can communicate any development regarding her request.

After a couple of days, Complainant went home to Bacolod City without knowing whether her lost SIM card could be replaced or not. On 06 November 2017, MCK called Complainant's sister informing her that there was still no resolution regarding her request because

Respondent was still fixing the issue with her lost SIM card. Complainant went to the Respondent's store in SM Bacolod to check if her request was addressed. No update was given to her even after calling the hotline of Respondent.

On 10 November 2017, Complainant came back to the same store in SM Bacolod. The employee attending her request told her that the pendency of an incomplete/unspecific previous cancellation request on her account prevented any subsequent transaction on her account from pushing through. She was told to keep the blank SIM card she previously received and try to call the hotline to have it activated instead. On 11 November 2017, Complainant called Respondent's hotline. The agent who answered her said that Respondent's store in SM Bacolod could do nothing unless she returns to the Respondent's store in Greenbelt 3.

Thereafter, Complainant's sister went to Respondent's store in Greenbelt 3, but MCK was on leave and none of the agents could help her. Complainant then called to inquire how she can file a complaint and was referred to the supervisor. After waiting for more than twenty minutes over the phone, Complainant was told that her problem had been fixed and that she just needed to go back to the Respondent's store in SM Bacolod and look for the branch manager or assistant manager so she can get her SIM card replaced. On the same day, Complainant went back only to find that the personnel she was asked to look for were both not on duty on that day. The officer in charge asked for another 24 to 48 hours to once again try to address her concern.

After two weeks, Complainant inquired again about the status of her cancellation request because she did not receive any feedback for almost a week. However, there was still no resolution to her concern.

Arguments of the Parties

On 20 November 2017, Complainant filed her Complaint-Affidavit of even date before this Commission. According to her, she was worried about the integrity of her data and privacy because her primary means of communication and the repository of her personal data for six (6) years is now left uncertain in the hands of a stranger.

Complainant alleges that "the inability of Globe to deactivate my lost Globe SIM, re-issue the same and restore my possession of my Globe

number that belonged to me for the past six (6) years, qualify as a breach of its obligations under Republic Act No. 10173 or the Data Privacy Act of 2012 and its Implementing Rules and Regulations."[1]

Complainant further alleges that Respondent violated Sections 25 and 28(d) of the Implementing Rules and Regulations ("IRR") of the Data Privacy Act of 2012 for failure to implement reasonable and appropriate security measures to protect the availability, integrity and confidentiality of her personal data.

For their part, Respondent argues in their Comment[2] dated 28 August 2018 that there are no violations of the Data Privacy Act alleged in the Complaint. According to Respondent, the facts in the complaint discussed matters relating to a SIM replacement issue and/or customer service issue which was resolved when the replacement SIM card was issued to Complainant on 21 March 2018. As such, these are beyond the jurisdiction of this Commission.

Respondent also contends that there was no allegation that Respondent disclosed or caused the disclosure of Complainant's personal information. There is neither a privacy violation nor a personal data breach involved. Respondent argues that Complainant failed to state the alleged compromised or breached personal data. It explained that a SIM card does not store information or data. It is only a microchip inserted in a mobile phone that connects to a particular cellular network. It is the phone, not the SIM card, that stores information or data. The access to the data in the lost mobile phone may be gained with or without the SIM card except if the phone is protected or encrypted.

In addition, Respondent argues that the proximate cause of the alleged breach of complainant's data privacy, if any, was her own negligence when she lost her mobile phone with the SIM card in a cab. They contend that it is physically impossible for Respondent to protect and control the data or information that their data subjects store in their mobile devices. It is also impossible for Respondent to prevent the unauthorized disclosure of the data stored in one's device when the owner himself did not put the necessary measures to protect the data or information stored in it. Respondent explained that the personal data of subscribers stored in their devices and/or SIM card, if applicable, are physically and legally beyond the protection required by law from PICs and/or PIPs. It is the duty of the complainant, as a

---

[1] *Records*, p. 5.
[2] *Ibid.* at pp. 29-38.

reasonable and diligent owner, to protect the contents of her mobile. Respondent cannot be liable for any unauthorized disclosure of information stored in complainant's device because it is physically and legally beyond the protection of Respondent.

Respondent stated that as personal information controller ("PIC") and personal information processor ("PIP"), it is only required to protect the collected personal information in its possession and not the personal information of the subscribers contained in the devices and SIMs that are in the actual possession of its subscribers.

Respondent alleges that it has complied with the requirements under the Data Privacy Act, as well as its IRR. Respondent implements reasonable and appropriate organizational, physical and technical security measures for the protection of personal data. Respondent, as required by law, implements security measure for the protection of all the collected personal information stored in its designated data centers from any form of natural or human dangers.

Issue

The issue to be resolved in this case is whether Respondent violated Sections 25 and 28(d) of the IRR of the Data Privacy Act for its delayed action on Complainant's request to deactivate her lost SIM Card and issue another one with the same number.

Discussion

At the outset it should be stressed that there is no question that complainant's own negligence in leaving her mobile phone in the taxi was the proximate cause of her personal data being exposed to risks arising from possible unauthorized access and disclosure.

Respondent is therefore justified when it stated in its Comment that:

> Inasmuch as it is physically impossible for Globe, or this Honorable Commission despite repeated information campaign and reminder how to protect a person's personal information, to control the data or information that a subscriber stored in his mobile device, it is likewise to [sic] physically impossible for Globe, much less the Honorable Commission, to protect and/or prevent the unauthorized disclosure of data/information stored in such mobile device when owner thereof himself has not put the necessary measures to protect such data/information himself.[3]

---

[3] *Ibid* at p. 35.

Nevertheless, it is apparent that Respondent is only concerned with the personal data of Complainant stored in her mobile phone. As it explained in its Comment:

> ... Respondent could only surmise that the "data" that she seeks to protect, which she claims to be in "the hands of a stranger whose intentions are demonstratively tainted" – refers to the data that are stored in her lost mobile phone – NOT in the Respondent SIM card. A SIM card is a microchip inserted in a mobile phone that connects it to a particular phone network – in this case to Globe's network. Clearly, a SIM it [sic] is not meant to be used to store information or data...[4]

In focusing only on the personal data stored in the mobile phone and characterizing the incident as a simple SIM card replacement and customer issue, Respondent ignores the very nature of Complainant's requests regarding the deactivation and reissuance of her SIM card and failed to take the necessary steps to protect the information stored in the SIM card that is associated with and used for the identification of the Complainant.

The United States of America's National Institute of Standards and Technology ("NIST") defined SIM cards as a removable smart card that "uniquely identifies the subscriber, determines the phone's number, and contains the algorithms needed to authenticate a subscriber to a network."[5]

While the SIM card itself does not contain the subscriber's mobile number, it contains, among others, the international mobile subscriber identity ("IMSI") number and integrated circuit card identifier ("ICCID")[6] that are used to uniquely identify the subscriber in the system of Respondent once it is activated. This allows that person to make and receive calls, send and receive SMS, use mobile data, and otherwise access and use the allocations of their account. Given this, in the same manner that a mobile number is considered personal information since it allows telecommunications companies such as Respondent to identify their subscribers, Complainant's activated SIM is also considered to contain personal information as far

---

[4] *Ibid.* at p. 32.
[5] Rick Ayers, et al., Cellphone Forensic Tools: An Overview and Analysis Update, NISTR 7387, United States of America National Institute of Standards and Technology, *available at* https://doi.org/10.6028/NIST.IR.7387, retrieved on 09 December 2019.
[6] *See* 3rd Generation Partnership Project: Technical Specification Group Terminals Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) Interface, 3GPP TS 11.11 v8.14.0 (2007-06) *available at* https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=419, retrieved on 09 December 2019.

as Respondent is considered and should therefore be protected in the same manner.

In its Comment, Respondent asserted that "the PIC and PIP could only implement reasonable and appropriate organizational, physical, procedural and technical security measures for the protection of personal data collected, and those that are within its control."[7] In this case, the deactivation of Complainant's SIM card to prevent further use and access by unauthorized persons is clearly within the control of Respondent especially since the matter had already been brought to its attention by Complainant several times.

Although the Complaint does not contain specific allegations relating to the misuse of Complainant's account, considering that the accidental loss of SIM cards is not an entirely uncommon occurrence, Respondent should have implemented the necessary mechanisms that will allow its data subjects, such as the complainant herein, to mitigate the potential damage resulting from their sim card being used by an unauthorized person.[8] This is all the more important given the risks that may result from a lost SIM card, ranging from unauthorized calls and texts being charged to the account of the subscriber to using the two-factor authentication codes sent to the mobile number, effectively allowing access the subscriber's accounts from social network accounts, bank accounts, and the like.

The fact that the proximate cause of these potential risks is the negligence of the complainant does not relieve Respondent of this obligation. After having been informed of the loss of Complainant's SIM card by complainant, the process for the deactivation of the SIM card was already entirely within the control of Respondent. Despite the diligent efforts Complainant took in following up her requests, her SIM card was only replaced on 21 March 2018 or more than four and a half months since the incident was first brought to the attention of Respondent on 04 November 2017.

While the records do not show the exact date when Complainant's old SIM card was deactivated, given the abovementioned risks, Respondent's inaction during the more than two weeks before the Complaint was filed is already too long. Respondent is reminded of its obligation to adopt and establish security measures that will allow it

---

[7] *Records*, p. 35.
[8] *See* Data Privacy Act, Sec. 20 (c)(3).

to "[take] preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach."[9]

For the reasons stated above, the Commission cannot agree with the Respondent that the issues raised regarding SIM card deactivation and replacement are merely in the nature of customer service.

Compliance with the Data Privacy Act entails more than simply ticking off boxes on a checklist such as the registration of a Data Protection Officer, conduct of a privacy impact assessment, creation of a data protection policy, or the exercise of breach reporting procedures. Companies must realize that compliance with the Data Privacy Act involves doing such activities within a framework of protecting the data subjects from very real risks, such as what Complainant faced in this case.

WHEREFORE, all the premises considered, the Commission finds no violation of the Data Privacy Act on the part of Respondent Globe Telecom, Inc. that is sufficient to warrant a recommendation for criminal prosecution. This Commission finds, however, that Respondent failed to adopt and implement the necessary policies and procedure relating to the prevention, correction, and mitigation against security incidents that can lead to a personal data breach.

The Commission hereby **ORDERS** Respondent Globe Telecom to submit a complete report on the measures it has undertaken or will undertake to address the issue of delayed SIM deactivation such as in this case, including the timeline for the implementation of such measures, within thirty (30) days from receipt of this Decision. Reference may be made to the requirements provided in the Implementing Rules and Regulations of the Data Privacy Act, particularly Section 28, paragraphs (c), (d), (e), and (f).

SO ORDERED.

Pasay City, 5 December 2019.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

---

[9] Implementing Rules and Regulations of DPA, Sec. 28 (d).

Concurring:

Sgd.
IVY D. PATDU
Deputy Privacy Commissioner

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

COPY FURNISHED

JCR

CASTELO UNGOS CASIÑO & TUBAYAN
Counsel for Respondent Globe Telecom, Inc.

ENFORCEMENT DIVISION GENERAL
RECORDS UNIT
National Privacy Commission

RBB

Complainant,

-versus-

NPC Case No. 19-531
(Formerly CID Case No. 19-G 531)
For: Violation of the Data Privacy Act of 2012

U-PESO.PH LENDING CORPORATION (UPESO)

Respondent.

x----------x

AGUIRRE, *D.P.C.:*

Before this Commission is a Complaint filed by the complainant RBB against the respondent U-PESO.PH Lending Corporation (UPESO) for an alleged violation of R.A. 10173 ("Data Privacy Act").

DECISION

The Facts

In her Complaint, the Complainant alleges that she has an outstanding loan with Respondent. Upon her default of payment, Respondent allegedly threatened to file a case of *estafa* against her. Complainant claims that she tried to communicate with Respondent regarding her situation, but the threats from Respondent continued.[1]

The parties were ordered to appear on 28 August 2019 for a Discovery Conference.[2] On the scheduled conference, however, only Respondent appeared. The Conference was reset to 17 October 2019 where only Respondent appeared and Complainant again failed to appear. Respondent was thus ordered to submit their responsive comment.[3]

---

[1] Complaints-Assisted Form dated 25 July 2019, p. 19.
[2] Order to Confer for Discovery dated 25 July 2019.
[3] Order dated 17 October 2019.

Arguments of the Parties

In her Complaint, Complainant alleges that these threats caused her sleepless nights, loss of appetite, and anxiety to the point of considering taking her own life.

In their Comment,[4] Respondent confirmed that Complainant is a borrower through their UPESO lending application. Complainant had previously settled four (4) loan obligations, and obtained her fifth loan with Respondent for P12,000.00 due on 18 June 2019. This due date was not met by Complainant. Respondent claims that, after several follow- ups, they could no longer contact Complainant.

In their Comment, Respondent argues:

> As for the allegations that the Complainant was being harassed or threatened by UPESO or its collecting agents when she failed to pay her obligations, [s]uch matters are civil in nature and are outside the jurisdiction of this Honorable Commission and must be conducted in proper courts.
>
> xxx
>
> The complainant only made allegations of harassment and threats because of her continued failure to settle her obligation and no proof as to the alleged harassment or threats made by the others were presented.

Issue

The sole issue here is whether Respondent committed a violation of the Data Privacy Act that warrants a recommendation for prosecution.

Discussion

It is important to note that Complainant states in her Complaints- Assisted Form that she learned about this incident by "receiving it in her own number."[5] As her Complaint excludes the issue of disclosure

---

[4] Comment dated 25 October 2019.
[5] Complaints-Assisted Form dated 25 July 2019, p.5.

of her personal information to third parties, and there are no other allegations on other uses of Complainant's information, we focus our discussion on Respondent's use of Complainant's information for purposes of collecting the amount she loaned.

The processing of personal information by Respondent, which resulted in communicating with Complainant through her mobile number, may be considered as "necessary for compliance with a legal obligation to which the personal information controller is subject" under Section 12 of the Data Privacy Act. In this case, Complainant admitted that she entered into a Contract of Loan with Respondent. This Contract created a legal obligation on the part of Complainant to pay her loan upon due date. Consequently, Respondent is permitted under Section 12 of the DPA to process Complainant's data to ensure the latter's compliance with her legal obligations.

It is thus valid for Respondent to communicate with Complainant through her mobile number which she provided.

As to Complainant's allegations of threats by Respondent to file a case of *estafa*, it must be emphasized that the Commission is not the competent authority to determine the allowable practices in debt collection.

Hence, there is nothing in the Complaint that would reasonably connect Respondent to any of the possible violations enumerated under the Data Privacy Act. Neither did Complainant provide supporting documents to her allegations. Notably, she failed to appear at the two (2) Discovery Conferences, where the second one was rescheduled because of her absence at the first.

Nevertheless, the Commission notes several problematic provisions in the Loan Agreement cited by Respondent in their Comment, such as:

> 14. Data Privacy. The Borrow hereby acknowledges, agrees, and consents that the Lender or its authorized officer's may collect, store, process and dispose data about the Borrower. **Any information and data received from the Borrower by the Lender may be used and utilized by the Lender, either directly or indirectly in the performance of the terms of this Agreement.**[6]

[6] Comment dated 25 October 2019, p. 8. Emphasis supplied.

Respondent later states in their Comment that:

> This means that the Complainant has consented for UPESO to contact her contact references and her contacts in case she continues to fail to pay her obligations with UPESO and to answer the calls and messages of UPESO.[7]

The Commission does not agree. Such vague and overbroad language in their loan agreement in no way complies with transparency, a general privacy principle. This is explained in the Implementing Rules and Regulations as such:

> The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

While the Commission finds that the allegations of Complainant do not fall under the purview of the Data Privacy Act, it finds it necessary to emphasize the need for personal information controllers such as Respondent to inform their data subjects of the purpose of the processing of their personal information in "clear and plain language." The requirement to use clear and plain language does not mean using layman's terms to substitute technical words at the risk of not capturing the complex concepts they represent. Rather, this requirement means that information should be provided in as simple a manner as possible, avoiding sentence or language structures that are complex.[8] The information provided should be concrete and definitive; it should not be phrased in "abstract or ambivalent terms or leave room for different interpretations"[9] such as in this case.

---

[7] *Ibid.*
[8] *See,* Guidelines on transparency under Regulation 2016/679 of the Article 29 Working Party (2017).
[9] *Ibid.*

WHEREFORE, on the basis of this Complaint, the Commission hereby resolves to **DISMISS** the Complaint of RBB against Respondent UPESO.PH Lending.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondent before any other forum or tribunal, if any.

SO ORDERED.
Pasay City, 21 May 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED

RBB
Complainant

MANZANAL & ANG LAW OFFICES
Counsel for Respondent

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

CA,
Complainant,

-versus-

WESTPARC CONDOMINIUM,
Respondent.
x----------x

NPC 18-004

For: Violation of the Data Privacy Act of 2012

VP,
Complainant,

-versus-

WESTPARC CONDOMINIUM,
Respondent.
x----------x

NPC 18-005

For: Violation of the Data Privacy Act of 2012

DECISION

AGUIRRE, *D.P.C.*;

Before this Commission is a Complaint filed by CA and VP (Complainants) against Westparc Condominium (Westparc) for an alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

In January 2018, Westparc's Condominium Association posted Circular No. WPCC-001-2018 (Circular) on the condominium's bulletin board.[1] The Circular urged condominium residents to submit a Unit Owner Information Sheet (201 File) for the purpose of updating and correcting inaccurate information in specific 201 files related to Westparc Condominium.[2] In the Circular, Westparc requested the submission of the following documents:

---

[1] Complaints-Affidavit, 28 February 2018, at 1, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2018).
[2] *Id.*

If Owned:

1. Completed Information Sheet of the Unit Owner with two Recent Colored Photos (2x2) with White Backgrou[n]d
2. Completed Information Sheet of the Occupants of the Condominium Unit with two Recent Colored Photos (2x2) with White Backgrou[n]d
3. At least 2 Valid Government Issued I.D. with picture
4. Condominium Certificate of Title (CCT)
5. Condominium Transfer Certificate of Title and Deed of Absolute Sale if not the First Owner of the Property
6. Completed Parking Sticker Application form as approved by the Building Manager (if with parking)
7. If unit is mortgaged or under financing. Certification or Clearance from Bank or any Financial Institution for purposes of move-in of either unit buyer or tenant
8. Copy of Passport if not a Filipino[3]

If Leased:

1. Completed Information Sheet of the Unit Owner with two Valid Government Issued I.D.s with photo, two Recent Colored Photos (2x2) with White Background and a Copy of Passport if not a Filipino
2. Completed Information Sheet of the Lessee with two Valid Government Issued I.D.s with photo, two Recent Colored Photos (2x2) with White Background and a Copy of Passport if not a Filipino
3. Completed Information Sheet of the Occupants of the Condominium Unit with two Valid Government Issued I.D.s. two Recent Colored Photos (2x2) with White Background and a Copy of Passport if not a Filipino
4. Notarized Lease Contract as Approved by the Building Manager
5. Condominium Certificate of Title (CCT)
6. Condominium Transfer Certificate of Title and Deed of Absolute Sale if Unit Owner is not the First Owner of the Property
7. Completed Parking Sticker Application form as approved by the Building Manager (if with parking)
8. If unit is mortgaged or under financing. Certification or Clearance from Bank or any Financial Institution for purposes of move-in of either unit buyer or tenant
9. Broker's Accreditation Form as Approved by the Building Manager (if Leased through a Broker)
10. Special Power Of Attorney (SPA) from the Unit Owner – for all authorized representatives of the Unit Owner[4]

---

[3] Circular No. WPCC-001-2018, 15 January 2018, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2018).
[4] *Id.*

Subsequently, Complainants alleged that they attempted to access their respective 201 files on multiple occasions by personally visiting the administration office, but they were unsuccessful.[5]

Due to the administration office's refusal to accommodate their verbal requests, on 07 February 2018, both Complainants, through counsel, sent letters to Westparc's administration office with the following demands:

> 1. The Association FURNISH COPIES OF RELEVANT BOARD RESOLUTIONS. MEETING MINUTES, OR SIMILAR DOCUMENTS SUPPORTING SUCH REQUIREMENT FOR SUBMISSION OF 201 FILES;
>
> 2. The Association TO ALLOW ACCESS AND INSPECTION OF, AND FURNISH COPIES OF THE 201 FILES OF OUR CLIENTS, MS. CA and MS. VP SO WE MAY INSPECT THE PERSONAL INFORMATION AND SENSITIVE PERSONAL INFORMATION IN POSSESSION OF THE CONDOMINIUM ASSOCIATION AND DETERMINE WHETHER THE CONDOMINIUM MISPLACED OR LOST ANY OF THE DOCUMENTS PERTAINING TO MS. CA AND MS. VP;
>
> 3. The Association FURNISH COPIES OF REGISTRATION WITH THE NATIONAL PRIVACY COMMISSION AS PERSONAL INFORMATION CONTROLLER; and
>
> 4. In case the Association is not registered as a personal information controller with the National Privacy Commission, that the ASSOCIATION IMMEDIATELY CEASE AND DESIST
> FROM IMPLEMENTING WPCC-001-2018. Should you fail to comply, we shall be constrained to avail any and all remedies available in law and equity to ensure the rights of Ms. VP and Ms. CA to peaceable enjoyment of their property.[6]

On the same date, Complainants sent another demand letter to Westparc "pertaining to the conduct of JAC [ ] purportedly the 'Security Officer' of Westparc Condominium."[7] After receiving a memorandum alleging that Complainants "inspected the installed

---

[5] Complaints-Affidavit, 28 February 2018, at 1, *in* CA v. Westparc Condominium, NPC 18-004 &
18-005 (NPC 2018).
[6] Demand Letter (RE: WPCC-001-2018, Demand to Furnish Relevant Documents, and in case of failure therefrom, cease and desist from implementation), 07 February 2018, at 1-2, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2018).
[7] Demand Letter (RE: Demand to provide copy of appointment papers of "Security Officer" JAC), 07 February 2018, at 1, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2018).

CCTV cameras and asked about details of the CCTV system," JAC reported an incident to the PNP against Complainants claiming that they violated a city ordinance and the Cybercrime Law.[8] Complainants claim that JAC cannot validly act as security officer because he was not appointed as such:

> JAC purports to be the in-house security officer of Westparc. We find this claim incongruous as Westparc engaged the services of ISSI as its security forces provider.
>
> Lacking appointment as Security Officer, JAC has NO BUSINESS AT ALL to require the security forces to furnish him copies of reports pertaining to our clients, residents of Westparc. Needless to say, this is a violation of the rights to privacy and peaceable enjoyment of property of our clients.[9]

Thus, Complainants demanded copies of the board resolutions appointing JAC as Security Officer.[10] Complainants also demanded that Westparc immediately cease allowing JAC to act as a Security Officer and retrieve any documents related to Westparc residents from him, if Westparc fails to comply with its request and if it did not officially appoint him as Security Officer .[11]

Complainants allege that as of 28 February 2018, they have not received any response from Westparc with regard to both demand letters.[12]

On 02 March 2018, Complainants filed two Complaint-Affidavits before the National Privacy Commission (NPC) accusing Westparc of violating the DPA.[13]

On 10 April 2018, the NPC, through its Complaints and Investigation Division (CID,) issued an Order directing the parties to attend a discovery conference set on 03 May 2018.[14]

---

[8] *Id.*

[9] *Id.* at 2.

[10] Complaints-Affidavit, 28 February 2018, at 1, *in* CA v. Westparc Condominium, NPC 18-004 &
18-005 (NPC 2018).

[11] Demand Letter (RE: Demand to provide copy of appointment papers of "Security Officer" JAC), 07 February 2018, at 2, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2018).

[12] Complaints-Affidavit, 28 February 2018, at 2, *in* CA v. Westparc Condominium, NPC 18-004 &
18-005 (NPC 2018).

[13] *Id.* at 1.

[14] Order to Confer for Discovery, 10 April 2018, at 1, *in* CA v. Westparc Condominium, NPC 18- 004 & 18-005 (NPC 2018).

During the Discovery Conference held on 03 May 2018, only Complainants and their representatives were present.[15] Complainants expressed their intent to request for the production of their 201 files and also sought copies of all documents related to them.[16]

Complainants stated that they would "like to demand for [the] authority by which the association is requiring all of the residents to comply with that [sic] directives to furnish personal and sensitive personal information to them."[17]

Complainants expressed concerns about the security of the documents, as they have no means to verify whether the "personal and sensitive personal information in [Westparc's] custody are appropriately protected by physical and technological safeguards."[18] Complainants also mentioned that given the issue on the security of the documents, there is potential unauthorized access that could harm their rights.[19]

During the discovery conference, Complainants discussed that after the filing of the complaint, they discovered the installation of a close- circuit television (CCTV) system with audio recording capabilities in the condominium.[20] They aver that the CCTV system is an "undue violation of their privacy rights [e]specially the privacy of their homes."[21] Complainants manifested that they will file a supplemental pleading regarding the installation of CCTV with audio system.[22]

On 04 May 2018, the CID directed Westparc to produce the documents that Complainants requested.[23] Complainants required Westparc to produce the following:

a. 201 files of Complainants

---

[15] Attendance Sheet for Discovery Conference, 03 May 2018, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2018).
[16] Transcript (Discovery Hearing/Conference), 05 May 2018, at 1-2, *in* CA v. Westparc
Condominium, NPC 18-004 & 18-005 (NPC 2018).
[17] *Id.* at 2.
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] Transcript (Discovery Hearing/Conference), 05 May 2018, at 2, *in* CA v. Westparc
Condominium, NPC 18-004 & 18-005 (NPC 2018).
[23] Order, 4 May 2018, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2018).

b. Actual copies of all documents that Respondent have pertaining to the Complainants

c. Authority by which the association is requiring all of the residents to comply with the directives to furnish personal information and sensitive personal information

d. Security measures implemented by the Respondent to protect personal information and sensitive personal information in their custody[24]

The deadline for the submissions was set for 13 May 2018.[25] CID also set another hearing for 15 May 2018.[26]

Westparc failed to comply with the deadline set by the CID for the submission of the required documents.[27] Further, during the 15 May 2018 Discovery Conference, only the Complainants' counsel was present.[28]

On 23 July 2018, Complainants filed a Supplemental Complaint raising concerns regarding the CCTV installation in Complainants' building.[29] They stated that "the unsecured layout of cables and network devices may have resulted in unauthorized access by third parties, thereby causing violation of [Complainants'] right to privacy."[30] According to Complainants, there is a "possibility that there may be unauthorized persons who may access and control the playback and recording system, as well as have the capability to generate copies of any and all captured data by the CCTV system, whether audio or video."[31] Thus, Complainants sought the intervention of the NPC to look into whether there was a violation of their privacy rights and take appropriate action accordingly.[32]

On 23 August 2018, the CID directed the conduct of an Onsite Investigation on Westparc – Cedar Condominium.[33]

---

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] Order, 27 December 2022, at 2, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC
2022).
[28] Attendance Sheet for Discovery Conference, 15 May 2018, in CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2018).
[29] Supplemental Complaint, 23 July 2018, at 1, *in* CA v. Westparc Condominium, NPC 18-004 & 18-
005 (NPC 2018).
[30] *Id.*
[31] *Id.* at 2.
[32] *Id.*
[33] Mission Order CID 18-002, 23 August 2018, *in* CA v. Westparc Condominium, NPC 18-004 & 18-
005 (NPC 2018).

On 27 December 2022, the CID issued an Order directing Westparc to submit the required documents enumerated in the 04 May 2018 Order and to submit a Verified Comment within fifteen (15) days from receipt of the Order.[34] Moreover, the CID required all parties to attend the preliminary conference set on 31 January 2023 and 28 February 2023.[35]

On 31 January 2023, none of the parties attended the Preliminary Conference.[36] Thus, it was reset to 28 February 2023.[37]

On 28 February 2023, both parties failed to attend the Preliminary Conference.[38] Hence, in an Order dated 28 February 2023, the CID directed the parties to submit their respective memoranda and emphasized that upon the lapse of the given periods for submission the case will be submitted for resolution.[39]

To date, the Commission has not received any submission from either party.

Issue

Whether Westparc is liable for violation of Complainants' right to access under Section 16 (c) of the DPA.

Discussion

The Commission finds Westparc liable for violation of the Complainants' right to access under Section 16 (c) of the DPA.

In administrative proceedings, Complainants carry the burden of proof to establish their allegations with substantial evidence.[40]

---

[34] Order, 27 December 2022, at 1, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2022).
[35] *Id.* at 2.
[36] Order, 31 January 2023, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2023).
[37] *Id.*
[38] Order, 28 February 2023, at 1, *in* CA v. Westparc Condominium, NPC 18-004 & 18-005 (NPC 2023).
[39] *Id.* at 2.
[40] Office of the Ombudsman v. Fetalvero, G.R. No. 211450 (2018).

Substantial evidence is defined as such relevant evidence that a reasonable mind may accept as adequate to support a conclusion.[41]

Section 1, Rule 131 of the Rules of Court provides a distinction between burden of proof and burden of evidence:

> Section 1. *Burden of proof and burden of evidence.* - Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim or defense by the amount of evidence required by law. Burden of proof never shifts.
>
> Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a *prima facie* case. **Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case**.[42]

Thus, in this jurisdiction, it is recognized that a party who alleges a fact has the burden of proving it.[43]

Complainants attached evidence in their submissions such as a photographed copy of the Circular, a photographed copy of a Unit Owner Information Sheet (201 File), and two (2) demand letters.

Once the complainant has established his case, the burden of evidence shifts to the respondent, who, in turn, has the burden to establish his defense.

Westparc, however, neglected to submit the documents as directed by CID in multiple Orders. Westparc also failed to appear without notice or justification, despite several opportunities to address the complaints against it.

NPC Circular 2016-04 (2016 Rules of Procedure) provides:

> Section 22. *Rendition of decision*. The Decision of the Commission shall adjudicate the issues raised in the complaint **on the basis of**

---

[41] Civil Service Commission v. Hernandez, G.R. No. 151095 (2004).
[42] 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. NO. 19-08-15-SC, Rule 131, § 1(1 May 2020). Emphasis supplied.
[43] Office of the Ombudsman v. Espina, G.R. No. 213500 (2017).

> **all the evidence presented** and its own consideration of the law.[44]

As such, on the basis of all the evidence presented, there is sufficient support for Complainants' claim that there is a violation of their right to access.

Under the right to access, individuals can request for access to their personal information held by a personal information controller (PIC). Section 16(c) of the DPA provides:

> Section 16. *Rights of the Data Subject.* The data subject is entitled to:
>
> . . .
>
> (c) **Reasonable access to, upon demand**, the following:
>
> **(1) Contents of his or her personal information that were processed;**
>
> (2) Sources from which personal information were obtained;
>
> (3) Names and addresses of recipients of the personal information;
>
> (4) Manner by which such data were processed;
>
> (5) Reasons for the disclosure of the personal information to recipients;
>
> (6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
>
> (7) Date when his or her personal information concerning the data subject were last accessed and modified; and
>
> (8) The designation, or name or identity and address of the personal information controller.[ ][45]

As alleged by Complainants, they attempted to access their respective
201 files on multiple occasions by personally visiting the

---

[44] National Privacy Commission, 2016 Rules of Procedure of the National Privacy Commission [NPC 2016 Rules of Procedure], rule III, § 22 (15 December 2016). Emphasis supplied.
[45] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 16 (c) (2012). Emphasis supplied.

administration office.[46] Due to the administration office's refusal to accommodate verbal requests, on 07 February 2018, both Complainants sent demand letters to Westparc.[47]

Westparc, however, denied Complainants' efforts to assert their right to access. Complainants' attempts to exercise their rights were met with a lack of responsiveness from Westparc, as indicated by its failure to address the data privacy concerns raised in the formal demand letters.[48]

The records further reveal Westparc's lack of interest, exemplified by its non-appearance and failure to submit required documents during the proceedings before the NPC. Despite being given sufficient notice, Westparc disregarded the NPC's orders and did not participate in the scheduled hearings. Given this, it forfeited its right to present its position on the matter.

Westparc's inaction and disregard for Complainants' right to access warrants the award of nominal damages.

The DPA provides for restitution for any aggrieved party under the Civil Code.[49] Section 37 of the DPA provides:

> Section 37. *Restitution.* Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.[50]

Article 2221 of the New Civil Code is clear that nominal damages may be awarded in recognition of the violated legal rights of a plaintiff or complainant:

> Article 2221. Nominal damages are adjudicated in order that a right of the plaintiff, which has been violated or invaded by the defendant, may be vindicated or recognized, and not for the purpose of indemnifying the plaintiff for any loss suffered by him.[51]

---

[46] Complaints-Affidavit, 28 February 2018, at 1, *in* CA v. Westparc Condominium, NPC 18-004 &
18-005 (NPC 2018).
[47] *Id.*
[48] *Id.*
[49] Data Privacy Act of 2012, § 37.
[50] *Id.*
[51] An Act to Ordain and Institute the Civil Code of the Philippines [CIVIL CODE], Republic Act No. 386, art. 2221 (1949).

The right to access in Section 16(c) of the DPA empowers data subjects to request for access to their personal information.[52] In this case, Complainants exercised this right by attempting to access their respective 201 files through verbal and written requests.[53] Westparc's refusal to accommodate these requests and its non-appearance during the proceedings before this Commission reflects a blatant disregard for Complainants' data privacy rights, specifically their right to access.

As recognition and vindication of Complainants' right to access, this Commission awards nominal damages in the amount of fifteen thousand pesos (P15,000.00) to each of the Complainants.

WHEREFORE, premises considered, this Commission:

1. **FINDS** Respondent Westparc Condominium **LIABLE** for violation of CA and VP's right to access under Section 16 (c) of Republic Act No. 10173 or the Data Privacy Act (DPA); and

   AWARDS nominal damages, in the amount of fifteen thousand pesos (P15,000.00) each to CA and VP for violation of their right to access under Section 16 (c) of the DPA.

SO ORDERED.

City of Pasay, Philippines.
13 November 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

---

[52] Data Privacy Act of 2012, § 16 (c).
[53] Complaints-Affidavit, 28 February 2018, at 1, *in* CA v. Westparc Condominium, NPC 18-004 &
18-005 (NPC 2018).

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

CA
Complainant

VP
Complainant

LNO
Counsel for Complainant

THE LAW OFFICES OF VILLAGRACIA & OPLE
Counsel for Complainant

WESTPARC CONDOMINIUM
Respondent

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

RMA

Complainant,

-versus-

NPC Case No. 17-065
For: Violation of the Data Privacy Act of 2012

INTERNATIONAL WORKPLACE GROUP PLC/REGUS

Respondent.

x----------x

DECISION

AGUIRRE, *D.P.C.:*

Before this Commission is a Complaint filed by the complainant RMA against the respondent International Workplace Group PLC/Regus, Inc. for an alleged violation of R.A. 10173 ("Data Privacy Act").

The Facts

On 10 December 2017, the complainant filed a Complaint through the official email address of the Complaints and Investigation Division (CID). The complainant stated therein:

> I'm working for International Workplace Group PLC (Regus) as an IT Network Consultant. There was a group of people in our Windows IT department who stole the local database of my personal skype account. This is against our Company's internal policy. They used my private messages against me. They have sent selected conversations to our Human Resource department, then our HR served a Notice to Explain Letter to me and I was suspended for 1 week. The decision was made and the penalty was just a written reprimand as the violation is very minor. After a couple of days, HR sent another Notice to Explain letter with attached fabricated conversations created by those malicious employees. I think they will not stop until I'm dismissed.[1]

---

[1] Records, Page 2.

On 28 February 2018, the National Privacy Commission (Commission), through the CID, issued an Order to Confer for Discovery that ordered both parties to appear before the Commission on 27 March 2018. The Order stated thus:

> Pursuant to Section 13 of Circular 16-04 of the National Privacy Commission, the Parties shall discuss whether discovery of information and of electronically stored information will be sought; issues relating to preservation of information; period to produce the information; method of asserting and preserving claims of privilege information, confidentiality, and proprietary status of information; appropriateness of allocating expenses of production of information; and any other issue relating thereto.[2]

Only the representatives from the respondent appeared on 27 March 2018.[3] Complainant having failed to attend the Conference, the presiding officer proceeded to discuss with the respondent the purpose of the hearing. It was agreed that the respondent would file a comment with their internal policy and the privacy policy attached in the Comment.[4]

On 25 April 2018, the respondent, through their Data Protection Officer, filed their Answer with the Commission.

Arguments of the Parties

In his Complaint, the complainant alleged that his "private and sensitive conversations" were among the personal information affected, as well as "log-in credentials for very important portals like online banking and other confidential information."[5] Complainant sought dismissal of the "malicious employees" of the respondent. [6] He prayed for damages equivalent to the amount he lost caused by his suspension and all the legal actions he will take. He also prayed for a Cease and Desist Order to be issued directing their Human Resource to stop processing any illegally acquired or fabricated information.

---

[2] *Id.*, at 4-5.
[3] *Id.*, at 10.
[4] Id., pp. 12-13.
[5] Ibid.
[6] Ibid.

Finally, his Complaint prayed for the issuance of a temporary ban on Respondent's processing of his data.[7]

In their Answer, the respondent specifically denies the allegation that they extracted from the complainant's personal Skype account, a series of chat messages between the complainant and the respondent's Head of Network, as well as those with Complainant's friend, RM, who worked for a different company, without his consent.[8]

Respondent asserts that the chat messages were voluntarily forwarded to Respondent's IT Service Operations Director EC, through an anonymous email address [ ]

According to the respondent, it did not violate any right of the complainant under the Data Privacy Act. Rather, they assert that it was the complainant who violated the respondent's company information policy, when, as shown in the chat messages, the complainant provided RM access to the respondent's infrastructure which would enable any external party to access their servers or firewall.[9] They admit that they should have meted out stiffer penalties to the complainant for his violation of the security policy, but only gave him a Written Reprimand.

The respondent asserts that it did not violate any of the rights of the complainant under the Data Privacy Act, and that the complainant failed to demonstrate that the respondent acted in a wanton, fraudulent, reckless, oppressive, or malevolent manner in dealing with the complainant.[10]

Issue

The sole issue to be resolved in this case is whether the respondent committed a violation of the DPA that warrants a recommendation for prosecution.

Discussion

Respondent did not commit a violation that warrants a recommendation for prosecution under the Data Privacy Act of 2012.

---

[7] *Id.*, at 2.
[8] *Id.*, at 29.
[9] *Id.*, at 30.
[10] *Ibid.*

In the Complaint, the complainant claims that there was a group of people in their Windows IT department who stole the local database of his personal Skype account.[11] The Commission notes, however, that the complainant only attached his BIR TIN ID and failed to provide any other supporting document to substantiate his claim that Respondent extracted "private and sensitive conversations, " as well as "log-in credentials for very important portals like online banking and other confidential information."[12]

The Commission further notes that, despite its issuance of an Order to Confer for Discovery to both parties, the complainant failed to appear at the Discovery Conference. Also, despite having been furnished a copy of Respondent's Answer which asserted that his allegations were "totally inaccurate and without basis," the complainant still failed to provide additional information or evidence to support his allegations.

The Complaint shall only be recommended for prosecution if it is supported with *relevant evidence which a reasonable mind might accept as adequate to justify a conclusion*.[13] The allegations in the complaint must be based on substantial evidence that there is a clear and real violation of the law.

In *Morales vs. Ombudsman, et al.*,[14] the Supreme Court explained:

> *The basic rule is that mere allegation is not evidence and is not equivalent to proof. Charges based on mere suspicion and speculation likewise cannot be given credence. When the Complainant relies on mere conjectures and suppositions, and fails to substantiate his allegations, the complaint must be dismissed for lack of merit.*[15]

The Commission's Rules of Procedure also provides:

> **Section 22. *Rendition of decision.*** – The Decision of the Commission shall adjudicate the issues raised in the complaint **on the basis of all the evidence presented** and its own consideration of the law.[16]

---

[11] *Id, at 2.*
[12] *Ibid.*
[13] Rules of Court, Rule 133, §5.
[14] 798 SCRA 609. 17 July 2016.
[15] *Id.*, at p. 627.
[16] NPC Circular No. 16-04 dated 15 December 2016 ("NPC Rules of Procedure"), Sec. 22, Emphasis supplied.

As such, on the basis of all the evidence presented, the Commission finds that there is insufficient evidence to support the complainant's claim that the respondent stole the local database of the complainant's personal Skype account, accessing private and sensitive conversations as well as login credentials.

Considering that there is nothing in the Complaint that would reasonably connect the respondent to any of the possible violations enumerated under the DPA, the Commission resolves to dismiss the Complaint for lack of substantial evidence required in establishing cases before quasi-judicial bodies.

WHEREFORE, all the above premises considered, the Commission hereby resolves to **DISMISS** the Complaint of RMA against International Workplace Group PLC/Regus.

SO ORDERED.
Pasay City, 31 January 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Concurring:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED

RMA
Complainant

JRB
Respondent's Data Protection Officer

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

EG,

Complainant,

NPC 21-111

-
versus-

JI, RO, and RR

Respondent.

For: Violation of the Data Privacy Act of 2012

x----------x

DECISION

NAGA, *P.C.;*

Before this Commission is a Complaint filed by EG against JI, RO, and RR (collectively, Respondents) for an alleged violation of Section 32 of Republic Act No. 10173, or the Data Privacy Act of 2012 (DPA).

Facts

On 01 June 2021, EG filed a Complaint-Affidavit with the NPC's Complaints and Investigation Division (CID), alleging that he was a resident of Chateau Elysée, a condominium in Parañaque City, while RespondentsJI works as an Administrative (Admin) Assistant, RO works as the Admin Manager, and RR as the Chief Security of Chateau Elysée Condominium. [1]

In his Complaint-Affidavit, EG alleged that he "had a verbal argument with another tenant in his building, a British-Filipino citizen, which alerted the security agency, including the respondent RR."[2] EG averred that "when things escalated, matters were reported to the building administrators and the British Filipino nurse, conducted their (*sic*) own private investigation about [the Complainant]."[3]

---

[1] Complaint-Affidavit dated 26 May 2021 of EG, at p. 1.
[2] *Id.*, at ¶ 4.
[3] *Id.*, at ¶ 5.

EG claimed that "[t]hey talked to the security and was able to secure a video footage of the Complainant, his identity, whereabouts, and other footage containing his personal information without his consent."[4]

EG alleged that "[i]n the meeting with the Barangay, Respondents JI and RO (sic), employees of Chateau Elysee Condominium, admitted that they [had] released the video footage to the British-Filipino Nurse and admitted that they did so without the consent of EG."[5]

EG further alleged that there was no privacy notice from the Condominium Corporation informing the tenants that the building administration was processing personal data.[6]

Subsequently, EG filed a complaint with the barangay due to alleged privacy violations.[7]

EG attached in his Complaint-Affidavit a letter addressed to the Respondents dated 01 December 2020.[8] In the letter, EGinformed the Respondent of the alleged privacy violation and demanded "for damages as reparation and indemnity for [the] unauthorized disclosure of personal information."[9]

An Order to Comment dated 30 June 2021 was issued ordering Respondents to file a verified comment within fifteen (15) calendar days from receipt of the Order.[10]

On 27 August 2021, an Order to Appear for Preliminary Conference was issued ordering the parties to appear virtually for Preliminary Conference on 13 October 2021 and 27 October 2021.[11]

---

[4] *Id.*, at ¶ 5.
[5] Complaint-Affidavit dated 26 May 2021 of EG, at ¶ 8.
[6] *Id.*, at ¶ 7.
[7] *Id.*, at ¶ 9.
[8] Complaint-Affidavit dated 26 May 2021 of EG, at p. 6, *See* Letter dated 1 December 2020 of LB.
[9] *Id.*
[10] *EG vs JI, RO and RR.*, NPC 21-111, Order to Comment dated 30 June 2021.
[11] *EG vs JI, RO, and RR*, NPC 21-111, Order to Appear for Preliminary Conference dated 27 August 2021.

Respondents filed their Comment dated 25 September 2021 praying that the complaint be dismissed for lack of merit.[12] Respondents averred that they were deployed in the condominium, with RO working as the "Admin Manager of Maininvest General Services Inc."; JI as an "Admin Assistant" of the same agency; and RR as a "Security Officer of Commander Security Services Inc[.]".[13]

Respondents stated that "EG [had] a misunderstanding or quarrel [with] one of the tenant[s] namely [JM and PM] at the lobby of Cluster
5."[14] Respondents alleged that EG filed a complaint before the Barangay due to the incident, and that Spouses JM and PM went to the Property Management Office and requested for the closed-circuit television (CCTV) footage to prove "that there [was] no physical interaction between the two parties and to enlightened (*sic*) the Barangay Lupon [on] what really happened [during] that time."[15]

Though not explicitly stated, the "British Filipino nurse" mentioned in EG's Complaint-Affidavit[16] can reasonably be inferred to be PM as mentioned in the subsequent submissions of the parties. This is bolstered by the fact that EG, in his Memorandum, alleged that he had a verbal argument with PM sometime in January 2020.[17]

Respondents also alleged that EG went to the administrative office to complain about RR for releasing the CCTV footage to the Spouses JM and PM.[18]

Respondents averred that as part of the protocol for this kind of request for investigation, JI, as the Admin Assistant, will only receive the complaint or request and collate relevant details which will then be endorsed to the Head of Security or Shift-in-Charge for investigation.[19] Here, JI, forwarded the request to obtain the CCTV to RR, who was the Security-in-Charge at that time.[20] Respondents alleged that JI had no authority nor jurisdiction to approve the release

---

[12] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 6.
[13] *Id.*, at p. 1.
[14] *Id.*, at pp. 1-2.
[15] *Id.*, at p. 2.
[16] Complaint-Affidavit dated 26 May 2021 of EG, at ¶ 5.
[17] Memorandum of Complainant EG dated 23 February 2022, at ¶ 4.
[18] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 3.
[19] *Id.*, at p. 2.
[20] *Id.*, at p. 2.

of any documents, personal information, or CCTV footage to any person without the approval of the proper authority.[21]

Respondents alleged that RR interviewed and investigated the Spouses JM and PM request and retrieved the CCTV footage as evidence to show the lack of physical altercation between Spouses JM and PM and EG.[22] Respondents averred that "[the Spouses JM and PM] presented a letter to RR from Barangay Moonwalk, a Subpoena, and a request letter requesting the evidence on the said incident."[23] Thus, RR was convinced to release the CCTV footage to assist the Spouses JM and PM "without the approval of the Management or the Security Agency."[24]

At the hearing before the Barangay, the Spouses JM and PM presented the CCTV footage received from RR which "is one of the pieces of evidence in helping the Barangay to resolve the issues of both parties and to amicably settle the issue between the conflicting parties."[25]

As their defense, Respondents alleged the following:

> 1. At the onset, [Respondents] were not furnished [with] a copy of the complaint and thus, had no opportunity to contest the allegations of the complainant.
> 2. The Complainant failed to comply [with] the substantial requirements for PRE-INVESTIGATION PHASE for failure to give the Respondent the opportunity to address the issue when it sent a defective demand letter as stated in Rule IV Section 1.[26]

Respondents further argued that EG "improperly informed the Respondents of the sufficient factual circumstances surrounding the alleged violation by failing to specify on the demand letter sufficient information on what is [sic] necessary action to be done and the nature of the alleged violation."[27]

---

[21] *Id.*, at p. 2.
[22] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 2.
[23] *Id.*, at p. 3.
[24] *Id.*, at p. 3.
[25] *Id.*, at p. 3.
[26] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 4.
[27] *Id.*, at p. 4.

Respondents argued that RO and JI should not be liable for the release of the CCTV footage.[28] RO was out of the office when the Spouses JM and PM requested the said footage and was unaware of the request.[29] Further, Respondents alleged that "JI was only performing her duty as an administrative assistant in recording, receiving the complaint, and endorsing the concerns or issues to the investigating department."[30]

Moreover, Respondents alleged that the actions RR took by providing the CCTV footage to the Spouses JM and PM, upon their request, was a "lawful exercise of rights and duties and not violative of any existing privacy laws, guidelines, or policies and done in good faith."[31]

After the preliminary conference on 13 October 2021, both parties manifested that they were willing to undergo mediation proceedings.[32]

In an Order dated 13 October 2021, the CID stated that:

> DL manifested that while respondents received the Order to Virtually Appear for Preliminary Conference dated 17 August 2021, no copy of the complaint and its annexes was attached as raised in the verified comment they have filed. Hence, he requested that respondents be given additional period of time to file amended or supplemental verified comment after receiving a copy of the complaint. Complainant, through counsel, opposed no objection thereto.[33]

The CID ordered that "a copy of the complaint and its attachments, Order to Comment dated 30 June 2021 and all verified comments be furnished" to the parties' specified addresses.[34]

Subsequently, EG filed a Manifestation with Motion dated 31 October 2021 with a prayer to terminate the mediation proceedings.[35] In the Manifestation, it was alleged that EGemailed his counsel and

---

[28] *Id.*, at p. 4.
[29] *Id.*, at p. 5.
[30] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 5.
[31] *Id.*, at p. 6.
[32] *EG vs JI, RO, and RR.*, NPC 21-111, Order (After the 1st Preliminary Conference on 13 October 2021) dated 13 October 2021.
[33] *Id.*
[34] *Id.*
[35] Manifestation with Motion of EG dated 31 October 2021, at p. 2.

expressed his unwillingness to enter into mediation with the Respondents.[36]

An Order dated 07 December 2021 was issued granting the motion to terminate the mediation process.[37] Moreover, the Respondents were ordered to submit their amended/supplemental verified comment within fifteen (15) days from receipt of the Order.[38] Further, the parties were ordered to appear for a preliminary conference on 26 January 2022.[39]

The Respondents filed their Joint Counter-Affidavit dated 28 December 2021 wherein they reiterated the discussions made in their initial Comment.[40]

In the Joint Counter-Affidavit, Respondents further alleged that:

> 6. The releasing of video footage (*sic*) in favor of JM and PM, the British-Filipino nurse, was decided solely by RR;
>
> a. RR is the Security Officer/CCTV System Operator, who assisted JM and PM do during the investigation of the facts and circumstances that transpired between subjects of the video footage. He released the same to JM and PM upon their request and consent as part of the evidence to prove that there was no physical interaction that transpired between them and the complainant during their confrontation last 9 January 2020.
>
> b. That JM and PM are one of the registered tenants of Chateau Elysee Condominium who provided all documents necessary for the release of the video footage involving them for proper investigation such as investigation request form and waiver declaring that the CCTV footage requested will be used only to resolve their issues with the complainant in the Barangay Moonwalk and not to post in social media or other media platforms. They [JM and PM] also declared taking full responsibility of any legal consequences that may arise from request especially the Data Privacy Act of 2012.[41]

---

[36] *Id.*, at p. 1.
[37] *EG vs JI, RO, and RR*, NPC 21-111, Order (on the Manifestation and Motion filed by the Complainant) dated 07 December 2021, at p. 1.
[38] *Id.*, at p. 1.
[39] *Id.*, at p. 2.
[40] Joint Counter-Affidavit dated 28 December 2021 of Respondents JI, RO and RR.
[41] *Id.*, at ¶ 6.

The CID issued an Order dated 04 January 2022 noting the submission of the Joint Counter Affidavit.[42]

In the second preliminary conference on 26 January 2022, the parties stipulated the following issues to be resolved:

> 1) whether or not the release of the CCTV footage constitutes a violation of the Data Privacy Act; and
>
> 2) whether or not Respondents RO and JI, who have not participated in the release of the video coverage would be held liable.[43]

The parties were ordered to simultaneously submit their respective memoranda.[44]

Respondents filed their Memorandum dated 22 February 2022, wherein they reiterated their claims and defenses in their past submissions and further made additional allegations.[45]

In their Memorandum, Respondents claimed that they "informed JM and PM regarding the legal action taken by [EG] for releasing the requested CCTV Footage."[46] Moreover, the Spouses JM and PM "provided a signed a letter to the Property Management Office of Chateau Elysée declaring the CCTV Footage they [got] from Chateau Elysée will be used as evidence to enlighten the Barangay Moonwalk on what truly happened during their confrontation with EG."[47]

Respondents alleged that "the CCTV System installed at the Chateau Elysée Condominium was provided by the Commander Security Services Inc. to the Condominium Corporation as part of the Contract Service Agreement and was publicly conveyed to all the members and unit owners based on this contract."[48] Respondents alleged that RR

---

[42] *EG vs JI, RO, and RR*, NPC 21-111, Order (Noting the Submission of Joint Counter Affidavit) dated 04 January 2022.
[43] EG vs JI, RO, and RR, NPC 21-111, Order (After the 2nd Preliminary Conference) dated 26 January 2022.
[44] EG vs JI, RO and RR, NPC 21-111, Order (Noting the Submission of Joint Counter Affidavit) dated 26 January 2022.
[45] Memorandum dated 22 February 2022 of Respondents JI, RO, and RR.
[46] *Id.*, at ¶ 7.
[47] *Id.*, at ¶ 7.
[48] *Id.*, at ¶ 17.

was "assigned to [the] position [of] Security Officer who will conduct [the] review, [restoration], and make (*sic*) an investigation report pertaining to the CCTV System operation as part of his duties and responsibilities."[49]

Respondents, as part of their defense, argued that the release of the CCTV footage was justified since it was in accordance with Section 7 of NPC Advisory No. 2020-04 in relation to Section 13 of the DPA.[50]

Moreover, the Respondents argue that the "consent of the other party (like [EG]) is not necessary particularly when its release is contrary to the interest of the non-consenting [party] and necessary for the defense of the data subject, which is considered a legitimate interest."[51]

Respondents also argued that the data subjects whose personal information were processed are those of Spouses JM and PM personal information, which was necessary for their defenses against EG's accusation in the barangay proceedings.[52]

EG submitted his Memorandum dated 23 February 2022, alleging that he is a "data subject and that his personal information is being processed by the building administrator and security personnel."[53] Moreover, EG alleged that "the release of PM's personal information for whatever purpose may be achieved without disclosure of the personal information of non-consenting subjects by masking portions of the video."[54]

Further, EG argued that as the personal information controller (PIC), Respondents were bound "to safeguard [the] personal information and not disclose said information without the data subject's consent."[55] EG further alleged that Respondents admitted that the CCTV was released without his consent and was therefore unauthorized.[56] EG also argued that the access to the CCTV Footage did not comply with the provisions of NPC Advisory No. 2020-04.[57] He also averred that

---

[49] Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, at ¶ 19.
[50] *Id.*, at ¶ 20.
[51] *Id.*, at ¶ 22.
[52] *Id.*, at ¶ 26.
[53] Memorandum of Complainant EG dated 23 February 2022, at ¶ 11.
[54] *Id.*, at ¶ 19.
[55] *Id.*, at ¶ 12.
[56] *Id.*, at ¶ 14.
[57] Memorandum of Complainant EG dated 23 February 2022, at ¶ 16.

"the lack of CCTV Notice on the premises shows their unawareness of their responsibilities under the law and of the sanctions it can bring."[58]

Issue

Whether Respondents committed a violation of the DPA.

Discussion

The Commission dismisses the complaint for lack of merit.

EG, as the complainant, has the obligation to prove by substantial evidence that either JI, RO, or RR committed a privacy violation under Section 32 of the DPA.

As already established in past rulings, in administrative proceedings such as in this Commission, the burden is on the Complainant to prove by substantial evidence that the allegations in the complaint are true.[59] In the case of *Billanes vs. Latido*, the Supreme Court defined substantial evidence as "that amount of evidence which a reasonable mind might accept as adequate to justify a conclusion."[60]

In EG's Memorandum, it was averred that Respondents "committed a violation upon the release of the video containing the personal information of a non-consenting subject."[61] Further, EG alleged that "the purpose could be achieved without disclosing personal information of a non-consenting subject by the testimony of witnesses or, should the video be indispensable, by masking of personal information of the non-consenting subject."[62] Lastly, EG averred that as a "[PIC], [Respondents] have the duty to safeguard personal information of the data subject and may only release personal information with the consent of the subject concerned."[63] EG alleged

---

[58] *Id.*, at ¶ 25.
[59] M vs B, G.R. No. 149335, 01 July 2003.
[60] *B vs L*, A.C. No. 12066, 28 August 2018.
[61] Memorandum of Complainant EG dated 23 February 2022, at ¶ 21.
[62] *Id.*, at ¶ 24.
[63] *Id.*, at ¶ 26.

that such unauthorized disclosure is penalized under Section 32 of DPA.[64]

Respondents, in their defense, argued that the "consent of the other party (like [EG]) is not necessary particularly when its release is contrary to the interest of the non-consenting [party] and necessary for the defense of the data subject, which is considered a legitimate interest."[65] Further, Respondents alleged that "the action made by [RR] by providing [the] CCTV Footage [to] JM and PM upon their request is a lawful exercise of [their] rights and duties and [is] not violative of any existing privacy laws, guidelines or policies and done in good faith to resolve the issues arising from the contending parties and to facilitate an amicable settlement between them."[66]

The Commission, after extensively reviewing the evidence and claims of both parties, finds that there is no substantial evidence to conclude that Respondents are liable since EG failed to establish that the processing of the CCTV footage was violative of Section 32 of the DPA or his data privacy rights.

Section 32 of the DPA provides:

> Section 32. Unauthorized Disclosure. – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).[67]

As discussed by the Commission in NPC 21-010 to 21-015,

> Based on a literal reading of Section 32 of the DPA, a PIC or a PIP is liable if it discloses to a third party personal or sensitive

---

[64] *Id.*, at ¶ 27.

[65] Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, at ¶ 22.

[66] *Id.*, at ¶ 22.

[67] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter VIII, § 32 (2012).

> personal information without the consent of the data subject. Following a literal reading, a PIC or PIP will have committed Unauthorized Disclosure if the disclosure is without the consent of the data subject even in the disclosure is justified by another lawful criterion for processing. It does not recognize that such disclosure may be based on other criteria for lawful processing enumerated in Sections 12 and 13 of the DPA. As such a literal reading of Section 32 of the DPA will result in absurdity.[68]

To be liable for Section 32 of the DPA, the following elements must concur:

1. The perpetrator is a personal information controller or personal information processor or any of its officials, employees or agents;
2. The information relates to personal or sensitive personal information;
3. The perpetrator disclosed personal or sensitive personal information;
4. The disclosure was made to a third party;
5. The personal or sensitive personal information disclosed is neither unwarranted nor false information;
6. The disclosure was not malicious nor done in bad faith; and
7. The disclosure was without any of the lawful bases for processing under Section 12 and 13 of the DPA.

As will be discussed below, not all of the elements for a Section 32 violation of the DPA are present in this case.

I. Respondent RR is an employee of a personal information processor.

The first element is present in this case as to RR. For clarity, a PIC "refers to a person or organization, who controls the collection, holding, processing, or use of personal information, including a person or organization, who instructs another person or organization to collect, hold, process use, transfer or disclose personal information on his or her behalf."[69]

---

[68] NPC 21-010 to 21-015, Decision dated 03 February 2022, at p. 11.
[69] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 3 (h) (2012).

Meanwhile, a personal information processor (PIP) "refers to any natural or juridical person qualified to act as such under this Act to whom a [PIC] may outsource the processing of personal data pertaining to a data subject."[70]

Respondents averred that they were deployed in the condominium, with RO working as the "Admin Manager of Maininvest General Services Inc."; JI as an "Admin Assistant" of the same agency; and RR as a "Security Officer of Commander Security Services Inc[.]"[71]

Further, in Respondents' Memorandum, it was stated that the CCTV System installed at Chateau Elysée Condominium was provided by Commander Security Services Inc. to the Condominium Corporation as part of the Contract Service Agreement.[72] From the circumstances, Commander Security Services Inc. acts as a PIP by virtue of its contract with the Condominium Corporation to install and operate a CCTV system within their premises. It can be inferred that the processing of information through the CCTV medium is being processed on behalf of the Chateau Elysée Condominium. It is Chateau Elysée Condominium that controls the processing of personal information through CCTV. Thus, based on the foregoing, the PIC in relation to the CCTV system is the Condominium Corporation.

In this respect, RR, as an employee of Commander Security Services Inc., is an agent acting on behalf of the PIP.

However, it is unclear from the records whether JI and RO may be considered PIPs in relation to EG complaint. It should be noted that JI and RO belong to a different agency from RR. They are employed by Maininvest General Services Inc. This agency's role as a PIP was not fully elaborated in this case. It fell to EG, as the complainant, to prove with substantial evidence how JI and RO actions are within the scope of the DPA either as agents acting on behalf of the PICs or PIPs.

In EG Memorandum, he lumps all the respondents together as violators of the DPA since they are allegedly PICs.[73] However, as the complainant, he had the burden of explaining how each respondent

---

[70] Data Privacy Act of 2012, § 3 (i).
[71] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 1.
[72] Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, at ¶ 17.
[73] Memorandum of Complainant EG dated 23 February 2022, at ¶ 12.

acted in violation of the DPA. After scrutinizing the records, the Commission cannot adequately conclude that JIand RO may fall under the same category as agents acting on behalf of the PIPs. There was no adequate discussion on the role of Mainvest General Services Inc., what personal data was processed by the agency or by JI and RO, and how their actions may characterize them as agents of the PICs or PIPs.

Thus, the first element is present for RR since he is an agent acting on behalf of the PIP. However, the first element is absent for JI and RO.

II. The CCTV footage contains personal information.

Personal information "refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information or, when put together with other information, would directly and certainly identify an individual."[74]

A CCTV "refers to closed-circuit television or camera surveillance system in a fixed or stationary location that can capture images of individuals or other information relating to individuals."[75] In NPC Advisory Opinion No. 2019-023, "if a camera surveillance footage is of sufficient quality, a person with the necessary knowledge will be able to reasonably ascertain the identity of an individual from the footage."[76]

Here, the CCTV footage contains personal information since it could identify parties such as EG through its system of recording videos or capturing images of the data subjects. Thus, the second element is present.

III. Respondent RR disclosed the personal information of EG.

---

[74] Section 3 (g) of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012
[75] National Privacy Commission, Guidelines on the use of Closed-Circuit Television (CCTV) Systems, NPC Advisory 2020-04, § 3 (c) (16 November 2020) (NPC Advisory 2020-04).
[76] National Privacy Commission Advisory Opinion No. 2019-023 dated 13 June 2019, Re: Processing of CCTV Footage Under the Data Privacy Act of 2012, at p. 2.

In EG Complaint-Affidavit, it was alleged that the Spouses JM and PM were able to secure the CCTV footage of the incident without his consent.[77] In Respondents' Comment, it was admitted that the CCTV footage was released after RR investigated the request and was convinced that the footage will be used in the barangay proceedings involving the dispute between EG and the Spouses JM and PM.[78]

Disclosure has been defined as "the release, transfer, provisions of, access to, or divulgence in any manner of information outside the entity holding the information."[79]

In this case, the act of RR releasing the CCTV footage to the Spouses JM and PM constituted an act of disclosure. Thus, the third element is present as to RR.

However, the third element is absent when it comes to JI and RO.

Based on Respondents' Comment, JI actions were limited to receiving the complaint and endorsing the concerns to the investigating department.[80] Particularly, JI endorsed the request of the spouses to RR, who was the security-in-charge at that time, who then investigated and eventually released the footage to the Spouses JM and PM.[81]

Further, while RO worked as the "Admin Manager" of the condominium, [82] Respondents argued that he was on official business at the time and was not in the office during the incident.[83] The records do not show any sufficient proof to refute this claim.

Thus, EG has not established with substantial evidence that either JI or RO actively participated in the release of the CCTV footage.

IV. The Spouses JM and PM are not third parties.

---

[77] Complaint-Affidavit dated 26 May 2021 of EG, at ¶ 5.
[78] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 3.
[79] Disclosure (Definition), 2017 Glossary of HIPAA Related Terms, Indiana University.
[80] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 5.
[81] *Id.*, at p. 3.
[82] *Id.*, at p. 2.
[83] *Id.*, at p. 5.

In EG Complaint, he alleged that "he did not give his consent in the disclosure of his personal information to strangers conducting their own private investigation about him."[84]

Respondents further alleged that the Spouses JM and PM requested a copy of the CCTV Footage "as evidence to show lack of physical interaction (*sic*) between the two parties and to enlighten the Barangay Moonwalk that only [a] simple misunderstanding of both parties had transpired."[85] Respondents also argued that the data subjects whose personal information was processed are those of Spouses JM and PM personal information, which was necessary for their defenses against EG accusation in the barangay proceedings.[86]

Meanwhile, under Section 7 of NPC Advisory No. 2020-04:

> SECTION 7. Data subject request for access. — **Any person whose image is recorded on a CCTV system has a right to reasonable access and/or be supplied with a copy of their own personal data from the footage,** subject to the provisions of Section 13 of this Advisory.
>
> xxx
>
> Where images of parties other than the requesting data subject and/or the person/s sought to be identified as part of the request (e.g. identification of malefactors for investigation or law enforcement purposes) appear on the CCTV footage, legitimate interest under Section 12(f) of the DPA may apply as basis for disclosing, subject to Section 9 of this Advisory.[87] (Emphasis supplied)

Here, the Spouses JM and PM cannot be reasonably considered third parties, given that they are also data subjects captured in the CCTV footage. As data subjects, Spouses KM and PM has a reasonable claim to access and obtain the CCTV footage used in the barangay dispute between EG and the Spouses JM and PM.

---

[84] Complaint-Affidavit dated 26 May 2021 of EG, at ¶ 11.
[85] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 2.
[86] Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, at ¶ 26.
[87] Section 7, of NPC Advisorty 2020-04, otherwise known as Guidelines on the use of Closed-Circuit Television (CCTV) Systems.

V. The personal information is neither unwarranted nor false information.

For a violation of Section 32 of the DPA to be committed, the personal or sensitive information should neither be unwarranted nor false.

In this case, there is no indication that the CCTV footage was falsified, altered, or considered unwarranted. Though EG alleged that the footage was disclosed without his consent, the disclosure was in relation to the barangay dispute. The presentation of the CCTV footage is warranted and necessary in the barangay dispute to prove the defense of Spouses JM and PM. Moreover, EG did not dispute the veracity of the CCTV footage that it was false or altered. Thus, the fifth element is present.

VI. There was no bad faith or malice on the part of Respondents.

The Supreme Court has defined "malice" as that which "connotes ill will or spite and speaks not in response to duty but merely to injure the reputation of the person defamed and implies an intention to do ulterior and unjustifiable harm."[88] As to bad faith, it "implies a conscious and intentional design to do a wrongful act for a dishonest purpose or some moral obliquity."[89]

Further, the Supreme Court ruled in *Wong vs. Wong:*[90]

> The rule is well-settled that he who alleges a fact has the burden of proving it and a mere allegation is not evidence. Thus once more, his self-serving assertion cannot be given credence. This is especially so in light of the presumption of regularity, which herein ought to prevail due to the absence of any clear and convincing evidence to the contrary.[91]

In this case, EG did not prove that Respondents acted with malice or bad faith in disclosing his personal information. Indeed, EG accused

---

[88] Delgado v. HRET, G.R. No. 219603, 26 January 2016
[89] *Montinola vs. Philippine Airlines*, G.R. No. 198656, 8 September 2014.
[90] *Tzu Sun Wong vs. Kenny Wong*, G.R. No. 180364, 03 December 2014.
[91] *Tzu Sun Wong vs. Kenny Wong*, G.R. No. 180364, 03 December 2014, citing *Alcazar vs. Arante*, G.R. No. 177042, 10 December 2012.

the Respondents of violating Section 32 of the DPA, which is a privacy violation falling outside Malicious Disclosure under Section 31 of the DPA. Thus, the sixth element is also present.

VII. There is a lawful basis on the part of Respondent RR in releasing the CCTV footage to Spouses JM and PM.

The seventh element is absent. EG alleged that the release of the CCTV footage was made without his consent.[92] However, consent is not the only criterion for lawful processing under the DPA.

Sections 12 (f) and 13 (f) of the DPA states:

> SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> xxx
>
> (f) The processing is necessary **for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties** to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.
>
> SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> xxx
>
> (f) The processing concerns such personal information as is **necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims**, or when provided to government or public authority.[93] (Emphasis supplied)

---

[92] Complaint-Affidavit dated 26 May 2021 of EG, at ¶ 11.
[93] Section 12 (f) and Section 13 (f) of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012

Further, Section 9 of NPC Advisory No. 2020-04, provides:

> SECTION 9. Legitimate interest three-part test. **In determining whether the data subject access request, in instances when the CCTV footage includes other data subjects, under Section 7**, or the third-party access request under Section 8(E) **may be allowed pursuant to legitimate interest as provided for under Section 12(f) of the DPA**, the following shall be considered:
>
> A. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve.
>
> B. Necessity test - The processing of personal information must be necessary for the purposes of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
>
> C. Balancing test - The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PICs or third party, considering the likely impact of the processing on the data subjects.
>
> In this regard, CCTV footages requested for purposes of the protection of lawful rights and interests or the establishment, exercise or defense of legal claims under Section 13(f) of the DPA may be considered as legitimate interest.[94]

It is apparent in the submissions of the parties that the CCTV footage obtained by the Spouses JM and PM was used as part of their defense in a complaint against them before the barangay. The CCTV footage was used to prove that there was no physical altercation between the Complainant and the Spouses JM and PM.[95] Thus, the release of the footage was necessary for the exercise of the spouses' defenses in the barangay proceeding. The purpose for the release of the footage was adequately shown through the Investigation Request Form,[96] and the Spouses JM and Pm's letter dated 31 January 2020.[97]

In the case of KRL vs. Trinity University of Asia, et. al., the Commission ruled:

---

[94], Guidelines on the use of Closed-Circuit Television (CCTV) Systems, NPC Advisory 2020-04, § 9

[95] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 2.

[96] Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, *See:* Annex "B".

[97] *Id.*, *See:* Annex "F".

> Although Section 13(f) applies to sensitive personal information while the information involved in this case is just personal information, the protection of lawful rights and interests under Section 13(f) by the respondent faculty members in this case is considered as legitimate interest pursuant to Section 12(f) of the DPA.[98]

In this case, although the CCTV footage is considered as personal information, Section 13 (f) is applicable since the processing of the CCTV is pursued under a legitimate interest for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims of Spouses JM and PM.

Moreover, in NPC 21-031, the Commission ruled:

> The phrase 'for the protection of lawful rights and interests of natural or legal persons in court proceedings' cannot be interpreted to relate only to the person asserting the lawful basis of the processing of personal information. It also contemplates situations where those persons whose lawful rights and interests are protected in court proceedings may not be the same individuals who processed the personal information, such as in the case of witnesses. Similarly, the next clause 'establishment, exercise or defense of legal claims' may be interpreted to refer to the legal claims of persons other than those who processed the personal information.[99]

Here, it was admitted that the CCTV footage was released after RR investigated the request and was convinced that the footage will be used in the barangay proceedings involving the dispute between EG and the Spouses JM and PM.[100] Considering that Section 13 (f) of the DPA may be invoked by persons other than those who processed the personal information, the act of RR in releasing the CCTV footage for the establishment of the defense of Spouses JM and PM in the Barangay proceeding is considered lawful processing.

---

[98] KRL vs. Trinity University of Asia, AA, MC, NCB, RG, GV, GCT, RR, MR, PB, CID Case no. 17- K-003, dated 19 November 2019.
[99] JCB vs. FRL, NPC 21-031, dated 03 March 2022
[100] Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 3.

Second, the release of the CCTV footage can be considered necessary since it is a crucial piece of evidence to prove the defense of the spouses in the barangay proceeding. It is not shown that there were other means to support their defenses other than the CCTV footage.

Lastly, there is no substantial evidence to show that the fundamental rights and freedom of EG have been overridden by the release of the CCTV footage. Thus, Respondent's lawful processing of EG's personal information was for the legitimate interest of Spouses JM and PM for their defense in the barangay proceedings.

In totality, not all of the elements are present to warrant a finding that the Respondents violated Section 32 of the DPA. There is a lack of substantial evidence to prove a privacy violation.

WHEREFORE, premises considered, this Commission resolves that the instant Complaint filed by EG against JI, RO, and RR is hereby **DISMISSED** for lack of merit.

SO ORDERED.

City of Pasay, Philippines. 22 September 2022.

JOHN HENRY D. NAGA
Privacy Commissioner

I CONCUR:

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

EG
Complainant

LB
Counsel for Complainant

JI, RO, and RR
Respondents

DL
Counsel for Respondents

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

RGC

Complainant,

-versus-

JK INCORPORATED & RECOVERY, INC.

Respondent.

NPC 21-054

For: Violation of the Data Privacy Act of 2012

x----------x

DECISION

NAGA, *P.C.;*

Before this Commission is a Complaint filed by RGC against JK Incorporated & Recovery, Inc. (JK Incorporated) for alleged privacy violations of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 19 March 2021, the Commission, through its Complaints and Investigation Division (CID), received RGC Complaints-Assisted Form dated 25 February 2021 (CAF).[1] RGC alleged:

> MS of [JK Incorporated] – accredited agency of PSBank contacted me via phone call and sent some messages to my relatives and friends at around 11 AM on Facebook disclosing [that I have] an obligation [with] them.[2]

To support his claim, C attached a screenshot of a message purportedly from MS:

---

[1] Complaints-Assisted Form dated 25 February 2021 of RGC.
[2] *Id.* at p. 3.

> Good Day! may we ask for your assistance regarding one of your friend/colleague/relative of RGC to relay to the person to coordinate with us the soonest time possible likewise, the person may refer to all our contact details indicated herewith. Thanks and hoping for your urgent feedback. Please look for any officer of under legal counsel of JTF Tel. no. 09630498730/092072092351XXX/XXX.[3]

RGC also claimed that the message was sent to his sister, RMC to disclose his obligation to JK Incorporated.[4]

Thus, RGC argued that based on the foregoing incident, JK Incorporated violated the DPA.[5] He also prayed that damages and a fine be imposed against JK Incorporated.[6]

On 23 June 2021, JK Incorporated was ordered by the CID to file a verified comment within fifteen (15) calendar days from the receipt of the Order.[7] The same Order also stated that after the lapse of the reglementary period, the parties shall be ordered to appear for a preliminary conference.[8]

On 15 July 2021, JK Incorporated filed its Comment with Affirmative Defense/s dated 08 July 2021 praying that the complaint be dismissed for lack of cause of action and lack of merit. [9] JK Incorporated averred that RGC CAF "states no cause of action and is frivolous, vexatious and made in bad faith."[10]

JK Incorporated argued that no personal data or information of RGC was divulged to any person.[11] It further stated that the screenshot attached to the CAF "does not mention of any obligation which the Complainant alleged."[12] JK Incorporated also stated that RGC claims

---

[3] Complaints-Assisted Form dated 25 February 2021 of RGC, *See* Annex "A", Screenshot of the Message from MS.
[4] Complaints-Assisted Form dated 25 February 2021 of RGC, at p. 4.
[5] *Id.* at p. 3.
[6] *Id.*, at p. 5.
[7] *RGC v. JK Incorporated & Recovery Inc.*, NPC 21-054, Order to Comment dated 23 June 2021, at p. 1.
[8] *Id.*
[9] Comment with Affirmative Defense/s dated 08 July 2021 of JK Incorporated & Recovery Inc.
[10] *Id*, ¶ 2.
[11] *Id.* ¶ 3.
[12] *Id.* ¶ 4.

about his relatives being contacted regarding his obligation is but a
"product of his lies and/or imagination."[13]

JK Incorporated further argued that the filing by RGC of the case is "a desperate attempt on his part to evade payment of his obligation."[14]

On 12 July 2021, the parties were ordered by the CID to appear for preliminary conferences on 05 August 2021 and 18 August 2021.[15]

On 05 August 2021, an Order (After 1st Preliminary Conference held on 05 August 2021) was issued wherein both parties manifested that they were willing to undergo mediation proceedings to explore the possibility of amicable settlement.[16]

After both parties filed their Applications for Mediation,[17] the CID issued an Order to Mediate dated 09 September 2022, wherein the complaint proceedings were to be suspended for sixty (60) days for the conduct of the mediation proceedings.[18]

On 13 October 2021, a Notice of Non-Settlement of Dispute was issued for failure of the parties to reach a settlement.[19] Thereafter, on the same date, the CID issued an Order (for Resumption of Complaints Proceedings and Submission of Documents and Memoranda) ordering the parties to submit their respective Memoranda together with a list of evidence presented to prove their respective claims or defenses.[20]

C filed his Memorandum dated 25 October 2021, alleging that in 2017, he applied for a "revolving loan/Flexi loan" from PS Bank, with the loan being approved for three (3) years in a row.[21] RGC alleged that

---

[13] Comment with Affirmative Defense/s dated 15 July 2021 of JK Incorporated & Recovery Inc., ¶ 4.
[14] *Id.* ¶ 5.
[15] *RGC v. JK Incorporated & Recovery Inc.*, NPC 21-054, Order to Comment dated 12 July 2021, at p. 1.
[16] *Id.*
[17] Application for Mediation dated 09 September 2022 of RGC and Application for Mediation of JK Incorporated & Recovery Inc. dated 09 September 2022.
[18] *RGC v. JK Incorporated & Recovery Inc.*, NPC 21-054, Order to Mediated dated 09 September 2022, at p. 1.
[19] *Id.*
[20] *Id.*
[21] Memorandum (Complainant) dated 25 October 2021, ¶ 5.

during his application and the credit investigation, "the bank never asked for a list of contact reference[s] to which the bank may contact in case Complainant failed to make good his obligation."[22]

In addition, RGC alleged that in April 2020, he could no longer avail of the loan scheme.[23] The bank demanded from him the payment of his full obligation and in November 2020, he received the Statement of Account.[24]

RGC claimed that on 07 December 2020, JK Incorporated contacted him about his outstanding loan via e-mail.[25] RGC tried to reason with JK Incorporated that he could not pay the obligation and asked for more time to pay it.[26] RGC averred that throughout January and February 2021, JK Incorporated flooded him with calls to pay his obligation.[27]

On 25 February 2021, RGC alleged that his Facebook friends received a message that read:

> Good Day! may we ask for your assistance regarding one of your friend/colleague/relative of RGC to relay to the person to coordinate with us the soonest time possible likewise, the person may refer to all our contact details indicated herewith. Thanks and hoping for your urgent feedback. Please look for any officer of under legal counsel of JTF Tel. no. XXX/XXX.[28]

As a result, RGC alleged that his Facebook friends contacted him to inform him that the message is circulating among his Messenger contacts.[29] Thus, this prompted RGC to inform JK Incorporated that it was illegal to access his personal information and that the latter maliciously disclosed his information to parties who were not privy to the transaction.[30] RGC claimed that after informing JK Incorporated, "the message was suddenly 'unsent'."[31]

---

[22] *Id*, ¶ 5.
[23] *Id*, ¶ 6.
[24] *Id*, ¶ 7.
[25] Memorandum (Complainant) dated 25 October 2021, ¶ 8.
[26] *Id*, ¶ 9.
[27] *Id*, ¶ 10.
[28] *Id*, ¶ 11.
[29] Memorandum (Complainant) dated 25 October 2021, ¶ 13.
[30] *Id.*
[31] *Id.*

RGC Memorandum provided the following pieces of evidence: 1) a screenshot of the purported Facebook message subject of the complaint,[32] the affidavit of RMC,[33] and the affidavit of RC.[34] JK Incorporated's act, according to RGC, was a violation of Section 29 (Unauthorized Access or Intentional Breach)[35] and Section 31 (Malicious Disclosure)[36] of the DPA. RGC further argued that none of the circumstances in Section 12 of the DPA were present to justify the use of RGC personal information.[37]

JK Incorporated filed its Memorandum dated 29 October 2021, alleging that it was the collecting agent of PS Bank.[38] On 03 December 2020, it received an endorsement from PS Bank regarding RGC loan.[39]

According to JK Incorporated, since RGC refused to answer its calls and emails, it resorted to the practice of "skip tracing".[40] Particularly, JK Incorporated alleged that since RGC could no longer be contacted despite several messages and calls, it visited his Facebook account.[41] JK Incorporated claimed that RGC Facebook Account contained a public post with several comments.[42] One of the comments came from RMC calling RGC "Kuya" (brother), and to whom RGC responded to as "Sis".[43] JK Incorporated inferred that they were related, thus, it messaged RMC.[44]

JK Incorporated posited that instead of settling the obligation, RGC filed the subject Complaint against it.[45]

---

[32] Memorandum (Complainant) dated 25 October 2021, Annex "A".
[33] *Id*, ¶ Annex "B".
[34] *Id*, ¶ Annex "C".
[35] *Id*, ¶ 20.
[36] Memorandum (Complainant) dated 25 October 2021, ¶ 22.
[37] *Id*, ¶ 28.
[38] *Id*, at p. 2.
[39] *Id.*
[40] Memorandum of the Respondent dated 29 October 2021, at p. 3.
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] Memorandum of the Respondent dated 29 October 2021, at p. 3.
[45] Complaints-Assisted Form dated 25 February 2021 of RGC.

It argued that RGC failed to state a cause of action since the complaint failed to allege the "manner and circumstances" of the commission of the offense charged.[46]

Further, JK Incorporated argued that it could not be liable for Section 29 of the DPA (Unauthorized Access or Intentional Breach) since it should be proven that "the offender [broke] in any way into the system where personal and sensitive personal information is stored."[47] Here, JK Incorporated contended that it could not have committed unauthorized access when the information was readily and publicly available on the internet, particularly on Facebook.[48]

JK Incorporated further argued that it could not be liable for Section 32 of the DPA (Malicious Disclosure) since the message only requested to relay the message to RGC and it never mentioned his loan obligation.[49] JK Incorporated also disputed RGC allegation that it sent messages to both RMC and to RC, since RMC was the only one identified by JK Incorporated through skip tracing.[50]

Thus, JK Incorporated prayed that the RGC complaint be dismissed.[51]

Issues

Whether JK Incorporated committed a violation of the DPA.

Discussion

The Commission dismisses the Complaint.

The Commission shall first discuss the act that was allegedly a violation of the DPA. RGC does not dispute the authority of JK Incorporated to collect outstanding obligations. Indeed, in his CAF, RGC mentions that JK Incorporated was an accredited agency of PS

---

[46] Memorandum of the Respondent dated 29 October 2021, at p. 4.
[47] *Id*, at p. 7.
[48] *Id.*
[49] *Id.*
[50] Memorandum of the Respondent dated 29 October 2021, at p. 9.
[51] *Id*, at p. 10.

Bank. [52] Rather, he specifically claims that JK Incorporated's act of
contacting persons in his social media list was violative of the DPA. [53]

JK Incorporated can be considered to have engaged in the practice of skip tracing after messaging at least one person, RMC, on Facebook in order to reach RGC. To recall, the message that was sent to RMC states:

> Good Day! may we ask for your assistance regarding one of your friend/colleague/relative of RGC to relay to the person to coordinate with us the soonest time possible likewise, the person may refer to all our contact details indicated herewith. Thanks and hoping for your urgent feedback. Please look for any officer of under legal counsel of JTF Tel. no. XXX/XXX.[54]

The Commission explained the concept of skip tracing in relation to the DPA in its Advisory Opinion No. 2018-059:

> The DPA does not prohibit the collection of personal information through skip tracing or probing, provided that the collection or any further processing is done in accordance with the law. In general, processing of personal data should adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. There should be procedures in place for data subjects to exercise their rights and appropriate security measures for data protection.
>
> xxx
>
> Collection agencies are considered personal information processors (PIPs) to whom a personal information controller (PIC) has outsourced the processing of personal data of borrowers. This is due to the nature of their business, which, in general, performs the processing of personal data for the benefit of other companies. As PIPs, collection agencies are expected to process personal data only in accordance with their agreement with a PIC.[55]

Thus, though skip tracing is not prohibited, the practice still has to comply with the DPA.

---

[52] Complaints-Assisted Form dated 25 February 2021 of RGC, at p. 3.
[53] Memorandum (Complainant) dated 25 October 2021, ¶¶ 21-24.
[54] *Id*, ¶ 11.
[55] National Privacy Commission Advisory Opinion 2018-059, Skip tracing and probing of contact details through the internet and third parties, (4 October 2018).

Second, for complaints before the Commission to prosper, the burden of proof required is substantial evidence, or "that amount of relevant evidence that a reasonable mind might accept as adequate to support a conclusion." [56] The Supreme Court has explained that:

> **[T]he complainant has the burden of proving by substantial evidence the allegations in his complaint**. The basic rule is that mere allegation is not evidence and is not equivalent to proof. Charges based on mere suspicion and speculation likewise cannot be given credence. [57] (Emphasis supplied)

Thus, RGC has the burden to prove by substantial evidence that a privacy violation was committed. However, in this case, RGC provided a screenshot of an alleged Facebook message to RMC from a certain MS and an affidavit supporting the said screenshot.[58] Such cannot be considered sufficient evidence to prove that unauthorized access and malicious disclosure was committed by JK Incorporated.

The mere screenshot of a message from MS does not show that JK Incoporated actually broke into a data system where his personal or sensitive personal information is stored. Further, such screenshot does not substantiate that the disclosure was malicious or was done in bad faith or involved unwarranted or false information relative to his personal data, since the screenshot only shows a message from MS asking for assistance to relay their message to RGC.

Consequently, absent the supporting evidence that JK Incorporated indeed broke into the system and that there is malice or bad faith in the disclosure of his personal information, such allegations cannot be given credence by the Commission.

In addition, the Commission stresses, "[t]he burden to establish the charges rests upon the complainant. The case should be dismissed for lack of merit if the complainant fails to show in a satisfactory manner the facts upon which his accusations are based. The respondent is not even obliged to prove his exception or defense."[59]

---

[56] *De Jesus v. Guerrero III* , G.R. No. 171491, 04 September 2009.
[57] *Id.*
[58] Memorandum (Complainant) dated 25 October 2021, Annex "A".
[59] *National Bureau of Investigation v. Najera*, G.R. No. 237522 (Resolution), 30 June 2020.

Taken all together, RGC pieces of evidence were not sufficient to prove that a privacy violation was committed since RGC failed to establish that the message sent by JK Incorporated was violative of his data privacy rights or that its actions rose to the level of a DPA violation, as will be further discussed below.

I. JK Incorporated adhered to the general data privacy principles of transparency, legitimate purpose, and proportionality.

There is no substantial evidence to prove that JK Incorporated violated the general data privacy principles of transparency, legitimate purpose, and proportionality.[60]

The Commission notes that based on the record, RGC did not adequately discuss how JK Incorporated's actions violated the general data privacy principles. There is insufficient evidence on record to show that JK Incorporated did not adhere to the principles.

As discussed, the act of skip tracing is not *per se* prohibited. Thus, JK Incorporated's actions do not automatically mean that it was contrary to law, morals, or public policy. There is no substantial evidence to show that JK Incorporated did not provide a specific or declared purpose for its processing of personal data or that the processing was incompatible with a declared or specified purpose. The record shows that the message was sent in relation to the collection of RGC's debt. This was resorted to because RGC was not responsive in settling his obligation.[61] Debt collection is not a prohibited purpose to process personal data. As long as it complies with the relevant laws, like the DPA and related NPC issuances, the processing of personal data for debt collection is a legitimate purpose.

Here, JK Incorporated's message to RMC was straightforward in its purpose, which was to ask for assistance in contacting RGC in order

---

[60] Data Privacy Act of 2012, chapter III, § 11. *See also* National Privacy Commission, Implementing Rules and Regulations of the Data Privacy Act of 2012, rule IV, § 18 (2016) (IRR of the DPA).
[61] *See* Memorandum of the Respondent dated 29 October 2021, at p. 3; Memorandum (Complainant) dated 25 October 2021, ¶ 10.

for him to coordinate with JK Incorporated. In fact, the message did not even disclose that RGC had a loan obligation. It was just a message asking for assistance to reach C RGC.

As to transparency, JK Incorporated has been in contact[62] with RGC prior to the skip tracing and that RGC is aware of the purpose to which his personal information is being processed by the former. Also, in terms of proportionality, the screenshot shows that JK Incorporated did not disclose any information other than his name, which is relevant and necessary for JK Incorporated to identify RGC in its request for assistance from RMC. Moreover, the message to RMC is proportional and not excessive since it did not disclose excessive information such as RGC's loan obligation.

Taken all together, the prevailing circumstances do not show any violation of the general data privacy principles. Thus, given the context of debt collection and JK Incorporated's position as a collecting agent, the message to RMC was transparent, legitimate, and proportional to the purpose in collecting RGC debt.

II. JK Incorporated is not liable for Section 29 (Unauthorized Access or Intentional Breach) of the DPA.

C alleged that JK Incorporated violated Section 29 of the DPA since "he never gave any contact information of any person to...[JK Incorporated]. However, without his authority, [JK Incorporated] accessed his Friends List [on] Facebook and started messaging the said contacts [through] Facebook Messenger." [63]

Section 29 of the DPA provides:

> SEC. 29. Unauthorized Access or Intentional Breach. – The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos

---

[62] Memorandum (Complainant) dated 25 October 2021, ¶ 8.
[63] *Id*, ¶ 21.

> (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.[64]

The case of *ACN v. DT* enumerated the elements of a violation of Section 29:

> 1. The data system stores personal or sensitive personal information;
> 2. The accused breaks into the system; and
> 3. The accused knowingly and unlawfully broke into the system in a manner which violates data confidentiality and security of the same. [65]

The first element is present. Though there was no substantial discussion on whether the data system stored personal data, the Commission notes that Facebook's Privacy Policy, at the time the message was sent, states: "[w]e collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others."[66] As to managing the information, it is stated that "[w]e store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services."[67] Thus, Facebook, particularly its Messenger platform, may be considered a data system that stores personal data.

However, there is a lack of substantial evidence to prove that the second and third elements exist. RGC has not proven that JK Incorporated broke into his Facebook account or into his Messenger platform to access his contacts, much more that it did so knowingly and unlawfully.

---

[64] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter VIII, § 29 (2012).

[65] NPC 18-109, 01 June 2021.

[66] Facebook Privacy Policy, 9 September 2016, *See* "What kinds of information do we collect".

[67] *Id*, *See* "How can I manage or delete information about me".

On the contrary, JK Incorporated stated that it was able to message R by visiting RGC's Facebook Account.[68] Further, it alleged that it was able to get RMC details through the comments of RGC's public Facebook post.[69] On this note, JK Incorporated argued that there could not be unauthorized access to information when it is available "readily and publicly" on Facebook.[70]

The Commission emphasizes that the availability of personal data in the public sphere does not mean that the DPA no longer applies, given that the DPA looks into the processing of personal data, regardless of whether it is publicly available or not. As provided in NPC Advisory Opinion No. 2018-059:

> It should be clarified that the public availability of personal information does not exclude it from the scope of the DPA. This law applies to the processing of all types of personal information, publicly available or not, and to any natural and juridical person involved in personal information processing. 'Processing' in this context refers to the collection, use, storage, disposal and any other operation performed upon personal information.[71]

There was also no evidence provided that RGC fully utilized the Facebook privacy tools, or that his intention was to keep his posts private. Nevertheless, in this case, the Commission finds that between the two allegations of the parties, it is more reasonable to conclude that JK Incorporated was able to get RGC and RMC's details by searching for their respective Facebook profiles.

Thus, there is no substantial evidence to find that JK Incorporated violated Section 29 of the DPA.

III. JK Incorporated is not liable for Section 31 (Malicious Disclosure) of the DPA.

---

[68] Memorandum of the Respondent dated 29 October 2021, at p. 3.
[69] *Id.*
[70] *Id*, at p. 7.
[71] NPC Advisory Opinion 2018-059, Skip tracing and probing of contact details through the internet and third parties, (4 October 2018). *See,* DPA definition of processing in footnote.

RGC alleged that JK Incorporated violated Section 31 of the DPA since "people who were not listed by [RGC] as reference list received messages from [JK Incorporated] about the fulfillment of [RGC's obligations.]"[72]

Section 31 of the DPA provides:

> SEC. 31. Malicious Disclosure. – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one
> (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).[73]

The elements of Section 31 are:

> 1. The perpetrator is a personal information controller or a personal information processor or any of its officials, employees or agents;
> 2. The perpetrator disclosed personal or sensitive personal information;
> 3. The disclosure was made with malice or in bad faith; and
> 4. The information disclosed was unwarranted or false information.[74]

Here, JK Incorporated claimed that it is the collecting agent of PS Bank and received the endorsement of RGC's loan obligation.[75]

Section 2 (i) of the DPA provides:

> (i) *Personal information processor* refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

---

[72] Memorandum (Complainant) dated 25 October 2021, ¶ 24.
[73] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter VIII, § 31 (2012).
[74] NPC 21-015, 03 February 2022
[75] Memorandum of the Respondent dated 29 October 2021, at p. 2.

As PS Bank's collecting agent, JK Incorporated may be considered a personal information processor (PIP). PS Bank is the one who has control over RGC's information, which it outsourced to JK Incorporated in order for it to collect RGC's outstanding loan balance. Thus, the first element is present.

As to the second element, RGC alleged that:

> MS of [JK Incorporated] – accredited agency of PSBank contacted me via phone call and sent some messages to my relatives and friends at around 11 AM on Facebook disclosing [that I have] an obligation [with] them.[76]

JK Incorporated'S act of contacting the "relatives" of RGC, is considered an act of disclosure since it divulged the full name of RGCin the Facebook message. Thus, the second element is present.

However, the third and fourth elements are absent. A reading of the message does not show that JK Incorporated acted in malice or bad faith in disclosing the personal information nor that the message contained any unwarranted or false information. To quote:

> Good Day! may we ask for your assistance regarding one of your friend/colleague/relative of RGC. to relay to the person to coordinate with us the soonest time possible likewise, the person may refer to all our contact details indicated herewith. Thanks and hoping for your urgent feedback. Please look for any officer of under legal counsel of JTF Tel. no. XXX/XXX.[77]

As to the third element, the Supreme Court defined malice as one which "connotes ill will or spite and speaks not in response to duty but merely to injure the reputation of the person defamed and implies an intention to do ulterior and unjustifiable harm."[78] Meanwhile, as to bad faith, it "implies a conscious and intentional design to do a wrongful act for a dishonest purpose or some moral obliquity."[79]

---

[76] Complaints-Assisted Form dated 25 February 2021 of RGC , at p. 3.
[77] *Id.* Annex A
[78] *Delgado v. HRET*, G.R. No. 219603, 26 January 2016.
[79] *Montinola vs. Philippine Airlines*, G.R. No. 198656, 8 September 2014.

Here, RGC failed to adduce sufficient proof that JK Incorporated acted with malice or bad faith in the disclosure of his personal information. In the screenshot that RGC himself provided, the message only shows that JK Incorporated is requesting for assistance from RMC. Nowhere in the message indicates spite, ill will, or any statement to injure RGC's reputation, and does not imply any intention to do a wrongful act against him since no other information was disclosed aside from his name.

To stress, the message to RMC only disclosed RGC's full name and did not mention RGC's loan or financial obligation at all. JK Incorporated only stated that it was seeking assistance to relay to RGC the need to coordinate with the name and contact number of its representative.

JK Incorporated's message was straightforward and was a request for RGC to contact its legal counsel. Aside from RGC's full name, no other information was disclosed by JK Incorporated besides the name and contact number of its legal counsel. These circumstances are not indicative of bad faith on the part of JK Incorporated, especially given the context that RGC allegedly was no longer responsive to its messages.[80] Thus, by itself, the message cannot be considered malicious or made in bad faith.

In terms of the fourth element, there is no indication that the name involved is unwarranted or a false information since RGC did not dispute that the name involved is false and it is, in fact, his full name. Nevertheless, the Commission notes that JK Incorporated only mentioned RGC's name, and not his loan obligation. The surrounding context shows that the information disclosed was warranted since it was necessary for JK Incorporated to identify RGC in its request for assistance from R.

Considering the foregoing, the Commission finds that JK Incorporated did not violate Section 31 of the DPA since not all the elements for Malicious Disclosure are present.

---

[80] *See* Memorandum of the Respondent dated 29 October 2021, at p. 3 .*Montinola vs. Philippine Airlines*, G.R. No. 198656, 8 September 2014.

After scrutinizing the evidence and arguments of both parties, the Commission cannot find that JK Incorporated committed a privacy violation under the DPA.

WHEREFORE, premises considered, this Commission resolves that the Complaint filed by RGC against JK Incorporated & Recovery, Inc. is hereby **DISMISSED**.

SO ORDERED.

City of Pasay, Philippines.
22 September 2022.

JOHN HENRY D. NAGA
Privacy Commissioner

I CONCUR:

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

RGC
Complainant

JK INCORPORATED & RECOVERY, INC.
Respondent

JTF
Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: POPULUS LENDING CORPORATION (PESOPOP) AND ITS RESPONSIBLE OFFICERS

INITIATED AS A *SUA SPONTE* NPC INVESTIGATION ON THE POSSIBLE DATA PRIVACY VIOLATIONS COMMITTED BY POPULUS LENDING CORPORATION (PESOPOP)
x----------x

NPC SS 21-008

For: Violation of the Data Privacy Act of 2012

DECISION

AGUIRRE, *D.P.C.;*

Before this Commission is a Fact-Finding Report with Application for the Issuance of a Temporary Ban on the Processing of Personal Data (FFR) dated 10 June 2021 against Populus Lending Corporation (Pesopop), the operator of the online lending application, Pesopop, and its responsible officers.

The Complaints and Investigation Division (CID) of the National Privacy Commission (NPC), pursuant to its power to conduct *sua sponte* investigations, filed an FFR against Pesopop. The FFR alleged that Pesopop committed violations of Sections 11, 16, and 25 of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) and Section 3(D)(4) of NPC Circular 20-01 or the Guidelines on the Processing of Personal Data for Loan-Related Transactions (Loan- Related Transactions Circular).[1] This concludes the *sua sponte* investigation conducted by the NPC.

Facts

[1] Fact-Finding Report, 10 June 2021, at 13, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

On 10 June 2021, the CID submitted its FFR against Pesopop following numerous reports of continuing privacy violations committed by several online lending applications (OLAs).[2] The CID initiated a *sua sponte* investigation against Pesopop pursuant to Section 7(b) of the DPA that mandates the NPC to institute investigations in cases it deems appropriate, and NPC Circular 21-01 (2021 Rules of Procedure) that permits the NPC to initiate *sua sponte* investigations and file complaints for DPA violations.[3] The FFR serves as the complaint, with the CID as the Nominal Complainant, in *sua sponte* investigations.[4]

On 14 May 2021, the CID downloaded Pesopop (version 1.5.1) from the Google Play Store on an Android device and simulated the registration process.[5]

Upon opening the Pesopop application (app), the user must provide a mobile number as the login credential.[6] Once the user has logged in, a pop-up will appear with the following statement:

> Access permission – In order to check your credit score, you must grant permission to access Storage, Phone State, Contacts and Location info. Without these information, you can't use Pesopop.[7]

To proceed, the user must click on the "Setting" button.[8] The next pop- up messages will request access to the following: (1) device's location;
(2) device's photos, media, and files; (3) contacts stored on the device; and (4) allow the app to make and manage phone calls.[9] Each pop-up message gives the user an option to select either "DENY" or "ALLOW."[10]

When the user clicks "DENY," he or she will be taken back to the previous "Access Permission" pop-up message.[11] On the other hand, when the user selects "ALLOW," the user will be directed to the Main

---

[2] *Id.* at 1.
[3] *Id.* at 4-5.
[4] *Id.* at 5.
[5] *Id.* at 2.
[6] *Id.*
[7] Fact-Finding Report, 10 June 2021, at 2, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*

Screen, where he or she can proceed to the loan processing screen within the app.[12]

The CID stated that the request for access to the phone contacts list will appear before the loan application process starts.[13] The CID found that the loan application will not proceed to the next step without giving access to the entire phone contacts list.[14] It added that there was no manual way of entering a character reference's phone number.[15]

When the CID examined the source code of the app, it showed that the app utilized the Android software development kit (SDK) that provides coding for contacts retrieval, wherein an application will have the ability to collect data from contacts.[16] The "AndroidManifest.xml" file explicitly contained a contacts permissions line ("android.permission.READ_CONTACTS").[17] The CID explained that when this is enabled, it gives the app permission to read the user's contacts data.[18]

The CID also stated that it was "unable to locate the Terms of Service or Loan Guarantee Agreement of Pesopop from the application, or from their website."[19] Upon checking Pesopop's website, the CID, however, found Pesopop's Privacy Policy which stated the personal data collected and the purpose for which the collected information will be used:

> **The Information We Collect**
>
> To our beloved customer, to avoid fraud. When you sign up for Pesopop account, in addition to your login username and password, we will also ask for your **name, email address, birthday, gender.** Need your authorization to agree to provided **phone book**, **camera, internet, location, list of your applications and any other information.**

---

[12] *Id.*
[13] Fact-Finding Report, 10 June 2021, at 2, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.* at 3.
[18] *Id.*
[19] Fact-Finding Report, 10 June 2021, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

We also need to collect your contact information. **We will request the "Read Contacts" permission. If you agree to the authorization, we will scan and upload the contact list information** to https://api.pesopop.com:18062 using the most secure data transfer protocol (HTTPS). We will store your personal information through DES and AES encryption. Storage time will not exceed your usage time.

The data is used only for the credit review process and will not be shared with third-party organizations without your permission. We are committed to encrypting the data and ensuring the security of the information. You click on the check the box below to indicate that you are fully aware of and agree to the application. Please feel free to use. If you do not agree to the authorization, the application will stop working and will not be able to serve you. Thank you for your understanding and cooperation.

If you do not have a successful loan, the information you leave will not be leaked, and the information you provide will only be used for loan review purposes, and the information will never be used for other purposes. ***If you do not repay during the repayment period, we have the right to access and use your personal contact information, including FB, Instagram, Google+, etc.***

Pesopop will Collect and Use of Information

These clauses explain how we will use and share your information. By using the Services, you agree that we and members of Pesopop shall use Customer Information in accordance with such clauses.

Pesopop will collect your personally identifiable information when you register a Pesopop account, use other Pesopop products or services, access Pesopop webpages, or participate in promotional or prize winning games. Pesopop also collects personally identifiable information from our business partners. When you register a Pesopop account, we will ask for your name, birthday and gender, in addition to your email address. Once you are successfully registered with Pesopop, we will be able to identify you when you log in to the server.

Information Collected by Third Parties

Pesopop may allow third parties, including advertising partners, to display advertisements on the APP. These companies may use tracking technologies, including cookies, to collect information about users of the APP who view or interact with these advertisements. Pesopop does not provide Personally Identifiable Information to these third parties.

Sharing Your Personally Identifiable Information

> Pesopop may share your Personally Identifiable Information (including, without limitation, your financial account information and social security number) with Payment Partners with whom Pesopop has a business relationship.
>
> Any third parties with whom Pesopop shares Personally Identifiable Information may have their own policies which describe how they use and disclose your information. Those policies will govern the use, handling, and disclosure of your information once Pesopop has transferred or shared it with those third parties as described in this Policy or the Pesopop Terms and Conditions.
>
> Pesopop will disclose your Personally Identifiable Information in response to a subpoena or similar investigative demand, a court order, or a request for cooperation from a law enforcement agency or other government agency; to establish or exercise our legal rights; to defend against legal claims; or as otherwise required by law. Pesopop will disclose your Personally Identifiable Information when Pesopop believes disclosure is necessary to investigate, prevent, or take action regarding illegal activity, suspected fraud, or other wrongdoing; to protect and defend the rights, property, or safety of Pesopop's parent company, its employees, its website users, or others; or to enforce the Terms and Conditions or other agreements or policies.
>
> In addition, Pesopop may transfer Personally Identifiable Information to an entity acquiring all or substantially all of its parent company's stock or assets.[20]

Based on the foregoing, the CID argued that Pesopop violated Sections 11, 16, and 25 of the DPA and Section 3(D)(4) of the Loan-Related Transactions Circular.[21]

First, the CID contended that Pesopop's processing of personal information does not adhere to the general privacy principles of transparency, legitimate purpose, and proportionality.[22]

The CID stated that pursuant to the transparency principle, a data subject must be aware of the nature, purpose, and extent of processing of their personal data, including the risks and safeguards involved, the

---

[20] *Id.* at 3-4.
[21] *Id.* at 13.
[22] *Id.* at 11.

identity of the personal information controller (PIC), their rights as a data subject, and how these can be exercised.[23] It elaborated that any information and communication relating to the processing of personal data should be accessible and easy to understand, using clear and plain language.[24] It also explained that this is commonly done through a privacy notice or privacy policy.[25]

The CID argued that Pesopop's Privacy Policy failed to "sufficiently and clearly inform the data subject of the extent of the processing of his/her personal data and how he/she can exercise his/her rights as a data subject."[26]

> Here, the Pesopop Privacy Policy's multiple declarations, "to avoid fraud"; "The data is used only for the credit review process and will not be shared with third-party organizations without your permission"; and "If you do not repay during the repayment period, we have the right to access and use the (sic) your personal contact information, including FB, Instagram, Google+, etc.", are contradictory phrases that do not conform with the general privacy of transparency.[27]

On the legitimate purpose principle, the CID elaborated that the processing of information under the DPA must be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.[28] The CID explained that this principle is adhered to when there exists a lawful criterion to process personal idata, such that the processing is grounded on at least one of the criteria provided under Sections 12 and 13 of the DPA.[29]

According to the CID, the access, retention, and storage of a data subject's phone contacts are considered processing activities under the DPA, and "as such, it needs to have legitimate purpose as provided by Sections 12 and 13 of the DPA."[30] Further, where consent is the basis of the processing, expressed consent must be freely given, specific,

---

[23] *Id.* at 6.
[24] *Id.*
[25] Fact-Finding Report, 10 June 2021, at 6, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[26] *Id.* at 6-7.
[27] *Id.* at 6.
[28] *Id.* at 7.
[29] *Id.*
[30] *Id.* at 8.

informed, and indication of will.[31] Thus, for consent to be considered valid, it should be informed consent, where the information provided is accessible, clear, and easily understood.[32] The CID elaborated that bundled consent does not meet the criteria for specific consent.[33] Further, where consent is the basis for processing, data subjects can object to the processing or withdraw consent.[34]

The CID argued that Pesopop's Privacy Policy is written and presented in such a way that the data subject is not given an opportunity to make an informed choice:

> The Privacy Policy states that to avoid fraud, Pesopop "*will scan and upload the contact list information…*"; "*will store your personal information ….*"; and that in case of non-payment of debt: "*we have the right to access and use your personal contact information, including FB, Instagram, Google+, etc.*"
>
> **Pesopop's Privacy Policy initially states that the data is used only for the credit review process and will not be shared with third-party organizations without the user's permission. However, a fine reading of the said policy shows that if the user, once he/she fails to repay during the repayment period, also consents or gives Pesopop the right to access and use the user's personal contact information, including FB, Instagram, Google+, etc.** The stored personal information, including the phone contact list, are not only used to know the customer for credit review, but it will be weaponized later on for debt collection if the need arises.[35]

The CID stressed that for data subjects to avail of the services of Pesopop, "they have no choice but to accept all the terms and conditions provided by [Pesopop] and give consent for all the purposes for which [Pesopop] intends to use the personal data" because otherwise, the data subject cannot obtain a loan.[36] The CID argued that the consent was not freely given and did not serve as an indication of will of the data subjects.[37] Thus, consent was not validly acquired.[38]

---

[31] Fact-Finding Report, 10 June 2021, at 8, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.* at 8-9. Emphasis supplied.
[36] *Id.* at 9.
[37] Fact-Finding Report, 10 June 2021, at 9 *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[38] *Id.*

Further, the CID saw no other reason for Pesopop to store the data subject's contacts list throughout the duration of the loan agreement other than for use in debt collection.[39] The CID stated that Pesopop's Privacy Policy provides that "if you do not repay during the repayment period, we have the right to access and use your personal contact information, including FB, Instagram, Google+, etc."[40]

Therefore, the CID asserted that Pesopop's processing of the data subjects' personal data was unauthorized because it did not have lawful basis to store the data subjects' phone contacts list and failed to validly acquire the data subjects' consent.[41]

The CID further asserted that Pesopop's requirement that users grant Pesopop permission to access their phone contacts violates the principle of proportionality.[42] The CID explained that it is "excessive and unnecessary in fulfilling its purpose of loan or debt collection, in the event that the information provided in the credit agreement is false, invalid or otherwise not responsive to its collection attempts."[43]

Second, the CID asserted that Pesopop's requirement to grant it the "permission to access several phone capabilities, such as contacts, photos, media and files, in order to successfully install, register, and avail of its loan facilities, and failing to provide a separate interface for a user to provide character references or co-makers of his own choosing" is in violation of Section 3(D)(4) of the Loan-Related Transactions Circular.[44] According to the CID, it is explicit in the Loan- Related Transactions Circular that processing of phone contacts list for use in debt collection is strictly prohibited.[45] Further, it argued that "in all instances, online lending apps must have a separate interface where borrowers can provide character references and/or co-makers to their loan application, of their own choosing."[46]

---

[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] Fact-Finding Report, 10 June 2021, at 9, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[44] *Id.* at 10.
[45] *Id.*
[46] *Id.*

The CID reiterated that "Pesopop's processing of personal data does not adhere to the [general] privacy principles of transparency, legitimate purpose, and proportionality."[47] The CID reiterated that the access, use, and storage of the phone contact list finds no legitimate basis under the DPA.[48] Thus, there is unauthorized processing under Section 25 of the DPA.[49]

The CID further argued that since Pesopop is a corporation, "it is its board of directors who decides and should have the duty of diligence."[50] Thus, according to CID, "liability should fall upon the Board of Directors, as responsible officers, who by their gross negligence, allowed the commission of violation of the DPA."[51]

Finally, the CID interposed that there is substantial evidence to warrant the issuance of a temporary ban on the processing of personal data against Pesopop through its app:

> From the discussion above, it was shown that Pesopop's processing of personal data is without adherence to the Data Privacy Principles enshrined in the DPA. It collects personal data without clearly informing the data subject the extent by which it will use the personal data. It also has no legitimate purpose from which it can anchor its personal data processing, particularly its storage and use of phone contacts, as free and informed consent was not validly acquired and there is no other basis in law. It likewise collects and processes more personal data in relation for the purposes it has expressed in its Privacy Policy.
>
> Further, there is sufficient information to support that Pesopop has the ability to access, store, and copy phone contact lists of its borrowers and utilizes that stored data for use in debt collection or to harass its borrowers, in direct violation of the issuance of this Commission in NPC Circular 20-01, Section 3 (D) (4).
>
> Hence, the issuance of a Temporary Ban on Pesopop is crucial to preserve and protect the rights of the data subject from further processing.[52]

---

[47] *Id.* at 11.
[48] *Id.*
[49] Fact-Finding Report, 10 June 2021, at 11, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[50] *Id.* at 12.
[51] *Id.* at 11.
[52] *Id.* at 12.

On 16 June 2021, the Commission issued an Order suspending the complaint proceedings until the resolution of the application for the issuance of a temporary ban.[53] It directed Pesopop to submit a position paper on the application for the issuance of a temporary ban within ten (10) days from its receipt of the Order.[54]

On 23 June 2021, the Commission attempted to personally serve the Order to Pesopop's office address.[55] It was reported, however, that Pesopop had already moved out.[56]

On 24 June 2021, the Commission served the Order by email to Pesopop's email address available on its official website.[57] Thus, Pesopop had until 04 July 2021 to file its position paper.[58] As of 12 August 2021, the Commission did not receive any position paper from Pesopop.[59]

On 05 July 2021, the CID submitted a Supplemental Fact-Finding Report with Application for Issuance of Temporary Ban on the Processing of Personal Data, impleading specific responsible officers of Pesopop, namely RCJ, FLB, JIS, MM, and WL (collectively, individual respondents), in their official capacities as responsible officers of Pesopop in line with Section 34 of the DPA.[60]

On 12 August 2021, the Commission issued an Order granting the application for the issuance of a temporary ban against Pesopop given that all the requisites for granting a temporary ban were satisfied:

> **WHEREFORE,** premises considered, this Commission **GRANTS** the Application for Temporary Ban on the processing of personal data filed by the Complaints and Investigation Division of the National Privacy Commission. A **TEMPORARY BAN ON PROCESSING OF PERSONAL DATA** is hereby issued against Respondent Populus Lending Corporation, as the operator of the online lending application, Pesopop.

---

[53] Order, 16 June 2021, at 1, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[54] *Id.*
[55] Order, 12 August 2021, at 2, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[56] *Id.*
[57] *Id.*
[58] *Id.* at 3.
[59] *Id.*
[60] Supplemental Fact-Finding Report, 05 July 2021, at 2, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

> Further, pursuant to the ORDER FOR TEMPORARY BAN, Respondent Populus Lending Corporation shall:
>
> 1. Immediately take down its online lending application, Pesopop, to ensure that it is no longer available for download, installation or use by data subjects; and
>
> 2. Stop personal data processing activities, including those activities outsourced to third parties, where the processing operations involves use of information from the phonebook, directory, and contact list of data subjects, disclosure of false or unwarranted information, and other unduly intrusive personal data processing methods.
>
> This **TEMPORARY BAN ON THE PROCESSING OF PERSONAL DATA** shall remain in effect until the final resolution of the *sua sponte* investigation against Respondent and its responsible officers.
>
> . . .
>
> Furthermore, Respondent Populus Lending Corporation and its responsible officers are **ORDERED, within ten (10) days** from receipt of this Order, to file a **COMMENT** on the allegations in the attached Fact-Finding Report, pursuant to Section 6 of Rule X of NPC Circular No. 2021-01 (2021 NPC Rules of Procedure).[61]

On 03 September 2021, Pesopop, through its counsel Zosa & Quijano Law Offices, submitted its Notice of Entry of Appearance with Motion for Reconsideration.[62] The individual respondents also manifested that they are adopting the Motion as their comment in compliance with the Order to comment dated 12 August 2021.[63]

In its Motion for Reconsideration, Pesopop argued that the Order granting the temporary ban "is not warranted [sic] and issued with grave abuse of discretion amounting to lack or excess of jurisdiction for having been issued without authority and in violation of Sec[tion] 3, Rule 9 of the 2021 NPC Rules of Procedure."[64] It contended that the second and third requisites for the issuance of a temporary ban were absent.[65] Pesopop stated that there was no mention in the assailed

---

[61] Order, 12 August 2021, at 10-11, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[62] Notice of Entry of Appearance with Motion for Reconsideration, 03 September 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[63] *Id.* at 6.
[64] *Id.* at 3.
[65] *Id.* at 2.

Order that the required motion has been filed to warrant the application.[66] It further stated that the NPC does not have *motu proprio* authority to apply for a temporary ban because it cannot post the necessary bond required and the exemption pertains only to the payment of filing fees and not to the posting of the required bond.[67]

Alternatively, Pesopop asserted that assuming the temporary ban was valid, the complete takedown of its application is "not warranted on the ground that the temporary ban only warrants a ban on the processing of personal data."[68] It explained that a complete takedown [sic] of the application is prejudicial because that would include taking down areas not related to the processing of personal data.[69]

Further, Pesopop explained that the inclusion of a request for the phone contacts list upon registration was "purely unintentional and a result of an inadvertent and honest mistake:"

> In this case, although respondent PesoPop requested for the inclusion of the phone contact list, the said list was limited to include five (5) persons from the contact list as character reference only. In other words, respondent PesoPop does not have access to the entire the [sic] phone contact list of its clients and/or its potential users.
>
> Moreover, although it was initially stated in the terms and conditions of use that, "If you do not repay during the repayment period, we have the right to access and use the [sic] your personal contact information, including FB, Instagram, Google+, etc.", respondent PesoPop never requested any of its clients to disclose their FB, Instagram and Google+ in the collection of debts or for whatever purpose.
>
> Therefore, **respondents respectfully assert that although there could have been a mistake in the data terms and privacy of respondent PesoPop**, the latter in good faith did not use and/or was able to obtain excess information considering that the request for access of the phone contact list was limited to only five (5) numbers solely used for character reference and that respondent PesoPop follows a strict collection policy without the use of harassment and/or excess of information.[70]

---

[66] *Id.*
[67] *Id.*
[68] Notice of Entry of Appearance with Motion for Reconsideration, 03 September 2021, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[69] *Id.*
[70] *Id.* at 3-4. Emphasis supplied.

Pesopop asserted that all elements of valid consent are present in this case.[71] It argued that the consent it obtained from its clients were not bundled and were voluntarily requested as many times as the access to the information was requested.[72] It stressed that its clients and potential users will "always have a choice in giving consent to the gathering, access, processing and storage of their personal data."[73] Citing the CID's technical and supplemental reports, Pesopop argued that users of the app were asked multiple requests for access to information.[74] Absent the grant of access to such information, the users would not have any chance to provide information, use, or even obtain a loan.[75]

Pesopop added that this is its first offense for a data privacy violation.[76] It explained that it "has not received any data privacy complaint from any other party other than the instant case."[77] For this purpose, Pesopop undertook "to immediately make a complete and thorough review and amendment of its existing data privacy terms and conditions and will revise the same to conform to the DPA."[78]

Lastly, Pesopop argued that the individual respondents did not actively participate in the processing of personal data of Pesopop's clients.[79] It asserted that there was no allegation and proof in the complaint that the individual respondents acted in gross negligence, fraud, bad faith, and malice.[80]

On 17 September 2021, the Commission directed Pesopop and the individual respondents to appear for a clarificatory hearing on 28 September 2021.[81]

---

[71] *Id.* at 5.
[72] *Id.* at 4.
[73] *Id.*
[74] Notice of Entry of Appearance with Motion for Reconsideration, 03 September 2021, at 4, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[75] *Id.*
[76] *Id.* at 5.
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] Notice of Entry of Appearance with Motion for Reconsideration, 03 September 2021, at 6, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[81] Order, 17 September 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

On 28 September 2021, the Commission conducted the Clarificatory Hearing.[82] As a result of the Clarificatory Hearing, the Commission directed Pesopop and the individual respondents to submit the following information and documents:

1. Revised Privacy Policy of Pesopop;
2. Revised Terms and Conditions or Terms of Service of Pesopop;
3. Revised Pesopop application;
4. Company Profile and a discussion of the business model of the corporation;
5. An explanation of the discrepancy between Counsel's representations in the Motion for Reconsideration on the access to the phone contact list and the Privacy Policy dated 10 September 2021;
6. A technical explanation on the purpose of the code "android.permission.READ_CONTACTS", which if enabled, gives the application permission to read the user's contacts data;
7. Collection Policy of the corporation;
8. An Agreement between the corporation and its third party collection partners or agents;
9. An Agreement between the corporation and its third party payment partners;
10. An explanation behind the drafting process of the Privacy Policy dated 10 September 2021;
11. Privacy Manual; and
12. Employee Manual, particularly on the provisions governing its employees' conduct of collecting debt and collection and usage of personal information.[83]

On 20 October 2021, the Respondents filed its Motion to Admit with Compliance and submitted the following documents:

1. Revised Privacy Policy of Pesopop;
2. Revised Terms and Conditions or Terms of Service of Pesopop;
3. Revised Pesopop application;
4. Company Profile and a discussion of the business model of the corporation;
5. An explanation of the discrepancy between Counsel's representations in the Motion for Reconsideration on the access to the phone contact list and the Privacy Policy dated 10 September 2021;

---

[82] Order, 28 September 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[83] *Id.* at 2.

6. A technical explanation on the purpose of the code "android.permission.READ_CONTACTS", which if enabled, gives the application permission to read the user's contacts data;
7. Collection Policy of the corporation;
8. An Agreement between the corporation and its third party collection partners or agents;
9. An Agreement between the corporation and its third party payment partners;
10. An explanation behind the drafting process of the Privacy Policy dated 10 September 2021;
11. Privacy Manual; and
12. Employee Manual, particularly on the provisions governing its employees' conduct of collecting debt and collection and usage of personal information.[84]

Meanwhile, the Enforcement Division (EnD) of the NPC continuously monitored the availability of the app pursuant to the temporary ban.[85] The EnD confirmed that, as of 06 September 2021, the app was no longer available for download on different platforms.[86]

Despite this, during the EnD's monitoring activity on 29 October 2021, it noticed that Pesopop was once again available for download in the Google Play Store and that it was last updated on 18 October 2021 to a new version (version 1.5.4).[87] The EnD further stated that links to download the app can be found in Pesopop's official Facebook page and official website.[88]

Thus, on 08 November 2021, the EnD issued a Letter to Pesopop regarding its compliance with the Commission's Order dated 12 August 2021.[89] The EnD relayed that:

> [D]uring a monitoring activity on 29 October 2021, EnD noticed that Pesopop is again made available for download in the Google

---

[84] Motion to Admit with Compliance, 20 October 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[85] Enforcement Division Memorandum, 03 November 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[86] Letter Re: Compliance with Order dated 12 August 2021 in NPC SS 21-008 entitled *"In re: Populus Lending Corporation (Pesopop) and its Responsible Officers"*, 08 November 2021, at 2, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[87] Enforcement Division Memorandum, 03 November 2021, at 1, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[88] *Id.*
[89] Letter Re: Compliance with Order dated 12 August 2021 in NPC SS 21-008 entitled *"In re: Populus Lending Corporation (Pesopop) and its Responsible Officers"*, 08 November 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

> Play Store. Google Download Links of the mobile application can also be accessed on Pesopop's official Facebook page, through the "Use App" buttons and in its official website through the buttons "Get it on Google Play" and "Download Pesopop now."
>
> As the Temporary Ban on the Processing of Personal Data against Pesopop "shall remain in effect until the final resolution of the *sua sponte* investigation against Respondent and its responsible officers," Pesopop is instructed to **EXPLAIN** the foregoing incident within **TEN (10) days** from receipt of this letter.
>
> Populus Lending Corporation is also **ORDERED** to **IMMEDIATELY ENSURE** that Pesopop is no longer available for download, installation or use by the data subjects in any manner until the Temporary Ban is lifted.[90]

On 15 November 2021, Pesopop submitted its Reply to the EnD's letter dated 08 November 2021.[91] Pesopop stressed that it has already filed its Motion for Reconsideration to the Order dated 12 August 2021 in which it argued that the temporary ban imposed is *void ab initio*:

> In the meantime, please be advised that my client has already filed a motion for reconsideration to the order dated 12 August 2021 which is now pending for resolution. Kindly note that one of the arguments raised by my client in their motion is that the Temporary Ban imposed is *void ab initio* on the ground that the same cannot be filed *motu propio* and that the same was issued without posting the required bond. **As such, the said motion for reconsideration filed maybe treated as a motion to lift and/or cancel the temporary ban.** In other words, when the motion for reconsideration will be granted it will have the same effect of nullifying the temporary ban ordered against my client.[92]

Nevertheless, Pesopop stressed that it has already manifested to the Commission that it will comply with all its orders.[93] It explained that it has already "modified its data privacy policy, modified its app to conform to its data privacy policy and submitted other compliance documents directed to be submitted by this Honorable Commission."[94]

---

[90] *Id.* at 2.
[91] Reply to letter dated 08 November 2021, 15 November 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[92] *Id.* at 1. Emphasis supplied.
[93] *Id.*
[94] *Id.*

On 19 November 2021, the EnD once again simulated downloading the app, account registration, and attempted a loan application.[95] It found that "based on the simulations of the two (2) versions, versions 1.5.1 and 1.5.4, no evident changes were present."[96] According to the EnD "the processes were similar, and the data being requested by the forms provided are still the same."[97] The EnD observed that the permissions requested during the registration and loan application processes in both versions were also the same:

> The "AndroidManifest.xml" file of the two (2) versions were also checked for comparison. Derived from the files [ANNEX D], the dangerous permissions (Contacts, Location, Storage, Telephone and Camera) were still present in the current version 1.5.4 which is available for download to the public.[98]

On 25 November 2021, the EnD issued a second Letter to Pesopop regarding its compliance with the Order dated 12 August 2021.[99] The EnD reiterated that the temporary ban against Pesopop remains in effect until the final resolution of the main case or upon further orders by the Commission or other lawful authority.[100] The EnD explained that the Motion for Reconsideration filed by Pesopop does not in any way lift or suspend the effectivity of the temporary ban, as the case is still pending with the Commission.[101]

Further, the EnD confirmed that as of date, despite the Commission's Order, the app is still available for download, installation, and use by the data subjects, in clear violation of the Order dated 12 August 2021.[102] The EnD ordered Pesopop to "immediately ensure that Pesopop is no longer available for download, installation or use by the data subjects in any manner until the temporary ban is lifted."[103]

As of 26 November 2021, the EnD reported that the app was no longer available for download in the Google Play Store and other

---

[95] Enforcement Division Memorandum, 23 November 2021, at 1, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] Letter Re: Compliance with Order dated 12 August 2021 in NPC SS 21-008 entitled "*In re: Populus Lending Corporation (Pesopop) and its Responsible Officers*", 25 November 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*

platforms.[104] On 06 December 2021, however, the EnD found that a new version of the app (version 1.5.5) was once again made available on the Google Play Store.[105] The EnD observed that the same permissions were still present when compared to the previous versions:

> Below is a summary of the app permissions present in the different versions of Pesopop:[106]

App Permissions	Version 1.5.1 (Investigated by CID)	Version 1.5.4	Version 1.5.5	Proposed revised version from the Motion
Location	Present and required	Present and required	Present and required	Present and required
Camera	Present and required	Present and required	Present and required	Present and required
Contacts	Present and required	Present and required	Present and required	Present and required
Phone	Present and required	Present and required	Present and required	Present and required
Storage	Present and required	Present and required	Present and required	Present and required

On 28 December 2021, the EnD issued a third Letter to Pesopop regarding its compliance with the Order dated 12 August 2021.[107] The EnD stated that during its conduct of regular monitoring, it found that the app was again available for download on Google Play Store.[108] The EnD reiterated that the temporary ban against Pesopop remains in effect until the final resolution of the main case, or upon further orders by the Commission or other lawful authority.[109] It ordered the immediate take down of the app:

---

[104] Enforcement Division Memorandum, 26 November 2021, at 1, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

[105] *Id.*

[106] *Id.* at 3.

[107] Letter Re: Compliance with Order dated 12 August 2021 in NPC SS 21-008 entitled *"In re: Populus Lending Corporation (Pesopop) and its Responsible Officers"*, 28 December 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

[108] *Id.* at 2.

[109] *Id.*

> Consequently, Populus Lending Corporation is hereby, **ORDERED**, for the last time to **IMMEDIATELY TAKE DOWN** the Pesopop application from Google Play Store and ENSURE that it is no longer available for download, installation, or use by the data subjects in any manner until the Temporary Ban is lifted.
>
> Further, Pesopop is instructed to **EXPLAIN** the foregoing incident within **FIVE (5) days** from receipt of this letter. Failure to comply with these orders shall be dealt with accordingly.[110]

On 02 January 2022, Pesopop replied to the EnD and informed the latter that it already removed the app from the Google Play Store.[111] It also reiterated that the temporary ban imposed is *void ab initio* for failure to post the required bond and claimed that it exposes the Commission to liability for damages if the temporary ban is not lifted.[112] It also prayed for the resolution of the pending Motion for Reconsideration.[113]

On 27 January 2022, the Commission issued a Resolution denying the Motion for Reconsideration and maintaining the temporary ban:

> **WHEREFORE,** premises considered, the Commission **ADMITS** the compliance documents submitted by Populus Lending Corporation and its responsible officers.
>
> The Commission **DENIES** the Motion for Reconsideration and **MAINTAINS** the Temporary Ban on the processing of personal data issued against Populus Lending Corporation and its responsible officers.
>
> Further, the Commission orders Populus Lending Corporation and its responsible officers and the Complaints and Investigation Division of the National Privacy Commission to **SUBMIT within ten (10) days from the receipt of this Order** their respective Memoranda on their respective arguments on the facts and issues for the resolution of this Commission.
>
> **SO ORDERED**.[114]

---

[110] *Id.*
[111] Compliance with letter dated 28 December 2021, 02 January 2022, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[112] *Id.*
[113] *Id.*
[114] Resolution, 27 January 2022, at 17, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).

The Commission stated that Pesopop has not sufficiently addressed the reasons for the issuance of the temporary ban.[115] Pesopop continued to make the app available for download while the temporary ban was in effect.[116] In addition, Pesopop did not submit all the documents and information required by the Order dated 28 September 2021.[117] The Commission also found that Pesopop has not rectified its operations to comply with the DPA and the issuances of the Commission.[118]

On 01 March 2022, Pesopop submitted its Memorandum.[119]

Pesopop reiterated its arguments in its Motion for Reconsideration. First, Pesopop contended that the temporary ban is *void ab initio* because there is no showing that it is necessary to protect national security, or public interest, or to preserve and protect the rights of data subjects, and no posting of the required bond.[120] It argued that "the initiation of a *sua sponte* investigation is unwarranted because there was no actual or threatened violation of the rights of data subjects."[121] Pesopop stated that at the time the CID initiated its investigation, there was no complaint filed by any of its customers against its practices.[122] Thus, Pesopop contended that the CID exceeded its authority.[123]

Second, Pesopop argued that its Revised Privacy Policy complies with the general privacy principles of transparency, legitimate purpose, and proportionality.[124]

Pesopop explained that the Revised Privacy Policy "sufficiently informs the data subject of the nature, purpose, and extent of the data processing activity."[125] It provides:

> **The Revised Privacy Policy of the respondents expressly provides that personal information will be stored through DES**

---

[115] *Id.* at 9.
[116] *Id.*
[117] *Id.* at 10.
[118] *Id.* at 16.
[119] Memorandum of the Respondents, 01 March 2022, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[120] *Id.* at 6-7.
[121] *Id.* at 6.
[122] *Id.*
[123] *Id.*
[124] *Id.* at 7.
[125] Memorandum of the Respondents, 01 March 2022, at 9, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).

> **and AES encryption and will be used primarily to prevent fraud, credit risk evaluation management, debt collection, identity verification, anti-money laundering, and to ensure compliance with laws, rules, and regulations.**
>
> In addition, **the Revised Privacy Policy provides for specific and concrete instances when personal information collected by respondents, including contact details, will be used.** Specifically, contact details will be used for purposes including character reference and identification, such as instances of suspected fraud or identity theft. Hence, not only are respondents' declared purposes fully compliant with the law, but they are also clearly meant to protect the rights of the data subject.
>
> Likewise, prior versions of the respondents' Privacy Policy's failure to specify a retention period for collected data has already been rectified in the latest version of respondents' Revised Privacy Policy**, which now clearly specifies the period within which respondents can retain the information collected from the data subject.** Thus, the Revised Privacy Policy sufficiently provides the extent to which personal data is processed.[126]

Pesopop argued that its Revised Privacy Policy "expressly declares that the processing of personal information is necessary for all purposes not prohibited by applicable law."[127] It stressed that there is no law which prohibits the collection of personal data for the purpose of facilitating online lending services.[128] It states:

> **The Revised Privacy Policy also expressly provides that the purpose for collecting personal information is to facilitate the use of the service as an online lending application and other related services**, including sharing information to third-party Payment Partners to help in facilitating online payments and who third-parties are even bound by the same Privacy Policy.
>
> . . .
>
> As a matter of fact, **the respondents' declared purpose for collecting personal information is expressly regulated by the National Privacy Commission under NPC Circular 20-01 (Guidelines on Processing Personal Data for Loan-Related Transactions).** In other words, the Honorable Commission itself recognizes that the respondents' declared purpose is legitimate because the Commission has even issued rules regulating Respondents' service. Therefore, the respondents' declared

---

[126] *Id.* at 8. Emphasis supplied.
[127] *Id.* at 9.
[128] *Id.* at 10.

purpose complies with the principle that the collection of personal data must be for a legitimate purpose.[129]

Pesopop posited that its Revised Privacy Policy provides that it will only collect information that are necessary, material, and relevant in its dealings with the data subject.[130] It provides:

> A cursory reading of the respondents' Revised Privacy Policy readily shows that the respondents' access to the data subject's contact details is not being used to collect debt, much less to harass in any way the borrower or his/her contacts. On the contrary, the respondents' Revised Privacy Policy expressly provides:
>
> > **[Respondents] will request contact list limited to five (5) phone contacts for character reference purpose and identity verification.** By giving us your home and/or mobile phone number, we have your permission to contact you or the phone contacts you provided us. This shall allow us to use text messaging, artificial or prerecorded voice messages, and automatic dialing technology, for all purposes not prohibited by applicable law.
>
> In other words, **the collection of the data subject's contact list is required only when the purpose is not contrary to law, such as for the purpose of character reference and identity verification, including instances of suspected fraud or identity theft, or for the servicing the account of the data subject.** Therefore, the respondents' processing of personal information is adequate, relevant, suitable, necessary, and not excessive in relation to its declared and specified purpose.[131]

Third, Pesopop contended that the data subjects validly consented to the agreement entered into with Pesopop.[132] It argued that prior to accepting the terms and conditions, the data subject is given the opportunity to read its Privacy Policy in full.[133]

Fourth, Pesopop maintained that a temporary ban applies only against the processing of personal data.[134] Thus, according to Pesopop, the

---

[129] *Id.* Emphasis supplied.
[130] *Id.*
[131] Memorandum of the Respondents, 01 March 2022, at 11-12, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022). Emphasis supplied.
[132] *Id.* at 12.
[133] *Id.*
[134] *Id.* at 13.

Commission "acted in excess or with grave abuse discretion in issuing the temporary ban against the online lending activities of (Pesopop)":

> [A]ssuming arguendo that a Temporary Ban is proper under the circumstances, **the Temporary Ban should have only covered the data processing activities of Populus Lending Corporation and not its online lending services, such as its online lending application.** Data processing and online lending services are two activities which exist independently of each other and are entirely separate and distinct from the other. To impose a blanket ban against any other activity other than data processing is beyond the scope of the powers and authority of this Honorable Commission.[135]

Fifth, Pesopop argued that the individual respondents, as directors and officers of Pesopop, should not be held personally liable because there is no allegation that they acted with bad faith, malice, or gross negligence.[136] It interposed that the fact that the individual respondents have continuously revised the Privacy Policy to comply with the Commission's Orders negates any allegation of bad faith.[137]

Lastly, Pesopop maintained that there is no longer any legal basis for the continued imposition of the temporary ban because its Revised Privacy Policy already complies with all the principles of proper data collection:

> **Firstly, the Revised Privacy Policy sufficiently informs the data subjects of the nature, purpose, and extent of the data processing activity.** The data subject is given the opportunity to read in full the Privacy Policy prior to accepting its terms and conditions. The party who seeks to adhere to the agreement is free to reject it entirely.
>
> **Secondly, the Revised Privacy Policy expressly declares that the processing of personal information is necessary for all purposes not prohibited by applicable law.** The declared purpose in collecting personal information for online lending application is not prohibited by law, morals, or public policy. There is no law which prohibits the collection of personal information for the purpose of facilitating online lending services.

---

[135] *Id.* at 13-14. Emphasis supplied.
[136] *Id.* at 15.
[137] Memorandum of the Respondents, 01 March 2022, at 15, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).

> **Lastly, the collection of personal information is not excessive because it adheres to well-defined standards in order to protect the rights of the data subject.** The collection of the data subject's contact list is required only when the purpose is not contrary to law, such as for the purpose of character reference and identity verification, including instances of suspected fraud or identity theft, or for servicing the account of the data subject.[138]

Pesopop prayed that the Commission nullify and set aside the temporary ban.[139]

On 11 March 2022, the CID filed its Memorandum.[140] It reiterated the arguments found in its FFR.[141] The CID stated that the Revised Privacy Policy submitted by Pesopop still does not conform with the principles of transparency, legitimate purpose, and proportionality.[142]

In addition, the CID argued that if found liable, the penalty shall be imposed upon the responsible officers, who by their gross negligence, allowed the commission of the violations.[143] The CID stressed that Pesopop continued to make the app available during the pendency of the temporary ban on the processing of personal information imposed upon Pesopop.[144] Further, the CID stated that based on their submissions and the EnD's findings, Pesopop has not rectified its operations to comply with the DPA, its Implementing Rules and Regulations (IRR), the Loan-Related Transactions Circular, and the lawful orders and issuances of the Commission.[145]

As to the individual respondents' liability, the CID explained that Pesopop's Board of Directors, despite their assertion that they have not actively participated in the processing of the data, have the duty to decide for the corporation, and as such, carry the duty of diligence.[146] Thus, the CID argued that "the violation of the corporation is a violation of the persons behind it, which are its officers or board."[147]

---

[138] *Id.* at 16-17. Emphasis supplied.
[139] *Id.* at 19.
[140] Memorandum, 11 March 2022, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[141] *Id.*
[142] *Id.* at 2.
[143] *Id.* at 8.
[144] *Id.* at 9.
[145] *Id.*
[146] Memorandum, 11 March 2022, at 9, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[147] *Id.*

Lastly, the CID interposed that there is sufficient legal and factual basis for the issuance of an order for a permanent ban on processing of personal data against Pesopop for the following reasons:

> **First, Respondent willfully and deliberately violated the issuance of the Order for Temporary Ban on 12 August 2021, when Respondent still made available for download its application on several instances.**
>
> Second, despite the Respondent's assertions that it does not have any intention to violate any data privacy law, rules and regulations, issuances and will always consider the privacy rights of its customer supreme, **it failed to rectify its Privacy Policy's provisions to comply with the DPA and its IRR, and Circular 2020-01.**
>
> In light of the Respondent Corporation's continued and willful violation of the Temporary Ban issued against it during the pendency of this case, and in order to preserve and protect the rights of the Respondent's Corporation's data subject from further processing, the CID respectfully recommends for an issuance of a Permanent Ban on processing of personal data, against the Respondent Corporation.[148]

The CID prayed that the Commission find Pesopop liable for violations of Sections 11, 12, 13, 16, and 25 of the DPA.[149] Further, it prayed that the Commission find sufficient legal and factual basis for the issuance of an order for a permanent ban on processing of personal data against Pesopop.[150]

On 31 March 2022, the Commission ordered Pesopop to show cause in writing why it should not be subject to contempt proceedings for failure to comply with its Order dated 12 August 2021 within ten (10) days from receipt of the Order.[151] The Commission stated that:

> Despite repeated orders from the Commission to take down the application, the application kept re-appearing on the list of applications available for download in the Google Play Store. The

---

[148] *Id.* at 10. Emphasis supplied.
[149] *Id.*
[150] *Id.*
[151] *Id.* at 4.

> Commission stresses that this is a blatant recurring violation of the Temporary Ban against Pesopop.[152]

On the same day, the Commission directed the EnD to coordinate with Google LLC (Google), which operated Google Play, to determine the number of users who may have downloaded the app during the pendency of the temporary ban.[153]

On 28 June 2022, Pesopop, through its new counsel, Vasig Abarquez Lumauig Abarquel Puno (VAL Law), filed its Entry of Appearance with Motion for Additional Time to File Reply/Comment.[154] Pesopop requested for an additional period of ten (10) days within which to file its Reply/Comment to the Show Cause Order.[155]

On 11 July 2022, Pesopop replied to the Show Cause Order.[156] Pesopop manifested that the app was no longer available for download, installation, or use in the Google Play Store, Apple Store, and Huawei App Gallery.[157] It also reiterated its arguments from its previous submissions.[158]

With regard to its alleged recurring violations, Pesopop explained that it had no intention to violate the temporary ban and it only allowed a limited launch of the app for its existing users upon the advice of its previous counsel:

> **Respondents, upon legal advice by previous counsel, allowed a *limited* launch of the PESOPOP application for *existing* users only for purposes of processing loans of EXISTING users, especially those who had pending obligations, and avoid incurring further losses from pre-existing liabilities.** With no malicious intent to violate the Temporary Ban, Respondents only sought to ensure that EXISTING users can access the necessary information in order to fulfill their outstanding obligations. Otherwise put, new users could not have used the PESOPOP

---

[152] Order, 31 March 2022, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[153] Memorandum, 31 March 2022, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[154] Entry of Appearance with Motion for Additional Time to File Reply/Comment, 28 June 2022, *in*
In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[155] *Id.* at 3.
[156] Reply (To the Show Cause Order dated 31 March 2022), 11 July 2022, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[157] *Id.* at 8.
[158] *Id.*

> application. PESOPOP no longer processed any new information/data from new applicants in compliance with the Temporary Ban.[159]

On 28 July 2022, the Commission issued an Order to the CID and Pesopop to appear for a clarificatory hearing on the alleged Pesopop's limited launch, on 11 August 2022.[160]

On 11 August 2022, the Commission conducted the Clarificatory Hearing.[161] Pesopop, through its counsel, explained that the limited launch was only for the purposes of servicing old users, and if a new user applies, the loan application will automatically be denied.[162]

During the Clarificatory Hearing, the Commission ordered Pesopop and the individual respondents to submit the following information and documents:

1. Proof in relation the alleged process of automatically rejecting new loan applications during the "limited launch" that occurred while the Temporary Ban issued by the Commission was in effect;
2. Proof that the version of the Pesopop mobile application launched on a "limited" basis was for the sole purpose of processing payments for existing loan obligations;
3. Android Package Kit (APK) files for versions 1.5.1, 1.5.4, and 1.5.5 of the Pesopop mobile application;
4. Total number of users of the Pesopop mobile application;
5. Total number of users of the Pesopop mobile application with existing loan obligations;
6. Total number of times the Pesopop mobile application was downloaded during the "limited launch";
7. Copy of the Board Resolution of its equivalent indicating who decided to publish the Pesopop mobile application in Google Play Store and other platforms while the Temporary Ban was in effect.[163]

---

[159] *Id.* at 9. Emphasis supplied.
[160] Order, 28 July 2022, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[161] Transcript, 11 August 2022, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[162] *Id.*
[163] Order, 11 August 2022, at 1-2, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).

On 02 September 2022, Pesopop submitted its Compliance.[164] It submitted the following:

> 3.1. Video entitled "PESOPOP-NO LONGER AVAILABLE FOR NEW USERS.mp4" showing the process of automatically rejecting new loan applications, including rejecting new users, during the "limited launch" that occurred while the Temporary Ban issued by the Commission was in effect. As can be seen from the video, new applicants are not given any verification codes and will not be able to register. Specifically, those attempting to register for a new account are given a notification that states:
>
> 'We have stopped the verification code service, so the new users are unable to fill in the code and register now.'
>
> 3.2. Video entitled "PESOPOP-NO LONGER AVAILABLE FOR EXISTING USERS.mp4" showing that the version of the Pesopop mobile application launched on a "limited" basis was for the sole purpose of processing payments for existing loan obligations. The video shows, among others, that the existing user received a loan amount, the fee incurred, and the amount to be repaid or already repaid. Further, the video shows that existing users cannot even be allowed to apply for new loans. Specifically, whenever existing users attempt to apply for a new loan, the user receives the following notification immediately:
>
> 'Not supported during maintenance.'
>
> 3.3. Android Package Kit (APK) files for versions 1.5.1, 1.5.4, and 1.5.5 of the Pesopop mobile application.[165]

Pesopop also manifested that it has twenty thousand nine hundred eighteen (20,918) users in total since its inception.[166] Out of which, fifteen thousand ten (15,010) users have existing and unpaid loan obligations.[167] Pesopop added that the app was downloaded eight thousand six hundred sixty-one (8,661) times by existing users during the limited launch.[168]

Pesopop, however, was not able to submit any board resolution or document showing the approval of the "limited launch."[169] It posited that it "only automatically implemented and launched the [app] upon

---

[164] Compliance, 02 September 2022, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[165] *Id.* at 1-2.
[166] *Id.* at 2.
[167] *Id.*
[168] *Id.*
[169] *Id.*

receiving notice that they could do so from their previous counsel."[170] Then, Mr. JIS, its incorporator and director, approved and implemented the limited launch pursuant to the previous counsel's advice.[171]

On 22 September 2022, the Commission directed the EnD to evaluate the APK files that Pesopop submitted and to provide the Commission an update on the EnD's coordination with the Federal Trade Commission (FTC-USA) regarding the number of users who may have downloaded the app from Google Play Store while the temporary ban is in effect.[172]

On 16 December 2022, the FTC-USA provided the EnD with information on the number of users who may have downloaded the app from the Google Play Store during the pendency of the temporary ban.[173]

On 28 December 2022, the EnD reported to the Commission that there was a total of eighty-four thousand nine hundred seventy-eight (84,978) acquisition counts of the app from August 2021 to October 2022.[174] From this, there were seventy-three thousand four hundred five (73,405) acquisition counts during the "limited launch" or from October 2021 to December 2021.[175]

In its report, the EnD narrated that on 02 January 2022, Pesopop informed the EnD that it already removed the app from the Google Play Store.[176] Despite this confirmation, there were still approximately two hundred eighty-eight (288) acquisition counts even after its removal based on information provided by FTC-USA.[177]

---

[170] Compliance, 02 September 2022, at 2, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[171] *Id.* at 3.
[172] Endorsement of NPC SS 21-008 In re: Populus Lending Corporation (Pesopop) and its responsible officers, 22 September 2022, at 2, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[173] Letter from US Federal Trade Commission, 16 December 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[174] Supplemental Enforcement Assessment Report, 28 December 2022, at 7, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[175] *Id.*
[176] 8th Supplemental Enforcement Assessment Report, 17 May 2023, at 3 *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2023).
[177] *Id.*

On 06 January 2023, the EnD requested additional information from Google, including the download count for new users and older users (re-installed or re-downloaded the application) and versions of the app installed or acquired from August 2021 onwards.[178]

Based on the information provided by Google through FTC-USA, the EnD found that there were only forty-one thousand thirty-two (41,032) old-time users and this encompasses the number of users who have reinstalled or downloaded the app.[179] Thus, this contradicts Pesopop's claims during the Clarificatory Hearing that the alleged "limited launch" from October 2021 to December 2021 exclusively serves its users who already have existing obligations to Pesopop.[180] It also reiterated that Pesopop blatantly uploaded versions 1.5.4 and 1.5.5 during the pendency of the temporary ban.[181]

Issues

I. Whether Pesopop committed violations of the DPA, including Unauthorized Processing of Personal Information and Sensitive Personal Information (Unauthorized Processing), and the Loan- Related Transactions Circular.

II. Whether Pesopop's violation of the DPA warrants a recommendation for prosecution.

Discussion

The Commission finds that Pesopop violated Section 25 of the DPA or Unauthorized Processing. Pesopop committed multiple violations of the DPA before and during the effectivity of the temporary ban. Pesopop willfully and deliberately violated the Commission's Order dated 12 August 2021 when it made its app available for download in several instances. Taken together, these acts are sufficient to warrant a recommendation for prosecution.

---

[178] *Id.* at 6.
[179] *Id.* at 8.
[180] *Id.*
[181] *Id.* at 9.

I. Pesopop committed violations of the DPA, including Unauthorized Processing, and the Loan-Related Transactions Circular.

A. Pesopop committed Unauthorized Processing.

Pesopop violated Section 25 of the DPA (Unauthorized Processing) when it processed personal data, including the data subjects' phone contacts list, without lawful basis under the DPA or any existing law.

Section 25 of the DPA provides:

> Section 25. *Unauthorized Processing of Personal information and Sensitive Personal information.* – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.[182]

In determining whether Unauthorized Processing occurred, three (3) elements must be established with substantial evidence:

1. The perpetrator processed the information of the data subject;
2. The information processed was personal information or sensitive personal information; and
3. The processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.[183]

All three (3) requisites are present. The circumstances, when taken together, substantially demonstrate that Pesopop processed the personal and sensitive personal information of its data subjects, particularly their phone contacts list, without lawful basis.

---

[182] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 25 (2012).
[183] In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS 21-006, 16 May 2022, at 31, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-21-006-2022.05.16-Wefund-Lending-Corporation-Decision-on-the-Main-Case-Final.pdf (last accessed 24 October 2023).

1. Pesopop processed the information of its users.

The first requisite for Unauthorized Processing is that the perpetrator processed information of the data subjects.[184]

The CID stated that Pesopop, through its app, processed the information of its users when it accessed the personal data of its users through app permissions such as READ_CONTACTS.[185]

Section 3 of the DPA defines processing as follows:

> Section 3. *Definition of Terms*. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:
>
> . . .
>
> (j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[186]

Pesopop's Privacy Policy states that Pesopop will process the personal data of its users:

> **Pesopop will Collect and Use of Information**
>
> . . .
>
> Pesopop will collect your personally identifiable information when you register a Pesopop account, use other Pesopop products or services, access Pesopop pages, or participate in promotional or prize winning games. Pesopop also collects personally identifiable information from our business partners. When you register a Pesopop account, we will ask for your name, birthday and gender, in addition to your email address. Once

---

[184] *Id.*
[185] Fact-Finding Report, 10 June 2021, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[186] Data Privacy Act of 2012, § 3 (j).

> you are successfully registered with Pesopop, we will be able to identify you when you log in to the server.[187]

Pesopop also explained that "the processing of personal data [is] only used for credit evaluation."[188] It further provided that it follows a strict collection policy.[189] It stated:

> Therefore, respondents respectfully assert that although there could have been a mistake in the data terms and privacy of respondent PesoPop, the latter in good faith did not use and/or was able to obtain excess information considering that the request for access of the phone contact list was limited to only five (5) numbers **solely used for character reference and that respondent PesoPop follows a strict collection policy without the use of harassment and/or excess of information.**[190]

Thus, it is undeniable that Pesopop indeed processed the personal data of its users and potential borrowers.

2. Pesopop processed the personal and sensitive personal information of its users.

The second requisite for Unauthorized Processing is that the information processed was personal information or sensitive personal information.[191]

The CID stated that Pesopop, through its app, collects the user's mobile number and requests for access to their storage, phone state, contacts, and location information.[192]

Pesopop's Privacy Policy also provides that it collects other information such as name, email address, birthday, and gender.[193] It states:

---

[187] Fact-Finding Report, 10 June 2021, at 3-4, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021). Emphasis supplied.
[188] Notice of Entry of Appearance with Motion for Reconsideration, 03 September 2021, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[189] *Id.* at 4.
[190] *Id.* at 4. Emphasis supplied.
[191] In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS 21-006, at 31.
[192] Fact-Finding Report, 10 June 2021, at 2, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[193] *Id.* at 3-4.

> **The Information We Collect**
>
> To our beloved customer, to avoid fraud. When you sign up for Pesopop account, in addition to your login username and password, we will also ask for your **name, email address, birthday, gender.** Need your authorization to agree to provided **phone book**, **camera, internet, location, list of your applications and any other information.**
>
> We also need to collect your contact information. We will request the "Read Contacts" permission. If you agree to the authorization, we will scan and upload the contact list information to https://api.pesopop.com:18062 using the most secure data transfer protocol (HTTPS). We will store your personal information through DES and AES encryption. Storage time will not exceed your usage time.[194]

Section 3 of the DPA defines personal and sensitive personal information as:

> Section 3. *Definition of Terms*. Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:
>
> . . .
>
> (g) Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
>
> . . .
>
> (l) Sensitive personal information refers to personal information:
>
> (1) About an individual's race, ethnic origin, marital status, **age**, color, and religious, philosophical or political affiliations;
> (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
> (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers,

---

[194] *Id.* Emphasis supplied.

previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.[195]

Undeniably, the name, gender, email address, birthday, information found in a user's storage, user's contacts, and user's location, when put together, will serve to identify a specific individual. Further, since the phone contacts list contain names and phone numbers, these may also be used to identify individuals other than the user. Thus, Pesopop processed the personal information of its users.

Further, the birthday of the user is considered sensitive personal information under Section 3 (l) of the DPA.[196] Thus, Pesopop likewise processed the sensitive personal information of its users.

Given these, Pesopop processed both personal and sensitive personal information of the users of its app, satisfying the second requisite for Unauthorized Processing.

3. Pesopop processed the personal and sensitive personal information of its users without their consent or lawful basis under the DPA or any existing law.

The third requisite is that the processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.[197]

In this case, Pesopop processed personal and sensitive personal information without lawful basis.

Pesopop claims that it processes its users' personal data following the lawful basis of consent.[198] In its Motion for Reconsideration, it argued that all the elements of valid consent are present because the consent that it obtained from its users were "not bundled and [were]

---

[195] Data Privacy Act of 2012, § 3 (g) (l). Emphasis supplied.

[196] *Id.* § 3 (l).

[197] In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS 21-006, at 31.

[198] Notice of Entry of Appearance with Motion for Reconsideration, 03 September 2021, at 5, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

voluntarily requested and provided as much time as the number of times access to information was requested."[199] Pesopop stressed that its users will "always have a choice in giving consent to the gathering, access, processing, and storage of their personal data."[200] The CID, however, contended that Pesopop did not validly obtain the consent of the users of the app.[201]

Personal information of a data subject may be processed when the data subject has given their consent to such processing.[202] Section 12 (a) of the DPA provides:

> Section 12. *Criteria for Lawful Processing of Personal Information.* The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> (a) **The data subject has given his or her consent**[.][203]

Sensitive personal information of a data subject, as a general rule, shall not be processed.[204] It is only permitted when the data subject consents to such processing or any of the other lawful criteria of processing under Section 13 of the DPA is present.[205] Section 13 (a) of the DPA allows the processing of sensitive personal information when the data subject has given their consent to the processing:

> Section 13. *Sensitive Personal Information and Privileged Information.* The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> (a) **The data subject has given his or her consent**, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing[.][206]

The DPA defines consent as follows:

---

[199] *Id.* at 4.
[200] *Id.*
[201] Fact-Finding Report, 10 June 2021, at 9 *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[202] Data Privacy Act of 2012, § 12 (a), § 13 (a).
[203] *Id.* § 12 (a). Emphasis supplied.
[204] *Id.* § 13.
[205] *Id.* § 13.
[206] *Id.* § 13 (a). Emphasis supplied.

> Section 3. *Definition of Terms*. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:
>
> . . .
>
> (b) Consent of the data subject refers to any **freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her.** Consent shall be **evidenced by written, electronic or recorded means.** It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so. [207]

Personal Information Controllers (PICs) who rely on consent as basis to process information must ensure that such consent is freely given, specific, informed, an indication of will, and evidenced by written, electronic or recorded means.[208] Absent any of these requirements, the consent given is not valid.

Consent is freely given if the data subject was given a real choice on the processing of their personal data.[209]

The CID argued that the consent was not freely given.[210] It contended that the users of the app have "no choice but to accept all the terms and conditions provided by [Pesopop] and give consent for all the purposes for which [Pesopop] intends to use the personal data" otherwise, they cannot avail of Pesopop's services.[211]

The premise of the CID's argument is wrong. As the Commission previously held, for consent to be freely given, the data subject must be given a real choice where there is no risk of deception, intimidation,

---

[207] *Id.* § 3 (b). Emphasis supplied.
[208] Data Privacy Act of 2012, § 3 (b).
[209] VVC v. CJB., NPC 19-134, 10 December 2021, at 10, *available at* https://privacy.gov.ph/wp- content/uploads/2023/05/NPC-19-134-VVC-v.-CJB-Decision-2021.12.10.pdf (last accessed 1 December 2023).
[210] Fact-Finding Report, 10 June 2021, at 9 *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[211] *Id.*

coercion or significant negative consequences if they do not consent to the processing.[212]

Freely given consent does not mean that data subjects can, in all instances, choose not to consent to the processing of their personal data and still expect to be provided the service they want from the PIC. Assuming all the purposes for processing are legitimate and necessary to provide the service sought to be availed of and the personal information collected is proportional, a PIC's denial of service to data subjects who do not consent to the processing of their personal data is valid. There is nothing in the DPA and its IRR that can be construed to prohibit this. It is a finding that the purposes are not legitimate and necessary or the information collected is not proportional that makes the processing problematic, not the denial of service if the data subject does not consent.

On the other hand, there is informed consent when the data subject is made aware of the content, manner, and purpose of processing prior to the collection of their personal data or as soon as practicable and reasonable.[213]

The CID stated that the Terms of Service or Loan Guarantee Agreement could not be found within the app.[214] The CID narrated that it only found the Privacy Policy of Pesopop after checking its website.[215]

In this case, valid consent could not have been given by the data subjects because they were not sufficiently informed of the specific nature, purpose, and extent of the processing. As the Commission previously held, uninformed consent is not valid consent.[216]

---

[212] MNLC, Inc. v. IKP, NPC 19-528, 29 October 2020, at 17, *available at* https://www.privacy.gov.ph/wp-content/uploads/2022/01/Decision_NPC-19-528-MNLC-v.- PXXX-Corporation.pdf (last accessed 04 January 2024).
[213] *See* National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule IV, § 19 (a) (3) (2016).
[214] Fact-Finding Report, 10 June 2021, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[215] *Id.*
[216] AMP v. HXXX Lending Technology Inc., NPC 19-621, 19 November 2020, at 6, *available at* https://www.privacy.gov.ph/wp-content/uploads/2022/01/Decision_NPC-19-621-AMP-v.- HXXX-Lending.pdf (last accessed 1 December 2023).

A reading of the Privacy Policy shows that users need to agree to provide access to their phone book, camera, location, list of their applications and any other information that Pesopop requires.[217] It states:

> Need your authorization to agree to provided **phone book, camera, internet, location, list of your applications and any other information.**
>
> We also need to collect your contact information. **We will request the "Read Contacts" permission. If you agree to the authorization, we will scan and upload the contact list information** to https://api.pesopop.com:18062 using the most secure data transfer protocol (HTTPS). We will store your personal information through DES and AES encryption. Storage time will not exceed your usage time.[218]

Further, Pesopop's Privacy Policy contained multiple declarations that were contradictory to each other.[219]

> Pesopop Privacy Policy's multiple declarations, **"to avoid fraud"; "The data is used only for the credit review process and will not be shared with third-party organizations without your permission"; and "If you do not repay during the repayment period, we have the right to access and use the (sic) your personal contact information, including FB, Instagram, Google+, etc.", are contradictory phrases that do not conform with the general privacy of transparency.** The Notice/Policy fails to sufficiently and clearly inform the data subject of the extent of the processing of his/her personal data and how he/she can exercise his/her rights as a data subject.[220]

This is a violation of the general privacy principle of transparency, which requires the PIC to ensure that the data subject is aware of the nature, purpose, and extent of the processing of their personal data.[221] The principle of transparency similarly requires that these materials be easily accessible and understandable by the data subjects and should be in clear and plain language.[222] Section 18 (a) of the IRR provides:

---

[217] Fact-Finding Report, 10 June 2021, at 3-4, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

[218] *Id.* Emphasis supplied.

[219] *Id.* at 6.

[220] *Id.* Emphasis supplied.

[221] Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 18 (a) (2016).

[222] *Id.*

> Section 18. *Principles of Transparency, Legitimate Purpose and Proportionality.* The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.
>
> a. Transparency. **The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data,** including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. **Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.**[223]

The requirement to use clear and plain language means that information should be provided in as simple a manner as possible.[224] The information should be concrete and definitive, leaving no room for different interpretations.[225] As the Commission previously held:

> The requirement to use clear and plain language does not mean using layman's terms to substitute technical words at the risk of not capturing the complex concepts they represent. Rather, this requirement means **that information should be provided in as simple a manner as possible**, avoiding sentence or language structures that are complex. **The information provided should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations** such as in the above-cited provision which uses the word 'any' several times, as well as wordings like 'including but not limited to'.[226]

Pesopop, as the PIC, should inform its users that it will process particular personal data for a specific and limited purpose.[227] In addition to the fact that Pesopop's Privacy Policy is not accessible found within the app and the information was not provided at the time the data subject was asked to consent, the statements in the Privacy Policy are contradictory, leaving room for doubt on the specific purpose for which a user's data will be processed. Initially, the Privacy Policy states that information will be collected "to avoid fraud" or used

---

[223] *Id.*
[224] *See* JRG v. CXXX Lending Corporation, NPC Case No. 19-450, 09 June 2020, at 6, *available at* https://www.privacy.gov.ph/wp-content/uploads/2022/01/Decision_NPC-19-450-JRG-v.- CXXX.pdf (last accessed 3 November 2023).
[225] In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS 21-006, at 34.
[226] *Id.* Emphasis supplied.
[227] *Id.* at 35.

only for the credit review process.[228] The Privacy Policy, however, later states that "if you do not repay during the repayment period, we have the right to access and use your personal contact information, including FB, Instagram, Google+, etc."[229]

The only explanation offered by Pesopop was that these were "purely unintentional and a result of an inadvertent and honest mistake."[230] It asserted that:

> **[A]lthough there could have been a mistake in the data terms and privacy of respondent PesoPop**, the latter in good faith did not use and/or was able to obtain excess information considering that the request for access of the phone contact list was limited to only five (5) numbers solely used for character reference and that respondent PesoPop follows a strict collection policy without the use of harassment and/or excess of information.[231]

As a result, the users or the data subjects were not able to make an informed decision on the processing of their personal data. They were not informed in a way that they could properly understand the specific nature, purpose, and extent of the processing the PIC is permitted to undertake. Thus, the consent given by the users was not informed consent.

As discussed earlier, absent any of the requirements for consent, the consent given is not valid. Because there was no informed consent, Pesopop cannot rely on consent as its lawful basis for processing the users' personal data.

The Commission takes this opportunity to emphasize that the general privacy principles continue to apply regardless of the applicable lawful basis for processing.[232]

The CID argued that "the access, retention, and storing of a data subject's phone contacts is considered a processing activity under the

---

[228] Fact-Finding Report, 10 June 2021, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[229] *Id.*
[230] Notice of Entry of Appearance with Motion for Reconsideration, 03 September 2021, at 3-4, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021). Emphasis supplied.
[231] *Id.* Emphasis supplied.
[232] *See* Data Privacy Act of 2012, § 11.

DPA, and as such, **it needs to have legitimate purpose as provided by Sections 12 and 13 of the DPA**."[233]

The CID is correct in stating that the processing of a data subject's phone contacts list needs to have basis under Section 12 or 13 of the DPA. These sections, however, refer to the lawful bases for processing personal and sensitive personal information and not to the general privacy principle of legitimate purpose.[234] As stated earlier, the general privacy principles continue to apply regardless of the applicable lawful basis for processing.[235]

The legitimate purpose principle requires that: (1) the purpose of the processing must be specified and declared to the data subject; and (2) the purpose must not be contrary to law, morals, or public policy.[236]

As discussed earlier, the first requisite of the legitimate purpose principle was not satisfied. The second requisite of the legitimate purpose principle requires the purpose to be within the limitations of the law, which should be understood to include the entire body of laws, rules, and regulations.[237] Additionally, the purpose of the processing should not go against prevailing morals or run counter to public policy. [238]

In this case, Pesopop violated the Loan-Related Transactions Circular when it requested access to the users' entire phone contacts list for debt collection and failed to provide a separate interface for them to provide character references.

The CID alleged that Pesopop accessed and stored the phone contacts list of its users in violation of the Loan-Related Transactions Circular.[239] Pesopop, in its Motion for Reconsideration, explained that:

---

[233] Fact-Finding Report, 10 June 2021, at 8, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021). Emphasis supplied.

[234] *See* Data Privacy Act of 2012, § 12-13.

[235] *Id.* § 11.

[236] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule IV, § 18 (2016).

[237] MLF v. Grab Philippines, NPC 19-142, 31 March 2022, at 8, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-19-142-MLF-v.-Grab-Philippines- 2022.03.31.-Decision.pdf (last accessed 10 January 2024).

[238] *Id.*

[239] Fact-Finding Report, 10 June 2021, at 9, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021). Emphasis supplied.

> In this case, although respondent PesoPop requested for the inclusion of the phone contact list, the **said list was limited to include five (5) persons from the contact list as character reference only.** In other words, respondent **PesoPop does not have access to the entire the phone contact list** of its clients and/or its potential users.
>
> . . .
>
> Therefore, respondents respectfully assert that **although there could have been a mistake in the data terms and privacy of respondent PesoPop, the latter in good faith did not use and/or was able to obtain excess information** considering that the request for access of the phone contact list was limited to only five (5) numbers solely used for character reference and that respondent PesoPop follows a strict collection policy without the use of harassment and/or excess of information.[240]

This explanation is insufficient and inconsistent with actual events that have led to numerous complaints filed with the NPC.

Section 3 (D) (4) of the Loan-Related Transactions Circular provides that:

> Section 3. *Guidelines*. The processing of personal data for evaluating loan applications, granting loans, collection of loans, and closure of loan accounts shall be subject to the following general guidelines:
>
> . . .
>
> D. Where online apps are used for loan processing activities, LCs, FCs, and other persons acting as such shall be prohibited from requiring unnecessary permissions that involve personal and sensitive personal information.
>
> . . .
>
> 4. **Access to contact details in whatever form**, such as but not limited to phone contact list or e-mail lists, the harvesting of social media contacts, and/or copying or otherwise saving these contacts for use in debt collection or to harass in any way the borrower or his/her contacts, are prohibited. **In all instances, online lending apps must have a separate interface where**

---

[240] Notice of Entry of Appearance with Motion for Reconsideration, at 3-4, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021). Emphasis supplied.

borrowers can provide character references and/or co-makers of their own choosing.[241]

Pesopop's processing of phone contacts lists violated the Loan-Related Transactions Circular because it required access to the users' phone contacts list and failed to provide a separate interface for character references. Thus, this violates the general privacy principle of legitimate purpose.

Further, Pesopop required access to the users' entire phone contacts list. This is not only contrary to the Loan-Related Transactions Circular but also goes against the general privacy principle of proportionality.

The proportionality principle requires that the processing must be adequate, relevant, suitable, and necessary, such that it is not excessive in relation to the declared and specified purpose.[242] As discussed in the Loan-Related Transactions Circular, online apps used for loan processing activities are prohibited from requiring unnecessary permissions which include access to contact details in whatever form.[243]

Pesopop's Privacy Policy stated that in case of non-payment during the repayment period, "[it has] the right to access and use [the user's] personal contact information, including FB, Instagram, Google+, etc."[244] This is excessive in relation to the declared purpose of avoiding fraud and loan collection. It is likewise prohibited in the Loan-Related Transactions Circular.[245]

In sum, Pesopop committed Unauthorized Processing. It processed the personal data of its users without any lawful basis under the DPA or any existing law and in violation of the general privacy principles.

B. Despite the effectivity of the temporary ban, Pesopop committed Unauthorized Processing.

---

[241] National Privacy Commission, Guidelines on the Processing of Personal Data for Loan-Related Transactions, Circular No. 01, Series of 2020 [NPC Circ. No. 20-01], § 3 (A) (14 September 2020). Emphasis supplied.

[242] Data Privacy Act of 2012, § 11 (c)(d).

[243] NPC Circ. No. 20-01, § 3 (A).

[244] Fact-Finding Report, 10 June 2021, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021). Emphasis supplied.

[245] NPC Circ. No. 20-01, § 3 (D) (4).

As argued by the CID in its Memorandum, Pesopop "willfully and deliberately violated the issuance of the Order for Temporary Ban on 12 August 2021, when Respondent still made available for download its application on several instances."[246]

While the temporary ban was in effect, the EnD, during its monitoring activities, found that a new version of the app (version 1.5.4) was available for download from the Google Play Store.[247] It was only after EnD sent two (2) letters ordering the app's immediate takedown, that the app was removed from the Google Play Store.[248] The EnD, however, on 06 December 2021, again discovered that a newer version of the app (version 1.5.5.) was available and accessible for download, prompting it to send a third letter to Pesopop.[249]

As to the first two letters it received, Pesopop mainly asserted that the temporary ban imposed upon it was *void ab initio* based on the absence of two requisites, (1) that it is necessary to protect national security, or public interest, or to preserve and protect the rights of data subjects, and (2) the posting of the required bond.[250]

As the Commission explained in its Order dated 27 January 2022, the temporary ban is valid because of the existence of undisclosed permissions that violated the data subjects' right to be informed.[251] Further, NPC, as a government agency, is exempt from filing fees and the posting of the required bond.[252] The Commission also found that Pesopop has not sufficiently addressed the reasons for the issuance of the temporary ban.[253]

As to its recurring violations, Pesopop explained that it had no intent to violate the temporary ban and that it only "allowed a limited launch

---

[246] Memorandum, 11 March 2022, at 10, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[247] 8th Supplemental Enforcement Assessment Report, 17 May 2023, at 9, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2023)
[248] *Id.* at 1.
[249] *Id.*
[250] Memorandum of the Respondents, 01 March 2022, at 6-7, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[251] Resolution, 27 January 2022, at 8, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[252] *Id.*
[253] *Id.* at 9.

of the [app] for existing users only for purposes of processing loans of existing users, especially those who had pending obligations, and avoid incurring further losses from pre-existing liabilities."[254]

Pesopop's defenses lack merit. First, intent to violate is not an element of Unauthorized Processing. Intent is completely immaterial.

Second, Pesopop explained that it only allowed a limited launch for its existing users.[255] This was, however, found to be untrue by the EnD, supported by information from Google and FTC-USA.[256] In fact, there were seventy-three thousand four hundred five (73,405) acquisition counts by new users during the "limited launch."[257] Nevertheless, the temporary ban did not distinguish between existing and new users. The temporary ban was clear in stating that:

> [P]ursuant to the ORDER FOR TEMPORARY BAN, Respondent Populus Lending Corporation shall:
>
> 1. Immediately take down its online lending application, Pesopop, to ensure that it is no longer available for download, installation or use by data subjects; and
>
> 2. **Stop personal data processing activities, including those activities outsourced to third parties, where the processing operations involves use of information from the phonebook, directory, and contact list of data subjects, disclosure of false or unwarranted information, and other unduly intrusive personal data processing methods.**[258]

Pesopop also argued that the temporary ban should only apply to processing of personal data and not to the whole app.[259] Pesopop, however, failed to delineate and provide evidence on which parts of the app did not involve the processing of personal data.

---

[254] Reply (To the Show Cause Order dated 31 March 2022), at 9, 11 July 2022, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[255] *Id.*
[256] 8th Supplemental Enforcement Assessment Report, 17 May 2023, at 8, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2023).
[257] *Id.*
[258] Order, 12 August 2021, at 10-11, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021). Emphasis supplied.
[259] Notice of Entry of Appearance with Motion for Reconsideration, 03 September 2021, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

The Commission finds that Pesopop repeatedly violated its Order dated 12 August 2021 imposing a temporary ban. Despite repeated orders from the Commission to take down the app, the app kept reappearing on the list of applications available for download in the Google Play Store.[260] While the Commission has given Pesopop several chances to explain, Pesopop's only defense was the so-called "limited launch" that was discovered to be contradictory to the findings of the EnD and the information provided by Google and FTC- USA.[261]

As earlier established, even before the imposition of the temporary ban, Pesopop processed personal data without the consent of its data subjects. It continued doing so despite the imposition of the temporary ban. Thus, without any lawful basis to process the information during the temporary ban, Pesopop likewise committed Unauthorized Processing during the effectivity of the temporary ban.

C. Pesopop's Revised Application and Privacy Policy continues to violate the DPA and the Loan-Related Transactions Circular.

Pesopop contended that it is no longer liable for violations of the DPA, its IRR, and the Commission's issuances since it has already revised its Privacy Policy to comply with the general privacy principles.[262]

As the Commission held in its Resolution dated 27 January 2022, Pesopop has not sufficiently addressed the reasons for the issuance of the temporary ban and rectified its operations to comply with the DPA, its IRR, and the Loan-Related Transactions Circular.[263]

In compliance with the Order dated 28 September 2021, Pesopop submitted its Revised Privacy Policy, Revised Terms and Conditions of Service, Revised Application, among other documents.[264]

---

[260] Order, 31 March 2022, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[261] 8th Supplemental Enforcement Assessment Report, 17 May 2023, at 8, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2023).
[262] Memorandum of the Respondents, 01 March 2022, at 7, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[263] Resolution, 27 January 2022, at 9 and 16, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[264] Motion to Admit with Compliance, 20 October 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

The EnD, however, observed that the Revised Privacy Policy does not fully abide by Section 16 of the DPA.[265] The EnD determined the following:

> [T]he revised Privacy Policy failed to:
>
> 1. discuss any methods utilized for automated access and the logic involved;
> 2. provide its contact details for except for an e-mail address: pesopop.cs@cashrocket.com.ph, which the users can use if they want to request for an update of information;
> 3. specify the retention period for data collected, except for generic terms stated like:
>   a. "Storage time will not exceed your usage time." And
>   b. "We will only keep your information for as long as we are either required to by law or as is relevant and material for the purposes for which it was collected."; and
> 4. discuss the existence of rights of data subjects, except the right to update their personal data or the right to rectify.
>
> Upon comparison of the Privacy Policies in the different versions of the app, it can be observed that the respondent made several changes from the Privacy Policy in the 1.5.1 version (the one investigated by CID) and Policies in the later versions, which are all the same. **Despite the changes, however, the revised Privacy Policy still lacks the required information mandated by the DPA and its IRR.**
>
> Further, the policy also failed to provide details on its use of profiling, automated processing, automated decision-making, or credit rating or scoring, and the categories of data considered in deciding whether to approve or disapprove a loan application. Despite informing its users that it will use the information it collects to prevent fraud, credit risk evaluation management, debt collection, identity verification, and anti-money laundering, activities that obviously involves profiling, credit rating or scoring.[266]

Pesopop argued that its Revised Privacy Policy "expressly declares that the processing of personal information is necessary for all purposes not prohibited by applicable law."[267] As discussed earlier,

---

[265] Resolution, 27 January 2022, at 11, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[266] *Id.* at 12-13. Emphasis supplied.
[267] Memorandum of the Respondents, 01 March 2022, at 9, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).

under the transparency principle, Pesopop should inform its users that it will process particular personal data for a specific and limited purpose.[268] The statement "necessary for all purposes not prohibited by applicable law" is just another way of saying that Pesopop can do anything that can legally be done under Philippine law. Being neither specific nor limited, this violates the general privacy principle of transparency.

Further, the EnD discovered that Pesopop's submissions show that the app still contains the undisclosed permissions identified in the FFR:

> **Based on the screenshots of the revised application submitted by Populus Lending Corporation, it can be deduced that the same dangerous permissions (Phone, Location, Storage and Camera) are still present.**
>
> The 'Notice' found in the application shows that the Contact list is one of the permissions needed to start the loan application. However, it was not shown in the screenshots the specific part where the application asks for the Contacts permission during the collection of information or loan application process.
>
> It can also be seen that Step 4, where the app asks for contact references based on the simulation of other versions, is missing in the attached screenshots as Step 5 is shown after Step 3. Thus, it cannot be verified whether the revised app offered a separate interface where borrowers can provide character references and/or co-makers of their own choosing as required by the NPC Circular 20-01.
>
> Further, the Division cannot verify if the revised application, which requires access to camera, turn off such permission by default, or at the very least, prompt the borrowers through appropriate means, i.e. just-in-time, pop-up notices, etc. that they may already turn off or disallow such permission as the same is no longer necessary for the operation of the application, after use during loan application or account creation.[269]

Aside from these, the EnD also found that the Revised Application still has access to the contacts list of the users of the app:

> **Consequently, it can be assessed, based on the statement made in their revised Privacy Policy, that the Revised Application**

---

[268] In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS 21-006, at 35.
[269] Resolution, 27 January 2022, at 14-15, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022). Emphasis supplied.

indeed still have access to the contacts of the user's phone, as stated:

> **We will request you to 'Read Contacts' permission. If you agree to the authorization, we will scan and upload the contact list information to https://api.pesopop.com:18062 using the most secured data transfer protocol (HTTPS).** We will store your personal information through DES and AES encryption.
>
> Storage time will not exceed your usage time.
>
> We will request contact list limited to five (5) phone contacts for character reference purpose and identity verification. **By giving us your home and/or mobile phone number, we have your permission to contact you or the phone contacts you provided us.** This shall allow us to use text messaging, artificial or pre- recorded voice messages, and automatic dialing technology, for all purposes not prohibited by applicable law. We may also send an email to any address where we reasonably believe we can contact you (include the contact list). Some of the purposes for calls and messages include suspected fraud or identity theft; obtaining information; transactions on or servicing of your account; and collecting on your account or collecting the delinquent account.

However, it was not shown in the Revised Application screenshots submitted, the supposed 'Step 4' where users will choose character reference from their phone contact list.
But, it should be noted that the app versions 1.5.4 and the 1.5.5. currently available in Google Play Store, have these features.

. . .

Clearly, the app's access to the phone contacts, though limited to five (5) contacts for character reference is a violation of the said circular, especially that the contact lists are not only for purpose of character verification but will also be used to contact them for debt collection as stated in the revised Privacy Policy:

> By giving us your home and/or mobile phone number, we have your permission **to contact you or the phone contacts you provided us.** This shall allow us to use text messaging, artificial or prerecorded voice messages, and automatic dialing technology, for all purposes not prohibited by applicable law. **We may also send an email to any address where we reasonably believe we can contact you (include the contact list).** Some of the **purposes for calls and messages include suspected fraud or identity theft;**

> **obtaining information; transactions on or servicing of your account; and collecting on your account or collecting the delinquent account.**[270]

This practice does not only violate the Loan-Related Transactions Circular but also Memorandum Circular 18, Series of 2019 of the Securities and Exchange Commission (SEC).

The SEC Memorandum Circular prohibits unfair debt collection practices of financial and lending companies.[271] Section 1(h) of the SEC Memorandum Circular states:

> Section 1. *Unfair Collection Practices.* F[inancing] C[ompanie]s, L[ending] C[ompanie]s, and T[hird] P[arty] S[ervice] P[rovider]s hired by them may resort to all reasonable and legally permissible means to collect amounts due them under the loan agreement, provided that, in the exercise of their rights and performance of their duties, they must observe good faith and reasonable conduct and refrain from engaging in unscrupulous and untoward acts. Without limiting the general application of the foregoing, the following conduct shall constitute unfair collection practices, which shall be subject to the penalties provided herein:
>
> . . .
>
> **h. Notwithstanding the borrower's consent, contacting the persons in the borrower's contact list other than those who were named as guarantors or co-makers shall also constitute unfair debt collection practice.**[272]

To reiterate, the legitimate purpose principle requires that the purpose for processing be within the limitations of the law.[273] This should be understood to include the entire body of laws, rules, and regulations, and not just the DPA, its IRR, and the Commission's issuances.[274]

Pesopop's access and use of the phone contacts list is an unfair debt collection practice, which is prohibited by the SEC Memorandum Circular. Pesopop's violation of the SEC Memorandum Circular, even

---

[270] *Id.* at 15-16. Emphasis supplied.
[271] Securities and Exchange Commission, Prohibition on Unfair Debt Collection Practices or Financing Companies (FC) and Lending Companies (LC), Memorandum Circular No. 18, Series of 2019 [SEC M.C. No. 19-18 (19 August 2019).
[272] *Id.* § 1 (h).
[273] MLF v. Grab Philippines, NPC 19-142, at 8.
[274] *Id.*

if it is an issuance from a different government agency, and the Loan- Related Transactions Circular, renders its purpose for processing as illegitimate. Thus, Pesopop's access and use of the phone contacts list go against the general privacy principle of legitimate purpose.

Given all these, despite the changes to its app and Privacy Policy, Pesopop still blatantly violated the DPA and the Loan-Related Transactions Circular.

II. Pesopop's violation of the DPA warrants a recommendation for prosecution. The penalty shall be imposed upon the responsible officers who participated in the commission of the offense.

Having established that Pesopop committed Unauthorized Processing before and during the effectivity of the temporary ban, the Commission proceeds to determine whether Pesopop's Board of Directors and corporate officers are liable based on Section 34 of the DPA.

The DPA imposes criminal penalties on specific offenses, which are imposed by courts of law after the conduct of a criminal trial.[275] Upon finding of a violation, the Commission may recommend to the Department of Justice the prosecution and imposition of penalties on the violations enumerated under the DPA.[276] These unlawful acts provided in Sections 25 to 32 are unauthorized processing of personal or sensitive personal information, processing personal or sensitive personal information for unauthorized purposes, accessing of personal or sensitive personal information, unauthorized access or intentional breach, improper disposal of personal or sensitive personal information, concealment of security breaches involving sensitive personal information, malicious disclosure, and unauthorized disclosure.[277] If the PIC or Personal Information Processor (PIP) is a juridical person, then the penalties are imposed on its responsible officers.[278]

---

[275] Data Privacy Act of 2012, §§ 25-37.
[276] *Id.* § 7 (i).
[277] *Id.* §§ 23-32.
[278] *Id.* § 34.

Corporations and other juridical entities cannot be prosecuted for crimes under Philippine law.[279] It is an established principle in criminal law that:

> Only natural persons can be the active subject [the criminal] because of the highly personal nature of the criminal responsibility.
>
> Since a felony is a punishable act or omission which produces or tends to produce a change in the external world, it follows that **only a natural person can be the active subject [the criminal] of a crime, because he alone by his act can set in motion a cause or by his inaction can make possible the completion of a developing modification in the external world.**[280]

Specific to violations committed by a corporation, the Revised Corporation Code provides that:

> Section 171. *Liability of Directors, Trustees, Officers, or Other Employees*. If the offender is a corporation, the penalty may, at the discretion of the court, be imposed upon such corporation and/or upon its directors, trustees, stockholders, members, officers, or employees **responsible for the violation or indispensable to its commission.**[281]

Jurisprudence provides that corporations have a separate and distinct personality from its officers:

> Bicol Gas is a corporation. As such, it is an entity separate and distinct from the persons of its officers, directors, and stockholders. It has been held, however, that **corporate officers or employees, through whose act, default or omission the corporation commits a crime, may themselves be individually held answerable for the crime.**[282]

Thus, as held by the Supreme Court, "[a] corporation can act only through its officers and agents, and where the business itself involves a violation of the law, the correct rule is that all who participate in it are liable."[283] Certain special laws provide for the particular officers

---

[279] *See* People v. Tan Boon Kong, G.R. L-35262 (1930).
[280] LUIS B. REYES, THE REVISED PENAL CODE CRIMINAL LAW BOOK 1 505 (2012). Emphasis removed. Emphasis supplied.
[281] An Act Providing for the Revised Corporation Code of the Philippines [Revised Corporation Code], Republic Act No. 11232, § 171 (2019). Emphasis supplied.
[282] Espiritu Jr. v. Petro Corporation, G.R. No. 170891 (2009). Emphasis supplied.
[283] People v. Tan Boon Kong, G.R. L-35262 (1930).

who shall be held responsible for corporate crimes.[284] In the DPA, this is specified in Section 34:

> Section 34. *Extent of Liability.* If the offender is a corporation, partnership or any juridical person, **the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.** If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.[285]

Therefore, Section 34 supplies the gap in Sections 25 to 32 of the DPA by specifying that the officers of erring corporations are the natural persons that may be held responsible for such violations and will be the accused in the criminal case that will be filed.[286]

As the Commission has emphasized in previous decisions, for juridical entities, a violation of Section 25 does not automatically result in a recommendation for prosecution.[287] Rather, there is a need to identify the proper responsible officers that shall be accused in the criminal case.[288]

Section 34 of the DPA explicitly states that a responsible officer can be subject to the imposable penalties in two instances: (1) participation in the commission of the crime, or (2) allowing the commission of the violation through gross negligence.[289]

The clause "who participated in, or by their gross negligence" should be viewed in relation to the acts of the responsible officers that reasonably caused the violation, without which the violation would

---

[284] JOSE R. SUNDIANG, SR. & TIMOTEO B. AQUINO, REVIEWER ON COMMERCIAL LAW 60 (2019).
[285] Data Privacy Act of 2012, § 34. Emphasis supplied.
[286] In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS 21-006, at 40.
[287] *Id.*
[288] *Id.*
[289] Data Privacy Act of 2012, § 34.

not have occurred.[290] Ultimately, however, this shall be applied on a case-to-case basis.[291]

The Commission has previously defined the phrase "participated in" as follows:

> The term "participated in," as found in Section 34 of the DPA, requires that **the responsible officers committed acts that reasonably caused the violation, without which the violation would not have occurred.** As such, the instance of "participated in" contemplates a situation wherein the officers and employees that will be recommended for prosecution are **"responsible" for and the root cause of the violation of the DPA in such a way that if they had not committed certain acts, then the violation would not have transpired.** Examples of this instance cover situations wherein the responsible officer directs the execution of the act resulting in the violation or through his acts, reasonably caused the commission of the violation without which such violation would not have occurred. Thus, a sense of causation is essential when determining if the responsible officers may be held liable based on participation.[292]

Given these, the first ground or "participation in the commission of the crime" has three elements:

1. There is an act that reasonably caused the violation;
2. The violation would not have occurred without the act;
3. The person:
    a. exercised a certain degree of responsibility over the act that caused the violation; or
    b. whose actions were indispensable to the commission of the crime.[293]

In this case, individual respondents RCJ, FLB, JIS, MM, and WL, in Pesopop's Motion for Reconsideration, argued that they did not actively participate in the processing of personal data of its clients.[294] They claimed that upon discovery of the Order dated 12 August 2021, they "immediately set a meeting to discuss and instruct the management of Pesopop to immediately review and amend the data

---

[290] In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS 21-006, at 41.

[291] *Id.*

[292] *Id.* at 43-44. Emphasis supplied.

[293] *See* Revised Corporation Code, § 171; Data Privacy Act of 2012, § 34.

[294] Notice of Entry of Appearance with Motion for Reconsideration, 03 September 2021, at 5, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

privacy terms and conditions to conform to the provision of the Data Privacy Act of 2012."[295] Further, they asserted that there was no allegation nor proof of gross negligence, fraud, bad faith and malice.[296]

It can no longer be said, however, that the individual respondents, as Pesopop's officers and directors, did not participate in the commission of these violations Pesopop repeatedly violated the temporary ban by making its app available for download in several instances during the effectivity of the temporary ban.

Applying the elements discussed earlier, there were acts that caused the violation, which was making the app available for download or the "limited launch" during the effectivity of the temporary ban and the revision of the app and policies. These acts were necessary for the violation to occur. Finally, it is the officers and directors who exercised a certain degree of responsibility over the limited launch and revisions which caused the violation of the temporary ban.

First, as stated by Pesopop in its Compliance, Mr. JIS, one of the individual respondents, as incorporator and director, approved and implemented the so-called "limited launch" which it argued was the reason why the app was made available for download during the temporary ban.[297]

Second, Pesopop explained that upon discovery of the individual respondents of the Commission's Order imposing the temporary ban, they "immediately set a meeting to discuss and instruct the management of Pesopop to immediately review and amend the data privacy terms and conditions to conform to the provision of the [DPA]."[298] Pesopop also stated that the individual respondents have continuously revised the Privacy Policy to comply with the Commission's Orders.[299] As earlier established, however, the Commission found the Revised Application and Privacy Policy not only wanting but violative of the DPA and the Loan-Related Transactions Circular.

---

[295] *Id.* at 5-6.
[296] *Id.* at 6.
[297] Compliance, 02 September 2022, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[298] Notice of Entry of Appearance with Motion for Reconsideration, 03 September 2021, at 5-6, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[299] Memorandum of the Respondents, 01 March 2022, at 15, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).

These show that the individual respondents, as directors and officers of Pesopop, directed both the relaunching of the app and revision of the app and policies during the temporary ban. The only conclusion then is that they allowed the repeated violations to happen which led to the commission of Unauthorized Processing during the effectivity of the temporary ban.

Even assuming that the individual respondents did not directly participate in the commission of Unauthorized Processing, their failure to prevent these acts, given the repeated nature and gravity of the violations, is tantamount to gross negligence.

The Supreme Court has consistently defined gross negligence as:

> [N]egligence characterized by the want of even slight care, or **by acting or omitting to act in a situation where there is a duty to act, not inadvertently but willfully and intentionally,** with a conscious indifference to the consequences, insofar as other persons may be affected. It is the omission of that care that even inattentive and thoughtless men never fail to give to their own property.[300]

Despite the imposition of the temporary ban and the repeated reminders from the EnD, the app remained continuously accessible. This continuous availability demonstrates the inaction of the individual respondents, which amounts to gross negligence. Thus, they could still be held liable for Unauthorized Processing based on their gross negligence.

Given the totality of the evidence presented, the Commission finds that the present case warrants a recommendation for prosecution.

The Commission emphasizes that PICs are accountable for the protection of the personal information of individuals and for the observation of the obligations under the DPA. At the core of these obligations are the general privacy principles. Following this, any person or entity that processes information should process information only for legitimate purposes that have been made known

---

[300] Fernandez v. Office of the Ombudsman, G.R. No. 193983, 14 March 2012. Emphasis supplied.

to the data subject.[301] They should only process as much information as is needed to achieve their clearly defined and stated business purposes or to comply with the provisions of law or regulation.[302]

WHEREFORE, premises considered, this Commission:

1. **FINDS** that Respondents Populus Lending Corporation (Pesopop) and its directors and officers, namely RCJ, FLB, JIS, MM, and WL, as responsible officers, violated Section 25 of Republic Act No 10173 or the Data Privacy Act of 2012 (DPA); and

2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice and **RECOMMENDS** the prosecution of the responsible officers for Unauthorized Processing of Personal or Sensitive Personal Information under Section 25 of the DPA.

SO ORDERED.

City of Pasay, Philippines.
26 September 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

---

[301] KGR v. BB, et. al., CID 18-E-040, 12 May 2020, at 5, *available at* https://privacy.gov.ph/wp- content/uploads/2023/05/CID-18-E-040-KGR-v.-BB-et-al.-Decision-2020.05.12.pdf (last accessed 04 December 2023)
[302] *Id.*

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

VASIG ABARQUEZ LUMAUIG ABARQUEZ PUNO LAW OFFICES
Counsel for Respondents

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

AQM,

Complainant,

-versus-

PIT, NPT, and CNB.

Respondents.

x----------x

NPC 22-112

For: Violation of the Data Privacy Act of 2012

DECISION

AGUIRRE, *D.P.C.;*

Before this Commission are separate Complaints filed by AQM (Complainant) against PIT, NPT , and CNB (collectively, Respondents) for alleged violations of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

Complainant was setting up a business in Don Salvador, Negros Occidental, with IT, the father of PIT and husband of NPT.[1] She narrated that the daughters of IT invited her to stay in their house in Brgy. Taculing, Bacolod City (family house) while the house she was planning to stay in was not yet available.[2]

On 08 December 2021, Complainant claimed that when she and IT went to Boracay to meet with a potential investor, PIT allowed his mother, NPT, back into the family house.[3] Complainant explained that NPT "abandoned [her family] for several years."[4] She alleged that PIT and NPT took Complainant's personal belongings, including her car and documents containing sensitive personal information which

---

[1] Complaint-Affidavit of AQM against PIT, 25 April 2022, at 3, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).

[2] *Id.*

[3] *Id.*

[4] *Id.* at 4.

included her US Visa Application, Community Tax Certificate (CTC), and Deed of Sale for her car.[5]

Complainant further alleged that PIT gave the documents to NPT who, with assistance from Atty. CNB, used these as evidence to support the allegations in her pleadings for two cases:

1. Reply with Opposition to the Motion to Lift/Recall Temporary Protection Order in a petition for issuance of permanent protection order against IT; and
2. Complaint-Affidavit in criminal case for concubinage against Complainant.[6]

Complainant stated that the documents contained her (1) name; (2) age; (3) address; (4) email address; (5) phone number; (6) passport number; (7) social media identifiers; (8) passport number; (9) all information stated in her CTC; and (10) all information in her Safe, Swift & Smart Passage (S-PaSS).[7]

Due to the incident, Complainant filed Complaint-Affidavits dated 25 April 2022, against Respondents for violations of the DPA.[8]

Complainant alleged that the processing of the "sensitive information" contained in her documents was unfair, illegal, and purely malicious.[9]

She added that Atty. CNB should not have included the documents in any of her pleadings knowing that these were taken without the Complainant's consent and knowledge.[10]

Complainant posited that the act of the Respondents constituted a "serious breach which should be immediately acted upon since their

---

[5] *Id.* at 3-4.

[6] *Id.* at 4.

[7] Complaint-Affidavit of AQM against PIT, 25 April 2022, at 2, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).

[8] Complaint-Affidavit of AQM against PIT, 25 April 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22- 112 (NPC 2022); Complaint-Affidavit of AQM against NPT, 25 April 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022); Complaint-Affidavit of AQM against CNB, 25 April 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).

[9] Complaint-Affidavit of AQM against PIT, 25 April 2022, at 4, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).

[10] Complaint-Affidavit of AQM against CNB, 25 April 2022, at 4, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).

continuous use of this [sic] documents containing all [her] sensitive information is detrimental and harmful to [her]."[11]

Complainant prayed for the Commission to find Respondents guilty of violations of the DPA.[12] She prayed that the penalty of imprisonment and fine be imposed on Respondents.[13] She also claimed that she is entitled to damages.[14]

On 13 July 2022, the National Privacy Commission (NPC), through its Complaints and Investigation Division (CID), ordered Respondents to submit their respective comments and directed the parties to appear for a preliminary conference after the lapse of the period to file comments.[15]

On 20 July 2022, PIT submitted his Comment.[16] He explained that he was the legitimate son of IT and NPT and that he personally knew Complainant who he alleged was the mistress of his father, IT.[17]

PIT stated that Complainant and his father have been living together in the family house since September 2020.[18] He explained that the family house was his parents' conjugal home.[19] He added that his father forced his mother out of family house in the year 2015.[20]

PIT narrated that his mother wanted to return to the family house but was disallowed by his father.[21] He added that when his mother learned that Complainant and his father were leaving for Boracay, she "reclaimed her rights over the conjugal house by entering the same."[22] Because of this, PIT alleged that upon his father's return, he threatened to inflict harm on NPT which prompted her to file a civil case for the issuance of a permanent protection order.[23]

---

[11] Complaint-Affidavit of AQM against PIT, 25 April 2022, at 4, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[12] *Id.* at 5.
[13] *Id.*
[14] *Id.*
[15] Order to File Verified Comment and Appear Virtually for Preliminary Conference, 13 July 2022,
in AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[16] Comment of PIT, 20 July 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[17] *Id.* at 1.
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.* at 2.
[22] Comment of PIT, 20 July 2022, at 3, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[23] *Id.*

PIT argued that the case should be dismissed outright because Complainant had no valid cause of action against him and the other Respondents.[24]

PIT stressed that it was his mother, NPT, and not him, who recovered the documents from the family house.[25] He explained that it was NPT who discovered that Complainant left documents where she admitted that she was living or staying at the family house with IT.[26]

He added that he did not take the documents from any government office:

> That I did not take these documents from the US Embassy or the government offices concerned, neither I (sic) extracted or processed these documents from the offices concerned and in fact, I have nothing to do with these documents[.][27]

He emphasized that the documents were left by Complainant in the family house.[28]

PIT further stated that the Complainant's address does not qualify as sensitive personal information.[29] Moreover, he argued that the information falls under the exception because the DPA does not cover the "title, business address, and office telephone number of the individual."[30]

Finally, PIT concluded by stating that Complainant filed the complaint before the NPC to harass his mother and "to expunge the documents which she used in the criminal case for 'concubinage' she filed against [Complainant] and [PIT's] father."[31]

On 20 July 2022, NPT filed her Comment.[32] She explained that she is legally married to IT and begot three (3) children.[33]

---

[24] *Id.* at 5.
[25] *Id.* at 6.
[26] *Id.* at 4.
[27] *Id.* at 6.
[28] Comment of PIT, 20 July 2022, at 7, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] Comment of NPT, 20 July 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[33] *Id.* at 1.

In addition to the arguments already raised by PIT in his Comment, NPT stated that Complainant left numerous documents at the family house, including her US Visa Application, CTC, car documents, and bank transactions showing that it was IT who was paying for the amortizations of her car, among other documents.[34]

NPT explained that after confirming that Complainant and IT were living together as husband and wife, she proceeded to file a criminal case for concubinage and violation of Republic Act No. 9262 or the Anti-Violence Against Women and their Children Act of 2004 against them.[35]

She added that Complainant filed several cases against her and PIT, including a criminal case for qualified theft, but all of these were dismissed by the respective investigating prosecutors for lack of probable cause.[36] In the case for qualified theft, the investigating prosecutor stated that:

> [T]he respondents did not unlawfully acquired (sic) the possession of the personal properties of the complainant. The evidence suggests that the personal properties of the complainant, which were contained in boxes as stated in the copy of the delivery receipt attached by the complainant, were left at the [family's] house.[37]

She reiterated PIT's argument that they did not obtain the documents from the US Embassy or any government office.[38] She pointed out that Complainant left the documents at the family house.[39]

Finally, NPT argued that the documents were not the only evidence to establish the commission of the crime of concubinage.[40]

---

[34] *Id.* at 4.
[35] *Id.*
[36] *Id.* at 5, Annexes C and E.
[37] *Id.* Annex E.
[38] Comment of NPT, 20 July 2022, at 7, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[39] *Id.*
[40] *Id.* at 8.

On 20 July 2022, Atty. CNB filed her Comment.[41] She explained that NPT engaged her services sometime in December 2020 when she filed a petition for issuance of permanent protection order against IT.[42]

She argued that since the documents were found in the family house, her client, NPT, submitted them as documentary evidence for the criminal case for concubinage and the petition for issuance of permanent protection order.[43] She prayed for the dismissal of the complaint against her and the other Respondents.[44]

On 25 July 2022, the CID noted the comments and annexes of the Respondents.[45]

On 30 August 2022, Complainant submitted her Reply to Comment.[46] Complainant explained that PIT and NPT have already been separated for seven (7) years.[47] She added that it was NPT who left the family house as stated in an affidavit that she executed in another case.[48]

She further argued that the documents were not just lying around in the family house.[49] She explained that the living quarters of IT , where the documents were kept, is a different and separate structure from the house that NPT occupied.[50]

She posited that the documents were illegally obtained.[51] She stressed that Respondents had no authority to go into IT's living quarters as it was locked and not part of the main house.[52] Thus, she contended that Respondents should be held liable for a violation of Section 29 (Unauthorized Access or Intentional Breach) under the DPA.[53]

She further contended that Respondents are liable for violating Sections 31 (Malicious Disclosure) and 32 (Unauthorized Disclosure)

---

[41] *Id.* at 7.
[42] *Id.* at 2.
[43] *Id.*
[44] Comment of CNB, 20 July 2022, at 5, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[45] Order Noting Respondents Verified Comments and Annexes, 25 July 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[46] Reply to Comment, 23 August 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[47] *Id.* at 1.
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.* at 6.
[52] Reply to Comment, 23 August 2022, at 6, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[53] *Id.* at 5.

of the DPA because their use of her personal and sensitive personal information in the criminal case for concubinage was "purely malicious and unauthorized" because the case has not been heard. [54]

On 31 August 2022, the CID issued an Order noting the Reply to Comment submitted by the Complainant.[55]

On 01 September 2022, Complainant's counsel filed his Entry of Appearance.[56]

On 02 September 2022, during the Preliminary Conference, Complainant's counsel manifested that he is requesting the return of the original copies of all the documents, as well as Complainant's laptop and tablet.[57] Atty. CNB manifested that the NPC is not the proper forum to allow the return of Complainant's devices because there is a case pending before the court where the proper motion could be filed.[58] Further, Respondents denied having the documents in their possession.[59]

On 05 September 2022, the CID noted the Entry of Appearance filed by Complainant's counsel and ordered the parties to submit their respective memoranda within thirty (30) calendar days from receipt of the Order.[60]

On 04 October 2022, Complainant submitted her Memorandum.[61] Aside from the allegations in her Complaint, she explained that the family house had two (2) structures.[62] The first structure was the old house where Complainant was temporarily residing, while the second structure was IT's living quarters.[63]

---

[54] *Id.* at 7.
[55] Order Noting the Complainant's Reply to Comment, 31 August 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[56] Entry of Appearance, 01 September 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[57] Order After the 1st Preliminary Conference held on 02 September 2022, Requiring the Parties to Submit their Respective Memoranda, and Cancelling the 2nd Preliminary Conference on 23 September 2022, 05 September 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[58] *Id.*
[59] *Id.* at 2.
[60] Order (After the 1st Preliminary Conference held on 02 September 2022, Requiring the Parties to Submit their Respective Memoranda, and Cancelling the 2nd Preliminary Conference on 23 September 2022) 05 September 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[61] Memorandum for the Complainant, 04 October 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22- 112 (NPC 2022).
[62] *Id.* at 2.
[63] *Id.*

She explained that before leaving for Boracay, she asked IT if she could leave her valuables, including her documents, in IT's living quarters.[64] She stated that IT's living quarters can only be opened through a digital lock and that only IT and PIT knew of the passcode.[65] She posited that PIT and NPT "intentionally breached" IT's living quarters and took her personal belongings [66]

On 06 October 2022, Respondents submitted their Memorandum.[67]

On 12 October 2022, Complainant filed a Manifestation with Motion to Quash Memoranda of Respondents, stating that Respondents filed their Memorandum out of time.[68] The Motion, however, was denied by the CID in the interest of substantial justice.[69]

Issue

Whether Respondents violated Section 25 of the DPA when they processed Complainant's documents.

Discussion

The Commission dismisses the case for lack of merit.

Section 25 of the DPA provides:

> Section 25. *Unauthorized Processing of Personal information and Sensitive Personal Information*. (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent

---

[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] Memorandum for the Respondent, 05 October 2022, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[68] Order Denying the Complainant's Manifestation with Motion to Quash Memoranda of Respondents, 19 October 2022, at 3, in AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[69] Id.

> of the data subject, or without being authorized under this Act or any existing law;[70]

In determining whether Unauthorized Processing occurred, three (3) elements must be established with substantial evidence:

1. The perpetrator processed the information of the data subject;
2. The information processed was personal information or sensitive personal information; and
3. The processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.[71]

1. Respondents processed the information of Complainant.

The first requisite for Unauthorized Processing is that the perpetrator processed information of the data subject.

Complainant stated that Respondents processed her information when they used her documents in a petition for issuance of permanent protection order and in a criminal case for concubinage.[72]

Section 3 of the DPA defines processing as follows:

> Section 3. *Definition of Terms*. Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:
>
> . . .
>
> (j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[73]

---

[70] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 25 (2012).
[71] In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS 21-006, 16 May 2022, at 31, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-21-006-2022.05.16-Wefund-Lending-Corporation-Decision-on-the-Main-Case-Final.pdf (06 May 2024).
[72] Complaint-Affidavit of AQM against PIT, 25 April 2022, at 4, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[73] Data Privacy Act of 2012, § 3 (j).

In this case, Respondents processed the personal data of Complainant in two instances: (1) when Respondents PIT and NPT obtained the documents from the family house; and (2) when Respondents subsequently used these documents as evidence to support their allegations in the petition for issuance of permanent protection order and criminal case for concubinage. These two acts are considered processing of personal data. Thus, Respondents processed Complainant's personal data, satisfying the first requisite for Unauthorized Processing.

2. Respondents processed Complainant's personal and sensitive information.

The second requisite for Unauthorized Processing is that the information processed was personal information or sensitive personal information.[74]

Complainant stated that the documents obtained and used by the Respondents contained her (1) name; (2) age; (3) address; (4) email address; (5) phone number; (6) passport number; (7) social media identifiers; (8) passport number; (9) all information stated in her CTC; and (10) all information in her S Pass.[75]

Section 3 of the DPA defines personal and sensitive personal information as:

> Section 3. *Definition of Terms.* Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:
>
> . . .
>
> (g) Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
>
> . . .
>
> (l) Sensitive personal information refers to personal information:

[74] In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS 21-006, at 31.
[75] Complaint-Affidavit of AQM against PIT, 25 April 2022, at 2, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).

> (1) About an individual's race, ethnic origin, **marital status, age**, color, and religious, philosophical or political affiliations;
> (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
> (3) **Issued by government agencies peculiar to an individual** which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
> (4) Specifically established by an executive order or an act of Congress to be kept classified.[76]

In this case, Respondents processed Complainant's personal information including her name, address, and contact details.[77] Respondents likewise processed Complainant's sensitive personal information in her US Visa Application including her age, marital status, and passport number.[78] Thus, the second requisite of Unauthorized Processing is likewise present.

3. Respondents processed Complainant's personal and sensitive information pursuant to Section 12(f) and Section 13(f) of the DPA.

The third requisite is that the processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.[79]

Complainant alleged that the processing of the "sensitive information" contained in her documents was unfair, illegal, and purely malicious.[80]

As discussed earlier, Respondents processed Complainant's personal data in two instances. First, when Respondents PIT and NPT obtained the documents from the family house. Second, when Respondents subsequently used these documents as evidence to support their

---

[76] Data Privacy Act of 2012, § 3 (g) (l). Emphasis supplied.
[77] Complaint-Affidavit of AQM against PIT, 25 April 2022, at 2, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[78] *Id.*
[79] In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS 21-006, at 31.
[80] Complaint-Affidavit of AQM against PIT, 25 April 2022, at 4, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).

allegations in the petition for issuance of permanent protection order and criminal case for concubinage.

In relation to the first act of processing or to Respondents obtaining the documents, there is no substantial evidence to conclude that the acquisition of the documents was unauthorized. As determined by the investigating prosecutor in resolving Complainant's criminal complaint for qualified theft against Respondents, Respondents did not unlawfully acquire Complainant's personal properties, including the documents, because the evidence showed that these "were left at the [family's] house."[81]

In addition, the evidence on record is inadequate to show that Respondents NPT and PIT did not have access to IT's living quarters. In fact, Complainant herself stated that PIT knew the passcode and had access to IT's living quarters.[82] Given this, PIT's entry to IT's living quarters was not illegal. Thus, Complainant failed to prove with substantial evidence that the acquisition of the documents was unauthorized.

On the second act of processing, Respondents argued that they submitted the documents as evidence for a petition for issuance of permanent protection order and a criminal case for concubinage .[83]

Section 13 of the DPA allows for the processing of sensitive personal information when it is necessary for the exercise or defense of legal claims:

> Section 13. *Sensitive Personal Information and Privileged Information.* The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> . . .
>
> (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the

---

[81] Comment of NPT, 20 July 2022, Annex E, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[82] Memorandum for the Complainant, 04 October 2022, at 2, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[83] Comment of CNB, 20 July 2022, at 2, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).

> **establishment, exercise or defense of legal claims**, or when provided to government or public authority.[84]

In this case, Respondents used the documents to build a case for concubinage against the Complainant.[85] Further, Respondents processed the documents to oppose the motion to lift temporary protection order in a petition for issuance of a permanent protection order.[86] This demonstrates that the processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural persons in court proceedings and the establishment of legal claims.

The Commission previously held that applying the qualifier "necessary" to the second instance in Section 13(f) serves to limit the potentially broad concept of "establishment of legal claims" consistent with the general privacy principles of legitimate purpose and proportionality.[87]

The legitimate purpose principle requires that the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.[88] This means that the processing done for the establishment of a legal claim should not be outside the limitations provided by law.[89]

In this case, the submission of the documents was in view of a criminal complaint for concubinage filed by Respondents against the Complainant and a petition for the issuance of a permanent protection order filed by Respondents against IT. The processing of the documents cannot be considered as wrongful or illegal. The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.[90]

---

[84] Data Privacy Act of 2012, § 13 (f) (l). Emphasis supplied.
[85] Complaint-Affidavit of AQM against PIT, 25 April 2022, at 4, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).
[86] *Id.*
[87] EA and TA v. EJ, EE and HC, NPC 17-018, 15 July 2019, at 8, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-17-018-EA-and-TA-v-EJ-Decision- 2019.07.15-.pdf (last accessed 07 May 2024).
[88] National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (b) (2016).
[89] EA and TA v. EJ, EE and HC, NPC 17-018, 15 July 2019, at 9.
[90] *Id.*

Further, the proportionality principle requires that processing must be adequate, relevant, suitable, and necessary, such that it is not excessive in relation to the declared and specified purpose.[91]

In this case, the documents were used to establish and support their allegations that Complainant was living or staying at the family house with IT for both the criminal case for concubinage and petition for issuance of permanent protection order.[92]

Therefore, Respondents had lawful basis to process Complainant's sensitive personal information under Section 13 (f) of the DPA.

Complainant's personal information was also processed pursuant to a lawful basis, specifically Section 12(f) of the DPA.

While Section 13(f) applies to sensitive personal information, the protection of lawful rights and interests under Section 13(f) is considered as legitimate interest pursuant to Section 12(f) of the DPA.[93] This can be understood to include the establishment of legal claims as a legitimate interest. Thus, Respondents had lawful basis under the DPA to process Complainant's personal information.

In sum, because Respondents had lawful basis to process Complainant's personal and sensitive personal information, the third requisite for Unauthorized Processing is absent. Thus, Respondents did not commit Unauthorized Processing under Section 25 of the DPA.

WHEREFORE, premises considered, the Commission resolves that the Complaint filed by AQM against PIT, NPT, and CNB is hereby **DISMISSED** for lack of merit.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases before any other forum or tribunal, if any.

SO ORDERED.

City of Pasay, Philippines.

---

[91] Data Privacy Act of 2012, § 11 (c) & (d).

[92] Comment of PIT, 20 July 2022, at 4, *in* AQM v. PIT, NPT, and CNB, NPC 22-112 (NPC 2022).

[93] KRL v. Trinity University of Asia. AA. MC, NCB. RG, GV, GCT, RR, MR, PB, CID 17-K-003. 19 November 2019, at 6, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/CID-17- K-003-KRL-v-Trinity-Decision-PSD-10Aug2020.pdf (last accessed 09 May 2024).

18 April 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

AQM
Complainant

JDL
Counsel for Complainant

PIT
Respondent

NPT
Respondent

CNB
Respondent

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

CCMC

Complainant,

-versus-

NPC Case No. 18-K-200
For: Violation of the Data Privacy Act of 2012

QUICKLEND, INC.

Respondent.

x----------x

DECISION

AGUIRRE, *D.P.C.:*

Before this Commission is a Complaint filed by Complainant CCMC against Respondent Quicklend, Inc. for an alleged violation of R.A. 10173 ("Data Privacy Act").

The Facts

The facts of this case are not disputed.

On 10 October 2018, Complainant received an email from Respondent with the subject "Early Payment Reminder."[1] It was a mass email sent by KR, an employee from Quicklend, Inc., a financing company to their clients, including Complainant:

> Greetings from Quicklend, Inc. This is to kindly remind you to maintain your loan payment amount in your payroll account which is due for Auto-Debit Deduction on October 15, 2018. Please be informed that there will be a daily P50.00 penalty fee while your Auto-Debit Deduction is unsuccessful due to insufficient funds. Thank you for your due diligence with us and helping us avoid possible collection problems and additional finance charges.[2]

Complainant noticed in the address bar that she was one among 136 recipients of the email and that one of the recipients was her manager

---

[1] Records, pp. 6-8.
[2] *Ibid.*, at p. 15.

at work.[3] The names and email addresses can be seen by all 136 recipients.[4]

On the same day, Complainant replied to the email, stating that they have breached the Data Privacy Act of 2012 as she did not authorize them to show her personal information to every one of their customers.[5]

On 11 October 2018, KR sent an email to Complainant apologizing for the email blast, which stated:

> Hi Ma'am,
>
> We apologize for what happened yesterday and I promise that this would not happen again. I also like to inform you that I'm already the one who's handling your account. Hoping for your consideration.[6]

On 30 October 2018, Complainant filed her Complaint with the National Privacy Commission[7] and sent KR a screencap of the complaint. Complainant approached the Data Protection Officer of Respondent, RBP, about the data breach.[8]

On 31 October 2018, RBP contacted Complainant over Facebook Messenger to apologize for the incident. He informed the Complainant that they imposed sanctions to the one in charge of her account and asked for understanding, asserting it was an honest mistake.[9]

On 5 November 2018, RBP emailed the Commission and explained the situation:

> Unfortunately, through excusable oversight, our staff Ms. KR, instead of placing the email addresses of our clients in the Blind Carbon Copy (BCC) portion of the email, she instead placed around one hundred thirty five (135) email addresses on the "TO" section of the mail.
>
> This is not our practice, we always place on the "Bcc:" the email addresses of our clients when we send them our reminders.

---

[3] *Ibid.*, at p. 7.
[4] *Ibid.* at p. 22.
[5] *Ibid.* at p. 15.
[6] *Ibid.* at p. 24.
[7] *Ibid.* at p. 6.
[8] *Ibid.* at p. 14.
[9] *Ibid.* at p. 27-32

> Therefore our clients, who received the email could see the other recipients. This mistake was unintentional and a mere oversight on the part of the employee.
>
> The Management convened the employees concerned who were in- charge of sending emails and took initial steps to prevent a recurrence of the incident.
>
> a. The assigned employees should be careful and circumspect in sending the email reminders, that when there are several recipients, their email addresses should be placed in the BCC portion; and
>
> b. The DPO and his team should review and recommend procedures to further enhance our data privacy procedure.
>
> c. The DPO and his team will report to Management on or before 25 November 2018 of his recommendations.[10]

On 7 November 2018, Respondent sent an email to the previous recipients of the email complained of, which stated:

> Dear Sir / Madam,
>
> We are writing to inform you of a recent incident that may affect the security of your personal information. We are providing this notice to ensure that you are aware of the incident so that you may take steps to protect your information should you feel it is appropriate to do so.[11]

On the same day, Respondent issued a memorandum of reprimand to KR, following her explanation and apology to Respondent.[12]

Arguments of the Parties

Complainant asserts in her Complaint that having her Manager as one of the recipients of this email will provide her employer, part of the financial sector, an impression that she has debts which may negatively affect her career. She stressed that she did not tell anyone about these debts, not even her family. She also states that she is worried that her personal email address and her name will be used for malicious acts in the future.[13]

---

[10] Records, p. 34.
[11] *Ibid.* at p. 39-41.
[12] *Ibid.* at p. 44.
[13] I*bid.* at p. 2.

She indicates in her Complaint that:

> I lost many hours dealing with this personal data breach, even while I am at work. I don't know what else could happen to my personal information, but it might bring identity theft or fraud against my name which I am taking very seriously.

In Complainant's letter to the Commission, received on 16 April 2019, she states that:

> On the said email, I only realized that my Manager was copied on the email. This gave her an impression that I have debts to which is critical in my career as I work in a BPO-Financial Industry. My reputation, my name and my email address was placed at risk. xxx And since I previously worked in Accenture, some acquaintances were copied on the email as these are work emails. Recently, I received an email from someone I do not know but luring and asking personal information.
>
> xxx
>
> If the Respondent would take full responsibility of this case, I would like to seek the following for breaching my personal information and damage to my reputation at work:
>
> 1. A written apology letter from Quicklend, not from their representative, admitting of the mistake they have done and explanation of process on how will they dispose my information since I am no longer their client;
> 2. Compensation on MORAL DAMAGES worth not more than Php 100, 000;
> - Threat of loss of trust and confidence of the company and my team
> - Potential threat to my work as I work in a financial industry
> - Defamation of my reputation and character was disclosed to 136 recipients of a debt reminder email.

Respondent states in their Comment that it is the company's normal practice to send routine reminders to their clients before their scheduled collection dates. They state that this is a "generic email that divulges no information other than that their payment is due for a particular collection period."[14]

In their Comment, they state that:

> In conclusion, we profusely apologize for the incident. We would like to emphasize that it was a purely clerical error and oversight. No malice

---

[14] I*bid.*, p. 13.

> was intended toward the recipients. We have already implemented measures that this will not happen again.[15]

In their Rejoinder, they stated that:

> The email blast is a gentle reminder to all clients, regardless of credit standing, and that it was not a delinquent notice that was meant to embarrass or harass and there is no personal information divulged.[16]
>
> xxx
>
> We deny the allegation that it caused moral damages because it was a purely clerical error and done in good faith. No malice was intended towards the recipients.
>
> The complainant is not entitled to any form of damages.

Issues

The issues to be resolved in this case are:

1. Whether personal information was involved; and
2. Whether there was a personal data breach.

Discussion

There was personal information involved.

Contrary to what Respondent asserts, personal information was divulged when Respondent's employee sent a mass email of an early payment reminder to 136 recipients, inadvertently copying the email addresses to the "To:" portion of the address bar, instead of "Bcc:" or blind carbon copy, as is supposed company practice.

The Data Privacy Act defines personal information as "any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."[17]

---

[15] Records, p. 15-16.
[16] Ibid. at, p. 15.
[17] R.A. 10173, Sec. 7(b).

In this case, Complainant's entry was "CCMC [email address]". Aside from this, there were other entries containing information that directly ascertained the identity of the other recipients.

The information disclosed did not just consist of the names and email addresses of respondent's clients. In some instances, the entries also contained the clients' middle names, employers, and even birthdates.

The incident is a personal data breach.

A personal data breach is defined in NPC Circular 16-03 as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed."[18]

It may be in the nature of an availability breach resulting from the loss, accidental or unlawful destruction of personal data; an integrity breach resulting from alteration of personal data or a confidentiality breach resulting from the unauthorized disclosure of or access to personal data.[19]

In this case, her name and email address, both personal information, together with the fact of her loan with Respondent, were disclosed to 135 other individuals. Respondent readily admits when they stated that the mass email placing recipients in the "To:" portion of the address bar instead of the "Bcc" portion was an inadvertence and not the company's regular practice.[20]

This admitted disclosure was not justified by Respondent under any of the lawful criteria for processing personal information under the Data Privacy Act, namely:

> (a) The data subject has given his or her consent;
>
> (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

---

[18] NPC Circular no. 16-03, dated 15 December 2018. Section 3(F).
[19] *Id.*
[20] Records, p. 13.

> (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
>
> (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
>
> (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[21]

Lacking any basis under the law, such disclosure of Complainant's personal information is considered unauthorized disclosure. This incident is in the nature of a confidentiality breach under NPC Circular 16-03.[22]

The fact that such unauthorized disclosure was a "mere oversight on the part of the employee"[23] does not relieve Respondent from the obligations provided by law and the Commission's issuances.

The Commission notes the delay of Respondent in notifying the Commission about the incident on 5 November and in notifying the affected data subjects on 7 November, despite having been informed by Complainant as early as 10 October 2018, when she replied to the email.

This is in contravention of NPC Circular 16-03 which states that the Commission and the affected data subjects shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.[24]

The 72 hour-requirement is not limited to working days, contrary to what Respondent proffers in their Comment. The intention for this period to be uninterrupted is underscored by the fact that it is stated as 72 "hours", which should not be in any way affected by holidays or weekends. Delay for notification to the Commission is only justified to the extent necessary to determine the scope of the breach, to prevent

---

[21] Data Privacy Act, Sec. 12.
[22] NPC Circular 16-03 dated 15 December 2016. Section 3 (f).
[23] Records, p. 34.
[24] NPC Circular 16-03 dated 15 December 2016. Section 17(a).

further disclosures, or to restore reasonable integrity to the information and communications system.[25] On the other hand, personal information controllers may request from the Commission either a delay in or exemption from notification of data subjects when it may hinder criminal investigation, or when it is not in the interest of the affected data subjects.[26] Such grounds were not alleged by Respondent.

The time requirement for notifying affected data subjects is meant to allow them to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.[27]

Respondents assert a supposed company practice of using blind carbon copy or "Bcc" instead of the "To" field when sending mass emails. Nevertheless, incidents such as this, and the protracted response thereto indicate Respondent's lack of policies and procedures for the data breach response team and other personnel. The guidelines issued by the Commission provide that such policies should include, among others:

1. A procedure for the timely discovery of security incidents, including the identification of person or persons responsible for regular monitoring and evaluation of security incidents;
2. Clear reporting lines in the event of a possible personal data breach, including the identification of a person responsible for setting in motion the incident response procedure, and who shall be immediately contacted in the event of a possible or confirmed personal data breach;
3. Conduct of a preliminary assessment for purpose of:
    1. Assessing, as far as practicable, the nature and scope of the personal data breach and the immediate damage
    2. Determining the need for notification of law enforcement or external expertise; and
    3. Implementing immediate measures necessary to secure any evidence, contain the security incident and restore integrity to the information and communications system;
4. Evaluation of the security incident or personal data breach as to its nature, extent and cause, the adequacy of safeguards in place, immediate and long-term damage, impact of the breach, and its potential harm and negative consequences to affected data subjects;
5. Procedures for contacting law enforcement in case the security incident or personal data breach involves possible commission of criminal acts;
6. Conduct of investigations that will evaluate fully the security incident or personal data breach;

---

[25] Id., at Sec. 17(b).
[26] Id., at Sec. 18(b).
[27] Id., at Sec. 18(a).

7. Procedures for notifying the Commission and data subjects when the breach is subject to notification requirements, in the case of personal information controllers, and procedures for notifying personal information controllers in accordance with a contract or agreement, in the case of personal information processors; and
8. Policies and procedures for mitigating the possible harm and negative consequences to a data subject in the event of a personal data breach. The personal information controller must be ready to provide assistance to data subjects whose personal data may have been compromised.[28]

The lack of such policies inevitably lead to inadvertences such as in this case. Respondent must realize the impacts of such personal data breaches to the data subjects.

WHEREFORE, all the above premises considered, the Commission hereby **ORDERS** Respondent to submit, **within thirty (30) days** from receipt of this Decision, their security incident management policy that is compliant with the guidelines stated in NPC Circular 16-03, pursuant to the undertaking in their 5 November 2018 letter to the Commission that a report to management will be made by 25 November 2018 regarding the review and recommendation of procedures by the DPO and his team.

SO ORDERED.
Pasay City, 17 January 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Concurring:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

---

[28] NPC Circular 16-03, dated 15 December 2016. Sec. 8.

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED

CCMC
Complainant

RBP
Respondent's Data Protection Officer
Quicklend, Inc.

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

JPV,

Complainant,

-

versus-

SOULEY MD SERVICES, INC.,

Respondent.

x----------x

NPC 22-201

For: Violation of the Data Privacy Act of 2012

DECISION

AGUIRRE, *D.P.C.*;

Before this Commission is a Complaint filed by JPV against Souley MD Services, Inc. (SMSI) for an alleged violation of Section 32 (Unauthorized Disclosure) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 16 December 2021, JPV suffered injuries as a result of the impact of super typhoon "Odette" that hit Southern Leyte.[1] JPV was then brought to the emergency room of Christ the Healer Hospital, an institution operated by SMSI, where Dr. JLT attended to her and sutured her shoulders.[2]

After the procedure, JPV claimed that she continuously experienced aggravated pains in her body and worsening fever, so she and her daughter CPV sought a "second opinion" from ACE Medical Center in Tacloban City.[3] At the subsequent hospital, the health care personnel commented that JPV failed to receive anti-tetanus shots and sarcastically remarked, "*mura man nagtahi og chorizo*" (the stitching was conducted as if it was a local sausage).[4]

---

[1] Complaint, 04 September 2022, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[2] *Id.*
[3] *Id.*
[4] *Id.*

Meanwhile, Dr. JLT narrated that when JPV was admitted to the Christ the Healer Hospital, immediate medical attention and suturing were conducted on her.[5] Dr. JLT recounted that the day after the medical procedure, JPV and her daughter requested to be discharged despite ongoing medication but were advised by the hospital staff to remain in the hospital for "health reasons."[6] Dr. JLT stated that JPV and CPV also offered a promissory note as a commitment to settle the outstanding hospital bills, as they are currently unable to make their payment.[7] Dr. JLT and the personnel of Christ the Healer Hospital were unaware that JPV went to ACE Medical Center for further medication.[8]

On 24 December 2021, SMSI narrated that it came across a Facebook post authored by a person named "CPV" which said:

> Hi kos ospital sa Sogod kung dis.a 1st na admit si mama after surviving the storm surge. Dia me karon sa tacloban nagpaadmit ug balik kay purya gaba inyo serbisyo sa amoa sanglit wala mi pambyad ato nga time. Naa mi pambayad oy pero gilamo2 ra ninyo tungod ky wala mi ikapakitang kwarta atong adlawa. Naa pay stiches ninyo nga murag dili professional ag nag-gama. Murag chorizo ag bukton sa ahong inahan sa iyang tahi! Ag Xray nga wa ninyo panumbalinga ang result. Nagkuha kos result ganiha, dec. 18 pami ngdischarge, unya hantod karon wa ninyo panumbalinga ag reading. Ingon ag attending nurse diri "basin nay development sa fracture sa tuhod sa inyo mama nga wala na-treat dayon"
>
> Not to forget, on the night of December 16, gipahuwat2 pa ninuo amonh inahan sa gawas ug pila ka minute atong gabiuna wa ninyo gipahiluna dayon kay kuno "BAYARAN SA ANG ANTI- GEN" kadakong atay. Nihangyo pas mama "PAHIGDAA SAKO NINYO KAY GIKAPOY NAKO KAAYO" WA MO KAILAG EMERGENCY!!! WAMO KAILAG KALAMIDAD!!!
>
> (Translated in English) Hi to the hospital at Sogod where my mother was first admitted after surviving the storm surge. We are here at Tacloban for medical re-admission since you provide us poor quality health care service, mainly because we don't have enough money to pay during that time. We have money for payment for your information but you provided us poor quality us we have no shoun [sic] money on that time. Your stiches were

---

[5] Complaint-Affidavit (of Dr. JLT), 24 December 2022, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[6] Complaint, 04 September 2022, at 2, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[7] *Id.*
[8] *Id.*

> like done by not professionals. The shoulder of my mother was like a chorizo because of your stiches. The result of the X-ray was neglected. I got the result a while ago, on December 18 we have been discharged, until now it was not responded/read. The attending nurse here said "maybe there was development as to the fracture of the knees of my mother that was not treated immediately*
>
> Not to forget, on the night of December 16, you caused our mother to wait for few minutes outside the hospital, you didn't make her comfortable immediately as you "waited for the payment of the Anti-gen" a big liver (bullshit). My mother asked for her to lie down as she was tired. You don't know what is emergency!!! what is calamity!!![9]

The Facebook post also received a series of comments from CPV's friends implying that Dr. JLT was the doctor who attended to her mother.[10]

On 24 February 2022, SMSI and Dr. JLT filed a complaint-affidavit for cyber libel before the Office of Provincial Prosecutor, Sogod, Southern Leyte against "CPV," the author of the Facebook post.[11]

According to SMSI, the Facebook post and comments "tarnished the image of Christ the Healer Hospital" as the malicious imputations in the post caused "dishonor and discredit" to the hospital not only in Southern Leyte but also in neighboring municipalities.[12]

On 07 September 2022, JPV filed a Complaint before the National Privacy Commission (NPC) against SMSI, Dr. JLT, and other corporate officers of SMSI for a violation of Section 32 (Unauthorized Disclosure) of the DPA.[13] According to JPV, she was stunned that SMSI attached and disclosed her medical records in the complaint-affidavit.[14]

JPV also argued that SMSI and Dr. JLT filed a complaint-affidavit against a "digital person" and a Facebook user named "CPV," whom they erroneously thought was her daughter.[15] She also said that she

---

[9] *Id.* Annex A.
[10] *Id.*
[11] Verified Comment, 09 November 2022, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[12] *Id.* at 2.
[13] Complaints-Assisted Form, 07 September 2022, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22- 201 (NPC 2022).
[14] Complaint, 04 September 2022, at 2, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[15] *Id.* at 1.

personally confronted her daughter, who denied writing about the social media post in question.[16]

On 19 September 2022, the NPC, through its Complaints and Investigation Division (CID), issued an Order (To File Verified Comment and Appear Virtually for Preliminary Conference).[17] In the Order, the preliminary conferences were set for 11 November 2022 and 09 December 2022.[18]

On 09 November 2022, SMSI filed its Verified Comment.[19] SMSI argued that the Complaint lacks merit as there is no violation of the DPA.[20] SMSI further argued that the medical records were attached in the Complaint filed in the National Prosecution Office to prove that JPV was "treated professionally and properly" at Christ the Healer Hospital contrary to what her daughter posted on Facebook.[21] SMSI stated that JPV's medical records served to refute the allegations about the medical treatment and the fact that she was not administered an anti-tetanus shot.[22]

It also stated that the medical records were necessary to prove whether the malicious Facebook post and comments really caused dishonor to the hospital.[23] It explained that in order to prove such, it is necessary and inevitable to attach the medical records of JPV.[24]

SMSI also added it was not their fault that JPV became the "talk of the town" since the hospital did not divulge the matter on social media.[25] SMSI claimed that it was JPV's daughter who posted about her confinement in Christ the Healer Hospital and maliciously posted statements that caused dishonor to the hospital and Dr. JLT.[26] SMSI also challenged JPV's allegation that "CPV," who posted on Facebook,

---

[16] *Id.*
[17] Order (To File Verified Comment and Appear Virtually for Preliminary Conference), 19 September 2022, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[18] *Id.*
[19] Verified Comment, 09 November 2022, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[20] *Id.*
[21] *Id.*
[22] *Id.* at 2.
[23] *Id.*
[24] *Id.*
[25] Verified Comment, 09 November 2022, at 3, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[26] *Id.*

is "virtually inexistent."[27] Lastly, SMSI argued that the medical records belonged to the hospital.[28]

On 14 November 2022, the CID issued an Order requiring the parties to submit their respective memoranda discussing and summarizing their respective causes of action.[29]

On 23 November 2022, JPV stated her Admissions and Denials to the annexes attached in the Verified Comment.[30] JPV admitted Complaint- Affidavit (Annex 2), NPC Resolutions dated 23 April 200[sic] (Annex 4) and 30 June 2022 (Annex 5), and the RTC Order dated 27 April 2022 (Annex 6) as to its existence and due execution.[31] Meanwhile, she denied the Board Resolution No. 6 (Annex 1) s. 2022, and the Facebook posts provided by SMSI (Annex 3).[32]

On 25 November 2022, the CID issued an Order noting Complainant's Compliance and Reminding the Parties to Submit their Simultaneous Memoranda.[33]

On 20 December 2022, SMSI submitted its Memorandum.[34]

In its Memorandum, SMSI argued that the use of the medical records is allowed under Section 13 (f) of the DPA, which allows for the processing of sensitive personal information when necessary for the protection of lawful rights and interests of natural and legal persons in court proceedings or the establishment, exercise, or defense of legal claims, or when provided to government or public authority.[35]

SMSI also argued that a data subject's rights are not applicable to the processing of personal data gathered for investigations in relation to criminal liabilities of a data subject under Section 37 of the Implementing Rules and Regulations of the DPA (IRR).[36] Lastly, SMSI

---

[27] *Id.*
[28] *Id.* at 2.
[29] Order, 14 November 2022, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[30] Compliance, 23 November 2023, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2023).
[31] *Id.* at 1-2.
[32] *Id.*
[33] Order (Noting the Complainant's Compliance and Reminding the Parties to Submit their Simultaneous Memoranda), 25 November 2022, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22- 201 (NPC 2022).
[34] Memorandum for Respondent, 20 December 2022, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[35] *Id.* at 4.
[36] *Id.* at 5.

reasoned that the medical records were owned by Christ the Healer Hospital and that CPV's posts caused dishonor and damage to it.[37] SMSI prayed that JPV's Complaint be dismissed.[38]

On 23 December 2022, JPV submitted her Memorandum.[39] According to JPV, the complaint-affidavit for the cyber libel case attached twenty
(20) medical records that pertain to her health status while being confined at the Christ the Healer Hospital.[40]

Upon knowledge of SMSI's disclosure, she sent a letter dated 16 March 2022 demanding SMSI to retract the medical records.[41] Despite her demand, SMSI refused to retract it.[42]

JPV also argued that she is not a party to the preliminary investigation for cyber libel, so the disclosure of her medical records was done without her consent or without any prior court or government approval.[43] Lastly, she reasoned that the introduction of her medical records was unnecessary, immaterial, and irrelevant to the crime of cyber libel because the disclosure of her medical records during preliminary investigation is premature,[44] the veracity behind the "chorizo-style of stitching" allegedly conducted by SMSI is immaterial and not among the elements for prosecuting the crime of cyber libel,[45] the medical records did not factually show that SMSI exercised extraordinary diligence in the manner of stitching and other medical procedures.[46]

JPV prayed for the following: (1) recommendation from the NPC for the filing of criminal case for twenty (20) counts of Unauthorized Disclosure and (2) indemnity in the form of moral damages of at least fifty thousand pesos (Php 50,000.00) and nominal damages of at least thirty thousand pesos (Php 30,000.00); (3) exemplary damages of at least thirty thousand pesos (Php 30,000.00).[47]

---

[37] *Id.* at 8.
[38] *Id.* at 10.
[39] Memorandum for Complainant, 23 December 2022, at 1, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[40] *Id.* at 3.
[41] *Id.*
[42] *Id.*
[43] *Id.* at 12.
[44] *Id.* at 13.
[45] Memorandum for Complainant, 23 December 2022, at 12, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[46] *Id.* at 13.
[47] *Id.* at 12.

Issue

Whether SMSI's use of JPV's medical records in a complaint for cyber libel violates the DPA.

Discussion

The Commission dismisses the case for lack of merit. SMSI did not violate the DPA when it used JPV's medical records in a complaint for cyber libel since the processing is with lawful basis under Section 13
(f) of the DPA.

In its cyber libel complaint, SMSI attached JPV's Admission and Discharge Records containing details on her diagnosis and operation and procedures administered, doctor's orders, nurse's notes, medical administration records, blood test results, antigen test results, temperature, pulse, and respiration (TPR) chart, discharge summary, and emergency room intervention form.[48]

Section 3 (l) of the DPA defines sensitive personal information:

> Section 3. *Definition of Terms*. Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:
>
> . . .
>
> (l) *Sensitive personal information* refers to personal information:
>
> 1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
> 2. About **an individual's health**, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
> 3. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

[48] Verified Comment, 09 November 2022, at 2, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).

> 4. Specifically established by an executive order or an act of Congress to be kept classified.[49]

Following this definition, since the medical records pertain to information about JPV's health, these are considered sensitive personal information. Considering that these are sensitive personal information, the processing should have lawful basis.[50]

Section 13 (f) of the DPA provides:

> Section 13. *Sensitive Personal Information and Privileged Information.* The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> . . .
>
> (f) The processing concerns such personal information as is **necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings,** or the **exercise or defense of legal claims**, or when provided to government or public authority.[51]

According to SMSI, it attached a copy of JPV's medical records to its complaint-affidavit for cyber libel in order to prove that JPV was "treated professionally and properly" at Christ the Healer Hospital and to negate her daughter CPV's alleged claims on Facebook.[52]

The purpose for attaching these medical records applies in both instances provided under Section 13 (f), namely: (1) they are necessary for the protection of lawful rights and interests in court proceedings, and (2) they are necessary for the establishment, exercise, or defense of legal claims.[53]

The qualifier "necessary" in the mentioned provision pertains to the general privacy principle of proportionality.

---

[49] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (l) (2012).

[50] *Id.* § 13.

[51] *Id.* § 13 (f).

[52] Verified Comment, 09 November 2022, at 2, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).

[53] Data Privacy Act of 2012, § 13 (f).

Section 11 of the DPA provides:

> Section 11. *General Data Privacy Principles*. The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and **proportionality.**
>
> Personal information must, be:
>
> . . .
>
> (c) Accurate, **relevant and, where necessary for purposes for which it is to be used the processing of personal information**, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;
>
> (d) **Adequate and not excessive in relation to the purposes for which they are collected and processed**[.][54]

Section 18 of the IRR also elaborates on proportionality:

> Section 18. *Principles of Transparency, Legitimate Purpose and Proportionality*. The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and **proportionality.**
>
> . . .
>
> c. Proportionality. The processing of information shall be **adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.** Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[55]

In this case, the medical records of JPV were necessary and relevant for the protection of lawful rights and interests of natural and legal persons, namely Dr. JLT and SMSI, the persons who were mentioned in CPV's social media post. The medical records were suitable and relevant to provide context and background information on the professional conduct of SMSI and their medical personnel while JPV

---

[54] *Id.* § 11 (c)(d). Emphasis supplied.
[55] National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule IV, § 18 (c). Emphasis supplied.

was their patient. The records were also relevant to the cyber libel case filed by SMSI to refute the allegations made by CPV on social media.

In CPV's social media post, she mentioned that Christ the Healer Hospital provided them with poor quality healthcare service because she and her mother did not have enough money to pay for the bills during that time.[56] She claimed that the stitches on her mother's shoulders appeared to have been performed by nonprofessionals, her mother's x-ray results were neglected, and the hospital displayed a lack of urgency in attending to her mother amidst the calamity.[57]

For an imputation to be considered libelous, it must be proven that the statements were defamatory and malicious.[58] Here, the medical records attached in the complaint-affidavit for cyber libel were relevant and necessary to prove that the medical personnel of the hospital attended to JPV immediately, professionally and properly, and that CPV's allegations made in the Facebook post were defamatory and malicious. The attached hospital records and test results served as SMSI's proof of how it treated JPV when she was admitted to the hospital, contrary to the statements made online.

SMSI used JPV's medical records to establish a case for cyber libel against JPV's daughter, the alleged author of the social media post. This falls directly under "processing is necessary for the establishment, exercise, or defense of legal claims."[59] The purpose of the disclosure of JPV's medical records was to build the case for cyber libel against the person who published the malicious imputations about the hospital and its personnel. Whether JPV was a party to the cyber libel case filed by SMSI is immaterial.

Given the foregoing, the use of JPV's medical records in the cyber libel case finds a lawful basis under Section 13(f) of the DPA.

In her Complaint, JPV charged SMSI and Dr. JLT of Unauthorized Disclosure as defined and penalized under Section 32 of the DPA:

> Section 32. *Unauthorized Disclosure*. (a) Any personal information controller or personal information processor or any of its

---

[56] Complaint, 04 September 2022, Annex A, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).
[57] *Id.* at 2.
[58] Diaz v. People, G.R. No. 159787 (2007).
[59] Data Privacy Act of 2012, § 13 (f).

> officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).
>
> (b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).[60]

To determine whether there is Unauthorized Disclosure, the following requisites must concur:

1. The perpetrator is a personal information controller or personal information processor;
2. The perpetrator disclosed information;
3. The information relates to personal or sensitive personal information;
4. The perpetrator disclosed the personal or sensitive personal information to a third party;
5. The disclosure was without any of the lawful basis for processing, consent or otherwise, under Sections 12 and 13 of the DPA; and
6. The disclosure is neither malicious nor done in bad faith and the information disclosed is not unwarranted or false information.[61]

As discussed, there is lawful processing under Section 13 (f) of the DPA when SMSI attached JPV's medical records for the establishment of the case on cyber libel. Thus, the fifth element is lacking in this case.

Considering that the requisites for Section 32 of the DPA (Unauthorized Disclosure) are not fully met, SMSI cannot be held liable.

---

[60] *Id.* § 32.
[61] JCB v. FRL, NPC 21-031, 03 March 2022, at 15, *available at* https://privacy.gov.ph/wp- content/uploads/2024/05/NPC-21-031-2022.03.03-JCB-v.-FRL-Decision-FinalP.pdf.

The Commission takes this opportunity to address SMSI's claim that they take ownership of the medical records.[62] Ownership of the physical or digital copies of the medical records does not result in the ownership of the personal data within those records such that they can use it in whatever way they want. The Commission emphasizes that any processing of personal data must not only comply with the general privacy principles but also have a lawful basis for the processing and be undertaken in a manner that is mindful of the rights of data subjects.

WHEREFORE, premises considered, the Commission resolves that the Complaint filed by JPV against Souley MD Services, Inc., is hereby **DISMISSED** for lack of merit.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases before any other forum or tribunal, if any.

SO ORDERED.

City of Pasay, Philippines.
05 June 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS

[62] Memorandum for Respondent, 20 December 2022, at 10, *in* JPV v. Souley MD Services, Inc., NPC 22-201 (NPC 2022).

Deputy Privacy Commissioner

Copy furnished:

JPV
Complainant

HCA
Counsel for Complainant

SOULEY MD SERVICES, INC.,
Respondent

MAM and GAP
Counsels for Respondent

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

MDT

Complainant,

-

versus-

BDO UNIBANK, INC.

Respondent.

NPC 22-006

For: Violation of the Data Privacy Act of 2012

x----------x

DECISION

NAGA, *P.C.;*

Before this Commission is a Complaint filed by MDT against BDO Unibank, Inc. (BDO) for alleged violations of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 21 January 2022, MDT filed his Complaints-Assisted Form (CAF) dated 20 January 2022.[1] In his CAF, alleged that he received a phone call from JACJAC (Caller) on 04 November 2021 who introduced himself as someone from BDO.[2] MDT stated:

> He asked if my name is MDT. After I replied "yes", [JAC] said there is an upgrade on my credit card and the scammer gave my earned points and he promised a ₱5,000 – Lazada voucher for the upgrade. The scammer then said my credit limit now of ₱200,000.00 will be increase *(sic)* to ₱250,000. To mail the Lazada voucher, the scammer then asked me if my address is*****. I replied "yes". The scammer said he will block my credit card and he will issue a new card. The scammer then asked if my credit card number is ****-xxxx-xxxx-****. I replied "yes". The scammer

[1] Complaints-Assisted Form dated 26 January 2022 of MDT

[2] *Id.*

> then asked for the expiration date and the CV number, which I gave to him."[3]

MDT alleged that based on the phone call, the caller knew his complete name, phone number, address, credit card limit, and credit card number.[4] Further, he alleged that only BDO has access to these private information.[5] MDT concluded that the caller had access to his private information, and consequently realized that he was scammed with a total amount of eighty-three thousand and twenty-eight pesos (Php 83,028.00).[6]

To support his claim, MDT attached his two Bangko Sentral ng Pilipinas (BSP) complaints dated 02 December 2021 and 12 January 2022 respectively which narrated the sequence of events of the incident.[7] MDT also attached in his CAF the screenshot of the transaction confirmation[8] received from BDO-Alert with Shopee Philippines Inc. amounting to eighty-three thousand and twenty-eight pesos (Php 83,028.00) as reflected in MDT's statement of account dated 25 November 2021.[9]

Thus, MDT prayed for a reversal of the sum of money charged in his credit card amounting to eighty-three thousand and twenty-eight pesos (Php 83,028.00) as well as all the charges in relation to the fraudulent transaction.[10] MDT also prayed for the Commission to find BDO to have violated Sections 26 and 32 of the DPA.[11]

On 11 February 2022, BDO was ordered by the Commission, through its Complaints and Investigation Division (CID), to file its Verified Comment.[12] The same Order also ordered the parties to appear for a

---

[3] *Id.*
[4] *Id.*
[5] Complaints-Assisted Form dated 26 January 2022 of MDT
[6] *Id.*
[7] *Id.*
[8] *Id.* Exhibit "A"
[9] Complaints-Assisted Form dated 26 January 2022 of MDT
[10] *Id.*
[11] *Id.*
[12] *MDT v. BDO*, NPC 22-006, Order to File Verified Comment dated 11 February 2022, at p. 1.

preliminary conference on 25 May 2022 and 22 June 2022 via Microsoft Teams.[13]

On 23 February 2022, BDO filed its Verified Comment dated 21 February 2022 praying that the complaint be dismissed with prejudice for lack of merit.[14]

In the Verified Comment, BDO denied MDT's request to cancel the transaction because it was processed and validated using a one-time password (OTP) sent to his mobile number, which had an advisory not to share it with anyone.[15] In a letter addressed to MDT, BDO alleged that they could not cancel the transaction because it was processed and validated using the OTP sent to him.[16] It further stated that there is nothing in the complaint to prove that BDO was the party liable for the disclosure of the personal information to the caller.[17]

Further, BDO argued that it did not commit any violation of the DPA since there was no unlawful disclosure of any information, and no unauthorized processing and accessing since it was MDT who provided all the confirmation of his personal information to the caller.[18] BDO also averred that MDT failed to state a cause of action in supporting his allegation of breach of data privacy against the former.[19] Moreover, BDO alleged that there is no intervention or participation on its part with regard to the confirmation of personal information that warrants the dismissal of the complaint, *thus:*

xxx

> 6. Complainant's confession to the existence of fraud, and voluntarily confirming his personal information to the caller, without intervention or participation on the part of the Bank whatsoever, warrant the dismissal of present complaint against BDO as there is clearly no breach of data privacy committed by the Bank. Complainant clearly responded to phishing, and even

---

[13] *Id.*
[14] Verified Comment dated 21 February 2022 of BDO
[15] *Id.*at p. 2.
[16] *Id.* Annex "1"
[17] Verified Comment dated 21 February 2022 of BDO at p. 3.
[18] *Id.*at p. 4.
[19] *Id.*at p. 4.

> provided the expiration date and CVV of his credit card that allowed the questioned transaction to proceed.[20]

On 02 March 2022, CID issued an Order dated 01 March 2022, noting the Verified Comment submitted by BDO.[21]

On 07 March 2022, MDT filed his Reply dated 05 March 2022 to the Verified Comment dated 21 February 2022.[22]

In his Reply, MDT repeatedly argued that the caller JAC knew his phone number, complete name, credit card number and limit, and his address which are considered his personal data.[23]

MDT further argued that BDO failed to protect and safeguard his personal data.[24] Thus, MDT stated that his personal data that were provided to BDO was unlawfully accessed and used by the caller to make him believe that the caller was from BDO.[25]

In addition, MDT stated that BDO only made an investigation on the validity of the transaction and not the fraud that involves breach of data privacy.[26] He questioned BDO on how the caller had access to his personal data and why its customer service representatives are not trained to analyze possible violation of breach of personal data.[27]

Furthermore, MDT argued that there is no phishing or vishing involved since the caller knew his personal data, and he merely confirmed the information provided by the caller.[28] He also stated that there is a cause of action due to the "unlawful access and fraudulent misuse of the personal data" of MDT.[29] Based on his submissions,

---

[20] *Id.*at p. 2.
[21] *MDT v. BDO,* NPC 22-006, Order Noting the Submission of Verified Comment of Respondent dated 01 March 2022
[22] Reply dated 05 March 2022 of MDT
[23] *Id.* at p. 1.
[24] *Id.* at p. 3.
[25] *Id.* at p. 3.
[26] Reply dated 05 March 2022 of MDT at p. 7.
[27] *Id.* at p. 7.
[28] *Id* .at p. 8.
[29] *Id.* at pgs. 5-6

MDT maintained that "there was an act or omission on the part of [BDO] ... to ensure appropriate privacy and security safeguard on [MDT's] personal data."[30]

Thus, MDT prayed a judgment in his favor, asking the Commission to order BDO to reverse the charged amount and all the finance charges associated with the subject transaction.[31] MDT also prayed for the Commission to order BDO the payment of attorney's and appearance fees, and to impose applicable penalties against BDO provided in Sections 26 and 32 of the DPA.[32]

On 11 March 2022, CID issued an Order noting the reply filed by MDT.[33]

On 25 May 2022, CID issued an Order after the first preliminary conference wherein both MDT and BDO were represented and assisted by their counsels, MTD and ABA, respectively.[34]

In the said Order, it was stated that during the discovery proceedings, MDT required the production of the phone call records made on 04 November 2021 at 05:54 P.M., 04 November 2021 at 10:40 PM, and 05 November 2021 at approximately 04:00 P.M. by Capas, Tarlac Waltermart BDO Branch, to the respondent.[35]

BDO manifested that if the phone calls were made through a landline, the recording might not be available; otherwise, a recording might have been made if it was made through a hotline number.[36] MDT reiterated that a confirmation number was provided for the 05 November 2021 phone call. [37]

---

[30] Reply dated 05 March 2022 of MDT at pgs. 5-6
[31] *Id.* at p. 8
[32] *Id.*
[33] *MDT v. BDO,* NPC 22-006, Order Noting the Reply filed by Complainant dated 11 March 2022
[34] *MDT v. BDO,* NPC 22-006, Order After the 1st Preliminary Conference held on 25 May 2022 and Reminding the Parties to Appear for the Second Setting of the Preliminary Conference for the Continuance of the Stipulations and/or Admissions of Facts and/or Documents dated 25 May 2022
[35] *Id.* at p. 1.
[36] *Id.* at pgs. 1-2
[37] *Id.* at p. 2

During the first preliminary conference, MDT manifested that the caller who called MDT, pretended to be from BDO which was denied by BDO and stated that MDT must prove this fact.[38]

MDT also manifested that the caller confirmed his name and address, but BDO denied having any personal knowledge of the manifested fact.[39] As to the Shopee transaction charged to the BDO credit card of MDT amounting to eighty-three thousand and twenty-eight pesos (Php 83,028.00) and that MDT replied to the BDO alert, it was admitted by the Respondent Counsel.[40]

Additionally, MDT manifested that the phone calls shall be discussed one by one to simplify the facts while BDO stated that these phone calls will be verified first to see if these were recorded in the BDO's system. Further, MDT made a stipulation stating that the caller has provided the credit card number and limit.[41] The stipulation was denied by BDO since it was not a privy to the said conversation between the caller and MDT.[42]

BDO manifested that MDT has provided the expiration date, and CVV number of his credit card to the caller and MDT has the physical possession of his credit card.[43] These manifestations were admitted by MDT.[44]

BDO also manifested that the OTP was sent to MDT which he disclosed to the caller.[45] MDT admitted such manifestation with qualification that "the caller asked the 6-digit number in his phone in order to process the Lazada voucher" and while he was on the phone call with the caller, another phone call came in from another number

---

[38] *MDT v. BDO*, NPC 22-006, Order After the 1st Preliminary Conference held on 25 May 2022 and Reminding the Parties to Appear for the Second Setting of the Preliminary Conference for the Continuance of the Stipulations and/or Admissions of Facts and/or Documents dated 25 May 2022 at p. 2

[39] *Id.* at p. 2

[40] *Id.* at pgs. 2-3

[41] *Id.*at p. 3.

[42] *MDT v. BDO*, NPC 22-006, Order After the 1st Preliminary Conference held on 25 May 2022 and Reminding the Parties to Appear for the Second Setting of the Preliminary Conference for the Continuance of the Stipulations and/or Admissions of Facts and/or Documents dated 25 May 2022 at p. 3.

[43] *Id.* at p. 3.

[44] *Id.* at p. 3.

[45] *Id.* at pgs. 3-4

of BDO, asking for a confirmation of the Shopee transaction in which he denied and he was assured that his credit card will be blocked.[46]

On 22 June 2022, an Order after the 2nd Preliminary Conference was issued by the CID.[47] In the same Order, for the continuation of stipulation of facts, BDO admitted the existence of two phone calls on 04 November 2021 with MDT and on the same date the subject credit card was blocked and the transaction was still pending.[48] However, BDO denied the existence of the phone call made on 05 November 2021 by BDO Capas, Tarlac, Waltermart branch for lack of record.[49] In response, MDT "questioned the essence of the confirmation number given to him via the 05 November 2021 telephone call."[50] Thus, BDO was ordered by the CID to submit compliance with regard to the verification of the nature of the confirmation number provided in the 05 November 2021 phone call. [51]

On 28 June 2022, CID issued an Order to Mediate to approve the Applications for Mediation dated 27 June 2022 and 24 June 2022, of MDT and BDO, respectively.[52] Thus, the proceedings of the case were suspended by virtue of the Order to Mediate.[53]

On 29 June 2022, BDO submitted its compliance dated 28 June 2022 to the Order dated 22 June 2022, stating that the confirmation number provided by MDT is a tracing number of the recorded call.[54] Thereafter, on the same date, CID issued an Order noting the compliance filed by BDO. [55]

---

[46] *MDT v. BDO,* NPC 22-006, Order After the 1st Preliminary Conference held on 25 May 2022 and Reminding the Parties to Appear for the Second Setting of the Preliminary Conference for the Continuance of the Stipulations and/or Admissions of Facts and/or Documents dated 25 May 2022 at pgs. 3-4
[47] *MDT v. BDO,* NPC 22-006, Order After the 2nd Preliminary Conference held on 22 June 2022, Respondent Subjected to Compliance Order and Requiring the Parties to Submit a Filled-Out Application for Mediation Form dated 22 June 2022
[48] *Id.* at p. 1.
[49] *Id.* at p. 1.
[50] *Id.* at p. 1.
[51] *MDT v. BDO,* NPC 22-006, Order After the 2nd Preliminary Conference held on 22 June 2022, Respondent Subjected to Compliance Order and Requiring the Parties to Submit a Filled-Out Application for Mediation Form dated 22 June 2022 at p. 1.
[52] *MDT v. BDO,* NPC 22-006, Order to Mediate dated 28 June 2022, Application for Mediation dated 27 June 2022 of MDT, and Application for Mediation of BDO dated 24 June 2022.
[53] *MDT v. BDO,* NPC 22-006, Order to Mediate dated 28 June 2022
[54] Compliance dated 28 June 2022 of BDO
[55] *MDT v. BDO,* NPC 22-006, Order Noting the Respondent's Compliance dated 01 July 2022

Subsequently, MDT submitted its Manifestation dated 01 July 2022 to the Compliance of BDO dated 28 June 2022.[56] MDT alleged that the compliance of BDO is incomplete since it merely confirmed that the confirmation number provided on the 05 November 2021 phone call is a tracing number.[57] Further, MDT reiterated that "there is a confirmation number issued, which means there is a record for the third phone call. "[58] Thus, MDT sought that the recording of the 05 November 2021 phone call be produced and prayed that an Order be issued for BDO to complete its compliance.[59]

On 19 July 2022, a Notice of Non-Settlement of Dispute was issued for failure of the parties to reach a settlement.[60]

On 21 July 2022, a Resolution was issued for MDT's Manifestation dated 01 July 2022, stating that BDO's compliance is insufficient and ordering the same to submit additional evidence to prove that the 05 November 2021 phone call recording is no longer available and to provide justifiable reason for its unavailability.[61] Thereafter, on the same date, the CID issued an Order (for Resumption of Complaints Proceedings and Requiring the Parties to Submit Simultaneous Memoranda) ordering the parties to submit their respective Memoranda discussing and summarizing their causes of action, claims, and defenses together with a list of evidence presented to prove their respective claims or defenses.[62]
On 27 July 2022, BDO filed its Compliance dated 26 July 2022 to the Resolution dated 21 July 2022. BDO stated that during the preliminary conference held on 25 May 2022, BDO's understanding of what is being asked is the actual voice recording of the phone call in BDO Waltermart, Capas, Tarlac Branch. BDO denied the existence of the phone call due to its understanding that what is being asked is the actual voice recording of the said conversation or phone call.[63] Moreover, BDO states that the tracing number exist but is not exclusively

---

[56] Manifestation dated 01 July 2022 of MDT
[57] *Id.* at pgs. 1-2
[58] *Id.* at p. 2
[59] *Id.* MDT at p. 2.
[60] *MDT v. BDO,* NPC 22-006, Notice of Non-Settlement of Dispute dated 19 July 2022
[61] *MDT v. BDO,* NPC 22-006, Resolution dated 21 July 2022 at pgs. 3-4
[62] *MDT v. BDO,* NPC 22-006, Order for Resumption of Complaints Proceedings and Requiring the Parties to Submit Simultaneous Memoranda dated 21 July 2022
[63] Compliance dated 26 July 2022 to the Resolution dated 21 July 2022 of BDO

associated with the actual voice record of the phone call since it was not recorded nor preserved.[64]

On 29 July 2022, CID issued an Order noting BDO's Compliance dated 21 July 2022.[65]

On the same date, MDT filed its Manifestation and Motion to the Compliance of BDO dated 26 July 2022.[66] MDT alleged that the Compliance of BDO is misleading since the issue being raised is the fraudulent charge in his credit card, BDO Waltermart, Capas, Tarlac branch is just a venue of the phone call, and there was a confirmation number to identify the phone call issued by the credit card department of BDO and not BDO Capas Branch.[67]

Thus, MDT prayed that an Order be issued requiring BDO to explain on why it should not be cited in contempt for its continual failure to comply with the Order of the Commission.[68]

On 30 July 2022, MDT filed its Second Manifestation to the Compliance of BDO to the Order dated 26 July 2022, to correct a typographical error with regard to one of the dates mentioned.[69]

On 01 August 2022, BDO filed its Memorandum dated 26 July 2022.[70] In its Memorandum, BDO stated that even if MDT reported the incident, it does not automatically cancel the subject transaction since an investigation on the matter shall be made before it acts on the request for the cancellation of the transaction.[71] Furthermore, BDO denied MDT's request since based on its investigation, the transaction was validated through an OTP.[72] BDO further averred that its denial

---

[64] *Id.* at pgs. 4-5
[65] *MDT v. BDO*, NPC 22-006, Order Noting the Respondent's Compliance (To the Resolution dated
21 July 2022) dated 29 July 2022
[66] Manifestation and Motion dated 29 July 2022 (Regarding Respondent's Compliance Dated 26
July 2022) by MDT
[67] *Id.*
[68] *Id.*
[69] Second Manifestation dated 30 July 2022 (Regarding Respondent's Compliance Dated 26 July
2022) by MDT
[70] Memorandum dated 26 July 2022 by BDO
[71] *Id.* at p. 3.
[72] *Id* .at p. 3.

of request to cancel the transaction is not considered as a breach of obligation on their part.[73] Thus, BDO prayed for the dismissal of the complaint for lack of merit.[74]

On 03 August 2022, MDT submitted his Memorandum dated 03 August 2022, alleging that BDO has committed personal data breach against him for failure to protect and safeguard from the unlawful access and fraudulent misuse of his personal data.[75] MDT also stated that BDO violated its contractual obligation since it failed to heed his instructions to not allow or process the Shopee transaction.[76]

Thus, MDT alleged that BDO is liable for violating Sections 26 and 32 of the DPA.[77] He therefore prayed that a judgment be rendered in his favor,[78] and for the Commission to order BDO the reversal of the amount charge from his credit card and all finance charges in relation to the subject transaction.[79] MDT also prayed to order BDO to pay attorney's fees and appearance fee as well as actual, moral, and exemplary damages.[80]

On 04 August 2022, the CID issued a Resolution denying MDT's Manifestation and Motion dated 29 July 2022, and ordering BDO to submit additional evidence or to provide justifiable reason for the unavailability of the 05 November 2021 phone call with confirmation number ********.[81]

Subsequently, BDO submitted its Compliance dated 09 August 2022 to the Resolution of the CID dated 04 August 2022.[82] BDO submitted a notarized sworn affidavit bearing the name of JDS who was in-charge of complaints with credit and debit cards under the Fraud

---

[73] *Id.* at pgs. 3-4
[74] Memorandum dated 26 July 2022 by BDO at p. 5.
[75] Memorandum dated 03 August 2022 by MDT at p. 9.
[76] *Id.* at p. 11.
[77] Complainant's Memorandum dated 03 August 2022 by MDT
[78] *Id.* at p. 22
[79] *Id.* at p. 22
[80] *Id.* at p. 22.
[81] Resolution dated 04 August 2022 (of Complainant's Manifestation and Motion (Regarding
Respondent's Compliance dated 26 July 2022 dated 29 July 2022; and Second Manifestation
(Regarding Respondent's Compliance dated 26 July 2022) dated 20 July 2022)
[82] Compliance dated 09 August 2022 to the Resolution dated 04 August 2022

Management Unit of BDO.[83] JDS stated that she was aware of the complaint of MDT and that the "05 November 2021 phone call is not presently available based on the routine and good faith operation of its electronic system and procedure."[84] Further, it was stated that "Our Team needs time to coordinate with the appropriate unit/s of the Bank to check the archives and verify its existence and/or availability, and retrieve the same, if feasible."[85]

Issues

Whether BDO violated Section 26 (Accessing Personal Information and Sensitive Personal Information Due to Negligence) and Section 32 (Unauthorized Disclosure) of the DPA.

Discussion

The Commission dismisses the Complaint for lack of merit and substantial evidence.

In this case, MDT has the burden to prove by substantial evidence that BDO violated Sections 26 and 32 of the DPA. However, MDT failed to provide sufficient information and evidence to substantiate the allegations he made in his complaint. As ruled in one of the cases decided by the Commission, "in administrative proceedings, the burden is on the Complainant to prove by substantial evidence the allegations in his Complaint are true."[86]

Based on the records and submissions, it was alleged that BDO violated the DPA. To support his claim, MDT attached in his CAF the Bangko Sentral ng Pilipinas (BSP) complaints form, screenshots of BDO-Alert messages, screenshots of correspondences, and letters from BDO.[87] However, the submitted evidence does not suffice to prove that there was unauthorized disclosure of information.

---

[83] *Id.* Annex "A"
[84] *Id.*
[85] *Id.*
[86] JLB v. Security Bank Corporation, CID-18-D-009, Decision dated 18 March 2021 at p. 4
[87] Complaints-Assisted Form dated 26 January 2022 of MDT

For complaints before the Commission to prosper, the burden of proof required is substantial evidence, or "that amount of relevant evidence that a reasonable mind might accept as adequate to support a conclusion." [88] The Supreme Court has explained that:

> **[T]he complainant has the burden of proving by substantial evidence the allegations in his complaint**. The basic rule is that mere allegation is not evidence and is not equivalent to proof. Charges based on mere suspicion and speculation likewise cannot be given credence. [89] (Emphasis supplied)

Rule 131 of the 2019 Amendments to the Revised Rules on Evidence also provides:

> Section 1. Burden of proof and burden of evidence. - **Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim or defense by the amount of evidence required by law**. Burden of proof never shifts.
>
> Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a prima facie case. Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case.[90]

In this case, MDT has the burden of proof to present evidence to support his claims against BDO, which he failed to establish. MDT did not deny that he provided his OTP and confirmed his personal information to the caller or an unverified person. The fact that the caller provided the information of MDT does not mean that BDO provided the information, which would result in unauthorized disclosure of data, nor would it result to negligence on the part of BDO. Further, MDT failed to establish that the information provided by the caller originated from BDO.

---

[88] *De Jesus v. Guerrero III* , G.R. No. 171491, 04 September 2009.
[89] *Id.*
[90] 2019 Amendment to the 1989 Revised Rules on Evidence, A.M. No. 19-08-15-SC, Rule 131, Section
1. Emphasis supplied

Hence, based on the submitted pieces of evidence, MDT failed to establish by substantial evidence that BDO was negligent in protecting his personal information.

I. BDO is not liable for Section 26 (Accessing Personal Information and Sensitive Personal Information Due to Negligence) of the DPA.

MDT alleged that BDO should be penalized for violating Section 26 of the DPA since BDO is the only one who should have access to his private information.[91]

Section 26 of the DPA provides:

> SEC. 26. *Accessing Personal Information and Sensitive Personal Information Due to Negligence.* – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.
>
> (b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.[92]

To be held liable under Section 26, the following requisites must be met:

---

[91] Complaints-Assisted Form dated 26 January 2022 of MDT
[92] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter VIII, § 26 (2012).

1. There is personal information or sensitive personal information;
2. The access was not authorized under the DPA or any existing law; and
3. The unauthorized access was due to the negligence of any person.[93]

The first element is present in this case since name, address, and contact number of MDT,[94] are considered personal information. Section 3 (g) of the DPA defines personal information as:

> *Personal information* refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[95]

Further, in this case, there is no sensitive personal information present since the data on a credit card does not fall within the definition under the DPA.[96] Sensitive personal information is defined by Section 3(l) of the DPA as personal information:

> (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
>
> (2) About an individual' s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
>
> (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

---

[93] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter VIII, § 26 (2012).

[94] Complaints-Assisted Form dated 26 January 2022 of MDT

[95] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter I, § 3(g) (2012).

[96] Section 3(l)(4) of the DPA: Sensitive personal information refers to personal information which is specifically established by an executive order or an act of Congress to be kept classified.

> (4) Specifically established by an executive order or an act of Congress to be kept classified.[97]

Based on the foregoing, none of the enumerations provided for under Section 3 (l) of the DPA is present in this case. It should be concluded that the data found on the credit card are not sensitive personal information. Additionally, in the discussion of sensitive personal information enumerations, it was held in NPC 18-G-077 that, "if the information does not fall under any of the enumerations, directly or indirectly, such information cannot be considered a sensitive personal information".[98] Hence, the details found on a credit card such as credit card number, CVV and expiration date are not sensitive personal information contemplated under the DPA.

As to the second element, MDT has failed to establish his claim that BDO, due to negligence, provided access to his personal or sensitive personal information without being authorized under the DPA or existing law. He was not able to show that BDO is privy to the alleged breach. The mere statement that his credit card information was known to the caller beforehand, and then confirmed the same, is insufficient to prove that it was BDO who negligently provided access to his personal information to the caller. Further, there is no evidence presented that only BDO is the only possible source of the information given by the caller to MDT.

Since MDT was not able to prove and present substantial evidence of BDO's involvement in the alleged breach, nor that his personal information was accessed due to BDO's negligence. Thus, it can be inferred that there is no negligence on the part of BDO in this case. To reiterate, there is nothing on the records which shows that BDO gave access to MDT's information to the caller due to its negligence. Hence, the third element is not present.

---

[97] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter I, § 3(l) (2012).
[98] NPC 18-G-077 (*unreported*), Decision dated 15 April 2021 at p. 9

Hence, failing to prove the second and third requisites under Section 26 are present, BDO cannot be held liable Section 26 of the DPA.

II. BDO is not liable for Section 32 (Unauthorized Disclosure) of the DPA.

Section 32 of the DPA provides:

> SEC. 32. *Unauthorized Disclosure*. – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).
>
> (b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).[99]

The case of NPC 21-111, enumerated the requisites for violation Section 32 of the DPA:

1. The perpetrator is a personal information controller or personal information processor or any of its officials, employees or agents;
2. The information relates to personal or sensitive personal information;
3. The perpetrator disclosed personal or sensitive personal information;
4. The disclosure was made to a third party;

---

[99] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter VIII, § 32 (2012).

5. The personal or sensitive personal information disclosed is neither unwarranted nor false information;
6. The disclosure was not malicious nor done in bad faith; and
7. The disclosure was without any of the lawful bases for processing under Section 12 and 13 of the DPA.[100]

To be liable under Section 32, the above-mentioned elements must be present. As defined under the DPA, a Personal Information Controller (PIC) "controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf."[101]

Here, BDO is a PIC as defined in the DPA. As a financial institution, it collects personal information and has control of the process in order to cater its banking purpose to its clients. Hence, the first element is present in this case.

The second element is also present. As discussed, MDT's name, address and contact number are personal information.

However, although the alleged breach involves personal information, there is no substantial evidence to prove that BDO has disclosed the personal data to the caller. For failure to prove that BDO disclosed the information of MDT to the caller, there is no doubt that there is no disclosure of information as an element of the third requisite. As such, the third element is not present in this case.

As to the fourth element, there is no evidence to prove that there was a disclosure of BDO to a third party. There is no unwarranted nor false information disclosed, as provided by the fifth element. There is no malicious nor disclosure done in bad faith, in relation to the sixth element. Lastly, since there is no disclosure of information on the part of BDO, the seventh element is evidently absent in this case.

---

[100] NPC 21-111 (*unreported*), Decision dated 22 September 2022 at p. 12
[101] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 3 (h) (2012).

Taking everything into account, the third, fourth, fifth, sixth and seventh elements are not present in this case since MDT failed to prove that BDO is involved in the disclosure of his personal data to the caller. There is also nothing on the record that BDO disclosed MDT's information to a third party. Additionally, there is no evidence to prove that bad faith nor malice was committed by BDO. Therefore, BDO cannot be held liable for the penalties provided for under Section 32 of the DPA.

Furthermore, MDT's request to produce the third phone call recording is not within the jurisdiction of this Commission to resolve. The request does not involve a data privacy issue. Moreover, assuming *arguendo* that the requested audio recording of the phone call made by MDT to BDO on 05 November 2021 was presented, it is beyond the authority and mandate of this Commission to decide the matter since it is not a data privacy issue. The production of the phone audio recording does not involve a processing of personal information nor will prove an unauthorized disclosure and/or access to sensitive information.

The purpose of presenting the audio recording is to prove that there was a conversation between MDT and BDO with regard to the action of the latter to block the credit card of the former.[102] This matter does not fall under the authority and jurisdiction of this Commission to resolve. Thus, regardless of the production and presentment of the audio phone recording, the subject recording is beyond the ambit of this Commission as provided for under the Data Privacy Act.

Further, as to MDT's prayer for the reversal of the unauthorized transaction credited against his account, the same is beyond the scope and jurisdiction of this Commission to resolve.

Based on the foregoing discussions, this Commission cannot find BDO liable for violation of the DPA. It must be noted that the safeguarding of personal information must be a joint obligation between the data

---

[102] Manifestation dated 01 July 2022 of MDT

subjects and the data controller or processor. Although PICs, like BDO, have the obligation to protect the privacy of data subjects, the data subjects on the other hand must exercise due diligence in protecting their personal information. One should not bear the loss or consequence arising from the negligence of another.

WHEREFORE, premises considered, this Commission resolves that the Complaint filed by MDT against BDO Unibank, Inc. (BDO) is hereby **DISMISSED**.

The Compliance and Monitoring Division is hereby **DIRECTED** to conduct a Compliance Check on the process of BDO in sending out its statement of accounts.

SO ORDERED.

City of Pasay, Philippines. 19 January 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

MTD
Counsel for Complainant

MBA
BDO UNIBANK, INC., LEGAL SERVICES GROUP
Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION GENERAL RECORDS UNIT
National Privacy Commission

JVT,
Complainant,

-versus-

VMA,
Respondent.
x----------x

NPC 18-018

For: Violation of the Data Privacy Act of 2012

LAR,
Complainant,

-versus-

VMA,
Respondent.
x----------x

NPC 18-019

For: Violation of the Data Privacy Act of 2012

CCW,
Complainant,

-versus-

VMA,
Respondent.
x----------x

NPC 18-020

For: Violation of the Data Privacy Act of 2012

MLS,
Complainant,

-versus-

VMA,
Respondent.
x----------x

NPC 18-027

For: Violation of the Data Privacy Act of 2012

DECISION

NAGA, *P.C.;*

Before this Commission are the consolidated Complaints filed by JVT, LAR, CCW, and MLS, (Complainants), against VMA for an alleged violation of the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 18 April 2018, JVT, LAR, CCW, and MLS filed their Complaint-Affidavits, respectively, alleging that VMA processed their Personal Data Sheets (PDS) for an unspecified, undeclared, and illegitimate purpose without their knowledge and consent.[1]

In their respective Complaint-Affidavits, JVT, LAR, and CCW averred that they are employees at the Office of the Transportation Cooperatives (OTC) under a Contract of Service (COS).[2] At the same time, MLS is the Board Secretary of the Technical Education and Skills Development Authority (TESDA).[3] Complainants alleged in their respective Complaints that VMA was the State Auditor IV of the Commission on Audit (COA) assigned as the Audit Team Leader of the OTC.[4]

Complainants stated that their PDS contained personal and sensitive personal information such as age, marital status, religious affiliation, education, and government-issued ID peculiar to an individual, including Tax Identification Number (TIN), Social Security System (SSS) ID, and Voter's ID.[5]

---

[1] Complaint-Affidavit dated 18 April 2018 of JVT, at p. 1, Complaint-Affidavit dated 18 April 2018 of LAR, at p. 1, Complaint-Affidavit dated 18 April 2018 of CCW, at p. 1 & Affidavit-Complaint dated 09 May 2018 of MLS at p. 1.

[2] *Id.*

[3] Affidavit-Complaint dated 09 May 2018 of MLS Annex "A".

[4] Responsive Comment dated 20 July 2018 of VMA, at p. 1.

[5] Complaint-Affidavit dated 18 April 2018 of JVT, at p. 2, Complaint-Affidavit dated 18 April 2018 of LAR, at p. 2, Complaint-Affidavit dated 18 April 2018 of CCW, at p. 2 & Affidavit-Complaint dated 09 May 2018 of MLS at p. 1.

Complainants alleged that VMA violated their rights as data subjects and their right to privacy by failing to uphold Section 11 (*General Privacy Principles*) and Sections 12 and 13 *(Criteria for Lawful Processing of Personal Information and Sensitive Personal Information*) of the DPA.[6]

On 09 May 2018, MLS alleged in his Affidavit-Complaint that he wrote a letter to VMA asking for an explanation on why no criminal, civil, or administrative charges should be filed against her for the alleged acquisition of his PDS from the Human Resource Personnel of the OTC without his consent and for an unknown purpose.[7] Moreover, MLS alleged that his right to data privacy has been violated by VMA and prayed for the award of One Million Pesos (Php1,000,000) in the form of damages.[8]

On 29 June 2018, the Commission's Complaints and Investigation Division (CID) ordered the parties to confer for discovery.[9] On 12 July 2018, Complainants failed to appear, and VMA manifested that she was unwilling to enter into an amicable settlement with the Complainants.[10] Hence, CID ordered VMA to file her Responsive Comment within ten (10) days from 12 July 2018 or until 22 July 2018.[11]Complainants were likewise ordered to file their reply upon receipt of respondent's comment.[12]

On 20 July 2018, VMA submitted her Responsive Comment (consolidated), alleging that she was the COA State Auditor IV

---

[6] Complaint-Affidavit dated 18 April 2018 of JVT, Complaint-Affidavit dated 18 April 2018 of LAR, & Complaint-Affidavit dated 18 April 2018 of CCW.

[7] Affidavit-Complaint dated 09 May 2018 of MLS Annex "A".

[8] Affidavit-Complaint dated 09 May 2018 of MLS.

[9] *JVT v. VMA,* NPC 18-018, Order to Confer for Discovery dated 29 June 2018, at p. 2, *LAR v. VMA,* NPC 18-019, Order to Confer for Discovery dated 29 June 2018, at p. 2, *CCW v. VMA,* NPC 18-020, Order to Confer for Discovery dated 29 June 2018, at p. 2, & *MLS v. VMA,* NPC 18-027, Order to Confer for Discovery dated 29 June 2018, at p. 2.

[10] *JVT v. VMA,* NPC 18-018, Order dated 12 July 2018 at, p. 1, *LAR v. VMA,* NPC 18-019, Order
dated 12 July 2018, at p. 1, *CCW v. VMA,* NPC 18-020, Order dated 12 July 2018, at p. 1, & *MLS v.*
VMA, NPC 18-027, Order Order dated 12 July 2018, at p. 1.

[11] *JVT v. VMA,* NPC 18-018, Order dated 12 July 2018, at p. 2, *LAR v. VMA,* NPC 18-019, Order
dated 12 July 2018, at p. 2, *CCW v. VMA,* NPC 18-020, Order dated 12 July 2018, at p. 2, & *MLS v.*
VMA, NPC 18-027, Order dated 12 July 2018, at p. 2.

[12] Consolidated Fact-Finding Report of Complaints and Investigation Division for Cases Nos. 18- 018, 18-019, 18-020 and 18-027 dated 24 April 2020, at p. 2,

assigned at OTC.[13] Moreover, VMA averred that her action in collecting the PDS of Complainants was done pursuant to Section 43 of Presidential Decree (PD) No. 1445:

> 1. The Auditors shall exercise such powers and functions as may be authorized by the Commission in the examination, audit and settlement of the accounts, funds, financial transactions, and resources of the agencies under their respective audit jurisdiction;
>
> 2. A report of audit for each calendar year shall be submitted on the last working day of February following the close of the year, by the head of each auditing unit through the Commission to the head or the governing body of the agency concerned and copies thereof shall be furnished the government officials concerned or authorized to receive them. Subject to such rules and regulations as the Commission may prescribe from time to time, the report shall set forth the scope of audit and shall include a statement of financial condition; a statement of surplus or deficit analysis; a statement of operations; a statement of changes in financial position; and such comments and information as may be necessary together with such recommendation with respect thereto as may be advisable, including a report of any impairment or capital noted in the audit. It shall also show specifically any program, expenditures, or other financial transaction or undertaking observed in the course of audit which in the opinion of the Auditor has been carried out or made without authority of law. The Auditor shall render such other reports as the Commission may require;
>
> 3. In the performance of their respective audit functions as herein specified, the auditors **shall employ such auditing procedures and techniques as are determined by the Commission under regulations that it may promulgate;**
>
> 4. The Auditors in all auditing units shall have the custody and be responsible for the safekeeping and preservation of paid expenses vouchers, journal vouchers, stubs of treasury warrants or checks, reports of collections and disbursements and similar documents together with their respective supporting papers, under regulations of the Commission. (underscoring supplied)[14]

---

[13] Responsive Comment dated 20 July 2018 of VMA, at p. 1.
[14] Responsive Comment dated 20 July 2018 of VMA, at pp. 1-2.

Further, VMA cited Section 39 of PD No. 1445:

> The Commission on Audit shall have the power, for purpose of inspection, to require the submission of the original of any order, deed, contract, or other document under which any collection of, or payment from, government funds may be made, together with any certificates, receipt, or other evidence in connection therewith xxx (underscoring supplied).[15]

VMA alleged that on 10 January 2018, she sent a letter received by the OTC requesting the management for the submission of data, including that of the COS Personnel.[16] It was also averred that "the COS is one of the areas required to be audited pursuant to the General Audit Instructions for CY 2017 and the Audit for the Specific Audit Instructions."[17]

Further, she claimed that the collection of Complainant's PDS was for
a legal reason:

> PDS which were submitted upon application of employees to the government office as support of their employment as COS is needed in the verification and evaluation process by the auditor to support the educational attainment, training experience, status of employment, etc., as provided in hiring these [COS] which is a must undertaking in the verification of the Contract of Services "on personnel hired by OTC as as part of the auditing procedures applied by the Audit Team to determine whether these personnel meet the qualification standards set by the OTC and whether hiring these number of personnel is really the need of the Agency and part of the Annual Procurement Plan (APP) of the OTC which is a legal reason pursuant to Section 39 and 43 of PD 1445 and not for any personal or other reasons.[18]

Lastly, she stated, "that the actions taken by the Audit Team Leader is what is ask (*sic*) of her in discharging her duties and responsibilities as the Auditor of the OTC."[19]

---

[15] *Id.*, at p. 2.
[16] *Id.*, at p. 2.
[17] *Id.*, at p. 2.
[18] Responsive Comment dated 20 July 2018 of VMA, at p. 2-3.
[19] *Id.*, at p. 3.

On 27 January 2021, the Commission issued a Minute Resolution remanding the instant case to CID to issue an order for VMA to provide a copy of her Responsive Comment to all the Complainants since VMA failed to furnished the Complainants of her Responsive Comment.[20] Further, the Commission order CID to direct the Complainants to file their Reply within ten (10) days upon receipt of the Respondent's Comment, such can be extended if deemed necessary by the CID.[21]

On 18 July 2022, the CID issued an Order directing VMA to furnish the Complainants with a copy of the Responsive Comment and to submit proof of receipt within five (5) calendar days from receipt of the Order.[22] Complainants were given a fresh period of fifteen (15) calendar days from receipt of the copy of the Responsive Comment to file their Reply to the Responsive Comment.[23] As such, VMA was aslo given a fresh period of fifteen (15) calendar days from receipt of the Reply to file her Rejoinder, copy furnished the Complainant.[24]

On 15 September 2022, the Commission received CCW's handwritten letter dated 20 August 2022 requesting that his name be withdrawn from the case.[25] CCW alleged in his letter that he was compelled to sign the Complaint since it is the order of the former OTC EV.[26] With this, he prayed that his name be removed as complainant of the instant case.[27] On 15 September 2022, the CID ordered CCW to submit a notarized affidavit of desistance within fifteen (15) calendar days from receipt of the Order.[28] CCW failed to submit the notarized Affidavit of Desistance to support his request.

---

[20] Minute Resolution dated 27 January 2021, at p. 2.

[21] *Id.*

[22] *v. VMA*, NPC 18-018, Order dated 12 July 2018 at, p. 2, *LAR v. VMA*, NPC 18-019, Order dated 12 July 2018 at, p. 2, *CCW v. VMA*, NPC 18-020, Order dated 12 July 2018, at p. 2, & *v. VMA*, NPC
18-027, Order Order dated 12 July 2018, at p. 2.

[23] *Id.*

[24] *Id.*

[25] Complainant CCW's Letter dated 22 August 2022.

[26] *Id.*

[27] *Id.*

[28] *JVT v. VMA*, NPC 18-018, Order dated 15 September 2022 at, p. 2, *LAR v. VMA*, NPC 18-019, Order dated 15 September 2022, at p. 2, *CCW v. VMA*, NPC 18-020, Order dated 15 September 2022, at p. 2, & *MLS v. VMA*, NPC 18-027, Order dated 15 September 2022, at p. 2.

Based on the records, the parties failed to comply to the Orders dated 18 July 2022 and 15 September 2022. Thus, the instant case shall be decided based on the records before the Commission.

Issue

Whether VMA violated Sections 11, 12, and 13 of the DPA.

Discussion

The Commission dismisses the complaint for lack of merit.

Complainants alleged that VMA, State Auditor IV, Audit team leader of DOTR2 Audit Group assigned at the OTC, requested and collected, for unspecified, undeclared, and illegitimate purpose, copy their PDS without their knowledge, information, consent, authorization, or much less agreed for its collection and processing.[29] Complainants argued that their rights to data privacy have been violated by VMA[30] and stated that the processing of personal information must conform to Section 11 (*General Privacy Principles*) and Sections 12 and 13 *(Criteria for Lawful Processing of Personal Information and Sensitive Personal Information*) of DPA. Lastly, Complainants alleged that the act of "VMA does not fall under any of the exemptions provided for under the law [DPA] "[31]

VMA argued that state auditors are required to audit contracts of services pursuant to the General Audit Instructions for CY 2017 and the Audit Area for the Specific Audit Instructions issued by the Cluster Director of the Cluster 7, National Government Sector, COA and the Supervising Auditor Department of Transportation 2 Audit Group for the preparation of the CY 2017 Annual Audit

---

[29] Complaint-Affidavit dated 18 April 2018 of JVT, at p. 1, Complaint-Affidavit dated 18 April 2018 of LAR, at p. 1, Complaint-Affidavit dated 18 April 2018 of CCW, at p. 1 & Affidavit- Complaint dated 09 May 2018 of MLS at p. 1.

[30] *Id.*

[31] Complaint-Affidavit dated 18 April 2018 of JVT, at p.4, Complaint-Affidavit dated 18 April 2018 of LAR at p.4, & Complaint-Affidavit dated 18 April 2018 of CCW, at p.4, & Affidavit- Complaint dated 09 May 2018 of MLS at p. 3.

Report/Management Letter.[32] She also alleged that the PDS of COS personnel hired by OTC were needed in the verification part of the auditing procedures to determine whether the qualification standards set by the OTC were met by these personnel, whether the hiring of such number of personnel was indeed necessary, and whether such hiring was part of the Annual Procurement Plan of the OTC pursuant to Sections 39 and 45 of P.D. 1445.[33] VMA argues that her actions were officially performed as part of her duties and responsibilities as the Audit Team Leader.[34]

I. The PDS contains personal and sensitive personal information.

The case involves VMA's processing of the PDS of the Complainants for audit purposes.[35] Processing "refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data."[36]

Complainants averred that their PDS was processed without their consent or authorization.[37] Further, the Complainants alleged that their PDS contained the following information "age, marital status, religious affiliation, education, and government-issued ID peculiar to an individual, including Tax Identification Number (TIN), Social Security System (SSS) ID, and Voter's ID."[38]

As discussed in VVC vs. CJB[39]:

---

[32] Responsive Comment dated 20 July 2018 of VMA, at p. 2.

[33] *Id.*, at p. 2-3.

[34] *Id.*, at p. 2.

[35] *Id.*, at pp. 2-3.

[36] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter I, § 3(j) (2012).

[37] Complaint-Affidavit dated 18 April 2018 of JVT, at p. 2, Complaint-Affidavit dated 18 April 2018 of LAR, at p. 2, Complaint-Affidavit dated 18 April 2018 of CCW, at p. 2 & Affidavit- Complaint dated 09 May 2018 of MLS at p. 1.

[38] *Id.*

[39] VVC v. CJB, NPC 19-134, Decision dated 10 December 2021.

A PDS is an **official document that contains personal and sensitive personal information of a government employee or official**. A PDS contains a government official of employee's personal background, qualifications, and eligibility, which necessarily includes personal and sensitive personal information as defined by the DPA:

> Section 3. Definition of Terms. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:
>
> (g) Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual
>
> . . . .
>
> (l) Sensitive personal information refers to personal information:
>
> (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
>
> (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
>
> (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
>
> (4) Specifically established by an executive order or an act of Congress to be kept classified.[40]

The processing of sensitive personal information, such as those contained in the PDS of the Complainants, is prohibited under the

---

[40] *Id.*, at pp. 7-8.

DPA, except when the data subjects have consented to the processing or when there are other lawful criteria for the processing of sensitive personal information. Section 13 of the DPA provides that sensitive personal information cannot be processed, except for the specific instances stated therein, to wit:

> SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> xxx
>
> (b) The processing of the same is provided for by existing laws and regulations: Provided, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
>
> (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
>
> (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, that such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;
>
> (e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
>
> (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.[41]

---

[41] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy

II. *The processing of the Complainants' PDS by VMA is permissible under the Data Privacy Act of 2012.*

In this case, Complainants averred in their respective Complaint-Affidavit that VMA, State Auditor IV, Audit Team Leader of DOTR 2 Audit Group assigned at the OTC, processed their personal information without their consent.[42] VMA, on her part, stated that she processed the personal information as part of her functions as the COA State Auditor IV and Audit Team Leader of the OTC.[43]

As established in the previous rulings of this Commission, consent is not the only basis for processing personal and sensitive personal information.[44] Under Sections 12 and 13 of the DPA, the processing of personal and sensitive personal information shall only be permitted based on other lawful criteria[45], to wit:

> SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> xxx
>
> (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to **fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate**; [46] (Emphasis supplied)

Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter III, § 13 (2012).

[42] Complaint-Affidavit dated 18 April 2018 of JVT, at p. 2, Complaint-Affidavit dated 18 April 2018 of LAR, at p. 2, Complaint-Affidavit dated 18 April 2018 of CCW, at p. 2 & Affidavit- Complaint dated 09 May 2018 of MLS, at p. 1.

[43] Responsive Comment dated 20 July 2018 of VMA, at p. 3.

[44] ACN v. DT, NPC 18-109, Decision dated 01 June 2021, at p. 10.

[45] VVC v. CJB, NPC 19-134, Decision dated 10 December 2021, at p. 15.

[46] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter III, § 12 (2012).

xxx

> SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> xxx
>
> (b) **The processing of the same is provided for by existing laws and regulations:** Provided, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information; [47] (Emphasis supplied)

Under Section 2 par. (1) of Article IX (D) of the 1987 Constitution of the Philippines:

> [COA] shall have the power, authority, and duty to examine, audit, and settle all accounts pertaining to the revenue and receipts of, and expenditures or uses of funds and property, owned or held in trust by, or pertaining to, the Government, or any of its subdivisions, agencies, or instrumentalities, including government-owned or controlled corporations with original charters, and on a post-audit basis [48]

To reiterate, VMA cited Sections 39 and 43 of PD 1445, describing the Powers, functions, and duties of Auditors as Representatives of the Commission on Audit.[49]

Section 39 (1) of PD 1445, provides:

> Section 39. Submission of papers relative to government obligations. (1) The Commission shall have the power, for purposes of inspection, to **require the submission of the original of any order, deed, contract, or other document under which any collection of, or payment from, government funds**

---

[47] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter III, § 13 (2012).

[48] Philippine Constitution, Article IX (D)(2). 1987.

[49] Responsive Comment dated 20 July 2018 of VMA, at pp. 1-2.

> **may be made, together with any certificate, receipt, or other evidence in connection therewith.** If an authenticated copy is needed for record purposes, the copy shall upon demand be furnished.[50]

While Section 43 of PD 1445 states:

> Section 43. Powers, functions, and duties of auditors as representatives of the Commission.
>
> 1. The auditors shall exercise such powers and functions as may be authorized by the Commission in the examination, audit and settlement of the accounts, funds, financial transactions, and resources of the agencies under their respective audit jurisdiction.
>
> 2. A report of audit for each calendar year shall be submitted on the last working day of February following the close of the year, by the head of each auditing unit through the Commission to the head or the governing body of the agency concerned, and copies thereof shall be furnished the government officials concerned or authorized to receive them. Subject to such rules and regulations as the Commission may prescribe from time to time, the report shall set forth the scope of audit and shall include a statement of financial condition; a statement of surplus or deficit analysis; a statement of operations; a statement of changes in financial position; and such comments and information as may be necessary together with such recommendations with respect thereto as may be advisable, including a report of any impairment of capital noted in the audit. It shall also show specifically any program, expenditure, or other financial transaction or undertaking observed in the course of audit which in the opinion of the auditor has been carried out or made without authority of law. The auditor shall render such other reports as the Commission may require.
>
> 3. In the performance of their respective audit functions as herein specified, the auditors shall employ such auditing procedures and techniques as are determined by the Commission under regulations that it may promulgate.
>
> 4. The auditors in all auditing units shall have the custody, and be responsible for the safekeeping and preservation of paid

---

[50] Ordaining And Instituting a Government Auditing Code of The Philippines. Presidential Decree No. 1445, Section 39, 1978.

> expense vouchers, journal vouchers, stubs of treasury warrants or checks, reports of collections and disbursements and similar documents together with their respective supporting papers, under regulations of the Commission.[51]

Based on the preceding, the COA is responsible for ensuring that government agencies and entities use public funds and resources efficiently, effectively, and in accordance with applicable laws and regulations. Its audit reports serve as a basis for improving government operations and holding officials accountable for their actions. The COA is an independent body constitutionally mandated to perform audit functions, among others.

Thus, VMA, as the designated Auditor of COA, processed complainants PDS in performance of her functions. The letter request shows that VMA has been given authority to process the PDS of Complainants, which contains personal and sensitive personal information, as part of her duties and responsibilities as the State Auditor IV of the OTC. The request was in connection to VMA's function to audit any contracts the OTC enters, including those involving COS personnel.

Moreover, she attached the letter request dated 10 January 2018, requesting that all Chiefs of concerned OTC Division/Office to submit records and reports, including Contracts for all COS personnel, in preparation for the CY 2017 Annual Audit Report.[52] The letter request shows that the purpose of VMA's collection of the PDS was to facilitate the preparation of the Audit Report and to meet the deadline imposed by law in the submission of the Annual Audit Report."[53]

The processing of personal and sensitive personal information contained in the PDS of the complainants made by COA, through VMA's letter requesting the collection of the former's PDS, is part of its Constitutional mandate.

---

[51] Ordaining And Instituting a Government Auditing Code of The Philippines. Presidential Decree No. 1445, Section 41, 1978.
[52] Responsive Comment dated 20 July 2018 of VMA. Annex "I".
[53] *Id.*

Considering the foregoing, this Commission finds the processing made by VMA in requesting and obtaining the PDS of Complainants has a lawful criteria to process the same as stated in Sections 12 (e) and 13 (b) of the DPA, specifically, the processing was done in fulfillment of its mandate and by existing laws and regulations pursuant to the 1987 Philippine Constitution and Government Auditing Code of the Philippines and COA regulations.

WHEREFORE, premises considered, this Commission resolves that the instant Complaint filed by JVT, LAR, CCW, and Atty. MLS against VMA for an alleged violation of the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) is hereby **DISMISSED** for lack of merit.

SO ORDERED.

City of Pasay, Philippines.
22 February 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

JVT
Complainant

LAR
Complainant

CCW
Complainant

MLS
Complainant

VMA
Respondent

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

SPOUSES JG and AG,

Complainant,

-versus-

SPOUSES CP and CC,

Respondent.

x----------x

NPC 23-036

For: Violation of the Data Privacy Act of 2012

DECISION

NAGA, *P.C.;*

Before the Commission is the Complaint filed by Spouses JG and AG (Complainants) against Spouses CP (MC) and CC (Respondents) for an alleged violation of Sections 25, 28, 31, and 32 of the Data Privacy Act of 2012 or Republic Act No. 10173 ("DPA").

Facts

On 15 March 2023, the Commission, through its Complaints and Investigation Division (CID) received the Complaints Assisted Form of Complainants (CAF).[1]

Complainants alleged that sometime in October 2020, Respondents filed a complaint for Syndicated Estafa against Complainants and several others before the National Bureau of Investigation (NBI).[2] The said complaint was eventually endorsed by NBI to the Office of the City Prosecutor of Quezon City (OCP-QC), docketed as NPS Docket No. INV-20B-01419, titled "Spouses CP (MC) and CC vs. Spouses JG and AG, AYG, LA, PN, Spouses JY and CY, and Spouses FC and JY."[3]

---

[1] Complaints-Assisted Form dated 14 March 2023 of Spouses JG and AG.
[2] *Id*, at p. 7.
[3] *Id*, at p. 7.

In the said proceedings before the OCP-QC, Complainants averred that Respondents "brought up and released documents" that pertain to a different case for Syndicated Estafa filed against the said Complainants, by one AL before the NBI, where Respondents were not parties to the said case.[4]

Complainants, in their CAF, averred that the personal and sensitive personal information pertains to their name, address, marital status, proceedings and documents before the NBI for Syndicated Estafa alleged to have been committed by them, the Disposal of Proceedings before NBI, and its Decision.[5]

Moreover, the Complainants claimed that in Respondents' Joint and Consolidated Reply Affidavit dated 22 October 2020 (Reply Affidavit) before the OCP-QC, they "illegally obtained, and subsequently disclosed the following personal and sensitive personal information as well as an Affidavit of Desistance with Mutual Release and Quitclaim filed in said case, despite such having absolutely no bearing on the case before the OCP-QC."[6] In the said Reply Affidavit, Respondents declared that they were able to secure a copy of the Affidavit of Desistance, to wit:

> 61. Upon further investigation, Complainant Spouses were able to secure a copy of the "Affidavit of Desistance with Mutual Release and Quitclaim" executed by AL in favor of respondents Spouses G and their daughter, respondent AYG in NBI Case No. 322649 filed against the same and all respondents herein.[7]

Additionally, in the same Reply Affidavit, Respondents admitted that
they secured assistance from "good minded persons" from NBI, to wit:

> 62. Interestingly, respondents Spouses G and daughter respondent AYG demanded confidentiality of this settlement from complainant AL. This is precisely the reason why complainant Spouses could not get any assistance from her in instant case. Fortunately, good minded persons with access to

---

[4] *Id*, at p. 7.
[5] Complaints-Assisted Form dated 14 March 2023 of Spouses JG and AG, at p. 2.
[6] *Id*, at p. 7.
[7] *Id*, at p. 7 and Annex 1 "Joint and Consolidated Reply Affidavit" at p. 28.

NBI records provided complainant Spouses with a copy of settlement.[8]

Complainants alleged that the acts done by Respondent of "accessing, processing and disclosing [C]omplainants' G's personal and sensitive personal information gives rise to criminal liability under the Data Privacy Act."[9] Hence, in their CAF, the Complainants pleaded that the Respondents be held liable under Sections 25, 28, 31, and 32 of the DPA.[10] Complainants also stated that "the culpable officers of the NBI may likewise be held liable together with Respondents," citing Republic Act No. 6713, the Code of Conduct and Ethical Standards for Public Officials and Employees and the Revised Penal Code.[11]

On 11 April 2023, the CID issued an Order (To File Verified Comment and Appear Virtually for Preliminary Conference) requiring the Respondents to file their Verified Comment within fifteen (15) days from receipt of the Order.[12] The CID likewise orders the parties to appear virtually for a Preliminary Conference on 16 May 2023, and 27 June 2023.[13]

On 04 May 2023, Respondents, through counsel, filed their Verified Comment dated 02 May 2023.[14] Respondents argued that they committed no violation, and the said Complaint must be dismissed for sheer and utter want of merit.[15]

In Respondents' Verified Comment, they argued that the complaint should be dismissed for not having been brought against the real parties in interest and should have impleaded the NBI in the complaint.[16] Respondents averred that NBI, as the Personal Information Controller or PIC, which disclosed the information to them, is "ultimately liable" for the disclosure made to the Respondents.[17]

---

[8] *Id*, at p. 7 and Annex 1 "Joint and Consolidated Reply Affidavit" at p. 28.
[9] Complaints-Assisted Form dated 14 March 2023 of Spouses JG and AG, at p. 8.
[10] *Id*, at p. 8.
[11] *Id*, at p. 9.
[12] *Spouses JG and AG vs. Spouses CP and CC*, NPC 23-036, Order (To File Verified Comment and Appear Virtually for Preliminary Conference) dated 11 April 2023.
[13] *Id*, at p. 2.
[14] Verified Comment dated 02 May 2023 of Spouses CP and CC.
[15] *Id*, at p. 9.
[16] *Id*, at p. 9.
[17] *Id*, at p. 11.

Second, Respondents argued that the Complainants failed to exhaust administrative remedies as the latter failed to inform the NBI in writing of the alleged disclosure.[18] Moreover, Respondents argued that Complainants failed to exhaust remedies and to show any good cause as to why the complaint should be given merit, as there is no serious violation or breach of the DPA.[19]

Third, the Respondents claim that they have a legal basis under Section 13 (f) to process Complainants' information.[20] Respondents argued that the disclosures were made to protect their rights and interests in NPS Docket No. INV-20B-01419.[21] Respondents posited that "the information obtained was submitted to [OCP-QC] through the Investigating Prosecutor conducting the preliminary investigation and was therefore submitted to it in accordance with its mandate of determining the legal claims of the respondents against the complainants therein, and as such is considered as having been provided to "government or public authority," under Section 13 (f) of the Data Privacy Act."[22]

Fourth, Respondents averred that Complainants' personal and sensitive personal information: name, address, and marital status, were already disclosed in the pleadings filed in NPS Docket No. INV- 20B-01419.[23]

Next, Respondents also argued that the Complainants are estopped from questioning the disclosure of information relating to the outcome of the case filed by AL against them.[24] In Complainants' Joint- Rejoinder Affidavit, they already voluntarily disclosed the Complaint- Affidavit of AL and the outcome of that case.[25]

Lastly, Respondents argued that the information disclosed by them in relation to the case filed by AL against Complainants is not inherently false or unwarranted.[26]

---

[18] Verified Comment dated 02 May 2023 of Spouses CP and CC, at p. 11.
[19] *Id*, at p. 12.
[20] *Id*, at p. 14.
[21] *Id*, at p. 16.
[22] Verified Comment dated 02 May 2023 of Spouses CP and CC, at p. 16.
[23] *Id*, at p. 20.
[24] *Id*, at p. 20.
[25] *Id*, at p. 20.
[26] Verified Comment dated 02 May 2023 of Spouses CP and CC, at p. 21.

On 08 May 2023, the CID issued an Order (Noting the Complainants Working Email Addresses and Respondents Comment and Reminding the Parties to Appear Virtually for the Preliminary Conference).[27]

On 16 May 2023, the CID issued an Order (After the 1st Preliminary Conference held on 16 May 2023, Cancelling the 2nd Preliminary Conference on 27 June 2023, Requiring the Respondents to Submit Manifestation, and Requiring the Counsel for Complainants to Submit Special Power of Attorney).[28]

On 26 May 2023, Respondents, through counsel, filed their Manifestation that they are not "inclined" to undergo mediation proceedings.[29] On the same date, the Complainants submitted their Special Power of Attorney appointing their counsel to act on their behalf.[30]

The CID issued an Order dated 29 May 2023, noting the submissions made by the parties.[31] The CID likewise ordered the parties to submit their respective Memoranda.[32]

On 13 June 2023, the Respondents sent their Memorandum dated 12 June 2023.[33] In their Memorandum, Respondents merely reiterated their previous defenses mentioned in their Verified Comment.[34]

In a Memorandum dated 21 June 2023, Complainants alleged that the Respondents are liable for violating Sections 25, 28, 31, and 32 of the DPA for disclosing their personal information and sensitive personal information with the OCP-QC without their consent, or without being

---

[27] *Spouses JG and AG vs. Spouses CP and CC*, NPC 23-036, Order (Noting the Complainants Working Email Addresses and Respondents Comment and Reminding the Parties to Appear Virtually for the Preliminary Conferences) dated 08 May 2023.

[28] *Id.*

[29] Manifestation dated 26 May 2023 of Spouses CP and CC.

[30] Special Power of Attorney dated 27 April 2023 of Spouses JG and AG.

[31] *Spouses JG and AG vs. Spouses CP and CC*, NPC 23-036, Order (Noting the Respondents Manifestation, Noting the Complainants Special Power of Attorney, and Requiring the Parties to Submit Simultaneous Memoranda) dated 29 May 2023.

[32] *Id*, at p. 2.

[33] Memorandum dated 12 June 2023 of Spouses CP and CC.

[34] *Id.*

authorized under Sections 12 and 13 of the DPA.[35] Moreover, the Complainants averred that the principle of real parties in interest does not apply in criminal cases, such as the violations under the DPA.[36] Additionally, the Complainants claim that their complaint falls under the exception provided in the DPA on the rule on exhaustion of administrative remedies because the allegations in the complaint involve a serious violation or breach of the DPA.[37] Lastly, Complainants stated that they are not estopped from questioning the disclosure since they only disclosed the information in response to Respondents' use of the information.[38]

On 04 October 2023, the CID issue a Notice dated 06 September 2023, informing that the case is submitted for the decision of the Commission.[39]

Issue

I. Whether the case should be outrightly dismissed for failure of the Complainants to exhaust administrative remedies; and

II. Whether Respondents are liable for violating Section 25 of the DPA.

Discussion

The Commission finds that the case should not be dismissed on procedural grounds and that Respondents are liable for violating Section 25 of the DPA.

I. Complainants did not violate the Rule on Exhaustion of Remedies.

Section 2, Rule II of NPC Circular No. 2021-01 (2021 NPC Rules of Procedure) provides:

---

[35] *Id*, at p. 4-17.
[36] *Id*, at p. 17.
[37] Memorandum dated 21 June 2023 of Spouses JG and AG, at p. 19.
[38] *Id*, at p. 22.
[39] *Spouses JG and AG vs. Spouses CP and CC*, NPC 23-036, Notice (that the Case is Submitted for Decision of the Commission) dated 06 September 2023.

> **SECTION 2.** ***Exhaustion of remedies.*** – No complaint shall be given due course unless it has been sufficiently established and proven that:
>
> > 1. **the complainant has informed, in writing, the personal information controller (PIC), personal information processor (PIP), or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same;** and
> > 2. the PIC, PIP, or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the PIC, PIP, or concerned entity within fifteen (15) calendar days from receipt of written information from the complainant.
>
> **The NPC may waive any or all of the requirements of this Section at its discretion** upon (a) good cause shown, properly alleged and proved by the complainant; or (b) **if the allegations in the complaint involve a serious violation or breach of the Data Privacy Act of 2012, taking into account the risk of harm to the affected data subject**, including but not limited to:
>
> > i. when there is grave and irreparable damage which can only be prevented or mitigated by action of the NPC;
> > ii. **when the respondent cannot provide any plain, speedy or adequate remedy to the alleged violation;** or
> > iii. the action of the respondent is patently illegal.[40] (Emphasis supplied)

In Complainants' CAF, they alleged that prior to filing their Complaint before the Commission, they were able to inform the Respondents in writing through the Joint Rejoinder-Affidavit dated 05 November 2020, stating that:

> 34. Notably, it is quite alarming, not to mention illegal and criminal, that complainants Spouses C were able to obtain access to the Affidavit of Desistance and Agreement with Revocation of Deed of Assignment despite being non-parties thereto We have been informed that information pertaining to any proceeding for any offense committed or alleged to have been committed by an individual, including the disposal of such proceedings, is considered as sensitive personal information protected by Republic Act No. 10173.[41]

---

[40] National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission, NPC Circular No. 2021-01, rule II, § 2 (28 January 2021) (2021 NPC Rules of Procedure).
[41] Complaints-Assisted Form dated 14 March 2023 of Spouses JG and AG, at p. 7 and Annex 1 "Joint and Consolidated Reply Affidavit" at p. 28.

In this case, Complainants' statement in their Joint Rejoinder-Affidavit is sufficient to inform and alert the Respondents that attaching their Affidavit of Desistance constitutes a possible violation of the DPA because of the alleged unauthorized processing of the Affidavit of Desistance which contains personal information and sensitive personal information.

In addition, the processing of the personal information and sensitive personal information involved, such as Complainants' names, address, marital status, and information regarding the Syndicated Estafa case, may pose a risk of harm to them as the affected data subjects since unauthorized acquisition of the following information may result to identity fraud, crimes, and other harm when used in a manner that could expose them to harassment, discrimination, or other risks such as the creation of fake accounts or accounts using other identifying information of another person without authority.

Further, assuming arguendo that Complainants' method of informing the Respondents was insufficient, the Complaint would still not be dismissible. Section 2, Rule II of the 2021 NPC Rules of Procedure states that the NPC may also waive the rule on exhaustion of remedies when the respondent cannot provide any plain, speedy or adequate remedy to the alleged violation,[42] such as in this case.

The personal and sensitive personal information of Complainants were already processed by the Respondents when they requested and accessed the Affidavit of Desistance with Mutual Release and Quitclaim which was thereafter submitted to OCP-QC in relation to NPS Docket No. INV-20B-01419.[43]

Thus, the Rule can no longer apply given that Respondents cannot take any appropriate action to remedy the situation since the Affidavit of Desistance with Mutual Release and Quitclaim was already included in the documents filed before the OCP-QC and cannot be withdrawn.

---

[42] National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission, NPC Circular No. 2021-01, rule II, § 2 (28 January 2021) (2021 NPC Rules of Procedure).
[43] Complaints-Assisted Form dated 14 March 2023 of Spouses JG and AG, at p. 7.

To emphasize, "the rules of procedure should be viewed as mere tools designed to facilitate the attainment of justice. Their strict and rigid application, which would result in technicalities that tend to frustrate rather than promote substantial justice, must always be eschewed."[44]

II. Respondents committed Unauthorized Processing under Section 25 of the DPA.

Section 25 of the DPA penalizes Unauthorized Processing of Personal Information and Sensitive Personal Information:

> SEC. 25. *Unauthorized Processing of Personal Information and Sensitive Personal Information.* – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.
>
> (b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.[45]

All the elements of unauthorized processing under Section 25 are present in this case, namely:

1. The accused processed the information of the data subject;
2. The information processed was personal information or sensitive personal information; and
3. The processing was done without the consent of the data subject, or without authority under this Act or any existing law.[46]

---

[44] Heirs of Amada Zaulda v. Zaulda, G.R. No. 201234, 17 March 2014.
[45] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter VIII, § 25 (2012).
[46] *Id.*

As to the first element, Section 3 (j) of the DPA defines processing as "any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data."[47]

Respondents processed Complainants' information when they attached the Affidavit of Desistance with Mutual Release and Quitclaim in the Joint and Consolidated Reply Affidavit dated 22 October 2020, "to establish that complainants had been previously charged with syndicated estafa also arising from the sale of shares of a corporation covering the same properties that were the subject of the estafa case filed by respondents against complainants."[48]

With the second element, Section 3 (g) of the DPA defines personal information as "any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."[49]

On the other hand, sensitive personal information under Section 3 (l) of the DPA refers to personal information:

> (1) About an individual's race, ethnic origin, **marital status**, age, color, and religious, philosophical or political affiliations;
>
> (2) About an individual's health, education, genetic or sexual life of a person, or to **any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;**
>
> (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

---

[47] *Id*, chapter I, § 3(j) (2012).
[48] Complaints-Assisted Form dated 14 March 2023 of Spouses JG and AG, at p. 7 and Annex 1 "Joint and Consolidated Reply Affidavit" at p. 28.
[49] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter I, § 3 (g) (2012).

> (4) Specifically established by an executive order or an act of Congress to be kept classified.[50]

In this case, the Affidavit of Desistance with Mutual Release and Quitclaim contained the Complainants' personal information and sensitive personal information such as their names, address, marital status, and information regarding the Syndicated Estafa case filed against them.[51]

Regarding the third element, the Complainants clearly did not consent to the use of their Affidavit of Desistance. Moreover, Respondents failed to show that their action finds basis under Section 12 (c) or Section 13 (b) of the DPA as they only stated that they were able to secure the Affidavit of Desistance from "good minded persons with access to NBI records."[52]

In Respondents' Comment dated 02 May 2023, they posited that there is "legal basis to process the affidavit of desistance under Section 13 (f) of the DPA, since they were complainants in the complaint docketed as NPS Docket No. INV-20B-01419 and the affidavit of desistance was in response to complainants' allegation during the course of preliminary investigations that the idea of setting up a condominium corporation over the subject properties was respondent MC's idea and was intended to counter complainants' allegation that it was respondent MC who caused the dispute that led to the filing of the estafa case; that the affidavit was submitted to the Office of the City Prosecutor as part of preliminary investigations, thus a submission to government or public authority under Section 13 (f); and that complainant's name, address, and marital status were already disclosed in the pleadings they filed in relation to NPS Docket No. INV-20B-01419."[53]

The Commission, however, finds these contentions untenable. Respondents cannot justify their use of Complainants' Affidavit of Desistance under Section 13 (f) of the DPA as one of the exceptions for processing sensitive personal information and privileged information, to wit:

---

[50] *Id*, chapter I, § 3 (l) (2012).
[51] Complaints-Assisted Form dated 14 March 2023 of Spouses JG and AG, at p. 7.
[52] *Id*, at p. 7 and Annex 1 "Joint and Consolidated Reply Affidavit" at p. 28.
[53] Verified Comment dated 02 May 2023 of Spouses CP and CC, at p. 16.

> (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.[54]

The Principle of Legitimate Purpose, as one of the General Data Privacy Principles under the DPA, provides that "personal information must be collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only."[55]

The Commission has previously held that "processing done for the establishment of a legal claim should not in any manner be outside the limitations provided by law.[56] The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings."[57]

In this case, the personal information and sensitive personal information obtained were secured through unauthorized means as can be clearly inferred from Respondents' admission that the subject documents were received from "good minded persons with access to NBI records."[58]

As to the identity of these "good minded persons," the evidence presented by the Respondents are bereft of any showing regarding their authority to acquire and release these records. Hence, Respondents' processing of Complainants' personal and sensitive personal information failed to comply with the General Data Privacy Principle of Legitimate Purpose as it is incompatible with a declared and specified purpose not contrary to law, morals, or public policy.[59]

---

[54] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter III, § 13(f) (2012).

[55] *Id*, chapter III, § 11(a) (2012).

[56] JBD v. JI and VVV, NPC 18-D-012, Decision dated 21 January 2021, at p. 13.

[57] *Id*.

[58] Complaints-Assisted Form dated 14 March 2023 of Spouses JG and AG, at p. 7 and Annex 1 "Joint and Consolidated Reply Affidavit" at p. 28.

[59] National Privacy Commission, Implementing Rules and Regulations of the Data Privacy Act of 2012, rule IV, § 18(b) (2016).

In view of the foregoing, the Commission finds that Respondents' act of processing Complainants' personal information and sensitive personal information by attaching and using the Reply Affidavit of Complainants in the proceedings before the OCP-QC without any lawful basis constitutes unauthorized processing under Section 25 of the DPA.[60]

WHEREFORE, premises considered, this Commission hereby:

1. **HOLDS** Respondent Spouses CP and CC liable for violating Section 25 of the Data Privacy Act of 2012; and
2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice and recommends the prosecution of Spouses CP and CC for Unauthorized Processing of Personal Information and Sensitive Personal Information under Section 25 of the DPA.

SO ORDERED.

City of Pasay, Philippines.
13 November 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

---

[60] Complaints-Assisted Form dated 14 March 2023 of Spouses JG and AG, at p. 7.

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

JG and AG
Complainants

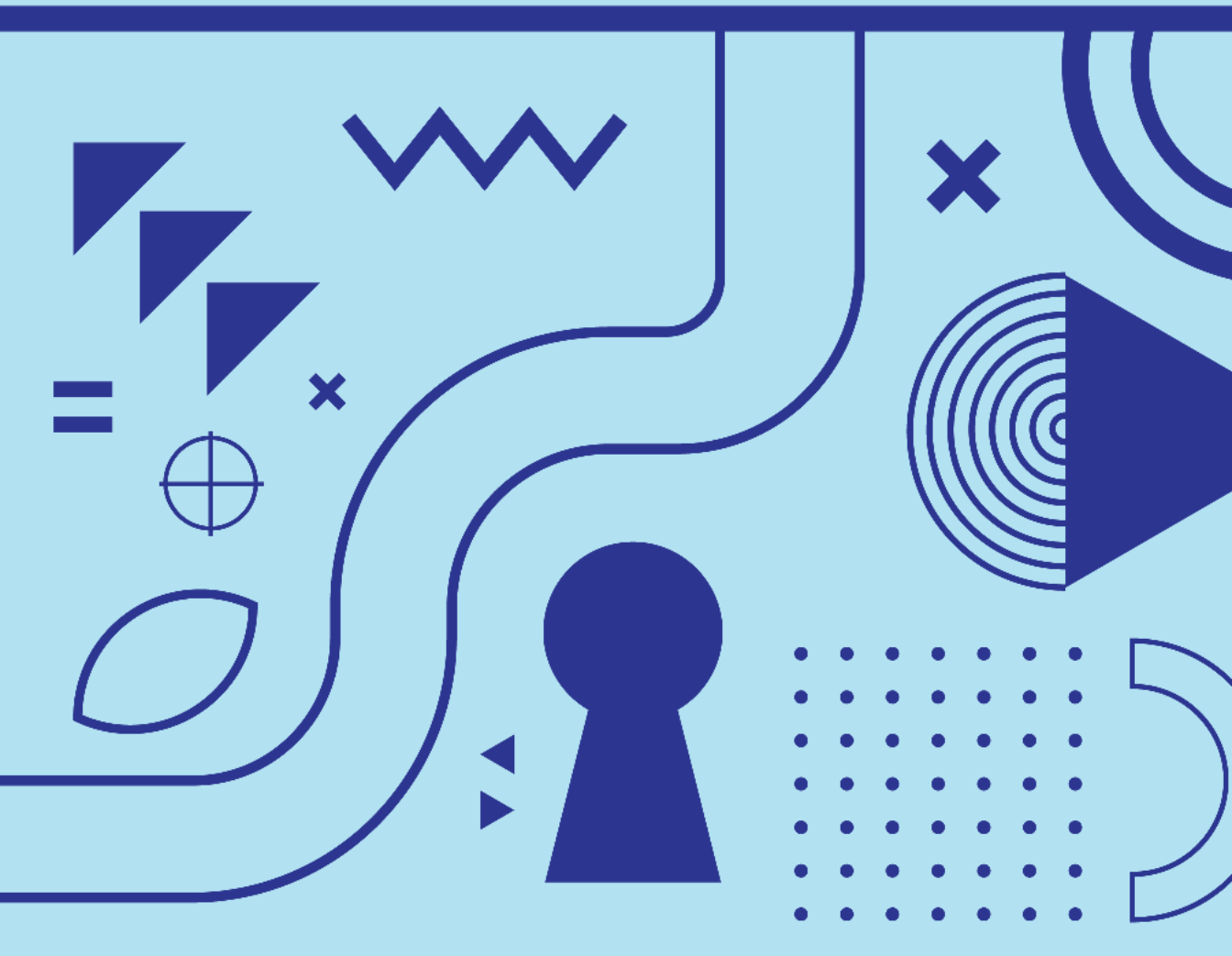
CP and CC
Respondents

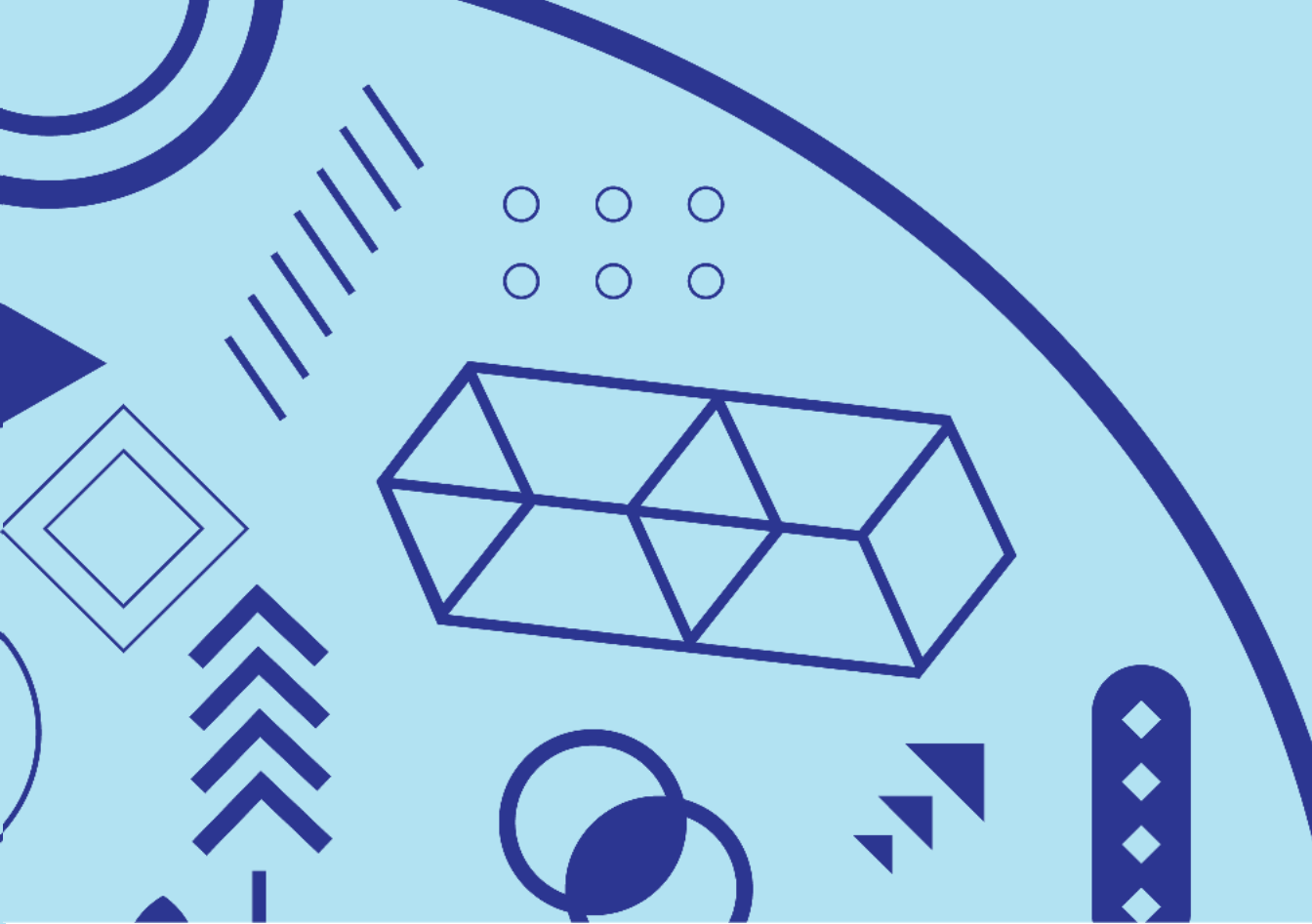
CRC
Counsel for Complainants

BMV and JO
Counsel for Respondents

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

ORDERS





IN RE: PHILIPPINE VETERANS BANK

NPC BN 22-185

x----------x

ORDER

Before the Commission are the requests for exemption and postponement from the notification requirement to the affected data subjects filed by Philippine Veterans Bank (PVB) dated 28 October 2022.[1]

Based on its Initial Report, the Finance Department of PVB conducted a mass transfer of its information technology (IT) equipment in June 2021 from Sterling Building to PVB's Head Office.[2] According to PVB, among the transferred equipment are ten (10) computers dedicated for simulation and testing of R system which is a system used by PVB to calculate economic variables.[3] PVB reported that by using the R system, the personal data uploaded therein are "loan borrower's name, birthdate, address of the collateral if real estate and/or model unit of vehicle if car loan, outstanding balance, insurance coverage and number of days past due, if applicable, of PVB loan borrowers for the year 2019."[4]

PVB also stated that the computers containing the R system "cannot be turned-on/logged-in successfully without being attached to the PVB domain" and that it can only be accessed by authorized users.[5] It also

---

[1] In re: Philippine Veterans Bank, NPC BN 22-185, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Date of Notification of Philippine Veterans Bank (28 October 2022).

[2] *Id.*, 1.b Chronology

[3] *Id.*, 1.b Chronology

[4] *Id.*, 1.b Chronology

[5] In re: Philippine Veterans Bank, NPC BN 22-185, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.b Chronology of Philippine Veterans Bank (28 October 2022).

stated that any attempt to access the system without permission, it will prompt the PVB administrator.[6]

During the inventory of the deployed IT equipment, two (2) computers cannot be traced in PVB's system.[7] PVB stated that it is conducting personal verification of all the units to confirm if the said units were lost or deployed but were unrecorded.[8]

On 28 October 2022, PVB notified the Commission and stated that it only discovered of the alleged breach on 25 October 2022.[9]

PVB also reported that there are thirty-two thousand two hundred seventy-four (32,274) affected data subjects who are loan borrowers of PVB.[10]

In justifying its request for exemption, PVB stated that the "lost computers do not contain sensitive personal information and there is no reason to believe that there may be an unauthorized access to the personal data considering the Bank's technical security measures in place.[11]

On the other hand, PVB justified its request for postponement when it stated that it has yet to complete its investigation.[12] PVB also stated that there is a possibility that the lost computers were deployed to other bank units.[13] Lastly, PVB stated that "individual notification is not possible and would require disproportionate effort since the data subjects involved are around 32,274."[14]

---

[6] *Id.*, 1.b Chronology
[7] *Id.*, 1.b Chronology
[8] *Id.*, 1.b Chronology
[9] In re: Philippine Veterans Bank, NPC BN 22-185, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.b Chronology of Philippine Veterans Bank (28 October 2022).
[10] *Id.*, in Date of Discovery.
[11] *Id.*, in Justification for Exemption.
[12] *Id.*, in Justification for Postponement.
[13] In re: Philippine Veterans Bank, NPC BN 22-185, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), in Justification for Postponement of Philippine Veterans Bank (28 October 2022).
[14] *Id.*, in Justification for Postponement.

On 11 January 2023, the Commission issued a Minute Resolution ordering PVB to submit proof to substantiate its requests for exemption and postponement from the notification requirement:

> Pursuant to Section 17 (D) of NPC Circular No. 16-03 (Personal Data Breach Management), the Commission may require additional information, if necessary, for the proper resolution of the request for Exemption.
>
> **WHEREFORE**, premises considered, the Commission hereby **ORDERS** Philippine Veterans Bank to **SUBMIT** within five (5) days upon receipt of this Minute Resolution proof to substantiate the request for Postponement and Exemption.
>
> Should Philippine Veterans Bank fail to provide the foregoing, this case shall be submitted for resolution based on the records before the Commission.
>
> **SO ORDERED.**[15]

To this date, PVB has yet to submit its compliance to the said Minute Resolution.

Rule V, Section 18(A) of NPC Circular No. 16-03 (Personal Data Breach Management) provides that the personal information controller (PIC) should notify the data subjects affected by the breach within seventy- two (72) hours upon knowledge of or reasonable belief that a personal data breach has occurred.[16] Such notification shall be made to "allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach."[17]

Further, Section 18(B) of the same Circular also provides that a PIC may be exempted from the notification requirement based on the Commission's determination that such notification would not be in the interest of the public or the affected data subjects.[18]

---

[15] *In re: Philippine Veterans Bank*, NPC BN 22-185, Minute Resolution dated 11 January 2023, at p. 1
[16] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V,
§ 18(A) (15 December 2016) (NPC Circular 16-03)
[17] NPC Circular 16-03, rule V, § 18(A).
[18] *Id.*

Moreover, a request for postponement may be authorized by the Commission if the notification may "hinder the progress of a criminal investigation related to a serious breach."[19]

In this case, PVB failed to provide proof that will substantiate its requests for exemption and postponement from the notification requirement.

As to its request to be exempt to notify, PVB was not able to submit proof that the notification would not be in the public interest or in the interest of the affected data subjects.

On the other hand, PVB stated that the bank has yet to complete its investigation, hence its request for postponement to notify.[20] However, PVB was not able to prove whether the investigation it conducted is a criminal investigation contemplated by NPC Circular No. 16-03. The mere report that PVB has yet to complete its investigation is not sufficient to grant the request to postpone the notification requirement to the affected data subjects.

Thus, this Commission emphasizes that PVB, as PIC, must be reminded of its obligation to notify the data subjects affected by the breach for them to take necessary precautions in order to mitigate further risk of exposure of their personal data.

WHEREFORE, premises considered, the requests of Philippine Veterans Bank (PVB) for exemption and postponement of notification of the data subjects affected by the breach is hereby **DENIED.**

The Commission **DIRECTS** the Compliance and Monitoring Division (CMD) to issue the appropriate orders necessary to evaluate and monitor the completeness of PVB's data breach notification and assess its breach management pursuant to NPC Circular No. 16-03 (Personal Data Breach Management)

---

[19] *Id.*, § 18(B)
[20] In re: Philippine Veterans Bank, NPC BN 22-185, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), in Justification for Postponement of Philippine Veterans Bank (28 October 2022).

SO ORDERED.

City of Pasay, Philippines.
26 January 2023.

JOHN HENRY D. NAGA
Privacy Commissioner

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NERISSA N. DE JESUS
Deputy Privacy

Commissioner Copy furnished:

VTV
Data Protection Officer

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: ASIA UNITED BANK CORPORATION

NPC BN 22-119

x----------x

ORDER

Before the Commission is the request for exemption from the notification of affected data subjects filed by Asia United Bank Corporation (AUB) dated 12 August 2022.[1]

According to AUB, its credit card delivery courier, Entrego, reported that on 05 August 2022, it erroneously emailed to Unionbank the Daily Progressive Report intended for AUB.[2] On the same date, Entrego stated that Unionbank called its attention to the erroneous email it sent.[3] Entrego then requested Unionbank to immediately delete the Daily Progressive Report in the email.[4] AUB further alleged that Unionbank confirmed the deletion of the erroneous email on the same date and provided proof of such deletion.[5]

AUB reported that the Daily Progressive Report contains information such as the credit cardholder's name, delivery address, pick-up and delivery dates, delivery recipient name and signature,[6] and recipient's ID type and number.[7]

---

[1] In re: Asia United Bank Corporation, NPC BN 22-119, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Date of Notification of Asia United Bank Corporation (12 August 2022).
[2] *Id.*, 1.b Chronology of Asia United Bank Corporation (12 August 2022).
[3] *Id.*, 1.b Chronology.
[4] *Id.*, 1.b Chronology.
[5] In re: Asia United Bank Corporation, NPC BN 22-119, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.b Chronology of Asia United Bank Corporation (12 August 2022).
[6] *Id.*, 1.b Chronology.
[7] *Id.*, 1.b Chronology.

Moreover, AUB stated that there are at least one thousand two hundred twenty-nine (1,229) data subjects involved in the alleged breach.[8] However, AUB mentioned that if the delivery recipient is not the cardholder himself/herself, then "a maximum of two thousand four hundred fifty-eight (2,458) data subjects are involved."[9]

In justifying its request for exemption, AUB stated that Unionbank "has already confirmed deletion of said email and report from its records."[10]

On 11 January 2023, the Commission issued a Minute Resolution ordering AUB to submit proof to substantiate its request for exemption to notify the data subjects:

> Pursuant to Section 17 (D) of NPC Circular No. 16-03 (Personal Data Breach Management), the Commission may require additional information, if necessary, for the proper resolution of the request for Exemption.
>
> **WHEREFORE,** premises considered, the Commission hereby **ORDERS** Asia United Bank Corporation to **SUBMIT** within five (5) days upon receipt of this Minute Resolution proof to substantiate the request for Exemption.
>
> Should Asia United Bank Corporation fail to provide the foregoing, this case shall be submitted for resolution based on the records before the Commission.
>
> **SO ORDERED**.[11]

In compliance with the Minute Resolution, AUB submitted its Supplemental Request for Exemption dated 18 January 2023.[12]

---

[8] *Id.*, 1.c Number of DS/Records.
[9] In re: Asia United Bank Corporation, NPC BN 22-119, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.c Number of DS/Records of Asia United Bank Corporation (12 August 2022).
[10] *Id.*, in Justification for exemption.
[11] *In re: Asia United Bank Corporation*, NPC BN 22-119, Minute Resolution dated 11 January 2023, at
p. 1.
[12] Supplemental Report for Exemption dated 18 January 2023 of Asia United Bank Corporation.

AUB explained in its Supplemental Request that Entrego promptly coordinated with Unionbank regarding the deletion of the Daily Progressive Report "both from the concerned mailbox and trash bin."[13]

Additionally, in justifying its request for exemption, AUB stated that the notification is not in the interest of the public or the affected data subjects as it may cause unnecessary worry and anxiety among them, citing In re: Health Delivery System, Inc, NPC BN 20-049.[14]

AUB also explained that Unionbank's acquisition and access to the Daily Progressive Report were only for less than six (6) hours and were deleted from its records within the same day.[15] AUB reiterated in its request for exemption that Unionbank "confirmed and provided proof that the erroneously emailed Daily Progressive Report has been deleted from its records."[16]

Lastly, AUB requested the Commission to allow it to submit the incident report from Entrego and the certification of deletion issued by Unionbank.[17]

On 20 January 2023, AUB sent to the Commission, via email, Entrego's incident report dated 06 August 2022.[18] The incident report stated that Entrego referred the incident to its Human Resources "for the imposition of disciplinary sanction on the erring employee for his negligence."[19] Entrego also stated that the Progressive Daily Report mistakenly sent to Unionbank was not password protected which violates Entrego's Information Security Policy and Data Privacy Governance and Management Manual.[20]

Rule V, Section 18(A) of NPC Circular No. 16-03 (Personal Data Breach Management) states:

---

[13] *Id.*, at p. 2.
[14] *Id.*, at pp. 2-3.
[15] *Id.*, at p. 3.
[16] Supplemental Report for Exemption dated 18 January 2023 of Asia United Bank Corporation, at p. 1.
[17] *Id.*, at p. 3.
[18] Electronic mail dated 20 January 2023 from Asia United Bank Corporation.
[19] Incident Report dated 06 August 2022 of Entrego.
[20] Electronic Mail dated 20 January 2023 from Asia United Bank.

> A. *When should notification be done.* The **data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.** The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. **It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.** It may be supplemented with additional information at a later stage on the basis of further investigation.[21] (Emphasis supplied)

Moreover, a request for exemption from the notification requirement, as determined by the Commission to be meritorious, may be granted if "such notification would not be in the public interest or in the interest of the affected data subjects."[22]

In this case, AUB failed to substantiate its request for exemption to notify the affected data subjects since it was not able to show that the notification would not be in the interests of the public or the affected data subjects. Specifically, AUB failed to submit proof that Unionbank actually deleted the erroneous email containing the Daily Progressive Report.

Thus, the Commission deems it proper to deny AUB's request for exemption from the notification requirement for failure to substantiate its request. It must be emphasized that the notification to the data subjects will allow them to undertake necessary precautions to mitigate the further exposure of their personal information especially if such information involves details regarding their financial capacity or status with the bank.

WHEREFORE, premises considered, this Commission **DENIES** the request of Asia United Bank Corporation (AUB) for the exemption of notification of the data subjects affected by the breach.

---

[21] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V,
§ 18 (A) (15 December 2016) (NPC Circular 16-03).
[22] NPC Circular 16-03, rule V, § 18 (B).

The Commission **DIRECTS** the Compliance and Monitoring Division (CMD) to issue the appropriate orders necessary to evaluate and monitor the completeness of AUB's data breach notification and assess its breach management pursuant to NPC Circular No. 16-03 (Personal Data Breach Management).

SO ORDERED.

City of Pasay, Philippines.
26 January 2023.

JOHN HENRY D. NAGA
Privacy Commissioner

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NERISSA N. DE JESUS
Deputy Privacy

Commissioner Copy furnished:

EMC
Data Protection Officer

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: MEDICARD PHILIPPINES, INC. **NPC BN 21-192**

x----------x

ORDER

Before this Commission is a Request for Extension and Alternative Means of Notification dated 29 December 2021, submitted by MediCard Philippines, Inc. (MediCard), through email, in relation to breach notification proceedings for a ransomware attack on its database servers.

The Facts

On 28 October 2021, the Commission issued a Resolution (Resolution) denying MediCard's request for exemption to notify the data subjects. It further ordered MediCard to notify the data subjects with corresponding proof of notification; submit its Full Breach Report; provide proof of its declaration that no company and data subject information was exposed and proof of security measures; and show cause in writing as to why it should not be subjected to contempt proceedings for failure to submit its Full Breach Report, *to quote*:

> **WHEREFORE,** premises considered, this Commission **DENIES** the request of MediCard Philippines, Inc. for the exemption or in notifying the data subjects affected by the breach.
>
> MediCard Philippines, Inc. is hereby **ORDERED** to comply with the following **within fifteen (15) days** from receipt of this Resolution:
>
> 1. **NOTIFY** the affected data affected subjects pursuant to Section 18 of the NPC Circular No. 16-03 and submit proof of compliance thereof, including the proof of receipt of the data subjects of such notification;

2. **SUBMIT** a Full Breach Report pursuant to Section 9 and 17 (D) of the NPC Circular No. 16-03;

3. **SUBMIT** proof of its declaration that no company and data subject information was exposed and proof of security measures indicated in the Forensic Report dated 12 October 2021; and

4. **SHOW CAUSE** in writing why it should not be held liable for its failure to submit its Full Breach Report within the prescribed period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.

SO ORDERED. [1]

On 29 December 2021, MediCard sent an email to the Commission stating that it received the Resolution on 16 December 2021. Further, MediCard claims that it needs additional time of fifteen (15) days within which to comply with the given orders of the Commission. The reason cited for additional time needed is for the MediCard to further coordinate with its third-party cybersecurity service provider owing to logistical and communication challenges brought about by the COVID-19 pandemic and the intervening holidays.[2]

Aside from the request for additional time to comply, MediCard stated that it is considering notifying the affected data subjects through alternative means.[3] MediCard claims that it does not have the affected data subjects' contact information (e.g. current mobile number, email address, and residential address). MediCard further stressed that for company-sponsored accounts, the data subjects' employer or company directly coordinates with MediCard for the claims and benefits. Hence, MediCard would have no visibility on the personal contact details of the data subject who is the employee- beneficiary.[4]

---

[1] Resolution dated 28 October 2021.
[2] MediCard Email Request dated 29 December 2021.
[3] Id.
[4] Id.

Thus, MediCard requests that the Commission allow it to notify the affected data subjects by: 1) sending a notification through the companies/employees of the affected data subjects; or 2) publication through its website.[5]

Issues

1. Whether MediCard's request for additional time to comply with the Commission's orders stated in its Resolution dated 28 October 2021 be granted; and
2. Whether MediCard's request for alternative means of notification be granted.

Discussion

The Commission grants MediCard's request for additional time to comply with its orders provided in the Resolution dated 28 October 2021. However, the Commission denies MediCard's request for the use of alternative means of notification.

The Commission grants the request for additional time to comply.

Section 17(C) of NPC Circular No. 16-03 (Personal Data Breach Management) provides:

> SECTION 17. *Notification of the Commission.* The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> xxx
>
> C. *When delay is prohibited.* There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the

[5] *Id.*

> 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless the personal information controller is granted additional time by the Commission to comply."[6]

Further, Section 18(A) of the same Circular states:

> **SECTION 18.** ***Notification of Data Subjects.*** The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> A. *When should notification be done.* The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.[7]

As previously ruled by the Commission in its Resolution dated 28 October 2021, this case falls under the mandatory notification requirement.[8] Further, MediCard shall comply with the periods as provided in NPC Circular No. 16-03. The Full Breach Report must be submitted within five (5) days from filing the initial report.[9] While, the notification to the affected data subjects must be made on the basis of available information within the 72-hour period.[10]

However, MediCard asks for additional period to comply with the Commission's orders indicated in its Resolution dated 28 October 2021 because of the logistical and communications challenges in

---

[6] Section 17(C) of the NPC Circular No. 16-03
[7] Section 18(A) of the NPC Circular No. 16-03.
[8] Resolution dated 28 October 2021. At page 5.
[9] Section 17(C) of the NPC Circular No. 16-03.
[10] Section 18(A) of the NPC Circular No. 16-03.

coordinating with its third-party cybersecurity service provider due to the intervening holidays and the COVID-19 pandemic.[11]

The Commission emphasizes that in cases of data breach, especially cases that fall under the mandatory notification rule, personal information controllers (PICs) must ensure compliance with their obligations under the law including the prompt adherence with the periods provided in the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other relevant issuances of the Commission such as NPC Circular No. 16-03.

However, in the interest of substantial justice and due process, the Commission exercises its authority to grant MediCard the additional non-extendible period of fifteen (15) days from receipt of this Resolution to comply with Commission's orders indicated in the Resolution dated 28 October 2021.

Individual notification has not been shown to be impossible or requires disproportionate effort as provided in Section 18(D) of the NPC Circular No. 16-03.

While the Commission grants MediCard additional period to comply with the Resolution, it denies Medicard's request to notify the affected data subjects through alternative means.

Section 18(D) of NPC Circular No. 16-03 provides the form of notification for affected data subjects, *thus:*

> **SECTION 18. *Notification of Data Subjects***. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> xxx
>
> *D. Form.* **Notification of affected data subjects shall be done individually, using secure means of communication, whether**

[11] MediCard Email Request dated 29 December 2021.

> **written or electronic**. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.
>
> The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach**: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner**: *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[12] (Emphases supplied)

Given that MediCard has yet to submit its Full Breach Report, and other crucial information regarding the data breach such as notification to the affected data subjects and proof of its security measures, there is insufficient information on whether the resort to alternative means of notification is proper.

MediCard has not proven that individual notification is not possible or would require disproportionate effort. According to MediCard the request for the alternative means in notifying the affected data subjects is due to the reason that it does have their contact information which includes their current mobile number, email address, and residential address.[13] However, a scrutiny of the record reveals that MediCard has the requisite contact details for the affected data subjects.[14]

In its Initial Report dated 22 September 2021, MediCard identified possible personal data that may have been subjected to the breach, which included email addresses of its MediCard Members or App users.[15] MediCard also identified that the possible personal data of its own employees may have been involved in the breach. Thus, given

---

[12] Section 18(D) of the NPC Circular No. 16-03.
[13] MediCard Email Request dated 29 December 2021.
[14] Initial Report dated 22 September 2021. At page 2.
[15] Id..

that it has the email addresses of both members and employees, MediCard has no reason to use alternative means of notification. MediCard must then pursue individual notification as provided under Section 18(D) of NPC Circular No. 16-03.

As for MediCard's claim that for company-sponsored accounts, only the data subjects' company or employer directly coordinates with it, MediCard should be reminded that under the law, it is considered a PIC. A PIC is defined as one "who controls the processing of personal data, or instructs another to process personal data on its behalf."[16] Control is present when the entity "decides on what information is collected, or the purpose or extent of its processing."[17]

The nature of MediCard's business in processing claims and medical benefits for beneficiaries means that it has the requisite ability to decide on what information is collected, including its purpose and extent of processing.

Consequently, as the PIC and given that it controls the information given for processing, MediCard is responsible for complying with the notification requirements under NPC Circular No. 16-03 in case of data breach. It has the obligation to exert diligent efforts to coordinate with the relevant companies in order to provide information to the affected data subjects.

Hence, MediCard shall notify its affected data subject individually, using secure means of communication, whether written or electronic pursuant to Section 18(D) of the NPC Circular No. 16-03.

WHEREFORE, premises considered, Medicard Philippines, Inc.'s request for an additional period of time to comply with the Resolution dated 28 October 2021 is hereby **GRANTED.** Further, its request for the notification of the affected data subjects through alternative means is hereby **DENIED.**

---

[16] Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 3(m).
[17] Id.

MediCard is **ORDERED** to comply **within a non-extendible period of fifteen (15) days upon receipt of the Resolution,** with the orders of the Commission as stated in its Resolution dated 28 October 2021.

SO ORDERED.

City of Pasay, Philippines.
13 January 2022.

JOHN HENRY D. NAGA
Privacy Commissioner

I CONCUR:

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

RTM
Data Protection Officer

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: GRAB PHILIPPINES **NPC CC 20-001**

x----------x

ORDER

Before the Commission is the Compliance/Manifestation of Grab Philippines (Grab PH) dated 03 March 2022 to the Resolution dated 03 February 2022.

On 03 February 2022, the Commission issued a Resolution requiring Grab PH to comply with the following:

> **WHEREFORE,** premises considered, this Commission hereby **NOTES** the following: 1) Motion to Resolve (Re: Compliance and Motion to Lift Cease-And-Desist Order dated 3 February 2020), dated 19 January 2022; and 2) Compliance and Motion to Lift Cease-And-Desist Order dated 3 February 2020, dated 22 June 2021, submitted by Grab PH.
>
> Grab PH is **ORDERED** to submit its Privacy Impact Assessment for its In-Vehicle Audio Recording project within fifteen (15) days from receipt of this Resolution.[1]

In compliance with the Resolution, Grab PH submitted its Privacy Impact Assessment (PIA) In-Vehicle Audio Recording dated 06 February 2020.[2]

On 03 March 2022, Grab PH submitted its Manifestation (Re: Resolution dated 03 February 2022) manifesting that "it has decided to indefinitely suspend the implementation of the In-Vehicle Audio Recording and In-Vehicle Video (CCTV) Recording projects."[3] Further, Grab PH manifested that "it has decided to implement only

---

[1] *In re: Grab Philippines,* NPC CC 20-001, Resolution dated 03 February 2022.
[2] Grab PH's Privacy Impact Assessment Consumer Verification via Selfie dated 06 February 2020.
[3] Grab Philippines Manifestation (Re: Resolution dated 03 February 2022) dated 03 March 2022, at p. 1.

the Consumer Verification via Selfie project as soon as the Cease-and- Desist Order (CDO) in the same is lifted by [the] Honorable Commission."[4]

The National Privacy Commission's Compliance and Monitoring Division (CMD) issued its Technical Report dated 17 May 2022[5] (Technical Report) to the Compliance submitted by Grab PH.

In the Resolution dated 03 February 2022, the Commission ordered Grab PH to submit its Privacy Impact Assessment (PIA) In-Vehicle Audio Recording.[6]

Nevertheless, this Commission deems it appropriate that Grab PH must first remediate the issues found in its PIA in accordance with the DPA.

In Grab PH's PIA on the Consumer Verification via Selfie dated 6 February 2020, it stated that:

> Consumer Selfie data retention period are as follows:
>
> xxx
>
> 3. Retain the Consumer selfie for the Consumers who are related to safety incidents. The data of Consumers involved in safety incidents are retained as long as Grab or its affiliate/successor offers its services to the public. We need to retail the data because if the Consumer decides to come back and create another account in the future, if an account has been blocked that has a safety incident, the Consumer will not be able to create it based on the selfie.[7]

In the Technical Report of CMD, it was indicated that:

> In this case, Grab PH may consider as the basis of its retention period the prescriptive periods in filing the appropriate action for the resolution of the safety incident in the proper court or

---

[4] *Id.*
[5] Compliance and Monitoring Division (CMD), Revised Technical Report on Grab Philippines' Consumer Verification via Selfie Project dated 17 May 2022.
[6] *In re: Grab Philippines.* NPC CC 20-001, Resolution dated 03 February 2022.
[7] Grab PH's Privacy Impact Assessment Consumer Verification via Selfie dated 06 February 2020, at p. 15-16.

> forum. Likewise, Grab PH may also consider defining the various gravity of its safety incidents and accordingly adjust the retention period depending on the gravity.[8]

Section 11 (e) of the DPA provides:

> SEC. 11. *General Data Privacy Principles.* – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.
>
> Personal information must be:
>
> xxx
>
> (e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law;[9]
>
> xxx

Here, Grab PH indicated in its PIA that the Consumer Selfie may be retained as long as necessary if it is related to safety incidents.[10] However, the Commission considers that while these may be limited to individuals involved in safety incidents, the retention for an indefinite period is contrary to the DPA.

The Commission deems it appropriate that by revising the retention period stated in Grab PH's PIA and aligning it to the DPA, it essentially acquaints the data subject on how the personal data is being retained consistent with its purpose to "reduce criminal incidents and improve safety to its riders."[11]

As to the disposal of selfie data, Grab PH indicated in its PIA:

---

[8] Compliance and Monitoring Division (CMD), Revised Technical Report on Grab Philippines' Consumer Verification via Selfie Project dated 17 May 2022, at p. 4.
[9] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter III, § 11 (e) (2012).
[10] Grab PH's Privacy Impact Assessment Consumer Verification via Selfie dated 06 February 2020, at p. 15-16.
[11] *Id.*, at p. 4.

> The disposal of selfie data stored in AWS S3 is done by the Grab Database Team, upon request and approval from the Grab Safety Engineering Team. Selfie data will be disposed if:
>
> - Requested by the Consumer (not available for users who have committed crime or have otherwise violated Code of Conduct and had their account access privileges revoked);
>
> - Selfie will be removed after the Consumer account becomes inactive i.e dormant, per Grab account archival policy, unless the account is related/involved in any safety incidents. Grab will delete the data of Consumers who are dormant after 180 days. The cleanup activity (of selfie data) is manually triggered by Grab Safety Engineers once in every six (6) months. The deletion process is triggered manually once in 6 months and safety teams are implementing to auto trigger the deletion process once in 6 months. (ETA to implement auto triggers is by the end of 2021). If consumers were involved in any safety incidents, their selfie will not be deleted.[12]

Rule IV, Section 19 D (3) of the Implementing Rules and Regulation of the Data Privacy Act of 2012 (IRR), provides that:

> Section 19. General principles in collection, processing and retention. The processing of personal data shall adhere to the following general principles in the collection, processing, and retention of personal data:
>
> d. Personal Data shall not be retained longer than necessary.
>
> xxx
>
> 3. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.[13]

In Grab PH's PIA, it was not mentioned whether the selfie data would be stored permanently on AWS S3 servers.[14] It is uncertain whether the

---

[12] *Id.*, at p. 18.
[13] National Privacy Commission, Implementing Rules and Regulations of the Data Privacy Act of 2012, rule IV, § 19 D (3) (2016).
[14] Grab PH's Privacy Impact Assessment Consumer Verification via Selfie dated 06 February 2020.

safe disposal of selfie data on the records is manifested in some other document.[15]

To adhere to the general privacy principles, the Commission requires Grab PH to submit in detail the secure manner of disposal of the consumer selfie upon its deletion from the AWS S3 system. The data subject has the right to be informed on how the personal data is being disposed of to prevent unnecessary processing.[16]

It must be noted that the PIA for Consumer Verification via Selfie is dated 06 February 2020 and the revised PIA for Consumer Verification via Selfie already includes Grab PH's compliance with the Commission's findings and the project's expansion to include users of Grab PH delivery services.[17]

Nonetheless, Grab PH must ensure that a regular conduct of the PIA is done to avoid security incidences and data breaches from occurring not only for this project but for its other systems, programs, measures, procedures, and technology products as well. Grab PH, the PIC, may require Amazon AWS, the PIP, to conduct a PIA to ensure that all possible risks were addressed.[18]

Based on the foregoing, the Commission deems it necessary that Grab PH must address the issues prior to the lifting of the Cease-and-Desist Order.

WHEREFORE, premises considered, the Commission hereby
ORDERS Grab Philippines to:

1) **REVISE** the retention period involving consumer selfie of individuals involved in safety incidents and **SUBMIT** the revised PIA incorporating such;

---

[15] *Id.*
[16] National Privacy Commission, Implementing Rules and Regulations of the Data Privacy Act of 2012, rule IV, § 19 D (3) (2016).
[17] Grab Philippines Compliance and Motion to Lift Cease-and-Desist Order. Dated 22 June 2021.
[18] National Privacy Commission (NPC) Advisory 17-03, 31 July 2017, Guidelines on Privacy Impact Assessment, at p. 5.

2) **SUBMIT** the documents detailing the secure manner of disposal of the consumer selfie upon deletion from the AWS S3 system; and
3) **INCLUDE** AWS S3 in the next conduct of Privacy Impact Assessment to ensure that all possible risks are addressed. If AWS S3 conducts its own PIA, consider appending the same to Grab PH's PIA.

Grab PH shall **SUBMIT** its compliance with the aforementioned directives of the Comission directly to the Compliance and Monitoring Division (CMD) within fifteen (15) upon receipt of this Order.

SO ORDERED.

City of Pasay, Philippines.
19 January 2023.

JOHN HENRY D. NAGA
Privacy Commissioner

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

DG
Data Protection Officer

QT
Counsel for Grab Philippines

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: METRO PACIFIC TOLLWAYS CORPORATION **NPC BN 23-015**

x----------x

ORDER

Before the Commission is Metro Pacific Tollways Corporation's (MPTC) requests for postponement and exemption to notify affected data subjects.

On 26 January 2023, MPTC was informed of a suspicious user activity caused by an individual who created several accounts or via multiple referrals in the MPT DriveHub application.[1] The MPT DriveHub application is MPTC's travel companion application that offers mobility solutions such as RFID transaction, trip planning, and roadside assistance to its registered users.[2]

MPTC surmised that the several accounts were created in an attempt to earn more points or raffle entries to win prizes in MPTC's "Download, Drive, & Win" promotion, which ran from 11 November 2022 to 31 January 2023.[3]

In its investigation, MPTC confirmed that the multiple duplicate registrations used the same email address and mobile number to register.[4] MPTC believed that this indicated a potential breach of the MPT DriveHub application system with possible access to others' personal information such as name, username, and email address.[5]

---

[1] Initial Notification through the Personal Data Breach Notification Form, 27 January 2023, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*

On 27 January 2023, MPTC notified the National Privacy Commission (NPC) of the breach through the Data Breach Notification Management System (DBNMS).[6]

In its initial report, MPTC stated that the number of data subjects affected is one hundred (100) but that the actual number is still to be determined.[7]

MPTC claimed that it was in the process of "conducting a comprehensive investigation to determine the details of the incident, [particularly] the potential exposure of personal information and the appropriate and necessary measures to be undertaken to address any vulnerabilities in its system."[8]

MPTC requested postponement to notify its affected data subjects.[9] It explained that it be allowed a reasonable period to notify its data subjects from the completion of the investigation in case its investigation determined that there was an actual breach.[10] It also argued that no notice to the data subjects is required at that point because its preliminary investigation indicated that there was no intrusion or access to personal information in its system.

On 06 February 2023, the Commission directed MPTC to submit proof to substantiate its request for postponement:

> **WHEREFORE,** premises considered, the Commission hereby **ORDERS** Metro Pacific Tollways Corporation to **SUBMIT** within five (5) days upon receipt of this Minute Resolution proof to substantiate the request for postponement to notify affected data subjects.
>
> Should Metro Pacific Tollways Corporation fail to provide the foregoing, this case shall be submitted for resolution based on the records before the Commission.
>
> **SO ORDERED.**[11]

---

[6] *Id.*
[7] Initial Notification through the Personal Data Breach Notification Form, 27 January 2023, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Minute Resolution, 06 February 2023, at 1, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).

On 09 February 2023, MPTC submitted its Compliance to the 06 February 2023 directive.[12]

MPTC requested the Commission to "instead grant an exemption to notify the affected data subjects."[13] It claimed that upon further investigation, there is "no evidence of personal information and sensitive personal information breach affecting data subjects."[14]

In its Compliance, MPTC reiterated that as a measure to address the breach, it conducted a comprehensive investigation to determine the details of the incident such as the mode of the attack, the vulnerabilities in its system, the identity of the hacker, and the potential exposure of personal information of other data subjects.[15]

MPTC maintained that the incident may have been done using a method called "Replay Attack", which permits the instant creation of several users.[16] MPTC defined Replay Attack as "an attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access."[17]

MPTC, however, claimed that the "attack was targeted more on inputting invalid raffle entries in an attempt to win, rather than on accessing personal data found in the MPT DriveHub databases."[18] Further, it firmly asserted that its investigation showed no evidence of leaked or extracted personal and sensitive personal information.[19]

MPTC's statements in its Compliance, however, is contrary to its prior representations in its initial report through the DBNMS. MPTC initially stated that there are one hundred (100) affected data subjects

---

[12] Compliance by Metro Pacific Tollways Corporation, 09 February 2023, at 1, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[13] *Id.*
[14] *Id.*
[15] *Id.* at 3.
[16] *Id.* at 2.
[17] *Id.*
[18] Compliance by Metro Pacific Tollways Corporation, 09 February 2023, at 2, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[19] *Id.* at 2-4.

although its actual number is still to be determined[20] and that there is possible access to personal information of others such as name, username, and email address.[21]

The Commission emphasizes that the notification requirement under NPC Circular 16-03 (Personal Data Breach Management) is for the protection and benefit of data subjects.[22] Section 11 of NPC Circular 16-03 requires a Personal Information Controller (PIC) to notify the Commission and the affected data subjects upon knowledge of or when there is reasonable belief by the PIC that a breach requiring notification occurred:

> Section 11. *When notification is required.* **Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred**, under the following conditions:
>
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.
>
> For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> B. There is reason to believe that the information may have been acquired by an unauthorized person; and
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[23]

---

[20] Initial Notification through the Personal Data Breach Notification Form, 27 January 2023, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[21] *Id.*
[22] In re: Breach Notification Report of Sun Life of Canada, CID BN 17-021, 10 September 2020, at 6, *available at* https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-BN-17-020-_- 029-09.22.2022-In-Re-Sun-Life-of-Canada_Resolution.pdf (last accessed 16 March 2023).
[23] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016). Emphasis supplied.

In addition, Section 13 of the same Circular provides that when the PIC is uncertain as to the need to notify, it shall take into account the likelihood of harm or negative consequences on the affected data subjects and how notification could reduce the risks arising from the data breach reasonably believed to have occurred.[24] The PIC shall also consider if the personal data reasonably believed to have been compromised involves at least one hundred (100) individuals:

> Section 13. *Determination of the Need to Notify*. Where there is uncertainty as to the need for notification, the personal information controller shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred.
>
> The personal information controller shall also consider if the personal data reasonably believed to have been compromised involves:
>
> . . .
>
> B. **At least one hundred (100) individuals**[.][25]

The Commission previously held that a PIC must notify its affected data subjects to allow them to take the necessary measures to protect themselves against possible effects of the breach:

> It is noteworthy that the avowed purpose of the required notification to data subjects of a breach incident is for them to take the necessary precautions or other measures to protect themselves against possible effects of the breach. Moreover, personal information controllers (PICs) are required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. It therefore follows that PICs should guarantee that the notification they sent to data subjects has been received. Otherwise, it defeats the very purpose of notification of data subjects.[26]

Given the inconsistencies in MPTC's submissions, however, the Commission cannot yet rule on MPTC's request for exemption to

---

[24] *Id.* § 13.

[25] *Id.* Emphasis supplied.

[26] In re: Batangas Bay Carriers, NPC BN 20-157, 17 December 2020, at 3, *available at* https://www.privacy.gov.ph/wp-content/uploads/2022/01/Resolution-NPC-BN-20-157-In-re- Batangas-Bay_Dec-17.pdf (last accessed 16 March 2023).

notify the data subjects without sufficient details on the number of those affected and personal or sensitive personal information involved in the incident.

Thus, it directs MPTC to submit additional information, and explain the disparity between its statements in its initial report and in its compliance with the directive dated 06 February 2023, regarding the number of data subjects and the personal or sensitive personal information involved, if any, in the incident.

WHEREFORE, premises considered, the Commission **ORDERS** Metro Pacific Tollways Corporation (MPTC) within ten (10) days from receipt of this Order to:

1. **SUBMIT** additional details on the number of data subjects and personal and sensitive personal information involved in the incident, if any; and

2. **EXPLAIN** the disparity between the number of data subjects and the involved personal and sensitive personal information stated in the initial report submitted through the DBNMS dated 27 January 2023 with the Compliance dated 09 February 2023.

SO ORDERED.

City of Pasay, Philippines.
16 March 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

CSM
Data Privacy Officer

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: E-SCIENCE CORPORATION **NPC BN 20-124**

x----------x

ORDER

AGUIRRE, D.P.C.:

This Resolution refers to the Full Breach Report submitted by E- Science Corporation ("E-Science") dated 18 August 2020 involving a data breach incident affecting approximately four thousand (4,000) test records of data subjects.[1]

The Facts

On 6 August 2020, this Commission issued a Resolution[2] with the following disposition:

> **WHEREFORE,** premises considered, E-Science Corporation is **ORDERED** to **1) SUBMIT** with dispatch a Full Report of the Personal Data Breach as required under Section 17(C) of NPC Circular No. 16-03; and **2) SHOW CAUSE** in writing why it should not be liable for failure to submit a Full Report within the required period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.
>
> Furthermore, the Commission **GRANTS** the request for Postponement of Notification to Data Subjects of E-Science Corporation and directs them to submit proof of compliance thereof within fifteen (15) days from submission of their Full Breach Report. Pending their verification of the full list of affected data subjects, E-Science Corporation is enjoined to use alternative means of notification under Section 18(d) of NPC Circular No. 16- 03.

On 18 August 2020, E-Science submitted a Full Breach Report[3] where it reiterated the contents of its Initial Report dated 2 July

[1] Full Breach Report dated 18 August 2020.
[2] Resolution dated 6 August 2020, *In re: E-Science Corporation*, NPC BN 20-124.

2020.[4] The Commission notes that in its Initial Report, E-Science stated that it is still currently doing further investigations and it has still not sent notifications to the affected data subjects so that it can prevent sending the same to unaffected individuals.[5] This was also indicated in the Full Breach Report it submitted.[6]

Moreover, a perusal of the written submissions made by E-Science reveals that it has not addressed the Show Cause Order issued by this Commission in the same Resolution.[7]

Discussion

This Commission hereby reiterates its Order against E-Science to Show Cause in writing why it should not be held liable for failure to submit a Full Breach Report within the required period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.

Section 17(C) of NPC Circular 16-03 provides that:

> There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72- hour period based on available information. **The full report of the personal data breach must be submitted within five (5) days**, unless the personal information controller is granted additional time by the Commission to comply.[8]

In this case, E-Science has submitted its Initial Report on 2 July 2020.[9] Thus, it should have submitted its Full Breach Report five
(5) days therefrom especially since E-Science did not request for and no additional time was granted by this Commission for the submission of such report. While it has requested for the postponement of notification to the affected data subjects on 3 July 2020,[10] which this Commission granted in the said Resolution,[11] the

---

[3] *Supra* note 1.
[4] Initial Data Breach Report dated 2 July 2020.
[5] *Ibid.*, at page 3.
[6] Full Breach Report dated 18 August 2020 at p. 4.
[7] *Supra* note 2.
[8] Emphasis supplied.
[9] *Supra* note 4.
[10] E-mail dated 3 July 2020 submitted by the Data Protection Officer of E-Science.
[11] *Supra* note 2.

submission of a Full Breach Report is a different requirement that E-Science should have complied with accordingly. Being provided under separate sections, E-Science should have known that the Notification of the Commission and Notification of Data Subjects are two (2) different and separate requirements under Sections 17(C) and 18(A) of NPC Circular No. 16-03, respectively, that personal information controllers should promptly comply.

WHEREFORE, premises considered, this Commission reiterates its **ORDER** against E-Science Corporation to **SHOW CAUSE** in writing **within five (5) days from receipt of this Resolution** why it should not be held liable for its failure to submit a Full Breach Report within the required period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.

The Full Breach Report dated 18 August 2020 submitted by E- Science Corporation is hereby **NOTED**, subject to the recommendations of the Compliance and Monitoring Division and further action of this Commission.

SO ORDERED.

Pasay City, Philippines;
27 August 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JYP
Data Protection Officer
E-Science Corporation

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: BREACH NOTIFICATION REPORT OF AXA PHILIPPINES INVOLVING JUICE AND WRAPPED IDEAS, INC.

CID BN No. 17-041

x----------x

ORDER

On 20 August 2019, the Commission issued a Resolution containing the following dispositive portion:

> WHEREFORE, all premises considered, it is resolved that there are no notable findings requiring further action from this Commission with regard to the data breach subject of the notification, and that AXA Philippines is ordered to submit a comprehensive report stating the above specifications and in compliance with Section 9 of Circular No. 16-03 within thirty (30) days of receipt of Resolution.

On 27 September 2019, AXA submitted its Compliance Report detailing the description of the personal data breach; actions and decisions of the incident response team; post-breach review and the outcome of the breach management and difficulties encountered; and compliance with notification requirements and assistance provided to affected data subjects.

In its Compliance Report, AXA conveyed that on 14 December 2017, after the report to this Commission was made and the partial list was retrieved, they informed known affected data subjects regarding this breach. They also conveyed that JWI was required to execute a certification that data collected for AXA has been deleted from all their systems, and said certification has been issued. AXA has terminated the services of JWI and removed them from their list of accredited suppliers. AXA likewise conducted a face-to-face data privacy training for the members of its Marketing Team on 20 December 2019.

On 14-15 September 2017, JWI mounted an event for AXA Philippines that utilized one iPad unit with a web-based registration app supported by a pocket Wi-Fi. During this event, the Distribution Team manned an activation booth and went around the food court to invite people to register. These individuals were considered "leads" to be contacted by the Marketing Team of AXA Philippines. On the first day of the event, the assigned project officer monitored the entries through the back-end Wordpress dashboard of the app. By the end of the event, there were a total of 107 entries for the first day and 118 entries for the second day.

Once the representative from JWI coordinated with their IT specialist for the extraction of the database from the two events, however, they found that only 49 entries were recorded for the first day and all the entries from the second day were gone. An internal investigation conducted by JWI confirmed that there were indeed data inputs during the dates of the events, as the app's server logs revealed records of users' transactions and logs into the app with time marks as early as 11:40 AM up to 6:41 PM of 15 September. The IT specialist also found that there was an "admin access" on the app's back-end on 18 September 2017 by an unidentified user, who exported and deleted entries.

AXA Philippines has since reported that it: (1) changed the log-in and password; (2) exported the database and saved it in a secure location; and
(3) continuously monitored the JWI server for possible intrusions of the app. AXA Philippines also reported that it ceased from engaging further with JWI after the incident, resolved to investigate employees who have dealt with JWI, and proposed to strengthen measures on third party engagements.

Notably, there is a lack of notification to the affected data subjects. While this may be attributed to the inability to do so due to the loss of personal information, the Commission takes note of a statement made in the breach notification report: *"We emphasize to the Honorable Commission at this point that: (1) The data subjects are not clients of AXA Philippines as they are supposedly potential "leads" to be contacted by our Marketing team..."* It must be noted, however, that Section 15 of Circular 16-03 provides that "the personal information controller shall notify... the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred. The obligation to notify remains with the personal information controller even if the processing of information is outsourced or subcontracted to a personal information processor." Hence, the fact that

the affected individuals were still "leads" and not clients of the personal information controller should not be a factor in considering whether to notify data subjects of a breach.

Upon consideration of the Investigator's Report and the Breach Notification of AXA Philippines, the Commission hereby resolves that there are no notable findings requiring further action from the Commission with regard to the data breach subject of the notification.

Taking note of the time that has lapsed since the incident, the Commission hereby requires a comprehensive report on the status of AXA Philippines' abovementioned investigation on the employees that have dealt with JWI, as well as its implementation of the "strengthened measures on third party engagements." Pursuant to Section 9 of Circular No. 16-03, the report shall also include:

A. A description of the personal data breach, its root cause and circumstances regarding its discovery;
B. Actions and decisions of the incident response team;
C. The outcome of the breach management, and difficulties encountered; and
D. Compliance with notification requirements and assistance provided to affected data subjects.

This report shall also include a procedure for a Post-Breach Review which must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor.

WHEREFORE, all premises considered, it is resolved that there are no notable findings requiring further action from this Commission with regard to the data breach subject of the notification, and that AXA Philippines is ordered to submit a comprehensive report stating the above specifications and in compliance with Section 9 of Circular No. 16-03 within **thirty (30)** days of receipt of this Resolution.

SO ORDERED.

City of Pasay, Philippines
20 August 2019.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
IVY D. PATDU
Deputy Privacy Commissioner

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

COPY FURNISHED:

IB
Data Privacy Officer
AXA Philippines

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FAMILYHAN CREDIT CORPORATION

Initiated as an Independent NPC Investigation into the Possible Data Privacy Violations Committed by Familyhan Credit Corporation

X----------X

NPC SS 20-001
For: Violation of the Data Privacy Act (DPA) of 2012

ORDER

This refers to the Motion to Lift Cease and Desist Order filed by Familyhan Credit Corporation (Familyhan) dated 21 June 2021.

Facts

On 15 October 2020, the Commission ordered Familyhan to cease and desist from the processing of personal data on their database:

> **WHEREFORE,** premises considered, Familyhan Credit Corporation and its responsible officers and members of the board, MTR, VBV, JPV, AA, and MDA are hereby ordered to:
>
> 1) File a **COMMENT,** within ten (10) days from receipt of this Order, on the allegations in the attached Fact Finding Report, pursuant to Section 24 of the NPC Rules of Procedure; and
>
> 2) **CEASE AND DESIST** from the processing of personal data on their database until the Commission issues a decision on the submission of the Comment, which shall be made no more than thirty (30) days from the expiration of the period to file a Comment or of the termination of the clarificatory hearing if one is held, pursuant to NPC Circular No. 20-02.
>
> **SO ORDERED.**[1]

[1] Order dated 15 October 2020.

On 25 January 2021, Familyhan filed its Comment to the Cease and Desist Order (CDO) and prayed that the Order and the initial findings of the Commission be reconsidered and dismissed:

> WHEREFORE, premises considered, it is most respectfully prayed unto this Honorable Office that the Initial findings of the Commission and the ORDER to CEASE AND DESIST from the processing of personal data on their database be RECONSIDERED AND DISMISSED for lack of merit.
>
> Other reliefs just and equitable under the circumstances are likewise prayed for.[2]

On 23 February 2021, the Commission issued an Order sustaining the CDO issued against Familyhan:

> **WHEREFORE,** premises considered, the Cease and Desist Order issued against Familyhan Credit Corporation and its responsible officers and members of the board, MTR, VBV JPV, AA, and MDA to cease and desist from the processing of personal data on Familyhan's database is hereby sustained until modified or lifted by the Commission upon showing that the factual or legal basis for which it was issued no longer exists.
>
> xxx[3]

On 21 June 2021, Familyhan filed a Motion to Lift the Cease and Desist Order.[4] The grounds alleged by Familyhan to lift the CDO are:

1. It stopped processing personal data on its database and ordered all its Loan Agents to discontinue processing personal data on its database. As further security, the access to its system was immediately cut off by the IT Department;[5]

2. In accordance with Section 12 of NPC Circular No. 20-02, the CDO to which it filed a Comment on 25 January 2021 is deemed automatically lifted;[6] and

---

[2] Comment (to the Order of the NPC dated 15 October 2020) dated 25 January 2021.
[3] Order dated 23 February 2021.
[4] Motion to Lift Cease and Desist Order dated 21 June 2021.
[5] Ibid. at par. 2.
[6] Ibid at par. 5-6.

3. The basis for which the CDO was issued no longer exists as it had already implemented measures to address the incident.[7]

Discussion

Section 4 of NPC Circular No. 20-02 (Rules on the Issuance of Cease and Desist Orders) provides the grounds for the issuance of a CDO:

> Section 4. Grounds for the Issuance of Cease and Desist Order. – No CDO shall be issued unless it is established by substantial evidence that all of the following concur:
>
> A. the Adverse Party is doing, threatening or is about to do, is procuring to be done, some act or practice in violation of the DPA, its IRR, or other related issuances;
>
> B. such act or practice is detrimental to national security or public interest, or the CDO is necessary to preserve and protect the rights of a data subject; and
>
> C. the commission or continuance of such act or practice, unless restrained, will cause grave and irreparable injury to a data subject.[8]

A CDO is issued by the Commission against acts which are potentially harmful and in violation of the Data Privacy Act of 2012 to mitigate the harm that it produced. The lifting of a CDO is dependent on whether such harmful acts had been addressed and remedied to avoid further harm to data subjects. Section 15 of NPC Circular No. 20-02 provides:

> Section 15. Motion to Lift Extended CDO. - At any time during the effectivity of the extended CDO, the Adverse Party may file a motion to lift said order on the ground that **the factual or legal basis for which it was issued no longer exists**, furnishing a copy thereof to the applicant. The motion shall contain or specify the material facts establishing the ground/s relied upon, the relevant documentary, testimonial and object evidence supporting the motion, and the proof of service of the copy of the motion to the applicant.[9]

---

[7] Ibid. at par. 7
[8] NPC Circular No. 20-02, Rules on the Issuance of Cease and Desist Orders, Section 4.
[9] Section 15, NPC Circular No. 20-02.

To properly determine whether the issues sought to be prevented by the CDO have been satisfactorily addressed, the Commission resolves to order the Applicant of the CDO, the Complaints and Investigation Division (CID) of the National Privacy Commission, to submit its Comment or Opposition to Familyhan's Motion, pursuant to Section 16 of NPC Circular No. 20-02 which provides:

> Section 16. Comment or Opposition to the Motion. - The applicant may file a comment/opposition to the motion to lift within ten (10) days from receipt thereof and furnishing a copy thereof to the Adverse Party. It shall contain the relevant documentary, testimonial and object evidence supporting its position, and shall specify the material dates relevant to the same and proof of service of the copy of the Comment/Opposition to the Adverse Party.[10]

WHEREFORE, premises considered, the Commission hereby **ORDERS** the Complaints and Investigation Division to **COMMENT** on the Motion within ten (10) days from receipt of this Order.

SO ORDERED.

City of Pasay, Philippines.
24 June 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

[10] Section 16, NPC Circular No. 20-02.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JRO
Counsel
Familyhan Credit Corporation

AVM
Collaborating Counsel
Familyhan Credit Corporation

SMA
President
Familyhan Credit Corporation

RA
Vice President
Familyhan Credit Corporation

MRO
Treasurer
Familyhan Credit Corporation

MJR
Corporate Secretary
Familyhan Credit Corporation

PPM
Director
Familyhan Credit Corporation

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FAMILYHAN CREDIT CORPORATION

Initiated as an Independent NPC Investigation into the Possible Data Privacy Violations Committed by Familyhan Credit Corporation

x----------x

NPC SS 20-001
For: Violation of the Data Privacy Act (DPA) of 2012

ORDER

This refers to the Compliance submitted by Familyhan Credit Corporation (Familyhan) in response to the Order dated 08 April 2021 and the Resolution dated 01 June 2021.

On 08 April 2021, the Commission conducted a Clarificatory Hearing for this case and issued an Order requiring Familyhan to submit the following documents:

1. The outsourcing agreement or any similar document between Familyhan Credit Corporation and its database service provider, indicating the terms of agreement between Familyhan Credit Corporation relating to the processing of its client-borrowers' personal data in a database;

2. Documentation on the policies or the approvals made for the Loan Disbursement Officers' access to the database prior to the personal data breach;

3. Documentation on the database's restricted download or copy paste functions;

4. The system activity logs cited by Familyhan Credit Corporation in relation to its investigation of unauthorized activity on its database as well as other documents in its possession pertinent to such investigation;

5. Documentation on the new policies and security measures implemented after the personal data breach, including but not

limited to the policy granting only the General Manager access to the subject database;

6. Documentation on the communications made by Familyhan Credit Corporation to its database service provider regarding its security measures following the personal data breach;

7. A status update on the Estafa case against AYA, KHT and CJ;

8. A copy of the 2020 Audited Financial Statements; and

9. A copy of the work permit of former employees AYA, KHT and CJ.

On 26 May 2021, Familyhan filed a Motion to Clarify Order relating to the deadline for the submission of its compliance and prayed that the Commission allow it to submit the documents within fifteen (15) days from its receipt of the Order. On 01 June 2021, the Commission issued a Resolution granting Familyhan a non-extendible period of fifteen
(15) day from receipt of the Resolution within which to comply with the aforementioned Order.

On 04 June 2021, Familyhan received a copy of the Resolution.[1] On 10 June 2021, Familyhan submitted its Compliance with the following attachments:

1. Annex A: a copy of the "Data Processing Agreement" between Familyhan and MBTech Solutions dated 1 September 2019;

2. Annex B: a copy of two (2) Memoranda: (1) Memorandum dated 2 July 2020 on the restriction of access to the system database.; and (2) Memorandum dated 2 February 2020 on absenteeism, AWOL, Cash Handling, Use of Phone and Unauthorized Data Transfer.

3. Annex C: a copy of the access logs of the FCC system from 3 March 2020 to 27 July 2020.

4. Annex D: a copy of a Memorandum dated 19 January 2021 addressed to all loan officers stating that effective 20 January 2021, only the General Manager has login access on the FCC

[1] Compliance (to Resolution dated 1 June 2021) dated 10 June 2021.

System and that there was a system update where a client can only open an email link once.

5. Annex E: screenshots of conversations between Familyhan's General Manager and MBTech discussing how the URL access works and how MBTech's "EIN."

6. Annex F: a copy of the Subpoena to Complainant and Witnesses dated 29 January 2021 as part of the update on the Estafa case against AYA, KHT and CJ.

7. Annex G: a copy of the Annual Income Tax Return of Familyhan, Statement of Financial Position, and Statement of Comprehensive Income

8. Annex H: a copy of the certificates of employment of AYA, KHT and CJ.

On 25 June 2021, Familyhan submitted its Financial Statement as an additional document for its Compliance.

Pursuant to Section 1, Rule VIII of NPC Circular No. 21-01,[2] the Commission conducted a clarificatory hearing for this case and the parties already complied with the order to submit additional documents. The Commission notes that Familyhan filed a Motion to Lift CDO dated 21 June 2021. However, as the Cease and Desist Order

[2] Section 1. Action on the recommendations of the Investigating Officer. – The Commission shall review the evidence presented, including the Fact-Finding Report and supporting documents. On the basis of the said review, the Commission may: (1) promulgate a Decision; (2) issue interlocutory orders on matters affecting personal data; or (3) order the conduct of a clarificatory hearing or the submission of additional documents, if in its discretion, additional information is needed to make a Decision. No motion for clarificatory hearing shall be entertained. In case the Commission finds that a clarificatory hearing is necessary, the following shall be observed:

a. The parties shall be notified of the scheduled clarificatory hearing at least five (5) calendar days before such schedule;
b. The Commission may require additional information and/or compel attendance of any person involved in the complaint;
c. The parties shall not directly question the individuals called to testify but may submit their questions to the Commission for their consideration;
d. The parties may be required to submit their respective memoranda containing their arguments on the facts and issues for resolution.

is considered a separate proceeding pursuant to Section 20 of NPC Circular No. 20-02,[3] this case is now submitted for resolution.

WHEREFORE, all premises considered, the Commission hereby **NOTES** the aforementioned submissions of Familyhan Credit Corporation.

This case is now submitted for resolution.

SO ORDERED.

City of Pasay, Philippines.
25 June 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

[3] Section 20, Rule IV of NPC Circular No. 20-02:

"Section 20. Separate Proceedings. - The investigation by the CID or the compliance check or breach handling by the CMD shall be treated as a separate and distinct proceeding from the CDO proceeding."

COPY FURNISHED:

JRO
Counsel
Familyhan Credit Corporation

SMA
President
Familyhan Credit Corporation

RA
Vice President
Familyhan Credit Corporation

MRO
Treasurer
Familyhan Credit Corporation

MJR
Corporate Secretary
Familyhan Credit Corporation

PPM
Director
Familyhan Credit Corporation

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FAMILYHAN CREDIT CORPORATION

Initiated as an Independent NPC Investigation into the Possible Data Privacy Violations Committed by Familyhan Credit Corporation

x----------x

NPC SS 20-001
For: Violation of the Data Privacy Act (DPA) of 2012

ORDER

On 8 April 2021, the Commission conducted a Clarificatory Hearing pursuant to its Order dated 23 February 2021. Respondent Familyhan Credit Corporation appeared through their President SA, their General Manager RB, and their legal counsel Atty. JRO. Atty. MVC appeared as counsel for all the individual respondents who were the previous members of the Board of Directors, namely, MTR, VBV, JPV, AA, and MDA. VBV was present.

During the Clarificatory Hearing, Familyhan Credit Corporation was ordered to submit the following documents to the Commission:

1. The outsourcing agreement or any similar document between Familyhan Credit Corporation and its database service provider, indicating the terms of agreement between Familyhan Credit Corporation relating to the processing of its client-borrowers' personal data in a database;

2. Documentation on the policies or the approvals made for the Loan Disbursement Officers' access to the database prior to the personal data breach;

3. Documentation on the database's restricted download or copy- paste functions;

4. The system activity logs[1] cited by Familyhan Credit Corporation in relation to its investigation of unauthorized activity on its database as well as other documents in its possession pertinent to such investigation;

5. Documentation on the new policies and security measures implemented after the personal data breach, including but not limited to the policy granting only the General Manager access to the subject database;

6. Documentation on the communications made by Familyhan Credit Corporation to its database service provider regarding its security measures following the personal data breach;

7. A status update on the Estafa case against AYA, KHT and CJ;

8. A copy of the 2020 Audited Financial Statements; and

9. A copy of the work permit of former employees AYA, KHT and CJ.

On the same day, the Commission received, through email, the following documents from VBV:

1. A Deed of Assignment dated 27 August 2019 stating thus:

> WHEREAS, the ASSIGNOR is the listed stockholder and owner of ninety hundred (sic) ninety thousand and eight hundred (99.98%) shares of stock ("the Assignor's Shares") of Familyhan Family Corporation (the "Corporation"), a corporation duly organized and existing under Philippine laws.
>
> WHEREAS, the ASSIGNOR is selling the above-mentioned shares of stocks to the ASSIGNEE and the latter has agreed to acquire the same;
>
> NOW, THEREFORE, for and in consideration of the foregoing premises and the sum of TWO MILLION AND FIVE HUNDRED PESOS (sic) Philippine currency (Php 2, 500, 000), receipt of which is hereby acknowledged, the

[1] Comment to the Order of the NPC dated 15 October 2020, Par. 24.

> ASSIGNOR hereby cedes, transfers and assigns unto the ASSIGNEE, his/her heirs, successors and assigns the Assignor's Shares of the Corporation xxx[2]

2. A Certificate Authorizing Registration dated 19 September 2019 by the Bureau of Internal Revenue (BIR) detailing the transfer of two million eight hundred ninety-nine thousand seven hundred (2,899,700.00) shares of stock from VBV and JPV to SMA

3. A Capital Gains Tax Return by the BIR involving the same transaction; and

4. A Document Stamp Tax Return by the BIR involving the same transaction, and proof of payment thereof.

WHEREFORE, all premises considered, the Commission hereby **ORDERS** Respondent Familyhan Credit Corporation to submit the above documents within **FIFTEEN DAYS (15)** from the date of the Clarificatory Hearing.

Failure to comply with this Order shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

The Commission **NOTES** the submission of the BIR-issued documents and Deed of Assignment from Respondent VBV. Furthermore, it **NOTES** the submission of the General Information Sheet for the Year 2020 in Familyhan Credit Corporation's Reply to the Order of the NPC dated 23 February 2021.[3]

Considering that MTR, VBV, JPV, AA, and MDA have sufficiently established that they were no longer connected to Familyhan Credit Corporation as of the date of the personal data breach which is subject of the Fact-Finding Report, the Commission **GRANTS** the prayer of Familyhan Credit Corporation to drop them from the investigation and to include the new members of the Board of Directors in all correspondences between the National Privacy Commission and Familyhan Credit Corporation, namely, SMA, RA, MRO, MJR, and PPM.

---

[2] Deed of Assignment dated 27 August 2019.
[3] General Information Sheet for 2020, submitted to the Securities and Exchange Commission on 27 November 2020.

SO ORDERED.

City of Pasay,
Philippines; 8 April 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

ATTY. JRO
Counsel
Familyhan Credit Corporation

ATTY. MSV
Counsel
Former Respondents MTR,
VBV, JPV, AA, and MDA

SMA
President
Familyhan Credit Corporation

RA
Vice President
Familyhan Credit Corporation

MRO
Treasurer
Familyhan Credit Corporation

MJR
Corporate Secretary
Familyhan Credit Corporation

PPM
Director
Familyhan Credit Corporation

MTR

VBV

JPV

AA

MDA

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: DEPARTMENT OF FOREIGN AFFAIRS - PASSPORT BREACH

NPC SS 19-001

INITIATED AS A *SUA SPONTE* NPC INVESTIGATION INTO THE POSSIBLE DATA PRIVACY VIOLATIONS COMMITTED BY THE DEPARTMENT OF FOREIGN AFFAIRS

x----------x

ORDER

This refers to a *sua sponte* investigation of the possible data breach arising from the alleged mishandling of personal information in relation to the issuance and printing of passports by third parties on behalf of the Department of Foreign Affairs (DFA).

Facts

In January 2019, the media reported the alleged mishandling of personal data in the issuance and printing of passports.[1] Based on the reports, the DFA, through Secretary TLL., announced that individuals renewing their passports were required to bring their birth certificates with them since the FOF DFA's previous third-party passport maker, "took away" passport applicants' data.[2]

Contrary to Secretary TLL's statement, former DFA Secretary PY maintained that there was neither a data breach nor a leak in the DFA.[3] He explained that FOF's contract had ended, and that APO Production Unit, Inc. (APUI) and United Graphic Expression Corporation (UGEC), through a joint venture, now operate and manage the DFA passport system.[4] APUI Chairman, Mr. MD, maintained that passport

[1] Fact-Finding Report, 14 July 2019, at 1, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019).
[2] *Id.*
[3] *Id.*
[4] *Id.*

data are with APUI and that the DFA has access to such data.[5] Secretary TLL, shortly thereafter, retracted his earlier statement that FOF did not run away with the data, but it only made the data inaccessible.[6]

As a result, the Commission, through its Complaints and Investigation Division (CID), conducted a *sua sponte* investigation on the alleged data breach that arose from the alleged mishandling of personal data of passport applicants.

On 14 January 2021, the Commission sent to Secretary TLL formal correspondence informing him that the Commission received reports of alleged mishandling of data being processed by third parties for the issuance and printing of passports on behalf of the DFA.[7] The Commission invited the DFA's Data Protection Officer and other authorized representatives to a Fact-Finding Conference on 16 January 2019.[8]

The DFA, through its Data Protection Officer, requested that the meeting be rescheduled to 25 January 2019.[9] It explained that there was no data breach because DFA and APUI remain in custody and control of the data, and the data has not been shared with or accessed by unauthorized third parties.[10]

On 21 January 2021, the Commission and the DFA held the Fact-Finding Conference where the DFA invited the Commission to conduct an on-site investigation of the APUI Printing Facility at Lima Technology Center in Batangas.[11]

On 30 January 2019, the Commission's on-site team did not proceed with the on-site investigation since it was denied access to the APUI Printing Facility.[12] Representatives from APUI and the DFA required the Commission's on-site team to execute a Non-Disclosure Agreement (NDA) before allowing access to the APUI Printing Facility.[13]

---

[5] *Id.*
[6] *Id.*
[7] Letter *from* Atty. GVS, Director IV, Legal and Enforcement Office, National Privacy Commission, *to* TLL, Secretary of Foreign Affairs, Department of Foreign Affairs (14 January 2019).
[8] *Id.*
[9] Letter *from* MGM, Data Privacy Officer, Department of Foreign Affairs, *to* Atty. GVS, Director IV, Legal and Enforcement Office, National Privacy Commission (14 January 2019).
[10] *Id.*
[11] Notice of On-Site Examination, 24 January 2019, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019).
[12] Memorandum *from* Complaints and Investigation Division, National Privacy Commission (30 January 2019).
[13] *Id.*

On 23 February 2021, the Commission, through the CID, issued an Order requiring the DFA to submit within fifteen (15) days from receipt thereof, an updated report detailing the facts surrounding the incident, a copy of the DFA's contract with the involved third-party provider, and proof or certification that passport applicant's data remains within the DFA's custody and control.[14]

On 18 March 2021, the DFA submitted its compliance with the Order dated 23 February 2021.[15] It submitted an updated report denying the alleged mishandling of the personal data of passport applicants, a certification stating that the server containing passport applicants' data is currently stored in a vault in the APUI Printing Facility, and is within the DFA's custody and control, and the Memorandum of Agreement and Supplemental Agreement between the DFA and the Bangko Sentral ng Pilipinas (BSP) on the implementation of a Machine-Readable Passport and Visa Project.[16] The DFA seeks the termination or dismissal of the *sua sponte* investigation for lack of sufficient basis.

On 17 September 2021, the CID submitted its report after a thorough assessment of the documents that the DFA submitted and the online passport appointment system available on the website, "passport.gov.ph".[17] As a result of its technical investigation, the CID determined that there was no exfiltration of passport applicants' personal data.[18] The CID also monitored the dark web for any signs of the purported data breach and found no traces of the exfiltration of data.[19]

The CID, however, discovered vulnerabilities in the website, "passport.gov.ph".[20] It learned that several pieces of personal information remain publicly available data and may be downloaded using a web browser and a specific search criterion.[21] It also determined that the appointment code is made of a pattern composed of the DFA Branch ID, Year, Month, Date, and Appointment Number.[22] With the use of a random appointment code, the CID was

---

[14] Order, 23 February 2021, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019).
[15] Letter *from* The Undersecretary for Civilian and Security and Consular Affairs *to* National Privacy Commission (18 March 2021).
[16] *Id.*
[17] Supplemental Fact-Finding Report, 17 September 2021, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019).
[18] Technical Report, 07 September 2021, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019), at 4.
[19] *Id.* at 3.
[20] *Id.* at 4.
[21] Supplemental Fact-Finding Report, 17 September 2021, at 3, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019).
[22] *Id.*

able to access other application forms.[23] The CID thus, concluded that the website, "passport.gov.ph" is vulnerable to an Insecure Direct Object References (IDOR) attack.[24]

The CID further assessed the website, "passport.gov.ph" and determined that attackers could bypass security controls, and use the website as a platform for attacks against its users.[25]

Discussion

A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed."[26] In this case, the Commission conducted a *sua sponte* investigation on the DFA passport system, including the website, "passport.gov.ph" to determine the circumstances of the incident and whether it meets the definition of a personal data breach.

The Commission, through the CID, conducted a technical investigation and discovered several vulnerabilities in the website, "passport.gov.ph" which put the security of the DFA passport system into question. Section 20 of the Data Privacy Act of 2012 (DPA) requires the implementation of appropriate measures on systems and computer network to protect the personal information in its custody:

> Section 20. *Security of Personal Information.* – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[27]

It is incumbent upon the personal information controller to implement the following security measures to its system:

> Section. 20. *Security of Personal Information.*

---

[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (k).
[27] *Id.* § 20.

x x x

(c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:

(1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;

x x x

(3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

Section 28 of the Implementing Rules and Regulations of the DPA further provides:

Section 28. *Guidelines for Technical Security Measures*. Where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:

x x x

b. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;

c. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and

> mitigating action against security incidents that can lead to a personal data breach;[28]

The Commission emphasizes the paramount duty of personal information controllers such as the DFA to implement adequate organizational, physical, and technical measures in order to secure the personal information of its data subjects and to prevent possible data breach incidents. For this reason, it is incumbent upon the DFA to address the vulnerabilities that the Commission identified in the DFA passport system.

WHEREFORE, premises considered, the Commission **ORDERS** the Department of Foreign Affairs (DFA) within thirty (30) days from receipt of this Order to:

(1) **ADDRESS** the vulnerabilities on the DFA passport system available on the website, "passport.gov.ph" by performing Vulnerability Assessment Penetration Testing on passport.gov.ph and adding a "noindex" parameter to the HTTP header to prevent any indexing of saved information by any search engine; and

(2) **SUBMIT** proof that it has addressed the vulnerabilities on the DFA passport system.

The Commission shall furnish the DFA with its Technical Report dated 07 September 2021 to guide the DFA in addressing the technical vulnerabilities identified in the DFA passport system.

SO ORDERED.

City of Pasay, Philippines.
11 November 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

[28] National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule I, § 28.

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

DEPARTMENT OF FOREIGN AFFAIRS
2330 Roxas Boulevard, Pasay City

MGM
Data Protection Officer
Department of Foreign Affairs

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: POLYTECHNIC UNIVERSITY OF THE PHILIPPINES **NPC BN 18-222**

x----------x

ORDER

Before the Commission is the Compliance submitted by Polytechnic University of the Philippines (PUP) dated 03 June 2022[1] in fulfillment of the Commission's directive in its Order dated 20 May 2022.[2]

In its letter dated 22 November 2018, the PUP notified the Commission of a breach in its information security.[3] It alleged that on 20 November 2018, it came across a post dated 18 November 2018 on the Facebook page of ZeroSecurity PH claiming that the latter was able to get three thousand eight hundred nine (3,809) emails from #PUPWebsite and #HalfofDatabaseEmails."[4] After seeing the post, the PUP Information and Communication Technology Office (PUP- ICTO) initiated a historical server activity audit and conducted a thorough review of the application and system logs:

1. PUP ICTO immediately checked the SIS database (DB) and cross checked the email addresses listed in the FB post in the database.
2. PUP ICTO checked unexpected query of records thru [sic] thorough review of SIS application logs and the DB system logs.
3. Changed the passwords of the admin user accounts that has [sic] registrar access to the system DB.

---

[1] In re: Polytechnic University of the Philippines, 03 June 2022, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[2] Order (To submit Post-Breach Report), 20 May 2022, at 2, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[3] Letter of Polytechnic University of the Philippines, 22 November 2018, at 1, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[4] *Id.*

4. PUP ICTO discussed the current situation to PUP Executive Committee and informed the latter of the counter-measures done by the ICTO.[5]

It discovered that nine hundred ninety-one (991) email addresses of PUP Student Information System (SIS) users matched with the three thousand eight hundred nine (3,809) emails posted on the ZeroSecurity PH's Facebook page.[6]

After conducting its initial investigation, PUP concluded that:

1. The e-mail records might have come from an old copy of the database which is in possession of someone who had worked before with PUP SIS enhancement.
2. There is no direct access to the online database and the hackers simply compiled it from different sources.[7]

The Commission, through its Complaints and Investigation Division (CID), issued an Order dated 20 May 2022 directing PUP to submit its Post Breach Report within fifteen (15) days from its receipt of the Order.[8]

On 07 June 2022, PUP submitted its Compliance dated 03 June 2022.[9] It expounded that:

> The 991 email addresses that matched with the email addresses published by the 'hackers' are old records. The email addresses belong to student[s] who already graduated or have dropped out from the University." Further investigation conducted by ICTO on system logs reveals that there was no direct access to the system database and that the records were compiled from different source/s and not the Student Information System as claimed by the *'hackers'*. Technically, no hacking was done but

---

[5] *Id.* at 2.
[6] *Id.*
[7] *Id.*
[8] Order (To submit Post-Breach Report), 20 May 2022, at 1-2, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[9] In re: Polytechnic University of the Philippines, 03 June 2022, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).

> mere exploitation of an old list (physical copy) of email addresses of students and some faculty members.[10]

Finally, PUP claimed that its "[a]ffected data subjects were prompted thru [sic] the Student Information System (SIS) to change their SIS passwords before they can access the SIS. They were also advised to take other important measures to ensure that their account is secured" and attached a screenshot of the notification prompt contained in the SIS page.[11]

NPC Circular 16-03 (Personal Data Breach Management) provides that a Personal Information Controller (PIC), upon knowledge of or when there is reasonable belief that a personal data breach requiring notification has occurred, is required to notify the affected data subjects within seventy-two (72) hours:

> Section 18. *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> A. *When should notification be done.* The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.
>
> The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.[12]

Data subject notification is an essential obligation of a PIC.[13] Prompt notification is essential so that affected data subjects may have the

---

[10] *Id.* at 2.
[11] *Id.* at 3-4.
[12] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16- 03], § 18 (A) (15 December 2016).
[13] NPC BN 21-035, 01 June 2021, at 4 (NPC 2021) (unreported).

opportunity to take the necessary precautions or remedial measures to protect themselves and their own data.[14]

Although the personal information involved in the breach were only the data subjects' email addresses and names, there is still a potential risk. As previously held by the Commission:

> Contrary to Respondent's claim, names and e-mail addresses are information that may be used to enable identity fraud. An e- mail address is considered personal information and **an unauthorized acquisition thereof could easily trace the identity of the data subject through the conduct of 'Phishing' attacks to obtain more information about the user which would then be used to access important accounts resulting to identity theft and financial loss.**[15]

PUP claimed in its Compliance that it notified the affected data subjects by posting a prompt in the SIS before its users are able to access the SIS.[16] As evidence, it attached a screenshot of the notification prompt:

> Good day! In line with PUP Security Protocol, your PUP SIS password was reset.
>
> . . .
>
> Remember, all transactions recorded on your account are your accountability.
>
> Thank you for taking the time to read this. We sincerely apologize for the annoyance of having to change your password, but, ultimately, we believe this simple step will result in a more secure PUP SIS experience.[17]

This notice, however, does not conform with the requirements of notification of data subjects:

---

[14] NPC Circ. No. 16- 03, § 18 (A).
[15] NPC BN 20-124, 10 September 2020, at 3 (NPC 2020) (unreported). Emphasis supplied.
[16] In re: Polytechnic University of the Philippines, 03 June 2022, at 3-4, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[17] *Id.* at 4.

> Section 18. *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> C. *Content of Notification*. The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;
> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
> 6. any assistance to be provided to the affected data subjects.
>
> Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.
>
> D. *Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.[18]

The notification prompt of PUP in its SIS is inadequate because it lacks the contents required in an appropriate notification to the affected data subjects.

The notification prompt also does not sufficiently demonstrate that the PUP individually notified its nine hundred ninety-one (991) PUP SIS users. A prompt on the system does not suffice as proper individual notification. The prompt merely states that the password has been reset and suggests "several important steps that [one] can take to ensure that [one's] account is secure," which PUP believes

---

[18] NPC Circ. No. 16- 03, 18 (C) – (D).

"will result in a more secure PUP SIS experience."[19] PUP, as the PIC, should individually notify the affected nine hundred ninety-one (991) SIS users so that they may be informed of the incident and adequately protect themselves from the consequences of the breach.

Further, given PUP's claims that the breach is the result of an "old list (physical copy) of email addresses of students and some faculty members"[20] that is "in possession of someone who had worked before with PUP SIS enhancement,"[21] it should demonstrate that it has created and implemented systems in place to safeguard both physical and online data.

Thus, the Commission orders PUP to individually notify the nine hundred ninety-one (991) PUP SIS users whose email addresses matched with the three thousand eight hundred nine (3,809) emails posted on the ZeroSecurity PH's Facebook page[22] and to submit proof of the security measures it took to prevent the incident from recurring.

WHEREFORE, premises considered, Polytechnic University of the Philippines is hereby **ORDERED** to comply with the following **within fifteen (15) days** from the receipt of this Order:

1. **NOTIFY** its affected data subjects and **SUBMIT** proof that it individually and directly informed its affected data subjects; and

2. **SUBMIT** proof of the security measures it implemented.

SO ORDERED.

City of Pasay, Philippines.
10 November 2022.

---

[19] In re: Polytechnic University of the Philippines, 03 June 2022, at 4, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[20] *Id.* at 2.
[21] Letter of Polytechnic University of the Philippines, 22 November 2018, at 2, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[22] *Id.*

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

MMM
President
Polytechnic University of the Philippines

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: CATHAY PACIFIC AIRWAYS LIMITED

NPC BN NO. 18-198

x----------x

ORDER

AGUIRRE, D.P.C.:

This Order refers to a breach notification report sent by Cathay Pacific Airways Limited (Cathay) involving one hundred two thousand two hundred nine (102,209) data subjects in the Philippines that were affected; roughly thirty-five thousand seven hundred (35,700) passport numbers from the Philippines that were exposed, and around one hundred forty-four (144) credit card numbers from the Philippines that were accessed.[1]

The Facts

Cathay is an airline company based in Hong Kong Special Administrative Region (HK SAR). As such, Cathay collects personal data of its passengers connected to its services.

The systems connected with the collection of data are composed of: (1) a customer loyalty system (System A) which is used for processing and recording membership of members of Asia Miles, Marco Polo Club and Registered Users; (2) a platform used to support various web- based applications (System B) which is a shared back-end database primarily used to support web-based applications; (3) a reporting tool (System C) that queries the customer information systems data warehouse; and (4) an Asia Miles redemption system (System D) which is a transient database allowing Asia Miles members to redeem non-air awards.[2] The personal data collected in the systems include the passenger name, phone number, address, email address, date of birth, nationality, passport number, identification number, frequent flyer

---

[1] "Data Breach Notification" dated 25 October 2018.

[2] Report on the measures taken to address the breach dated 15 November 2018, p. 4.

membership number, customer service remarks, and historical travel information depending on the system.[3]

Among Cathay's wholly owned subsidiaries are Hong Kong Dragon Airlines Limited (HK Dragon) and Asia Miles Limited (Asia Miles Ltd). Cathay manages and provides IT support services to HK Dragon and in effect, the personal data of HK Dragon's passengers also resides in Cathay's information systems. Asia Miles Ltd manages and operates Asia Miles, a program provided for the frequent flyer members of Cathay. Together with Cathay, its subsidiaries are also headquartered in HK SAR and their information systems reside within the said territory.[4]

On 13 March 2018, Cathay noted a suspicious activity on its network caused by a brute force attack[5] resulting in approximately five hundred (500) staff users being locked out of their accounts and which affected Cathay, HK Dragon and Asia Miles Ltd. [6]

Based on the examination of the source of the traffic, it was found that a server outside the Philippines was at issue. [7] Upon becoming aware that any of its database was potentially affected, Cathay commenced investigations into the nature of the personal data contained in each database and the purpose of use for that data.[8]

Cathay reported that it engaged a leading cybersecurity firm (CS FIRM) to assist in the investigation, conduct dark web searches for stolen personal data, advise on defensive and containment measures to take, and conduct of a full sweep of its entire environment.[9] Cathay stated that it also worked with other third parties including hosting and managed security providers, experienced counsel with data privacy and cybersecurity experts to coordinate and direct these efforts.[10]

---

[3] Report on the measures taken to address the breach dated 15 November 2018.
[4] Data Breach Notification dated 25 October 2018.
[5] A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing a combination correctly. Technical Report dated 30 October 2020.
[6] Technical Report dated 30 October 2020, p. 1.
[7] *Id.* at *Note 2*.
[8] Report on the measures taken to address the breach dated 15 November 2018, p. 11.
[9] *Id.* at *Note 2*.
[10] *Ibid.*

During the investigation on the nature and scope of the attack and what personal data may have been compromised, Cathay was subjected to continued attacker activities, such as continued remote access to the environment, lateral movement through its networks and installation of additional malware and utilities.[11] It was determined that the systems affected by the incident are System A, System B, System C and System D. [12]

The CS FIRM identified two (2) attackers in the environment. The key activities are as follows:

1. On 31 March 2018, an attacker activity was detected in relation to System C where two database extracts may have been created and accessed by the attacker.

2. On 04 April 2018, CS FIRM discovered that archives had been placed on a server that contained the database backup of the System B and may have been a subject of attacker activity.

3. On 04 May 2018, the attacker remotely accessed Cathay's environment and exfiltrated files identified as partial database backups for the System A.

4. On 06 May 2018, an additional malware was uncovered relating to System C.

5. On 08 May 2018, the attacker accessed the administration console of the System D website to view customer redemption and transaction data and export a database backup.[13]

A total of forty-one (41) user accounts were stolen during the attack. This included accounts that have administrator rights[14] on its systems. Cathay stated that the attackers used malware that was unique with previously unknown signatures and therefore was not detected by Cathay's up-to-date anti-virus system. The attackers also took steps to

---

[11] Report on the measures taken to address the breach dated 15 November 2018, p. 11.
[12] *Ibid.*, at p. 4.
[13] *Ibid.*, at p. 12.
[14] Having administrator rights (sometimes shortened to admin rights) means a user has privileges to perform most, if not all, functions within an operating system on a computer. These privileges can include such tasks as installing software and hardware drivers, changing system settings, installing system updates. They can also create user accounts and change their passwords.

avoid detection, deployed counter forensics, and hid the malware they were using.

By mid-October 2018, it was revealed that the passengers' personal
data of Cathay, HK Dragon and Asia Miles Ltd were affected.

Based on Cathay's analysis, a total of one hundred two thousand two hundred nine (102,209) data subjects in the Philippines were affected; roughly thirty-five thousand seven hundred (35,700) passport numbers from the Philippines were exposed and around one hundred forty-four (144) credit card numbers from the Philippines were accessed. These personal data compromised are not cumulative as there may be individuals who fall into all three categories.[15]

On 25 October 2018, Cathay submitted its breach notification report[16] through its counsel, BCCS Office (BCCSLAW) to the National Privacy Commission. Cathay stated that it "has very recently established the types of personal data involved and the number of data subjects in the Philippines whose personal data may have been accessed."[17]

Cathay claimed that no data subject's travel or loyalty profile was accessed in full, no passwords were compromised, and that Cathay found no evidence that any of the personal data has been released.

On 29 October 2018, the Complaints and Investigation Division (CID) ordered Cathay to submit: (1) further information on the measures it had taken to address the breach, which Cathay complied with on 15 November 2018; and (2) an explanation for the failure to timely notify this Commission, which Cathay complied with on 20 November 2018.

In its email dated 15 November 2019, Cathay explained that it had to first fully understand the nature of the personal data affected to provide a meaningful notification to the affected data subjects. It argued that it applied the findings from its data analysis to be able to implement breach notifications in accordance with various legal requirements and prepare a disclosure plan for communications with the affected data subjects, regulators and stakeholders.

---

[15] Data Breach Notification dated 25 October 2018, p. 3.
[16] *Ibid.*
[17] *Id.*, at p. 2.

On 20 November 2018, Cathay sent another response to the Order dated 29 October 2018 issued by this Commission through the CID. With its recognition of the importance of timely notification with the Commission, Cathay claimed that it reacted promptly upon discovering suspicious activity relative to the breach that occurred within its system. It denied delay in notifying regulators as well as the affected data subjects, arguing that it provided notification as soon as practically possible.

In an Order,[18] the CID required Cathay to submit, within fifteen (15) days from receipt, additional documents and/or details regarding the details on how the third-party actor gained entry and the vulnerability of the data processing system that led to it, as well as the security measures in place; and an update on the physical, organizational and technical measures undertaken after the incident. The CID also required Cathay to specify the period and reason for the retention of the personal data including the travel information and expired credit card numbers of the data subjects affected.

On 31 December 2020, Cathay, through its counsel, BCCSLAW, submitted an extension request on the matter, *to wit:*

> x x x While Cathay is exerting best efforts to respond to the Order by the deadline, it anticipates its inability to do so because of difficulties in quickly gathering the required information from the relevant personnel during this holiday season.
>
> Considering that the information and details needed to completely respond to the Order are still being gathered at this time, Cathay respectfully requests to be granted an extension of fifteen (15) days from 2 January 2021, or until 17 January 2021, to respond to the Order.

In its Resolution,[19] the CID granted Cathay's Motion for an Extension of fifteen (15) days from 2 January 2021, or until 17 January 2021, to respond to the said Order.

---

[18] NPC Order dated 16 December 2020.
[19] NPC Resolution dated 05 January 2021.

In its Response, Cathay alleged that based on the tools, tactics and procedures used, the incident was caused by unauthorized access believed to have been conducted by two groups of attackers, *to wit:*

- Group One: The earliest evidence of activity by what is suspected as Group One occurred on 15 October 2014. The last known activity by Group One was on 22 March 2018. It was found that a keylogger malware[20] had been installed on the BRIO server to harvest user account credentials. Using the stolen but valid user account credentials, the attackers accessed Cathay's IT System via its VPN (bypassing the VPN restriction) and the personal data contained therein Group One also moved laterally through the network and placed credential dumping tools in order to extract domain credentials. Group One used the BRIO server to access Cathay's customer information system (**CIS**).

- Group Two: The earliest evidence of activity by what is suspected to be Group Two occurred on 10 August 2017 and the last known activity by Group Two was on 11 May 2018. Group Two exploited a vulnerability of an internet facing server, which enabled them to bypass authentication and gain administrative access. This also enabled Group Two to move laterally within Cathay's environment and install malware and credential harvesting tools. Group Two accessed database backup files of CLS and EBSP, and also accessed iRedeem. In addition, on 28 August 2018, Cathay's IT team detected and prevented an attempted attack which is suspected to have been carried out by Group Two. [21]

Cathay alleged that prior to the incident, the following security measures were taken to ensure personal data was protected against unauthorized or accidental access, processing, erasure, loss, or use, including to prevent its network from attacks:

- Cathay's network was protected from the Internet by 3-leg firewalls;

---

[20] Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored.
[21] CATHAY's Response dated 15 January 2021.

- Cathay's B2C commercial websites were protected by Content Delivery Network with Web Application Firewall (WAF) capabilities;

- Two-Factor Authentication was implemented for privileged IT Support staff;

- Forward proxy and reverse proxy were used to remove malicious outbound and inbound web-based traffic;

- Direct access to customer information systems data warehouse (accessible via the System C server) was granted to authorized users only; and

- A firewall was used to segregate Cathay's network from its service providers' networks. [22]

After the incident, Cathay stated in its Report that it adopted administrative and technical security measures to protect personal data contained in its information systems from any unauthorized or accidental access, processing or use, *to wit:*

1. Information Security Policies and Standards
   Cathay enforces security requirements for staff and all subcontractors, service providers, or agents who have access to Cathay's data.

   xxx

2. Security Incident & Response
   All IT incidents are managed in accordance with appropriate incident response procedures. Cathay has a defined incident response procedure to handle security incidents.

   Cathay monitors and alerts suspicious security events and subscribes to incident response services from renowned security service providers to handle specific situations and get intelligence on potential and actual attacks;

3. Human resource security
   Cathay has clearly defined roles and responsibilities for employees. Screening is carried out before employment

---

[22] CATHAY's Response dated 15 January 2021, p. 5.

with terms and conditions of employment applied appropriately;

Cathay implements phishing simulation exercises to measure the security awareness of employees and a regular security awareness program to train new joiners and existing personnel about their IT security obligations. This program includes training about security practices and a security incident reporting channel;

4. Disaster Recovery
Cathay implements appropriate disaster recovery and business resumption plans. Cathay reviews both business continuity plans and risk assessments regularly. Business continuity and disaster recovery plans are tested and updated regularly to ensure that they are up to date and effective;

5. Compliance
IT security policies and standards are monitored and maintained on a regular basis to ensure compliance.

Cathay has conducted regular internal and external audits and security testing to ensure continuous compliance and effectiveness of security controls and processes over Cathay's data;

Technical measures

1. Operations Security
Cathay has policies on how to classify information assets and security measures according to their classification.

Cathay issues guidelines on configuration hardening to secure the system and get updates on an ongoing basis.

Cathay implements an event monitoring and correlation tool that provides real time analysis and alerting of security issues and has monitoring and auditing facilities for any changes to accounts with privileged access to systems and databases.

Cathay installs and maintains appropriate anti-malware solutions on different channels: servers, workstations, inbound and outbound emails, internal email, and web browsing. All solutions are updated on a timely basis to ensure they can protect Cathay's systems effectively.

Cathay implements regular security testing on its information systems. All new systems are subject to such testing.

Periodic security scans and tests are conducted to assess the security posture of information systems; all new systems are security tested. All major systems are regularly patched to ensure system integrity and prevent attacks.

Encrypted removal storage devices and network storage are provided to protect sensitive information during storage and transmission.

When media are to be disposed of or reused, procedures are implemented to prevent any subsequent retrieval of any sensitive data stored in them.

2. Network Security
Cathay maintains network security controls, including web application firewalls, denial of service protection, host- based & network-based firewalls, intrusion detection and prevention systems, network surveillance system, network segmentation, virtual private networks, secure web proxies, secure wireless networks, secure routing and access control lists to protect against malicious attacks.

Cathay's network is protected from the public network by multiple layers of firewalls and split into difference areas or zones. This zoning allows granular control of the data that can pass between these zones.

xxx

Cathay implements services to handle fraudulent actions by preemptively identifying possible attacks and fraudulent sites and to take down suspicious web sites in due course.

Cathay uses authorized public certificate authority for certificate management lifecycle. Secure algorithms and protocols are used. Cathay has internal certificate authority, with the use of hardware security module for internal certificate management.

Cathay enforces security controls to prevent incoming virus, spam and phishing emails and protect against spoofing emails.

3. Access Control

All Cathay's employees are assigned unique user IDs to authenticate to the system to ensure accountability

Cathay has established a password policy that prohibits sharing of passwords, governs what to do if a password is disclosed, and requires passwords to be changed on a regular basis and default passwords to be altered. All passwords must fulfil the minimum requirements and are stored in hashes.

Unattended workstations on company premises are protected from unauthorized access by a password-protected screensaver.

Access rights to information are granted based on a "need- to-know" basis and in accordance with "least privilege" principles.

Privileged accounts are managed through the Privilege Identity Management System. All access to privileged accounts is logged and justified. Automatic reset of password of privilege accounts is enforced.

Identity Management System is used to provide and remove staff accounts from the system automatically to ensure prompt access removal.

Cathay has standard operating procedures to define user roles and their privileges, how access is granted, changed and terminated; addresses appropriate segregation of duties; and defines the logging/monitoring requirements and mechanisms.

Cathay has procedures in place to ensure that all requested changes are authorized and obsolete access rights for the centralized identity store are revoked appropriately

Cathay has a Data Loss Prevention solution for selected users that detects potential data breaches/data exfiltration transmissions and prevents such transmissions by monitoring, detecting and blocking

Physical security

Cathay maintains physical security systems at all company sites where there are information systems that use, process,

> transmit or store Cathay's data. Access to data centers is restricted to authorized personnel only.
>
> Physical access controls have been implemented for all such sites to prohibit unauthorized access. Access to all company sites is monitored 24x7 by security personnel and surveillance cameras. All access tokens or keys must be returned when a staff member is leaving Cathay. Visitor access to such sites is pre-registered and requires approval. Visitors are to be escorted.
>
> Cathay uses uninterrupted power supplies to ensure power availability to data centers and employs environmental devices to ensure a stable and sustainable operating environment for the computing facilities. Cathay has contingency plans defined and tested to ensure that core services are not disrupted by incidents. [23]

Aside from conducting an immediate investigation on the brute force attack resulting in staff users being locked out of their accounts, Cathay stated in its report dated 15 November 2018 that it performed the following actions to address the breach:

1. Upon becoming aware that any particular database was potentially impacted, Cathay commenced investigations into the nature of the personal data contained in each impacted database and the purpose of use for that data;

2. Cathay engaged a leading cybersecurity firm, CS FIRM, to assist in the investigation;

3. CS FIRM was also engaged to conduct searches of the dark web and assess whether the compromised personal data appeared in Chinese underground markets or in English speaking darknet community to identify possible misuse of the personal data accessed which normally involves monetizing such information;

4. Cathay also began working with other third parties including hosting and managed security providers, experienced counsel

---

[23] Administrative and Technical Measures. Attachment 1, CATHAY's Response dated 15 January
2021.

with data privacy and cybersecurity expertise to coordinate and direct these efforts;

5. In relation to the personal data compromised, Cathay applied the process of reconstruction, consolidation, de-duplication and made a detailed analysis of the incident to determine the scope of data accessed, as well as the number of affected data subjects;

6. Cathay offered various service channels to assist the data subjects who are affected by the incident such as a dedicated sub-page of Cathay's website Cathaypacific.com and an enquiry mechanism therein, a dedicated customer call center with a toll-free number for Hong Kong and other countries, including the Philippines, and a dedicated email address at [ ];

7. Cathay notified the regulators of different jurisdictions about the incident including coordination with the Cyber Security and Technology Crime Bureau of the Hong Kong Police on the investigation of the incident; and

8. Cathay sent notifications to all affected data subjects via email, post and general/substitute notice.

In its Report dated 15 November 2018, Cathay reported the following measures undertaken to prevent the incident from recurring: [24]

1. Cathay worked with a forensic investigation firm, as well as other cybersecurity experts; and

2. Cathay narrated its IT security program upgrade that commenced from 2014 under the overall infrastructure upgrade program;

3. Cathay enforced a comprehensive framework of data protection policies, manuals and guidelines, ensuring the fair, lawful and secure processing of personal data;

4. Cathay established a robust data protection organization;

---

[24] Report on the measures taken to address the breach dated 15 November 2018.

5. Cathay implemented a Privacy Impact Assessment (PIA) process;

6. Cathay maintains a Record of Processing Activities (RPA). Cathay has a designated Data Governance team responsible for the management and ongoing maintenance of the RPA;

7. Cathay has established a supplier management process;

8. Cathay regularly reviews and enhances its cybersecurity policies and processes;

9. Cathay has further enhanced its Personal Data Incident response protocols;

10. Cathay has in place training programs for its employees to strengthen their security awareness;

11. Cathay has enhanced its user, vendor, endpoint, network life cycle control framework;

12. To further enhance its data security, Cathay has enhanced its:
    a. Enterprise-wide encryption program;
    b. Enterprise test data management framework;

13. Cathay has reviewed its identity management coverage;

14. Cathay has reviewed its remote access security and established a policy to govern the remote access lifestyle;

15. Cathay has further enhanced its network segmentation;

16. Cathay is implementing unified cloud security platform for managing the security of its overall SaaS infrastructure. Additionally, Cathay has reviewed protection of application API's to prevent security attacks and abuse;

17. Cathay has subscribed to threat intelligence feeds providing up-to-date information on the latest cybersecurity threats;

18. Cathay is extending the coverage of its data loss prevention program;

19. Cathay has completed PCI DSS (Payment Card Industry Data Security Standard) Attestation of Compliance audits; and

20. Remediation measures had been taken to enhance the security and monitoring of its environment, including:[25]
    a. Enhancing visibility;
    b. Rebuilding its systems;
    c. Blocking of threat actors;
    d. Resetting passwords and monitoring changes;
    e. Provision of authentication;
    f. Upgrading user directory; and
    g. Restriction and segmentation of network traffic.

Discussion

Upon careful examination of the reports and documents submitted by Cathay, the Commission finds the absence of any proof of the said notification to the affected data subjects. NPC Circular No. 16-03[26] requires that all actions made by a personal information controller should be property documented. This includes compliance with the notification requirements and assistance to affected data subjects:

> **SECTION 9.** ***Documentation.*** All actions taken by a personal information controller or personal information processor shall be properly documented. Reports should include:
>
> A. Description of the personal data breach, its root cause and circumstances regarding its discovery;
>
> B. Actions and decisions of the incident response team;
>
> C. Outcome of the breach management, and difficulties encountered; and

---

[25] Administrative and Technical Measures. Attachment 1, CATHAY's Response dated 15 January 2021.
[26] National Privacy Commission, Personal Data Breach Management, Circular No. 16-03 (December 15, 2016).

> D. Compliance with notification requirements and assistance provided to affected data subjects.
>
> A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor.

As to the manner of notification to the affected data subjects, Section 18(A) of NPC Circular No. 16-03 provides that:

> The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. **It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.** It may be supplemented with additional information at a later stage on the basis of further investigation.[27]

Moreover, Section 18(D) of same Circular provides that:

> Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach**: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish means

---

[27] National Privacy Commission, Personal Data Breach Management, Circular No. 16-03 (December 15, 2016). Emphasis supplied.

> through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[28]

The Commission, in its Resolution for NPC BN 20-161, emphasized the importance of ensuring that affected data subjects receive timely notification:

> It is noteworthy that the avowed purpose of the required notification to data subjects of a breach incident is for them to take the necessary precautions or other measures to protect themselves against possible effects of the breach. Moreover, personal information controllers (PICs) are required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. It therefore follows that PICs should guarantee that the notification they sent to data subjects has been received. Otherwise, it defeats the very purpose of notification of data subjects.[29]

Notification of the affected data subjects in cases of personal data breach is an essential obligation in data privacy protection. Section 20(f) of the DPA of 2012[30] states that:

> SEC. 20. *Security of Personal Information.* –
>
> xxx
>
> (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

---

[28] *Id.* Emphasis supplied.

[29] NPC BN 20-161, 17 December 2021.

[30] An Act Protecting Individual Personal Information In Information And Communications Systems In The Government And The Private Sector, Creating For This Purpose A National Privacy Commission, And For Other Purposes [DATA PRIVACY ACT], Republic Act No. 10173 (2012).

The Commission notes that Cathay failed to provide proof of notification to affected data subjects and their receipt thereof and merely stated the following in its Notice of Information Security Breach:[31]

> **I. Measures Taken to Address the Breach**
>
> x x x
>
> **d. Action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification.**
>
> Notification of all affected data subjects, including all affected data subjects in the Philippines, was done via three channels:
>
> (i) **By email**: for the affected data subjects who are Marco Polo Club members, Asia Miles members and Registered Users of Cathay (the "**Member Group**"), where Cathay had an email address in its records.
>
> (ii) **By post**: for the affected data subjects who are part of the Member Group, where Cathay had a postal address (and did not have an email address) in its records and for the affected data subjects located in the US where notification by post is required by law.
>
> **(iii) By general/ substitute notice**: for affected data subjects that do not fall within categories (i) and (ii) above. A general notice was placed on the website https://infosecurity.cathaypacific.com ("**Website**") to notify the affected data subjects in Hong Kong and the rest of the world (excluding the US) who Cathay was unable to contact. For the US, a substitute notice was placed on the Website in accordance with the legal requirements of the various US states to notify the affected data subjects for whom Cathay did not have contact details. The US substitute notice is a US specific notice which consists of elements required by the laws of the various US states.
>
> On 25 October 2018, Cathay commenced sending the personalised email notifications to the Member Group. Cathay completed sending the personalised email

[31] E-mail from PRC & KRI," Re: Notice of Information Security Breach: Cathay Pacific Airways Ltd (Hong Kong) Ref. No. CID BN No. 18-198." dated 15 November 2018.

> notifications to the Member Group on 28 October 2018. 3,252,559 email notifications were sent to the Member Group.
>
> On 2 November 2018, Cathay commenced the dispatch of 74,792 postal mail notifications to the affected data subjects in the Member Group for whom Cathay does not have an email address and as required by US state laws. This batch of physical letters was dispatched on 8 November 2018. A further batch of 265,511 postal mail notifications was dispatched on 12 November 2018 to the affected data subjects with invalid email addresses.
>
> Remaining data subjects have been notified either via the substitute notice (US) or via the general notice on the Website which went live on 24 October 2018, shortly after the Hong Kong Stock Exchange announcement.
>
> Of those notified by email or post, there are approximately 64,035 data subjects believed to be in or from Philippines who Cathay contacted by email and approximately 5,024 data subjects who have postal addresses in the Philippines that Cathay contacted by mail.

The Commission notes that Cathay did not provide proof of its reported notification of sixty-four thousand thirty-five (64, 035) data subjects believed to be from the Philippines by email and five thousand twenty-four (5, 024) data subjects who have postal addresses in the Philippines by mail. There is also no explanation on the discrepancy between these numbers and Cathay's analysis of a total of one hundred two thousand two hundred nine (102,209) affected data subjects in the Philippines; roughly thirty-five thousand seven hundred (35,700) exposed passport numbers from the Philippines and around one hundred forty-four (144) accessed credit card numbers from the Philippines.[32]

WHEREFORE, all premises considered and pursuant to the requirements of Section 18(A) and Section (D) of Circular No. 16-03**,** the Commission **ORDERS** Cathay Pacific Airways Limited to submit evidence of notification to the affected data subjects in or from the Philippines and explain any discrepancy from its abovementioned

---

[32] Data Breach Notification dated 25 October 2018, p. 3

analysis of affected data subjects, exposed passport numbers, and accessed credit card numbers, **within fifteen (15) days** from receipt of this Order.

SO ORDERED.
City of Pasay, Philippines;
18 March 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

ATTY. PRC
Betita, Cabilao, Casuela, Sarmiento Law
Representative of Cathay Pacific Airways Limited

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FYNAMICS LENDING INC. OPERATING PONDOPESO ONLINE LENDING APPLICATION

x----------x

NPC 19-910

For violation of the Data Privacy Act of 2012

ORDER

On 01 October 2020, the Commission conducted a Clarificatory Hearing pursuant to Section 21 of NPC Circular No. 16-04. Respondent Fynamics Lending, Inc. and the individual respondents ML, CW, and BBS were represented by Atty. LAQ and Atty. EAT from the Gonzales & Quismorio Law Offices, while the individual respondents KF, JCG and HAD were represented by Atty. FG from the law firm of Gorosin, Garcia & Associates.

During the Clarificatory Hearing, counsels for Fynamics Lending, Inc. were ordered to submit the following documents to the Commission:

1. The diagram of the organizational structure of Fynamics Lending, Inc. that was supposed to be attached as Annex "A" of the Affidavit of MTA, attached as Annex "B" of the Compliance filed by Fynamics Lending, Inc. on 20 February, 2020;
2. Board Resolutions, if any, discussing the following matters:
    - Authorizing ML, President, on behalf of Fynamics Lending, Inc., to enter into the Master Service Agreement with Asiapac dated 12 October 2018 ; and
    - Appointing the officers of Fynamics Lending, Inc. or authorizing the President to make appointments for the positions of General Manager, General HR Manager, and other officers of Fynamics Lending, Inc.
3. Documentation on the current status of the Master Service Agreement between Fynamics Lending, Inc. and Asiapac;
4. Details surrounding the presentation attached as Annex "E" of the Compliance filed by Fynamics Lending, Inc. on 20 February, 2020, such as: who delivered the presentation, to whom it was delivered, when it was delivered, etc.;

5. Documentation on the number of complaints filed with Fynamics Lending, Inc. in relation to the collection practices of Asiapac;
6. Documentation on the number of Asiapac employees terminated as a result of the complaints filed with Fynamics Lending, Inc.;
7. Details on the utilization, if any, by Fynamics Lending, Inc. of the following provisions in the Master Service Agreement dated 12 October 2018;
    - Article VI, Section 2. *Unprofessional Practices in the Performance of the Service and Breach of the Contract*; *Penalties.*
    - Article VIII, Section 3(d). *Duration of the Agreement and Termination; Termination; Performance evaluation yields an unsatisfactory result.*
8. Documentation of the issue relayed by Fynamics Lending, Inc. regarding alleged scammers who represent themselves to the public as agents of Pondopeso, including any notices issued to the public informing them of this issue; and
9. Information on the background of individual respondents ML, CW, and BBS.

The Commission hereby **ORDERS** Respondent Fynamics Lending, Inc. to submit the above documents within **FIFTEEN DAYS (15)** from the date of the Clarificatory Hearing.

Failure to comply with this Order shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

SO ORDERED.

City of Pasay, Philippines
01 October 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

(On Official Business)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

GONZALES AND QUISMORIO LAW OFFICES
Counsel for Respondents Fynamics Lending, Inc., ML, CW, and BBS

GOROSIN GARCIA & ASSOCIATES
Counsel for Respondents KF, JCG and HAD

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FYNAMICS LENDING INC. OPERATING PONDOPESO ONLINE LENDING APPLICATION

x----------x

NPC 19-910

For violation of the Data Privacy Act of 2012

ORDER

The Commission notes the Notice of Withdrawal filed by the law firm of Romulo Mabanta Buenaventura Sayoc& de los Angeles dated 21 September 2020, which states:

> The law firm of ROMULO MABANTA BUENAVENTURA SAYOC & DE LOS ANGELES respectfully manifests it is withdrawing as counsel for FYNAMICS LENDING INC., ML, CW, AND BBS (collectively, the "Respondents") in the above- captioned case, pursuant to the instructions that it received from the RESPONDENTS.
>
> Undersigned counsel has been informed by the RESPONDENTS that the RESPONDENTS will be henceforth represented by the Gonzales & Quismorio Law Offices at the[x x x]Third Floor, Reylilia Building, Commonwealth Avenue corner Mercury Street, Fairview, Quezon City, Metro Manila and Atty. LAQ at [ ].

The Commission likewise notes the Entry of Appearance with Urgent Motion to Reset Clarificatory Hearing filed by the Gonzales and Quismorio Law Offices dated 22 September 2020, which states:

> 1. The undersigned Law Firm respectfully enters its appearance as counsel for FYNAMICS LENDING, INC. (Pondo Peso). Henceforth, it is requested that all orders and such other legal processes of the Honorable Office be sent to its address indicated below.
>
> xxx

> 4. Considering that the undersigned have just been engaged and is in the process of securing case documents from the Respondent and the previous counsel, the undersigned will need more time to finish securing the aforementioned documents and to study the same. Thus, the undersigned is constrained to move for the resetting of the clarificatory hearing scheduled on 24 September 2020 at 2:00 PM to a later date.

Following such submissions, the clarificatory hearing scheduled on 24 SEPTEMBER 2020 at 2:00 PM is hereby reset to **1 OCTOBER 2020** at **9:30 AM.**

Respondents are directed to **APPEAR** and address inquiries relating to the previous submissions made for this case. To enable the Commission to take the necessary measures for the security of the hearing, Respondents shall **SUBMIT** to the Commission, before the date of the hearing, the names and designations of their representatives or counsel, if any. Such representatives or counsel should be competent to address the inquiries relating to the previous submissions made for this case.

In light of the restrictions brought about by the pandemic due to COVID-19, such clarificatory hearing shall be conducted via remote appearance through [ ] and guided by NPC Advisory No. 2020-02 or "Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission."

Failure to comply with this Order shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

SO ORDERED.

City of Pasay, Philippines
23 September 2020

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND E. LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JWZ
Data Protection Officer of Fynamics Lending, Inc.

ML
President

CW
Director

BBS
Director

GONZALES AND QUISMORIO LAW OFFICES
Counsel for Respondent Fynamics Lending, Inc.

ROMULA MABANTA BUENAVENTURA SAYOC & DE LOS ANGELES
Former Counsel for Fynamics Lending Inc., ML, CW and BBS.

GOROSIN GARCIA & ASSOCIATES
Counsel for Respondents KF, JCG and HAD

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FYNAMICS LENDING INC. OPERATING PONDOPESO ONLINE LENDING APPLICATION	**NPC 19-910** *For violation of the Data Privacy Act of 2012*

x----------x

ORDER

On 15 October 2019, the Commission received an Answer by respondent Fynamics Lending Inc. and some of its directors, ML, CW, and BBS (hereafter "Respondents") containing certain statements that lacked substantiation.

On 8 January 2020, the Commission issued an Order directing Respondents to submit within ten (10) days from receipt of such Order the pertinent documents to support such allegations, such as:

> 1. The official company document containing the functional statements of each director and officer of the corporation; and
>
> 2. The outsourcing agreement with the third-party service provider/processor referred to in their Answer as of 29 August 2019 (the date of the Fact-Finding report) containing the provisions they mentioned in Paragraph 19.[1]

On 20 February 2020, the Commission received a Compliance submission from Respondents that included the following attached documents:

1) A copy of the by-laws of Fynamics (Annex A);
2) An original copy of the Affidavit executed by MTA, General HR Manager at Fynamics (Annex B);
3) A copy of the Master Service Agreement executed by Fynamics and Asiapac (Annex C);
4) Code of Conduct of Asiapac (Annex D);

---

[1] Order dated 8 January 2020.

5) A copy of the presentation of Fynamics on its ongoing efforts for data collection and usage as well as optimization of data collection systems (Annex E); and
6) A copy of the certification issued by Fynamics' external legal counsel, Gonzales & Quismorio Law Offices (Annex F).

Under NPC Circular No. 16-04 or the NPC Rules of Procedure, the Commission may order the conduct of a clarificatory hearing if, in its discretion, additional information is needed to make a Decision.

After due consideration of the evidence presented as of the date of this Order, the Commission finds that a clarificatory hearing is needed for the proper disposition of this case.

WHEREFORE, in the interest of conducting an exhaustive investigation and pursuant to the NPC Rules of Procedure, the Commission hereby resolves to **ORDER** Respondents to appear for a clarificatory hearing on **24 SEPTEMBER 2020** at **2:00 PM**, in relation to its submissions for the case of NPC 19-910**.**

In light of the restrictions brought about by the pandemic due to COVID-19, such clarificatory hearing shall be conducted via remote appearance through [Link] and guided by NPC Advisory No. 2020-02 or "Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission."

To enable the Commission to take the necessary measures for the security of the hearing, the Respondents are **DIRECTED,** before the date of the hearing, to submit the names and designations of its representatives to the clarificatory hearing who should be competent to address inquiries relating to the previous submissions made for this case.

Failure to comply with this Order shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

SO ORDERED.

City of Pasay, Philippines
20 August 2020

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.

RAYMUND E. LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

ROMULA MABANTA
BUENAVENTURA SAYOC &
DE LOS ANGELES
Counsel for Fynamics Lending Inc., ML, CW, and BBS

GOROSIN GARCIA & ASSOCIATES
Counsel for Respondents KF JCG and HAD

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: THE MANUFACTURERS LIFE INSURANCE CO. (PHILS), INC.

CID BN 19-097

x----------x

ORDER

On 23 January 2020, the Commission issued a Resolution containing the following dispositive portion:

> WHEREFORE, all premises considered, the Request for Reconsideration of the Resolution dated 6 September 2019 is hereby DENIED and Manulife is hereby ordered to NOTIFY the data subjects without further delay. Manulife shall SUBMIT an Affidavit of Compliance including details of notification and assistance provided to data subjects, to be submitted within fifteen (15) days from receipt of this Resolution.

On 13 March 2020, they submitted a sworn Affidavit of Compliance from their Chief Operations Officer, stating the following:

> 3. I certify that on 13 March 2020, the Corporation completed the preparation of the Notification Letters and have delivered such letters to the messengerial personnel of the Corporation for mailing to the data subjects affected by CID BN 19-097. A copy of the letter is attached herewith as Annex "A".
>
> 4. I further certify that as stated in the Notification Letter, the Corporation reviewed the data subjects/affected clients' policy transactions to identify any possible instance of fraud or account takeover. This was done as the Client List inadvertently disclosed contains policy information only.
>
> Based on the Corporation's review, there appears to be no suspicious activity that has taken place involving the data subjects/affected clients' policies. Nevertheless, the Corporation continues to regularly monitor the said policies as part of its assistance to the data subjects/affected clients.

> In addition, follow-up inquiries or request for additional information by the data subjects/affected clients are actively responded to by the Corporation. xxx

On 3 April 2020, the Enforcement Division issued its findings on the compliance report. Its assessment stated thus:

> Upon reviewing the Compliance Report and Affidavit of Compliance submitted by Manulife on 13 March 2020, as well as its breach notification report submitted on 13 June 2019, we found that the measures undertaken by Manulife Phils. Comply with R.A. 10173 or the Data Privacy Act, its Implementing Rules and Regulations, and NPC Circular 16-03 on Personal Data Breach Management.
>
> The affidavit of compliance contained a certification as to the notification of affected data subjects as well as assistance provided to them. Moreover, Manulife implemented several measures subsequent to the breach. xxx

WHEREFORE, all premises considered, the Commission resolves that the matter of CID BN 19-097 ("In Re: The Manufacturers Life Insurance Co. (Phils), Inc.") be considered **CLOSED**.

SO ORDERED.

Pasay City, 18 June 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.

JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JFJ
Data Protection Officer
Manulife Philippines

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: BREACH NOTIFICATION REPORT OF SPROUT SOLUTIONS, INC. AFFECTING MARIE FRANCE GROUP OF COMPANIES

CID BN No. 17-46 and 17-47

x----------x

ORDER

On 25 July 2019, the Commission issued a Resolution containing the following dispositive portion:

> WHEREFORE, all premises considered, this Commission finds that Sprout Solutions, Inc. and Marie France Group of Companies are required to notify the data subjects affected by this data breach, furnishing them the required information enumerated in Section 18(c) of the Commission's Circular No. 16-03. Sprout Solutions, Inc. and Marie France Group of Companies are ordered to submit proof of their compliance within thirty (30) days from receipt of this Resolution.

On 5 September 2019, the Commission received a Manifestation of Compliance from Sprout Solutions, Inc. It received a Supplemental Manifestation of Compliance on 6 September 2019.

The Manifestation of Compliance contained the following: (1) Acknowledgment letter to the NPC stating that Sprout Solutions, Inc. and Marie France Group of Companies have received the 25 July 2019 Resolution on 8 August; (2) Template letter-notice patterned after Section 18(c) of the Implementing Rules and Regulations of the Data Privacy Act of 2012; (3) Affidavit executed by Sprout's Data Privacy Officer and Vice President for Operations and Legal, AC, with respect to Notices addressed to KMC Employees; and (4) Affidavit of Service executed by Sprout's Legal Counsel, LVO, with respect to Notices addressed to Marie France employees.

On 18 September 2019, the Commission received a Compliance letter from Marie France Group of Companies. Attached to the said letter were the following: (1) DPO Memorandum 19-001 which was sent to the affected employees of the MF Group; (2) Copies of the duly accomplished acknowledgment receipt of the affected employees who are still employed by the MF group; (3) A copy of the e-mail sent to the employees who failed to sign the acknowledgment receipt because their schedule did not permit them or they were on leave at the time the memorandum was sent; and (4) A copy of the transmittal sheet as proof of mailing of the DPO Memorandum by registered mail.

On 27 September 2019, the Enforcement Division issued its findings on the compliance reports. Its assessment stated thus:

> Upon reviewing the Compliance Reports submitted by Sprout Solutions Phil., Inc. and Marie France Group of Companies on 2 and 6 September 2019, we found that the reports have fully complied with the Order of this Commission.
>
> It was found that the notification sent to all affected data subjects complied with the requirement of Section
> 18 (c) of NPC Circular No. 16-03 on contents of notification. Further, Sprout and Marie France notified the affected data subjects individually through registered mail in compliance with Section 18(d) of the same circular. Affidavits were executed by Sprout's officers attesting to the sending of individual notice by registered mail.

WHEREFORE, all premises considered, the Commission resolves that the matters of NPC BN 17-046 and 17-047 are considered **CLOSED.**

SO ORDERED.

City of Pasay, Philippines
28 October 2019.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.

IVY D. PATDU
Deputy Privacy Commissioner

Sgd.

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

COPY FURNISHED:

EPJ
Corporate Legal Counsel
Marie France Group of Companies

AC
VP, Operations And Legal

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: VULNERABILITY ASSESSMENT OF JOLLIBEEDELIVERY.COM

CID BN No. 17-043

x----------x

ORDER

On 05 November 2019, the Commission issued an Order with the following dispositive portion:

> WHEREFORE, all premises considered, this Commission resolves to:
>
> 1. GRANT the lifting of the suspension on the operations of jollibeedelivery.com;
> 2. ORDER JFC to file a Monthly Progress Report for three (3) months following the launch of the new jollibeedelivery.com website;
> 3. ORDER JFC to conduct regular audit and monitoring to ensure the implementation of security measures and the protection of processing of personal information, without need of furnishing the Commission.

Jollibee Foods Corporation ("JFC") has since submitted its Monthly Progress Reports on 11 December 2019, 13 January 2020 and 14 February 2020. These reports include:

1. Operational updates on the launch of the website, focused on operations training of participating stores to fully onboard everyone to the features of the new platform and to sustain the new process;
2. Security updates showing how Tillster provides continuous security and vulnerability checks and patching as needed to keep the SaaS platform secured and efficient and JFC's conduct of their own Vulnerability Assessment and Penetration Testing (VAPT); and
3. Strategic initiative updates on the possibilities of fully utilizing the SaaS features of Tillster, improving the efficiency of services, and the proactive review and upgrade of the system's IT infrastructure.

On 19 March 2020, the Enforcement Division issued its findings on JFC's compliance, thus:

Upon review of the Monthly Progress Reports submitted, it is evident that JFC is continuously monitoring the development of the website and their plans to fully market the same. It can be assessed that they proactively monitor risks and threats and those that were previously declared to the Commission have been properly addressed and qualified.

Further, JFC continuously updates the system's IT infrastructure to keep up with the technological advances and independently conducts VAPT on demand using their own toll for due diligence.

In view of the foregoing and considering the comprehensive reports previously submitted, the development and improvements made on their delivery website, the efforts exerted to closely work with the NPC to resolve this issue and comply with the DPA, its IRR and issuances, this Division finds that the acts and efforts of JFC to develop their website keeping the principle of Privacy by Design in mind, warrant termination of this case.

WHEREFORE, all premises considered, the Commission resolves that the matter of CID BN 17-043 ("In Re: jollibeedelivery.com") be considered **CLOSED**.

SO ORDERED.

City of Pasay, Philippines 18 June 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

MRG
Data Protection Officer
Jollibee Group of
Companies

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: BREACH NOTIFICATION REPORT OF SUNLIFE OF CANADA

CID BN 17-021

x----------x

ORDER

In a Resolution dated 29 July 2019, the Commission required Sun Life of Canada (Philippines), Inc. ("Sun Life") to comply with the notification of data subjects, stating:

> In this case, despite the measures implemented by Sun Life, it cannot be said that there is no real risk of serious harm to the affected data subjects. Circular No. 16-03 requires, as a general rule, that the affected data subjects be notified. It is only in cases "where the Commission determines that such notification would not be in the public interest or in the interest of affected data subjects" may exemption be allowed. No evidence has been submitted to negate the possibility that other persons may have taken advantage of the same vulnerability to access the data.

On 9 September 2019, the Commission received a letter from Sun Life in response to the Resolution, requesting for reconsideration thereof, stating, among others:

> It is respectfully submitted that there is no vulnerability pertaining to access in this case that may be exploited by others. The inadvertent disclosure resulted from an advisor's erroneous inputting of an email list...While it is granted that such data may be (sic) render the data subject's insurance accounts vulnerable, we respectfully submit that it is not likely that the incident will give rise to real risk of serious harm to the rights of the data subject xxx
>
> xxx
>
> In the event that the Honorable Commission decides to deny our request, we likewise respectfully seek an extension of time of 30 days from receipt of the decision to notify the affected data subjects.
>
> xxx

On 23 September 2019, the Enforcement Division issued its findings regarding the Request for Reconsideration:

> Moreover, Sun Life has not provided any update or information as to the accomplishment of the measures it has previously enumerated to undertake to address the breach. In particular, Sun Life has not provided any update as to the pending confirmation of email deletion from clients who inadvertently received the email; results of the sweep of all group email addresses in Office 365; and information as to its checking with Microsoft for the possible removal of the type ahead feature of Office 365.
>
> xxx
>
> The Commission has found that "despite the measures implemented by Sun Life, it cannot be said that there is no real risk of serious harm to the affected data subjects." It has also been determined that "no evidence has been submitted to negate the possibility that other persons may have taken advantage of the same vulnerability to access the data." Sun Life's only response to this lack of evidence is its own conclusion that there is "no vulnerability pertaining to access in this case that may be exploited by others."

In a Resolution dated 28 October 2019, the Commission denied the Request for Reconsideration by Sun Life, stating thus:

> As assessed by the Enforcement Division, notification of the affected data subjects allows them to take the necessary precautions and to avail themselves of measures that would protect them against possible effects of the breach, including their own monitoring for irregular activities that may arise from compromised data.
>
> As to the claim of Sun Life that there is "no vulnerability pertaining to access in this case that may be exploited by others", it must be noted that the Commission's issuances define "vulnerability" as a "weakness of a data processing system that makes it susceptible to threats and other attacks." It is not confined to technical measures nor does it exclude organizational or physical gaps such as employee error in this case.

On 23 December 2019, Sun Life sent a letter to the National Privacy Commission (NPC) requesting to meet with the Enforcement Division to clarify the requirements of the Resolutions issued, stating thus:

> In that meeting, we intend to clarify the requirements in the July Resolution and to substantiate the grounds stated in our Request for Reconsideration dated 9 September 2019. Considering the foregoing, we respectfully seek the Honorable Commission's kind understanding and indulgence and request for the deferment of the running of the period within which to comply with the requirements of the July Resolution until we have met with the Enforcement Division.

On 29 January 2020, the Enforcement Division met with Sun Life's team including its data protection officer and consumer welfare head. During the said meeting, Sun Life's representatives provided additional proof for their position that there is minimal risk of serious harm to the affected data subjects despite the Commission's Resolution already denying its Request for Reconsideration.

On 3 February 2020, Sun Life sent an email to the Enforcement Division outlining its submissions. In the submitted outline, Sun Life states the following as the main points for its "Grounds for Reconsideration":

1) Timeliness of notifying the data subjects;
2) There is no risk of serious harm to the affected data subjects because of the following:
   a. There is minimal probability of fraud and account takeover due to controls in place of Sun Life;
   b. The nature of data exposed are low risk and are not used in the client validation process across all channels of Sun Life;[1] and
   c. The nature of data exposed is not sufficient to perpetuate fraud.
3) Sun Life continuously educates employees and advisors on Data Privacy through face-to-face trainings, e-learning courses and the annual Data Defender's campaign.

On 07 July 2020, Sun Life, through its Data Protection Officer, filed a letter with the Commission stating thus:

> While waiting for the final decision on Sun Life's request filed on 23 December 2019, Sun Life nonetheless notified all the affected data subjects. Below is the status of compliance with the Resolution:

---

[1] Policy number, issue date, owner name, insured name, basic plan, face amount, mode of payment and premium amount.

Data subjects notified via email or ordinary mail	175
Clients yet to be notified via ordinary mail	108
Will no longer be notified (deceased)	5

We will file an updated report once all data subjects have been successfully notified. Attached herewith as Annex "A" is a sample of the notification letter. xxx

On 28 July 2020, Sun Life sent another letter containing an update on the notification status as of 28 July 2020, thus:

Data subjects successfully notified via email or ordinary mail	237	82%
Data subjects who will no longer be notified (deceased)	5	2%
Data subjects who were not successfully notified	46	16%

In relation to Section 18 of NPC's Circular 16-03 on Personal Data Breach Management, Sun Life established *"all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach."* Unfortunately, despite several delivery attempts and service calls, a total of 46 data subjects cannot be located. Some are no longer in their registered address, while others cannot be contacted. A few cannot be reached because of closed work/business/residential property due to the quarantine. xxx

At the outset, the Commission notes that the recourse taken by Sun Life is not recognized under the NPC Circular on Personal Data Breach Management.[2]

By meeting with the Enforcement Division and submitting additional documents, Sun Life attempted to ask for further reconsideration regarding its notification to affected data subjects even after the Commission already denied their Request for Reconsideration. With this denial, the Resolution dated 29 July 2019 has already become final and executory. The Commission also notes that the additional information

[2] NPC Circular 16-03. Personal Data Breach Management. Dated 15 December 2016.

provided to the Enforcement Division was not included in their 9 September 2019 Request for Reconsideration with the Commission. It is basic that a division cannot overturn a decision or resolution of the administrative agency it belongs to.

In addition, Sunlife's continued refusal to notify the affected data subjects is inconsistent with its statements in its previously filed Request for Reconsideration, thus:

> In the event that the Honorable Commission decides to deny our request, we likewise respectfully seek an extension of time of 30 days from receipt of the decision to notify the affected data subjects.

While the Commission notes its eventual notification of some of the data subjects, this partial compliance comes after a significant amount of time has passed since the Resolution dated 29 July 2019 that ordered the submission of proof of its Compliance within thirty (30) days from the date of receipt thereof and the 28 October 2019 Resolution that denied Request for Reconsideration.

The Commission also notes that Sun Life's 07 July 2020 letter characterizes its 28 December 2019 letter as another request for reconsideration. Aside from the fact that a second request or motion for reconsideration is not allowed under NPC Circular 16-03, Sun Life also mischaracterizes the nature of its 28 December 2019 letter since the body of that letter merely requests for a face to face meeting with the Enforcement Division to clarify its requirements and for the Commission to toll the thirty (30)-day period provided in the Resolution dated 29 July 2019.

This unreasonable delay of Sun Life to comply with the Commission's Resolutions dated 29 July 2019 and 28 October 2019 may already constitute Failure to Notify as provided in NPC Circular 16-03:

> Section 20. Failure to Notify. In case the personal information controller fails to notify the Commission or data subjects, or there is **unreasonable delay** to notification, the Commission shall determine if such failure is justified. xxx[3]

---

[3] *Id.*, at Section 20. Emphasis supplied.

WHEREFORE, the above premises considered, the Commission resolves to **ORDER** Sun Life of Canada (Philippines), Inc. to show cause in writing, within fifteen (15) calendar days from receipt of this Order, why it should not be liable for Failure to Notify under Section 20 of NPC Circular 16-03 and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.

SO ORDERED.

City of Pasay, Philippines
23 July 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

ATC
Chief Compliance Officer

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: BREACH NOTIFICATION REPORT OF ROSEWOOD HOTEL GROUP

CID BN No. 17-005

x----------x

ORDER

On 05 August 2019, the Commission issued a Resolution containing the following dispositive portion:

> WHEREFORE, all premises considered, it is resolved that there are no notable findings requiring further action from this Commission with regard to the breach subject of the notification, and that the Rosewood Hotel Group be ordered to submit a comprehensive report in compliance with Section 9 of Circular No. 16-03 within **thirty (30)** days of receipt of this Resolution.

On 9 September 2019, the Commission received a comprehensive report from the Rosewood Group, containing the additional information required by the Commission, such as:

1. A full chronology of the discovery of the breach, which was from the time they were notified by Sabre of the incident and was informed of the extent of unauthorized access.
2. A full chronology of the actions taken and decisions made upon knowledge of the breach, where they narrated how they coordinated with Sabre in mitigating the damage, notified law enforcement and payment card brands to help mitigate harm to the affected data subjects, and how they identified the affected data subjects and located their contact information, including their establishment of call center to further assist them;
3. A discussion on their compliance with the required notification to data subjects, attaching thereto a copy of the notification letter, guidelines for reporting to the

Federal Trade Commission for US residents, and State-specific instructions for US residents;

4. A presentation of their Data Security Incident Response Plan where revisions were made in light of the lessons learned from this breach incident.

On 4 March 2020, the Enforcement Division issued its findings on the compliance report. Its assessment stated thus:

> The comprehensive report by the Rosewood Group was submitted within the period prescribed and upon reviewing, we found that the measures undertaken and the notification sent comply with R.A. 10173 or the Data Privacy Act, its Implementing Rules and Regulations, and NPC Circular 16-03 on Personal Data Breach Management.
>
> After the breach, the Rosewood Group reviewed their Data Security Incident Response Plan and made revisions to it in light of the lessons learned from the incident, which includes specific steps that the company will take upon receiving the reports from their service providers.

WHEREFORE, all premises considered, the Commission resolves that the matter of NPC BN 17-005 ("In Re: Breach Notification Report of Rosewood Hotel Group") be considered **CLOSED**.

SO ORDERED.

City of Pasay,
Philippines 2 July 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

SGH

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: POPULUS LENDING CORPORATION (PESOPOP) AND ITS RESPONSIBLE OFFICERS

NPC SS 21-008

For: Violation of Data Privacy Act of 2012

INITIATED AS A *SUA SPONTE* NPC INVESTIGATION INTO THE POSSIBLE DATA PRIVACY VIOLATIONS COMMITTED BY POPULUS LENDING CORPORATION (PESOPOP)

x----------x

ORDER

On 11 August 2022, the Commission conducted a Clarificatory Hearing in relation to the alleged "limited launch" of the online lending application, Pesopop, during the effectivity of the Temporary Ban against Populus Lending Corporation, as the operator of Pesopop, and its responsible officers (Respondents).

Attys. MTEP, LQ-A, RSC, SA, Mr. RS, and Ms. JR appeared for the Complainant.

Attys. CEA, RAJP, JJAP, and KMSM appeared for the Respondents.

During the Clarificatory Hearing, the Commission ordered Respondents to submit the following information and documents:

1. Proof in relation to the alleged process of automatically rejecting new loan applications during the "limited launch" that occurred while the Temporary Ban issued by the Commission was in effect;
2. Proof that the version of the Pesopop mobile application launched on a "limited" basis was for the sole purpose of processing payments for existing loan obligations;

3. Android Package Kit (APK) files for versions 1.5.1, 1.5.4, and 1.5.5 of the Pesopop mobile application;
4. Total number of users of the Pesopop mobile application;
5. Total number of users of the Pesopop mobile application with existing loan obligations;
6. Total number of times the Pesopop mobile application was downloaded during the "limited launch";
7. Copy of the Board Resolution or its equivalent indicating the person or persons who approved the "limited launch" of the Pesopop mobile application; and
8. Copy of the Board Resolution or its equivalent indicating who decided to publish the Pesopop mobile application in Google Play Store and other platforms while the Temporary Ban was in effect.

WHEREFORE, premises considered, Populus Lending Corporation, as the operator of the online lending application, Pesopop, and its responsible officers are hereby **ORDERED** to submit the above identified information and documents to the Commission **within a non-extendible period of ten (10) days from receipt of this Order**.

Failure to comply with this Order shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

SO ORDERED.

City of Pasay,
Philippines. 11 August
2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

VASIG ABARQUEZ LUMAUIG ABARQUEZ PUNO LAW OFFICES
Counsel for Respondents

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: POPULUS LENDING CORPORATION (PESOPOP) AND ITS RESPONSIBLE OFFICERS

INITIATED AS A *SUA SPONTE* NPC INVESTIGATION INTO THE POSSIBLE DATA PRIVACY VIOLATIONS COMMITTED BY POPULUS LENDING CORPORATION (PESOPOP)

x----------x

NPC SS 21-008

For: Violation of Data Privacy Act of 2012

ORDER

On 12 August 2021, the Commission issued an Order granting the Application for Temporary Ban on the processing of personal data against Populus Lending Corporation as the operator of the online lending application, Pesopop, and its responsible officers (Pesopop).[1] The dispositive portion of the Order provides:

> **WHEREFORE,** premises considered, this Commission **GRANTS** the Application for Temporary Ban on the processing of personal data filed by the Complaints and Investigation Division of the National Privacy Commission. A **TEMPORARY BAN ON PROCESSING OF PERSONAL DATA** is hereby issued against Respondent Populus Lending Corporation, as the operator of the online lending application, Pesopop.
>
> Further, pursuant to the **ORDER FOR TEMPORARY BAN**, Respondent Populus Lending Corporation shall:
>
> 1. Immediately take down its online lending application, Pesopop, to ensure that it is no longer available for download, installation or use by data subjects; and
>
> 2. Stop personal data processing activities, including those activities outsourced to third parties, where the processing operations involves use of information from the phonebook,

[1] Order, 12 August 2021, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).

> directory, and contact list of data subjects, disclosure of false or unwarranted information, and other unduly intrusive personal data processing methods.
>
> This **TEMPORARY BAN ON THE PROCESSING OF PERSONAL DATA** shall remain in effect until the final resolution of the *sua sponte* investigation against Respondent and its responsible officers.[2]

On 08 November 2021, 25 November 2021, and 28 December 2021, the Enforcement Division (EnD) of the National Privacy Commission sent letters to Pesopop after it determined that the application kept re- appearing on the list of applications in the Google Play Store despite the fact that the Temporary Ban was still in effect.[3] The EnD ordered Pesopop to take down the application[4] and to submit its explanation regarding the matter.[5]

Pesopop stated in its Replies that the application was already removed from the Google Play Store and reiterated its arguments that the imposition of the Temporary Ban was void *ab initio*.[6] Hence, the Commission ordered Pesopop to explain why it should not be subjected to contempt proceedings for failure to comply with the Temporary Ban.[7]

On 11 July 2022, Pesopop submitted its Reply to the Show Cause Order dated 31 March 2022.[8] It explained that the application was made available for existing users, especially those who have pending obligations:

> 33. Respondents, upon legal advice by previous counsel, allowed a *limited* launch of the PESOPOP application for *existing* users

---

[2] *Id.* at 10-11.
[3] *See* Letter re: Compliance with Order dated 12 August 2021, 08 November 2021, in In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021); Letter re: Compliance with Order dated 12 August 2021, 25 November 2021, in In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021); Letter re: Compliance with Order dated 12 August 2021, 28 December 2021, in In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[4] *Id.*
[5] *See* Letter re: Compliance with Order dated 12 August 2021, 08 November 2021, in In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021); Letter re: Compliance with Order dated 12 August 2021, 28 December 2021, in In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[6] *See* Re – Reply to letter dated 08 November 2021, 15 November 2021, in In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021); Re – Compliance to letter dated 28 December 2021, in In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[7] Order, 31 March 2022, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[8] Reply to the Show Cause Order dated 31 March 2022, 11 July 2022, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).

> only for purposes of processing loans of EXISTING users, especially those who had pending obligations, and avoid incurring further losses from pre-existing liabilities. With no malicious intent to violate the Temporary Ban, Respondents only sought to ensure that EXISTING users can access the necessary information in order to fulfill their outstanding obligations. Otherwise put, new users could not have used the PESOPOP application. PESOPOP no longer processed any new information/data from new applicants in compliance with the Temporary Ban.[9]

Considering the foregoing, the Commission deems it best to call for a clarificatory hearing on Pesopop's "limited launch" of the application while the Temporary Ban was in effect. This shall aid the Commission in the final resolution of the *sua sponte* investigation against Pesopop.

WHEREFORE, premises considered, the Complaints and Investigation Division (CID) of the National Privacy Commission and Respondent Populus Lending Corporation, as the operator of the online lending application, Pesopop, and its responsible officers are directed to **APPEAR** and address inquiries relating to the case.

The Commission sets a Clarificatory Hearing on **11 August 2021, Thursday, at 10:00 o'clock in the morning via Microsoft (MS) Teams.**

To enable the Commission to take necessary measures for the proper conduct of the hearing, the **PARTIES** shall **SUBMIT** to the Commission, **at least three (3) days before the date of the hearing**, the names and designations of their respective authorized representatives or counsel, if any.

Such representatives or counsel should be competent to address the inquiries relating to the previous submissions made for this case and should have valid authority to appear on behalf of Respondents.

SO ORDERED.

City of Pasay, Philippines.
28 July 2022.

---

[9] *Id.* at 9.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

VASIG ABARQUEZ LUMAUIG ABARQUEZ PUNO LAW OFFICES
Counsel for Respondents

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: POPULUS LENDING CORPORATION (PESOPOP) AND ITS RESPONSIBLE OFFICERS

NPC SS 21-008

INITIATED AS A *SUA SPONTE* NPC INVESTIGATION INTO THE POSSIBLE DATA PRIVACY VIOLATIONS COMMITTED BY POPULUS LENDING CORPORATION (PESOPOP)

For: Violation of Data Privacy Act of 2012

x----------x

ORDER

On 12 August 2021, the Commission issued an Order granting the Application for Temporary Ban on the processing of personal data against Populus Lending Corporation as the operator of the online lending application, Pesopop, and its responsible officers (Pesopop).[1] The dispositive portion of the Order provides:

> **WHEREFORE,** premises considered, this Commission **GRANTS** the Application for Temporary Ban on the processing of personal data filed by the Complaints and Investigation Division of the National Privacy Commission. A **TEMPORARY BAN ON PROCESSING OF PERSONAL DATA** is hereby issued against Respondent Populus Lending Corporation, as the operator of the online lending application, Pesopop.
>
> Further, pursuant to the **ORDER FOR TEMPORARY BAN**, Respondent Populus Lending Corporation shall:
>
> 1. Immediately take down its online lending application, Pesopop, to ensure that it is no longer available for download, installation or use by data subjects; and
>
> 2. Stop personal data processing activities, including those activities outsourced to third parties, where the processing operations involves use of information from the phonebook,

[1] Order, 12 August 2021, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).

> directory, and contact list of data subjects, disclosure of false or unwarranted information, and other unduly intrusive personal data processing methods.
>
> This **TEMPORARY BAN ON THE PROCESSING OF PERSONAL DATA** shall remain in effect until the final resolution of the *sua sponte* investigation against Respondent and its responsible officers.
>
> . . .
>
> **SO ORDERED.**[2]

On three separate occasions, the Commission, through its Enforcement Division (EnD), identified that the Pesopop application was made available for download, installation, or use in the Google Play Store despite the imposition of the Temporary Ban against it.

First, on 08 November 2021, the EnD sent a letter to inform Pesopop that during a monitoring activity on 29 October 2021, it noticed that the application was made available for download in the Google Play Store.[3] As a consequence, Pesopop was "ordered to immediately ensure that Pesopop is no longer available for download, installation or use by the data subjects in any manner until the Temporary Ban is lifted."[4] Pesopop was also instructed to submit its explanation regarding the matter within ten (10) days from receipt of the letter.[5]

Second, on 25 November 2021, the EnD sent another letter to Pesopop to reiterate its order to take down the application from the Google Play Store.[6]

Third, on 28 December 2021, the EnD sent a similar letter to Pesopop, in which it also instructed Pesopop to explain why the application was made available for download in the Google Play Store despite the Temporary Ban.[7]

---

[2] *Id.* at 10-11.
[3] Letter re: Compliance with Order dated 12 August 2021, 08 November 2021, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[4] *Id.*
[5] *Id.*
[6] Letter re: Compliance with Order dated 12 August 2021, 25 November 2021, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[7] Letter re: Compliance with Order dated 12 August 2021, 28 December 2021, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).

In all three instances, Pesopop failed to sufficiently explain why the application was made available for download in the Google Play Store during the period when the Temporary Ban was still in effect. In its Replies to the letters sent by the EnD, it only informed the Commission that the application was already removed from the Google Play Store.[8] Further, Pesopop merely reiterated the argument it raised in its Notice of Entry of Appearance with Motion for Reconsideration dated 03 September 2021 that the imposition of the Temporary Ban was void *ab initio*.[9]

Despite repeated orders from the Commission to take down the application, the application kept re-appearing on the list of applications available for download in the Google Play Store.[10] The Commission stresses that this is a blatant recurring violation of the Temporary Ban against Pesopop.

Section 8, Rule IX of NPC Circular No. 2021-01 (NPC 2021 Rules of Procedure) provides that "the [T]emporary [B]an on processing of personal data shall remain in effect until the final resolution of the main case, or upon further orders by the Commission or other lawful authority."[11] Considering that the *sua sponte* investigation has not been finally resolved and that there is no order from the Commission or other lawful authority to lift the Temporary Ban, Pesopop must adhere to the Order dated 12 August 2021 that imposed the Temporary Ban on its processing of personal data.

Given the foregoing, the Commission finds it proper to require Pesopop to explain why it should not be held in contempt for violating the Temporary Ban.

WHEREFORE, premises considered, Respondent Populus Lending Corporation, as the operator of the online lending application, Pesopop, is hereby **ORDERED** to **SHOW CAUSE** in writing on why it should not be subject to contempt proceedings for

---

[8] *See* Re – Reply to letter dated 08 November 2021, 15 November 2021, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021); Re – Compliance to letter dated 28 December 2021, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2022).
[9] *See Id.*
[10] *See* Letter re: Compliance with Order dated 12 August 2021, 08 November 2021, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021); Letter re: Compliance with Order dated 12 August 2021, 28 December 2021, *in* In re: Populus Lending Corporation (Pesopop) and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[11] National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], rule IX, § 8 (28 January 2021).

failure to comply with the Order dated 12 August 2021 **within ten (10) days** from the receipt of this Order.

SO ORDERED.

City of Pasay, Philippines.
31 March 2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

ZOSA & QUIJANO LAW OFFICES
Counsel for the Respondent

POPULUS LENDING CORPORATION
Respondent

RCJ
President

FLB

Corporate Secretary and Treasurer

JIS
Director

MM
Director

WL
Director

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: MOVIE AND TELEVISION REVIEW AND CLASSIFICATION BOARD

NPC BN 17-010

x----------x

ORDER

Before the Commission is a request filed by the Movie and Television Review and Classification Board (MTRCB) for additional time to comply with the Commission's directives and for permission to notify its remaining data subjects through alternative means.

MTRCB submitted its Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to Comply with Directives and for Permission for Other Modes of Public Notification dated 14 February 2022 (Compliance and Motion).

To recall, the Commission issued an Order dated 15 April 2021 directing MTRCB to do the following:

> **WHEREFORE,** premises considered, the Commission **ORDERS** the Movie and Television Review and Classification Board to comply with the following:
>
> (1) **NOTIFY** the data subjects affected by the breach incident **within fifteen (15) days** from receipt of this Order;
>
> (2) **SUBMIT** proof of notification that ensures all data subjects were made aware of the breach, **within fifteen (15) days** from receipt of this Order; and
>
> (3) **SUBMIT** the results of the independent security audit **within three (3) months** from receipt of this Order.

SO ORDERED. [1]

MTRCB received the Order on 06 May 2021 and, on 12 May 2021, proceeded to post a Notice of Data Breach on its website (www.mtrcb.gov.ph).[2] Thereafter, MTRCB, in a Letter dated 18 May 2021, informed the Commission that it has notified its data subjects by posting a notice of data breach on its website.[3] It stated that "[it is] aware of the requirements of NPC Circular 16-03 regarding the sending of an individual notification to affected data subjects. However, [it finds] the individual notification an arduous task[.]"[4] The Commission, through a Compliance Letter from its Enforcement Division (EnD) dated 15 October 2021, directed MTRCB to strictly comply with the 15 April 2021 Order by individually notifying the affected parties:

> In your letter, you informed the Commission that you have posted a notice of a data breach on your website on May 12, 2021. However, this could not be considered as a valid form of notification absent prior approval of the NPC.
>
> The Enforcement Division (EnD) reiterates that individual notification is the general rule. The Commission has repeatedly ordered MTRCB to individually notify the data subjects despite its prior request for alternative means of notification. Moreover, we would like to take this opportunity to remind you that it is the Personal Information Controller's (PIC) responsibility to ensure that all data subjects are made aware of the breach.[5]

In a letter dated 02 November 2021, MTRCB informed the Commission that:

> [T]he affected data subjects were already notified via electronic mail from 25-29 October 2021. The total data subjects affected as reported to NPC is five hundred seventy-three (573). This is

---

[1] Order, 15 April 2021, at 7, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).
[2] Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to Comply with Directives and for Permission for other Modes of Public Notification, 14 February 2022, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).
[3] Letter Re: Compliance to National Privacy Commission (NPC) Order No. CID BN 17-010, 18 May 2021, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).
[4] *Id.*
[5] Enforcement Division Letter Re: Compliance to National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 15 October 2021, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).

> composed of two hundred seventy-four (274) individuals (Annex A) and two hundred ninety-nine (299) companies (Annex B). From the 274 affected individuals, the breakdown below shows the number of individuals notified, deceased and those not notified due to the unavailability of contact records from the Information Technology Unit, Human Resources Management Unit and Property and Supply Unit, to wit:
>
> - Emailed: 180 individuals
> - Deceased: 17 individuals
> - No Record: 77 individuals[6]

The EnD, through a Compliance Letter dated 28 January 2022, responded by requesting MTRCB to submit proof that it sent the notifications and proof that the affected data subjects it notified received the breach notification.[7] As for the deceased data subjects, the EnD requested that MTRCB notify the deceased data subject's next of kin if it can be ascertained from MTRCB's company records.[8] After which, the EnD clarified that:

> If MTRCB, even after diligent search, still renders it unable to determine the contact of a deceased data subject's kin, it may seek approval of the Commission to use alternative means of communication in accordance with Section 18(D) of NPC Circular 16-03.
>
> As it appears that 77 individuals were not notified due to the unavailability of contact records, MTRCB may likewise seek approval of the Commission to use alternative means of communication under Section 18(D) of NPC Circular 16-03.
>
> We note that MTRCB has earlier posted a public notification of the breach through its website. However, individual notification of data subjects remains to be the general rule. Hence, prior approval of the Commission is required.[9]

Thus, MTRCB served and individually notified the affected parties through email.[10] By collating email addresses from its records,

---

[6] Compliance to National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 02 November 2021, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017). Emphasis removed.
[7] Compliance with National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 28 January 2022, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).
[8] *Id.* at 2.
[9] *Id.*
[10] Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to Comply with Directives and for Permission for other Modes of Public Notification, 14 February 2022, at 2, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).

MTRCB was able to notify one hundred seventy-seven (177) out of two hundred seventy-four (274) affected individuals.[11] The remaining ninety-seven (97) affected individuals that were not notified are broken down as follows: seventy-eight (78) could not be served because MTRCB has no record of their email addresses and nineteen
(19) were determined to be deceased.[12] As for the successfully served data subjects, one hundred two (102) out of the one hundred seventy- seven (177) successfully served individuals have acknowledged receipt of the notification.[13] Out of the nineteen (19) deceased individuals, MTRCB found the contact information for the next of kin of one (1) data subject who was served the notice and acknowledged the same.[14]

MTRCB claimed that it exerted diligent efforts to locate the data subjects, however, the contact details of the remaining unnotified data subjects are not available in its existing records.[15] Therefore, it "prayed for the allowance of other modes of public notification by allowing the posting of the Notice in its website."[16]

As to the conduct of an independent security audit, MTRCB submitted its Contract for the Conduct of Vulnerability Assessment and Penetration Testing of MIDAS with Next Generation Global Inc.[17] MTRCB explained, however, that "the testing has not been completed due to administrative and budgetary constraints."[18] It prayed for an extension until 31 July 2022, the expected end of contract, to comply with the directive of submitting an independent security audit.[19]

Discussion

The Commission grants MTRCB's request for alternative means of
notification of the remaining unnotified data subjects and denies the

---

[11] *Id.*
[12] *Id.* Annex A.
[13] *Id.* at 2, Annex A-1 to A-102, Annex B within Annex A.
[14] *Id.* Annex B within Annex A
[15] *Id.* at 2.
[16] Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to Comply with Directives and for Permission for other Modes of Public Notification, 14 February 2022, at 2, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).
[17] *Id.* at 2, Annex B.
[18] *Id.* at 2.
[19] *Id.*

request for extension of the submission of an independent security audit.

Data subject notification is an essential obligation of a Personal Information Controller (PIC).[20] PICs are required to "establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach."[21] Section 18 (D) of NPC Circular 16-03 (Personal Data Breach Management) provides that a PIC may seek the Commission's approval to use alternative means of notification in lieu of individual notification in certain cases:

> Section 18. *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> D. *Form*. Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.
>
> The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: ***Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner**: *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[22]

In this case, the Affidavit of JAT, the designated Unit Head of MTRCB's Information Technology Unit in charge of information technology infrastructure and information systems, attested that:

---

[20] NPC BN 21-035, 01 June 2021, at 4 (NPC 2021) (unreported).
[21] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16- 03], § 18 (D) (15 December 2016).
[22] *Id*. Emphasis supplied.

> [F]rom 25 to 29 October 2021, I cause[d] the service of a copy of the Notice of Data Breach, to the affected parties, via electronic mail through the email address [ ], of the 274 individuals affected by the data breach, we were able to serve the Notice of Data Breach to 177 affected individuals, whose email addresses we were able to collate from the records of the MTRCB[.]
>
> . . .
>
> From the 177 individuals [...] who were successfully served with a copy of the Notice of Data Breach, 102 have acknowledged receipt of the Notice. Their email responses to the said Notice, are hereto attached as ANNEX "A-1" to "A- 102[.]"[23]

The Commission considers MTRCB to have sufficiently individually notified the one hundred seventy-seven (177) affected individuals that were notified by email.

Out of one hundred seventy-seven (177) individuals, only one hundred three (103) data subjects acknowledged the individual notification by email.[24] The remaining seventy-four (74) data subjects, however, are still considered to have been sufficiently notified despite their lack of reply. The Circular on Personal Data Breach Management only mandates that the data subject be sufficiently informed and notified.[25] Data subjects cannot be forced to respond to the notification, provided that proper notification is done. The obligation of the PIC to notify affected data subjects is fulfilled regardless of the data subject's response to the notification. What is important is that the email notification was sent and the data subject has access to the information contained in the notification should he or she need it.

As for the remaining ninety-seven (97) data subjects, MTRCB explained that:

> Of the 97 that MTRCB was [unable] to serve the Notice, MTRCB ascertained that 78 of these could not be served because of the

---

[23] Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to Comply with Directives and for Permission for other Modes of Public Notification, 14 February 2022, Annex A, *in* In re: Movie and Television Review and Classification Board, NPC BN No. 17-010 (NPC 2017).

[24] *Id.* Annex A-1 to A-102, Annex B within Annex A.

[25] *See* NPC Circ. No. 16-03, § 18.

> absence of email address records, and 19 of which have been determined to be deceased through the diligent search of records from the records of the Board Secretary, Human Resources Unit, and the Property and Supply Unit of the MTRCB[.][26]

To support this, JAT's Affidavit stated that:

> From the 19 parties who were determined to be deceased, we found contact information for the next of kin of one party, who were similarly sent the Notice of Data Breach to and acknowledged the same. The Acknowledgment of the said next of kin is hereto attached as ANNEX "B"[.][27]

The Commission acknowledges the diligent efforts exerted by MTRCB by attempting to locate the parties and going through its Board Secretary, Human Resources Unit, and Property and Supply Unit records. Given, however, that it does not have the contact information of the remaining affected data subjects and the next of kin of deceased data subjects, the Commission notes that individual notification to the remaining unnotified ninety-seven (97) data subjects is impossible. As such, the Commission grants the MTRCB's request for alternative means of notification for the remaining data subjects who have not been individually notified due to the unavailability of contact information despite its exhaustive efforts to locate them.

As for the security audit, the Commission in a Compliance Letter dated 23 June 2022 informed the MTRCB that:

> As to the conduct of security audit, we find that there is considerable amount of delay in MTRCB's responsive action to prevent the likelihood of another breach from occurring since the breach incident occurred in September 2017.
>
> . . .
>
> In view of the foregoing, you are hereby required to:

---

[26] Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to Comply with Directives and for Permission for other Modes of Public Notification, 14 February 2022, at 2, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).

[27] *Id.* Annex A.

. . .

> (2) **SUBMIT** a written explanation for the cause of delay of conducting the security audit with supporting documentary evidence within ten (10) days from receipt of this letter;
>
> (3) **SUBMIT** a report on the results of the security audit within thirty (30) days from receipt of this letter.[28]

In its Compliance dated 14 February 2022, it stated that it is requesting for an "extension of until 31 July 2022, the expected end of contract, to comply with the directive to comply with the submission of the independent security audit."[29] In its prayer in the same Compliance, however, it requested that it be "granted an additional three (3) months of time to allow NEXT GENERATION to finish the independent security audit."[30] The Commission notes, however, that three (3) months from the date of the pleading is 14 May 2022, which is earlier than the requested date of extension in the body of the pleading.

Following the request made by MTRCB in its prayer, it should have submitted the independent security audit last 14 May 2022. To date, MTRCB has not complied with the directive of the Commission to submit the results of its independent security audit. The Commission emphasizes that PICs should comply with obligations they themselves undertake. It was MTRCB that specified the date for extension, but it itself has not complied with its own deadline. Therefore, regardless of the actual date of extension requested, the request for extension of MTRCB is denied.

WHEREFORE, premises considered, Movie and Television Review and Classification Board is hereby **ORDERED within fifteen (15) days** from the receipt of this Order to comply with the following:

> (1) **NOTIFY** and **SUBMIT** to the Commission proof that it implemented notification through alternative means together with the text of the notification; and

---

[28] Enforcement Division Letter Re: Compliance with National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 23 June 2022, at 2, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).
[29] Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to Comply with Directives and for Permission for other Modes of Public Notification, 14 February 2022, at 2, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).
[30] *Id.* at 3.

(2) **SUBMIT** a report on the results of the independent security audit.

SO ORDERED.

City of Pasay, Philippines.
14 July 2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

ATTY. ALN
Officer-in-Charge
Office of the Executive Director
Movie and Television Review and Classification Board

ATTY. JSP
Data Protection Officer
Movie and Television Review and Classification Board

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: MOVIE AND TELEEVISION REVIEW AND CLASSIFICATION BOARD
x----------x

CID BN NO. 17-010

ORDER

AGUIRRE, D.P.C.:

This Order refers to a letter submitted by the Movie and Television Review and Classification Board (MTRCB) dated 04 February 2021. The letter contains a comprehensive report on its compliance with the previous orders of the Commission.

The Facts

On 20 September 2017, the MTRCB notified the Commission of a cybersecurity incident which led to a breach of the data stored in its system.[1]

The breach was estimated to have occurred between the first week of September 2017 until its discovery on 19 September 2017.[2] Upon initial assessment, two (2) out of the three (3) backup servers were compromised. Consequently, the files in the affected servers (Servers 1 and 2) were maliciously encrypted and renamed with a file extension (.arena).

The personal information affected includes publicity materials, and the backup copies of MTRCB's database for Electronic New Government Accounting Management System (e-NGAS). This database contains the following information: (1) MTRCB Members of the Board, Employee, and Organic Staff Names and Tax Identification Numbers (TIN); (2) Contracted Vendors/Suppliers Business Name

---

[1] Records at pp. 1-3.
[2] *Ibid.*

and TIN; (3) Monetary Remittances through MTRCB Payroll and Vendor Payments; and (4) List of MTRCB's Property Plant Equipment.[3]

According to MTRCB's data breach notification, the personal data of five hundred seventy-three (573) data subjects were affected. These include one hundred ninety-three (193) current and former employees and board members, as well as three hundred eighty (380) active and former suppliers, contractual employees, and consultants of MTRCB.[4]

Shortly after its breach notification report, on 21 September 2017, MTRCB sent a letter[5] to the Commission requesting for the postponement of the notification of the data subjects for twenty (20) days. MTRCB also reported that since the discovery of the breach, it was in close contact with the proper government agencies such as the Department of Information and Communications Technology ("DICT") and the Philippine National Police ("PNP") for the expeditious resolution of the case.[6]

On 5 October 2017, the Commission sent an e-mail[7] to MTRCB in response to the latter's data breach incident report. The Commission required MTRCB to submit a full breach report following the requirements set forth in NPC Circular No. 16-03 on Data Breach Management within five (5) days from receipt of the e-mail.[8]

On 10 October 2017, MTRCB submitted its full breach report along with a request for exemption from notification of data subjects.[9] In its full breach report, MTRCB outlined its proposed remedial measures including an application for Vulnerability and Penetration Test (VAPT) with the DICT, installation of new antivirus software, and reformatting of the servers to prevent the spread of the virus to workstations.[10]

---

[3] *Id.* at p.1.
[4] Id. at p.12.
[5] Re: Request for Postponement of Notification for Data Subjects affected by Data Breach at pp. 4- 5.
[6] *Id* at p. 5.
[7] *Id.* at p. 10.
[8] *Id.*
[9] *Id.*, at pp. 11-14.
[10] *Id.*

As to the actions taken to inform the data subjects, the MTRCB explained that upon close coordination with the DICT and PNP Anti Cyber Crime Group, both agencies were not able to provide information that the encrypted data were passed on or at risk of being uploaded on the internet for exploitation. In support of its request for exemption from notification of the data subjects, MTRCB also argued that ransomware attacks only encrypt data for extortion particularly by demanding a ransom to decrypt the infected files.[11]

On 31 January 2018, the Commission issued a Compliance Order[12] against MTRCB directing the latter to do the following:

1. Appoint or designate a Data Protection Officer within one (1) month from the receipt of the Order;

2. Create a Privacy Management Program based on risk assessment within three (3) months from receipt of Order;

3. Implement appropriate organizational, physical, and technical security measures in accordance with the provisions of NPC Circular No. 16-03, on Security of Personal Data in Government Agencies and submit a progress report within six (6) months from receipt;

4. To cause the conduct of an independent security audit of all its personal data processing systems including those hosted by service providers, within six (6) months from receipt of Order, and;

5. Notify the data subjects affected in accordance with NPC Circular No. 16-03 within fifteen (15) days from receipt of the Order.[13]

On 08 March 2018, MTRCB, in a letter, acknowledged the receipt of the Compliance Order. However, it reiterated its request to be exempted from notifying the data subjects affected by the breach.[14] MTRCB

---

[11] *Id.* at p. 14.
[12] *Id.* Compliance Order at pp. 24-26.
[13] *Id.* at p.25.
[14] Letter from MTRCB dated 7 March 2018.

averred that the encoded employee numbers of the data subjects contained in the compromised backup e-NGAS database were only dummy data and thus could not be used for malicious purposes. According to MTRCB, the data was only made up using either a TIN number or a combination of made-up number and TIN number.[15]

In case the exemption was not feasible, MTRCB requested for a sixty (60)-day extension period from the date of the letter for it to determine the specific number of data subjects affected. It also requested alternative means of notification of the data subjects.[16]

On 06 January 2021, the Legal and Enforcement Office ("LEO") sent a Compliance Letter[17] to MTRCB instructing it to submit a comprehensive report of its implementation and compliance with the order of the Commission dated 31 January 2018.

In a letter dated 04 February 2021, received by LEO on 17 February 2021, MTRCB submitted its comprehensive report[18] on its compliance with the previous orders of the Commission. MTRCB reported that it has already created a Privacy Management Program and has implemented its security measures in accordance with NPC Circular No. 16-01 or the Security of Personal Data in Government Agencies. As to the conduct of an independent security audit, MTRCB said that it was already processing the necessary documentary requirements for engaging the services of a security audit provider. As to the notification of data subjects, MTRCB reiterated its request for exemption and alternate means of notification to the affected data subjects, which was not responded to by the Commission.[19]

Discussion

The Commission notes the following actions of the MTRCB to comply with the 31 January 2018 Compliance Order:

---

[15] *Id.*
[16] *Id.*
[17] Compliance Letter Re: Compliance Order dated 31 January 2018.
[18] Comprehensive report of MTRCB's implementation of and compliance with the NPC Order dated 31 January 2018.
[19] *Id.*

(1) Appointment of a Data Protection Officer;[20]

(2) Creation of a Privacy Management Program (PMP) based on risk assessment;[21]

(3) Implementation of appropriate organizational, physical and technical security measures in accordance with the provisions of NPC Circular No. 16-01 on Security of Personal Data in Government Agencies and submission of a progress report within six (6) months from receipt of the order.[22]

The Commission notes the MTRCB's submission of its PMP, Privacy Impact Assessment, updates, and reports. However, MTRCB has yet to comply with the following directives: (1) Conduct of an independent security audit of all its personal data processing systems including those hosted by service providers; and (2) Notification of data subjects.

In a letter dated 07 March 2018, MTRCB requested to be exempted from notifying the data subjects. If the extension is not feasible, it requested for a sixty (60)-day extension period.

At the outset, it should be emphasized that notification of data subjects of a personal data breach is the general rule and exemptions are allowed only under specific circumstances. Section 18(A) of NPC Circular No. 16-03, provides the rule:

> **SECTION 18. Notification of Data Subjects.** The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> A. *When should notification be done*. The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period **if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects**. It shall be undertaken in a manner that would allow data subjects to

---

[20] Email from the Compliance and Monitoring Division dated 3 February 2021.
[21] Annex A, Letter dated 4 February 2021.
[22] Letter dated 4 February 2021.

> take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation. **(Emphasis supplied)** [23]

The purpose of the requirement to notify data subjects of a breach incident is for them to take the necessary precautions or such other measures to protect themselves against possible effects of the breach. Personal information controllers (PICs) are likewise required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach.[24]

Section 18(B) of NPC Circular No. 16-03 provides for the criteria of exemption, thus:

> **If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement**, or the postponement of the notification**. A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.** The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.[25]

As of date, MTRCB has yet to submit proof of notification of the affected data subjects. If indeed MTRCB deemed it necessary to notify the data subjects and asked the Commission in good faith for an extension period of sixty (60) days, then it should have proceeded to notify the data subjects after the lapse of the sixty (60)-day period.

As indicated in the breach notification report, the personal data of at least five hundred seventy-three (573) individuals were compromised. The affected data involves sensitive personal information or any other information that may be used to enable identity fraud. Given this

---

[23] NPC Circular 16-03, Personal Data Breach Management. Dated 15 December 2016. Emphasis supplied.
[24] *Ibid.*
[25] Emphasis supplied.

situation, the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects.

Even after multiple requests of postponement of or exemption from notification of data subjects, the Commission, on 31 January 2018, issued a Compliance Order to MTRCB which included, among others, an order to proceed with the notification of data subjects. Such Compliance Order is proof that the Commission has not found any ground to dispense with the notification requirement and MTRCB failed to prove that it was indeed entitled to exemption.

As regards the independent security audit, MTRCB stated in its report that it is still preparing to conduct it on all its personal data processing systems including those hosted by service providers. The Commission deems it reasonable to require compliance with this within three (3) months from receipt of this Resolution.

WHEREFORE, premises considered, the Commission **ORDERS** the Movie and Television Review and Classification Board to comply with the following:

(1) **NOTIFY** the data subjects affected by the breach incident **within fifteen (15) days** from receipt of this Order;

(2) **SUBMIT** proof of notification that ensures all data subjects were made aware of the breach, **within fifteen (15) days** from receipt of this Order; and

(3) **SUBMIT** the results of the independent security audit **within three (3) months** from receipt of this Order.

SO ORDERED.

City of Pasay, Philippines.
15 April 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

MLN
Officer-in-Charge
Office of the Executive Director
Movie and Television Review and Classification Board

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FYNAMICS LENDING INC. OPERATING PONDOPESO ONLINE LENDING APPLICATION

NPC No. 19-910
For violation of the Data Privacy Act of 2012

x----------x

ORDER

On 15 October 2019, the Commission received an Answer by respondent Fynamics Lending Inc. and some of its directors, ML, CW, and BBS (hereafter "Respondents").

In their Answer, they argue that:

1. It is not true that Fynamics and its directors/officers have "knowledge of the practices of its agents or other people clothed with the authority to collect outstanding loans" because, in fact, the collection agents who committed debt-shaming practices did so without the knowledge of Fynamics and its directors/officers. It then follows that without any knowledge of Fynamics and its officers, the respondents could not have consented to the acts of the collection agents, whether expressly or impliedly.[1]

2. Fynamics recognizes that even if the collection of loan repayments was outsourced to a third-party service provider, it was not amiss in its duty to ensure that the third-party service provider/processor and the collection agents under its employ comply with the DPA and the basic principles of personal data protection. In particular, collection agents are supposed to use only a provided computer software to contact the user/borrower or third parties. They were not allowed to use their personal phones to contact the user or other parties, which is what these collection agents did.[2]

The Commission notes that Respondents failed to provide any evidence in their Answer to support these arguments.

---

[1] Answer dated 15 October 2019, par. 18.
[2] Answer dated 15 October 2019, par. 19.

WHEREFORE, in the interest of conducting an exhaustive investigation, and in the exercise of its mandate to compel any entity, government agency or instrumentality to abide by its orders or to take action on a matter affecting privacy,[3] the Commission hereby orders Fynamics Lending Inc. and the individual respondents ML, CW, and BBS, to **SUBMIT** within **TEN (10) days** from receipt of this Order the pertinent documents to support the abovementioned allegations, such as:

1. The official company document containing the functional statements of each director and officer of the corporation; and
2. The outsourcing agreement with the third-party service provider/processor referred to in their Answer as of 29 August 2019 (the date of the Fact-Finding report) containing the provisions they mentioned in Paragraph 19.

Failure to comply with this Order shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

SO ORDERED.

City of Pasay,
Philippines 8 January
2020

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.

JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Sgd.

RAYMUND E. LIBORO
Privacy Commissioner

[3] R.A. 10173, Section 7 (d).

COPY FURNISHED:

ROMULA MABANTA BUENAVENTURA SAYOC & DE LOS ANGELES
Counsel for Fynamics Lending Inc., ML, CW, and BBS

GOROSIN GARCIA & ASSOCIATES
Counsel for Respondents KF, JCG and HAD

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: VULNERABILITY ASSESSMENT OF JOLLIBEEDELIVERY.COM

CID BN No. 17-043

x----------x

ORDER

On 05 November 2019, the Commission issued an Order with the following dispositive portion:

WHEREFORE, all premises considered, this Commission resolves to:

> 1. GRANT the lifting of the suspension on the operations of jollibeedelivery.com;
> 2. ORDER JFC to file a Monthly Progress Report for three (3) months following the launch of the new jollibeedelivery.com website;
> 3. ORDER JFC to conduct regular audit and monitoring to ensure the implementation of security measures and the protection of processing of personal information, without need of furnishing the Commission.

The reported breach concerns the alleged unauthorized access to the customer database of *jollibeedelivery.com,* the delivery website for Jollibee Foods Corporation (JFC). In the course of its investigation, the Complaints and Investigation Division (CID) identified the incident as a "proof of concept" performed by members of Secuna Software Technologies, a domestic cybersecurity firm. A proof-of-concept in the world of cybersecurity is a type of media, either from text, document, image, or video, that demonstrates how to compromise or exploit a certain system. The test-hack of the website was initiated by a certain marketing PR team representative of JFC, who made representations with Secuna despite them not being officially engaged by the corporation.

The CID confirmed, through a vulnerability assessment, that the website *jollibeedelivery.com* and its subdomains *jfc.com.ph* were vulnerable to web defacement or cross-site scripting, cross-site request forgery, and clickjacking, to name a few. The team noted as well that the subdomains did not have SSL encryption and that there was a vulnerable link where

data scraping was possible. They confirmed that it was possible, with the use of certain tools, to access personal information from accounts without the required username and password.

As a response to these findings, JFC voluntarily took down the delivery website of Jollibee, as well as those of its other brands such as Chowking, Greenwich, Mang Inasal, and Red Ribbon.

Following these events, the Legal and Enforcement Office issued an Order dated 4 May 2018, where JFC was ordered to:

1. SUSPEND forthwith the operations of *jollibeedelivery.com* and all other data processing open to the public through the internet and restrict external access to their networks, for an indefinite time until the site's identified vulnerabilities are addressed, as validated by a duly certified penetration testing methodology;

2. SUBMIT a security plan to be implemented in rehabilitating said system to ensure the integrity and retention of the database and its content within ten (10) calendar days upon receipt of the Order;

3. EMPLOY Privacy by Design in the reengineering of JFC Group data infrastructure;

4. CONDUCT a new Privacy Impact Assessment, considering the vulnerabilities exposed in the Commission's penetration tests and in subsequent penetration tests ordered;

5. FILE a Monthly Progress Report on this matter until the issues raised in this Order are resolved.

Since this Order, JFC submitted two (2) Monthly Progress Reports dated 17 May 2018 and 01 July 2018. After the submission of these reports, an evaluation was made by the CID on the system, and the same vulnerabilities were still exposed. The Commission also notes that, as of this writing, no formal request has been made by JFC to lift the suspension of the subject website's operation.

WHEREFORE, all premises considered, it is resolved that the operations of *jollibeedelivery.com* and all of JFC's other data processing through the internet remain suspended, and that external access to their networks be restricted, until the identified deficiencies are addressed to the satisfaction of the Commission.

SO ORDERED.

City of Pasay, Philippines
06 August 2019.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
IVY D. PATDU
Deputy Privacy Commissioner

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

COPY FURNISHED:

MRG
Data Protection Officer,

ENFORCEMENT DIVISION
Legal and Enforcement Office

GENERAL RECORDS UNIT

IN RE: BREACH NOTIFICATION REPORT OF AXA PHILIPPINES INVOLVING JUICE AND WRAPPED IDEAS, INC.

CID BN No. 17-041

x----------x

ORDER

On 20 August 2019, the Commission issued a Resolution containing the following dispositive portion:

> WHEREFORE, all premises considered, it is resolved that there are no notable findings requiring further action from this Commission with regard to the data breach subject of the notification, and that AXA Philippines is ordered to submit a comprehensive report stating the above specifications and in compliance with Section 9 of Circular No. 16-03 within thirty (30) days of receipt of Resolution.

On 27 September 2019, AXA submitted its Compliance Report detailing the description of the personal data breach; actions and decisions of the incident response team; post-breach review and the outcome of the breach management and difficulties encountered; and compliance with notification requirements and assistance provided to affected data subjects.

In its Compliance Report, AXA conveyed that on 14 December 2017, after the report to this Commission was made and the partial list was retrieved, they informed the known affected data subjects regarding this breach. They also conveyed that JWI was required to execute a certification that data collected for AXA has been deleted from all their systems, and said certification has been issued. AXA has terminated the services of JWI and removed them from their list of accredited suppliers. AXA likewise conducted a face-to-face data privacy training for the members of its Marketing Team on 20 December 2017. They also reported that its Procurement Team has since implemented an improved vendor risk assessment framework, which includes, among others: (1) an assessment on the third party's information security procedure when entering into

Data Sharing Agreements or Outsourcing Agreements; (2) examination of policy and collection controls, access controls, and physical security; (3) processes to check accuracy and correctness of personal information; (4) existence of contingency controls and retention, disposal, breach procedure; and (5) training and compliance.

For its post-breach review, AXA reported having implemented several improvements such as: (1) an improved and revised Data Breach Management process; (2) regular meeting with the Data Privacy Committee; (3) policy to ensure the training of all employees on Data Privacy on at least an annual basis; (4) inclusion of data privacy in the internal quality assessment process; (5) required approval by the Data Protection Officer for projects and third party engagements in dealing with processing of personal information; and (6) an improved central repository and logging system for their documents.

Upon review of the Compliance Report submitted by AXA Philippines on 27 September 2019, the Commission finds that AXA has timely complied with the Order of this Commission in the Resolution of NPC BN 07-041, dated 20 August 2019, to submit a comprehensive report. The Post-Breach Review Report of AXA is substantially in compliance with Section 9 of Circular No. 16-03.

WHEREFORE, all premises considered, it is resolved that the matter of NPC BN 17-041 is hereby considered **CLOSED.**

SO ORDERED.

City of Pasay, Philippines 24 October 2019.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
IVY D. PATDU

On Official Travel
RAYMUND ENRIQUEZ LIBORO

Deputy Privacy Commissioner

Privacy Commissioner

COPY FURNISHED:

IB
Data Privacy Officer
AXA Philippines

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FINTECHNOLOGY, INC. (FUNDKO) **NPC BN 18-239**

x----------x

ORDER

Before the Commission is the Post-Breach Report dated 13 July 2022 (Post-Breach Report) submitted by Fintechnology, Inc. (FundKo) in compliance with the Order dated 27 May 2022 (Order) of the Commission, through its Complaints and Investigation Division (CID).[1]

FundKo is a web-based peer-to-peer lending platform that connects verified borrowers and lenders.[2] FundKo submitted its Breach Notification dated 22 December 2018, stating that "one of FundKo's registered lenders was able to inspect through his browser the "source code" (or HTML code) of the FundKo marketplace site (https://fundko.com/dashboard), which contained the information of the data subjects."[3] Thus, the incident resulted in the exposure of personal and sensitive personal information to any party who would access the site using the same process.

FundKo alleged that as of 19 December 2018, there has been thirty- four loans on the website which are vulnerable as these contain borrower information that is sensitive.[4]

Moreover, FundKo stated that the information exposed and accessible are composed of the Birthday, City of Residence, Civil

---

[1] Post Breach Report dated 13 July 2022 of Fintechnology, Inc. (FundKo).
[2] Notification of a Privacy Breach Incident dated 22 December 2018 of Fintechnology, Inc. (FundKo).
[3] Notification of a Privacy Breach Incident dated 22 December 2018 of Fintechnology, Inc. (FundKo), at p. 1.
[4] *Id.*

Status, E-mail, Full Name, Gender, Mobile Number, Social Security System (SSS) Number, Tax Identification Number, and Address.[5]

As to the measures to address the breach, FundKo averred that their customer support team immediately forwarded the concern to their Data Protection Officer (DPO) for review.[6] Moreover, FundKo stated that "the incident was validated by the DPO that the lender's concern is verified by viewing multiple loans on the website following the lender's inspection procedure."[7] Thereafter, the DPO raised the issue to the Technical Team led by JC and further documented the incident via e-mail for the upper management's reference.[8]

FundKo declared that one of its developers, DV, informed that they have updated the website and fixed the concern as of 5:49PM of 19 December 2018.[9] FundKo claimed that the website has been in existence since October 2016 and was designed and developed by Asiatic Innovation Phils., Inc.[10]

As per the team lead of the tech team (JC), the issue has been resolved and is an "isolated case."[11] However, FundKo received feedback from JC that the same was not an isolated case as their DPO ran a random check to multiple loans prior to the documentation.[12]

FundKo alleged that they already informed the clients who were possibly affected by the breach and has issued notifications informing them to take steps for them to ensure that any information which might have leaked be kept secured.[13] Further, FundKo stated

---

[5] Notification of a 0Privacy Breach Incident dated 22 December 2018 of Fintechnology, Inc. (FundKo), at p. 1-2.
[6] Notification of a Privacy Breach Incident dated 22 December 2018 of Fintechnology, Inc. (FundKo), at p. 2.
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] Notification of a Privacy Breach Incident dated 22 December 2018 of Fintechnology, Inc. (FundKo), at p. 2.
[11] *Id.*
[12] *Id.*
[13] *Id.*

that the notification was made through email and has also tried to reach the affected clients through their phone numbers.[14]

Lastly, FundKo averred that its management already raised the concern to Guevent Investments Development Corporation Advisory and Assurance Team as well as its legal counsel. [15]

On 12 January 2021, the Commission, through the Complaints and Investigation Division (CID), issued an Order requiring FundKo to submit a Full Report.[16] In the Order, the Commission stated that the report was insufficient to appreciate and determine the severity and nature of the confidentiality breach and whether FundKo notified the affected data subjects.[17] Moreover, FundKo was directed by the Commission to submit proof of personal data breach notification to the affected data subjects.[18]

On 27 May 2022, the CID issued another Order requiring FundKo to submit its Post Breach Report.[19] In the said Order, the Commission directed FundKo to provide a copy of the investigation conducted by its technical team and DPO and reiterating its previous directive to provide proof of data subject notification.[20]

On 10 June 2022, FundKo's counsel filed an Entry of Appearance with Motion for Extension of Time dated 09 June 2022, praying that an additional fifteen (15) days be given to submit their Post Breach Report.[21]

---

[14] Notification of a Privacy Breach Incident dated 22 December 2018 of Fintechnology, Inc. (FundKo), at p. 2.
[15] Notification of a Privacy Breach Incident dated 22 December 2018 of Fintechnology, Inc. (FundKo), at p. 2.
[16] *In re: Fintechnology, Inc. (FundKo), NPC BN 18-239*, Order (To Submit Full Breach) dated 12 January 2021.
[17] *Id.*
[18] *Id.*
[19] *In re: Fintechnology, Inc. (FundKo), NPC BN 18-239*, Order (To Submit Post Breach Report) dated 27 May 2022.
[20] *Id.*
[21] Entry of Appearance with Motion For Extension of Time (to Submit Post-Breach Report) dated 08 June 2022 of Fintechnology, Inc. (FundKo).

On 16 June 2022, the CID issued a Resolution granting the Motion for Extension of Time to submit the Post Breach Report of FundKo.[22]

On 28 June 2022, FundKo's counsel filed an Omnibus Motion for Second Extension of Time to Submit Post Breach Report and To Secure Copies of All Documents in Relation to the Instant Case, praying that another fifteen (15) days be granted and allowing FundKo to secure copies of Breach Notification Report and all other documents relative to the instant case.[23]

On 29 June 2022, the CID issued a Resolution granting FundKo's
Motion for Extension.[24]

On 14 July 2022, FundKo submitted its Post Breach Report dated 13 July 2022.[25] In their Post Breach Report, they reiterated its previous allegation in their Initial Report, and added their measures taken to address the breach.[26] FundKo stated that "among the measures were:
1) updated the platform to prevent unintentional disclosure of the personal and sensitive information of borrowers; 2) notifying all affected data subjects via email and their mobile number; 3) strict monitoring over the updated FundKo platform in order to ensure that all stored information is secured and protected."[27]

Further, they stated that since the data was not stolen, efforts for its recovery were not anymore exerted and instead, they strictly monitored the situation to prevent the happening of any other similar glitch.[28]

---

[22] *In re: Fintechnology, Inc. (FundKo), NPC BN 18-239,* Resolution (Granting the Motion for Extension) dated 16 June 2022.
[23] Omnibus Motion for Second Extension of Time to Submit Post Breach Report and to Secure Copies of All Documents in Relation to the Instant Case dated 28 June 2022 of Fintechnology, Inc. (FundKo).
[24] *In re: Fintechnology, Inc. (FundKo), NPC BN 18-239,* Resolution (Granting the Omnibus Motion for Extension with Request to Secure Case Files) dated 29 June 2022.
[25] Post Breach Report dated 13 July 2022 of Fintechnology, Inc. (FundKo).
[26] *Id.*
[27] *Id.*, at p. 2-3.
[28] *Id.*, at p. 3.

As for its Post Breach Measures, FundKo stated that they implemented a new Privacy Policy to promote transparency in data collection and ensure protection of data.[29]

Moreover, a new FundKo dashboard was deployed and has a "Firebase authentication" where the role of any user is authenticated before they can view the components of the dashboard page.[30]

FundKo claimed that they no longer heard from the 34 affected data subjects and claimed that this was only an isolated case, and that the website is no longer accessible.[31]

Upon evaluation of FundKo's Post-Breach Report, the Commission finds that the PIC has not sufficiently complied with the Order to provide proof of notification to the affected data subjects.

Section 18 (D) of NPC Circular No. 16-03 or the Personal Data Breach Management states:

> *D. Form*. Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.
>
> The **personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach**[.][32] (Emphasis supplied)

Based on FundKo's submission, they repeatedly claimed that they already informed and notified the affected data subjects of the incident.[33] As early as in their Initial Notification dated 22 December 2018, FundKo claimed that the notification was made through email and has also tried to reach the affected clients through their phone

---

[29] Post Breach Report dated 13 July 2022 of Fintechnology, Inc. (FundKo), at p. 3.
[30] *Id.*, at p. 4.
[31] *Id.*, at p. 4.
[32] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V,
§ 18 (D) (15 December 2016) (NPC Circular 16-03).
[33] Notification of a Privacy Breach Incident dated 22 December 2018 of Fintechnology, Inc. (FundKo); Post Breach Report dated 13 July 2022 of Fintechnology, Inc. (FundKo).

numbers.[34] In their Post Breach Report, they reiterated that they already informed the thirty-four (34) affected data subjects and claimed that they no longer heard from them.[35] However, no proof to the same was provided by FundKo.

Thus, the Commission, in order to holistically resolve the matter deems it proper that FundKo, as Personal Information Controller (PIC), shall submit proof of notification sent to the affected data subjects. FundKo is sternly reminded of its obligation to comply with the orders of the Commission.

WHEREFORE, premises considered, Respondent Fintechnology, Inc. (FundKo) is hereby **ORDERED** to submit proof of notification to the affected data subjects **within fifteen (15) days** from the receipt of this Order directly to the Compliance and Monitoring Division (CMD).

The Commission **DIRECTS** the Compliance and Monitoring Division (CMD) to issue the appropriate orders necessary to evaluate and monitor the completeness of Fintechnology, Inc.'s (FundKo) data breach notification and assess its breach management pursuant to NPC Circular 16-03 (Personal Data Breach Management).

SO ORDERED.

City of Pasay, Philippines.
13 November 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

---

[34] Notification of a Privacy Breach Incident dated 22 December 2018 of Fintechnology, Inc. (FundKo), at p. 2.
[35] Post Breach Report dated 13 July 2022 of Fintechnology, Inc. (FundKo), at p. 4.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

BU
Data Protection Officer

ECQ
Counsel for Fintechnology, Inc.

COMPLAINTS AND INVESTIGATION DIVISION COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION GENERAL RECORDS UNIT
National Privacy Commission

IN RE: PHILIPPINE STATISTICS AUTHORITY **NPC BN 23-239**

x----------x

ORDER

Before the Commission is the request for postponement and use of alternative means of notification filed by the Philippine Statistics Authority (PSA) through the Data Breach Notification Management System (DBNMS) dated 10 October 2023.[1]

In its initial report in the DBNMS, it was stated that on 07 October 2023, a PSA employee came across a post by Diablox-Phantom #01 in Facebook.[2] The said Facebook post was captioned, "Philippines Statistics Authority | PSA Data Leak: Sample Record Database Full 42Billion."[3] "Mas Magandang mamatay sa digmaan kesa tanggapin ang maling pamumuno ng bayan, kung panaginip lamang ang umasa sa pagunlad ng bayan, managinip tayo hanggang sa kamatayan MMM2k23."[4]

On 08 October 2023, the Facebook page of Diablox-Phantom #01 was no longer active, however, there is a newly created account under the name Diablox-Phantom #02 with shared identical links.[5] Also, PSA stated that it discovered that when the posted Uniform Resource Locator (URL) is clicked, it redirects to phishing and clickbait websites.[6] In addition, it is also reported that there are social media sites that posted the same statements and links, such as Deep Web Konek, ES, and Philippine I.T. Security Forums.[7]

---

[1] *In re: Philippine Statistics Authority* NPC BN 23-239, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS) (10 October 2023).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *In re: Philippine Statistics Authority* NPC BN 23-239, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS) (10 October 2023).
[6] *Id.*
[7] *Id*

Moreover, on 09 October 2023, PSA's Information Technology (IT) team identified a suspicious file stored in its Network Attached Storage (NAS).[8] PSA stated that based on its logs, the file was uploaded to the storage on 15 September 2023 and that on 26 September 2023, there were downloads in the server not authorized by any PSA personnel.[9] In the initial report, PSA stated that there are "possible files containing responses pertaining to demographic information of survey respondents."[10]

To address the breach, PSA stated that it took offline its NAS, Management Information System (MIS), and FilePinas to prevent unauthorized access. It also activated its Data Breach Response Team (DBRT), conducted an investigation to identify the root cause of the incident for any weaknesses in the MIS, and performed Vulnerability Assessment and Penetration Testing (VAPT) to determine the vulnerabilities in its system.[11]

Further, PSA requested for the postponement to notification of affected data subjects, stating that the "affected data subjects [are] yet to be identified" as its justification for its request[12]

On 20 October 2023, the Commission issued a Minute Resolution ordering PSA to submit proof to substantiate its request for postponement to notify the affected data subjects:

> Pursuant to Section 17 (D) of NPC Circular 16-03 (Personal Data Breach Management), the Commission may require additional information, if necessary, for the proper resolution of the request for postponement to notify the affected data subjects
>
> **WHEREFORE**, premises considered, the Commission hereby **ORDERS** Philippine Statistics Authority to **SUBMIT** within five (5) days upon receipt of this Minute Resolution proof to substantiate the request for postponement to notify the affected data subjects.

---

[8] *Id.*
[9] *In re: Philippine Statistics Authority* NPC BN 23-239, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS) (10 October 2023).
[10] *Id.*
[11] *Id.*
[12] *Id.*

> Should the Philippine Statistics Authority fail to provide the foregoing, this matter shall be submitted for resolution based on the records before the Commission.
>
> **SO ORDERED**.[13]

On 31 October 2023, PSA submitted its Compliance to the Minute Resolution.[14]

In its Compliance, PSA reiterated that "request for postponement of notification to data subjects was made as it was not possible to identify the number of data subjects within seventy-two (72) hours from the discovery of the security incident."[15] Further, PSA was able to identify the affected system and the affected group of data subjects, seventy- two (72) hours after the discovery of the incident.[16] It was identified that the affected group of data subjects belonged to the Community Based Monitoring System (CBMS).[17]

For context, the CBMS contains information obtained by a team composed of Enumerators, Team Supervisors, Area Supervisors, Head Area Supervisors, and PSA Provincial and Regional Focal persons collected from the head of households.[18]

As to the number of affected data subjects, PSA declared that there are approximately ninety-three thousand seven hundred sixty (93,760) affected data subjects by the mean of averaging the members per household, thus:

> At the moment, approximately 23,440 households are affected by the incident. On the average a household is composed of four members. Thus, approximately 93,760 individuals are affected. There is also an estimated 49,000 Enumerators, Team Supervisors Area Supervisors, Head Area Supervisors and PSA Provincial

---

[13] *In re: Philippine Statistics Authority* NPC BN 23-239, Minute Resolution dated 21 October 2023, at p. 1.
[14] Compliance (With Request for Alternative Mode of Notification) by Philippine Statistics Authority dated 31 October 2023.
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] Compliance (With Request for Alternative Mode of Notification) by Philippine Statistics Authority dated 31 October 2023.

> and Regional Focal persons whose personal information are affected.[19]

Additionally, according to PSA, it intends to notify the affected data subjects through the head of the households since the information was collected through them.[20] It will also hire additional manpower to conduct house-to-house delivery of notification.[21] However, considering the number of data subjects, it stated that it needs to "employ also additional means to reach the [data subjects] in the most expedient time."[22] Thus, PSA requests for the use of alternative means of notifying the affected data subjects.[23]

Subsequently, PSA claimed that it will train personnel who will conduct the notification through the heads of the households.[24] Further, the said manpower personnel tasked to conduct the notifications "will be trained to use a secure means of communication, proper identification of the data subject to be notified and will be required to submit an Oath of Data Privacy."[25]

Lastly, PSA stated that it will set up a help desk or a portal where affected data subjects can obtain more detailed information with regard to the incident.[26] Its Legal Service (LS) and the Data Protection and Security Unit (DPSU) will oversee the proposed procedure of data subject notification.[27] Additionally, the LS and DPSU of PSA will train its personnel and will conduct random audits to ensure its compliance with NPC Circular No. 16-03 (Personal Data Breach Management).[28]

The Commission denies PSA's request for postponement of data subject notification and request for use of alternative means of data subject notification.

---

[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] Compliance (With Request for Alternative Mode of Notification) by Philippine Statistics Authority dated 31 October 2023
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] Compliance (With Request for Alternative Mode of Notification) by Philippine Statistics Authority dated 31 October 2023.
[27] *Id.*
[28] *Id.*

Section 18 (B) of NPC Circular No. 16-03 provides:

> *B. Exemption or Postponement of Notification.* If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification. A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects. **The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.**[29] (Emphasis supplied)

To reiterate, PSA's justification for its request for postponement is that the affected data subjects are yet to be identified. However, such justification does not fall within the circumstances when the Commission may authorize the postponement of data subject notification. In this case, notifying the affected data subjects will not hinder the progress of a criminal investigation. Thus, PSA's request for postponement of data subject notification does not fall within the ambit of the above-stated provision.

Additionally, PSA requests for the use of alternative means of notification. According to PSA, it "intends to notify the data subjects through the head of household as the information was collected through them."[30]

Section 18 (D) of NPC Circular No. 16-03 states that:

> D. Form. **Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic.** The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.
> **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects**

---

[29] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V,
§ 18(B) (15 December 2016) (NPC Circular 16-03).
[30] Compliance (With Request for Alternative Mode of Notification) by Philippine Statistics Authority dated 31 October 2023

> **are made aware of the breach:** Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach. (Emphasis supplied)

The Commission emphasizes that the notification to the affected data subjects must be done individually.[31] Also, the Commission stresses that PSA has the obligation to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach.[32] PSA, as the PIC, must not automatically resort to the use of alternative means of notification without exhausting reasonable mechanisms to notify all data subjects affected by the breach.

In seeking the approval of the Commission to use alternative means of data subject notification, PSA failed to justify that "individual notification is not possible or would require disproportionate effort" as stated in Section 18(D) of NPC Circular No. 16-03. Nothing in its submission proves that individual notification is not possible or would need disproportionate effort to notify the affected data subjects.

Further, the Commission finds that notification of the head of the household alone is insufficient. It bears stressing that notification of the head of the household is not tantamount to notification to the affected members of the household. Notwithstanding that the information was collected through the head of the household, data subjects who are members of the household whose personal data was affected by the breach, must also be notified of such incident in order to allow them to take precautions against the likelihood of harm or risk that the incident might cause.[33]

Moreover, the Commission underscores the necessity for PICs to identify the affected data subjects and personal data involved in

---

[31] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18(D) (15 December 2016) (NPC Circular 16-03).
[32] *Id.*
[33] National Privacy Commission. Personal Data Breach Management, NPC Circular 16-03, rule V,
§ 13 (15 December 2016) (NPC Circular 16-03).

breach incidents. In this case, it must be noted that individuals whose personal data are involved, such as sensitive personal information as defined in Section 3(l) of the DPA, and any other information that may be used to enable identity fraud as provided in Section 11(A) of the NPC Circular No. 16-03 are considered the affected data subjects. Thus, individuals whose personal data falls under the definition of the aforementioned provisions must be individually notified.

Furthermore, in establishing all mechanisms to ensure that affected data subjects are made aware of the breach, PSA may carry out the individual notification through sending the data subject notification of members of the household whose personal data is affected by the breach to the head of the household. PSA must provide an individual data subject notification to the members of the household affected by the breach through the head of the household.

In terms of notification to the Commission, although there is no requirement under Section 17(D) of NPC Circular No. 16-03 to determine the precise number of affected data subjects, PICs must employ due diligence and effort in determining the number of affected data subjects to ensure accurate notification to the Commission, especially if the PIC has the information to already determine the precise number of affected data subjects.

WHEREFORE, premises considered, the Commission **DENIES** Philippine Statistics Authority's request for postponement of notification to the affected data subjects and request for the use of alternative means of data subject notification.

The Philippine Statistics Authority is hereby directed to **NOTIFY** all affected data subjects individually through the head of the household.

Further, the Commission **DIRECTS** the Compliance and Monitoring Division (CMD) to issue appropriate orders necessary to evaluate and monitor the completeness of the Philippine Statistics Authority's data breach notification and assess its breach management pursuant to NPC Circular No. 16-03 (Personal Data Breach Management).

SO ORDERED.

City of Pasay, Philippines.
13 November 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

EPA
Data Protection Officer
PHILIPPINE STATISTICS AUTHORITY

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: LAZADA E-SERVICES PHILIPPINES, INC.

NPC BN 18-152

x----------x

ORDER

Before the Commission is the Compliance of Lazada E-Services Philippines, Inc. (Lazada) dated 25 February 2022 in accordance with the Order dated 03 February 2022.

E-Konflux Solutions, Inc. (E-Konflux), a member of the Lazada Group of Companies, provides outsourced customer care services, such as outsourced call center operations, to several Lazada Group companies in Southeast Asia, including Lazada E-Services Philippines, Inc.[1]

On 07 August 2018, during the conduct of internal checks, E-Konflux discovered that a former employee, JB (JB), sent an email on 30 May 2018 (first email), from his E-Konflux work email address to both his personal email address and an email address with his current employer, Shopee.[2]

The e-mail was sent one day before his last working day with E-Konflux and transmitted a file (CS Response Compilation) that contained a compilation of past customer service response logs.[3]

For this reason, the names and e-mail addresses of Lazada's customers were laid out as the logs were not anonymized.[4] One log in the CS Response Compilation set out a Lazada customer's first name and

---

[1] Lazada E-Services Philippines, Inc. Notification/Advisory on Possible Data Breach, 10 August 2018, at 1, *in* In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).
[2] *Id.*
[3] *Id.*
[4] *Id.*

bank account number, and one log set out a different Lazada
customer's first name and physical shipping address.[5]

Lazada alleged that from their preliminary internal checks, it does not seem that any other bank account, payment card details, or physical shipping addresses were disclosed.[6]

Additionally, E-Konflux discovered that JB also sent an e-mail from his personal e-mail address to his work email address on 17 October 2017 (second email), transmitting various customer service response logs in which the names and e-mail addresses of Lazada customers were set out, as well as the CS Response Compilation.[7]

Around one thousand two hundred (1,200) unique customer e-mail addresses were set out in the customer service response logs attached to the two e-mails.[8] These logs are a database of email responses and template response scripts that were accumulated during the employee's time with the company.[9]

The scripts include an "information combination" depending on the issues raised by the customers, such as name and email address, name and physical address, or name and bank account number.[10]

On 10 August 2018, Lazada notified the Commission regarding the incident for a possible data breach.[11] In addition, it also enumerated the initial remediation steps it took to address the situation, namely:

> 1. Our team has made a police report againstJB, and is studying other available legal remedies, including filing a formal case against JB;
> 2. At Lazada's instruction, E-Konflux is initiating audit and manual screenings of all customer service agent workstations

---

[5] Lazada E-Services Philippines, Inc. Notification/Advisory on Possible Data Breach, 10 August 2018, at 1, *in* In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] Final Breach Notification Evaluation Report, 29 November 2022, *in* In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).
[10] *Id.*
[11] Lazada E-Services Philippines, Inc. Notification/Advisory on Possible Data Breach, 10 August 2018, in In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).

in E-Konflux, and requiring that all customer service response logs be anonymized; and

3. At Lazada's instruction, E-Konflux will also explore if it is possible to "re-configure" all workstations of customer service agents servicing Lazada, with the result that they will not be able to send e-mails to non-Lazada e-mail addresses.[12]

On 05 November 2020, the Commission, through its Complaints and Investigation Division (CID), ordered Lazada to submit a Full Report expounding the details of the incident with emphasis on the lacking information from the initial notification report received and attaching the specified documents therein.[13]

As of 03 February 2022, Lazada has yet to comply with the Order to submit a Full Breach Report. Hence, the Commission issued an Order with the following dispositive portion:

> **WHEREFORE**, premises considered, **LAZADA E-SERVICES PHILIPPINES, INC.** is hereby **ORDERED**:
>
> 1. **TO SHOW CAUSE** why it should not be held in contempt, subject to appropriate proceedings, for its failure to abide by the Commission's Order to submit a Full Breach Report dated 05 NOVEMBER 2020;
>
> 2. **TO SUBMIT A FULL BREACH REPORT** containing the proper information and annexes pursuant to the aforementioned Order.
>
> **LAZADA E-SERVICES PHILIPPINES, INC.** is hereby given a period of fifteen (15) days from receipt hereof to submit its compliance through email at complaints@privacy.gov.ph.
>
> **SO ORDERED.**[14]

On 25 February 2022, Lazada sent its Final Breach Report stating that there is no sensitive personal information compromised by the subject incident.[15] Also, it reiterated the remedial measures taken to minimize

---

[12] *Id.*
[13] Order to Submit Full Report, 05 November 2020, *in* In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).
[14] Order for Compliance, 03 February 2022, *in* In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).
[15] Final Breach Report, 25 February 2022, at 3, *in* In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).

the harm and to address the breach, attaching therein the Police Report it filed against JB.[16]

In addition, Lazada submitted its response to the Show Cause Order, explaining that at the time the 10 August 2018 Notification was sent to the Commission, JF (JF) was then the acting Data Protection Officer (DPO) of Lazada PH.[17]

However, Lazada expounded that before the issuance of the 05 November 2020 Order, Lazada PH had already registered CC with the Commission as its official or replacement DPO because of JF's resignation.[18]

Accordingly, the Commission finds that Lazada must notify the affected data subjects due to the considerable number involved, submit proof of such notification and proof of the measures it allegedly took in order to address the incident.

Section 18 (A) of NPC Circular No. 16-03 provides:

> **SECTION 18. Notification of Data Subjects**.
> The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> ***A. When should notification be done.*** The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.
> The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented

[16] *Id.*
[17] Response to Show Cause Order, 25 February 2022, at 1, *in* In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).
[18] *Id.*

> with additional information at a later stage on the basis of further investigation.[19]

In this case, Lazada has yet to notify the affected data subjects because of its belief that the only purpose of JB in sending the logs to himself is to help him in performing his job as a customer service agent, and no unauthorized processing of any personal information transpired.[20]

Based on E-Konflux's initial investigation, the inclusion of customers' names and addresses appears to be merely incidental to the primary purpose as to why JB sent those e-mails and/or stored copies of those files - to secure a database of customer service responses which he can use, particularly in his current employment with Shopee.[21]

Further, Lazada stated that notwithstanding the lapse of time since the questioned e-mails were released, at present, there are still no reported incidents or complaints from any of its customers whose names and/or addresses were included.[22]

It is therefore Lazada's assessment that aside from the fact that only the name and email address of the customers were primarily involved in the incident, no subsequent processing of the information in violation of the customers' privacy rights occurred.[23]

In addition, Section 13 (B) of the same Circular provides:

> **SECTION 13. Determination of the Need to Notify**.
> Where there is uncertainty as to the need for notification, the personal information controller shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred. The personal information controller shall also consider

---

[19] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §18 (15 December 2016).
[20] Final Breach Report, 25 February 2022, at 3, in In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).
[21] Lazada E-Services Philippines, Inc. Notification/Advisory on Possible Data Breach, 10 August 2018, at 1, *in* In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).
[22] *Id.*
[23] Final Breach Report, 25 February 2022, at 3, in In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).

> if the personal data reasonably believed to have been compromised involves:
>
> A. Information that would likely affect national security, public safety, public order, or public health;
> **B. At least one hundred (100) individuals;**
> C. Information required by applicable laws or rules to be confidential; or
> D. Personal data of vulnerable groups.[24]

In Lazada's Breach Notification Report, it stated that the data subject of the incident involved the names and addresses of around one thousand two hundred (1,200) Lazada customers which were embedded within the response scripts used by JB.[25]

On this note, the Commission reiterates the importance of the obligation of Personal Information Controllers (PICs) in notifying the affected data subjects in cases of breach that falls under the instances mentioned by law.[26]

In a number of cases, the Commission emphasized the importance of ensuring that affected data subjects receive timely notification, viz:

> It is noteworthy that the avowed purpose of the required notification to data subjects of a breach incident is for them to take the necessary precautions or other measures to protect themselves against possible effects of the breach. Moreover, personal information controllers (PICs) are required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. It therefore follows that PICs should guarantee that the notification they sent to data subjects has been received. Otherwise, it defeats the very purpose of notification of data subjects.[27]

Notification to the affected data subjects is fundamental in order to allow them to take the necessary precautions or other measures to protect themselves against the possible effects of the breach, especially

---

[24] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §13 (15 December 2016).
[25] Lazada E-Services Philippines, Inc. Notification/Advisory on Possible Data Breach, 10 August 2018, at 2, *in* In Re Lazada E-Services Philippines, Inc., NPC BN 18-152 (NPC 2018).
[26] In Re Crosta Crociere S.p.A., NPC BN 21-185, Resolution dated 23 September 2021, at p. 6.
[27] In Re Health Delivery System, Inc., NPC BN 20-049, Resolution dated 01 July 2021, at p. 5.

given that the incident involved herein consists of more than one hundred (100) individuals.[28]

WHEREFORE, premises considered, the Commission hereby **ORDERS** Lazada E-Services Philippines, Inc. to notify the affected data subjects and to submit the proof of notification and the measures it reportedly took regarding the breach directly to the Compliance and Monitoring Division (CMD).

SO ORDERED.

City of Pasay, Philippines.
02 August 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(On official leave)
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

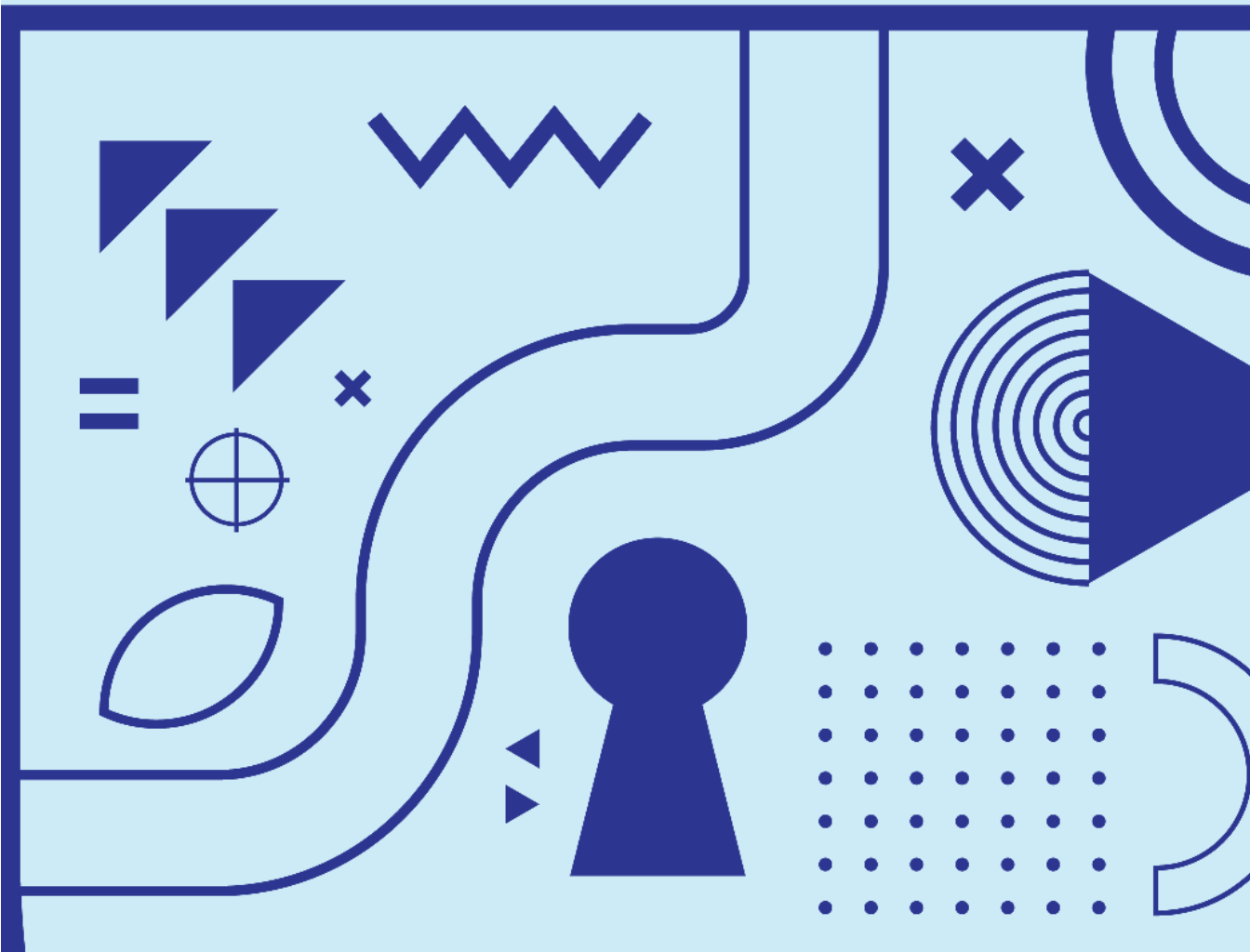
---

[28] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §13 (15 December 2016).

BJ
Data Protection Officer
Lazada E-Services Philippines, Inc.

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

RESOLUTIONS





IN RE: E-SCIENCE CORPORATION **NPC BN 20-124**

x----------x

RESOLUTION

***AGUIRRE*, D.P.C.:**

This Resolution refers to the (1) Update Report dated 30 September 2020[1] and the Supplemental Report[2] dated 16 October 2020 submitted by E-Science Corporation (E-Science) in response to the Resolution of this Commission ordering it to submit proof of compliance on the Notification of Data Subjects, and (2) its Explanation[3] to the Show Cause Order of this Commission.

The Facts

On 10 September 2020, this Commission issued a Resolution[4] with the following disposition, to wit:

> **WHEREFORE**, premises considered, the Request for Exemption to Notify the Data Subjects of E-Science Corporation is hereby **DENIED**. E-Science Corporation is **ORDERED** to submit proof of compliance on the Notification of the Data Subjects within five (5) days from receipt of this Resolution.

In response to the said Resolution, E-Science submitted an Update Report dated 30 September 2020[5] where it enumerated in chronological order the actions it has taken in notifying the data subjects:

(a) On 25 September 2020, E-Science received the Commission's Resolution where it was ordered to immediately release the breach notification to the affected data subjects. E-Science's

---

[1] Notification to the data subjects as compliance for NPC BN No. 20-124 submitted by E- Science Corporation dated 30 September 2020.
[2] Update to E-Science Notification to the data subjects as compliance for NPC BN No. 20-124 submitted by E-Science Corporation dated 16 October 2020.
[3] Show Cause for NPC BN No. 20-124 submitted by E-Science Corporation dated 14 October 2020.
[4] Resolution dated 10 September 2020, *In re: E-Science Corporation*, NPC BN 20-124.
[5] *Supra* note 1.

Data Protection Officer (DPO) called for an internal meeting to plan and execute the notification. Thereafter, the DPO drafted the notification letter for ACABAR, its customer where its employees are the affected data subjects in this breach incident. The DPO detailed the incident to ACABAR through phone and e-mail communication. After such communication, it released a formal letter via e-mail documenting the incident and the Notification letter to ACABAR with the list of possible affected data subjects;

(b) On 28 September 2020, ACABAR acknowledged the receipt of the notification. To ensure proper information and notification, ACABAR prepared the information material to be used to communicate the incident to its employees. ACABAR reportedly prefers to send SMS to all employees to notify them since they are on remote locations and do not have access to e-mail; and

(c) On 30 September 2020, ACABAR told E-Science that the former needs to inform first its principal before sending the message to all the employees, and consult its legal and data privacy officer to make sure that the correct message will be sent. A log will also be sent to E-Science within the week confirming that the message was sent to all the employees. As of 5:00 PM of the day, E-Science was still waiting for the confirmation logs. It then updated this Commission of this report and said that it will send the confirmation logs as soon as they are received.

E-Science expressed its hope that such report satisfies the Commission's Order[6] for it to submit proof of compliance on the Notification of Data Subjects.

On 16 October 2020, E-Science submitted a Supplemental Report[7] where it merely stated that ACABAR has already notified the affected data subjects through an internal messaging system but no proof was attached thereof. It also stated in the same report the contents of the notification message that was claimed to have been sent to the affected data subjects.

[6] *Ibid.*

[7] *Supra* note 2.

As to the Show Cause Order of this Commission, a Resolution[8] was issued on 06 August 2020 with the following disposition, to wit:

> **WHEREFORE,** premises considered, E-Science Corporation is **ORDERED** to **1) SUBMIT** with dispatch a Full Report of the Personal Data Breach as required under Section 17(C) of NPC Circular No. 16-03; and **2) SHOW CAUSE** in writing why it should not be liable for failure to submit a Full Report within the required period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.
>
> Furthermore, the Commission **GRANTS** the request for Postponement of Notification to Data Subjects of E-Science Corporation and directs them to submit proof of compliance thereof within fifteen (15) days from submission of their Full Breach Report. Pending their verification of the full list of affected data subjects, E- Science Corporation is enjoined to use alternative means of notification under Section 18(d) of NPC Circular No. 16- 03.

On 27 August 2020, this Commission reiterated the Show Cause Order through a Resolution[9] with the following disposition, to wit:

> **WHEREFORE**, premises considered, this Commission reiterates its **ORDER** against E-Science Corporation to **SHOW CAUSE** in writing **within five (5) days from receipt of this Order** why it should not be held liable for failure to submit a Full Report within the required period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.

In response to the Show Cause Order, E-Science submitted an Explanation[10] where it enumerated all the actions it has taken to notify this Commission about the breach incident. It also claimed that its initial e-mail on 02 July 2020 was the Initial Report, and its formal report using the full breach report template of the Commission, dated 02 July 2020 but submitted on 03 July 2020, was the Full Breach Report.[11] Hence, E-Science contended that it should not be subjected to contempt proceedings since the Full Breach Report was submitted within the required period.

Discussion

[8] Resolution dated 06 August 2020, In re: *E-Science Corporation*, NPC BN 20-124.
[9] Resolution dated 27 August 2020, In re: *E-Science Corporation*, NPC BN 20-124.
[10] *Supra* note 3.
[11] *Ibid.*

This Commission hereby finds that E-Science's Update Report and Supplemental Report does not satisfy the Order directing it to submit proof of compliance on the Notification of Data Subjects.

On Proof of Compliance

In the Commission's Resolution dated 10 September 2020, it was categorically stated that E-Science should have promptly notified the affected data subjects the moment it has confirmed that the names, e-mail addresses and testing logs of the affected data subjects were indeed involved in the subject breach incident.[12] This Commission also found that E-Science should now be prepared to proceed with the required notification of the data subjects without further delay considering that it has already completed its full investigation on the incident.[13]

Notwithstanding such findings of this Commission in its Resolution, it can be recalled that the E-Science's Request for Postponement of Notification to Data Subjects was previously granted in an earlier Resolution dated 06 August 2020 where it was also directed to submit proof of compliance thereof within fifteen (15) days from submission of its Full Breach Report.[14] However, instead of submitting the required proof of compliance, it submitted a Request for Exemption to Notify Data Subjects.[15] This was denied by this Commission in a Resolution dated 10 September 2020 and E- Science was ordered to submit proof of its compliance within five (5) days from receipt of the same.[16]

On 30 September 2020, E-Science appealed to this Commission to be satisfied with its Update Report.[17] It explained that, pending the submission of the confirmation logs, it has already communicated the breach incident in detail to its customer ACABAR, which will be the one to send the notification to the affected data subjects who are the latter's employees.

On 16 October 2020, E-Science submitted a Supplemental Report[18] claiming that ACABAR has already notified the affected data

---

[12] *Supra* note 4.
[13] *Ibid.*
[14] *Supra* note 8.
[15] Exemption Request to Notify the Data Subjects for NPC BN No. 20-124 submitted by E- Science Corporation dated 18 August 2020.
[16] *Supra* note 4.
[17] *Supra* note 1.
[18] *Supra* note 2.

subjects through an internal messaging system. However, no proof thereof was attached.

Regardless of the internal arrangement or procedure between E- Science and ACABAR, particularly that concerning the notification of the affected data subjects, the former should have already fully complied with the required notification considering the time period that has already lapsed. It should have already included all the actions necessary to coordinate with ACABAR in order to proceed with the notification and acquire the confirmation logs. The various requests of E-Science to this Commission have already unnecessarily prolonged the period for it to notify the affected data subjects. It should be stressed that such period should only be within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller (PIC) or personal information processor (PIP) that a personal data breach has occurred.

This requirement to notify data subjects is not a mere technical procedure to be followed by PICs or PIPs. It is intended to make the affected data subjects aware of the breach incident so that they can take all the necessary and possible measures to protect their personal data or information. Section 18 (A) of NPC Circular 16-03 provides that:

> **The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred**. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects**. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.** It may be supplemented with additional information at a later stage on the basis of further investigation.[19]

Moreover, Section 18 (D) of the same Circular also provides that:

> Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. **The personal information controller**

[19] Emphasis supplied.

> **shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach**: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[20]

Nevertheless, taking into consideration all the actions of E-Science concerning its intention to comply with the subject Order, this Commission hereby reiterates its Resolution dated 10 September 2020 for the submission of proof of compliance, which should include confirmation logs or any documentation of the data subjects' receipt of the Notification.

On the Explanation to the Show Cause Order

As regards E-Science's Explanation[21] to the Show Cause Order, this Commission finds it sufficient. This Commission, however, takes this opportunity to address the contentions made by E-Science where it considered its initial e-mail as the Initial Report and the subsequent formal report as the Full Breach Report.

On 02 July 2020, E-Science, through its Data Privacy Officer (DPO), sent an e-mail[22] to this Commission, stating that:

> This is to notify your commission that **we have identified a possible database breach**. This email serves as the initial notification. **We are still internally investigating the security incident, and will comply with the proper content notification** content.
>
> FYI, **I have been trying to reach your hotline to better understand the notification content** and formal counsel from your office.[23]

Section 17(C) of NPC Circular 16-03 provides that:

---

[20] Emphasis supplied.
[21] *Supra* note 3.
[22] E-mail dated 02 July 2020 sent by E-Science Corporation to the National Privacy Commission.
[23] Emphasis supplied.

> There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, **the Commission shall be notified within the 72- hour period based on available information**. The full report of the personal data breach must be submitted within five (5) days, unless the personal information controller is granted additional time by the Commission to comply.[24]

The initial e-mail sent by E-Science did not include any information that may be available to it at that time. It merely stated that it has identified a possible data breach. By the mere fact that it has identified a possible data breach, it follows that it has received any information that has led into such knowledge. Otherwise, E-Science could not have sent the said e-mail and reported that there was a possible data breach if it has not received any relevant information at all. Hence, said e-mail cannot be considered as the Initial Report since it did not contain any details of the incident.

Moreover, the DPO also stated in the e-mail that they are still investigating the security incident, and they will comply with the proper notification content. By stating that they will comply with the proper notification content, it follows that E-Science will both comply with the submission of the Initial Report and the Full Breach Report, which it failed to do so. In the same e-mail, the DPO also stated that they are trying to reach the Commission's hotline to better understand the notification content. Thus, it can be inferred that the said e-mail is not yet their initial report as they are still trying to understand the notification content that they are yet to comply with.

Lastly, another fact to consider is that both the initial e-mail and formal report are dated 02 July 2020. While it is true that the latter was submitted on 03 July 2020 and that the submission was in accordance with the breach report template of this Commission, the formal report stated that E-Science is still currently doing further investigations.[25] Thus, the formal report cannot be considered as the full breach report yet. It appears that E-Science merely advanced such argument as a mere afterthought and in conscious indifference to the consequences of its negligence to submit the Full Breach Report within the required period.

---

[24] Emphasis supplied.
[25] Initial Data Breach Report dated 02 July 2020.

Be that as it may, considering the actions of E-Science to comply with the directives of this Commission, and the principle that the power of contempt should be used sparingly, judiciously, and with utmost restraint, this Commission considers the Explanation of E- Science sufficient to the Show Cause Order.

WHEREFORE, premises considered, E-Science Corporation is **ORDERED** to submit the confirmation logs or other proof of receipt in compliance to the Notification of the Data Subjects **within five**
(5) days from receipt of this Resolution.

Furthermore, having found the Explanation of E-Science Corporation sufficient, the Show Cause Order is hereby considered as a **CLOSED** matter.

SO ORDERED.

Pasay City, Philippines
22 October 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JYP
Data Protection
Officer E-Science
Corporation

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: AIG SHARED SERVICES - BUSINESS PROCESSING INC. AND AIG SHARED SERVICES CORPORATION – MANAGEMENT SERVICES (ROHQ)

NPC BN 18-033

x----------x

IN RE: MEDICARD PHILIPPINES, INC. - FESTIVAL ALABANG CLINIC

NPC BN 18-076

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is the consolidated breach notifications submitted by AIG Shared Services Corporation – Management Services (ROHQ) (AIGSS-MS) by AIG Shared Services – Business Processing Inc. (AIGSS-BPI) (collectively, AIGSS) and by Medicard Philippines, Inc. - Festival Alabang Clinic (Medicard).

Facts

On 12 March 2018, AIGSS-MS notified the National Privacy Commission (NPC) of a breach:

> In accordance with RA. 10173, "Data Privacy Act of the Philippines", this is to notify the Commission of a recent personal data breach that happened in our organization. Unfortunately, **sensitive personal information of one (1) employee was inadvertently sent to unintended recipients by our medical service provider [i.e. Annual Physical Exam (APE) results were sent to all affected data subjects instead of sending it individually].** The full report of the personal data breach will be

> sent separately. We will also send the acknowledged notification letter by the data subject to you as soon as we receive it.[1]

It attached a Privacy Risk Incident Report (Report) stating that the following personal data of its employees were involved: full name, employee ID, and medical information.[2] AIGSS-MS explained that "human error" was the "principal root cause," and that Medicard was also a responsible party.[3] It stated that the potential harm that may result from the incident was "emotional distress" and "reputational damage."[4] AIGSS-MS reported that it informed the affected data subjects and obtained confirmation from the recipients that the email was deleted and not reproduced.[5] Finally, it reported that it already informed Medicard and was waiting for its response on the matter.[6]

On 14 March 2018, AIGSS-BPI also notified the NPC of the breach.[7] On 23 May 2018, Medicard submitted its breach notification, stating:

1. Nature of the Breach/Incident: Unintended disclosure of Annual Physical Exam (APE) Results
    a. Appointment Officer voluntarily performed the duty of Records Technician to send APE Results of 6 data subjects the neglecting protocol last March 9, 2018.
    b. The unencrypted APE Results were sent to unintended recipients within AIG.
2. Personal Data Possibly Involved: APE Results
3. Remedial Measures to Address the Breach/Incident:
    a. Deletion of all copies of the email containing unencrypted APE Results.
    b. Disciplinary action for the Appointment Officer.

---

[1] Personal Data Breach Notification from AIG Shared Services Corporation - Management Services (ROHQ), 12 March 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018). Emphasis supplied.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] Personal Data Breach Notification from AIG Shared Services Corporation - Business Processing Inc., 14 March 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

c. Reorientation of all clinic personnel of existing security measures.
d. Segregation of duties and limit number of clinic personnel who sends APE Results.
e. Company-wide Data Privacy and Information Security Awareness Program.

Kindly see attachments for the details.[8]

Medicard submitted two email threads to its notification: the first involved the email thread of the breach itself,[9] and the second involved AIGSS and Medicard's correspondence after the breach.[10] AIGSS initiated the correspondence to inform Medicard of the breach.[11] It stated that it was expecting Medicard to perform all measures "to protect [AIGSS'] employees' sensitive personal information."[12] AIGSS also requested an explanation from Medicard, its next steps in addressing the breach, and its assistance in ensuring the email is deleted.[13] Finally, Medicard submitted an email apology sent by Medicard's Alabang Officer to AIGSS.[14]

On the notification of the affected data subjects, Medicard explained:

> We did not perform immediate breach notification because we considered the incident as low/minimal risk and would not cause harm to the 6 data subjects because the recipients of the APE Results were all within AIG. MediCard is committed to complying with RA 10173. We would like to ensure that we are complying with the breach notification requirements even though AIG claimed that they have already reported the breach/incident to the Commission.[15]

---

[8] Personal Data Breach Notification from Medicard Philippines, Inc., 23 May 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018). Emphasis supplied.
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] Personal Data Breach Notification from Medicard Philippines, Inc., 23 May 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2018). [15] *Id.*

On 07 August 2018, the NPC, through the Complaints and Investigation Division (CID), directed AIGSS to submit its Full Report within five (5) days from receipt.[16]

On 21 September 2018, AIGSS requested an additional period of seven
(7) days, or until 28 September 2018, to submit the Full Report.[17] It explained that it needed additional time because of "[t]he volume and nature of the information that it needs to review, as well as AIGSS's desire to provide [the Commission] a Full Report that is both comprehensive and in full compliance with the Memorandum."[18]

On 28 September 2018, AIGSS submitted its Full Report in compliance with the Memorandum dated 07 August 2018.[19]

AIGSS explained that between 11 February 2018 and 02 March 2018, the Annual Physical Exam (APE) of six (6) AIGSS employees was conducted in the Medicard Festival Alabang Clinic. [20] On 09 March 2018, AIGSS' Human Resources Employee (HR employee) requested scanned copies of the APE results of the six (6) employees from the Medicard Alabang Officer to comply with the Occupational Health Permit requirements due on the same day.[21]

The HR employee asked the Medicard Alabang Officer to send the APE results to the Medicard Nurse based in the AIGSS iHub Clinic (iHub Medicard Nurse).[22] In turn, the HR employee instructed the iHub Medicard Nurse to "encrypt and password protect each APE result before sending it individually" to the six (6) employees.[23] The Medicard Alabang Officer, however, sent all the APE results to four (4)

---

[16] Memorandum, 07 August 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[17] Request for extension, 21 September 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[18] *Id.*
[19] Full Report, 28 September 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[20] *Id.* at 1.
[21] *Id.*
[22] *Id.*
[23] *Id.*

out of the six (6) employees, instead of the iHub Medicard Nurse.[24] Further, it was sent without following "the agreed process for handling APE results."[25]

AIGSS stated that on 10 March 2018, one (1) of the four (4) recipient employees reported the incident to the AIGSS Privacy Team.[26] The Privacy Team then initiated a review of the incident and implemented "remediation measures to contain the breach."[27]

The affected data subjects were five (5) employees of AIGSS–BPI and one (1) employee of AIGSS–MS.[28] The following personal information were affected: "1) Full Employee Name, 2) Employee ID Number, 3) Age, 4) [Civil] Status, and 5) Medical Information."[29] AIGSS maintained, however, that other than the AIG Employee ID "there were no other personal information compromised which could enable identity theft."[30]

On measures to address the breach, AIGSS reported that within seventy-two (72) hours, it obtained email confirmation from the four
(4) recipients that "the email had been deleted and was not retained or used by them."[31]

On the notification of the affected data subjects, AIGSS reported that it sent an email to the six (6) affected employees to notify them of the incident.[32] AIGSS explained that this was "because they were AIGSS employees at the time the incident occurred."[33]

---

[24] *Id.* at 2.
[25] Full Report, 28 September 2018, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.* at 3.
[30] *Id.*
[31] Full Report, 28 September 2018, at 3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[32] *Id.* at 5.
[33] *Id.*

AIGSS also reported sending an email to Medicard on 13 March 2018 "informing them about the incident and demanding for an explanation on why the agreed process for distributing APE results was not followed."[34] AIGSS asked for Medicard's remedial measures to ensure the incident does not occur again.[35] On 15 March 2018, AIGSS reported that Medicard responded and advised AIGSS that it had taken the following remedial measures: refresher training for all Medicard staff, implementation of more stringent protocols to safeguard its clients' sensitive personal information, and reduction or limitation of the number of staff that can access clients' sensitive personal information.[36]

On 13 January 2021, the CID issued an Order to Medicard, directing it to submit a Full Report on the breach notification dated 23 May 2018.[37]

On 02 February 2021, Medicard submitted its compliance with the Order dated 13 January 2021:

> On March 9, 2018, 6:42am, AIG-HR staff Ms. AMB emailed Ms. JL2[sic] (Appointment Officer) of MediCard-Festival Alabang Clinic to send the APE results of 6 employees before 12nn on the same day. From the same email, she then instructed 2 other AIG Personnel (CRN and ihub nurse) to send the said APE results to the 6 employees. At 11:39am of the same day, Ms. JL of MediCard Festival Clinic sent the APE results. However, she included the 6 employees on the said email neglecting the instructions given by Ms. AMB.
>
> On March 10, 2018, 1:18am, upon receiving Ms[.] JL's email, Ms[.] AMB of AIG replied that the APE results were sent to [ ] unintended recipients and that she [was] clear of her instructions that she only authorized CRN and ihub nurse to send the results to their owners and not her.
>
> Ms. JL sent her apologies to Ms. AMB following the incident (email dated March 10, 9:22am) and explained that she thought it was allowed to send the results to the employees since they need to submit it as part of the requirement for their health

---

[34] *Id.* at 3.
[35] *Id.*
[36] *Id.* at 4.
[37] Order, 13 January 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

> permit. She also voluntarily performed the duty of a Records Technician to send the APE results due to the urgency of the request.[38]

Medicard also submitted the following documents with its compliance: a screenshot of Clause 7 from Medicard and AIGSS' contract;[39] an email to AIGSS providing a narration of the breach and the countermeasures it implemented;[40] and a copy of the email thread where AIGSS requested its employees to delete the email.[41]

As proof of the security measures it implemented, Medicard also submitted the following documents: a memorandum from Medicard's Clinic Services Department addressed to all personnel, reminding them of minimum requirements in handling personal and sensitive personal information;[42] a Notice of Disciplinary Action to the Medicard Alabang Officer imposing a ten-day suspension;[43] screenshots of Medicard's internal information campaign on procedures to protect personal information;[44] a memorandum requiring attendance of Medicard employees, contractuals, and consultants to a data privacy and information security awareness training;[45] a memorandum requiring the encryption of digitally processed personal information within Medicard's system; and a memorandum announcing th0e implementation of security features of "Sophos Email Appliance (email gateway)" starting 01 October 2018.[46]

On 26 February 2021, the CID sent another Order to AIGSS, directing it to submit a Full Report on the breach notification in 2018.[47]

---

[38] Full Report, 02 February 2021, at 2-3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] Full Report, 02 February 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[45] *Id.*
[46] *Id.*
[47] Order, 26 February 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

On 11 March 2021, AIGSS filed a Motion for Extension to submit its compliance with the Order dated 26 February 2021.[48] It explained:

> The current deadline you have provided to us to respond to the Order falls on Monday, 15 March 2021 (given that 13 and 14 March fall on the weekend). However, as the matter that is the subject of the Order occurred sometime ago (the matter occurred three years ago and our last correspondence with your good office was in September of 2018), we require further time to collate the information surrounding this matter.
>
> In the circumstances, we are humbly requesting your good office for an extension of time **until 29 March 2021** to respond to your Order.[49]

On 29 March 2021, AIGSS submitted its compliance with the Order dated 26 February 2021.[50] At the outset, AIGSS argued that any investigations by the NPC should be directed at Medicard, who was the PIC of the affected data subjects.[51] It noted that the description of the Order dated 26 February 2021 stated the NPC was investigating "Possible Data Privacy Violations Committed by [AIGSS-BPI] and [AIGSS-MS]."[52] AIGSS explained:

> We believe that any investigations which your good office wishes to conduct in this matter should not be directed at either AIGSS- BPI or AIGSS-MS as we were not the Personal Information Controllers of the personal information found in the results of the annual physical examinations ("APE"). We have explained below that Medicard Philippines, Inc. ("Medicard") was the Personal Information Controller of the APE results. You may, therefore, wish to contact Medicard directly (if not already done) should you have any queries regarding this matter as they will be in the best position to provide you with the relevant information relating to this matter.[53]

---

[48] Motion for Extension, 11 March 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines – Festival Alabang Clinic, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[49] *Id.* at 1.
[50] Compliance, 29 March 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[51] *Id.* at 1.
[52] *Id.*
[53] *Id.*

AIGSS then explained that "Medicard is a licensed healthcare provider and Health Maintenance Organization which offers Corporate Health Programs."[54] AIGSS – MS and AIGSS-BPI participated in Medicard's Corporate Health Program "for the purposes of offering employees medical benefits."[55] As part of these medical benefits, employees were entitled to an annual physical examination.[56] According to AIGSS, "six (6) employees (5 from AIGSS-BPI and 1 from AIGSS-MS) attended one of Medicard's own free-standing clinics, the Medicard Alabang Clinic, at Festival Supermall, Alabang, Muntinlupa City between February 11 and March 2, 2018 for their annual physical examinations."[57]

AIGSS then proceeded to discuss the breach, substantially reiterating its narration in the Personal Data Breach Notification.[58] It added that "[t]he APE results were also not meant to be sent directly to the AIG Shared Services Human Resources officer."[59] It clarified that "Medicard ought to have instead sent an email to each of the 6 employees individually, attaching only the APE results of the employee to whom each of the emails was addressed."[60]

AIGSS also reiterated its position that Medicard is the PIC.[61] It stated that the notification to the Commission on 12 and 14 March 2018 was made only "as a courtesy and out of an abundance of caution on behalf of [AIGSS'] employees."[62] It explained:

> 5. [T]he purposes for which Medicard collects, uses, discloses and/or processes the personal information found in the results of APEs as well as the methods used by Medicard in collecting, using, disclosing and processing the said personal information is entirely in the control of Medicard. Medicard provides the APE

---

[54] *Id.*
[55] *Id.*
[56] Compliance, 29 March 2021, at 1-2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[57] *Id.* at 2.
[58] *Id.* at 1-2.
[59] *Id.* at 2.
[60] *Id.*
[61] *Id.* at 1.
[62] Compliance, 29 March 2021, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

> results directly to the employees and not to either AIGSS-BPI or AIGSS-MS. In the circumstances, Medicard was the Personal Information Controller in respect of the personal information found in the APE results and was obliged to protect such personal information from, amongst other things, accidental disclosure.
>
> . . .
>
> 7. As AIGSS-BPI and AIGSS-MS were aware of the matter, we informed your good office about the matter through our emails of March 12 and 14, 2018 as a courtesy and out of an abundance of caution on behalf of our employees. For the avoidance of doubt, any obligation to notify your good office of this matter pursuant to the Data Privacy Act of 2012 ("Privacy Act") falls on Medicard as the Personal Information Controller which disclosed the APE results of the 6 employees and not AIGSS-BPI nor AIGSS-MS.[63]

Issue

Whether AIGSS and Medicard were able to sufficiently address the breach and to implement security measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. The incident does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03 (Personal Data Breach Notification). Only the first two requisites are present in this case. The third requisite of real risk of serious harm is absent because of the security measures that AIGSS implemented.

Section 11 of NPC Circular 16-03 provides:

> Section 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.

---

[63] *Id.*

A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords, and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
B. There is reason to believe that the information may have been acquired by an unauthorized person; and
C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[64]

Following this, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[65]

The first requisite is present. The information involved is sensitive personal information and other information that may enable identity fraud.

The information inadvertently emailed by the Medicard Alabang Officer includes the employees' age, civil status, and medical information,[66] and Medicard ID number.[67] These are considered

---

[64] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).
[65] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-SS-22-001-and-NPC-SS-22-008- 2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 02 August 2023).
[66] Full Report, 28 September 2018, at 3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[67] *Id.* at 3.

sensitive personal information under Section 3 (l) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA). [68]

Further, the information involved may enable identity fraud, since it may be "made the basis of decisions concerning the data subject, including the grant of rights or benefits."[69] AIGSS stated that "Medicard is a licensed healthcare provider and Health Maintenance Organization which offers Corporate Health Programs."[70] AIGSS–MS and AIGSS-BPI participated in Medicard's Corporate Health Program "for the purposes of offering employees medical benefits."[71] This, taken together with the fact that the information compromised included employee information and Medicard ID number, may enable identity fraud for the purpose of claiming medical benefits.

Medicard also submitted a screenshot of Clause 7 from Medicard and
AIGSS' Agreement, which provides:

> **7. AUTHORITY TO EXAMINE MEDICAL RECORDS.** The COMPANY hereby represents and warrants that, at the time of the effectivity of this Agreement and **effectivity of coverage of each MEMBER and his dependents,** it has obtained from the MEMBER and his dependents the required consents authorizing MediCard and any of its authorized representatives to: (a) obtain, examine and process the MEMBER'S personal information, including the medical records of their hospitalization, consultation, treatment or any other medical advice in connection with the **benefit/claim availed under this Agreement;** and (b) disclose such information to the COMPANY and its representatives[.][72]

The use of "dependents" and "benefit/claim" in Clause 7 shows that, apart from providing medical examinations for Occupational Health

---

[68] *See* An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (l) (2012).

[69] NPC Circ. No. 16-03, § 11 (A).

[70] Compliance, 29 March 2021, at 1, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

[71] *Id.* at 1.

[72] Full Report, 02 February 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

Permit requirements, the Agreement between Medicard and AIGSS includes Medicard health insurance coverage for AIGSS employees and their dependents.[73] The name, age, and civil status of the employee, taken together with their employee ID number, are necessary considerations for Medicard's decision to grant medical benefits or claims of AIGSS' employees.

Given the foregoing, unauthorized acquisition of the personal data and APE results may be used to fraudulently assume the identity of an AIGSS employee covered by Medicard's Corporate Health Program.

The second requisite is also present. Unauthorized persons acquired the personal data and APE results in the emailed Excel file.[74]

The Commission held that a loss of control over personal data held in custody is enough for a PIC to have "reason to believe that the information may have been acquired by an unauthorized person."[75]

AIGSS admitted that the Medicard Alabang Officer sent all the APE results in a single email to four (4) out of the six (6) employees, instead of the iHub Medicard Nurse.[76] Medicard reiterated this in its breach notification dated 23 May 2018[77] and in its compliance dated 02 February 2021.[78] Hence, both AIGSS and Medicard admitted that the PIC lost control and unauthorized persons acquired the personal data of the data subjects.

Further, the HR employee instructed the iHub Medicard Nurse, and not the Medicard Alabang Officer, to "encrypt and password protect each APE result before sending it individually" to the six (6)

---

[73] *Id.*
[74] *Id.* at 2-3.
[75] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).
[76] Full Report, 28 September 2018, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[77] Personal Data Breach Notification from Medicard Philippines, Inc., 23 May 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2018). [78] Full Report, 02 February 2021, at 2-3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

employees.[79] The Medicard Alabang Officer, however, voluntarily undertook to send the APE results without following "the agreed process for handling APE results."[80]

Finally, AIGSS submitted a copy of the email from the employee who reported the breach.[81] The employee reported that their x-ray result file was incorrectly placed in another person's APE file, which shows that the recipients were able to open and view the contents of the APE results.[82]

The lack of security measures enabled the viewing of such personal information by the four (4) AIGSS employees, which should be sufficient to form a reasonable belief for the PIC.[83]

Nonetheless, the third requisite is not present due to the security measures that AIGSS implemented after the breach.

The Commission takes this opportunity to discuss the factors considered in determining the presence of the third requisite of mandatory breach notification. Section 11 (C) of NPC Circular 16-03 provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> . . .
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give

---

[79] Full Report, 28 September 2018, at 1, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[80] *Id.* at 2.
[81] Compliance, 29 March 2021, Annex 3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[82] *Id.*
[83] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).

> rise to a real risk of serious harm to any affected data subject.[84]

For this purpose, the phrase "likely to give rise to a real risk" in Section 11 (C) means that a link exists between the breach and the possible resulting harm to any affected data subject.[85] The risk must be apparent and not the product of mere speculation.[86] Serious harm means that the consequences and effects to any affected data subject is significant based on the surrounding circumstances of the breach.[87]

In determining whether the unauthorized acquisition is likely to give rise to real risk of serious harm, a PIC or the Commission may consider several factors, such as: the nature and amount of information involved in the breach, the period of time that has lapsed since the breach, objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.

In this case, the unauthorized acquisition of information was due to the inadvertent transmittal of all the APE results to the four (4) AIGSS employees.[88] There is no showing that the AIGSS employees deliberately intended to obtain the information of other employees, as one of the four (4) recipient employees even reported the incident to the AIGSS Privacy Team.[89] The erroneous transmittal stemmed from the Medicard Alabang Officer's misunderstanding of the directive to send the results to the iHub Medicard Nurse,[90] as shown in the Medicard Alabang Officer's explanation in the breach's email thread.[91]

---

[84] NPC Circ. No. 16-03, § 11.
[85] NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8 (NPC 2023) (unreported).
[86] *Id.*
[87] *Id.*
[88] Full Report, 28 September 2018, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[89] Compliance, 29 March 2021, Annex 3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[90] Full Report, 28 September 2018, at 1, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[91] Personal Data Breach Notification from Medicard Philippines, Inc., 23 May 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

Thus, the objective of the unauthorized acquisition was not for fraudulent purposes.

It must be emphasized that the nature and amount of information involved in the breach—name, employee ID number, age, civil status, and medical information—are important details with respect to availing the medical benefits under Medicard's Corporate Health Program.[92]

Nonetheless, the security measures implemented by AIGSS prevented the occurrence of the risk of serious harm to the affected data subjects.

AIGSS notified the affected data subjects.[93] After one (1) of the recipient employees reported the incident on 10 March 2018,[94] AIGSS' Privacy Team initiated a review of the incident on the same date and implemented "remediation measures to contain the breach."[95] Thereafter, AIGSS reported that within seventy-two (72) hours it obtained email confirmation from the four (4) recipient employees that "the email had been deleted and was not retained or used by them."[96] Furthermore, AIGSS reported that it sent an email to all six (6) affected employees to notify them of the incident.[97] The notification states:

> Dear [],
>
> We very much regret to advise you that we recently became aware of an incident involving your sensitive personal data. In compliance with the Data Privacy Act (Republic Act 10173) and AIG Shared Services Data Privacy Reporting Procedure, we are informing you that your APE Results containing sensitive personal information were inadvertently sent by a Medicard employee to unauthorized recipients last March 9, 2018.

---

[92] Compliance, 29 March 2021, at 1-2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[93] *Id.* Annex 5-A to 5-D.
[94] Full Report, 28 September 2018, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[95] *Id.*
[96] *Id.* at 3.
[97] *Id.* at 5.

> You may get your own APE results in the attachment then delete all communications pertaining to the subject and its attachments. Please do not forward to any other users and refrain to reproduce it. Rest assured that we are coordinating and in communication with Medicard to ensure that all measures are being taken to protect your sensitive personal information and ensure that this will not happen again. A request has been sent to unauthorized recipients to delete all communications pertaining to the subject and its attachments. We will also request Medicard to do the same on the person who sent the email and a confirmation that it has been deleted.
>
> You can reach out to me or to BP Jr. our Data Protection Officer for AIG Shared Services – Business Processing Inc. (email address at [ ] with contact number [ ] ; cell number [ ]) for additional information regarding the breach, and for any support or clarification.
>
> Lastly, please send us a confirmation that you have deleted the said email.
>
> Thank you[.][98]

As proof of notification, AIGSS submitted an email notification regarding the breach (sent on 12 March and 13 March 2018), and confirmation of deletion from the four (4) recipients.[99]

Section 18 (C) of NPC Circular 16-03 provides the required content of proper notification of affected data subjects:

> Section 18. *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> C. *Content of Notification.* The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;

---

[98] Compliance, 29 March 2021, Annex 5-A to 5-D, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[99] *Id.*

3. measures taken to address the breach;
4. measures taken to reduce the harm or negative consequences of the breach;
5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. any assistance to be provided to the affected data subjects.

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.[100]

Further, Section 18 (D) of NPC Circular 16-03 provides the required form of proper notification:

> Section 18. *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> D. *Form.* Notification of affected data subjects shall be done **individually, using secure means of communication, whether written or electronic.** The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and **to safeguard against further unnecessary disclosure of personal data.** The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish **means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.**[101]

---

[100] NPC Circ. No. 16-03, § 18 (C).
[101] *Id.* § 18 (D).

The notification sent to affected data subjects must contain sufficient information on the nature of the breach incident, the personal data involved, the measures taken by the PIC to address the breach and to reduce harm or negative consequences of the breach, and the assistance it extended to its affected data subjects.[102] Further, the form of notification must be individual and must be made through secure means of communication, whether written or electronic.[103] The PIC must provide the data subject with the means to exercise their rights and obtain more detailed information relating to the breach.[104]

In this case, the Commission finds that the email notification complied with the requirements under Section 18 (C) and Section 18 (D) of NPC Circular 16-03.[105] The email notification contained information on the nature of the breach incident, the personal data involved, the measures taken by AIGSS to address the breach and to reduce harm or negative consequences of the breach, and a contact number that data subjects can use to obtain assistance and information.[106] Further, it was sent individually through email.[107] Thus, the notification enabled the affected data subjects to take measures to protect themselves from the consequences of the breach.

The Commission acknowledges the efforts of AIGSS to promptly notify the affected data subjects and implement security measures. In contrast, however, the Commission strongly reprimands Medicard for its failure to take action and its mere reliance on the measures taken by AIGSS.

The Commission agrees with AIGSS that Medicard is the PIC. As explained by AIGSS in its Compliance dated 29 March 2021:

> 5. The annual physical examinations of these 6 employees and any tests for the purposes of these examinations were carried out by Medicard at its Alabang clinic by Medicard's doctors, nurses, and staff based on their professional knowledge, skill, and expertise. AIGSS-MS and AIGSS-BPI naturally ha no input into

---

[102] NPC BN 18-198, 23 September 2021, at 4 (NPC 2021) (unreported).
[103] NPC Circ. No. 16-03, § 18 (D).
[104] *Id.*
[105] *Id.* § 18 (C) - (D).
[106] NPC BN 18-198, 23 September 2021, at 4 (NPC 2021) (unreported).
[107] NPC Circ. No. 16-03, § 18 (D).

> the conduct of such physical examinations. **The purposes for which Medicard collects, uses, discloses, and/or processes the personal information found in the results of APEs as well as the methods used by Medicard in collecting, using, disclosing, and processing the said personal information is entirely in the control of Medicard. Medicard provides the APE results directly to the employees and not to either AIGSS-BPI or AIGSS-MS.** In the circumstances, Medicard was the Personal Information Controller in respect of the personal information found in the APE results and was obliged to protect such personal information from, amongst other things, accidental disclosure.[108]

Clause 7 of the Agreement between AIGSS and Medicard[109] further confirms that Medicard is the PIC:

> [I]t is hereby agreed that it is the sole responsibility of the COMPANY to obtain from the MEMBERS the consent herein specified and that **MediCard shall have all the right to rely on the representation by the COMPANY that this consent shall have been duly and timely obtained.** The COMPANY shall hold MediCard free and harmless from and against any and all suits or claims, actions, or proceedings, damages, costs and expenses, including attorney's fees, which may be filed, charged or adjudged against MediCard or any of its directors, stockholders, officers, employees, agents, or representatives in connection with or arising from the **use by MediCard of the MEMBER'S medical records and other personal information pursuant to this Agreement and disclosure of such information to the COMPANY and its representatives pursuant to MediCard's reliance on the COMPANY'S representation and warranty that MediCard has the authority to examine, use or disclose, as the case may be, said medical records or personal information.**[110]

While there is shared responsibility between AIGSS and Medicard in that AIGSS was responsible for obtaining its employees' consent for processing of their information, ultimately it is still Medicard that processes their personal information to provide health insurance coverage. Moreover, it was Medicard's own personnel that

---

[108] Compliance, 29 March 2021, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021). Emphasis supplied.
[109] Full Report, 02 February 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[110] *Id.* Emphasis supplied.

inadvertently sent the APE results to the four (4) AIGSS employees, neglecting the protocol of encryption and password protection.[111]

There is no showing, however, in any of Medicard's submissions that it made efforts to notify its affected data subjects. It merely stated in its Full Report that it did not notify because it deemed the incident as "minimal/low risk."[112] It reasoned as follows:

> **We did not perform immediate breach notification because we considered the incident as low/minimal risk and would not cause harm to the 6 data subjects because the recipients of the APE Results were all within AIG.** MediCard is committed to complying with RA 10173. We would like to ensure that we are complying with the breach notification requirements even though AIG claimed that they have already reported the breach/incident to the Commission.
>
> MediCard was invited by Deputy Commissioner Ivy Patdu for a meeting last May 22, 2018 to discuss about Data Sharing Agreement and the AIG incident was brought up. We were advised by DepCom Patdu and Atty Mike to perform a breach notification and not to rely on AIG's notification to ensure that Medicard performed its duty as PIC.[113]

The Commission finds that Medicard's reasoning is not justified. If Medicard was truly committed to complying with its obligations under the DPA, as it claims, it should have promptly notified both the NPC and the affected data subjects upon receipt of AIGSS' email informing it of the incident as early as 13 March 2018.[114] Instead, Medicard sent a notification to the NPC only on 23 March 2018, fourteen (14) days after the breach.[115] Even worse, there is no showing that Medicard made any effort to notify the data subjects.

---

[111] Full Report, 28 September 2018, at 1, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[112] Personal Data Breach Notification from Medicard Philippines, Inc., 23 May 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018). Emphasis supplied.
[113] *Id.* Emphasis supplied.
[114] *Id.*
[115] *Id.*

The Commission sternly reminds Medicard that although it was appropriate to implement security measures within its organization, such measures were prospective and insufficient to protect the affected data subjects from the risk they were already exposed to.[116] The purpose of notification is to provide data subjects with an opportunity to take the necessary precautions to protect their own data against the possible effects of the breach.[117] As such, PICs such as Medicard are required to "establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach."[118] Data subject notification is an essential obligation of a PIC,[119] and Medicard utterly failed to fulfill such obligation in this case.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-033 In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation – Management Services (ROHQ) (AIGSS), and NPC BN 18-076 In re: Medicard Philippines, Inc. – Festival Alabang Clinic (Medicard) is **CLOSED.**

The Commission **DIRECTS** the Compliance and Monitoring Division (CMD) to conduct a Compliance Check on the sufficiency of Medicard's security measures involved in the processing of personal data.

SO ORDERED.

City of Pasay, Philippines.
02 August 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

---

[116] Resolution, NPC BN 20-149 In re: National Privacy Commission 20 August 2020, at 6 (NPC 2020) *available at* https://www.privacy.gov.ph/wp-content/uploads/2022/01/Resolution-NPC-BN-20- 149-In-re-NPC.pdf (last accessed 02 August 2023).
[117] NPC Circ. No. 16-03, § 18 (D).
[118] *Id.*
[119] Order, NPC BN 21-035, 01 June 2021, at 4 (NPC 2021) (unreported).

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

(on official leave)
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

SG
Data Protection Officer
AIG Shared Services – Business Processing, Inc.
AIG Shared Services Corporation – Management Services (ROHQ)

RCM
Data Protection Officer
Medicard Philippines, Inc.

COMPLAINTS AND INVESTIGATION DIVISION
COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: MANUFACTURERS LIFE INSURANCE CO.

NPC BN 18-213

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is a confidentiality breach involving the misdelivery of a Variable Unit Linked (VUL) Statement of Account (SOA) belonging to a Manufacturers Life Insurance Co. (Manulife) client.

Facts

On 13 November 2018, a Manulife agent emailed its Customer Care to report that his client, VL, received a VUL SOA by mail.[1] The VUL SOA, however, belonged to another Manulife client, LTE.[2]

Manulife sent an Incident Notification dated 30 November 2018 to the National Privacy Commission (NPC). Manulife explained that it learned of the incident on 14 November 2018.[3] The VUL SOA contained the following information: "1) Name of client; 2) Address;
3) Policy number; 4) Name of insured; and 5) Account summary (face amount, units bought/sold, premium amount, balances, charges/fees, current value, payments, etc.)."[4]

---

[1] Full Report, 21 October 2020, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[2] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[3] *Id.*
[4] *Id.*

Manulife also reported that it discovered that "LTE's outdated mailing address resulting [sic] to the same being delivered to her old address now being occupied by VL."[5]

As a result, Manulife immediately requested VL to surrender or return the misdelivered VUL SOA to her agent.[6] Manulife also asked its Information Services (IS) Team to immediately conduct an investigation of the incident.[7]

Manulife's IS Team initially reported to management that "[t]he old address supplied by the client, which address had already been previously updated, was erroneously tagged as the client's current mailing address"[8] and that "only VUL SOAs were affected."[9]

As its measures to address the breach, Manulife reported that the IS Team implemented fixes to ensure the system generating the VUL SOAs would use the correct and updated addresses of its clients.[10] In the meantime, Manulife stated that "no VUL SOAs were generated and sent out."[11] The fixes were reported to have been completely implemented on 16 November 2018.[12] Manulife did not affirm whether VL fulfilled its request to surrender or to destroy the VUL SOA.

Manulife maintained that "[d]espite the information contained in the VUL SOA," it had appropriate measures in place to minimize the risk of harm or fraud that may arise from the misdelivery.[13] It argued:

> Should a person call the Company's hotline, minimum validation procedures are in place to verify the identity of the client. These validation questions pertain to information that cannot be found in the VUL SOA. For other transactions involving the client's policy, specific forms have to be filled out and identification documents need to be submitted.

---

[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*

> In light of the validation requirements in place that sufficiently protect the client from identity theft and fraud, or some other serious harm, it is respectfully asserted that Manulife Philippines is not required to notify the affected client. Nevertheless, rest assured that the Company will make the necessary notification if further investigation reveals that the same is warranted.[14]

On 06 October 2020, the NPC, through its Complaints and Investigation Division (CID), issued an Order directing Manulife to submit its Full Report within fifteen (15) days from receipt.[15] With respect to Manulife's Incident Notification dated 30 November 2018, the CID concluded that "the notification did not provide the process conducted to notify the affected data subject."[16] The CID also found that the Incident Notification did not "offer assistance that may be required to mitigate any possible damage that may be caused by the incident."[17]

On 21 October 2020, Manulife submitted its full report in compliance with the CID's Order. It reiterated its narration in the Incident Notification dated 30 November 2018, with additional details as to security measures it had taken since the breach occurred.[18] Manulife also submitted a copy of its Data Privacy Manual.[19]

On 14 November 2018, or the day after the breach, the IS Team investigated the VUL SOA generation.[20] It confirmed that LTE's old mailing address, which was now VL's current address, was erroneously tagged as LTE's current mailing address in the Client Administration System (CAS).[21] According to Manulife, the IS Team reported that the CAS "fetched the first address recorded in a policy record instead of the most current one."[22] The IS Team concluded that this error resulted from a system patch done at the end of October

---

[14] Incident Notification, 30 November 2018, at 1-2, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[15] Order, 06 October 2020, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[16] *Id.* at 1.
[17] *Id.*
[18] Full Report, 21 October 2020, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[19] *Id.*
[20] *Id.* at 1-2.
[21] *Id.* at 1.
[22] *Id.* at 1-2.

2018.[23] The issue was then escalated to Manulife's Data Protection Officer.[24]

After an investigation by its Operations team and IS team, Manulife reported that it discovered the erroneous tagging similarly affected a total of one hundred (100) printed VUL SOAs.[25] Nonetheless, Manulife reported that it was able to stop its courier from sending eighty-nine (89) of the printed VUL SOAS.[26] Manulife explained that:

> Out of the 11 delivered VUL SOAs:
> - 8 were actually received by the correct clients;
> - 1 had the correct address;
> - 1 was sent to the client's office address where he was still connected at that time;
> - 1 pertained to a client who was outside of the Philippines. This client was contacted by a Manulife agent and did not pose any complaint or issue regarding his non-receipt of the SOA.[27]

As such, Manulife concluded that other than LTE, no other clients were impacted by the incident.[28]

According to Manulife, the personal data of LTE involved and disclosed to VL were: "a) Name of affected client as Policy Owner and Insured; b) Address, old address of affected client which was now the address of the unintended recipient; c) Policy number of affected client; and d) Account summary (face amount, units bought/sold, premium amount, balances, charges/fees, current value, payments)."[29] Nonetheless, Manulife argued that the personal data involved is insufficient for VL to access LTE's Manulife account.[30] Further, Manulife argued that VL remained unaware of LTE's current address.[31]

---

[23] *Id.*
[24] Full Report, 21 October 2020, at 2, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[25] *Id.*
[26] *Id.* at 1-2.
[27] *Id.* at 2.
[28] *Id.*
[29] *Id.* at 3.
[30] Full Report, 21 October 2020, at 3, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[31] *Id.*

Manulife also explained why "there is a low likelihood of any adverse
impact on the data subject":[32]

> a) It is highly unlikely that the data received by the **sole** unintended recipient, the very same person who reported the incident to her Manulife agent, would be used for identity theft or other nefarious purposes by the recipient.
>
> b) It should also be noted that validation procedures are in place to verify the identity of a client who calls or communicates with the Company. These validation questions pertain to information that cannot be found in the VUL SOA that was sent to the unauthorized recipient. This means that the information the unauthorized recipient got from the VUL SOA would not be sufficient for her to conduct transactions on the policy belonging to the other client.
>
> c) Further, for major transactions involving a client's policy (such as change of address or beneficiary, surrender of policy, policy loans), specific forms have to be filled out and signed by the client, and valid identification documents have to be submitted.[33]

Manulife also reported taking "safeguards to minimize harm or mitigate impact of the breach."[34] It explained that it stopped sending VUL SOAs immediately upon learning of the error and "until the system issue was identified and fixed."[35] It also stated that it checked LTE's policy for possible suspicious transactions[36] and that "[t]o date, there has been no red flag for any account takeover or fraud on the data subject's account."[37]

Manulife stated that once the issue with its CAS was resolved, it performed a qualitative check and an audit on the VUL SOAs sent out for the next thirty (30) days, "to ensure that the correct information were being picked up in the SOAs" prior to being sent out to clients.[38] Manulife also reported adding "enhancements to the software

---

[32] *Id.* at 2.
[33] *Id.*
[34] *Id.* at 3.
[35] *Id.*
[36] Full Report, 21 October 2020, at 3, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[37] *Id.*
[38] *Id.*

development lifecycle" to avoid recurrence of the incident.[39] It also stated that "mandatory testing and Quality Assurance were made compulsory prior to the release of any SOA."[40] According to Manulife, "[a]s far as practicable, taking into consideration the inherent and residual risks, all system enhancements involving clients' data have undergone the necessary testing and signoffs before they were implemented."[41]

On remedial measures to address the breach, Manulife reiterated that it advised VL to either return the VUL SOA to Manulife or to destroy it.[42] Similar to its Incident Notification,[43] however, Manulife did not confirm whether VL returned or destroyed the VUL SOA.

Manulife also reported engaging the services of a third-party service provider, KPMG, to "conduct an evaluation of existing processes, systems and controls that impact data privacy."[44] Manulife explained that this third-party independent evaluation was "supposed to have been done at the early part of [2020] but was delayed due to the current COVID-19 situation."[45]

Given the foregoing measures, Manulife argued that the incident "has almost no adverse impact on the Company and the public at large."[46] Manulife maintained that "[i]f at all, the incident led the Company to improve its existing systems and processes to better protect its clients' information."[47] Manulife also noted that "to date, it has not received any complaint arising from mis-directed [sic] VUL SOAs."[48]

Finally, Manulife requested exemption from the notification of the affected data subject.[49] It reasoned:

---

[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] Full Report, 21 October 2020, at 1-2, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[43] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[44] Full Report, 21 October 2020, at 3, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[45] *Id.*
[46] *Id.* at 2.
[47] *Id.*
[48] *Id.*
[49] *Id.* at 4.

> In determining whether there was a need to notify the data subject of the incident, the primary consideration was the likelihood of harm or negative consequence caused by the mis- delivered VUL SOA.
>
> In light of the validation requirements in place that sufficiently protect the client from identity theft and fraud, or some other serious harm, it is respectfully requested that pursuant to Section 19, Rule V of the National Privacy Commission Circular 16-03 on Personal Data Breach Management, the Company be exempted from Notification Requirements. This request is bolstered by the fact that despite the lapse of two years from the incident, there was in fact no suspicious transaction on data subject's account.[50]

On 09 December 2022, the CID assessed that the matter does not fall within mandatory notification under NPC Circular 16-03 (Personal Data Breach Management):

> It must be remembered that Manulife specified that they have a validation procedure in place to verify the identity of a client who calls or communicates with their Company. These validation questions pertain to information which cannot be found in the SOA sent to the unintended recipient. But it may not be easily possible since confirmation for such change and account log-in are required.
>
> Although there is reason to believe that the information may have been acquired by unauthorized individuals, we determine **that the limited personal data affected by the subject breach cannot be used to enable identity fraud** to claim any benefits arising from the insurance contract. **Also, when the unintended recipient immediately reported the mixed-up to Manulife, the recipient's action negated any risk which may arise from the incident caused by a system patch.** Thus, the likelihood of giving rise to real risk of serious harm to the affected data subjects is very low, if not, negligible.
>
> Thus, with only two (2) out of three elements for a mandatory breach notification present in this case, it is hereby determined that notification, in this case, is not required.[51]

The CID stated that the incident was addressed, and that Manulife satisfactorily complied with the Order.[52] It concluded that the matter

---

[50] Full Report, 21 October 2020, at 4, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[51] Final Breach Notification Evaluation Report, 09 December 2022, at 6, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[52] *Id.* at 8.

does not fall under mandatory breach notification as provided in NPC Circular 16-03,[53] and as such, Manulife was not required to notify its affected data subject.[54]

Issue

Whether Manulife sufficiently addressed the breach incident and implemented security measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. The incident does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03. Only the first two requisites are present in this case. The third requisite of real risk of serious harm is absent because of prior and subsequent security measures implemented by Manulife.

Section 11 of NPC Circular 16-03 provides:

> Section 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
> B. There is reason to believe that the information may have been acquired by an unauthorized person; and
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give

[53] *Id.*
[54] *Id.*

> rise to a real risk of serious harm to any affected data subject.[55]

Following this, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[56]

The first requisite is present. The nature of the information involved may enable identity fraud.

In this case, the information on the VUL SOA is considered "information about the financial or economic situation of the data subject" under Section 11 (A) of NPC Circular 16-03.[57] It contains specific information on LTE's life insurance policy, namely "Account summary (face amount, units bought/sold, premium amount, balances, charges/fees, current value, payments)"[58]

Further, the information on the VUL SOA is considered information "which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits" under Section 11 (A).[59] The VUL SOA includes a Manulife client's name, address, policy number, and name of insured,[60] which are necessary considerations for Manulife's decision to grant insurance claims and release of proceeds, if any.

---

[55] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).
[56] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does Initiated as a Sua Sponte NPC Investigation on Possible Data Privacy Violations Committed in Relation to the Alleged Hack and Breach of the Commission on Elections System or Servers, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-SS-22-001-and-NPC-SS-22- 008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 31 January 2023).
[57] NPC Circ. No. 16-03, § 11 (A).
[58] Full Report, 21 October 2020, at 3, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[59] NPC Circ. No. 16-03, § 11 (A).
[60] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).

Other similar information referred to in the last sentence of Section 11(A) of NPC Circular 16-03 need not necessarily be personal information.[61] For mandatory breach notification, Section 20 (f) of Republic Act No. 10173 or the Data Privacy Act (DPA) only requires that the information may enable identity fraud:

> Section 20. *Security of Personal Information.*
>
> . . .
>
> (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or **other information that may, under the circumstances, be used to enable identity fraud** are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.[62]

Further, Section 11 (A) of NPC Circular 16-03 itself includes the phrase "shall include, but not be limited to," which means the enumeration is not an exclusive list:

> Section 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, **"other information" shall include, but not be limited to:** data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of

---

[61] NPC Circ. No. 16-03, § 11 (A).
[62] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (f) (2012). Emphasis supplied.

> identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.[63]

In other words, "other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits" does not necessarily refer to personal information, so long as the information may enable identity fraud.[64]

In this case, the name of the insured, and policy number are important—if not the most important—details with respect to a life insurance policy. The outdated address on the VUL SOA provides even more specific details that may be used to assume the policy holder's identity.

Given the foregoing, and the fact that VL did not surrender or provide confirmation of the destruction of the VUL SOA, unauthorized acquisition of the information on the VUL SOA may be used to fraudulently assume the identity of the policy holder LTE.

The second requisite is also present. An unauthorized person acquired the information in LTE's VUL SOA.

The Commission held that a loss of control over personal data held in custody is enough for a Personal Information Controller (PIC) to have "reason to believe that the information may have been acquired by an unauthorized person."[65]

In this case, Manulife categorically stated in its Incident Report[66] and Full Breach Report[67] that VL received the VUL SOA. It even stated that VL was advised either to return it or destroy it.[68] Hence, Manulife

---

[63] NPC Circ. No. 16-03, § 11. Emphasis supplied.
[64] *Id.* § 11 (A).
[65] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).
[66] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[67] Full Report, 21 October 2020, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[68] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).

admitted and confirmed that there was loss of control by the PIC and the acquisition of the affected data subjects' personal data by an unauthorized person.

Nonetheless, the third requisite is not present due to the security measures implemented by Manulife.

The Commission takes this opportunity to discuss the determination of the presence of the third requisite of mandatory breach notification. Section 11 (C) of NPC Circular 16-03 provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> . . .
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[69]

For this purpose, the phrase "likely to give rise to a real risk" in Section 11 (C) means that a link exists between the breach and the possible resulting harm to any affected data subject.[70] The risk must be apparent and not the product of mere speculation.[71] "Serious harm" means that the consequences and effects to any affected data subject is significant based on the surrounding circumstances of the breach.[72]

In determining whether the unauthorized acquisition is likely to give rise to real risk of serious harm, a PIC or the Commission may consider several factors, such as: the nature and amount of information involved in the breach, the period of time that has lapsed since the breach, objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.

---

[69] NPC Circ. No. 16-03, § 11.
[70] NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8 (NPC 2023) (unreported).
[71] *Id.*
[72] *Id.*

In this case, the unauthorized acquisition of information was due to the erroneous delivery to VL[73] There is no showing that she deliberately intended to obtain LTE's information, as she reported the misdelivery to her agent, who in turn reported the issue to Manulife.[74] Thus, the objective of the unauthorized acquisition was not for fraudulent purposes.

Nonetheless, the nature and amount of information involved in this matter may enable identity fraud. The name of the policy holder, name of the insured, and policy number are important, if not the most important, details with respect to claims on an insurance policy, and the other information such as address and account summary provides even more specific details. Despite Manulife's request to VL, it did not affirm in any of its submissions that VL actually surrendered or confirmed the destruction of LTE's VUL SOA.

Given the foregoing circumstances, including the possibility of fraudulent actions or claims in relation to LTE's insurance policy, there was a real risk of serious harm to the data subject in this case. Manulife itself admitted this risk when it stated that "the appropriate measures in place to minimize the risk of identity theft or fraud that may arise from the misdelivered VUL SOA."[75]

The security measures implemented by Manulife, however, prevented the occurrence of the risk of serious harm to the affected data subject.

Manulife was able to substantiate its claim of "low likelihood of any adverse impact on the data subject"[76] due to the validation measures that it had in place. Manulife stated that "for major transactions involving a client's policy (such as change of address or beneficiary, surrender of policy, policy loans), specific forms have to be filled out and signed."[77] Thus, any person intending to conduct a transaction as

---

[73] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[74] *Id.*
[75] Full Report, 21 October 2020, at 3, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[76] *Id.* at 2.
[77] *Id.*

to an insurance policy must also submit valid identification documents, in addition to the validation questions, to Manulife.[78]

Manulife also reported continuously monitoring the generation of VUL SOAs.[79] As of 21 October 2020, when Manulife filed its Full Breach Report, it stated that it had continuously monitored LTE's policy for possible suspicious transactions, and that "there has been no red flag for any account takeover or fraud on the data subject's account."[80]

Manulife also flagged the erroneous tagging that similarly affected a total of one hundred (100) printed VUL SOAs.[81] It was able to stop its courier from sending eighty-nine (89) VUL SOAs, and to monitor and resolve the delivery of the remaining eleven (11).[82] In fact, Manulife explained in its Full Report that:

> Out of the 11 delivered VUL SOAs:
> - 8 were actually received by the correct clients;
> - 1 had the correct address;
> - 1 was sent to the client's office address where he was still connected at that time;
> - 1 pertained to a client who was outside of the Philippines. This client was contacted by a Manulife agent and did not pose any complaint or issue regarding his non-receipt of the SOA.[83]

Manulife also reported halting the generation of VUL SOAs altogether while its IS Team implemented fixes for the issue of erroneous tagging of addresses.[84]

To reiterate, the security measures implemented by Manulife—the requirement of answering validation questions and submitting identification documents for any changes or major transactions on a client's insurance policy, halting the generation and delivery of VUL

---

[78] *Id.*
[79] *Id.* at 3.
[80] *Id.*
[81] Full Report, 21 October 2020, at 2, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[82] *Id.* at 1-2.
[83] Full Report, 21 October 2020, at 2, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[84] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).

SOAs until the client address tagging issue was fixed, and constant monitoring until 21 October 2020—were sufficient to protect LTE from fraudulent transactions resulting from the disclosure of her information. This removed the real risk of serious harm to the affected data subject.

Given the foregoing, the Commission finds that Manulife was able to address the breach and implement security measures to prevent real risk of serious harm from occurring. As such, the matter does not fall under mandatory breach notification.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-213 In re: Manufacturers Life Insurance Co. is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines. 29 June 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

JJN
Assistant Vice President,
Head of Risk
Management & Data
Protection Officer
Manufacturers Life Insurance Co.

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: METRO PACIFIC TOLLWAYS CORPORATION **NPC BN 23-015**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is the notification dated 27 January 2023 submitted by Metro Pacific Tollways Corporation (MPTC) involving a possible data breach in its MPT DriveHub application.

Facts

On 27 January 2023, MPTC notified the National Privacy Commission (NPC) of a possible data breach through the Data Breach Notification Management System (DBNMS).[1]

In its report, MPTC narrated that on 26 January 2023, it discovered suspicious user activity in its MPT DriveHub application caused by an individual who created several accounts or via multiple referrals.[2] MPTC surmised that several accounts were created in an attempt to earn more points or raffle entries to win prizes in MPTC's "Download, Drive, & Win" promotion, which ran from 11 November 2022 to 31 January 2023.[3]

In its investigation, MPTC confirmed that the multiple duplicate registrations used the same email address and mobile number to register.[4] MPTC believed that this indicated a potential breach of the

---

[1] Initial Notification through the Personal Data Breach Notification Form, 27 January 2023, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[2] *Id.*
[3] *Id.*
[4] *Id.*

MPT DriveHub application system with possible access to others' personal information such as name, username, and email address.[5] MPTC also stated that the number of data subjects affected is one hundred (100) but that the actual number is still to be determined.[6]

MPTC requested for postponement to notify its affected data subjects.[7] It requested a reasonable period to notify its data subjects from the completion of the investigation in case its investigation determined that there was an actual breach.[8] It also argued that no notice to the data subjects is required at that point because its preliminary investigation indicated that there was no intrusion or access to personal information in its system.[9]

On 06 February 2023, the Commission directed MPTC to submit proof to substantiate its request for postponement.[10]

On 09 February 2023, MPTC submitted its Compliance with the directive.[11] MPTC requested the Commission to "instead grant an exemption to notify the affected data subjects."[12] It claimed that upon further investigation, there is "no evidence of personal information and sensitive personal information breach affecting data subjects."[13]

MPTC suggested that the incident may have been done using a method called "Replay Attack", which permits the instant creation of several users.[14] MPTC defined Replay Attack as "an attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access."[15]

---

[5] *Id.*
[6] *Id.*
[7] Initial Notification through the Personal Data Breach Notification Form, 27 January 2023, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[8] *Id.*
[9] *Id.*
[10] Minute Resolution, 06 February 2023, at 1, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[11] Compliance by Metro Pacific Tollways Corporation, 09 February 2023, at 1, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[12] *Id.*
[13] *Id.*
[14] *Id.* at 2.
[15] *Id.*

MPTC, however, maintained that the "attack was targeted more on inputting invalid raffle entries in an attempt to win, rather than on accessing personal data found in the MPT DriveHub databases."[16]

MPTC asserted that its investigation indicated "no queries, data extraction, nor malicious activities performed on the MPT DriveHub databases."[17] Thus, it concluded that there were no leaked or extracted personal data.[18]

The Commission noticed a disparity between MPTC's statements in its initial report and in its compliance with the directive dated 06 February 2023.[19] Thus, it issued an Order dated 16 March 2023 directing MPTC to explain the disparity and submit additional information:

> **WHEREFORE,** premises considered, the Commission **ORDERS** Metro Pacific Tollways Corporation (MPTC) within ten (10) days from receipt of this Order to:
>
> 1. **SUBMIT** additional details on the number of data subjects and personal and sensitive personal information involved in the incident, if any; and
>
> 2. **EXPLAIN** the disparity between the number of data subjects and the involved personal and sensitive personal information stated in the initial report submitted through the DBNMS dated 27 January 2023 with the Compliance dated 09 February 2023.
>
> **SO ORDERED.**[20]

On 27 July 2023, MPTC submitted its Reply to the Order.[21] MPTC
reiterated that "following an investigation on the matter, it found that

---

[16] *Id.*
[17] Compliance by Metro Pacific Tollways Corporation, 09 February 2023, at 2, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[18] *Id.*
[19] Order, 16 March 2023, at 6, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023)
[20] *Id.*
[21] Reply by Metro Pacific Tollways Corporation, 27 July 2023, at 1, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).

there was no data breach involving data subject and/or their
personal information."[22]

MPTC explained that "at the time of the submission of its initial report through the [DBNMS], it was not yet determinable whether there was a reportable breach. However, out of an abundance of caution, [MPTC] thought it prudent to submit the initial report nonetheless."[23]

MPTC concluded that there was no reportable personal data breach, but rather a security incident.[24]

Issue

Whether the incident subject of MPTC's notification dated 27 January 2023 is a personal data breach requiring mandatory notification to the affected data subjects.

Discussion

The Commission resolves to close the matter. The incident subject of MPTC's notification dated 27 January 2023 is a security incident and not a personal data breach. As such, is not subject to mandatory breach notification under NPC Circular 16-03 (Personal Data Breach Management).

There is a distinction between a security incident and a personal data breach.[25] Section 3 of NPC Circular 16-03 defines "Personal Data Breach" and "Security Incident" as follows:

> Section 3. *Definition of Terms.* For the purpose of this Circular, the following terms are defined, as follows:

---

[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] In re: University of the Philippines – Visayas, NPC BN 18-045, 10 November 2022, at 4, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-BN-18-045-2022.11.10-In-re- University-of-the-Philippines-Visayas-Resolution-Final.pdf (last accessed 29 August 2023).

. . .

F. "Personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:

1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
2. Integrity breach resulting from alteration of personal data; and/or
3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.

. . .

J. "Security incident" is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place[26]

MPTC reported that an individual was able to create several accounts in its MPT DriveHub application using the same email address and mobile number.[27]

MPTC reported the incident to the NPC because of its initial belief that this indicated a potential breach of the application system with possible access to others' personal information.[28]

MPTC, however, later explained that the submission of the initial report was out of caution and prudence despite at that time, it was not yet determined whether there was a reportable breach.[29]

---

[26] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 3 (F) & (J) (15 December 2016).
[27] Initial Notification through the Personal Data Breach Notification Form, 27 January 2023, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[28] *Id.*
[29] Reply by Metro Pacific Tollways Corporation, 27 July 2023, at 1, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).

MPTC claimed that its further investigation showed "no evidence of personal information and sensitive personal information breach affecting data subjects."[30] It suggested that the incident was "targeted more on inputting invalid raffle entries in an attempt to win, rather than on accessing personal data found in the MPT DriveHub databases."[31]

The accuracy of MPTC's proposition regarding the reason for the creation of multiple accounts is inconsequential in this case. Nevertheless, what is clear and determinable from MPTC's reports is that the incident only involved the creation of multiple accounts.

Based on the evidence on record, the creation of multiple accounts did not lead to an unauthorized access of the MPT DriveHub databases nor an acquisition by an unauthorized person of any personal information from the databases. MPTC's investigation indicated no evidence of leaked or extracted personal and sensitive personal information.[32] It also did not find any malicious activities performed in its MPT DriveHub databases.[33]

Therefore, the incident is considered a security incident since there is no personal data that was compromised. The incident did not indicate any breach in MPTC's DriveHub databases that led to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data stored or processed in the databases.

WHEREFORE, premises considered, the Commission **NOTES** the submissions of Metro Pacific Tollways Corporation (MPTC) and resolves that the matter of NPC BN 23-015 In re: Metro Pacific Tollways Corporation is **CLOSED**.

SO ORDERED.

---

[30] Compliance by Metro Pacific Tollways Corporation, 09 February 2023, at 1, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[31] *Id.* at 2.
[32] *Id.* at 2-4.
[33] *Id.* at 2.

City of Pasay, Philippines.
17 August 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

ATTY. CSM
Data Privacy Officer
Metro Pacific Tollways Corporation

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: POLYTECHNIC UNIVERSITY OF THE PHILIPPINES **NPC BN 18-222**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is the Compliance dated 19 January 2023 submitted by Polytechnic University of the Philippines (PUP) following the Commission's directives to individually notify its affected data subjects and submit proof of notification.[1]

Facts

To recall, on 22 November 2018, PUP sent a letter to the National Privacy Commission (NPC) formally notifying the latter of an incident concerning possible information security breach.[2]

PUP alleged that on 20 November 2018, it came across a post on ZeroSecurity PH's Facebook page.[3] The post claimed that it was able to obtain three thousand eight hundred nine (3,809) email addresses from the PUP Website.[4]

On 20 May 2022, the NPC, through its Complaints and Investigation Division (CID), issued an Order requiring PUP to submit a Post-Breach Report detailing the incident that prompted the notification of the

---

[1] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[2] Notification Letter to the Commission, 22 November 2018, at 1, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2018).
[3] *Id.*
[4] *Id.*

incident.[5] In compliance, PUP submitted its Post-Breach Report on 07 June 2022.[6]

In its Post-Breach Report, PUP reported that it cross-referenced all three thousand eight hundred nine (3,809) emails with its PUP Student Information System (SIS).[7] It determined, however, that only nine hundred ninety-one (991) email addresses matched with the SIS.[8] PUP confirmed that all the nine hundred ninety-one (991) matched email addresses "belong to student[s] who have already graduated or have dropped out from the University."[9]

PUP also claimed that the investigation on system logs revealed that "there was no direct access to the system database and that the records were compiled from different sources and not from the [SIS]".[10] PUP explained that "no hacking was done but mere exploitation of an old list (physical copy) of email addresses of students and some faculty members."[11]

Further, PUP maintained that it notified all the affected data subjects through a prompt in the SIS to change their passwords and "take other important measures to ensure that their account is secured."[12]

On 10 November 2022, the Commission issued an Order where it held PUP's notification "inadequate because it lack[ed] the contents required in an appropriate notification to the affected data subjects."[13] Thus, the Commission directed PUP to individually notify its affected data subjects:

> **WHEREFORE**, premises considered, Polytechnic University of the Philippines is hereby **ORDERED** to comply with the following **within fifteen (15) days** from the receipt of this Order:

---

[5] Order, 20 May 2022, at 1, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[6] Post-Breach Report, 07 June 2022, at 1, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[7] *Id.* at 2.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] Post-Breach Report, 07 June 2022, at 3, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[13] Order, 10 November 2022, at 5, *in* In re: Polytechnic University of the Philippines, NPC BN 18- 222 (NPC 2022).

1. **NOTIFY** its affected data subjects and **SUBMIT** proof that it individually and directly informed its affected data subjects; and
2. **SUBMIT** proof of the security measures it implemented.

SO ORDERED.[14]

In compliance with the Order, on 19 January 2023, PUP submitted a list of the names of the nine hundred ninety-one (991) affected data subjects with their corresponding email addresses.[15] It also submitted the generated email delivery receipts which showed a copy of the notification sent, its date of sending, and the recipient email addresses.[16]

PUP also enumerated the information security solutions it implemented and attached screenshots of the dashboard of each security solution.[17] These include:

1. Next Generation Firewall Using Checkpoint – this can detect and block sophisticated attacks by enforcing security policies at the application, ports, and protocol levels;[18]
2. Vulnerability Assessment Tools Using Teneble.IO Solution – this is a tool designed to automatically scan for new and existing threats that can target an application;[19]
3. Network Monitoring & Performance Management Tools Using Solarwinds Solutions – these tools gather and analyze network data to provide network administrators with information related to the status of network appliances, network traffic or the sources of network problems and traffic anomalies;[20]
4. Network Access Control Using Forescout Solutions – this enables PUP to restrict unauthorized or non-compliant devices and users from accessing the corporate network and helps

---

[14] Order, 10 November 2022, at 6, *in* In re: Polytechnic University of the Philippines, NPC BN 18- 222 (NPC 2022).
[15] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*

ensure that all devices connected to PUP network are compliant with its security policies; and[21]

5. Patch Management Tools using ZENWorks Solutions – this gives the administrator control over operating system, platform, or application updates. This is often necessary to correct errors, bugs, or vulnerabilities in the software.[22]

Issue

Whether PUP notified its data subjects and sufficiently addressed the breach and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. PUP individually notified its affected data subjects, submitted sufficient proof of notification, and implemented security measures to prevent the recurrence of the breach. PUP sufficiently complied with the Commission's Order dated 10 November 2022.

It is the obligation of a Personal Information Controller (PIC), such as PUP, to ensure that it promptly notifies its affected data subjects of the breach.[23] Section 18 (D) of NPC Circular 16-03 (Personal Data Breach Management) states:

> Section 18. *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> D. *Form*. **Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic.** The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.[24]

---

[21] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[22] *Id.*
[23] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).
[24] *Id.* § 18 (D). Emphasis supplied.

Section 18 (C) of the NPC Circular 16-03 also provides the information required to be provided to data subjects:

> Section 18. *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> C. *Content of Notification.* The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;
> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
> 6. any assistance to be provided to the affected data subjects.[25]

In this case, PUP individually notified its affected data subjects of the breach through electronic mail.[26]

In compliance with the directive to submit proof that it individually notified its affected data subjects, PUP submitted screenshots of the electronic mails it sent to the individual email addresses of nine hundred ninety-one (991) affected data subjects.[27] Due to the large number of the recipients, PUP sent the notification in four (4) batches.[28] The first, second, and third batches each resulted in the notification of two hundred and fifty (250) affected data subjects, while the fourth batch resulted in the notification of two hundred and forty-one (241) affected data subjects.[29]

---

[25] *Id.* § 18 (C).
[26] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[27] *Id.*
[28] *Id.*
[29] *Id.*

PUP also submitted to the Commission a copy of the individual notification it sent to the affected data subjects.[30]

The notification sent by PUP sufficiently informs the affected data subjects of the nature of the breach and the personal data possibly involved in the breach:

> The 991 email addresses that matched with the email addresses published by the 'hackers' are old records. The email addresses belong to students who already graduated or have dropped out from the University. Further investigation conducted by ICTO on system logs reveals that there was no direct access to the system database and that the records were compiled from different source/s and not from the Students Information System as claimed by the 'hackers. Technically, no hacking was done but mere exploitation of an old list (physical copy) of email addresses of students and some faculty members.[31]

Further, the notification enumerated the measures PUP took to address the breach and to reduce the harm or negative consequences of the breach.[32] It enumerated PUP's actions, such as cross-checking the email addresses listed in the Facebook post with the SIS database; placing prompt in its SIS informing students to change passwords and secure account; conducted an audit of the System Log; checking the SIS' vulnerabilities; and securing and improving the security measures in the program.[33] It also contained the contact information of PUP's Data Protection Officer in case the affected data subjects should require further assistance.[34]

As part of a PIC's data breach management, it should implement policies and procedures for managing security incidents, including data breaches, following Section 4 of NPC Circular 16-03.[35] This includes ensuring implementation of organizational, physical, and technical security measures and data privacy policies intended to prevent or minimize the occurrence of a data breach and assure the timely discovery of a security incident:

---

[30] *Id.*
[31] *Id.*
[32] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[33] *Id.*
[34] *Id.*
[35] NPC Circ. No. 16-03, § 4.

> Section 4. *Security Incident Management Policy*. A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:
>
> . . .
>
> B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident[.][36]

PUP demonstrated that it implemented security measures to prevent or minimize the occurrence of a data breach. As verified by the CID of the National Privacy Commission:

> PUP redeveloped its web security and improved technical security measures particularly the Student Information System.
>
> . . .
>
> The security measures implemented after the incident enabled PUP to strengthen its organizational and technical measures to protect the personal data against any accidental or unlawful destruction, alteration, and disclosure.[37]

In addition, PUP submitted further proof of the information security solutions and measures that it implemented.[38] It explained the various software it installed for the security of its systems in relation to the incident that transpired on 20 November 2018.[39] PUP presented screenshots of the dashboards showing that each software is active and running in its systems.[40] Given PUP's submissions, the Commission finds that the measures undertaken by PUP have sufficiently addressed the breach and prevent a recurrence of the incident.

---

[36] *Id.* § 4 (B).
[37] Final Breach Notification Evaluation Report, 14 October 2022, at 8, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[38] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[39] *Id.*
[40] *Id.*

WHEREFORE, premises considered, the Commission resolves that the matter of NPC BN 18-222 In re: Polytechnic University of the Philippines is **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
03 February 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

MANUEL M. MUHI
President
Polytechnic University of the Philippines

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: SMART COMMUNICATIONS, INC. **NPC BN 18-142**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is a confidentiality breach concerning the disclosure of the names and e-mail addresses of tourists who registered for a free LTE Subscriber Identity Module (SIM) card from SMART Communications, Inc. (SMART).

Facts

On 29 July 2018, SMART received an email from JS, a tourist visiting the Philippines.[1] He informed SMART that its registration platform (Google Forms) where tourists register for a free LTE Tourist SIM contained an option to view the *"summary of previous responses."*[2] According to JS, through this option, registrants may view the earlier responses that indicate the names and e-mail addresses of SMART's prospective customers.[3]

SMART claimed that it immediately disabled and took down the functionality to view a summary of previous responses from the registration portal.[4] SMART also reported that its initial investigation showed that "no data exfiltration happened," and that "access to data may have been possible only by viewing the list on the screen."[5]

---

[1] Data Breach Notification – SMART LTE Tourist SIM Registration Matter, 01 August 2018, at 1, *in*
In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2018).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*

On 01 August 2018, SMART notified the National Privacy Commission (NPC) of the incident containing a narration of the remedial actions it took.[6]

On 24 April 2020, the NPC, through its Complaints and Investigation Division (CID), requested SMART to submit an updated breach notification report that includes the results of the investigation SMART conducted.[7]

On 15 November 2021, the CID, ordered SMART to submit a full report detailing the incident.[8]

On 03 December 2021, SMART submitted its Compliance in relation to the incident.[9]

According to SMART, it took the following measures to address the breach:

> 1. The settings of the Google Forms were reviewed and it was determined that the data breach could be resolved by removing the "see previous responses" option.
>
> . . .
>
> 2. The Company also conducted an inventory of other campaigns using Google forms to check that settings do not allow viewing of previous responses.
> 3. A refresher course on data privacy was conducted among members of the Marketing Operations team.
> 4. Disciplinary proceedings were also initiated for employees responsible for the error in the Google Forms settings.
> 5. As a long term remediation, Smart no longer uses Google Forms for campaigns requiring data submission (such as registration or surveys) from participants/customers. The Company uses Office 365 and requires previous clearance from our Cyber Security Operations Group.[10]

---

[6] *Id.*
[7] Order, 24 April 2020, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2020).
[8] Order, 15 November 2021, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[9] Compliance to Order dated 15 November 2021, 01 December 2021, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[10] *Id.*

SMART also reported that the incident concerned a total number of "three thousand tree hundred thirty-five (3535) [sic] affected data subjects, broken down as follows: (a) 3123 responses for the English Google Forms, (b) 153 responses for the Japanese Google Forms, (c) 100 responses for the Korean Google Forms, and (d) 69 responses for the Chinese Google Forms."[11] SMART revealed that it also addressed the settings for the Google Forms in other languages including Korean, Chinese, and Japanese.[12]

On 23 December 2021, the CID ordered SMART to submit a Post- Breach Report containing the proper documentation on the actions SMART has taken.[13]

On 11 January 2022, SMART submitted its Post-Breach Report in compliance with the directive dated 23 December 2021.[14] It attached proofs on the following: (1) how the data exposed were presented to those who will click the "*view summary of previous responses*" functionality, (2) that the information exposed were only names and email addresses, and (3) that no sensitive personal information was disclosed during the incident, (4) that SMART already uses Office 365 instead of Google forms in collecting data from customers requiring data submission and that the clearance from its Cyber Security Operations Group is required prior to collection.[15]

On 26 October 2022, the Commission ordered SMART to submit the Full Breach Report.[16]

On 11 November 2022, SMART submitted its compliance to the 26 October 2022 Order reiterating its own submissions in response to the previous Orders. [17]

---

[11] *Id.* Annex A.
[12] *Id.*
[13] Order, 23 December 2021, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[14] Compliance to Order dated 23 December 2021, 11 January 2022, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2022).
[15] *Id.* Annex A-D.
[16] Order (To Submit Full-Breach Report), 26 October 2022, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2022).
[17] Compliance, 11 November 2022, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2022).

Based on the CID's assessment dated 18 January 2023, the security measures adopted by SMART upon knowledge of the incident are sufficient to address the same and prevent or mitigate its recurrence.[18]

Issue

Whether SMART conducted proper breach management, including the implementation of reasonable and appropriate security measures.

Discussion

The Commission finds that SMART conducted proper breach management and implemented reasonable and appropriate security measures upon knowledge of the incident. Thus, the Commission resolves to close the case.

Section 20 (a) and (b) of the Data Privacy Act of 2012 (DPA) mandates a Personal Information Controller (PIC) to implement reasonable organizational, physical, and technical measures intended for the protection of personal information:

> Section. 20. *Security of Personal Information.* (a) **The personal information controller must implement reasonable and appropriate organizational, physical and technical measures** intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.
>
> (b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.[19]

---

[18] Final Breach Notification Evaluation Report, 18 January 2023, at 7, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2023).
[19] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (a) and (b) (2012). Emphasis supplied.

Further, SMART enumerated in its submissions the measures it took to address the breach following Section 17 (D) (3) of NPC Circular 16- 03 (Personal Data Breach Management):

> Section 17. *Notification of the Commission*. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification*. The notification shall include, but not be limited to:
>
> 3. Measures Taken to Address the Breach
>
> a. description of the measures taken or proposed to be taken to address the breach;
>
> b. actions being taken to secure or recover the personal data that were compromised;
>
> c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
>
> d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
>
> e. the measures being taken to prevent a recurrence of the incident.[20]

As an immediate response, it disabled the option in the Google Forms to prevent a recurrence of the same incident.[21] Additionally, SMART informed that it corrected the settings for Google Forms for the other languages.[22]

To immediately address possible concerns on the unintended disclosure, SMART also established an *ad hoc* team to monitor complaints from registered users that could have resulted from this incident.[23]

---

[20] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §17 (D) (3) (15 December 2016).
[21] Data Breach Notification – SMART LTE Tourist SIM Registration Matter, 01 August 2018, at 1, *in*
In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2018).
[22] Compliance to Order dated 15 November 2021, 01 December 2021, Annex A (Full Report), *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[23] Data Breach Notification – SMART LTE Tourist SIM Registration Matter, 01 August 2018, at 1, *in*
In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2018).

According to SMART, it reviewed its campaigns that also used Google Forms to determine if its registration settings would still allow previous responses to be viewed by other users.[24]

As an organizational measure, SMART conducted a data privacy refresher course among the members of its Marketing Operations Team.[25] Similarly, SMART conducted annual data privacy e-learning courses for its employees.[26]

SMART also initiated disciplinary proceedings for the employees responsible for the error in setting up the Google Form that led to the incident.[27] SMART reported in its Post-Breach Report that the erring employee is no longer with SMART.[28]

As a technical measure, SMART conveyed that it transitioned from Google Forms to Office 365 for their future campaigns requiring data submission from participants or customers.[29] It averred that the latter platform requires previous clearance from its Cyber Security Operations Group prior to collection of data.[30] As proof of such, SMART attached an excerpt of its manual entitled "Company's Work Tools Security Standards" and "Company's Information Security Compliance Management Standards."[31] The manual specifically prohibited the use of public cloud-based services such as Google Drive and implemented the rule that all confidential information should be saved in the company-provided cloud storage.[32]

SMART also reported that its Marketing Team also implemented tracking and analytics on the website to enable tracking of views and

---

[24] Compliance to Order dated 15 November 2021, 1 December 2021, Annex A (Full Report), *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Compliance to the Order dated 23 December 2021, 11 January 2022, at 2, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[29] Compliance to Order dated 15 November 2021, 1 December 2021, Annex A (Full Report), *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[30] *Id.*
[31] *Id.*
[32] *Id.*

downloads.[33] According to SMART, this will enable detection from the logs of views and downloads of information posted on their website.[34]

Based on the foregoing, the Commission finds that SMART as a PIC took sufficient steps to address the incident and mitigate any negative effects, if any. SMART implemented reasonable and appropriate organizational and technical measures to protect the personal data of its data subjects.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-142 In re: SMART Communications, Inc. is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines. 30 March 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

---

[33] *Id.*
[34] *Id.*

Copy furnished:

LBJ
Chief Data Privacy Officer
Smart Communications, Inc.

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: DYNA DRUG CORPORATION **NPC BN 18-120**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is Dyna Drug Corporation's (DDC) Compliance dated 04 May 2022 following the Commission's directive to submit a Post Breach Report and proof of notification to its affected data subjects.

Facts

DDC's Quality Management Department (QMD) used a subscription- based site Typeform to collect customer survey data from March to June 2017.[1]

On 03 July 2018, DDC sent an email to the National Privacy Commission (NPC) informing the latter that its online 2017 customer survey data held by Typeform was breached on 03 May 2018.[2]

DDC forwarded to the NPC an email dated 29 June 2018 from Typeform.[3] The email stated that Typeform's engineering team discovered on 27 June 2018 that an unknown third-party gained access to its server and downloaded certain information including some of the data which DDC's respondents provided through Typeform.[4]

---

[1] Breach Incident Report, 04 July 2018, at 2, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2018).

[2] Email *from* Dyna Drug Corporation *to* NPC Reports, National Privacy Commission (03 July 2018).

[3] *Id.*

[4] Email *from* Typeform *to* Dyna Drug Corporation (29 June 2018).

On 04 July 2018, DDC submitted to the NPC its Breach Incident Report containing a detailed report of the incident.[5] DDC reported that there were ninety-two (92) affected data subjects.[6] Further, the personal data involved are their full names, office address, email addresses, office telephone numbers, and mobile numbers.[7]

DDC also stated the measures it took to address the breach and prevent its recurrence.[8] It claimed that it already deleted the 2017 survey form that was the subject of the breach.[9] It added that it will not renew its subscription with Typeform and will use a different online survey host for its 2018 survey.[10] It further informed the Commission that its Communications Officer will coordinate with its Information Technology team (IT) to ensure the security of the host site and its internal Internet Protocol (IP) address in the event attackers try to breach.[11]

Further, DDC showed that it already notified its affected data subjects. by submitting a screenshot of the email it sent to the affected data subjects on 04 July 2018.[12] It informed the affected data subjects that their information was exfiltrated by an unauthorized third party through a breach in Typeform's system:

> Dear Valued Customer,
>
> You are receiving this e-mail because you were one of our respondents to our 2017 Customer Survey. This was accessed on[]line via Typeform.
>
> We just received a message that Typeform had a data breach, which affected one (or more) of the typeforms we sent out. Typeform report[ed] that an external attacker managed to get unauthorized access to respondent data and downloaded it.

---

[5] Email *from* Dyna Drug Corporation *to* NPC Reports, National Privacy Commission (04 July 2018).
[6] Breach Incident Report, 04 July 2018, at 1, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2018).
[7] *Id.*
[8] *Id.* at 2.
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] Breach Incident Report, 04 July 2018, Annex B, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2018).

> Typeform responded immediately and fixed the source of the breach to prevent any further intrusion.
>
> If your name and email was downloaded by the attackers, then we recommend that you watch out for potential phishing scams, or spam emails. Please be careful in opening links sent by advertisements or senders you do not know.
>
> As Dyna Drug's course of action, we have deleted your information from our account in Typeform.
>
> If you have any other questions, feel free to contact us by replying to this email or thru telephone number[.][13]

On 18 April 2022, the Commission, through its Complaints and Investigation Division (CID), issued an Order directing DDC to submit a Post Breach Report detailing the incident:

> Pursuant to Section 9, Rule IV of the National Privacy Commission Circular No. 16-03 on Personal Data Breach Management, you are hereby required to submit a Post Breach Report detailing the incident that prompted the notification to the Commission:
>
> 1. DDC's investigation report;
> 2. Certification that the survey form has been deleted;
> 3. What were the security enhancement implemented by DDC and proof thereof;
> 4. Policy on third-party Online Survey Host;
> 5. Results of coordinating with IT on ensuring the security of the host site and review on the internal IP address to check its vulnerability from a direct attack on its internal systems and processes concerning personal data privacy;
> 6. How many of the 92 data subjects affected were notified and provide proof of notification;
> 7. Proof of other security measures implemented to address the breach and prevent its recurrence;
> 8. Updated Privacy Policy of DDC; and
> 9. Certification from DDC that data subjects have been appropriately notified.

---

[13] *Id.*

DYNA DRUG CORPORATION is hereby given a period of fifteen (15) days from receipt hereof to submit its compliance through email at complaints@privacy.gov.ph.

SO ORDERED.[14]

On 04 May 2022, DDC submitted its Compliance with the Order.[15]

DDC re-submitted the Breach Incident Report it submitted on 04 July 2018 which contained DDC's investigation report on the incident.

DDC also submitted a Certification signed by its Data Protection Officer (DPO) and its Managing Director, which stated that DDC's former Communications Officer already deleted the 2017 survey form on 03 July 2018.[16] DDC also presented an email from Typeform dated 27 April 2022 wherein Typeform confirmed the deletion of DDC's survey form in the Typeform platform.[17]

On the matter of DDC's security enhancement measures, it admitted that it had not implemented any policy related to the Data Privacy Act (DPA) in 2018.[18] In 2019, it further admitted that there was still no policy implemented on "Third-party Online Survey Host[s]".[19] Nevertheless, DDC claimed that after the incident, it changed and revised its customer survey forms by removing the collection of personal identifiable information of the data subjects.[20]

Further, it submitted a copy of its Customer Satisfaction Survey Procedures and Computer Software and Hardware Maintenance Policy, which became effective on 21 September 2021[21] and 17 January 2022,[22] respectively.

---

[14] Order, 18 April 2022, at 1, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[15] Compliance, 04 May 2022, at 1, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[16] Certificate of Survey Form Deletion, 02 May 2022, at 1, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[17] Post Breach Report, 04 May 2022, at 3, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] Customer Satisfaction Survey Procedures, 21 September 2021, at 1, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[22] Computer Software and Hardware Maintenance Policy, 17 January 2022, at 1, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).

DDC also submitted its Data Privacy Manual which became effective on 06 April 2022.[23] DDC pointed out that its policies regarding third- party online survey host is found in Section 12 of its Data Privacy Manual[24] that sets out its policies on Outsourcing and Subcontracting Agreements.[25]

With regard to the notification of the affected data subjects, DDC already presented proof of its notification when it attached in its Breach Incident Report a screenshot of the email it sent to the affected data subjects.[26] Nevertheless, DDC acknowledged that the screenshot in the Report only captured a part of the email recipient field which listed up to only thirty (30) affected data subjects.[27] Therefore, DDC submitted a Certification signed by its DPO and Managing Director which stated that DDC successfully delivered the notifications to the ninety-two (92) affected data subjects on 04 July 2018.[28]

Issue

Whether DDC notified its affected data subjects and sufficiently addressed the breach and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. DDC's submissions show that it properly notified its affected data subjects, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

It is the obligation of a Personal Information Controller (PIC), such as DDC, to ensure that it promptly and properly notifies its affected data

---

[23] Data Privacy Manual, 06 April 2022, at 1, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[24] Post Breach Report, 04 May 2022, at 4, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[25] Data Privacy Manual, 06 April 2022, at 14, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[26] Breach Incident Report, 04 July 2018, Annex B, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2018).
[27] *Id.* at 5.
[28] Certification of Notification, 02 May 2022, at 1, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).

subjects of the breach.[29] Further, the Commission has consistently pointed out that the purpose of the required notification to the data subjects of a breach is to allow them to take the necessary precautions or other measures to protect themselves against its possible effects.[30]

In this case, DDC notified its affected data subjects through email.[31] It informed them that a breach occurred in Typeform's system which allowed an unauthorized person to gain access and exfiltrate their data in the system.[32] The notification also specified that the recipient data subject was affected because he or she was a respondent to DDC's 2017 Customer Survey collected through Typeform.[33]

DDC also advised its affected data subjects to watch out for potential phishing scams, spam emails, or any links from unknown senders.[34] This allowed the data subjects to take the necessary precautions to protect themselves against the possible effects of the breach considering that the exfiltrated data included their names and email addresses.[35]

Further, DDC informed the data subjects that it deleted the information from its affected data subjects' accounts in Typeform.[36] DDC provided the data subjects with its contact information in case they have any further concerns regarding the breach.[37]

DDC also presented evidence of the notifications sent through email by attaching a screenshot of the email notification.[38] The screenshot also showed that the email addresses of the recipient data subjects were inputted in the blind carbon copy (BCC) field.[39] This conforms to the requirement under Section 18 (D) of NPC Circular 16-03 (Personal

---

[29] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).
[30] *Id.*
[31] Breach Incident Report, 04 July 2018, Annex B, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2018).
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] Breach Incident Report, 04 July 2018, Annex B, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2018).
[38] *Id.*
[39] *Id.*

Data Breach Management), which provides that notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic.[40]

Although the screenshot presented by DDC captured only a part of the email BCC recipient list,[41] it, nevertheless, submitted a Certification by its DPO to assure the Commission that all ninety-two (92) affected data subjects were notified through email.[42]

DDC sufficiently addressed the breach and adopted measures to prevent its recurrence. DDC claimed that it changed and revised its customer survey forms by removing the collection of personal information of the data subjects.[43]

DDC confirmed that the deletion of the 2017 customer survey form and respondents' information with Typeform.[44] In addition, DDC terminated its subscription with Typeform and decided to use a different host to conduct its online 2018 survey.[45]

On 21 September 2021, DDC introduced a new process for the conduct of its Customer Satisfaction Survey.[46] The process measures customer satisfaction in relation to the company's quality management system at planned intervals.[47] The survey activity is set to be conducted semi- annually.[48] In addition, the process includes a new method for identifying participants for the survey.[49]

---

[40] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).
[41] Breach Incident Report, 04 July 2018, Annex B, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2018).
[42] Certification of Notification, 02 May 2022, at 1, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[43] Post Breach Report, 04 May 2022, at 3, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[44] *Id.*
[45] Breach Incident Report, 04 July 2018, at 2, *in* In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2018).
[46] Customer Satisfaction Survey, 21 September 2021, at 1, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2021).
[47] *Id.*
[48] *Id.*
[49] *Id.* at 2.

DDC also adopted a Computer Software and Hardware Maintenance Policy to maintain the security of its own systems.[50] DDC's computer hardware and software must undergo periodic maintenance to improve the performance of its operating system.[51] All computer hardware must be tagged for identification, and only approved company products must be installed.[52] Employees are required to provide access to all DDC computer systems for scheduled maintenance to enhance operating system performance.[53] During such maintenance activities, unauthorized removal of hardware or software components is strictly prevented to safeguard the computer system.[54]

Further, DDC requires the conduct of diagnosis for new security risks and vulnerabilities,[55] regular scanning for virus detection,[56] and monitoring to detect system issues or disruption within its organization.[57] This allows DDC to update and configure its operation system to mitigate the identified risks and vulnerabilities.[58]

Lastly, DDC also adopted a Data Privacy Manual to ensure the safety and security on processing of all personal data of its data subjects.[59] It provided guidelines for the implementation of organizational security measures,[60] physical security measures,[61] and technical security measures.[62] It also provided for procedures on managing breach and security incidents.[63]

DDC's Data Privacy Manual also contained provisions on outsourcing and subcontracting agreements[64] which may serve as its guideline should it outsource the collection of customer survey responses.

---

[50] Computer Software and Hardware Maintenance Policy, 17 January 2022, at 1, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.* at 2.
[55] *Id.*
[56] Computer Software and Hardware Maintenance Policy, 17 January 2022, at 2, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[57] *Id.* at 3.
[58] *Id.* at 2.
[59] Data Privacy Manual, 06 April 2022, at 1, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[60] *Id.* at 6.
[61] *Id.* at 8.
[62] *Id.* at 10.
[63] *Id.* at 17.
[64] *Id.* at 14.

It provided for the appointment of a Data Protection Officer (DPO) to make the necessary control measures in securing personal information and preserve the rights of the data subjects and to be the advisor of DDC's Managing Director in data protection improvement initiatives.[65]

It also outlined the creation of a Data Breach Response Team responsible for implementing security incident management policies, managing incidents, and ensuring compliance with the DPA.[66]

DDC, through its DPO, also implements preventive measures such as an annual Privacy Impact Assessment and Privacy Audit;[67] backup systems are in place in case of data recovery and restoration;[68] backup systems have their own backups to ensure data restoration in the event of data losses;[69] and security breaches are reported directly to the DPO who assesses the breach and notifies the NPC. [70]

Given the foregoing, the Commission finds that the measures undertaken by DDC has sufficiently addressed the incident and prevents its recurrence.

WHEREFORE, premises considered, the Commission resolves that the matter of NPC BN 18-120 In re: Dyna Drug Corporation is **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
17 August 2023.

---

[65] Data Privacy Manual, 06 April 2022, at 17, in In re: Dyna Drug Corporation, NPC BN 18-120 (NPC 2022).
[66] *Id.* at 17-18.
[67] *Id.* at 18.
[68] *Id.*
[69] *Id.*
[70] *Id.*

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

KTG
Data Protection Officer
Dyna Drug Corporation

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: CEBU AIR, INC. **NPC BN 18-075**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is a breach notification report submitted by Cebu Air, Inc. (Cebu Pacific) in compliance with the Order dated 06 January 2021.

Facts

On 18 May 2018, Cebu Pacific, owner of Cebu Pacific Airlines, received reports from two (2) passengers that they were each presented with the booking information of four (4) other passengers after making their own booking on www.cebupacificair.com.[1]

On 21 May 2018, Cebu Pacific notified the Commission of the breach.[2] According to Cebu Pacific, it believed the incident happened after releasing "the latest version of its Web-based Booking Manager on 18 May 2018" earlier that day.[3] The information involved the following details: Booking Reference Number, Date Booked, Status of Booking, Originating and Destination airports, Date of Departure, and Flight Number, Originating and Destination Airports, Date of Return, Flight Number, Name of the Passengers.[4]

Nonetheless, Cebu Pacific explained:

---

[1] Breach Notification Report – 18 May 2018 Event, 21 May 2018, *in* In re: Cebu Pacific, NPC BN 18- 075 (NPC 2018).
[2] *Id.*
[3] *Id.* at 1.
[4] *Id.*

> No personal information (e.g., passport number, credit card information, passwords, birthday, or email address) was shown immediately other than the name of the guests, the combination of the four elements above was assessed as providing an opportunity for fraudulent changes to existing bookings. However, the combined information can enable a person to modify the booking of those guests associated with the Booking Details.[5]

On 25 May 2018, Cebu Pacific submitted its Full Breach Report.[6] Cebu Pacific reiterated its earlier statement that no other personal information, such as passport number, credit card information, passwords, birthday, or email addresses, was exposed:

> No personal information (e.g., passport number, credit card information, passwords, birthday, or email address) was shown immediately other than the name of the passengers. However, the combination of the four elements above was assessed as providing an opportunity for fraudulent modification of existing bookings associated with the exposed details.[7]

According to Cebu Pacific, its Data Protection Officer (DPO) learned about the incident at 1:00 p.m. of the same date as the breach and immediately reached out to the systems owner, systems support team, and technical support team.[8] The teams verified that the released version of the website contained a bug.[9] The DPO held a conference with the teams to identify extent of the breach and remediation measures.[10]

According to Cebu Pacific, the teams identified "critical factors that should be considered in relation to the confidentiality breach"[11] during the meeting:

> a. Unauthorized disclosure of booking details only happened when an "anonymous guest" created a new booking. 'Anonymous guest' refers to a person who makes a booking

---

[5] *Id.*
[6] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075
(NPC 2018).
[7] *Id.* at 2.
[8] *Id.*
[9] *Id.*
[10] *Id.*

without an existing account in the Corporation's booking management system.

b. Not all anonymous guests who created a new booking were shown the booking details of other passengers.

c. An anonymous guest could not view the same booking information after leaving the booking page. The same held true even if the anonymous guest saved the Uniform Resource Identifier (URI) pertaining to the booking details.[12]

Cebu Pacific determined that while the web booking system was online between 9:15 a.m. and 3:30 p.m., six hundred seventy-four (674) bookings were modified.[13] Cebu Pacific stated "these were the only bookings where possible fraudulent activity could have occurred."[14]

At 3:30 p.m., Cebu Pacific reported that it had also "rolled back the latest version of its web-based Booking Manager, so as to prevent any further exposure."[15]

Cebu Pacific reported that by the time it rolled back the latest version of their website, six hundred seventy-eight (678) bookings were already modified or changed.[16] It reported that it released an email, through its Contact Center, to the contact persons of each of the six hundred seventy-eight (678) bookings that were modified when the website was live, to verify the authenticity of the change in their respective bookings.[17] Cebu Pacific included a template of the email in its Full Breach Report, which had contained a Reference code to validate the recipient of the email.[18] The email states:

Manage Booking Notification
Today at

7:08 Hi

[redacted],

We noticed that there was a change made to your booking on May 18, 2018. This is for your flight with booking reference ABC123.

---

[12] *Id.*
[13] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075
(NPC 2018).
[14] *Id.* at 3.
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.* at 5.

> If this was you, please disregard this email. No further action is needed.
>
> If this wasn't you, please contact us by replying to this email.
>
> Sincerely,
> **Your Cebu Pacific**
> **Team**
>
> . . .
>
> **Note:**
> *"Please do not delete or modify below Reference code to receive your response."*[19]

After the conference with the systems owner, the systems support team, and technical support team on 18 May 2018, Cebu Pacific reported that it resolved to take the following actions:

> 2.3 Long-Term Remediation — the Corporation further proposed the following actions:
>
> 2.3.1 Send confirmatory notification to every changed booking;
> 2.3.2 Require log-on before allowing any change to a booking; and
> 2.3.3 Review the development and production release processes for increased robustness.[20]

On 19 May 2018, Cebu Pacific called a Disruption Management Team (DMT) Conference to investigate its logs.[21] The purpose of the DMT is "to deal with all unusual events like aviation security, hazardous weather, Information Systems issues, and other similar events."[22] Cebu Pacific reported, however, that it could not identify exactly how many records were exposed:

> Despite these efforts. the Corporation could not exactly determine how many records were exposed other than the eight booking details reported by the two passengers. The failure mode identified indicated that there could have been more than eight such records exposed, but given the nature of the information exposed (as detailed in Section I of this Breach Notification Report), the identified fraud risk extended only to

---

[19] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 5, *in* In re: Cebu Pacific, NPC BN 18-075
(NPC 2018).
[20] *Id.* at 3.
[21] *Id.* at 2.
[22] *Id.*

> the 678 bookings, where a change was executed during the existence of the website bug.[23]

Cebu Pacific determined that based on updated information, "there were only 332 booking changes executed by the anonymous guests and that 346 ("Others") booking changes were effects of system updates."[24]

Cebu Pacific reported that it "constantly monitored customer communication channels for the 332 booking changes."[25] As of 24 May 2018, or before its submission of the Full Breach Report, Cebu Pacific claimed it did not receive "any confirmed fraudulent booking modification either through its Contact Center or customer emails."[26]

Cebu Pacific also reported that it also reviewed documentation "relevant to the system development policies and practices in the business and operations areas" during the DMT Conference.[27] Cebu Pacific explained:

> When the Corporation's review of the system development policies and practices concluded, the teams agreed to incorporate two additional preventive controls: (i) Add severity ranking to the release prioritization level to show increased rigor as early as the testing phase before releasing any system update; and (ii) Add another approver with executive authority when promoting code to the production environment.[28]

Cebu Pacific concluded that it would take the following measures to minimize if not eliminate further damage that may arise from the breach:

> 5.1 Notify Contact when a Booking Is Changed
>
> The Corporation will notify the contact of any booking that will be changed. As a detective control, this approach will enable the Corporation to identify when a fraud is made on a booking and execute the appropriate course of action to protect its passengers.

---

[23] *Id.* at 3.
[24] *Id.*
[25] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075
(NPC 2018).
[26] *Id.* at 4.
[27] *Id.*
[28] *Id.*

> 5.2 System Development Policies, Practices, and Processes
>
> The Corporation will implement the controls it identified in its review as described in Section 3.5 of this report.
>
> 5.2.1 Add severity ranking to the release prioritization level. The severity ranking will enable the Corporation to evaluate whether a particular bug can be an acceptable risk when a system update is released
>
> 5.2.2 Add another approver with executive authority. This will enable the Corporation to strengthen the accountability culture in its system development area.[29]

On 07 January 2022, the Commission, through the Complaints and Investigation Division (CID) issued an Order to Cebu Pacific via email, directing to submit a Post Breach Report and supporting documents within fifteen (15) days from receipt:

> This Commission finds the breach notification report lacking details to fully appreciate and determine the compliance of Cebu Pacific with the Data Privacy Act and the issuances of this Commission.
>
> Thus, pursuant to Section 9, Rule IV of the NPC Circular No. 16- 03 on Personal Data Breach Management, you are hereby required to submit a Post Breach Report detailing the incident that prompted the notification to the Commission, **provide documentation/ reports as to determination of the extent and number of data subjects affected, the security measures conducted before, during and after the security incident and remedial measures taken to address the incident and prevent its recurrence.**
>
> You are hereby given a period of fifteen (15) days from receipt hereof to submit your compliance through email at complaints@privacy.gov.ph.
>
> SO ORDERED. Pasay City. 06 January 2021 [sic].[30]

---

[29] *Id.* at 6.
[30] Order, 06 January 2021 [sic], at 1, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).

Cebu Pacific submitted a Post-Data Breach report dated 19 January 2022 to comply with the CID's Order.[31] Cebu Pacific reiterated its findings in its Full Breach Report, and re-attached it as Annex A.[32]

Cebu Pacific explained further that "[a]part from the eight (8) records reported by the two (2) passengers, however, [it] was unable to determine whether other records were similarly exposed due to safety features built into the system meant to enhance data privacy."[33] It reported monitoring its channels until 25 May 2018. It also reported that it engaged a data breach monitoring service "to investigate the dark web"[34] Cebu Pacific stated that it was able to validate "that no [personal information] appeared in the dark web."[35]

The CID recommended to close the matter based on its assessment,[36] because it does not fall within mandatory notification under NPC Circular 16-03 (Personal Data Breach Management):

> In this case, it appears that only the name and other flight details were compromised. Clearly, the personal data affected in this breach incident only involved personal information. Cebu Pacific reiterated that passport numbers, credit card information, passwords, birthdays, or email addresses were not compromised.
> While it may be true that the incident involved an unauthorized disclosure of passenger flight details to another passenger, with the limited information involved, we cannot think that they may be used to enable identity theft or identity fraud or pose a real risk of serious harm to the data subjects.
>
> **At most, Cebu Pacific specified the possible effect of the incident as to providing an opportunity to change the existing booking details. But which may not be easily possible since confirmation for such change and account log-in are required.**
>
> Although there is reason to believe that the information may have been acquired by unauthorized individuals, we determine that the limited personal data affected by the subject breach cannot be used to enable identity fraud and the incident may not

---

[31] Post-Data Breach Report for May 2018 Case, 19 January 2022, *in* In re: Cebu Pacific, NPC BN 18- 075 (NPC 2018).
[32] *Id.* at 6.
[33] *Id.* at 2.
[34] *Id.*
[35] *Id.*
[36] Final Breach Notification Evaluation Report, 13 November 2022, at 9, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2022).

> likely lead to a risk of serious harm and damage to affected data subjects.
>
> Thus, with only one (1) out of three elements for a mandatory breach notification present in this case, it is hereby determined that notification, in this case, is not required.[37]

The CID concluded that the breach posed only minor risks to data subjects, and the Personal Information Controller (PIC) implemented reasonable and appropriate measures to address the incident.[38] According to the CID, there was also no possible violation of the Data Privacy Act (DPA),[39] and as such, notification was not required.[40]

Issue

Whether Cebu Pacific notified its data subjects, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. Cebu Pacific showed that it notified its data subjects and implemented sufficient security measures to address the breach incident, which prevented the real risk of serious harm from materializing.

Contrary to the CID's assessment, however, this matter falls under mandatory breach notification.

Section 11 of NPC Circular 16-03 provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity

---

[37] *Id.* at 8.
[38] *Id.* at 9.
[39] *Id.*
[40] *Id.* at 8.

> fraud. For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> B. There is reason to believe that the information may have been acquired by an unauthorized person; and
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[41]

Following this, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[42]

The first requisite is present in this case. The information involved may enable identity fraud.

Cebu Pacific admitted that the exposed information may be and may have been used to fraudulently modify bookings.[43] It reported that it reached out to the six hundred seventy eight (678) affected passengers to "verify the authenticity of the change in their booking" on the same date as the incident.[44] After investigation, it determined on 21 May 2018 or three (3) days after the breach, three hundred thirty-two (332) booking changes were executed by anonymous guests, while three hundred forty-six (346) others were the effects of system updates.[45]

---

[41] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).
[42] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-SS-22-001-and-NPC-SS-22-008- 2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 22 February 2023).
[43] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075
(NPC 2018).
[44] *Id.* at 3.
[45] *Id.*

Cebu Pacific reiterated that the exposed personal information did not involve "passport numbers, credit card information, passwords, birthdays, or email addresses."[46]

Further, after the breach, Cebu Pacific constantly monitored its customer communication channels for the three hundred thirty-two
(332) anonymous booking changes.[47] Cebu Pacific also reported that it had implemented a log-in requirement for modifications to bookings made within this period.[48]

As of 24 May 2018, Cebu Pacific reported that it had continued to monitor its channels until 25 May 2018[49] and that it did not receive any confirmed fraudulent booking modification.[50]

Nonetheless, the risk that the compromised information will be used for identity fraud is still only lessened, not eliminated, and this was admitted by Cebu Pacific itself.[51] The first requisite is satisfied by the fact that the compromised information enables an unauthorized person to fraudulently modify a passenger's booking as if it were the unauthorized person's own booking.

The second requisite is also present in this case. There was acquisition by an unauthorized person.

The Commission has held that a loss of control over personal data held in custody should be enough for a PIC to have "reason to believe that the information may have been acquired by an unauthorized person."[52]

---

[46] Post-Data Breach Report for May 2018 Case, 19 January 2022, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2022).
[47] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075
(NPC 2018).
[48] Post-Data Breach Report for May 2018 Case, 19 January 2022, at 3, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2022).
[49] *Id.* at 2.
[50] *Id.*
[51] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075
(NPC 2018).
[52] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).

In this case, Cebu Pacific admitted that two (2) passengers reported having seen others' booking details and names.[53] Further, it admitted in its Full Breach Report that it could not ascertain the exact number of exposed records, and that "[t]here is a possibility that thousands of records could have been exposed to other passengers."[54] The mere viewing of such personal information by the two passengers and other unidentified, unauthorized persons should be sufficient to form a reasonable belief for the PIC.[55]

Given the totality of the circumstances, including the possibility of fraudulent changes being made to the booking of data subjects, the third requisite of real risk of serious harm to the data subject was also present in this case. Nevertheless, the security measures implemented by Cebu Pacific prevented the materialization of such risk of serious harm to the affected data subjects.

Cebu Pacific reported rolling back the released version containing a bug.[56] In its Full Breach Report, Cebu Pacific explained that "this will remove the identified vulnerability which caused the personal breach" and "will prevent any other possible exploit that could threaten the Corporation's further exposure."[57] In total, the released version was up for six (6) hours and fifteen (15) minutes before Cebu Pacific shut it down as a preventive measure.

Cebu Pacific also reported that it constantly and continuously monitored the three hundred thirty-eight (338) booking modifications made during the time the web-based Booking Manager was live.[58] The monitoring continued up to 25 May 2018.

---

[53] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 1, *in* In re: Cebu Pacific, NPC BN 18-075
(NPC 2018).
[54] *Id.* at 2.
[55] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).
[56] Post-Data Breach Report for May 2018 Case, 19 January 2022, at 1, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2022).
[57] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075
(NPC 2018).
[58] Post-Data Breach Report for May 2018 Case, 19 January 2022, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2022).

Cebu Pacific also reported implementing a log-in requirement prior to booking modification[59] and sending of email notification to the passenger for validation thereof.[60]

Further, Cebu Pacific reported the addition of preventive controls with respect to releasing system updates.[61] In its Full Breach Report, it explained:

> When the Corporation's review of the system development policies and practices concluded, the teams agreed to incorporate two additional preventive controls: (i) Add severity ranking to the release prioritization level to show increased rigor as early as the testing phase before releasing any system update; and (ii) Add another approver with executive authority when promoting code to the production environment.[62]

Finally, Cebu Pacific also sent emails to its affected data subjects, which gives notice to the recipient that a change was made to their booking on 18 May 2018 (the date of the incident) between 9:15 a.m. and 3:30 p.m.[63] The email states that if there were any unauthorized changes made to the booking, the recipient could contact Cebu Pacific by replying to the same email thread.[64] As such, the email enabled the data subjects to take measures to protect themselves from the consequences of the breach by contacting Cebu Pacific regarding any unauthorized changes.

To reiterate, the first two requisites of mandatory breach notification are present because the nature of the information involved in the breach enables identity fraud and Cebu Pacific admitted there may have been unauthorized acquisition of the information.[65] Nonetheless, the third requisite of real risk of harm to the data subjects did not materialize due to the security measures implemented by Cebu Pacific immediately after the breach. The security measures of the log-in requirement, email notification for validation, email notification to the three hundred thirty-eight (338) passengers whose bookings were affected on 18 May 2018, and constant monitoring until 25 May 2018

---

[59] *Id.*
[60] *Id.* at 3.
[61] *Id.*
[62] *Id.*
[63] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 5, *in* In re: Cebu Pacific, NPC BN 18-075
(NPC 2018).
[64] *Id.*
[65] *Id.* at 1.

enabled the data subjects to take measures to protect themselves if there were any unauthorized modifications to their booking.

Given the foregoing, the Commission finds that Cebu Pacific's Post- Data Breach Report and Full Breach Report show that it was able to sufficiently notify its affected data subject, address the breach, and implement security measures to prevent its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-075 In re: Cebu Pacific is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
22 February 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

RAE
Data Protection Officer
Cebu Air, Inc.

Cebu Pacific Building, Domestic Road
Pasay City 1301, Philippines
cebupacificair.com;
dpo@cebupacificair.com;

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: PHILIPPINE LONG DISTANCE TELEPHONE COMPANY, INC.

NPC BN 18-073

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is Philippine Long Distance Telephone Company, Inc.'s (PLDT) Compliance dated 21 July 2022 following the directives to submit a Post-Breach Report and proof of notification to its affected data subjects.[1]

Facts

On 18 May 2018, PLDT notified the Commission of a breach.[2] It narrated that on 15 May 2018, its employees reported having received emails from PLDT's own Email Dispatch System.[3] PLDT uses its Email Dispatch System to send service communications e-mail to its customers.[4]

The reported emails contained two (2) marketing campaigns entitled
"What is trending in Philippines??" and "Get this birthday card."[5]

PLDT stated that its Cyber Defense Team conducted an initial investigation which showed that the web application portal of its Email Dispatch System has been compromised by exploiting a vulnerability in its bypass authentication.[6] It explained that the

---

[1] Compliance of PLDT to Order dated 01 July 2022, 21 July 2022, at 1, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2022).
[2] Notification Letter to the Commission, 18 May 2018, at 1, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2018).
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*

perpetrator used the existing contact list in the Email Dispatch System to send the unauthorized e-mails containing the marketing campaigns.[7]

PLDT added that its initial assessment suggests that around five hundred eighty-four thousand seven hundred ninety-three (584,793) email addresses of individual data subjects may have been involved in the incident.[8]

PLDT also claimed that it immediately halted the operations of the Email Dispatch System and took down its web application upon its discovery of the breach.[9] PLDT added that access to the system was made limited through the corporate network and was only kept active for purposes of the investigation.[10]

On 01 July 2022, the Commission, through its Complaints and Investigation Division (CID), issued an Order requiring PLDT to submit a Post-Breach Report detailing the incident that prompted the notification to the Commission:[11]

> Thus, pursuant to Section 9, Rule IV of the National Privacy Commission Circular No. 16-03 on Personal Data Breach Management, Philippine Long Distance Telephone Company, Inc., is hereby required to submit a Post Breach Report detailing the incident that prompted the notification to the Commission;
>
> A. Description of the personal data breach, its root cause and circumstances regarding its discovery;
> B. Actions and decisions of the incident response team;
> *- Provide a copy of the forensic investigation report conducted by the PLDT Cyber Defense Team*
> C. Measures conducted to address the incident and prevent its recurrence; and
> D. Compliance with notification requirements and assistance provided to affected data subjects, and proofs thereof, if applicable.

---

[7] *Id.*
[8] Notification Letter to the Commission, 18 May 2018, at 2, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2018).
[9] *Id.*
[10] *Id.*
[11] Order, 01 July 2022, at 1, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2022).

> The **PHILIPPINE LONG DISTANCE TELEPHONE COMPANY, INC.**, is hereby given a period of fifteen (15) days from receipt hereof to submit its compliance through email at complaints@privacy.gov.ph.[12]

PLDT submitted a Post-Breach Report on 21 July 2022.[13] It reiterated the information in its initial report regarding the circumstances surrounding the breach and its discovery.[14]

Further, PLDT maintained that it escalated the incident to its Cyber Security Operations Group (CSOG) for investigation and remediation on the same day it discovered the breach.[15]

PLDT claimed that its investigation revealed that the emails subject of the breach did not contain any malicious malware.[16] It also claimed that no other personal information of PLDT customers was involved in the breach aside from the email addresses in the Email Dispatch System.[17] Further, it maintained that the design of the Email Dispatch System disabled any exfiltration of data outside of the PLDT environment. Thus, PLDT concluded that the email database of the system had not been downloaded nor acquired by the perpetrator of the breach.[18]

In addition, PLDT reported that it has already discontinued the use of the Email Dispatch System after the incident as a measure to address the incident and prevent its recurrence.[19]

Lastly, PLDT maintained that its "Deputy Data Privacy Officer [already] wrote to the affected data subjects to explain to them what happened, what personal information was involved, what PLDT has done to prevent damage from this incident as well as the recurrence of the breach, and what the affected data subjects can do if they

---

[12] Order, 01 July 2022, at 1-2, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2022).
[13] Post-Breach Report, 21 July 2022, at 1, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2022).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.* at 2.
[18] *Id.*
[19] Post-Breach Report, 21 July 2022, at 2, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2022).

received the suspicious email."[20] PLDT attached a copy of the email notification sent to its affected data subjects.[21]

PLDT also prepared an email on "Frequently Asked Questions and Suggested Answers for Spam Email Received Incident"[22] and an advisory on handling guidelines for spam emails received by PLDT Home customers.[23] PLDT attached a copy of the email with a sample image of the unauthorized email and other details of the incident.[24]

Issue

Whether PLDT notified its data subjects and sufficiently addressed the breach and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. PLDT's submissions show that it notified its affected data subjects, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

It is the obligation of a Personal Information Controller (PIC), such as PLDT, to notify its affected data subjects of a breach.[25] Section 18 (C) of NPC Circular 16-03 (Personal Data Breach Management) provides the information required in notifying the affected data subjects:

> Section 18. *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> C. *Content of Notification*. The notification shall include, but not be limited to:
> 1. nature of the breach;

---

[20] *Id.*
[21] *Id.* Annex B.
[22] *Id.* at 2.
[23] *Id.*
[24] *Id.* Annex A.
[25] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).

2. personal data possibly involved;
3. measures taken to address the breach;
4. measures taken to reduce the harm or negative consequences of the breach;
5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. any assistance to be provided to the affected data subjects.[26]

In this case, a copy of the notification sent by PLDT to its affected data subjects shows that it complied with the required contents for the notification under Section 18 (C) of NPC Circular 16-03.[27]

In its email notification, PLDT informed the data subjects of the incident involving the data subjects' registered email addresses.[28] PLDT narrated that an external user, who is not in any way authorized by PLDT, sent the emails using the email admin@pldthome.com to the registered email address of its customers.[29]

PLDT further assured the data subjects that "there has been no unauthorized downloading or access to [their] personal customer information in [PLDT's] records. [Its] system configuration does not allow porting out of data. Also, the spam emails did not contain any malicious codes and/or links to malicious commands or controls that will let any external user get further data from [its] system."[30]

Following the information regarding the breach and the personal data involved in the breach, PLDT stated that it has turned off all access and operations of its email campaign facility.[31]

---

[26] *Id.* § 18 (C).
[27] Post-Breach Report, 21 July 2022, Annex B, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2022).
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*

PLDT also provided the contact information of its Deputy Data Privacy Officer to whom further questions or concerns may be addressed.[32]

Apart from the email notification, PLDT provided additional assistance to the affected data subjects by providing as well an advisory on handling guidelines for spam emails received by PLDT Home customers.[33]

Further, PLDT sufficiently addressed the breach and prevented its recurrence. PLDT's immediate investigation of the incident revealed that the breach was caused by exploiting a vulnerability in the bypass authentication of its Email Dispatch System.[34]

PLDT determined that the suspicious e-mails did not contain any malware. While a vulnerability may have been exploited and there was access to their customers' e-mail addresses the design of PLDT's system disabled and prevented any exfiltration of data outside of its environment.[35]

Thus, PLDT's investigation concluded that only email addresses, and no other personal information of PLDT customers, were involved in the breach,[36] and that no exfiltration of the email database may have been possible.[37] As such, the immediate taking down of the system sufficiently addressed the breach since it prevented further access and use of the registered email addresses to send more unauthorized emails and the possibility of exfiltrating other personal information of PLDT's data subjects.

Considering that the breach was due to a vulnerability in the bypass authentication of the Email Dispatch System, PLDT's immediate discontinued use prevents the recurrence of the incident.

---

[32] *Id.*
[33] Post-Breach Report, 21 July 2022, at 2, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2022).
[34] Notification Letter to the Commission, 18 May 2018, at 1, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2018).
[35] Post-Breach Report, 21 July 2022, at 2, *in* In re: Philippine Long Distance Telephone Company, Inc., NPC BN 18-073 (NPC 2022).
[36] *Id.*
[37] *Id.*

Given the foregoing, the Commission finds that the measures undertaken by PLDT has sufficiently addressed the incident and prevents its recurrence.

WHEREFORE, premises considered, the Commission resolves that the matter of NPC BN 18-073 In re: Philippine Long Distance Telephone Company, Inc. is hereby **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
16 March 2023

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

LBJ
Data Privacy Officer
Philippine Long Distance Telephone Company, Inc.

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: CITY GOVERNMENT OF ILOILO - INTERNAL AUDIT SERVICES **NPC BN 18-046**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is the breach notification submitted by the City Government of Iloilo - Internal Audit Services (City of Iloilo) relating to the hacking of its website (iloilocity.gov.ph) resulting in the leakage of information on its Taxpayers Dashboard Services (TDS).

Facts

On 16 March 2018, Francis Rodolfo T. Cruz (Cruz), head of the Information Systems Office (ISO) of the City of Iloilo, discovered that the City's website was hacked, and information included in the TDS was posted on a Facebook page known as "Iloilo Blackhats."[1] Cruz then took down the website immediately.[2]

On 19 March 2018, Cruz reported the incident to the Philippine National Police - Anti-Cybercrime Group (PNP-ACG) Visayas Field Unit.[3]

On 11 April 2018, the City of Iloilo notified the National Privacy Commission (NPC) of the breach.[4]

---

[1] Notification to the Commission, 11 April 2018, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2018).
[2] Post-Breach Report, 11 November 2021, at 1, *in* In re: City Government of Iloilo– Internal Audit Services, NPC BN 18-046 (NPC 2021).
[3] *Id.* Annex D.
[4] Notification to the Commission, 11 April 2018, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2018).

The City of Iloilo reported that one hundred thirty-one (131) businesses utilized the TDS for their Online Business Permits Renewal Process for the Calendar Year (CY) 2018.[5]

The TDS contains taxpayers' information specifically their account numbers, business names, business addresses, contact persons/representatives, genders, e-mail addresses, contact numbers, gross sales/receipts per month for CY 2017, and lines of business.[6]

On 25 October 2018, the NPC, through the Complaints and Investigation Division (CID), invited the City of Iloilo's City Government Department Head II who was the designated Data Protection Officer (DPO), for a meeting on 03 December 2018 to discuss the breach incident.[7]

On 19 October 2021, the NPC, through the CID, required the City of Iloilo to submit a Post Breach Report containing:

1. Results of the investigation conducted by the Internal Audit Services of Iloilo City as well as the PNP Anti-Cyber Crime Group;
2. Proof of notification conducted on the affected data subjects;
3. Documentation on the security measures conducted before, during, and after the incident; and
4. Remedial measures undertaken to address the incident and prevent its recurrence.[8]

On 08 November 2021, the City of Iloilo filed a Motion for Additional Time to Submit the Post-Breach Report for the following reasons: (1) change in DPO, (2) physical transfer of the Office of the Internal Audit Services which resulted to the difficulty of locating most of the documents on the matter, (3) another case load of the DPO.[9]

---

[5] *Id.*
[6] *Id.*
[7] Breach Notification of the Office of the Internal Audit Services of the City of Iloilo, 25 October 2018, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2018). [8] Order, 19 October 2021, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2021).
[9] Motion for Additional Time (To Submit the Post-Breach Report), 08 November 2021, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2021).

On 09 November 2021, the NPC granted the Motion.[10]

On 11 November 2021, the City of Iloilo submitted its Compliance.[11]

The City of Iloilo reported that there were one hundred thirty-one
(131) business establishments affected by the hacking of the website:
"sixty-one (61) were corporations, one (1) was a cooperative, sixty-five
(65) were sole proprietorships, two (2) were partnerships, and two (2) were only test data."[12]

The City of Iloilo explained that the PNP-ACG discovered that the Iloilo Blackhats also posted about the hacked websites of West Visayas State University and Central Philippine University[13] and that in all of these instances, the PNP-ACG was unable to identify the perpetrator.[14]

As an immediate measure, the City of Iloilo temporarily shut down the website "to safeguard the other information posted and for the PNP to take control and continue their probe."[15]

The City of Iloilo reported that passwords for the website are already encrypted and it has adopted "different levels of security" on its other online platforms.[16]

It also procured licensed operating systems (OS) "to prevent the easy invasion of the unit itself."[17] When it comes to transfer of data within the department, the City of Iloilo also advised employees to utilize the Local Area Network (LAN) or e-mail or as long as transfer is not made through external drive or universal serial bus (USB).[18]

---

[10] Resolution (of the Motion for Extension of Time dated 08 November 2021), 09 November 2021, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2021).
[11] Post-Breach Report, 11 November 2021, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2021).
[12] *Id.* at 6.
[13] *Id.* at 2.
[14] *Id.*
[15] Breach Notification of the Office of the Internal Audit Services of the City of Iloilo, 25 October 2018, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2018). [16] Post-Breach Report, 11 November 2021, at 3, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2021).
[17] *Id.*
[18] *Id.*

On 31 January 2022, the CID ordered the City of Iloilo to submit a report containing the proper documentation of the actions already taken.[19]

On 17 February 2022, the City of Iloilo submitted its Compliance.[20]

The City of Iloilo added that the TDS has a "dedicated firewall in place" and it can only be accessed by authorized personnel of the City of Iloilo.[21] It emphasized that upon knowledge of the incident, it promptly disabled online access to the TDS.[22] The City of Iloilo attached proof of its allegations to the Compliance.[23]

Based on the CID's assessment dated 11 January 2023, the City of Iloilo
implemented appropriate security measures to address the incident.[24]

Issue

Whether the City of Iloilo conducted proper breach management, including the implementation of reasonable and appropriate security measures pursuant to NPC Circular 16-03 (Personal Data Breach Management).

Discussion

The Commission finds that the City of Iloilo conducted proper breach management and implemented reasonable and appropriate security measures in addressing the breach. Thus, the Commission resolves to close the case.

---

[19] Order (To submit supporting documents/proof), 31 January 2022, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2022).
[20] Compliance, 17 February 2022, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2022).
[21] *Id.*
[22] *Id.*
[23] Post-Breach Report, 11 November 2021, annexes I-R, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2021).
[24] Final Breach Notification Evaluation Report, 11 January 2023, at 7, *in* In re: City Government of Iloilo– Internal Audit Services, NPC BN 18-046 (NPC 2023).

Section 17(D) (3) of NPC Circular 16-03 provides the obligation of a Personal Information Controller (PIC) to notify the Commission of a personal data breach.[25] It provides the content of notification specifically the measures that a PIC must take to address the breach:

> Section 17. *Notification of the Commission.* The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification.* The notification shall include, but not be limited to:
>
> . . .
>
> 3. Measures Taken to Address the Breach
>
> A. description of the measures taken or proposed to be taken to address the breach;
>
> B. actions being taken to secure or recover the personal data that were compromised;
>
> C. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
>
> D. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
>
> E. the measures being taken to prevent a recurrence of the incident.[26]

Based on the records, the City of Iloilo implemented security and subsequent measures to ensure that the risk of harm will not materialize.

As an immediate measure, the City of Iloilo reported the incident to the PNP-ACG and a blotter was made.[27] Temporarily, the TDS and the official website were shut down and the City of Iloilo utilized the Bulletin Board Service (BBS).[28]

---

[25] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], § 17 (D) (3) (15 December 2016).
[26] *Id.*
[27] Post-Breach Report, 11 November 2021, annex N, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2021).
[28] *Id.* at 5.

According to the City of Iloilo, the National Bureau of Investigation (NBI), together with its Information Technology Specialist, assisted its ISO in conducting a system audit to "locate the whereabouts of the perpetrator."[29]

It sought the assistance of the Department of Information and Communication Technology (DICT) in "identifying the system's security flaws and ensuring that the system adheres to security standards."[30]

To prevent the recurrence of the breach, the City of Iloilo utilized "security tokens" for each user to facilitate access to the website.[31]

As an organizational measure, the City of Iloilo advised its employees to use the LAN or e-mail when transferring files or data.[32]

The City of Iloilo procured licensed OS to prevent infiltration of data.[33] It reported that passwords are already encrypted and adopted "different levels of security" in its online service platforms.[34]

The security incident also prompted the City of Iloilo to improve its security infrastructure.[35] It stated that "web monitoring services and "anti-denial of service" were implemented in every online service."[36]

Further, the City of Iloilo stressed that the TDS has a "dedicated firewall in place" and access is limited to authorized personnel of the City of Iloilo.[37] It also disabled online access to the TDS and "checked its readiness before it was put back online."[38]

---

[29] *Id.* Annex N.
[30] *Id.* at 5.
[31] *Id.*
[32] *Id.*
[33] Post-Breach Report, 11 November 2021, at 3, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2021).
[34] *Id.*
[35] *Id.* Annex N.
[36] *Id.*
[37] Compliance, 17 February 2022, at 1, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2022).
[38] *Id.*

The City of Iloilo recounted that among the one hundred thirty-one (131) registrants of the TDS: "sixty-one (61) were corporations, one (1) was a cooperative, sixty-five (65) were sole proprietorships, two (2) were partnerships, and two (2) were merely test data."[39]

Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) protects the processing of personal data of an individual or natural person.[40] Given this, the information relating to a juridical entity does not constitute personal data.

Here, since most of the information possibly leaked from the website were information on juridical entities, the City of Iloilo is not mandated to notify these affected entities.

Nonetheless, the City of Iloilo is reminded of its obligation to continuously update its security measures and ensure that it will be in a position to safeguard the personal data of its constituents.

Based on the foregoing, the measures that the City of Iloilo took after the incident enabled it to strengthen its security measures in compliance with the DPA and its Implementing Rules and Regulations (IRR).[41] Given this, following NPC Circular 16-03, the actions that the City of Iloilo took are sufficient to close the matter.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-046 In re: City Government of Iloilo - Internal Audit Services is considered **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
17 August 2023.

---

[39] Post-Breach Report, 11 November 2021, annex O, *in* In re: City Government of Iloilo – Internal Audit Services, NPC BN 18-046 (NPC 2018).
[40] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 4 (2012).
[41] *See* National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule VI, § 25 (2016).

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

ATTY. FGG
City Legal Officer III/Data Protection Officer
City Government of Iloilo – Internal Audit Services

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: ATENEO DE ZAMBOANGA UNIVERSITY

NPC BN 18-019

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is a breach incident involving the unauthorized change in bank account numbers of some of the Ateneo de Zamboanga University - School of Medicine (AdZU) employees resulting in the delay in the payment of salaries.

Facts

On 15 February 2018, a staff member of AdZU called ADC, the payroll officer, to complain about the non-payment of a faculty doctor's salary for the period of 01 to 15 February 2018.[1]

Upon checking, ADC discovered the discrepancy in the bank account number in the payroll compared to that submitted by the faculty member.[2] According to AdZU, the salaries of forty-two (42) employees were changed to a specific bank account number and resulted to the miscrediting of the employees' salaries to the wrong bank account.[3] Additionally, the bank accounts of two (2) other employees were changed for the payroll period of 15 to 31 January 2018.[4]

---

[1] Post Breach Report - Report of the Fact-Finding Committee on the case of the Payroll Breach dated 7 March 2018, 5 April 2022, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2022).

[2] Data Breach Notification No. 2018-01, 17 February 2018, at 2, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2018).

[3] *Id.*

[4] *Id.*

On the same day, the University Human Resources (HR) Director, University Accountant, University Treasurer, and ADC met to discuss the matter.[5] They also met with the Data Privacy Officer (DPO) and Director of the Center for Information and Technology Services (CITS) to further investigate the matter.[6] AdZU discovered that the account numbers of the employees were changed to the account number of one of the CITS employees, Mr. NB, and the latter's cousin's bank account.[7]

On 16 February 2018, AdZU's Human Resource and Development Office (HRADO) Director sent a letter to NB to submit a written explanation regarding the crediting of the salaries of the employees.[8]

On 17 February 2018, AdZU notified the National Privacy Commission (NPC) of the incident.[9]

On 27 February 2018, NB wrote a letter to the HRADO Director admitting his guilt for tampering with the 31 January and 15 February 2018 payrolls.[10] NB explained that he changed the employees' bank account numbers "due to his great need for money for maintenance medicines and therapy of his ailing mother."[11] He also expressed that "he is the sole breadwinner of the family and had to support the education of his siblings."[12] In his letter, NB described how he was able to get the password of the desktop of the University Treasurer, who regularly approves the payroll and bank transmittal.[13]

According to NB, he was called one day to the Finance Office to fix the University Treasurer's computer.[14] While fixing the computer, he discovered a malware in a temporary folder.[15] It was in this folder where NB said he "s[aw] some passwords and memorize[d] the password of the Treasurer" which he used to gain access to AdZU's

---

[5] *Id.* at 3.
[6] *Id.*
[7] Report of the Fact-Finding Committee on the case of the Payroll Breach, 07 March 2018, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2018).
[8] *Id.*
[9] Data Breach Notification No. 2018-01, 17 February 2018, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2018).
[10] Report of the Fact-Finding Committee on the case of the Payroll Breach, 07 March 2018, at 1, *in*
In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2018).
[11] *Id.* at 2.
[12] *Id.*
[13] *Id.*
[14] *Id.* at 1.
[15] *Id.*

payroll system.[16] As a result, he changed the bank account numbers of some of the employees to his bank account number.[17]

AdZU also reported that NB already admitted his guilt prior to his letter to HRADO through an e-mail sent to his CITS superior on 20 February 2018.[18]

On 16 March 2022, the NPC, through the Complaints and Investigation Division (CID), ordered AdZU to submit a Post-Breach Report containing the proper documentation on the actions it took:

> 1. Description of the personal data breach, its root cause and circumstances regarding its discovery;
> 2. Actions and decisions of the incident response team;
> 3. Outcome of the breach management, and difficulties encountered;
> 4. Compliance with notification requirements and assistance provided to affected data subjects, if any; and
> 5. A copy of the report on the investigation on the breach incident, pursuant to the Report dated 17 February 2018.
>
> **ATENEO DE ZAMBOANGA UNIVERSITY** is hereby given a period of fifteen (15) days from receipt hereof to submit their compliance through email at complaints@privacy.gov.ph.
>
> **SO ORDERED.** [19]

On 05 April 2022, AdZU submitted a Post-Breach Report.[20]

AdZU reported that upon receiving the incident report of the payroll officer in-charge of the HR Office, the Incidence Response Team consisting of the DPO, the Director of the HRADO, and the Director of CITS immediately met.[21]

---

[16] Report of the Fact-Finding Committee on the case of the Payroll Breach, 07 March 2018, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2018).
[17] *Id.*
[18] *Id.*
[19] Order (To Submit Post Breach Report), 16 March 2022, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2022).
[20] Post-Breach Report, 05 April 2022, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18- 019 (NPC 2022).
[21] *Id.*

The Finance Office requested the bank to freeze the two (2) bank accounts where the salary of the affected employees was credited.[22] Additionally, AdZU reported that their CITS immediately reviewed the access logs of the payroll system to determine how the unauthorized changes were made and to identify the perpetrator.[23]

AdZU also requested assistance from the National Bureau of Investigation (NBI) Cyber Security in Zamboanga City to guide the incident response team for further actions to be taken.[24]

NB was later found guilty by AdZU for "culpable payroll breach on two separate occasions."[25] AdZU signified that it would not pursue legal action against NB provided that he tender his resignation and return the amount that was deposited in his and the third party's bank accounts.[26] NB issued a promissory note to guarantee his obligation to pay.[27]

As part of AdZU's breach management, AdZU reported that the incident prompted CITS to conduct a review of its systems to further increase security and to avoid similar incidents in the future.[28]

AdZU reported that it immediately disabled all login credentials as soon as the suspect was identified.[29] It also reported that it immediately notified its affected data subjects of the incident and credited their salaries.[30]

AdZU conducted an Information Technology (IT) audit and reviewed appropriate IT policies and procedures.[31] It also conducted digital data

---

[22] *Id.*
[23] *Id.* at 2.
[24] *Id.* at 1.
[25] Letter *to* Mr. NB, 08 March 2018, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2018).
[26] *Id.*
[27] Promissory Note, 04 June 2018, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2018).
[28] Post-Breach Report, 05 April 2022, at 2, *in* In re: Ateneo de Zamboanga University, NPC BN 18- 019 (NPC 2022).
[29] Letter of the CITS Director to Ateneo de Zamboanga University DPO, 04 April 2022, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2022).
[30] Post-Breach Report, 05 April 2022, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18- 019 (NPC 2022).
[31] Letter of the CITS Director to Ateneo de Zamboanga University DPO, 04 April 2022, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2022).

inventory and put in place appropriate controls and safeguards.[32] Additionally, AdZU's Finance Office updated passwords and other credentials, especially its IT programs and applications.[33]

Issue

Whether AdZU conducted proper breach management, including the implementation of reasonable and appropriate security measures.

Discussion

The Commission finds that AdZU conducted proper breach management and implemented reasonable and appropriate security measures in addressing the breach. The Commission resolves to close the matter.

Section 20 (a) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) provides that a Personal Information Controller (PIC) should implement reasonable and appropriate measures to protect personal information:

> Section 20. *Security of Personal Information* -
> a. The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[34]

Similarly, Section 17 (D) (3) of NPC Circular 16-03 (Personal Data Breach Management) provides for the obligation of a PIC to notify the Commission of a personal data breach.[35] The provision provides the content of notification specifically the measures that a PIC took to address the breach:

---

[32] *Id.*
[33] *Id.*
[34] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (a) (2012).
[35] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], § 17 (D) (3) (15 December 2016).

> Section 17. *Notification of the Commission*. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification.* The notification shall include, but not be limited to:
>
> . . .
>
> 3. Measures Taken to Address the Breach
>
> a. description of the measures taken or proposed to be taken to address the breach;
> b. actions being taken to secure or recover the personal data that were compromised;
> c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
> d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
> e. the measures being taken to prevent a recurrence of the incident.[36]

The Commission recognizes that AdZU complied with its obligation to implement measures to minimize the potential harm and adverse effects of the breach to its employees. Based on AdZU's submissions, it performed actions that could prevent and mitigate the likelihood of a similar incident.

According to AdZU, there was an immediate investigation conducted by its Incidence Response Team consisting of AdZU's DPO, Director for HRADO, and the Director for CITS.[37] AdZU's Finance Office then immediately requested the bank to freeze the two (2) bank accounts where the salary of the affected employees was credited.[38]

AdZU directly sought assistance from the NBI Cyber Security in Zamboanga City to guide AdZU on other actions to be taken.[39]

---

[36] *Id.*
[37] Post-Breach Report, 05 April 2022, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18- 019 (NPC 2022).
[38] *Id.* at 2.
[39] *Id.*

AdZU, through its HRADO, immediately informed their employees about the incident and their salaries were promptly credited.[40]

AdZU also penalized the erring employee and ensured that the money that was still in the bank account of NB was "put on hold and can no longer be withdrawn."[41] AdZU likewise disabled NB's login credentials on the different resources and programs of the university.[42]

Internally, the incident caused AdZU to review its systems.[43] AdZU's CITS revisited the access logs of its payroll system to identify the perpetrator.[44] It also led AdZU to conduct an IT review audit and digital data inventory to streamline its IT policies and procedures.[45]

As a security measure, AdZU's Finance Office secured its programs and applications by updating passwords and other credentials.[46]

As part of AdZU's organizational measures, an orientation for the Finance Office on how to secure digital assets was also conducted.[47]

The Commission notes that there is no evidence on record that indicates that there was lack of appropriate security measures on the part of AdZU. The access to the university's payroll system was caused by employee malfeasance. While there is no measure that will completely guarantee absolute security, this is all the more true in cases where employee malfeasance is a factor. Nevertheless, the Commission reminds PICs to proactively carry out measures to ensure that security protocols will rule out or mitigate these risks as much as possible.

---

[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] Post-Breach Report, 05 April 2022, at 2, *in* In re: Ateneo de Zamboanga University, NPC BN 18- 019 (NPC 2022).
[44] *Id.*
[45] Letter of the CITS Director to Ateneo de Zamboanga University DPO, 04 April 2022, at 1, *in* In re: Ateneo de Zamboanga University, NPC BN 18-019 (NPC 2022).
[46] *Id.*
[47] *Id.*

Based on the foregoing, the actions that AdZU took subsequent to the incident facilitated the enhancement of its organizational, physical, and technical measures pursuant to the DPA and NPC Circular 16-03.

Thus, the actions that AdZU took are sufficient to close the matter.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-019 In re: Ateneo de Zamboanga University is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
11 May 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

(on official leave)
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

FR. RVE, S.J.
Data Protection Officer
Office of the Vice President for Administration
Ateneo de Zamboanga University

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: EASYTRIP SERVICES CORPORATION

NPC BN 17-028
NPC BN 18-180

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is the breach notification submitted by Easytrip Services Corporation (ESC) involving the unauthorized access and manipulation of an ESC account by means of an illicit Structured Query Language (SQL) injection in a mobile application.

Facts

On 25 October 2017, an ESC sales personnel detected a post on the "Buy and Sell Philippines" Facebook group selling ESC load "at 30% off through the PayMaya mode of payment."[1] ESC reported that it did not authorize the post as a valid promotion during that time.[2]

The seller of the ESC load was named "CB" who is not an ESC employee, customer, or business partner.[3] Since this was not an official promotion, the sales personnel reported the matter to the ESC Operations Management for investigation.[4]

After further investigation, ESC discovered that the seller enticed potential customers to top-up an amount of One Thousand Pesos (Php 1,000.00) in their ESC accounts at the cost of only Seven Hundred Pesos (Php 700.00).[5] After the transaction, the buyer would have to pay the

---

[1] Full Report, 19 September 2018, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018~~7~~).
[2] *Id.*
[3] *Id.* at 2.
[4] *Id.*
[5] *Id.*

seller in the latter's PayMaya account by paying through a 7-11 branch.[6]

Subsequently, ESC created a dummy account and contacted the seller through Facebook Messenger.[7] Thereafter, the dummy account asked the seller to reload One Thousand Pesos (Php 1,000.00) as a prerequisite to receiving the payment.[8]

ESC narrated that "it ran all auditing and logging tools on the system to capture the said reloading activity."[9] After the transaction, ESC stated that an additional One Thousand Pesos (Php 1,000.00) was added to the running balance.[10] ESC, however, discovered that there was no description, credited amount, or total amount added to the Statement of Account (SOA) to show that a legitimate reload transpired.[11]

ESC further stated that "the balance of the dummy account gained an additional One Thousand Pesos (Php 1,000.00) despite the fact that there was no actual monetary transaction with ESC."[12] ESC explained that there were "no traces of the typical logs" that is usually remarked in a legitimate transaction.[13]

On 03 November 2017, ESC notified the National Privacy Commission (NPC) of the incident.[14] ESC explained that an infiltrator with username "sa7" managed to perform a SQL injection on the account using an Android Balance Inquiry Application called "finandroid."[15] This enabled the seller to access and manipulate certain information in the ESC account.[16]

---

[6] Full Report, 19 September 2018, at 2, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] Full Report, 19 September 2018, at 2, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[13] *Id.*
[14] Easytrip Breach Report, 03 November 2017, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2017).
[15] *Id.*
[16] Full Report, 19 September 2018, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).

ESC identified that SQL injection was performed in a specific part of a mobile application dedicated to ESC customer inquiries.[17] This part of the application was specifically related to information on the account balance of ESC customers.[18]

ESC stated this specific system covers the following information: (1) balance of the account; (2) name of account holder; (3) account number;
(4) last reload of account; and (5) the on-board unit number.[19] ESC's investigation reveals that the compromised data include the balance of the dummy account.[20]

To address the issue, ESC's third party company, Egis Projects Philippines Incorporated Software Development Center (EPPI SDC) reported that ESC adopted the following measures:

a. Disabled identified Web Service and Applications possibly used by perpetrator;
b. Created a new secured web service;
c. Updated and secured ESC Android Mobile POS Reloading;
d. Updated and secured ESC Android Mobile POS Balance Inquiry for POS;
e. Disabled Online Reloading facility for GP, upgrade Work in Progress;
f. Pending update and deployment of Android Mobile balance inquiry for ESC Customer;
g. Investigation and audit of other web services.[21]

ESC reported that it "adjusted sensitivity and adaptability of *PFsense firewall* to block additional IP threats on the firewall" to reduce the harm or negative consequences of the breach.[22]

Specifically, ESC's measures include "caching of Web Server content to lessen server load, creating page rules for Hypertext Transfer Protocol Secured (HTTPS), twenty-four (24) hours reporting on all passing through web traffic, Internet Protocol (IP) white listing and

---

[17] Full Report, 19 September 2018, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] Easytrip Breach Report, 03 November 2017, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2017).
[22] *Id.*

block listing, and checking of all incoming web browser for possible threats."[23]

ESC hired a security expert for additional mitigation and resolution to prevent a recurrence of the incident,.[24] It also subscribed to "Anti Distributed DenialofService (DDoS) Attack" which aims to filter network traffic for threats and other suspicious activities.[25] It created a "DdoS Playbook" to protect and provide alerts to the organization for imminent threats in similar future scenarios.[26] It implemented an infrastructure upgrade to gather "recent patches and upgrades regarding newly upgraded cyber threats."[27] Lastly, ESC subscribed to Cloudflare, an IT service management company, to further strengthen its security.[28]

ESC narrated that apart from the dummy account that the seller accessed, there were no indications that other accounts were accessed.[29] ESC also explained that neither received complaints nor reports since the date of the incident that would indicate otherwise.[30]

On 19 September 2018, ESC submitted its Full Report on the incident.[31]

On 20 May 2022, ESC submitted a Comprehensive Technical Report in reference to the incident.[32]

On 22 June 2022, ESC provided additional information and proof in reference to the Data Breach Report submitted on 03 November 2017.[33] ESC likewise submitted proof of the remediation efforts it conducted as a Personal Information Controller (PIC).[34]

---

[23] Easytrip Breach Report, 03 November 2017, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2017).
[24] *Id.*
[25] *Id.*
[26] Full Report, 19 September 2018, at 5, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] Compliance, 11 November 2022, Annex C, *in* In Re: Easytrip Services Corporation, NPC BN 17- 028 and NPC BN 18-180 (NPC 2022).
[33] *Id.* Annex D.
[34] *Id.*

On 27 October 2022, the NPC, through its Complaints and Investigation Division (CID), ordered ESC to submit a full breach report detailing the incident containing the following information: (1) nature of the breach, (2) personal data possibly involved, and (3) remedial measures taken subsequent to suspected breach.[35]

On 11 November 2022, ESC submitted its Full Report containing its initial notification to the NPC, its Full Report submitted on 19 September 2018, the letter containing the Comprehensive Technical Report dated 20 May 2022, and the letter containing additional information and proof dated 22 June 2022.[36]

Issue

Whether the breach incident falls under mandatory breach notification.

Discussion

The Commission finds that this matter does not fall under mandatory breach notification. Thus, the Commission resolves to close the case.

Section 11 of the NPC Circular 16-03 (Personal Data Breach Management) provides:

> Section 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:
>
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.
>
> For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation

[35] Order (to submit Full-Breach Report), 27 October 2022, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2022).
[36] Compliance, 11 November 2022, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2022).

> of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> B. There is reason to believe that the information may have been acquired by an unauthorized person; and
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[37]

As such, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[38]

The first requisite provides that the breach involves sensitive personal information or information that may be used to enable identity fraud. Section 3 (l) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) defines sensitive personal information as:

> Section 3. *Definition of Terms*.
>
> . . .
>
> (l) Sensitive personal information refers to personal information:
>
> (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

---

[37] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §11 (15 December 2016).
[38] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does Initiated as a *Sua Sponte* NPC Investigation on Possible Data Privacy Violations Committed in Relation to the Alleged Hack and Breach of the Commission on Elections System or Servers, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-SS-22-001-and- NPC-SS-22-008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 31 January 2023).

> (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
>
> (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
>
> (4) Specifically established by an executive order or an act of Congress to be kept classified.[39]

In this case, the account balance and account number of the dummy account were the only compromised personal information as a result of the breach.[40] These are not considered as sensitive personal information as defined under Section 3 (l) of the DPA nor as information that may enable identity fraud.

In fact, the account number and balance of the dummy account, absent any accompanying information, may not be considered personal information since it does not specifically point to the identity of a specific person. Thus, the first requisite is not present.

For the second requisite, there is reason to believe that the information may have been acquired by an unauthorized person. The seller, an unauthorized person, gained access to the dummy account's number and balance through the mobile application.[41]

Lastly, the third requisite that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject is absent in this case.

---

[39] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (l) (2012).
[40] Full Report, 19 September 2018, at 2-3, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[41] *Id.* at 1.

To determine whether there is a likelihood that the unauthorized acquisition of information will give rise to a real risk of serious harm, there shall be a relation between the incident and any possible resulting harm to affected data subjects. The risk shall be apparent and not a product of mere speculation. Consequently, "serious harm" means that the consequences and effects to any affected data subject is significant based on the surrounding circumstances of the breach.

In determining whether the unauthorized acquisition is likely to give rise to a real risk of serious harm, a PIC or the Commission may consider several factors such as: the nature of the information involved in the breach, amount of information of a data subject, period of time lapsed from the breach, purpose of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of information involved in the breach, if any.

Here, there was no reported harm to any other data subject since it was only the dummy account's information that was compromised. There were also no significant consequences or effects as a result of the incident since there were no reports or complaints received by ESC coming from other ESC account holders.[42]

The nature of the information involved in the breach only involves fabricated information since the dummy account was only created by the ESC team to entrap the seller.

With regard to the amount of information involved, the breach only affected the account and balance of the dummy account and it did not affect the ESC database which includes other customer information such as license plates, taxpayer identification number (TIN), addresses, and contact numbers.[43]

Further, no other personal data was involved in the breach because
ESC's team immediately ran all auditing and logging tools on the

---

[42] Full Report, 19 September 2018, at 5, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[43] *Id.* at 1.

system to capture the said reloading activity between the seller and the dummy account.[44]

As part of ESC's security measures, it hired third party security experts to strengthen its technical measures and to avoid the extent of the potential misuse and exposure of information involved in the breach.[45] ESC also added security measures to prevent data leakage by Internet Protocol (IP) Blocking, disabling its internet control message protocol (ICMP), strengthening its web application firewall (WAF), creating a new web service, creating ESC android mobile reloading and balance inquiry, and disabling online reloading facility for global payments.[46] Thus, ESC observed stringent technical measures to minimize any possible harm or any potential negative consequences of the breach to its customers.

Considering all these factors, the unauthorized acquisition did not give rise to a real risk of serious harm to any affected data subject. Thus, the third requisite is absent.

Since the first and third requisites for mandatory breach notification are absent in this case, the Commission finds that the breach reported by ESC does not require mandatory breach notification.

Section 20 (a) and (c) of the DPA provides for the obligation of PICs in implementing security measures for the protection of personal information:

> Section 20. *Security of Personal Information.*
>
> (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.
>
> . . .

---

[44] *Id.* at 2.
[45] Easytrip Breach Report, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[46] Full Report, 19 September 2018, at 4, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).

> (c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:
>
> (1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
>
> (2) A security policy with respect to the processing of personal information;
>
> (3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and
>
> (4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.[47]

The Commission takes this opportunity to remind PICs of their constant responsibility to protect the personal data of its data subjects against accidental, unlawful, or unauthorized interference. When implementing security measures, the PIC should consider the nature of the personal information, current data privacy best practices, and security measures considering the developments in technology and the risks that data subjects are being subjected to in order to guarantee that the personal data it processes are continuously safeguarded.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 17-028 and NPC BN 18-180 In re: Easytrip Services Corporation is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
11 May 2023.

---

[47] Data Privacy Act of 2012, § 20.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

(on official leave)
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

LAL
Data Protection Officer
Easytrip Services Corporation

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: MOVIE AND TELEVISION REVIEW AND CLASSIFICATION BOARD

NPC BN 17-010

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is the Movie and Television Review and Classification Board's (MTRCB) breach notification and management in compliance with NPC Circular 16-03 (Personal Data Breach Management).

Facts

To recall, MTRCB requested for exemption from notification of its data subjects on 07 March 2018.[1] MTRCB also requested for a sixty-day extension period if the exemption is not feasible.[2]

On 15 April 2021, the Commission denied MTRCB's request for exemption and extension, ordered MTRCB to submit proof of notification to its data subjects, and submit the results of its independent security audit:

> **WHEREFORE**, premises considered, the Commission **ORDERS** the Movie and Television Review and Classification Board to comply with the following:
>
> (1) **NOTIFY** the data subjects affected by the breach incident **within fifteen (15) days** from receipt of this Order;

---

[1] Letter Re: Request for Exemption, Extension and Alternate means of Notification for Affected Data Subjects, 07 March 2018, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2018).
[2] *Id.*

(2) **SUBMIT** proof of notification that ensures all data subjects were made aware of the breach **within fifteen (15) days** from receipt of this Order; and

(3) **SUBMIT** the results of the independent security audit **within three (3) months** from receipt of this Order.

SO ORDERED.[3]

The Commission explained that MTRCB had not submitted proof of notification of its data subjects.[4] If MTRCB deemed it necessary to notify the data subjects and asked for the extension in good faith, it should have proceeded to notify the data subjects after the lapse of sixty (60) days.[5] The Commission also highlighted the fact that the sensitive personal information or other information that may enable identity fraud of at least five hundred seventy-three (573) individuals were compromised.[6] Taking everything into consideration, the breach was likely to give rise to a real risk to the data subjects' rights and freedoms.[7] Finally, the Commission also considered the issuance of the Compliance Order dated 31 January 2018 as proof that the Commission had not found ground to dispense with the notification requirement.[8] The Commission maintained that MTRCB failed to prove it was entitled to exemption, even after multiple requests for postponement or exemption from notification.[9]

MTRCB manifested that it received the Order dated 15 April 2021 on 06 May 2021.[10] MTRCB posted a Notice of Data Breach (Notice) on its website (www.mtrcb.gov.ph) on 12 May 2021.[11] It also informed the Commission that it notified its data subjects by posting the Notice on its website as an alternative means of notification instead of individual notification. MTRCB explained that while "[it is] aware of the requirements of NPC Circular 16-03 regarding the sending of an individual notification to affected data subjects. However, [it finds] the

---

[3] Order, 15 April 2021, at 7, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2021).
[4] *Id.* at 6.
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.* at 7.
[9] Order, 15 April 2021, at 7, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2021).
[10] Letter Re: Compliance to the National Privacy Commission (NPC) Order No. CID BN 17-010, 18 May 2021, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2021).
[11] *Id.*

individual notification an arduous task, as [it] learned that the number of affected data subjects amounted to five hundred seventy-three (573)."[12] The Notice states:

> **NOTICE OF DATA BREACH**
>
> On 19 September 2017, 10:27 a.m. we became aware of unauthorized access to our server. Upon investigation, we learned that certain data from our server was subsequently locked due to the ransomware attack, the extent of which is that all files within the affected servers have been maliciously encrypted and have been renamed with a file extension. This data may include name and Tax Identification Numbers (TIN) of MTRCB personnel, contracted vendors and supplier's business name.
>
> At present, we have no indication that there has been unauthorized activity with respect to any user's account on our website. We are not currently aware of evidence of access to any databases that host user data.
>
> As a precaution, the Agency has strengthened its information security by implementing various and strict security measures, such as, the conduct of regular vulnerability assessments and the creation of projects that enhance the current security measure of the Agency.
>
> We have already set up a MTRCB Data Action Response Center to provide assistance to those who may have been affected by the data breach in which information is access without authorization. For more information, contact the MTRCB Data Action Response Center at 8376-7380 loc. 115.
>
> We apologize for, and deeply regret, any inconvenience this may cause. We take the security of information very seriously and appreciates everyone's continued support.[13]

The National Privacy Commission (NPC), through its Enforcement Division (EnD), issued a Compliance Letter on 15 October 2021 and directed MTRCB to comply strictly with the Order dated 15 April 2021:

> In your letter, you informed the Commission that you have posted a notice of a data breach on your website on May 12, 2021. However, this could not be considered as a valid form of notification absent prior approval of the NPC.

---

[12] *Id.*
[13] *Id.* Annex A.

> **The Enforcement Division (EnD) reiterates that individual notification is the general rule. The Commission has repeatedly ordered MTRCB to individually notify the data subjects despite its prior request for alternative means of notification**. Moreover, we would like to take this opportunity to remind you that it is the Personal Information Controller's (PIC) responsibility to ensure that all data subjects are made aware of the breach.[14]

On 02 November 2021, MTRCB reported that the affected data subjects were already notified via email on 25 to 29 October 2021.[15] MTRCB submitted a list of two hundred seventy-four (274) individuals and their notification status,[16] and a list of two hundred ninety-nine (299) companies affected.[17] MTRCB explained:

> [F]rom the 274 affected individuals, the breakdown below shows the number of individuals notified, deceased and those not notified due to the unavailability of contact records from the Information Technology Unit, Human Resources Management Unit and Property and Supply Unit, to wit:
>
> - Emailed: 180 individuals
> - Deceased: 17 individuals
> - No Record: 77 individuals[18]

MTRCB also submitted copies of the email notification sent to the data subjects, which showed multiple recipients under the "Bcc:" field.[19]

On 28 January 2022, the EnD issued another Compliance Letter to the MTRCB.[20] The EnD requested MTRCB to submit proof that it sent the

---

[14] Enforcement Division Letter Re: Compliance to the National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 15 October 2021, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2021). Emphasis supplied.
[15] Letter Re: Compliance to National Privacy Commission Order No. CID BN 17-010 dated 15 April 2021, 02 November 2021, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2021).
[16] *Id.* Annex A.
[17] *Id.* Annex B.
[18] *Id.* at 1.
[19] *Id.*
[20] Enforcement Division Letter Re: Compliance to the National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 28 January 2022, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).

notifications and that the affected data subjects received the same.[21] As for the seventeen (17) deceased data subjects, the EnD requested that MTRCB notify their next of kin, if they can be ascertained from company records.[22] The EnD further provided:

> If MTRCB, even after diligent search, still renders it unable to determine the contact of a deceased data subject's kin, it may seek approval of the Commission to use alternative means of communication in accordance with Section 18(D) of NPC Circular 16-03.
>
> As it appears that 77 individuals were not notified due to the unavailability of contact records, MTRCB may likewise seek approval of the Commission to use alternative means of communication under Section 18(D) of NPC Circular 16-03.
>
> We note that MTRCB has earlier posted a public notification of the breach through its website. However, individual notification of data subjects remains to be the general rule. Hence, prior approval of the Commission is required.[23]

Thus, the EnD directed the MTRCB to submit proof of receipt of notification of the data subjects and to notify the next of kin of the deceased data subjects pursuant to the transmissibility of rights of data subjects.[24] The EnD also directed MTRCB to submit the results of an independent security audit.[25]

MTRCB submitted its Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to comply with Directives and for Permission for Other Modes of Public Notification (Compliance with Motion) dated 14 February 2022.[26] It reported that one hundred three (103) out of one hundred seventy-seven (177) individuals notified acknowledged receipt and it attached proof of the individual acknowledgments.[27]

---

[21] *Id.* at 1.
[22] *Id.* at 2.
[23] *Id.*
[24] *Id.*
[25] *Id.* at 2-3.
[26] Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to comply with Directives and for Permission for Other Modes of Public Notification, 14 February 2022, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[27] *Id.* Annex A-1 to A-103.

MTRCB also reported that it found the contact information for the next of kin of one (1) deceased data subject, and that they had acknowledged receipt of the notification.[28] MTRCB requested that the Commission grant the use of alternative means of notification:

> 9. As the MTRCB further exerts diligent efforts to locate the parties, it appears the contact details of those who have not been notified as of yet, are those not contained in the records existing with the Board, and as thus, the MTRCB prays for the allowance of other modes of public notification by allowing the posting of the *Notice* in its website[.][29]

MTRCB also explained that it could not submit the results of the independent security audit and requested for extension:

> 10. In further compliance with the *Order* dated 15 April 2021, on 15 December 2021, the MTRCB entered into a *Contract for the Conduct of Vulnerability Assessment and Penetration Testing of* MIDAS with **NEXT GENERATION TECHNOLOGIES GLOBAL, INC.** (NEXT GENRATION) for NEXT GENERATION to conduct an independent audit into MTRCB'S systems;
>
> 11. However, **the testing has not been completed due to administrative and budgetary constraints.** Thus, **MTRCB humbly prays for an extension of until 31 July 2022, the expected end of contract, to comply with the directive to comply with the submission of the independent security audit.** Should the audit be completed earlier, MTRCB endeavors to provide the results of the independent security audit to the Honorable Commission, immediately upon its receipt.[30]

Thus, MTRCB prayed for the following reliefs:

> *WHEREFORE*, premises considered, the MTRCB respectfully prays from the Honorable Commission that:
>
> 1. The submission on the 103 data subjects acknowledging receipt of Notice be NOTED as compliance to this Honorable Commission's Order dated 15 April 2021;

---

[28] *Id.* at 2.
[29] *Id.*
[30] *Id.* Emphasis supplied.

> 2. MTRCB be granted alternative means of public notice, by posting the notice in M'I'RCB's website for the data subjects of which it has not located; and
>
> 3. MTRCB's be granted an additional three (3) months of time to allow NEXT GENERATION to finish the independent security audit;
>
> Other reliefs just and equitable under the premises are likewise prayed for.[31]

On 23 June 2022, the EnD issued another Compliance Letter to the MTRCB.[32] It found that the MTRCB provided proof of notification sent to only 103 out of 177 data subjects.[33] Further, the EnD explained there was a "considerable amount of delay in MTRCB's responsive action to prevent the likelihood of another breach from occurring since the breach incident occurred in September 2017."[34] As such, it directed MTRCB to comply with the following:

> In view of the foregoing, you are hereby required to:
>
> (1) **SUBMIT** proof of receipt of the remaining 74 out of the 177 individuals who were sent Notices within ten (10) days from receipt of this letter;
> (2) **SUBMIT** a written explanation for the cause of delay of conducting the security audit with supporting documentary evidence within ten (10) days from receipt of this letter;
> (3) **SUBMIT** a report on the results of the security audit within thirty (30) days from receipt of this letter.
>
> We urge you to comply with this directive to avoid further liabilities in accordance with law.[35]

---

[31] *Id.* at 2.
[32] Enforcement Division Letter Re: Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to comply with Directives and for Permission for Other Modes of Public Notification, 14 February 2022, 23 June 2022, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[33] *Id.* at 1.
[34] Compliance Letter from Enforcement Division, 23 June 2022, at 3, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[35] *Id.*

On 07 July 2022, the MTRCB responded to the EnD.[36] MTRCB reported that fifty-four (54) more recipients sent their acknowledgment, bringing the total to one hundred fifty-seven (157) individuals notified[37] and attached copies of the acknowledgement of receipt.[38] MTRCB also reported that despite continuous efforts, it was unable to obtain confirmation from the remaining twenty (20) recipients.[39] It submitted an Affidavit of the Head of MTRCB's Information Technology Unit, which states that the Head of the IT Unit personally sent out the Notice of Data Breach to all the affected data subjects, including the remaining twenty (20) individuals.[40]

MTRCB explained that the delay in the conduct of the independent security audit was due to several factors: constraints in the approved budget for procurement;[41] subsequent delays in bidding and procurement;[42] the delayed release of the Notice of Award (NOA) and Notice to Proceed (NTP) dated 30 June 2021 to Next Generation;[43] and the need to redo the bidding process under Section 38.1 of the Implementing Rules and Regulations of Republic Act No. 9184, or the Government Procurement Act.[44] Nonetheless, MTRCB stated that the audit was eventually and successfully completed on 27 May 2022.[45] It reported:

> In the course of the audit, Next Generation identified the following areas of weakness that require the attention of the Board:
>
> a. Remote Code Executions
> b. SQL Injections
> c. Cross Site Scripting
> d. Insecure Communications
>
> Next Generation likewise made recommendations on how to resolve the issues they identified and the MTRCB IT Unit is

---

[36] Letter Re: Compliance with National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 07 July 2022, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[37] *Id.* at 1-2.
[38] *Id.* Annex A.
[39] *Id.* at 2.
[40] *Id.* Annex B.
[41] *Id.* at 2.
[42] Letter Re: Compliance with National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 07 July 2022, at 2, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[43] *Id.* at 2-3.
[44] *Id.* at 3.
[45] *Id.*

> currently working to implement these recommendations, including the procurement of a web application firewall and Endpoint Detection and Security Solution within the year. Upon the Commission's request, we will be glad to provide it a copy of the *Report of the Final Vulnerability Assessment and Penetration Testing Report* dated 27 May 2022 submitted by Next Generation which we have kept in confidence in light of the sensitive security matters contained therein.[46]

On 14 July 2022, the Commission issued an Order granting the MTRCB's request for alternative means of notification.[47] The Commission emphasized that what is important is that the email notification was sent and the data subject has access to the information contained in the notification, should he or she need it.[48] As such, the remaining seventy-four (74) out of one hundred seventy-seven (177) data subjects who did not reply were still considered to have been sufficiently notified.[49] The Commission also acknowledged the diligent and exhaustive efforts exerted by MTRCB to locate the parties and their next of kin.[50] Given that MTRCB does not have their contact information, individual notification would be impossible.[51] As such, the Commission granted the request for alternative means of notification for the remaining ninety-seven (97) data subjects whose contact details were missing or who were determined to be deceased.[52]

The Commission, however, denied MTRCB's request for an extension to submit the results of the independent security audit.[53] The Commission emphasized that PICs should comply with obligations they themselves undertake,[54] and that "it was MTRCB that specified the date for extension, but it itself has not complied with its own deadline."[55]

Thus, the Commission directed MTRCB to comply with the following:

---

[46] *Id.* at 3-4.
[47] Order, 14 July 2022, at 5, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[48] *Id.* at 6.
[49] *Id.* at 9.
[50] *Id.* at 7.
[51] *Id.*
[52] *Id.*
[53] Order, 14 July 2022, at 5, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[54] *Id.* at 8.
[55] *Id.*

> **WHEREFORE,** premises considered, Movie and Television Review and Classification Board is hereby **ORDERED within fifteen (15) days** from the receipt of this Order to comply with the following:
>
> (1) **NOTIFY** and **SUBMIT** to the Commission proof that it implemented notification through alternative means together with the text of the notification; and
> (2) **SUBMIT** a report on the results of the independent security audit.
>
> **SO ORDERED.**[56]

On 18 August 2022, the EnD issued another Compliance Letter to the MTRCB.[57] The EnD directed the MTRCB to submit hardcopies of its letter dated 07 July 2022, the original or certified true copies of the letter's annexes, and the Final Vulnerability Assessment and Penetration Testing Report dated 27 May 2022 prepared by Next Generation.[58]

On 31 August 2022, the MTRCB responded to the EnD's Compliance Letter dated 18 August 2022.[59] It submitted the hardcopy of its letter dated 07 July 2022, along with original or certified true copies of the annexes,[60] a certified true copy of the Final Vulnerability Assessment and Penetration Testing Report dated 27 May 2022 by Next Generation,[61] and the Affidavit by the Head of the Information Technology Unit of the MTRCB dated 07 July 2022.[62]

On 03 November 2022, MTRCB submitted its compliance with the Order dated 14 July 2022.[63] MTRCB confirmed that the Notice of Breach on 19 September 2017 was posted on the advisory page of its website, https://midas.mtrcb.gov.ph/site/#!/advisories, and on its

---

[56] *Id.* at 9.
[57] Enforcement Division Letter Re: Compliance with National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 18 August 2022, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[58] *Id.* at 2.
[59] Letter Re: Compliance with National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 31 August 2022, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[60] *Id.* Annex A.
[61] *Id.* Annex B.
[62] *Id.* Annex C.
[63] Compliance, 03 November 2022, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).

official Facebook page.[64] To support this, MTRCB submitted a copy of the "Notice of Data Breach on 19 September 2017,"[65] a screenshot of MTRCB's advisory page where the Notice was posted,[66] and a screenshot of MTRCB's Facebook page,[67] The notification states:

> **NOTICE OF DATA BREACH ON 19 SEPTEMBER 2017**
>
> Pursuant to the approval for alternative means of notification by the National Privacy Commission in its Order dated 17 July 2022, the Movie and Television Review and Classification Board (MTRCB) seeks to advice all affected parties of the Data Breach subject of this Notice.
>
> On 19 September 2017, we became aware of an unauthorized access to our server. Upon investigation, we learned that a certain set of data from our server was locked due to a ransomware attack. The files within the data set were encrypted and renamed with a file extension. Said data may include the name and Tax Identification Number (TIN) of MTRCB personnel, as well as contracted vendors, and suppliers' business names.
>
> Of the two hundred seventy-four (274) user accounts affected, seventy-seven (77) were not notified because of lack of contact information.
>
> To date, there is still no indication of any unauthorized activity in connection to the user accounts affected by the data breach. Be that as it may, we have applied stricter data security measures, including the conduct of a vulnerability assessment to enhance MTRCB's data security.
>
> We have tasked our MTRCB Data Action Response Center to aid those who believe they may have been affected by the data breach. If you have concerns or need for further information, kindly contact them at 8376-7380 loc. 115.
>
> Again, we apologize for the inconvenience brought about by this incident.[68]

---

[64] Letter Re: Compliance with National Privacy Commission (NPC) Order dated 14 July 2022 for NPC BN 17-010, 03 November 2022, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[65] *Id.* Annex A.
[66] *Id.* Annex B.
[67] *Id.* Annex A.
[68] *Id.*

MTRCB also manifested that on 30 August 2022, it received the Compliance Letter dated 18 August 2022 from the EnD.[69] MTRCB stated that it had filed its compliance on 31 August 2022. It also stated that the hard copy of its letter dated 07 July 2022 with original or certified true copies of the annexes and the Final Vulnerability Assessment and Penetration Testing Report dated 27 May 2022 were sent to and received by the Commission on 01 September 2022.[70] MTRCB stated that "in the interest of limiting the exposure of the sensitive security matters contained in the Assessment," it hoped this initial submission last 31 August 2022 satisfied the Commission's directive in the Order dated 14 July 2022.[71] MTRCB also submitted a copy of the EnD's Compliance Letter dated 18 August 2022,[72] a screenshot of EnD's acknowledgment email dated 01 September 2022,[73] and finally, a screenshot of LBC Track and Trace.[74]

Issue

Whether the MTRCB conducted proper breach notification and management in compliance with NPC Circular 16-03.

Discussion

MTRCB conducted proper breach management through notification of data subjects through individual and alternative means, and implementation of security measures. Thus, the Commission resolves to close the matter.

The notification of data subjects is an essential obligation of a Personal Information Controller (PIC).[75] The purpose of notification is to provide data subjects with an opportunity to take the necessary precautions to protect their own data against the possible effects of the

---

[69] *Id.*
[70] Letter Re: Compliance with National Privacy Commission (NPC) Order dated 14 July 2022 for NPC BN 17-010, 03 November 2022, at 2, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[71] *Id.*
[72] *Id.* Annex D.
[73] *Id.* Annex E.
[74] *Id.* Annex F.
[75] NPC BN 21-035, 01 June 2021, at 4 (NPC 2021) (unreported).

breach.[76] As such, PICs are required to "establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach."[77]

Section 18 (C) of NPC Circular 16-03 (Personal Data Breach Management) provides the required contents of proper notification of affected data subjects:

> Section 18. *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> C. *Content of Notification.* The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;
> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
> 6. any assistance to be provided to the affected data subjects.
>
> Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.[78]

The notification sent to the affected data subjects must contain sufficient information on the nature of the breach incident, the personal data involved, the measures taken by the PIC to address the breach and to reduce harm or negative consequences of the breach, and the assistance it extended to its affected data subjects.[79]

---

[76] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (D) (15 December 2016).
[77] *Id.*
[78] *Id.* § 18 (C).
[79] NPC BN 18-198, 23 September 2021, at 4 (NPC 2021) (unreported).

MTRCB complied with the contents of notification required under Section 18 (C) of NPC Circular 16-03. Both the Notice dated 12 May 2021[80] and the "Notice of Data Breach on 19 September 2017"[81] narrated how the breach occurred through a ransomware attack and the information that was compromised, an explanation of the security measures taken by MTRCB to address the breach, and the contact number of its Data Action Response Center to enable the data subjects to obtain information and assistance. As such, both notifications, sent individually and through alternative means, enabled the affected data subjects to take measures to protect themselves from the consequences of the breach.

Further, Section 18 (D) of NPC Circular 16-03 provides the form of notification:

> Section 18. *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> D. *Form.* Notification of affected data subjects shall be done **individually, using secure means of communication, whether written or electronic.** The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and **to safeguard against further unnecessary disclosure of personal data.** The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish **means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.**[82]

---

[80] Letter Re: Compliance to the National Privacy Commission (NPC) Order No. CID BN 17-010, 18 May 2021, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2021).
[81] Compliance, 03 November 2022, Annex A, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[82] NPC Circ. No. 16-03, § 18 (D). Emphasis supplied.

The form of notification must be individual and must be made through secure means of communication, whether written or electronic.[83] The PIC must provide the data subject the means to exercise their rights and obtain more detailed information relating to the breach.[84]

MTRCB properly notified the affected data subjects through individual and alternative means of notification.

MTRCB individually emailed a copy of the Notice dated 12 May 2021 to the affected data subjects.[85] As proof, it attached a list of the two hundred seventy-four (274) data subjects' notification status[86] and copies of the individual email notifications it sent from 25 to 29 October 2021.[87]

In its Compliance with Motion dated 14 February 2022,[88] MTRCB submitted proof that one hundred three (103) out of one hundred seventy-seven (177) individuals notified through email acknowledged receipt.[89] Nonetheless, the EnD found that MTRCB's individual notification complied with the Commission's directive in the Compliance Order dated 31 January 2018:

> The EnD finds that MTRCB has exerted diligent efforts and exhausted available means to ascertain in entirety the contacts of the affected data subject from the records of its Board Secretary, Human Resources Unit, and the Property and Supply Unit. It even searched for the contacts of the next of kin of the deceased data subjects.
>
> To comply with EnD's Compliance letter dated 23 June 2022, informing MTRCB of the need to comply with the Decision of the Commission, MTRCB sent a letter dated 07 July 2022 and reported to the Commission that fifty-four (54) out of the seventy-four (74) individuals sent with Notice of Data Breach acknowledged its email. The remaining twenty (20) has yet to

---

[83] *Id.*
[84] *Id.*
[85] Letter Re: Compliance to the National Privacy Commission (NPC) Order No. CID BN 17-010, 18 May 2021, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2021).
[86] *Id.* Annex A.
[87] *Id.* Annex C.
[88] Compliance to the Order dated 15 April 2021 with Motion for Extension of Time to comply with Directives and for Permission for Other Modes of Public Notification, 14 February 2022, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[89] *Id.* Annex A-1 to A-103.

> acknowledge the email. To cure this lacking compliance, its IT Unit Head executed an affidavit with the attached acknowledgment receipt of the individuals who were sent notices attesting that she personally sent the email but has yet to receive the acknowledgment.[90]

In the Order dated 14 July 2022, the Commission considered MTRCB to have sufficiently individually notified all one hundred seventy- seven (177) affected individuals that were notified by email.[91] The Commission held:

> [T]he remaining seventy-four (74) data subjects, however, are still considered to have been sufficiently notified despite their lack of reply. The Circular on Personal Data Breach Management only mandates that the data subject be sufficiently informed and notified. Data subjects cannot be forced to respond to the notification, provided that proper notification is done. The obligation of the PIC to notify affected data subjects is fulfilled regardless of the data subject's response to the notification. What is important is that the email notification was sent and the data subject has access to the information contained in the notification should he or she need it.[92]

Section 18 (D) of NPC Circular 16-03 provides that a PIC may seek the Commission's approval to use alternative means of notification in lieu of individual notification in certain cases:

> Section 18. *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> D. *Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: ***Provided*, that where individual**

---

[90] Final Enforcement Assessment Report, 23 November 2022, at 9-12, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[91] Order, 14 July 2022, at 6, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[92] *Id.* at 6.

> **notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner:** *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[93]

In the Order dated 14 July 2022, the Commission granted MTRCB's request for alternative means of notification.[94] The Commission explained:

> The Commission acknowledges the diligent efforts exerted by MTRCB by attempting to locate the parties and going through its Board Secretary, Human Resources Unit, and Property and Supply Unit records. Given, however, that it does not have the contact information of the remaining affected data subjects and the next of kin of deceased data subjects, the Commission notes that individual notification to the remaining unnotified ninety- seven (97) data subjects is impossible. As such, the Commission grants the MTRCB's request for alternative means of notification for the remaining data subjects who have not been individually notified due to the unavailability of contact information despite its exhaustive efforts to locate them.[95]

Following this, MTRCB implemented notification through the use of alternative means provided in Section 18(D) of NPC Circular 16-03. It posted the "Notice of Data Breach on 19 September 2017" on the advisory page of its website, https://midas.mtrcb.gov.ph/site/#!/advisories,[96] and on its official Facebook page,[97] MTRCB attached screenshots of the posts to its compliance dated 03 November 2022 as proof.[98]

Further, the EnD found that the MTRCB implemented proper notification through alternative means in posting both the Notice of

---

[93] NPC Circ. No. 16-03, § 18 (D). Emphasis supplied.
[94] Order, 14 July 2022, at 7, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[95] *Id.*
[96] Letter Re: Compliance with National Privacy Commission (NPC) Order dated 14 July 2022 for NPC BN 17-010, 03 November 2022, Annex B, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[97] *Id.* Annex A.
[98] *Id.*

Data Breach (uploaded on 12 May 2021)[99] and the "Notice of Data Breach on 19 September 2017"[100] on its website:

> Both notifications describe the nature of the breach, which the MTRCB depicts as unauthorized access to its server due to a ransomware attack. It further identified the personal data possibly involved, i.e., the name and Tax Identification Numbers (TIN) of MTRCB personnel, contracted vendors, and supplier's business name. The second notification also provided measures taken by the MTRCB to address the breach such as strengthening its information security by implementing various and strict security measures, particularly the conduct of regular vulnerability assessments and the creation of projects that enhance the current security measure of the Agency. Lastly, the notification also informed the public that the MTRCB has set up the MTRCB Data Action Response Center []to assist those who may have been affected by the data breach in which information is accessed without authorization.[101]

Thus, MTRCB properly notified the remaining ninety-seven (97) data subjects through the use of alternative means of notification.

Finally, MTRCB complied with the directive to submit the results of an independent security audit.

MTRCB manifested that the audit was eventually and successfully completed on 27 May 2022.[102] It submitted its Final Vulnerability Assessment and Penetration Testing Report.[103] When the Commission issued the Order dated 14 July 2022 directing the submission of the results of the independent security audit,[104] MTRCB requested that the

---

[99] Letter Re: Compliance to the National Privacy Commission (NPC) Order No. CID BN 17-010, 18 May 2021, at 1, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2021).
[100] Compliance, 03 November 2022, Annex A, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[101] Final Enforcement Assessment Report, at 9, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).
[102] Letter Re: Compliance with National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 07 July 2022, at 3, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[103] Letter Re: Compliance with National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 31 August 2022, Annex B, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[104] Order, 14 July 2022, at 9, *in* In re: Movie and Television Review and Classification Board, NPC BN No. 17-010 (NPC 2022).

Commission consider its initial submission to the EnD as its compliance.[105]

The Commission considers MTRCB's submission to the EnD as its compliance with the directive in the Order dated 14 July 2022.

In the course of the audit, Next Generation identified "areas of weakness" and issues that should be resolved by MTRCB.[106] For its part, MTRCB manifested that its IT unit was working to implement these recommendations, "including procurement of a web application firewall and Endpoint Detection and Security Solution within the year."[107]

The EnD also conducted its own assessment of the MTRCB website https://midas.mtrcb.gov.ph and found that it was "likely vulnerable to digital attacks."[108] The EnD reported that while these findings that are significant, "they do not pose as much of a threat as high or critical."[109] It recommended that MTRCB update its website to address existing vulnerabilities and conduct periodical vulnerability assessment to address its "Medium to Low" risk level.[110]

The EnD also verified that MTRCB complied with the Commission's directives in Compliance Order dated 31 January 2018:

> Based on a careful review of the orders issued by the Commission En Banc and the available documents on record, the Enforcement Division finds that MTRCB has complied with the following directives: **(1) Appointment of a Data Protection Officer; (2) Creation of a Privacy Management Program based on risk assessment; (3) Implementation of appropriate organizational, physical and technical security measures** in accordance with the provisions of NPC Circular No. 16-01 on Security of Personal

---

[105] Letter Re: Compliance with National Privacy Commission (NPC) Order dated 14 July 2022 for NPC BN 17-010, 03 November 2022, at 2, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[106] Letter Re: Compliance with National Privacy Commission (NPC) Order No. CID BN 17-010 dated 15 April 2021, 07 July 2022, at 3, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2022).
[107] *Id.* at 4.
[108] Final Enforcement Assessment Report, at 12, *in* In re: Movie and Television Review and Classification Board, NPC BN 17-010 (NPC 2017).
[109] *Id.*
[110] *Id.*

> Data in Government Agencies and Submission of a progress report within six (6) months from receipt of the order.[111]

Given the foregoing, the Commission finds that MTRCB conducted proper breach notification and management in compliance with Section 18 (C) and Section 18 (D) of NPC Circular 16-03.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 17-010 In re: Movie and Television Review and Classification Board is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
13 July 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

(on official leave)
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

---

[111] *Id.* at 7-8. Emphasis supplied.

Office of the Executive Director
Movie and Television Review and Classification Board

ATTY. JSP
Data Protection Officer
Movie and Television Review and Classification Board

ATTY. CAN
Legal Affairs Division
Movie and Television Review and Classification Board

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: BUSINESS WORLD, INC. **NPC BN 18-006**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is the Full Breach Report dated 15 August 2022 submitted by Business World, Inc. (Business World) in compliance with the directive of the Commission in the Order dated 30 June 2022.[1]

Facts

Business World submitted its Initial Report dated 12 January 2018 informing the Commission that on 09 January 2018, it found a Facebook post of the group "Cyber-Chaos team" entitled "BusinessWorld database dump by Cyberchaos".[2] The Cyber-Chaos team claimed that it "played with [sic] online security" of Business World's online resource, www.bworldonline.com.[3]

According to Business World, it found that the list in the "data dump" included email addresses with the extension, "@bworldonline.com", and email addresses associated with other companies.[4]

Upon Business World's further investigation, it found that its new WordPress Content Management System (CMS) may have been compromised, including the personal details of thirty (30) of its

---

[1] Full Breach Report, 15 August 2022, *in* In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).
[2] Initial Report, 12 January 2018, at 1, *in* In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).
[3] *Id.*
[4] *Id.*

employees.[5] Business World reported that the compromised personal details were the employees' username, password, email address, first and last names, and administrative identification number.[6]

Business World also reported the following initial remediation steps to address the incident:

> 1. We contacted the Paste Bin site (where the relevant data was 'dumped') and, pursuant to our request, the lists that contain the personal data of the data subjects affected by this incident were taken down;
> 2. We initiated contacting the group Cyber-Chaos team and requested that they take down their post on the subject 'data dump'. At the same [time], we submitted a report to Facebook requesting that the relevant post on the subject 'data dump' be removed/taken down. To date, we are awaiting the response of Facebook to our take-down request;
> 3. We changed the root passwords and other related access rights/tools to the servers/systems that cater to our online resource/portal;
> 4. We are currently reviewing our online resource/portal to check whether there are other data 'missing', and/or have other 'malicious content';
> 5. We are currently crafting and implementing 'heightened security measures' on our servers and systems; and
> 6. Our breach management and response team already reached out to the affected data subjects concerning this incident.[7]

The Commission, through its Complaints and Investigation Division (CID), issued an Order dated 30 June 2022 directing Business World to submit its Full Breach Report within fifteen (15) days from receipt of the Order.[8]

On 29 July 2022, Business World requested an extension to submit its Full Breach Report until 14 August 2022.[9] It claimed that since the

---

[5] *Id.* at 1-2.
[6] *Id.* at 2.
[7] *Id.* at 2.
[8] Order (To submit Full Breach Report), 30 June 2022, at 1, *in* In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).
[9] Email *from* JDN, Business World, Inc., *to* Complaints and Investigation Division, National Privacy Commission (29 July 2022).

incident, there were manpower changes in the company and that the employee who reported the incident to the Commission is no longer connected with the company.[10]

On 01 August 2022, the CID resolved to grant Business World's
request and directed it to submit the Full Breach Report within fifteen
(15) days or until 15 August 2022.[11]

On 15 August 2022, Business World submitted its Full Breach Report.[12] It reported that on 08 January 2018 it received an email about the incident from "an affected user outside of Business World," who claimed that only her email address was exposed due to the breach.[13]

Upon investigation, Business World discovered that the WordPress version it was using "became the entry point of the hackers to conduct a Structured Query Language (SQL) Injection.[14] Thereafter, the Cyber-Chaos team reportedly posted the "data dump" on pastebin.com.[15]

Further, Business World reported that the incident occurred when it was migrating its database from the old BusinessWorld website to the new WordPress-based site.[16]

Business World informed that the incident affected thirty (30) employees and one thousand four hundred seventy-five (1,475) individuals outside Business World.[17] It identified that as to the affected employees, the data exposed included the employees' username and password for the old website, their email address with the extension "@bworldonline.com", and the employees' first and last

---

[10] *Id.*
[11] Resolution of Motion for Extension, 01 August 2022, at 1, *in* In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).
[12] Email *from* ASD, Business World, Inc., *to* Complaints and Investigation Division, National Privacy Commission (15 August 2022).
[13] Full Breach Report, 15 August 2022, at 1, *in* In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.* at 2.

name.[18] As to the affected individuals outside Business World, their email addresses were exposed.[19]

With regard to the measures it took to minimize harm or mitigate the impact of the breach, Business World reported the following:

> i. We have built our own Wordpress site that is no longer dependent on 7th Media's customizations, enabling us to set updates to automatic, helping ensure that we are protected from exploits discovered of the said CMS
> ii. Usernames and passwords were randomly generated so that anyone trying to do a brute force attack will have a very difficult time
> iii. Passwords of users are reset every month
> iv. The URL of the login screen is changed every month
> v. The login screen has been geo-blocked and can only be accessed by Philippine IP addresses
> vi. We have changed hosting services to Conversant Content Delivery Network (CDN) and Web Application Firewall (WAF)...we have not been hacked since.
> vii. We have installed Wordpress plugins such as Succuri Security and Blackhole for Bad Bots as additional layers of protection for our website.
> viii. Plugins are updated every Friday
> ix. The Wordpress Database is cleaned and optimized every Friday
> x. The old database that was compromised has been taken offline immediately after the incident has been discovered
> xi. Server credentials are changed every month.
> xii. No users from outside BusinessWorld are registered in the Wordpress CMS[.][20]

According to Business World, it informed affected employees personally and sent notification letters to affected non-employees about the incident and the measures that must be done.[21] As proof of its notification to the affected individuals outside the company, Business World submitted a copy of the notification letter dated 17 January 2018.[22]

---

[18] *Id.*
[19] Full Breach Report, 15 August 2022, at 2, *in* In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).
[20] *Id.* at 2-3.
[21] *Id.* at 3.
[22] *Id.* Annex.

Issue

Whether Business World sufficiently complied with the Order dated 30 June 2022.

Discussion

The Commission resolves to close the case upon finding that Business World sufficiently complied with the Order dated 30 June 2022. Business World sufficiently notified the affected data subjects and implemented measures to prevent the recurrence of the breach.

The notification letter dated 17 January 2018 that Business World sent to its affected individuals included the information required under NPC Circular 16-03 (Personal Data Breach Management). Section 18
(C) of NPC Circular 16-03 provides:

> Section 18. *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> C. Content of Notification. The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;
> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
> 6. any assistance to be provided to the affected data subjects.

> Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.[23]

In the letter-notification dated 17 January 2018, Business World informed the affected data subjects of the nature of the breach by reporting that the hacker group Cyber-Chaos team claimed that it gained access to Business World's data and posted the data online.[24] It further identified that the incident involved the email addresses of Business World's subscribers.[25]

Business World assured the affected data subjects that the website, where the email addresses were posted, has been immediately taken down.[26] It also informed the affected data subjects that it has taken action "to further strengthen the security of [its] system" and advised them to regularly change their passwords.[27]

The letter dated 17 January 2018 also specified Business World's email address, where affected data subjects can ask for further information regarding the breach.[28]

Given the foregoing, the Commission finds that Business World has sufficiently notified the affected data subjects of the breach.

In addition, the Commission notes the remedial measures taken by Business World. Business World built its own WordPress site that enables automatic updates and it implemented additional layers of security on its website for protection against vulnerabilities it has identified.[29] It also took down the old database that was compromised immediately after the discovery of the incident.[30]

---

[23] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §18 (C) (15 December 2016).
[24] Full Breach Report, 15 August 2022, Annex, *in* In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.* at 2.
[30] Full Breach Report, 15 August 2022, at 3, *in* In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).

Business World's random generation of usernames and passwords and the monthly resetting of the passwords provide more security and protection to the personal data of the data subjects.[31] These measures are sufficient to address the breach and prevent the recurrence of the incident.

WHEREFORE, premises considered, Commission resolves that NPC BN 18-006 – In Re: Business World, Inc. is hereby **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
10 November 2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

ASD
Data Protection Officer
Business World, Inc.

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

---

[31] *Id.* at 2.

JRC,

Complainant,

-versus-

NPC 21-218

For: Violation of the Data Privacy Act of 2012

BANK OF THE PHILIPPINES ISLANDS
Respondents.

x----------x

RESOLUTION

Before this Commission is the Mediated Settlement Agreement between JRC (Complainant) and Bank of the Philippines Islands (Respondent).

Facts

On 03 September 2021, the instant complaint[1] was filed with the NPC Complaints and Investigation Division based on the following facts:

> Last July 1, 2021 at 2:15PM, I was a victim of [ph]ishing scam. I received a call form MM with CP number XXX who introduces herself as an employee of BPI Head Office wherein she offered me to waive my credit card annual fee for lifetime because I have a good credit standing. She asked my last 4 digit credit card number, confirmed the expiration, asked the batch number which is the CVV for verification purposes so that I can avail the offer. I solely entrusted to this person that she was a BPI legit employee because all I know, only BPI known my Credit Card Information. My credit card issued only last March, 2021. I never used my credit card online. They can check my past purchases

[1] Complaints Assisted Form dated 02 September 2021.

> which is only limited. So how come that this scammer had known my Credit Card Account Information? There were a leakage of my personal information. I entrusted BPI to collect it because I know it is confidential. They cannot protect their client information. It is unfair that I shouldered payment for this fraudulent transaction because of their negligence. They must do an urgent action to help their client about this kind of incident so that as a cardholder felt secured to this reputable bank since I reported it immediately. I am hoping for your consideration and resolution on this matter. Thank you!"[2]

On 14 April 2022[3] and 20 April 2022,[4] Complainant and Respondent filed their Application for Mediation, respectively, and the mediation conferences were conducted on the following dates: 10 May 2022;[5] 07 June 2022;[6] 28 June 2022;[7] 12 July 2022;[8] 25 July 2022;[9] 01 August 2022;[10] and 08 August 2022.[11]

Despite the Order to Mediate dated 01 August 2022[12] to further conduct mediation conference on 08 August 2022, through the sincere effort of the parties to arrive at an amicable resolution of their dispute, they were able to execute a Mediated Settlement Agreement (MSA) on 05 August 2022.[13] In the MSA, the parties agreed, among others, that:

> 3. The Complainant undertakes to pay Respondent the amount of Php 31,250.03. Complainant shall remit to Respondent ONE THOUSAND THREE HUNDRED TWO PESOS AND EIGHT
> CENTS (Php 1,302.08) per month for twenty-four (24) months starting September 2022 up to August 2024. The payment shall follow the usual process of paying the bank's credit card transactions.
>
> 4. The Respondent undertakes (1) to furnish the Commission a copy of Complainant's monthly statement of account as proof of compliance within ten (10) days from the billing's due date, and
> (2) within ten (10) days after the end of the 24-month period, to

---

[2] *Id.*
[3] Application for Mediation of Complainant dated 14 April 2022.
[4] Application for Mediation of Respondent dated 20 April 2022.
[5] Order to Mediate dated 25 April 2022
[6] Order to Mediate dated 31 May 2022
[7] Order to Mediate dated 07 June 2022
[8] Order to Mediate dated 28 June 2022
[9] Order to Mediate dated 12 July 2022
[10] Order to Mediate dated 25 July 2022
[11] Order to Mediate dated 01 August 2022
[12] Supra, Note 10.
[13] Mediated Settlement Agreement dated 05 August 2022.

issue a completion certificate or acknowledgement stating the payment of the full amount herein stated.[14]

Discussion

Rule III, Section (e)(3) of the Implementing Rules and Regulations of the Data Privacy Act of 2012 provides:

> The Commission shall adjudicate on complaints and investigations on matters affecting personal data: Provided, that in resolving any complaint or investigation, except where amicable settlement is reached by the parties, the Commission shall act as collegial body. This includes:
>
> xxx
>
> 3. **Facilitating or enabling settlement of complaints through the use of alternative dispute resolution processes, and adjudicating on matters affecting any personal data**[.][15] (Emphasis Supplied)

The parties formally expressed their intention to mediate the case by filing their Application for Mediation dated 14 April 2022[16] and 20 April 2022,[17] respectively. Pursuant to the Commission's power to facilitate or to enable settlement of complaints through alternative dispute resolution processes,[18] the parties were invited to a Mediation Conferences on 10 May 2022;[19] 07 June 2022;[20] 28 June 2022;[21] 12 July 2022;[22] 25 July 2022;[23] 01 August 2022;[24] and 08 August 2022.[25]

Before the scheduled Mediation Conference on 08 August 2022,[26] the parties agreed to settle their differences through the execution of an

---

[14] Id. at pages 1-2.
[15] Rule III, Section (e)(3) of the Implementing Rules and Regulations of the Data Privacy Act of 2021
[16] Application for Mediation of Complainant dated 12 April 2022.
[17] Application for Mediation of Respondent dated 20 April 2022.
[18] Supra. Note 8
[19] Supra, Note 5.
[20] Supra, Note 6.
[21] Supra, Note 7.
[22] Supra, Note 8
[23] Supra, Note 9.
[24] Supra, Note 10
[25] Supra, Note 11
[26] *Id.*

MSA dated 05 August 2022. The contents of the MSA were thoroughly explained to and understood by the parties.

After a thorough study and adjudication of the case, the Commission finds that the MSA dated 05 August 2022, executed by and between Complainant and Respondent is not contrary to law, public policy, morals, or good customs.

Thus, this Commission finds the executed MSA dated 05 August 2022, executed by and between Complainant and Respondent, as valid and enforceable. The parties are reminded to strictly observe its terms and conditions.

WHEREFORE, premises considered, this Commission resolves to **CONFIRM** the Mediated Settlement Agreement dated 05 August 2022 executed by and between the Complainant, JRC and Respondent, Bank of the Philippines Islands.

IN VIEW OF THE FOREGOING, the Enforcement Division (EnD) is enjoined to monitor the permanent deletion of personal information in relation to the remittances after the lapse of the data retention period. Further, the EnD is directed to require Respondent to submit within ten (10) days from receipt of the Resolution the monthly due date of Complainant's credit card.

SO ORDERED.

City of Pasay, Philippines.
19 August 2022.

JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

JRC
Complainant

BPI LEGAL AFFAIRS AND DISPUTE RESOLUTION DIVISION
Counsel for Respondent
Attn: BDN

LEGAL DIVISION ENFORCEMENT DIVISION GENERAL RECORDS UNIT
National Privacy Commission

IN RE: LEAPFROGGR, INC. **NPC BN 18-229**

x----------x

RESOLUTION

NAGA, *P.C.;*

Before the Commission is the Compliance submitted by Leapfroggr, Inc. (Leapfroggr) to the Order of the Commission dated 10 November 2022.

Facts

On 10 November 2022, the Commission issued an Order requiring Leapfroggr "to submit an affidavit, sworn oath or its equivalent showing proof of notification to the two affected data subjects, the contents of the notification, and the corresponding receipt of the notification."[1] The dispositive portion of the Order reads:

> **WHEREFORE,** premises considered, **LEAPFROGGR, INC.** is hereby **ORDERED** to **SUBMIT** proof of notification to the affected data subjects **within fifteen (15) days** from the receipt of this Order:
>
> **SO ORDERED.[2]**

On 21 December 2022, Leapfroggr submitted its compliance with the Order wherein it attached separate affidavits of LYB[3]and TMR.[4]

Issue

---

[1] *In re: Leapfroggr, Inc.*, NPC BN 18-229, Order dated 10 November 2022, at p. 4
[2] *Id.*
[3] Affidavit dated 21 December 2022 of LYB.
[4] Affidavit dated 21 December 2022 of TMR.

Whether Leapfroggr sufficiently complied with Commission's Order dated 10 November 2022.

Discussion

The Commission finds that Leapfroggr has sufficiently complied with the Order dated 10 November 2022.

As reflected in the submissions made by Leapfroggr, the affidavits of LYB and TMR sufficiently proved that it actually notified the affected data subjects.

Rule V, Section 18 (D) of NPC Circular No. 16-03 (Personal Data Breach Management) provides:

> D. *Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. **The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified**, and to safeguard against further unnecessary disclosure of personal data. **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach**[.] x x x *Provided further*, that the personal information controller shall establish means through which the **data subjects can exercise their rights and obtain more detailed information relating to the breach.**[5]

In the Order dated 10 November 2022, the Commission noted that Leapfroggr's attachment of screenshots of email notifications to TMR and LYB in its Post-Breach Report dated 03 February 2022 were inadequate to prove that the email was received by TMR.[6] Thus, Leapfroggr was ordered to submit an affidavit showing proof of notification to the affected data subjects.[7]

---

[5] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18(D) (15 December 2016) (NPC Circular 16-03).
[6] *In re: Leapfroggr, Inc.*, NPC BN 18-229, Order dated 10 November 2022, at p. 3
[7] *Id.*, at p. 4

Accordingly, Leapfroggr submitted its compliance containing two (2) separate affidavits from TMR and LYB stating that they received an email from Leapfroggr dated 29 November 2018 notifying them of a data breach incident.[8]

This Commission finds that these affidavits submitted by Leapfroggr, containing statements that the email notifications were received by TMR and LYB, are sufficient proof that it has indeed notified the affected data subjects of the incident.

Moreover, the email notifications dated 29 November 2018 provided detailed information relating to the breach.[9] Leapfroggr explained that in its usual export process, its "system schedules the export and when it can start automatically converting *[sic]* patient profiles to Word documents."[10] When the process is done, a zip file protected by a password, is created and a message will be generated which is sent to the "messenger inside the SeriousMD application."[11]

Further, Leapfroggr explained that the generated message "should have been an automated message but [it] manually sent the generated message instead."[12]

In addition, Leapfroggr stated that in addressing the breach, the erroneous message and the exported file were deleted immediately,[13] the export process was changed,[14] and the manual sending of files was disabled, changing the process to automated sending.[15]

The Commission reminds the personal information controllers (PICs) like Leapfroggr, and personal information processors (PIPs) of their obligation under the Data Privacy Act of 2012 (DPA). Under the DPA, notification to the affected data subjects is required especially in breach cases that involves sensitive personal information or other information that may be used to enable identity fraud and are reasonably believed

---

[8] Affidavits dated 21 December 2022 of LYB Land TMR.
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] Affidavits dated 21 December 2022 of LYB and TMR.
[13] *Id.*
[14] *Id.*
[15] *Id.*

to have been acquired by an unauthorized person, which may likely give rise to a real risk of serious harm to the affected data subjects.[16]

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-229 "In re: Leapfroggr, Inc." is hereby considered **CLOSED.**

SO ORDERED.

City of Pasay, Philippines. 19 January 2023.

JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

---

[16] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter V, § 20 (f) (2012).

SS
Data Protection Officer

BDC
Head of the Organization

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: ASIA UNITED BANK CORPORATION **NPC BN 22-107**

x----------x

RESOLUTION

NAGA, *P.C.;*

Before the Commission are the requests for exemption from the requirement of notification of affected data subjects and extension to submit full report submitted by Asia United Bank Corporation (AUB) dated 25 July 2022.

Facts

On 25 July 2022, AUB submitted to the Commission an initial report of a data breach through the Data Breach Notification Management System (DBNMS).[1]

Based on the initial report, AUB stated that during the onset of the pandemic, delays in the handover of delivery receipts occurred due to the minimal workforce of Entrego, its service provider.[2] AUB made continuous follow-ups with Entrego to surrender the required delivery receipts, but to no avail.[3] It was only on 18 July 2022 that Entrego reported to AUB that certain delivery receipts that serve as proof of delivery of credit cards were lost.[4]

---

[1] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Date of Notification of Asia United Bank Corporation (25 July 2022).
[2] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.b Chronology.
[3] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.b Chronology.
[4] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.a How breach occurred + DPS Vulnerability.

AUB reported that there are two hundred sixteen (216) recorded affected data subjects.[5] However, AUB added that "the recipients of the two hundred sixteen (216) delivered credit cards are not the cardholders themselves."[6] AUB stated that:

> However, if it is to be assumed that the recipients of the 216 delivered credit cards are not the cardholders themselves, then a maximum of 432 (i.e., 216 x 2) data subjects may expected *(sic)* to be affected - however, this number is highly speculative. It must be stressed that there are no copies of government-issued identification documents collected by Entrego - delivery receipts only state type of identification card and corresponding identification card number of the recipient of delivery.[7]

As for the personal data involved, AUB reported that the "[g]overnment-issued ID number unique to cardholder *(sic)* authorized representative; the fact that an AUB credit card was issued to a specific person" is information that may enable identity fraud.[8]

For the measures taken to address the breach, AUB stated that:

> While it does not seem to be possible to recover/locate the lost delivery receipts, the affected delivered credit cards are in the process of being verified as having been successfully delivered to the correct cardholders. Based on initial investigation results, credit cards successfully reached the cardholders and have not been involved in fraud.[9]

Moreover, AUB reported that the security or recovery of personal data is "not possible under the circumstances."[10] In mitigating the harm, AUB also declared that an investigation was undertaken to determine

---

[5] *In re: Asia United Bank Corporation,* NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.c Number of DS/Records.
[6] *In re: Asia United Bank Corporation,* NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.c Number of DS/Records
[7] *In re: Asia United Bank Corporation,* NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.c Number of DS/Records.
[8] *In re: Asia United Bank Corporation,* NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 2.b. Other info that may enable identity fraud. [9] *In re: Asia United Bank Corporation,* NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.a Measures to address the breach.
[10] *In re: Asia United Bank Corporation,* NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.b. Measures to secure/recover personal data?

if any of the delivered credit cards had been involved in fraud.[11] AUB reported that based on the investigation, the credit cards were successfully delivered to the cardholders, and no fraud had occurred.[12]

AUB is then requesting for exemption from the requirement of notification of the affected data subjects.[13] It stated that the request is "being made because it is unlikely that the breach will give rise to a real risk to the rights and freedoms of data subjects; rather, notification may cause unnecessary panic to cardholders."[14] AUB also mentioned that:

> [I]t is not possible to trace who the actual delivery recipients had been other than to confirm whether the cardholders in fact eventually received the delivered credit cards. As such, it is not possible to undertake notification if the delivery recipient (whose name, signature and ID details are printed on a delivery receipt) is a person other than the cardholder.[15]

AUB is also requesting a fifteen-day extension "to submit full report in order to give time for the completion of the investigation. Progress of investigation is dependent on response time/quality of feedback from Entrego."[16]

In a Minute Resolution dated 07 November 2022, the Commission resolved the requests for exemption and extension with the following dispositive portion:

> **WHEREFORE,** premises considered, the Commission hereby **ORDERS** Asia United Bank Corporation to **SUBMIT** within fifteen (15) days upon receipt of this Minute Resolution the following:

---

[11] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.c Actions to mitigate harm?
[12] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.c Actions to mitigate harm?
[13] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), in Justification for Exemption.
[14] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), in Justification for Exemption.
[15] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), in Justification for Exemption.
[16] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), in Explain the reason for the request for extension of time to submit.

> (1) Proof to substantiate the request for Exemption and Extension;
> (2) Further details and evidence of the security measures that have been implemented in response to the breach; and
> (3) Full Breach Report.
>
> Should Asia United Bank Corporation fail to provide the foregoing documents, this case shall be submitted for resolution based on the records before the Commission.
>
> **SO ORDERED.** [17]

Subsequently, AUB submitted its Compliance dated 22 November 2022 which contains the "full report of security incident,"[18] attaching thereto a "Certificate of Delivery of Parcel" from Entrego,[19] and a Certification from MVS, the incumbent Senior Vice President and Cards Business Group Head of AUB.[20]

Further, AUB attached in its full report copies of the Certificates of Delivery Parcel issued by Entrego and clarified that "there are two hundred eighty-seven (287) individuals affected by the alleged breach" consisting of the "cardholders and/or the credit card recipients."[21]

Issue

Whether to grant AUB's requests for (1) exemption from notification of affected data subjects and (2) extension to submit its full report.

Discussion

The Commission resolves to deny the requests for (1) exemption from notification of data subjects and (2) a fifteen-day extension to submit its full report.

---

[17] *In re: Asia United Bank Corporation*, NPC BN 22-107, Minute Resolution dated 07 November 2022, at p. 1.
[18] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation.
[19] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, Annexes "A" and "B".
[20] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, Annex "C".
[21] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, in p. 2.

I. The incident falls under the mandatory notification requirements.

The Commission finds that the incident falls within the scope of mandatory breach notification requirement, thus, notification of the affected data subjects is necessary to protect them from the risk of serious harm.

Rule V, Section 11 of NPC Circular No. 16-03 (Personal Data Breach Management) provides:

> **SECTION 11.** ***When notification is required.*** Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:
>
> A. The personal data involves **sensitive personal information or any other information that may be used to enable identity fraud.** For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> B. There is reason to believe that the **information may have been acquired by an unauthorized person**; and
>
> **C.** The personal information controller or the Commission believes that **the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.**[22] (Emphasis supplied.)

Based on the records, all the abovementioned requirements for mandatory breach notification are present.

First, AUB listed government-issued identification (ID) numbers as sensitive personal information.[23] AUB also reported that the

---

[22] NPC Circular No. 16-03, Rule V, § 11.
[23] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 3.

cardholder's full name, delivery address, as well as the credit card recipient's name, and signature are information that may be used to enable identity fraud.[24]

To note, government-issued IDs with peculiar information pertaining to an individual are considered sensitive personal information.[25] As regards the cardholder's full name, delivery address, credit card recipient's name, and signature, such information may be used to enable identity fraud. Further, these can be obtained wrongfully by another person and may be used by them to perpetuate fraud or deception, usually for economic gain. Here, the fact that the lost proofs of delivery pertain to credit cards, the data about the financial situation of the data subjects are also involved.

The second requirement is also present in this case. AUB mentioned in its initial report that:

> In case certain lost delivery receipts were lost/misplaced outside the premises of Entrego, **there is a possibility that said delivery receipts would find their way to malicious persons.** However, malicious/unauthorized usage may be limited given the breadth of information involved.[26]

Accordingly, AUB undertook an investigation to determine if the "delivered cards had been involved in fraud."[27] AUB reported that the credit cards had "successfully reached the cardholders and have not been involved in fraud."[28] However, AUB failed to sufficiently prove that indeed, no fraud has occurred. In its full report dated 22 November 2022, AUB failed to discuss the likely consequences of the lost delivery receipts.[29] Rather, AUB emphasized that the incident is attributable to Entrego.[30]

---

[24] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 3.
[25] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 3(l)(3) (2012).
[26] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.e Likely Consequences
[27] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.c Actions to mitigate harm?
[28] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.c Actions to mitigate harm?
[29] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 2.
[30] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 2.

Lastly, since AUB failed to sufficiently show that no fraud has occurred due to the lost of delivery receipts, the Commission finds that the personal and sensitive personal information involved can lead to potential harm or negative consequences to the credit cardholders or their authorized representatives. Thus, Section 11(C) of NPC Circular No. 16-03 applies.

It is noteworthy that AUB, as Personal Information Controller (PIC) has the obligation to notify the affected data subjects in case of breach which is within the scope of mandatory notification requirement. Thus, AUB is required to notify the affected data subjects in order to allow them to take the necessary steps or other measures to protect themselves against the negative effects of the breach.

II. Exemption from notification may be authorized by the Commission if such notification would not be in the public interest or in the interest of the affected data subjects.

AUB justifies its request for exemption by stating that the "notification may cause unnecessary panic to cardholders."[31] AUB also stated that "it is not possible to trace who the actual delivery recipients had been other than to confirm whether the cardholders in fact eventually received the delivered credit cards."[32] The Commission finds this justification unwarranted since in its full report, AUB was able to furnish this Commission copies of certificates of delivery of the credit cards showing the names of the recipients.[33]

Rule V, Sections 18 (A) and (B) of NPC Circular No. 16-03 provide:

> A. *When should notification be done.* **The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief** by the personal information controller or personal information processor that a personal data breach has occurred.[34] (Emphasis supplied)

---

[31] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Justification for Exemption.
[32] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Justification for Exemption.
[33] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 2.
[34] NPC Circular 16-03, Rule V, § 18(A).

> B. *Exemption or Postponement of Notification.* If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification. **A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.** The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.[35] (Emphasis supplied)

In this case, AUB requested for exemption from notifying the data subjects since "it is unlikely that the breach will give rise to a real risk to the rights and freedoms of data subjects; rather, notification may cause unnecessary panic to cardholders."[36] Section 18(A) of NPC Circular No. 16-03 requires the PIC to notify the affected data subjects within seventy- two (72) hours upon knowledge or reasonable belief that a breach has occurred. Section 18(B) thereof provides that exemption from notifying the data subjects may be granted if the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.

AUB failed to show proof that such notification would not be in the public interest or in the interest of the affected data subjects to warrant the exemption from notifying the affected data subjects. Even though this Commission has ordered AUB to submit proof substantiating its requests for exemption, AUB still failed to do so.[37]

Thus, for failure to notify the affected data subjects within seventy- two (72) hours upon knowledge or reasonable belief of the occurrence of the breach, the Commission deems it proper for AUB to notify the two hundred eighty-seven (287) individuals affected. This is for them to take the necessary measures to protect themselves against the potential negative consequences resulting from the breach.

---

[35] NPC Circular 16-03, Rule V, § 18(B).
[36] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Justification for Exemption.
[37] *In re: Asia United Bank Corporation*, NPC BN 22-107, Minute Resolution dated 07 November 2022, at p. 1.

III. AUB is required to submit its Full Breach Report

In its Initial Report, AUB reported that based on its investigation, the credit cards were successfully delivered to the cardholders and no incident of fraud has occurred.[38] However, AUB failed to make a report on the actions taken to inform the data subjects regarding the breach.[39]

On the other hand, the full incident report of AUB dated 22 November 2022 does not mention any actions taken to inform the affected data subjects. Rather, it emphasized on Entrego's responsibility to deliver the credit cards to the cardholders and AUB's direct control is limited only to the issuance of credit cards.[40] AUB also stated that:

> On the viewpoint of AUB, all credit cards subject of delivery by Entrego are in inactive/blocked status, and upon receipt by the relevant cardholders, require activation by each cardholder through a standard verification process.
>
> ...
>
> As such, while unfortunate, AUB deems it unnecessary at this time to inform the Data Subjects on the loss of the delivery receipts. Notifying the Data Subjects of this incident may cause unnecessary panic on the part of the Data Subjects and blow the matter out of proportion, making it appear that the security measures of AUB are lax – although the loss of delivery receipts was accidental and purely attributable on the part of Entrego, a reputable courier. This reputational risk on the part of AUB will cause AUB irreparable harm as a financial institution with good standing, outweighing whatever imagined benefits there are to notifying the Data Subjects on such loss.[41]

However, this Commission finds that AUB shall submit its Full Breach Report containing the complete information required provided in Section 17(D) of the NPC Circular No. 16-03, including but not limited to the measures to secure/recover personal data and actions

---

[38] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.a Measures to address the breach; *see* 3.c Actions to mitigate harm?
[39] *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.d. Actions to inform data subjects.
[40] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 4.
[41] DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 4.

performed or proposed to mitigate possible harm, among others.[42] In addition, the Commission also finds that AUB must submit proof of security measures it implemented as reported in its Initial Report dated 25 July 2022 and Full Incident Report dated 22 November 2022.

WHEREFORE, premises considered, this Commission resolves that the request for exemption and extension from the requirement of notification of the two hundred eighty-seven (287) affected data subjects of Asia United Bank Corporation (AUB) is hereby **DENIED**.

AUB is **ORDERED,** within fifteen (15) days from receipt of this Resolution, to comply with the following:

1. **NOTIFY** the affected data subjects including the proof receipt of the data subjects of such notification;

2. **SUBMIT** its Full Breach Report; and

3. **SUBMIT** proof of security measures to address the breach.

SO ORDERED.

City of Pasay, Philippines.
01 December 2022.

JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

---

[42] NPC Circular 16-03, Rule V, § 17(D).

Copy furnished:

EMC
Data Protection Officer

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: DEPARTMENT OF TRADE AND INDUSTRY **NPC BN 18-220**

x----------x

IN RE: DEPARTMENT OF TRADE AND INDUSTRY – RIZAL PROVINCIAL OFFICE **NPC BN 18-231**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission are the breach notifications submitted by the Department of Trade and Industry (DTI) and the Department of Trade and Industry – Rizal Provincial Office (DTI-Rizal) involving the forcible entry of unauthorized persons resulting in the loss of office equipment such as laptops and storage devices.

Facts

On 11 November 2018, DVG, a member of DTI-Rizal's utility staff called ROP, an administrative staff officer, to inform the latter that the DTI- Rizal office was robbed.[1]

According to DVG, he discovered the gate of the office was unlocked and the windows and drawers were opened.[2] He narrated that "papers were scattered on the floor and it suggested that someone entered the office and searched for something."[3]

---

[1] Incident Report, 27 November 2018, Annex A, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2018).
[2] *Id.*
[3] *Id.*

When ROP arrived at the office, the Philippine National Police (PNP) of Rizal was already conducting the investigation.[4] The Scene of the Crime Operatives (SOCO) also assisted in the investigation and identified that the following items were taken from the DTI-Rizal Office: two (2) laptops, two (2) external hard drives, one (1) power bank, one (1) camera, one (1) cap, and Three Thousand Pesos (Php 3, 000.00) in cash.[5]

With the help of the PNP, DTI-Rizal recovered one (1) hard drive.[6] The two (2) laptops and the other hard drive, however, remain unrecovered.[7]

According to DTI-Rizal, the laptops were used for the One Town One Product Staff (OTOP) program of DTI-Rizal and contained the following files: (1) OTOP videos, (2) photos involving OTOP owners,
(3) photos of seminar speakers, and (4) photos of DTI-Rizal staff.[8] The OTOP Program is a "DTI-wide stimulus program locally implemented by DTI-Rizal to assist Micro, Small, and Medium-scale enterprises (MSMEs)."[9]

Meanwhile, the hard drives were mainly used by DTI-Rizal's Negosyo Center Business Counselor.[10] It contains the following files: (1) an OTOP Directory including the name of business, name of business owner, contact numbers, and e-mail address, (2) OTOP seminar files including proposals, post-activity reports, client satisfaction feedback, and post training evaluation reports, (3) accomplishment reports including full name and designation of the account officers, (4) action photos of seminars and activities from January to November 2018, (5) collaterals, (6) blank International Organization for Standardization (ISO) forms, and (7) forty (40) MSME Business Permit files which include scanned copies of valid business name certificates and 2018

---

[4] *Id.*
[5] Breach Notification, 27 November 2018, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2018).
[6] *Id.*
[7] Full Breach Report, 03 January 2022, at 5, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[8] *Id.* at 3.
[9] Compliance, 29 July 2022, Annex D, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[10] Full Breach Report, 03 January 2022, at 4, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).

Mayor's Permits.[11] These permits include business name, business territorial scope, full name of business owner, business certificate number, and expiration date.[12] The hard drives were reported to be unencrypted.[13]

DTI-Rizal stated that the incident involved three (3) alleged suspects, two (2) of which are minors.[14] The two (2) minor suspects sold the unrecovered items and were eventually apprehended by the law enforcement officers.[15]

On 12 November 2018, DTI-Rizal notified the forty (40) affected data subjects who are MSME business permit owners through Short Message Service (SMS).[16]

DTI-Rizal attached an affidavit of KPL, an employee of DTI-Rizal, evidencing that she has personally informed all the data subjects about the incident.[17]

On 27 November 2018, DTI and DTI-Rizal notified the National Privacy Commission (NPC) of the security incident.[18]

On 08 October 2020, the NPC, through the Complaints and Investigative Division (CID), issued an Order requiring DTI-Rizal to submit a Full Report detailing the incident with emphasis on the lacking information from its initial notification.[19]

---

[11] *Id.*
[12] *Id.*
[13] *Id.* at 2.
[14] Breach Notification, 27 November 2018, Annex A, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2018).
[15] Full Breach Report, 03 January 2022, at 5, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[16] *Id.* at 4.
[17] Compliance, 26 May 2022, Annex D, *in* In Re: Department of Trade and Industry, NPC BN 18- 220 and NPC BN 18-180 (NPC 2022).
[18] Breach Notification, 27 November 2018, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2018).
[19] Order, 08 October 2020, at 1, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2020).

On 22 October 2020, DTI-Rizal submitted its Compliance with the Order dated 08 October 2020.[20]

On 29 April 2021, the CID sent a letter addressed to DTI-Rizal clarifying whether: (1) there were actual sensitive and other personal information stored in the laptop, (2) the unauthorized acquisition may lead to serious risks such as enabling identity fraud, (3) the stolen laptops were password protected to avoid unauthorized access to the files.[21] The CID also requested an update on the progress of the final investigation of the security incident and as well as the status of equipment retrieval and file recovery.[22]

With respect to NPC BN 18-220 In re: DTI, a breach notification involving the same incident, the CID issued an Order on 07 December 2021 requiring DTI to submit a Full Report expounding on the details stated in the initial notification report to further help with the investigation of the breach incident.[23]

On 23 December 2021, DTI requested for an additional fifteen (15) calendar days to comply with the Order dated 07 December 2021.[24]

On 24 December 2021, the CID granted DTI's request for extension.[25]

On 27 December 2021, DTI-Rizal conducted a Privacy Impact Assessment (PIA) on DTI-Rizal's OTOP Program.[26]

---

[20] Compliance, 22 October 2020, at 1, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2020).
[21] Letter of the CID to DTI, 29 April 2021 at 1, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2021).
[22] *Id.*
[23] Order (To Submit Full Breach Report), 07 December 2021, at 1, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2021).
[24] Letter of DTI to CID, 23 December 2021, at 1, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2021).
[25] Resolution of the Motion for Extension of Time dated 23 December 2021, 23 December 2021, at 1, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2021).
[26] Letter of DTI to CID, 29 July 2022, Annex D, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).

On 03 January 2022, DTI submitted its Full Report detailing the security incident.[27]

On 10 May 2022, the CID ordered DTI to submit a Post-Breach Report containing the proper documentation on the actions taken within fifteen (15) days from receipt of said Order.[28] On 30 September 2022, the CID issued a similar Order to DTI-Rizal.[29]

On 26 May 2022, DTI submitted its Post-Breach Report with proper documentation on the actions taken.[30]

On 11 July 2022, the CID ordered DTI to submit a Supplemental Post- Breach Report documenting the actions taken with regard to DTI- Rizal's organizational and physical measures.[31]

On 29 July 2022, DTI submitted a Supplemental Post-Breach Report containing proper documentation on the actions taken.[32] It submitted proof that only certain persons are authorized to access the office, storage area, vault, and steel cabinets.[33]

With regard to DTI-Rizal's PIA, it reported that "the information collected from data subjects are likely to raise privacy concerns or expectations as they can be used for identity/business fraud for loan applications/business scams during the validity of the documents."[34] DTI-Rizal, however, submitted that "none of the affected data subjects reported negative consequences as a result of the said breach."[35] DTI- Rizal added that it observes a one (1) year retention period on company profiles in the OTOP Directory.[36] DTI-Rizal explained that the OTOP Support Staff is designated to update information and to

---

[27] Compliance, 03 January 2022, at 1, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[28] Order (To Submit Post-Breach Report), 10 May 2022, at 1, *in* In Re: Department of Trade and Industry – Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2018).
[29] *Id.*
[30] Compliance, 26 May 2022, at 1, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[31] Order (To Submit Post-Breach Report), 11 July 2022, at 1, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[32] Compliance, 29 July 2022, at 1, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[33] *Id.* Annex B.
[34] *Id.* Annex D.
[35] *Id.* at 3.
[36] *Id.* Annex D.

determine whether the information is necessary for retention or disposal.[37]

On 17 October 2022, DTI submitted a Post-Breach Report containing proper documentation on the actions taken.[38] DTI-Rizal clarified that it previously submitted the required information.[39]

DTI emphasized that the types of personal information involved in the breach includes the scanned 2017-2018 business permit files of MSME programs totaling forty (40) MSME business permit files.[40] These involve scanned copies of business name certificates containing the full name of the business owner and a copy of the 2018 Mayor's Permits containing the business address of the owner.[41]

The breach also includes the Directory of 2018-2019 "Otopreneurs" containing the name of contact person, name of company, nature of business, address, contact numbers, email addresses, and the Individual Accomplishment Reports of the OTOP Account Officer for 2018 containing the full name and designation of the account officer.[42]

On 28 October 2022, NPC BN 18-220 In re: DTI and NPC BN 18-231 In re: DTI-Rizal were consolidated since they pertain to the same breach notification report.[43]

Issue

Whether DTI- Rizal conducted proper breach management, including the implementation of reasonable and appropriate security measures.

Discussion

---

[37] *Id.*
[38] Post-Breach Report, 17 October 2022, at 1, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] Memorandum, Complaints and Investigation Division, at 1, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).

The Commission finds that DTI-Rizal conducted proper breach management and implemented reasonable and appropriate security measures in addressing the breach. The Commission resolves to close the matter.

Section 20 (a) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) provides that a Personal Information Controller (PIC) should implement reasonable and appropriate measures to protect personal information:

> Section 20. *Security of Personal Information.*
>
> a. The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[44]

Similarly, Section 17 (D) (3) of NPC Circular 16-03 (Personal Data Breach Management) provides the obligation of a PIC to notify the NPC of a personal data breach.[45] The provision also outlines the content of notification specifically the measures that a PIC took to address the breach:

> Section 17. *Notification of the Commission.* The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification.* The notification shall include, but not be limited to:
>
> . . .
>
> 3. Measures Taken to Address the Breach
>
> a. description of the measures taken or proposed to be taken to address the breach;

---

[44] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (a) (2012).

[45] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], § 17 (D) (3) (15 December 2016).

b. actions being taken to secure or recover the personal data that were compromised;
c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
e. the measures being taken to prevent a recurrence of the incident.[46]

Based on its submissions, DTI-Rizal narrated the measures it took to address the breach following Section 20 (a) and Section 17 (D) (3) of NPC Circular 16-03.

DTI-Rizal posted an advisory on the bulletin board outside the office informing the public that a robbery incident took place in the office.[47] The advisory warned all concerned that the "incident may have resulted [in] an accidental loss of personal data" and that DTI-Rizal has "taken measures to secure the office to prevent similar incidents in the future."[48] DTI-Rizal also added the contact number of its Data Protection Officer (DPO) in case concerned data subjects have privacy- related queries.[49] DTI-Rizal attached pictures to support its implementation to its Compliance.[50]

DTI-Rizal also notified the forty (40) affected data subjects who are MSME business permit owners the day immediately after the incident through SMS.[51]

As part of DTI-Rizal's remedial measures, a security guard regularly reports to the office on a twelve (12) hour duty.[52] DTI-Rizal also

---

[46] Id. § 17 (D) (3).
[47] Breach Notification, 27 November 2018, Annex D, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2018).
[48] *Id.*
[49] Full Breach Report, 03 January 2022, Annex B, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[50] *Id.*
[51] Compliance, 26 May 2022, Annex D, *in* In Re: Department of Trade and Industry, NPC BN 18 - 220 and NPC BN 18-180 (NPC 2022).
[52] Full Breach Report, 03 January 2022, Annex B, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).

reported that it negotiated with the building owner for increased security in the establishment.[53]

As a physical measure, DTI-Rizal installed iron grills and shutters for the windows and it replaced the padlocks for the staircase gates.[54] It also added steel filing cabinets with locks for equipment storage.[55]

Additionally, seven (7) closed-circuit television (CCTV) cameras were installed on December 2018.[56] According to DTI-Rizal, the Provincial Director is authorized to monitor all CCTV footages, while DTI-Rizal's Finance and Administrative Unit (FAU) and Information Technology (IT) Officers are in-charge of overseeing and coordinating the use of the CCTV.[57] DTI-Rizal attached pictures evidencing the implementation.[58]

As an organizational measure, DTI-Rizal designated DPOs and a data security officer.[59] According to DTI-Rizal, only authorized persons have access to the office, storage, vault, and steel cabinets.[60] DTI-Rizal also provided data privacy trainings to its staff from 2018-2020.[61] A copy of the certificate of attendance was attached to DTI-Rizal's Compliance.[62] It also posted data privacy notices in both their client and employee work spaces.[63]

As a technical measure, DTI-Rizal partnered with DTI-Rizal's IT Team to come up with additional security measures to protect the records and data of the office.[64]

---

[53] Compliance, 17 October 2022, at 4, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[54] *Id.*
[55] Full Breach Report, 03 January 2022, Annex B., *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[56] *Id.*
[57] Breach Notification, 27 November 2018, Annex C, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2018).
[58] Full Breach Report, 03 January 2022, Annex B, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[59] Compliance, 29 July 2022, Annex A, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[60] *Id.* Annex B.
[61] Full Breach Report, 03 January 2022, at 6, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[62] *Id.* Annex E.
[63] Full Breach Report, 03 January 2022, Annex D, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[64] *Id.* Annex G.

DTI-Rizal reported that all employees are required to use passwords on laptops issued by the office.[65] DTI-Rizal utilizes BitLocker as an encryption tool for added protection to the records in the computer units.[66] DTI-Rizal advised employees to safeguard their external hard drives such as Universal Serial Bus (USB) Storages and Secure Digital (SD) Cards in safe and secured locations.[67] According to DTI-Rizal, it also implements cloud-based storage through Office 365.[68]

Based on the foregoing, the measures that DTI-Rizal took after the incident have shown its commitment in complying with the Data Privacy Act of 2012 and the Commission's issuances.

The Commission takes this opportunity to remind PICs, such as DTI- Rizal, of their responsibility to observe constant vigilance against theft or robbery in their premises. This is an essential practice to strengthen its mandate to protect the personal data of its data subjects.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-220 Department of Trade and Industry and NPC BN 18-231 In re: Department of Trade and Industry – Rizal Provincial Office (DTI-Rizal) is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
30 June 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

---

[65] *Id.* at 2.
[66] *Id.* Annex G.
[67] Full Breach Report, 03 January 2022, Annex G, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).
[68] Compliance, 17 October 2022, at 3, *in* In Re: Department of Trade and Industry - Rizal Provincial Office, NPC BN 18-220 and NPC BN 18-180 (NPC 2022).

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

(on official leave)
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

AMV
Officer-in-Charge, Knowledge Management and Information Service and Acting DTI Data Protection Officer
Department of Trade and Industry

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: PACIFIC PLAZA TOWERS CONDOMINUM CORPORATION **NPC BN 18-138**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is a breach involving unauthorized access to and use of email addresses of Pacific Plaza Towers Condominium Corporation's (PPTCC) condominium residents and unit owners.

Facts

On 27 July 2018, PPTCC notified the National Privacy Commission (NPC) of a breach:

> On 14 July 2018, a certain LES sent an e-mail to residents of the condominium with the subject "Please for Solidarity for Pacific Plaza Tower Terminated Workers" (the "14 July 2018 E-mail"). As of the date of this letter, what is known is that this email was sent to eighty-eight (88) e-mail addresses which corresponds to eighty-seven (87) individuals (the "Subject E-mail Addresses"). One of the recipients had two (2) e-mail addresses.
>
> One of the recipients of the 14 July 2018 E-mail is Ms. GGG President of PPTCC. Considering the contents of the 14 July 2018 E-mail and the fact that it was sent to a substantial number of residents of the condominium by an outsider, Ms. GGG, who was mindful of the possible implications, immediately informed the PPTCC Management of the existence of the email, particularly so that an investigation can be conducted. At that time, it was not known who LES was or how LES was able to obtain the e-mail addresses.[1]

[1] Personal Data Breach Notification from Pacific Plaza Towers Condominium Corporation, 27 July 2018, at 1-2, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2018).

After investigation, PPTCC determined that the sender, LES, was connected to the employees of an independent contractor previously engaged in a service contract with PPTCC.[2] It explained:

> Upon investigation, there is reason to believe that the LES who sent the email is the same LES or Atty. RSE who appears to be connected with the Solidarity of Unions in the Philippines for Empowerment and Reforms ("Super Federation"). Super Federation is the national labor federation that is apparently assisting certain employees of Polystar General Services ("Polystar") in connection with their labor issues against the latter. Polystar, in turn, is a duly licensed independent contractor with whom PPTCC had a service contract that expired on 30 June 2018.[3]

PPTCC reported that it cross-referenced the list of email addresses to whom LES sent his email against a segment of its own list.[4] PPTCC's list was an Excel file of email addresses of the current and previous PPTCC residents or unit owners as of 2014.[5] According to PPTCC, its list was stored in a computer at its Job Order Center (JOC) and was "password-protected, and only selected PPTCC employees have access thereto."[6]

After comparing the two lists, PPTCC concluded that there was reasonable basis to believe the list of email addresses to whom LES sent his email was accessed without authority and that "a data breach requiring notification has occurred,"[7] since LES was an outsider.[8] It claimed it was still investigating "the specific manner by which the e- mail addresses were accessed from the records of PPTCC, and the person directly responsible for the unauthorized access[.]"[9]

PPTCC stated that "at least one [of] the names/e-mail addresses in the e-mail of [LES] is already deceased, which tends to show that LES was merely copying from a list of e-mails without really knowing the individual recipients."[10] PPTCC also stated that the email addresses

---

[2] *Id.*
[3] *Id.*
[4] *Id.* at 1.
[5] *Id.*
[6] *Id.*
[7] Personal Data Breach Notification from Pacific Plaza Towers Condominium Corporation, 27 July 2018, at 2, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2018).
[8] *Id.*
[9] *Id.*
[10] *Id.*

"may be used not only to annoy or harass the account owners, as was already done by LES, but also to access online accounts connected to this e-mail addresses, among others."[11]

PPTCC reported that it was investigating certain individuals "on their possible participation in the breach."[12] It also consulted with legal counsel regarding sending a cease and desist letter and filing a case against those involved, including LES.[13] PPTCC also stated that it sent notifications to the affected data subjects.[14] PPTCC stated that it restricted physical access to the "concerned facilities."[15] It also installed additional CCTV cameras in various areas "to monitor and deter unauthorized access."[16] It also stated that it would install an additional biometric access control system.[17] Finally, PPTCC reported that it reviewed company domain controller policies "to ensure that only those authorized personnel have access to confidential data."[18]

On 01 August 2018, PPTCC sent an update to the NPC, through its Complaints and Investigation Division (CID), stating that "as of today, there are no new matters or information to report with respect to the data breach[.]"[19]

On 16 March 2021, the CID issued an Order directing PPTCC to submit the results of its investigation:

> For a full appreciation of the circumstances surrounding this report and the incident, it is necessary to require the PPTCC to provide the results of their investigation on how said email addresses were made know to the outsider, security measures to address and prevent the recurrence of the security incident.
>
> You are hereby given a period of fifteen (15) days from receipt hereof to submit your compliance through e-mail at complaints@privacy.gov.ph.

---

[11] *Id.*
[12] *Id.*
[13] Personal Data Breach Notification from Pacific Plaza Towers Condominium Corporation, 27 July 2018, at 2, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2018).
[14] *Id.*
[15] *Id.* at 3.
[16] *Id.* at 2.
[17] *Id.*
[18] *Id.*
[19] Personal Data Breach Notification from Pacific Plaza Towers Condominium Corporation, 27 July 2018, at 3, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2018).

SO ORDERED. Pasay City, 16 March 2021.[20]

On 21 September 2021, the CID issued an Order, reiterating its directive to PPTCC and directing it to also submit proof of its security measures and measures taken to notify the data subjects:

> For a full appreciation of the circumstances surrounding this report and the data breach that it describes, it is necessary to require the PPTCC:
>
> 1. To provide the results of the proposed security measures;
> 2. Existing physical access restriction at the time of the incident;
> 3. Other measures and policies the PPTCC has implemented to prevent the recurrence of the incident;
> 4. Measures taken to notify the affected data subjects and assistance offered, if any.
>
> You are hereby given a period of fifteen (15) days from receipt hereof to submit your compliance through e-mail at complaints@privacy.gov.ph.
>
> **SO ORDERED.** Pasay City, 21 September 2021.[21]

On 14 October 2021, PPTCC submitted its compliance.[22] It apologized for the delayed submission, attributing it to "the ongoing pandemic and the corresponding quarantine restrictions that it entails."[23]

On measures implemented after the breach, PPTCC reported that it investigated some individuals on their possible participation in the incident.[24] Due to lack of evidence, however, PPTCC stated it could not determine or verify all the individuals who may have been involved.[25] Further, while PPTCC initially filed a complaint with the NPC against LES, it stated that it "wants to move on and formally reiterates herein that it is no longer interested in pursuing the case against Atty. RE."[26]

---

[20] Order, 16 March 2021, at 1, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2021).
[21] Order, 21 September 2021, at 1, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2021).
[22] Compliance, 14 October 2021, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2021).
[23] *Id.* at 1.
[24] Compliance, 14 October 2021, at 1, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2021).
[25] *Id.*
[26] *Id.*

PPTCC also claimed that it notified the affected data subjects about the breach, "including the measures undertaken to address the same."[27] It stated that "these data subjects were also assured of assistance and information relating to the matter."[28]

Further, PPTCC stated that at the time of the incident, it restricted physical access through biometric access control to "primary entry / exit points," except for its workstation areas.[29] It also installed additional CCTV cameras in its Business Center and workstation areas later to "monitor and deter unauthorized access to confidential information."[30] It also installed biometric access control in its IT Room.[31]

Finally, PPTCC reported that "a SONICWALL firewall device has been installed in the network infrastructure for additional data security,"[32] that "the domain user access privilege has been reviewed and set business unit groups to access only files / folders intended for them,"[33] and that "ERP-Document Management System has been implemented."[34] PPTCC said this was to ensure that only authorized users can access confidential information and copying information required approval from the information security officer.[35]

On 18 July 2022, the CID issued an Order directing PPTCC to submit a Supplemental Post-Breach Report containing proof of implementation of the following: notification to data subjects;[36] trainings and seminars pertaining to Data Privacy Awareness, if any;[37] other organizational, physical, and technical security measures implemented after the breach to prevent its recurrence;[38] and a flowchart of the reporting procedures in relation to data breach incidents, as well as proof of implementation thereof.[39]

---

[27] *Id.*
[28] *Id.*
[29] *Id.* at 2.
[30] Compliance, 14 October 2021, at 2, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2021).
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] Order, 18 July 2022, at 1, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18- 138 (NPC 2022).
[37] *Id.*
[38] *Id.*
[39] Order, 18 July 2022, at 1, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18- 138 (NPC 2022).

On 11 October 2022, the CID re-sent the Order dated 18 July 2022 to PPTCC.[40] To date, the Commission has not received any submissions from PPTCC.

Issue

Whether PPTCC sufficiently addressed the breach and implemented security measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. The incident does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03 (Personal Data Breach Management). Nevertheless, PPTCC sufficiently addressed the breach and implemented security measures to prevent its recurrence.

Section 11 of NPC Circular 16-03 on mandatory breach notification provides:

> Section 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
> B. There is reason to believe that the information may have been acquired by an unauthorized person; and
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[41]

---

[40] Email from PPTCC, 11 October 2022, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2022).
[41] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).

Following this, the requisites for mandatory breach notification to the Commission are:

1. The breach involves sensitive personal information, or information that may, under the circumstances, be used to enable identity fraud;[42]
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[43]

The first requisite is absent in this case. The nature of the information in this case is neither sensitive personal information nor other information that may enable identity fraud.

This should be read together with Section 20 (f) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA). Section 20 (f) expressly requires the consideration of the specific circumstances of a breach in determining whether other information involved in the breach may enable identity fraud:

> Section 20. *Security of Personal Information.*
>
> . . .
>
> (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or **other information that may, under the circumstances, be used to enable identity fraud** are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach,

---

[42] NPC BN 18-158, 13 November 2023, at 10 (NPC 2023) (unreported).
[43] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does Initiated as a Sua Sponte NPC Investigation on Possible Data Privacy Violations Committed in Relation to the Alleged Hack and Breach of the Commission on Elections System or Servers, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-SS-22-001-and-NPC-SS-22- 008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 31 January 2024).

> to prevent further disclosures, or to restore reasonable integrity to the information and communications system.[44]

The Commission previously held that a data subject's name and email may be considered under "other information that may enable identity fraud."[45] The Commission explained:

> This Commission takes this opportunity to stress that information that may be used to enable identity fraud under Section 11 (A) is not limited to the categories of information listed therein, such as data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> **Contrary to Respondent's claim, names and e-mail addresses are information that may be used to enable identity fraud. An e-mail address is considered personal information and an unauthorized acquisition thereof could easily trace the identity of the data subject through the conduct of "Phishing" attacks to obtain more information about the user which would then be used to access important accounts resulting to identity theft and financial loss.**[46]

In that case, the Commission, after considering the circumstances, determined that the names and email addresses of the data subjects are information that may be used to enable identity fraud.[47] The PIC reported that a hacker accessed and implanted ransomware in an online database.[48] Because of these particular circumstances, the Commission concluded that the hacker may contact and send malicious emails directly to the data subjects.[49]

Here, LES use of the email addresses would not have enabled identity fraud.

---

[44] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (f) (2012). Emphasis supplied.

[45] NPC BN 20-124, 10 September 2020, at 3 (NPC 2020) (unreported).

[46] *Id.* Emphasis supplied.

[47] *Id.* at 4.

[48] *Id.*

[49] *Id.*

In its initial report, PPTCC stated that the email addresses used by LES belonged specifically to current or previous PPTCC condominium residents or unit owners.[50] PPTCC also explained that LES was connected with employees of an independent contractor, with whom PPTCC had a service contract:

> Upon investigation, there is reason to believe that the LES who sent the email is the same LES or Atty. RSE who appears to be connected with the Solidarity of Unions in the Philippines for Empowerment and Reforms ("Super Federation"). **Super Federation is the national labor federation that is apparently assisting certain employees of Polystar General Services ("Polystar") in connection with their labor issues against the latter. Polystar, in turn, is a duly licensed independent contractor with whom PPTCC had a service contract that expired on 30 June 2018.**[51]

Given LES connection with Super Federation, PPTCC concluded that his intent was to use the email addresses to show solidarity with the Polystar General Services (Polystar) employees over their labor disputes.[52]

PPTCC's statement clarifies that LES use of the email addresses was only to bring attention to the labor issues of the Polystar employees.[53] The targeted use of the email addresses in this case shows that the purpose for their acquisition is to use them in the labor dispute and not to perpetrate identity or any kind of fraud. Given the specific circumstances of the case, email addresses alone do not provide for adequate means of committing identity fraud. As such, the email addresses of the data subjects cannot be considered as other information that may enable identity fraud.

The second requisite is present in this case. There was acquisition of the information by an unauthorized person.

---

[50] Personal Data Breach Notification from Pacific Plaza Towers Condominium Corporation, 27 July 2018, at 1, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2018).
[51] *Id.* at 1-2. Emphasis supplied.
[52] *Id.*
[53] *Id.*
[53] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).

The Commission previously held that a loss of control over personal data held in custody is enough for a personal information controller (PIC) to have "reason to believe that the information may have been acquired by an unauthorized person."[54]

In this case, PPTCC reported that it was still investigating "the specific manner by which the e-mail addresses were accessed from the records of PPTCC, and the person directly responsible for the unauthorized access[.]"[55] Nonetheless, it stated that there was reasonable basis to believe the list was accessed without authority and "a data breach requiring notification has occurred"[56] since LES was an outsider.[57] Hence, PPTCC admitted that it lost control and that unauthorized persons acquired the personal information of the data subjects, which satisfies the second requisite.

The third requisite is also absent. There is no real risk of serious harm in this case.

The Commission takes this opportunity to discuss the factors considered in determining the presence of the third requisite of mandatory breach notification. Section 11 (C) of NPC Circular 16-03 provides:

> Section 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> . . .
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[58]

For this purpose, the phrase "likely to give rise to a real risk" in Section 11 (C) means that a link exists between the breach and the possible

---

[54] *Id.*
[55] Personal Data Breach Notification from Pacific Plaza Towers Condominium Corporation, 27 July 2018, at 2, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2018).
[56] *Id.*
[57] *Id.*
[58] NPC Circ. No. 16-03, § 11.

resulting harm to any affected data subject.[59] The risk must be apparent and not the product of mere speculation.[60] Serious harm means that the consequences and effects to any affected data subject are significant based on the surrounding circumstances of the breach.[61]

In determining whether the unauthorized acquisition is likely to give rise to real risk of serious harm, a PIC or the Commission may consider several factors, such as: the nature and amount of information involved in the breach, the period of time that has lapsed since the breach, objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.

In this case, the objective of the unauthorized acquisition was to express solidarity with the workers of Polystar. Aside from his connection with Super Federation, LES himself titled the email "Please for Solidarity for Pacific Plaza Tower Terminated Workers."[62] Thus, it may be reasonably concluded that the objective of the unauthorized acquisition was to express solidarity with the workers of Polystar and not some malicious or fraudulent purpose.

Further, the nature and amount of information involved was limited to the email addresses of current and former PPTCC condominium residents or unit owners.[63] This limited information, used by LES to show solidarity with Polystar workers, did not include other details that would enable identity fraud. Thus, further exposure or misuse of the information is unlikely.

Finally, PPTCC implemented sufficient security measures on the information prior to and after the breach. It reported that it had kept the list of email addresses stored in a computer at its JOC, which was password-protected, and accessed only by selected PPTCC employees.[64] After the breach, it implemented physical security measures such as restricting physical access to its premises through

---

[59] NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8 (NPC 2023) (unreported).
[60] *Id.*
[61] *Id.*
[62] Personal Data Breach Notification from Pacific Plaza Towers Condominium Corporation, 27 July 2018, at 1-2, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2018).
[63] *Id.*
[64] *Id.* at 1.

biometric access control[65] and installing additional CCTV cameras.[66] It also implemented technical security measures by installing a firewall device in its network infrastructure,[67] reviewing and adjusting domain user access privileges,[68] and implementing a document management system.[69]

Given the foregoing factors and the remedial measures taken by PPTCC, the unauthorized acquisition did not give rise to a real risk of serious harm to any affected data subject. Thus, the third requisite is absent.

Considering that the first and third requisites are absent, the matter does not fall under mandatory breach notification. Nevertheless, PPTCC conducted proper breach management, including the implementation of reasonable and appropriate security measures. The measures implemented by PPTCC are sufficient to address the breach and to prevent its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-138 In re: Pacific Plaza Towers Condominium Corporation is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines. 13 November 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

---

[65] Compliance, 14 October 2021, at 2, *in* In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138 (NPC 2021).
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

RRO
Data Protection Officer
Pacific Plaza Towers Condominium Corporation

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: KGJS FLEET MANAGEMENT MANILA, INC. **NPC BN 18-135**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*:

Before the Commission is KGJS Fleet Management Manila, Inc.'s (KGJS) breach notification involving the reposting of the contents of its website to another website resulting in the disclosure of personal information of its employees.

Facts

On 20 July 2018, a KGJS employee reported that it received a text message on his company-issued mobile phone about an inquiry for a job opening.[1] According to the job applicant, he/she obtained the information on the job opening, which includes the employees' personal information, from *www.Indeed.com* (Indeed), a website for job listings.[2]

KGJS narrated that the personal information of its employees can be accessed on Indeed using the keyword "kgjs" on the website's search feature.[3] KGJS deduced that the personal information came from its own website and other possible website sources such as Philippine Overseas Employment's (POEA) website.[4]

KGJS clarified that there was no agreement between KGJS and Indeed about the re-posting of its website content.[5] Further, its employees

---

[1] Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 2, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).
[2] *Id.*
[3] *Id.*
[4] *Id.*

have no knowledge of authorizing Indeed to post information related to job openings.[6]

On 23 July 2018, the employee received another call from the same mobile number inquiring about a sea-based job opening posted on Indeed.[7] The employee reported this matter to his manager and to KGJS' Data Protection Officer (DPO).[8] The DPO then conveyed the same information to the Data Breach Response Team.[9]

On 24 July 2018, KGJS notified the National Privacy Commission (NPC) of the incident involving the personal information of its employees.[10]

KGJS explained that a total of four (4) of its employees were affected by the re-posting on Indeed's website.[11] Two (2) of the employees' information such as their full name, designation, company direct line, and company mobile number were listed directly on its company website.[12] Two (2) other employees' information such as company mobile numbers, a "wrong" email address of an employee, and their full names as official representatives of KGJS, according to KGJS, were possibly obtained from the POEA website.[13]

KGJS indicated that this information was publicly posted on its website to serve as contact persons for inquiries on crew requirements or sea-based job openings.[14]

KGJS averred that the posting of its employees' personal information on Indeed may "result to identity theft and unauthorized transfer and re-posting of web content/article."[15] KGJS also stated that there might be "possible misinterpretation" of the its job posting or "possible misinformation" between the employee and the applicants.[16] Lastly,

---

[6] *Id.*
[7] Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 3, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).
[8] *Id.*
[9] *Id.*
[10] *Id.* at 1.
[11] *Id.* at 2.
[12] *Id.*
[13] Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 3, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).
[14] *Id.*
[15] *Id.*

KGJS reasoned that "applicants who are web visitors and users of Indeed may presume that the job posting is legitimate and may result to unauthorized collection of personal information and resume."[17]

On 27 July 2018, KGJS updated the NPC on its breach notification.[18] KGJS explained that it removed the affected employees' personal information from its company website on 24 July 2018.[19] It also sent an email notification to the affected employees about the incident.[20] Indeed also removed the job posting as confirmed through an email sent on 26 July 2018.[21]

On 30 July 2018, KGJS submitted a Full Report[22] where it claimed that there was "no database breach"[23] and no sensitive personal information was involved.[24]

KGJS reported that its employees' personal data posted in the POEA website has already been corrected and updated.[25] KGJS also reported that it also submitted a letter of information to POEA regarding the incident.[26]

KGJS also "de-indexed" and removed the personal data on its website to reduce the risk of "indexed searching" and to prevent the recurrence of the incident, [27] It also conducted a Privacy Impact Assessment (PIA) of its website.[28]

Issue

---

[17] *Id.*
[18] Update as of 27 Jul 18 – Security Incident dated 20 Jul 18 of Article/Web Content in Company Website, 27 July 2018, at 1, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] Full Report as of 30 Jul 18: Security Incident dated 20 Jul 18 of Article/Web Content in Company Website, 30 July 2018, at 1, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18- 135 (NPC 2018).
[23] Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 2, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).
[24] *Id.* at 5.
[25] *Id.* at 3.
[26] Update as of 27 Jul 18 – Security Incident dated 20 Jul 18 of Article/Web Content in Company Website, 27 July 2018, at 1, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).
[27] Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 5, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).
[28] *Id.* at 6.

Whether KJGS sufficiently addressed the incident and implemented security measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. KGJS implemented reasonable and appropriate security measures to address the incident. Nonetheless, the incident does not amount to a personal data breach.

Section 3 (F) of NPC Circular 16-03 (Personal Data Breach Management) defines a personal data breach:

> Section 3. *Definition of Terms.* For the purpose of this Circular, the following terms are defined, as follows:
>
> . . .
>
> F. **"Personal Data Breach"** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, personal data transmitted, stored, or otherwise processed. It may be in the nature of:
>
> 1. An availability breach resulting from loss, accidental, or unlawful destruction of personal data;
> 2. Integrity breach resulting from alteration of personal data; and/or
> 3. A confidentiality breach resulting from the unauthorized disclose of or access to personal data.[29]

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access to personal data transmitted, stored, or otherwise processed.[30]

In this case, the website Indeed is a metasearch engine that consolidates job listings from websites and recruiting companies.[31]

---

[29] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], § 3 (F) (15 December 2016).
[30] *Id.*
[31] *See* Adam Hayes, Indeed v. Linked-in: What is the Difference, *available at* https://www.investopedia.com/articles/personal-finance/020215/indeed-vs-linkedin.asp (last accessed November 2023).

Indeed provides job seekers access to job listings and allows them to post resumes and research companies.[32]

When a user searches for job listings on Indeed, one can see job listings that Indeed scans from the internet and collates into a user's search results.[33]

When a user clicks the "Apply on company site" button, Indeed will send the user's job application to the employer's applicant tracking system (ATS).[34] The ATS is a software that employers use during the recruitment and hiring process to streamline the hiring process.[35]

Indeed explained that if a user applies directly on the company's website, the user will not receive any communication from Indeed about his or her application status.[36] The employer may communicate with the applicant through its own hiring platform, or through email.[37]

Considering that the purpose of posting job openings on Indeed is to maximize visibility and attract as many potential candidates as possible, the information of the KGJS employees or recruiters that were posted on Indeed would have been used in a way that was still consistent with the original purpose for posting it on KGJS's website.

KGJS' reasoning that the posting on Indeed may result to "identity theft and unauthorized transfer" and "unauthorized collection of personal information and resume"[38] is speculative. Through the ATS, it is the recruiting company itself that handles the collection of any applicant information and not Indeed.

---

[32] *See* About Indeed, *available at* https://ph.indeed.com/about (last accessed January 2023).
[33] *See* About Jobs on Indeed: What You Need to Know, *available at* https://support.indeed.com/hc/en-us/articles/115002786323-About-Jobs-on-Indeed-What-You- Need-to-Know (last accessed 31 January 2024).
[34] *Id.*
[35] *See* What are Applicant Tracking Systems, *available at* https://www.indeed.com/career- advice/career-development/what-are-applicant-tracking-systems (last accessed 31 January 2024).
[36] *Id.*
[37] *See* About Jobs on Indeed: What You Need to Know, *available at* https://support.indeed.com/hc/en-us/articles/115002786323-About-Jobs-on-Indeed-What-You- Need-to-Know (last accessed 31 January 2024).
[38] Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018,

As stated by KGJS, Indeed possibly obtained the information of the employees from the KGJS and POEA website.[39] These websites are accessible to the public particularly for the purpose of recruitment and placement through a manning agency.[40]

Given these reasons, the incident cannot be considered a confidentiality breach resulting from the unauthorized disclosure of or access to personal data. There is no unauthorized access to the systems maintained and managed by KGJS nor was there any breach of security protecting the personal data processing system of KGJS.

Additionally, the details of the personal data of the recruitment officers of KGJS, such as names and designation, are publicly and readily available.[41] In addition, the contact numbers for inquiries on job openings are their company contact numbers and not their personal phone numbers.[42]

NPC Circular 16-03 only pertains to personal data of an individual or natural person.[43] Since the contact number involved is the contact number of KGJS, a juridical person, this incident does not amount to a personal data breach as contemplated by NPC Circular 16-03.

Even though the matter is not considered a reportable breach, KGJS implemented reasonable and appropriate security measures to address the incident. KGJS implemented measures to minimize any potential risks associated with the incident, therefore minimizing any adverse effects on the individuals whose data were impacted.

KGJS immediately requested the removal of its employees' information on Indeed.[44] Indeed confirmed the removal through

---

[39] *Id.* at 2.
[40] Final Breach Notification Evaluation Report, 21 March 2023, at 5, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2023).
[41] Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 2, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).
[42] *Id.*
[43] *See* NPC Circ. No. 16-03.
[44] Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 5, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

email.[45] KGJS also conducted the removal of its employees' personal information from its own website.[46]

KGJS also notified the four (4) employees through email whose data may have been acquired from the security incident.[47] KGJS provided them with an update on the initiatives undertaken to address the matter.[48]

Lastly, KGJS modified its website to ensure that it does not appear in search results on any third-party websites.[49]

Based on the foregoing, the actions taken by KGJS following the incident allowed it to enhance its security measures and are sufficient to close the case in accordance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) and NPC Circular 16-03.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-135 In re: KGJS Fleet Management Manila, Inc. is considered **CLOSED.**

SO ORDERED.

City of Pasay,
Philippines.
13 November 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

---

[45] Full Report as of 30 Jul 18: Security Incident dated 20 Jul 18 of Article/Web Content in Company Website, 30 July 2018, at 1, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18- 135 (NPC 2018).
[46] Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 5, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).
[47] *Id.*
[48] *Id.*
[49] *Id.*

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

CG
Data Protection Officer
KGJS Fleet Management Manila, Inc.

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: ACTIVE NETWORK, LLC. **NPC BN 18-035**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is Active Network, LLC's (Active) breach notification and management in compliance with NPC Circular 16-03 (Personal Data Breach Management).

Facts

On 19 March 2018, Active notified the National Privacy Commission (NPC) about a "security incident that may have involved unauthorized access to the personal information of 1,715 residents of the Philippines."[1]

In its Initial Report, Active narrated it identified suspicious activity on one of its systems.[2] The investigation conducted by Active and cybersecurity firms revealed that unauthorized third parties potentially accessed personal information provided by users between December 2016 and September 2017.[3] Active alleged that throughout this period, unauthorized third parties deployed codes designed to collect information manually entered by users on the checkout page of Active's website.[4] Consequently, personal details provided during the checkout process may have been accessed by these unauthorized third parties.[5]

---

[1] Initial Report, 19 March 2018, at 2, *in* In Re: Active Network, LLC. NPC BN 18-035 (NPC 2018).
[2] *Id.* at 4.
[3] *Id.* at 2.
[4] *Id.*
[5] *Id.*

Active explained that the personal information potentially accessed because of the incident includes names, addresses, email addresses, credit or debit card numbers, expiration dates, and cardholder verification codes.[6]

Upon discovering the "suspicious activity", Active stated that it "engaged leading cybersecurity firms to investigate the incident" and took measures "to enhance monitoring tools and security controls" to prevent similar activity in the future.[7]

Active also maintained that it reported the incident to "relevant payment card brands and related entities and to regulatory authorities in the United States and other jurisdictions.[8]

Active manifested that it had already notified the one thousand seven hundred fifteen (1,715) data subjects affected by the incident.[9] It also submitted a copy of the notification template in the Initial Report:

> Dear [NAME]:
>
> We are writing to inform you that we recently became aware of a security incident involving the ACTIVE Network, including ACTIVE Works and ACTIVE Endurance ("Active") which may have impacted your personal information.
>
> **What Happened**
>
> Active recently identified suspicious activity on one of its systems. We worked with leading cybersecurity firms to determine that the activity related to transactions manually keyed in by users while checking out on the Active website between December of 2016 and September of 2017. During this time period, unauthorized third parties distributed code that was designed to gather information manually keyed in by users on Active's checkout page, and personal information that you provided as part of the checkout process may have been accessed by these unauthorized third parties.
>
> **What Information Was Involved**
>
> The information may have included your name, address, email address, credit or debit card number, expiration date, and

---

[6] *Id.*
[7] Initial Report, 19 March 2018, at 2, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[8] *Id.*
[9] *Id.* at 3.

cardholder verification code (the three- or four-digit value included on the front or back of payment cards and used for verification of certain transactions).

What We Are Doing

As soon as Active identified the suspicious activity, it engaged leading cybersecurity firms to investigate the incident and took steps to enhance its monitoring tools and security controls. Active has also taken steps to contain and remediate the incident and has notified regulatory authorities in the United States. Active is in the process of reporting the incident to the National Privacy Commission.

What You Can Do

We encourage you to be diligent in watching for unauthorized activity associated with your payment card accounts and to quickly report suspicious activity to your bank or credit card company. The phone number to call is usually on the back of the credit or debit card.

For More Information

We apologize for any inconvenience this incident may cause. You may contact us at [], between 8:00pm and 2:00pm (Manila time), Monday through Friday, if you have any questions or would like additional information about this incident.[10]

On 07 September 2018, the NPC, through the Complaints and Investigative Division (CID), directed Active to submit a Full Report on the incident within five (5) days from the receipt of the Memorandum.[11] In addition, the CID instructed Active to submit the following:

1. A copy of the report, within five (5) days of receipt of the Order, sent to the relevant payment card brands and related entities and to regulatory authorities in the United States and other jurisdictions;
2. Consolidated results of the investigation, within fifteen (15) days from receipt of the Order conducted by hired cybersecurity firms;
3. List of reported related incidents, within fifteen (15) days from receipt of the Order, from their data subjects in the Philippines.[12]

---

[10] *Id.* at 4-5.
[11] Memorandum, 07 September 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[12] *Id.*

On 19 September 2019, Active requested for an extension of time until 16 October 2018 or thirty (30) days from receipt of the Memorandum, to submit the Full Breach Report.[13] Active stated that it needed time to gather information and documents from different business units as well as third parties, thus, it will not be able to submit the Full Breach Report on the deadline.[14] Active, however, provided the following details in their request for extension:

- The investigation on the data breach has been completed.
- Philippine residents or citizens were affected by the data breach and such individuals have been notified on 19 March 2018.
- Third-party security experts have been engaged to investigate the data breach and they have since completed their investigation.[15]

On 15 October 2018, Active submitted its Compliance,[16] which included a Response to the Memorandum dated 07 September 2018, and the full report of the details of the incident as directed by the CID.[17] In its report, Active reiterated the chronology of the events that led to the alleged loss of control over the personal data.[18]

Active determined that an unauthorized individual utilized customer credentials to enter its network.[19] Active believes that the unauthorized individual took the credentials, initially designated for customer use to access specific sections of the system, from a customer rather than from Active, possibly through methods like phishing or social engineering.[20]

When it discovered the breach, Active implemented changes "to completely segment or airgap the point of entry of the unauthorized third party and customers from the remainder of Active's environment."[21] This measure ensures that neither the unauthorized

---

[13] Request for Extension, 19 September 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[14] *Id.*
[15] *Id.*
[16] Compliance, 15 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[17] Response to NPC's Memorandum dated 07 September 2018, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[18] *Id.*
[19] *Id.* at 2.
[20] *Id.*
[21] *Id.*

individual nor any other unapproved entity can use that specific point of entry for access.[22]

Active claimed that the investigation reveals that the unauthorized individual managed to gain additional access to Active's network and "the presentation layer of an application that is part of the checkout process."[23] Active believes that this access facilitated the injection of a malicious JavaScript code to overwrite the original JavaScript file associated with the entry of payment card data.[24] Although the malicious code has been removed from Active's systems, it operated on the browsers of customers, collecting information entered on the checkout page.[25]

Active noted that due to their regular release of new codes into production every three weeks, the malicious JavaScript code was eradicated with each new production release.[26] Based on Active's investigation, the attacker would then re-enter Active's systems and reintroduce the malicious code with each new release.[27] This pattern persisted until mid-September 2017, "resulting in a 'start/stop' cadence to the attacker activity,"[28] which posed challenges in identification, diagnosis, and investigation. Active has taken numerous steps to halt and address this activity.[29]

Active reaffirmed its belief that the unauthorized party inserted the malicious JavaScript between December 2016 and September 2017.[30] It stated that it initially found out about the concerns regarding transactions in October 2017.[31] Due to the complex nature of the incident, Active had to engage "multiple leading third-party forensics firms to determine what had occurred and who had been impacted."[32] Active enumerated the factors which complicated the incident:

---

[22] *Id.*
[23] Response to NPC's Memorandum dated 07 September 2018, at 2, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[24] *Id.* at 3.
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] Response to NPC's Memorandum dated 07 September 2018, at 3, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[30] *Id.*
[31] *Id.*
[32] *Id.*

- Many of the initial reports of fraud were found to not be fraudulent activity. They were instead identified as normal chargebacks.
- The malicious JavaScript code was no longer present on Active's systems at the time of the investigation, and the unauthorized third party had undertaken extensive efforts to cover their tracks.[33]
- While the investigation was able to identify unauthorized access to the network, it was unable to identify data exfiltration from the network.
- As discussed above in response to question 1(a), the "start/ stop" cycle of attacker activity - whereby Active would release new production code that did not include the malicious JavaScript code every three weeks, after which the unauthorized third party would re-enter the systems and insert the malicious JavaScript code into the new code - made the situation difficult to investigate and diagnose.[34]

Active noted that this incident potentially impacted approximately 1,715 data subjects residing in the Philippines.[35] Active clarified, however, that it believes only a small subset of this total number was actually affected by the malicious JavaScript.[36] Active alleged that it chose to be cautious in its analysis by considering any data subject that could not be definitively excluded as potentially impacted.[37]

Active also stated that the personal data breach may result in payment card fraud[38] since the information involved includes the "name, address, email address, credit or debit card number, expiration date, and cardholder verification code (the three- or four-digit value included on the front or back of payment cards and used for verification of certain transactions).[39]

To address the breach, Active provided a list of primary remediation and containment measures that it took.[40] This includes enhanced endpoint protection technology and continuous 24x7 monitoring

---

[33] *Id.*
[34] *Id.* at 4.
[35] Response to NPC's Memorandum dated 07 September 2018, at 4, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.* at 5.
[40] *Id.*

through full system/network logging.[41] Active also strengthened both its access and authentication protocols with increased use of multifactor authentication alongside improvements in system audit policies, restricted service account use, and limited remote access.[42] Monitoring has been significantly heightened, incorporating File Integrity Monitoring to detect changes in production code and various forms of monitoring to analyze activity within the Active environment.[43] An enterprise-wide password reset has been executed, and segmentation in the Active environment has been enhanced, including specific "air gapping" or complete segmentation to isolate compromised areas.[44]

Lastly, Active notified the affected data subjects in the Philippines on
19 March 2018.[45] In its notification template, Active encouraged recipients to watch out for unauthorized activity and to quickly report any such activity to the relevant bank or payment card brand.[46] At the time of notification, Active claimed that it provided a toll-free call center which individuals could contact for questions or for additional information.[47] Active also mentioned that to their understanding, "any fraudulent activity in relation to the potentially compromised credit cards will be dealt with through the usual procedures of the issuing banks."[48]

Issue

Whether Active notified its affected data subjects, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. Active's submissions
show that it properly notified its affected data subjects, sufficiently

---

[41] Response to NPC's Memorandum dated 07 September 2018, at 5, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.* at 6.
[46] Initial Report, 19 March 2018, at 4, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[47] *Id.* at 5.
[48] Response to NPC's Memorandum dated 07 September 2018, at 6, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).

addressed the breach, and implemented measures to prevent its recurrence.

It is the obligation of a Personal Information Controller (PIC), such as Active, to ensure that affected data subjects of the breach are promptly and properly notified.[49] The Commission has consistently emphasized that the purpose of the required notification to the data subjects of a breach is to allow them to take the necessary precautions or other measures to protect themselves against its possible effects.[50]

Section 17 (D) (3) of NPC Circular 16-03 provides the obligation of a PIC to notify the NPC of a personal data breach and outlines the content of notification, specifically the measures that a PIC should take to address the breach:

> Section 17. *Notification of the Commission*. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification.* The notification shall include, but not be limited to:
>
> . . .
>
> 3. Measures Taken to Address the Breach
>
> a. description of the measures taken or proposed to be taken to address the breach;
> b. actions being taken to secure or recover the personal data that were compromised;
> c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
> d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
> e. the measures being taken to prevent a recurrence of the incident.[51]

---

[49] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).
[50] *Id.*
[51] NPC Circ. No. 16-03, § 17 (D) (3).

In this case, Active notified its affected data subjects through a letter sent through email.[52] Active informed the affected data subjects about the security incident involving Active, as seen in the notification template attached to the Initial Report.[53] It included an explanation on the nature of the incident revealing suspicious activity on its systems related to manually keyed transactions on the Active website between December 2016 and September 2017.[54]

Active informed the affected data subjects that unauthorized third parties accessed personal information, including names, addresses, email addresses, and payment card details.[55] It also explained how it responded to the security incident by engaging cybersecurity firms, enhancing security controls, and notifying regulatory authorities.[56] Active advised the data subjects to remain vigilant for unauthorized activity on their payment card accounts and provided a contact number for inquiries.[57]

Active took measures to sufficiently address the breach and adopted measures to prevent its recurrence. Active promptly informed affected data subjects about the breach, acknowledging the real risk of serious harm.[58] This immediate communication allowed data subjects to take necessary precautions against potential adverse effects. It also established a toll-free hotline to facilitate communication with potentially affected data subjects, making it easier for them to obtain information and have their questions addressed promptly.[59]

Active engaged the services of a third-party cybersecurity firm to investigate the breach incident and significantly bolstered its technical security measures to effectively address the breach and fortify its cybersecurity defenses against potential future threats.[60]

These measures include the enhancement of endpoint protection technology to strengthen security as well as continuous monitoring

---

[52] Initial Report, 19 March 2018, at 3, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[53] *Id.* at 2.
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] Initial Report, 19 March 2018, at 2-3, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[59] *Id.* at 3.
[60] *Id.* at 2.

and full system/network logging.[61] Active also improved its access and authentication protocols through the expanded usage of multifactor authentication.[62]

Active strengthened its system audit policies and imposed restrictions on the use of service accounts and limited remote access. Monitoring measures were significantly intensified, incorporating File Integrity Monitoring to detect and alert on changes to the production code.[63] Active also executed an enterprise-wide password reset to render compromised credentials ineffective.[64] Active also implemented enhanced segmentation, including specific "air gapping," effectively isolated the point of entry used by the unauthorized party, preventing further unauthorized access.[65]

Given the foregoing, the Commission finds that the measures undertaken by Active have sufficiently addressed the incident and prevents its recurrence.

WHEREFORE, premises considered, the Commission resolves that the matter of NPC BN 18-035 In re: Active Network, LLC is **CLOSED**.

SO ORDERED.

City of Pasay, Philippines. 13 November 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

---

[61] Response to NPC's Memorandum dated 07 September 2018, at 5, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.* at 5-6.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

PP
Compliance Officer
Active Network, LLC

JAH
Counsel for Active Network, LLC

ANGARA ABELLO CONCEPCION REGALA & CRUZ LAW OFFICE
Counsel for Active Network, LLC

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: E-SCIENCE CORPORATION **NPC BN No. 20-124**

x----------x

RESOLUTION

***AGUIRRE*, D.P.C.:**

This Resolution refers to the request for Postponement of Notification to affected data subjects of E-Science Corporation ("E- Science") dated 3 July 2020, involving a data breach incident affecting approximately four thousand (4,000) test records of data subjects, for it is still investigating the matter internally.[1]

The Facts

On 26 June 2020, one of E-Science's databases was accessed by a hacker and a schema was created containing a message asking for a ransom. The hacker further stated that E-Science's databases were already downloaded and backed up in their servers. They also warned E-Science that if they do not receive the payment in the next nine (9) days, they will *"sell the database to the highest bidder or use them otherwise."*[2] The sensitive personal information affected were approximately four thousand (4,000) test records of data subjects from eight (8) different organizations including names, e- mail addresses, and work addresses. They claim that no other personal information, passwords, financial data, and real-time data were accessed.[3]

After the said attack was identified, E-Science has conducted the following safeguards that would minimize harm and mitigate the impact of the personal data breach:

[1] E-mail dated 3 July 2020 submitted by the Data Protection Officer of E-Science.
[2] Data Breach Report dated 2 July 2020, at p. 2.
[3] *Ibid*, at pp. 2-3.

(1) June 30: An investigation was started by the Network and Systems Team;
(2) July 1: A meeting between the management and the people involved agreed on a set of preventive measures;
(3) July 2: An initial notification was sent to the National Privacy Commission; and
(4) Other internal security action items have been laid out.[4]

Furthermore, E-Science has described in full the measures taken or proposed to be taken to address the said breach, *to wit:*

(1) Set-up a system where there is a centralized accessibility monitoring of E-Science IP addresses;
(2) Reset all VPN credentials;
(3) Make sure code repository and databases are accessible via VPN or from network in the office only;
(4) No sensitive information is used for test data in Dev/QA instances, and review in UAT instances;
(5) Make sure no sensitive data like password is saved in source code, which then goes to the code repository;
(6) Comply to Web and Device Security Test before releasing a product;
(7) Implement database credentials rotation;
(8) Review project accesses of AWS accounts;
(9) Set multifactor authentication in AWS accounts to on;
(10) Set a standard on naming database schema;
(11) Create and use unique database credentials, instead of current practice of using shared accounts; and
(12) Review the accounts registered to databases and code repository. Also, monitor internal user access.[5]

E-Science has also reported that it was able to restore the test data from back up and that security measures are implemented and monitored regularly. However, it has not yet sent notifications to the affected data subjects because it is still currently doing further investigations so that it can prevent sending the same to unaffected individuals.[6]

---

[4] *Ibid.*, at p. 2.
[5] *Ibid.*, at p. 3.
[6] *Ibid.*, at p. 3.

Hence, on 3 July 2020, E-Science sent an e-mail to the Commission requesting for notification extension to the affected data subjects since it is still investigating the matter internally.[7]

Discussion

This Commission grants the herein request for notification extension or postponement of notification to data subjects of E- Science in accordance with NPC Circular No. 16-03 (Personal Data Breach Management).

Under Section 18(A) of NPC Circular No. 16-03, the personal information controller ("PIC") shall notify the data subjects affected by a personal data breach within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the seventy-two (72) hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.

However, the PIC may request for postponement of the notification when it is not reasonably possible to notify the data subjects within the prescribed period. **Section 18(B) of NPC Circular No. 16-03** provides that:

> **If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for** an exemption from the notification requirement, or **the postponement of the notification.** A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects. The Commission may authorize the

[7] E-mail dated 3 July 2020 submitted by the Data Protection Officer of E-Science.

> postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.[8]

In this case, the hacked data include four thousand 4,000 test records of data subjects from eight (8) different organizations that contain names, e-mail addresses, and work addresses. Moreover, E-Science opted not to send notifications yet in order to prevent sending the same to unaffected individuals.

Considering the large number of test records involved in this data breach incident that not only reach hundreds but thousands, the Commission acknowledges that it may not be reasonably possible for E-Science to notify the affected data subjects within the prescribed period of seventy-two (72) hours upon its knowledge of the said data breach incident. Moreover, E-Science's reasoning that it did not send notifications to prevent sending the same to unaffected individuals is also plausible. To do otherwise may just result to further data breach incidents particularly if it would send notifications without appropriate, accurate, and sufficient safeguards in place in view of the thousands of records involved or affected. Therefore, granting the request for postponement to notify data subjects is proper.

Meanwhile, while E-Science has submitted an Initial Report to notify the Commission of the data breach incident and has acted upon the matter on the notification to data subjects with the request for postponement thereof, it has not however submitted a Full Breach Report as required by NPC Circular No. 16-03.

Under Section 17(C) of NPC Circular No. 16-03, it provides that:

> [T]he Commission shall be notified within the 72-hour period based on available information**. The full report of the personal data breach must be submitted within five (5) days**, unless the personal information controller is granted additional time by the Commission to comply.[9]

[8] Emphasis supplied.
[9] Emphasis supplied.

The Commission has received on 2 July 2020 an Initial Report on the said data breach incident of E-Science. However, no Full Breach Report has been submitted until now. Further, E-Science did not request for and no additional time was granted by this Commission for the submission of the such report. It should be noted that Notification of the Commission and Notification of Data Subjects are two (2) different and separate requirements under Sections 17(C) and 18(A) of NPC Circular No. 16-03, respectively. Thus, the PIC should promptly comply with both sections accordingly.

WHEREFORE, premises considered, E-Science Corporation is **ORDERED to 1) SUBMIT** with dispatch a Full Report of the Personal Data Breach as required under Section 17(C) of NPC Circular No. 16-03**;** and **2) SHOW CAUSE** in writing why it should not be liable for failure to submit a Full Report within the required period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.

Furthermore, the Commission **GRANTS** the request for Postponement of Notification to Data Subjects of E-Science Corporation and directs them to submit proof of compliance thereof within fifteen (15) days from submission of their Full Breach Report. Pending their verification of the full list of affected data subjects, E-Science Corporation is enjoined to use alternative means of notification under Section 18(d) of NPC Circular No. 16- 03.

SO ORDERED.

Pasay City,
Philippines 6 August
2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JYP
Data Protection
Officer E-Science
Corporation

COMPLIANCE AND MONITORING DIVISION GENERAL RECORDS UNIT
National Privacy Commission

IN RE: ROSEWOOD HOTEL GROUP **NPC BN 18-008**
x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is Rosewood Hotel Group's (Rosewood) breach notification involving an incident that affected its guest reservation system.

Facts

On 19 January 2018, Rosewood Hotel Group (Rosewood) notified the National Privacy Commission (NPC) about a data security issue that affected its guest reservation information maintained on the Sabre Hospitality Solutions (Sabre) system.[1]

Sabre is a service provider utilized by Rosewood and other major hotel brands to process guest reservations.[2] Under Rosewood's contract with Sabre, Sabre is obligated to protect Rosewood's guest data from unauthorized use, access, or disclosure with at least reasonable care and the same measures that Sabre uses to protect its own information.[3] The contract also requires Sabre to remain in compliance with the Payment Card Industry Data Security Standard (PCI DSS).[4]

In December 2017, Sabre informed Rosewood that it discovered that between 29 May 2016 and 11 January 2017 an unauthorized party gained access to Rosewood's guest information by obtaining account credentials from Sabre without its authorization.[5]

---

[1] Letter *from* SGH *to* the National Privacy Commission, 19 January 2018, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2018).
[2] *Id.*
[3] Full Breach Report, 11 April 2022, at 3, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[4] *Id.*
[5] Letter *from* SGH *to* the National Privacy Commission, 19 January 2018, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2018).

Sabre explained that the unauthorized party utilized social engineering techniques to improperly access the system.[6] Sabre's investigation revealed that once the system is accessed, the unauthorized party inappropriately reset the password, and in some instances, changed the email address associated with the credentials.[7] In other instances, the unauthorized party would use the credentials to access a limited set of hotel bookings where some reservations included credit card details as payment information.[8]

According to Sabre, the reservation information affected by the incident involved guests' names and payment card information, including cardholder name, payment card number, expiration date, and security code.[9]

Rosewood stated that none of the affected hotels are in the Philippines, however, approximately nineteen (19) Philippine residents were affected by this incident.[10] Rosewood clarified that the issue occurred on Sabre's systems and did not affect Rosewood's own systems.[11]

Sabre also informed Rosewood that other hotel brands were similarly impacted by this issue.[12]

On 10 March 2022, the NPC, through the Complaints and Investigation Division (CID), ordered Rosewood to submit a Full Breach Report and Supporting Documents in relation to its initial notification.[13] The CID also inquired whether the system affected in the breach notification report in 2017 was related or involved the same system affected in the present breach.[14]

---

[6] Post-Breach Report, 01 June 2022, at 3, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[7] *Id.*
[8] *Id.*
[9] Letter *from* SGH *to* the National Privacy Commission, 19 January 2018, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2018).
[10] *Id.* at 2.
[11] *Id.* at 1.
[12] *Id.*
[13] Order (To Submit Full Breach Report and Supporting Documents), 10 March 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[14] *Id.*

On 28 March 2022, Rosewood, through its counsel, filed for a Motion for Extension of Time to submit a full breach report since Rosewood is domiciled in the United States of America (USA) and the information and documents needed would come from Rosewood.[15]

On 29 March 2022, the CID granted Rosewood's request for an extension of time.[16]

On 11 April 2022, Rosewood submitted its Full Breach Report.[17] Prior to the present breach notification matter, Rosewood explained that there was a similar breach notification report involving the same system in 2017.[18] It clarified that the system involved in the 2017 Report to the NPC was Sabre's SynXis Central Reservation System (CRS), which is also the same system affected in the present breach notification.[19]

Rosewood explained that the cause of the issue described in the 2017 report was a compromised Sabre internal account that enabled an unauthorized party to access Sabre's SynXis CRS.[20] Here, the unauthorized party used social engineering tactics against Sabre.[21] It obtained Rosewood account credentials to access Sabre's SynXis CRS and reset email credentials without authorization from Rosewood.[22]

Rosewood informed the CID that it notified some of the affected data subjects through postal mail.[23] Rosewood also posted notices on its website to notify individuals whose contact information could not be found.[24]

---

[15] Motion for Extension of Time, 28 March 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[16] Resolution (of the Motion for Extension of Time dated 28 March 2022), 29 March 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[17] Full Breach Report, 11 April 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[18] *Id.* at 2.
[19] *Id.* at 1.
[20] *Id.*
[21] *Id.* at 2.
[22] *Id.* at 1.
[23] Full Breach Report, 11 April 2022, at 8, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).

On 11 May 2022, the CID issued an Order directing Rosewood to submit a Post-Breach Report containing the proper documentation on the actions it took.[25]

On 01 June 2022, Rosewood submitted its Post-Breach Report.[26]

Rosewood also clarified that only fourteen (14) data subjects are affected in the Philippines instead of nineteen (19) as it initially reported.[27] Rosewood explained that some of the entries appeared to be duplicates.[28]

Rosewood also reported that it revisited its contract with Sabre in order to enhance its security measures against "human dangers" such as social engineering and hacking incidents.[29] The amended contract requires Sabre to ensure that its personnel engaged in processing personal data are dedicated to maintaining confidentiality and must implement suitable technical and organizational safeguards to mitigate risks associated with processing personal data.[30] Lastly, the contract requires Sabre to promptly notify Rosewood upon knowledge of any breaches involving personal data.[31]

Issue

Whether Rosewood conducted proper breach management, including the implementation of reasonable and appropriate security measures.

Discussion

The Commission finds that Rosewood conducted proper breach management and implemented reasonable and appropriate security measures upon knowledge of the incident. Thus, the Commission resolves to close the case.

---

[25] Order (To submit Post-Breach Report), 11 May 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[26] Post-Breach Report, 01 June 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[27] *Id.*
[28] *Id.*
[29] *Id.* at 4.
[30] *Id.*
[31] *Id.* at 2.

Section 20 (a) and (b) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) mandates a Personal Information Controller (PIC) to implement reasonable organizational, physical, and technical measures intended for the protection of personal data:

> Section. 20. *Security of Personal Information.* (a) **The personal information controller must implement reasonable and appropriate organizational, physical and technical measures** intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.
>
> (b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.[32]

Further, Section 17 (D) (3) of NPC Circular 16-03 (Personal Data Breach Management) provides for the PIC's obligation to inform its data subjects of the measures it took to address the breach:

> Section 17. *Notification of the Commission.* The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification.* The notification shall include, but not be limited to:
>
> . . .
>
> 3. Measures Taken to Address the Breach
>   a. description of the measures taken or proposed to be taken to address the breach;
>   b. actions being taken to secure or recover the personal data that were compromised;
>   c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;

---

[32] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (a) & (b) (2012). Emphasis supplied.

d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;

e. the measures being taken to prevent a recurrence of the incident.[33]

As an immediate response, Rosewood informed relevant payment card companies about the security incident.[34] Sabre also separately provided notice to the credit card companies.[35] Sabre also disabled the impacted accounts and addressed the unauthorized access to its system.[36]

Sabre also hired a cybersecurity expert to conduct a forensic investigation and reported the incident to the law enforcement authorities in the USA.[37]

Rosewood notified the Philippine residents through postal mail.[38] In its submissions, Rosewood attached a copy of its notification to the affected data subjects.[39] The notification included a narration of the security incident and all the measures it took to address the breach.[40] Rosewood also provided its contacts details for data subjects to inquire about any questions they may have regarding the matter.[41]

For affected data subjects that Rosewood could not contact, Rosewood released a statement on its website outlining the details of the incident that occurred.[42]

Rosewood implemented a "call center" staffed by employees tasked with answering calls from data subjects whose data has been compromised.[43] Its employees are available to address any inquiries or

---

[33] *Id.*
[34] Full Breach Report, 11 April 2022, at 6, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[35] Letter *from* SGH *to* the National Privacy Commission, 19 January 2018, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2018).
[36] Full Breach Report, 11 April 2022, at 6, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[37] *Id.* at 2.
[38] *Id.* at 8.
[39] *Id.* annex 2.
[40] *Id.*
[41] *Id.*
[42] Post-Breach Report, 01 June 2022, annex 9, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022)
[43] Full Breach Report, 11 April 2022, at 9, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).

provide additional information and assistance.[44] The task involves advising affected data subjects to regularly review their account statements and promptly notify their credit card issuer of any suspicious activity.[45]

To prevent the recurrence of the incident, Sabre took steps to improve its information security program like addressing the secure use of the privileged credentials of SynXis CRS.[46] It also enhanced its password policies and procedures and implemented multi-factor authentication for remote access to SynXiS CRS.[47]

Sabre implemented safeguards such as conducting application and code scanning, maintaining appropriate and up-to-date antivirus protection, conducting regular penetration testing of SynXis CRS components, employing enhanced behavior analytics tools, and undergoing third-party information security assessment.[48]

As an organizational measure, Rosewood maintains that it reviewed its internal policies and procedures to assist Rosewood employees with identifying, responding to, and managing data security incidents, including breaches involving personal data.[49] It also reviewed its Data Security Incident Response Plan in response to data security incidents at Sabre and revised the plan.[50]

Based on the foregoing, the actions taken by Rosewood following the incident allowed it to enhance its security measures and are sufficient to close the matter in accordance with the DPA and NPC Circular 16- 03.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-008 In re: Rosewood Hotel Group is considered **CLOSED.**

SO ORDERED.

---

[44] *Id.*
[45] *Id.*
[46] *Id.* at 6.
[47] *Id.*
[48] *Id.* at 7.
[49] Full Breach Report, 11 April 2022, at 7, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[50] *Id.*

City of Pasay, Philippines.
18 April 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

SGH
Counsel for Rosewood Hotel Group
Parlade, Hildawa, Eco & Panga Law

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: BREACH NOTIFICATION REPORT OF SUN LIFE OF CANADA (PHILIPPINES), INC.

NPC BN 17-027

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is the Compliance dated 11 March 2020 submitted by Sun Life of Canada (Philippines), Inc. (Sun Life) in fulfillment of the directive in the Resolution dated 25 July 2019.[1]

Facts

On 25 July 2019, the Commission issued a Resolution denying Sun Life's request for exemption from notification of data subject upon finding that notification to a single data subject, who is a client of Sun Life, "would not involve costly and disproportionate effort."[2] The dispositive portion of the Resolution states:

> WHEREFORE, this Commission DENIES the request for exemption from the notification requirements, and ORDERS Sun Life of Canada (Philippines) to NOTIFY affected data subject.
>
> Sun Life is further ORDERED to submit a full breach report, including details of notification, thirty (30) days from receipt of this Order.
>
> SO ORDERED.[3]

---

[1] Letter re: Resolutions of the Commission En Banc dated 25 July 2019 and 24 October 2019 (NPC BN No. 17-027 "In Re: Breach Notification Report of Sun Life of Canada (Philippines), Inc.", 05 May 2022, Annex A, *in* In Re: Sun Life of Canada (Philippines), Inc., NPC BN 17-027 (NPC 2022).

[2] NPC BN 17-027, 25 July 2019, at 2 (NPC 2019) (unreported).

[3] NPC BN 17-027, 25 July 2019 (NPC 2019) (unreported).

On 05 September 2019, Sun Life submitted a letter seeking reconsideration of the Resolution.[4] It argued that the notification would only cause "undue alarm" to the data subject considering that the data subject's accounts have remained intact and that no related complaints have been received since the incident was reported.[5] It further claimed that "it is not likely that the information inadvertently disclosed will be used for fraud."[6]

On 24 October 2019, the Commission issued a Resolution denying Sun Life's request for reconsideration since there was no sufficient ground to overturn the Resolution dated 25 July 2019.[7]

On 18 April 2022, the National Privacy Commission's Enforcement Division (EnD) sent a letter to Sun Life instructing it to comply with the Resolution dated 15 July 2019 and to submit proof of notification to the affected data subject.[8]

Sun Life responded to the EnD's letter and reported that it submitted its compliance on 11 March 2020 after it notified the affected data subject.[9] It also submitted a copy of its Compliance dated 11 March 2020 and copies of the email dated 11 March 2020 and the letter dated 09 March 2020 that it sent to the affected data subject.[10]

The Compliance Report dated 11 March 2020 specified that Sun Life completed all the measures it claimed to have initiated to address the breach.[11] These measures included the following:

- Data fix was done in client portal database to correct the email addresses of the affected clients.
- Email addresses of both clients were updated in system.

---

[4] Letter Re: Breach Notification Report of Sun Life of Canada (Philippines), Inc., 05 September 2019, *in* In Re: Sun Life of Canada (Philippines), Inc., NPC BN 17-027 (NPC 2022).
[5] *Id.*
[6] *Id.*
[7] NPC BN 17-027, 24 October 2019, (NPC 2019) (unreported).
[8] Letter Re: Resolutions of the Commission En Banc dated 25 July 2019 and 24 October 2019 (NPC BN 17-027) "In Re: Breach Notification Report of Sun Life of Canada (Philippines), Inc.", 18 April 2022, *in* In Re: Sun Life of Canada (Philippines), Inc., NPC BN 17-027 (NPC 2022).
[9] Letter re: Resolutions of the Commission En Banc dated 25 July 2019 and 24 October 2019 (NPC BN No. 17-027 "In Re: Breach Notification Report of Sun Life of Canada (Philippines), Inc.", 05 May 2022, *in* In Re: Sun Life of Canada (Philippines), Inc., NPC BN 17-027 (NPC 2022).
[10] *Id.* Annex A and B.
[11] Letter re: Resolutions of the Commission En Banc dated 25 July 2019 and 24 October 2019 (NPC BN No. 17-027 "In Re: Breach Notification Report of Sun Life of Canada (Philippines), Inc.", 05 May 2022, Annex A, *in* In Re: Sun Life of Canada (Philippines), Inc., NPC BN 17-027 (NPC 2022).

- The client who was able to access the other client's policy information was instructed to delete any information he may have copied or downloaded from the portal.
- Sun Life's IT department has checked for similar occurrences and none were found.
- Sun Life's Client Portal controls were enhanced, such that: 1) a client can only have one username, and 2) improvement of audit logs were made in the new Client portal.[12]

Further, the Compliance Report dated 11 March 2020 stated that Sun Life notified the affected data subject on 09 March 2020.[13]

In its letter sent to the affected data subject, Sun Life provided information about the incident and the data subject's personal information involved in the breach.[14] It further assured the data subject that it immediately corrected the error, that the data subject's account has been secured, and that no unauthorized transaction was made.[15] It also provided contact details in case the data subject would need more information or assistance.[16]

Issue

Whether Sun Life complied with the Resolution dated 25 July 2019.

Discussion

The Commission resolves to close the case upon finding that Sun Life has complied with the Resolution dated 25 July 2019.

The information provided in the Compliance Report dated 11 March 2020 and the attached copies of the email and the letter sent to the affected data subject are deemed sufficient to prove that Sun Life adequately notified the affected data subject of the details of the breach.

---

[12] *Id.*
[13] *Id.*
[14] *Id.* Annex B.
[15] *Id.*
[16] *Id.*

Sun Life's letter dated 09 March 2020 included the information required under NPC Circular 16-03 (Personal Data Breach Management).

Section 18 (C) of NPC Circular 16-03 provides:

> Section 18. ***Notification of Data Subjects***. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> C. Content of Notification. The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;
> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
> 6. any assistance to be provided to the affected data subjects.
>
> Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay. [17]

The letter specified the nature of the breach as it reported the processing error that resulted in the consolidation of the data subject's policies with another client.[18] It further identified the personal information of the data subject that Sun Life sent by mistake to the other client, particularly his name, address, birthdate, policy number, due date, total accumulated dividends, and cash surrender value[19]

---

[17] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §18 (C) (15 December 2016).
[18] Letter re: Resolutions of the Commission En Banc dated 25 July 2019 and 24 October 2019 (NPC BN No. 17-027 "In Re: Breach Notification Report of Sun Life of Canada (Philippines), Inc.", 05 May 2022, Annex B, *in* In Re: Sun Life of Canada (Philippines), Inc., NPC BN 17-027 (NPC 2022).
[19] *Id.*

Sun Life assured the data subject that it has corrected the error and has secured the account of the data subject through its authentication process.[20] It also advised the data subject to update his password if it included any of the disclosed personal information.[21] It also included its contact details where the data subject can ask for additional information or assistance.[22]

Given the foregoing, the Commission finds that Sun Life has sufficiently notified the affected data subject of the breach.

In addition to this, the Commission notes the measures Sun Life took to address the breach as enumerated in the Compliance Report dated 11 March 2020.

WHEREFORE, premises considered, Commission resolves that NPC BN 17-027 – In Re: Sun Life of Canada (Philippines), Inc. is hereby **CLOSED**.

SO ORDERED.

City of Pasay,
Philippines.
22 September 2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

---

[20] *Id.*
[21] *Id.*
[22] *Id.*

Copy furnished:

ATC
Chief Compliance Officer

MJC
Data Protection Officer

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

EA and TA,

Complainant,

-versus-

NPC Case No. 17-018
For: Violation of Section 25 (b) of the Data Privacy Act of 2012

EJ, EE and **HC,**

Respondents.

x----------x

RESOLUTION

AGUIRRE, D.P.C.

For consideration of the Commission is the Motion for Reconsideration filed by Complainants EA and TA (Complainants) of the Decision dated 15 July 2019 which dismissed the Complaint against the Respondents EJ, EE and HC (Respondents) on the ground that the elements for a violation of Section 25 (b) of the Data Privacy Act of 2012 (DPA) were not sufficiently established.

In Complainants' Motion for Reconsideration, they argued that the Commission's reliance on Section 13(f) of the Act is "misplaced and runs contrary to established law."[1] They state thus:

> 5. Moreover, the Decision states that the "establishment...of legal claims" as an exemption from the prohibition on processing sensitive personal information will set a dangerous precedent in allowing unauthorized persons from processing such personal sensitive information to their own nefarious ends. [2]

---

[1] Motion for Reconsideration dated 09 August 2019, p. 1.
[2] *Ibid.*, at 2.

In Respondents' Comment / Opposition, they stressed that the Motion for Reconsideration, being just a rehash of the Complaint, did not raise new matters that could serve as basis for this Commission to reconsider its Decision. [3]

Discussion

The Commission denies the Complainants' Motion for Reconsideration.

Complainants' arguments relating to the exemption provided under Section 13(f) regarding the "establishment of legal claims" proceed from the erroneous assumption that a pending case is required. As this Commission has held in its Decision:

> "To require a[n existing] court proceeding for the application of Section 13(f)... would not only be to disregard the distinction provided in the law but the clear letter of the law as well. After all, the very idea of 'establishment ... of legal claims' presupposes that there is still no pending case since a case will only be filed once the required legal claims have already been established."[4]

Considering that an existing court proceeding is not required, Complainants' claim that a subpoena duces tecum is always required for the production of documents under Section 13(f) has no basis. The Commission emphasizes that, contrary to the claim of Complainants, there is no violation of Section 26, Rule 132 of the Rules of Court[5] since what was released to the respondents were just certified copies while the original records remained with the Philippine Statistics Authority.

Further, the Commission takes this opportunity to emphasize that it is not for this Commission to determine the merits of the legal claims that may be established pursuant to Section 13(f). As such, contrary to the

---

[3] Comment and/or Opposition to the Motion for Reconsideration dated 20 August 2019.

[4] Decision dated 15 July 2019, p. 9.

[5] Section 26. *Irremovability of public record.* — Any public record, an official copy of which is admissible in evidence, must not be removed from the office in which it is kept, except upon order of a court where the inspection of the record is essential to the just determination of a pending case.

claim of the Complainants, the supposed dismissal of the Falsification case that was filed against the herein Complainants, where the documents from the Philippine Statistics Authority were used, does not negate the respondents' reliance on Section 13(f).

Finally, regarding their argument that allowing the exemption for the "establishment of legal claims" sets a dangerous precedent, the Complainants should note that this exemption is provided in the DPA itself. In any case, in its determination of the lawfulness of processing, the Commission does not rely on the bare assertions that a controller relied on Section 13(f) as its basis.

The determination of a valid reliance on the second part of Section 13(f), i.e. "the processing is necessary for the establishment, exercise or defense of legal claims," requires a consideration of the relationship of the parties at the time of the processing, taking into consideration the juridical ties between them. Whether the legal claim that is established, exercised, or defended, resulted in the filing of an actual case is immaterial since the exercise of these remedies is a decision independent from the existence of a cause of action.

Aside from this, Section 13(f) also requires compliance with the general principles particularly, transparency, legitimate purpose, and proportionality, as well as compliance with the limitations provided by law. This involves, among others, compliance with the procedures set out by law, including those established by government agencies such as the Philippine Statistics Authority in this case for the release of documents in their possession.

The Decision has discussed the principles of legitimate purpose and proportionality. It stated thus:

> As regards legitimate purpose, the Implementing Rules and Regulations (IRR) of the Data Privacy Act provides that the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.[6] This means that the processing done for the establishment of a legal claim

---

[6] Implementing Rules and Regulations of the Data Privacy Act of 2012 (hereinafter, "IRR"), § 18(b).

> should not in any manner be outside the limitations provided by law. The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.
>
> In this case, the collection of the subject documents was in view of the falsification case that was eventually filed with the Regional Trial Court of Roxas City, Iloilo. The processing of the documents for this cannot be considered as wrongful or illegal.
>
> xxx
>
> Aside from legitimate purpose, the qualifier "necessary" also pertains to the general privacy principle of proportionality. Under the IRR, the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed **only if the purpose of the processing could not reasonably be fulfilled by other means**.
>
> The proportionality principle, as manifested in the qualifier "necessary" serves as a sufficient test in determining whether the processing is justified in relation to the declared purpose.
>
> In this case, considering that the documents were used in the falsification case and absent any showing that its use was unjustified, it cannot therefore be said that the processing done by Respondents was not necessary.[7]

The principle of transparency normally relates to the information provided by controllers through their privacy policies, notices, or terms and conditions regarding how personal information of data subjects may be used to establish, exercise, or defend legal claims. In discussing when information about the processing of personal information should be disclosed to the data subject, Section 11 of the DPA provides:

> "Personal information must, be:,
>
> (a) Collected for specified and legitimate purposes determined and declared before, or **as soon as reasonably practicable after collection**, and later processed in a way

---

[7] *Supra*, Note 4.

> compatible with such declared, specified and legitimate purposes only xxx"[8]

This Commission acknowledges, however, that situations may arise where strict compliance with the principle of transparency may "render impossible or seriously impair the achievement of the objectives of [the] processing."[9] In these cases, the controller may continue their processing to establish their legal claims while taking appropriate measures to protect the data subject's rights and freedoms.

If the controller decides to pursue and exercise their legal claim/s by availing of the appropriate remedy provided by law, such as filing a case in court or a quasi-judicial body, the existing requirements of due process during the course of the proceedings should cause the controller to comply with the declaration required under Section 11 of the DPA.

If, after going through the initial processing to establish their claim, the controller decides not to pursue their legal remedy for whatever reason, the controller is bound to comply with their obligations under the Data Privacy Act, including the disposal of the personal information processed.

WHEREFORE, the foregoing considered, this Commission resolves to
DENY the Motion for Resolution filed by Complainants EA and TA.

SO ORDERED.

Pasay City, 5 November 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.

---

[8] Emphasis supplied.
[9] General Data Protection Regulation, Article 14, par. 5(b).

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

EA

TA

EJ

EE

HC

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT

CID BN No. 17-036

IN RE: 2016 UBER DATA BREACH

RESOLUTION

For consideration of this Commission is the data breach notification dated 27 November 2017 of Uber Technologies, Inc.

Section 18 of Circular No. 16-03 provides when notification of data subjects should be done, thus:

> "The data subjects shall be notified within seventy-two (72) hours **upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred**. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is **likely to give rise to a real risk to the rights and freedoms of data subjects.** It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation."[1]

On 14 November 2016, Uber was contacted by an individual who claimed he had accessed Uber user information.[2] The company's security team determined the unauthorized actor had obtained access to a private Uber developer page on GitHub, a third-party software development platform.[3] Using credentials located there, the unauthorized actor was able to access and download certain archived driver and rider data stored in Amazon Web Services, a third-party

---

[1] National Privacy Commission Circular No. 16-03, §18(a). Emphasis supplied.
[2] Records, p. 87.
[3] *Ibid.*

cloud-based storage environment used by Uber. [4] There was no breach of the Uber corporate systems or infrastructure.[5]

The security team quickly determined the means of access, shut down a compromised credential and took other steps intended to confirm that the actors had destroyed and would not use or further disseminate the information.[6] Uber also implemented additional measures to improve its security posture, including instituting additional access controls for services used by engineers such as GitHub.[7] The unauthorized actor's access to this data began on 13 October 2016, and to the best of Uber's knowledge, there was no further access by the actor to this data after 15 November 2016.[8]

On 20 November 2017, Uber B.V., through its CEO, DK, announced on the Uber website that there was a data breach involving parts of its user database that occurred sometime in 2016.[9] DK announced that the data breach was discovered following a review, and that the persons involved in concealing the breach were no longer connected with Uber.[10] DK also said that the perpetrators of the breach destroyed the exposed data after having received financial consideration therefor.[11] At the time of the announcement, this Commission was made to understand that there were more than 50 million users and 7 million drivers across the world who were affected by the breach.[12] We were also informed that what was exposed did not involve credit card information, and it did not involve trip histories.[13]

The compromised data was stored on Amazon Web Service Simple Storage Service ("S3"). S3 allows businesses to store large amounts of data in "buckets", or directories.[14] Access to this requires a login credential consisting of an authorized access key ("access key ID") and a companion secret key.[15]

After the incident, Uber secured the services of Mandiant, an independent cybersecurity firm to review and assess what happened.[16] Thereafter, a teleconference call was held so that this Commission may

---

[4] *Ibid.*
[5] *Ibid.*
[6] *Ibid.*
[7] *Ibid.*
[8] *Ibid.*
[9] *Id.*, at p.65.
[10] *Ibid.*
[11] *Ibid.*
[12] *Ibid.*
[13] *Ibid.*
[14] *Id.*, at p.66.
[15] *Ibid.*
[16] *Ibid.*

clarify its queries with Uber.[17] During the call, Uber admitted that there was one Filipino whose Philippine driver's license was exposed and that his number was initially among those considered as having been exposed in the United States.[18] Uber then informed this Commission that the affected driver was notified of his exposure, and that steps were being taken to inform Filipinos of the breach.[19] In addition, Uber also put up notices in the Help section of the Uber app and on the main Uber website.[20] A dedicated Uber address [ ] was also indicated.[21] Uber reported that only one in-app inquiry about the incident, and two e-mails to the dedicated address were received,[22] but these were not related to the incident.[23]

Since this incident occurred, Uber has constantly communicated and updated this Commission on the status of their investigation and the efforts they took to mitigate the impact of the breach. Considering that the data has not been found by the Commission's investigators in the surface, deep, or dark web; that the employees responsible for the response to the incident have been let go; and that there were extensive measures to reach out to the public, the matter is one where the Commission determines that the further notification of affected data subjects is no longer required. Also, considering that there appears to be no immediate harm to the data subjects, no further action is recommended on this matter.

WHEREFORE, all premises considered, this Commission finds no further action necessary in this matter without prejudice to such other reliefs in case any new information arises.

SO ORDERED.

City of Pasay, Philippines
31 July 2019.

---

[17] *Ibid.*
[18] *Ibid.*
[19] *Ibid.*
[20] *Ibid.*
[21] *Ibid.*
[22] *Ibid.*
[23] *Ibid.*

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
IVY D. PATDU
Deputy Privacy Commissioner

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy

Commissioner COPY FURNISHED:

UBER TECHNOLOGIES, INC.
Market Street
San Francisco, California

IN RE: FAMILYHAN CREDIT CORPORATION

INITIATED AS AN INDEPENDENT NPC INVESTIGATION INTO THE POSSIBLE DATA PRIVACY VIOLATIONS COMMITTED BY FAMILYHAN CREDIT CORPORATION

x----------x

NPC SS 20-001

For: Violation of the Data Privacy Act of 2012

RESOLUTION

AGUIRRE, *D.P.C.;*

This Commission resolves a Motion to Lift Cease and Desist Order filed by Familyhan Credit Corporation (FCC) dated 21 June 2021.

Facts

On 15 October 2020, the Commission ordered FCC to cease and desist from the processing of personal information on their database:

> **WHEREFORE,** premises considered, Familyhan Credit Corporation and its responsible officers and members of the Board, MTR, VBV, JPV, AA, and MDA are here by ordered to:
>
> 1) File a **COMMENT**, within ten (10) days from receipt of this Order, on the allegations in the attached Fact-Finding Report, pursuant to Section 24 of the NPC Rules of Procedure; and
> 2) **CEASE AND DESIST** from the processing of personal data on their database until the Commission issues a decision on the submission of the Comment, which shall be made no more than thirty (30) days from the expiration of the period to file a Comment or of the termination of the clarificatory hearing if one is held, pursuant to NPC Circular No. 20-01.
>
> **SO ORDERED.**[1]

[1] Order, 15 October 2020, at 7, *in* In re: Familyhan Credit Corporation.

FCC filed its Comment to the Cease and Desist Order (CDO) on 25 January 2021. It prayed that the Commission reconsider and dismiss the Order dated 15 October 2020 for lack of merit. [2]

The Commission sustained the CDO in an Order dated 23 February 2021. The Commission held that the CDO may be modified or lifted by the Commission only upon FCC's showing that the factual or legal basis for which it was issued no longer exists:

> **WHEREFORE,** premises considered, the Cease and Desist Order issued against Familyhan Credit Corporation and its responsible officers and members of the board, MTR, VBV, JPV, AA, and MDA to cease and desist from the processing of personal data on Familyhan's database is hereby sustained until modified or lifted by the Commission upon showing that the factual or legal basis for which it was issued no longer exists x x x.[3]

On 08 April 2021, the Commission conducted a Clarificatory Hearing with FCC where it ordered FCC to submit additional documents.[4]

On 26 May 2021, FCC submitted a Motion to Clarify Order requesting additional time to submit the documents the Commission required during the Clarificatory Hearing. FCC also requested, by email, "for the possible amicable settlement and resolution of the case."[5]

The Commission issued a Resolution dated 01 June 2021 granting a non-extendible fifteen-day period to submit the documents and denying the request for amicable settlement. The Commission emphasized that it is not in the position to enter an amicable settlement in a *sua sponte* investigation. Such would be a disservice to the data subjects who faced the risks and harm posed by the acts allegedly committed by FCC.[6]

On 21 June 2021, FCC filed a Motion to Lift Cease and Desist Order (Motion to Lift CDO), and prayed:

> **WHEREFORE**, premises considered, it is most respectfully prayed unto this Honorable Office that the ORDER to CEASE

---

[2] Comment by Familyhan Credit Corporation, 25 January 2021, at 5.
[3] Order, 23 February 2021, at 4, *in* In re: Familyhan Credit Corporation.
[4] Order, 08 April 2021, *in* In re: Familyhan Credit Corporation.
[5] E-mail *from* AVM, Collaborating Counsel of Familyhan Credit Corporation *to* National Privacy Commission (26 May 2021).
[6] Resolution, 01 June 2021, at 4, *in* In re: Familyhan Credit Corporation.

> AND DESIST from processing personal data on the LFA be LIFTED.
>
> Other reliefs just and equitable under the circumstances are likewise prayed for.[7]

FCC maintains that it stopped processing personal information on its database and ordered its loan agents to discontinue from doing the same.[8] It states that the loan agents' access to its system has also been cut off by its IT Department.[9] It further alleges that the CDO issued by the Commission on 15 October 2020 is deemed automatically lifted pursuant to Section 12 of the Rules on the Issuance of Cease and Desist Order (NPC Circular No. 20-02), and that the basis for issuing the CDO no longer exists since new security measures were introduced to its system.[10]

The Commission issued an Order dated 24 June 2021 directing the Complaints and Investigation Division (CID) of the National Privacy Commission (NPC) to Comment on FCC's Motion to Lift CDO.[11]

Issue

Whether FCC's Motion to Lift CDO should be granted.

Discussion

The Commission denies FCC's Motion to Lift CDO. The Extended CDO remains in force and effect.

FCC hinges its prayer on the following: *first*, the CDO is automatically lifted pursuant to Section 12 of NPC Circular No. 20-02, and *second*, the basis for which the CDO was issued no longer exists. Both reasons cited by FCC are untenable.

First, contrary to FCC's allegations, the issued CDO is not automatically lifted in line with Section 12 of NPC Circular No. 20-01.

---

[7] Motion to Lift Cease and Desist Order by Familyhan Credit Corporation, 21 June 2021, at 3.
[8] *Id*, at 1.
[9] *Id*.
[10] *Id*, at 2.
[11] Order, 24 June 2021, at 4, *in* In re: Familyhan Credit Corporation.

Section 12 of NPC Circular 20-02 refers to an ex-parte CDO. It allows the Commission to lift or extend the effectivity of an issued CDO after the adverse party is given an opportunity to be heard.[12] It grants the Commission a thirty-day period within which the Commission decides to lift or extend the issued CDO.[13] Section 12 provides:

> **Section 12. Decision on the Issued CDO**. – If after giving the Adverse Party the opportunity to be heard, it appears that the applicant is entitled to have the act or practice enjoined and that there is a need for the extension of the issued CDO, the Commission shall extend its effectivity, otherwise, the same shall be lifted.
>
> The decision whether to extend or lift the issued CDO shall be made no later than thirty (30) days from the expiration of the period for the Adverse Party to file a comment or the termination of the clarificatory hearing if one is held. In the event that the Commission fails to render its decision within the said period, the CDO shall be deemed automatically lifted.[14]

In the Order dated 23 February 2021, the Commission extended the issued CDO within the period provided by law.[15] As a result, the nature of the issued CDO is that of an Extended CDO that remains in force and effect until the Commission modifies or lifts it. The applicable provision is Section 13 of NPC Circular No. 20-02, which provides:

> **Section 13. When CDO is Extended**. – The extension of the CDO issued by the Commission shall also include an order to submit the necessary compliance report within the time prescribed for monitoring purposes. The concerned NPC unit shall ensure that a copy of such order be immediately furnished to each party subject thereto.
>
> **The extended CDO shall remain in force and effect until the same is modified or lifted by the Commission upon showing that the factual or legal basis for which it was issued no longer exists.**[16]

---

[12] National Privacy Commission, NPC Circular No. 21-02, "Rules on the Issuance of Cease and Desist Orders" [NPC Circ. No. 21-02], § 12 (6 October 2020). Emphasis supplied.
[13] *Id.*
[14] *Id.*
[15] Order, *supra* note 3, at 4.
[16] NPC Circ. No. 21-02, § 13. Emphasis supplied.

FCC will recall that it was given the opportunity to be heard when the Commission issued an Order dated 15 October 2020 and required FCC to file a Comment on the Fact-Finding Report.[17] An opportunity to be heard means an opportunity to explain or to adduce any evidence a party may have to in support of his defense.[18] It must be emphasized that an opportunity to be heard is not strictly limited to the conduct of a hearing. No less than the Supreme Court explained that:

> In administrative proceedings, the essence of due process is simply the opportunity to explain one's side. **One may be heard, not solely by verbal presentation but also, and perhaps even much more creditably as it is more practicable than oral arguments, through pleadings.** An actual hearing is not always an indispensable aspect of due process. **As long as a party was given the opportunity to defend his interests in due course, he cannot be said to have been denied due process of law, for this opportunity to be heard is the very essence of due process.** x x x.[19]

Here, FCC was given several opportunities to present its side. It submitted a Comment on the Fact-Finding Report dated 21 January 2021, a Comment on the Order dated 25 January 2021, and an Answer dated 01 February 2021. However, none of these submissions warranted a lifting of the issued CDO, as provided in the Commission's Order dated 23 February 2021.[20]

In paragraph 6 of the Motion to Lift CDO, FCC claims that "it is clear from the Rules … the [CDO] dated 15 October 2020 to which FCC filed a Comment on 25 January 2021 is deemed automatically lifted."[21] FCC erroneously relies on the last sentence of Section 12, which states:

> **Section 12. Decision on the Issued CDO**. – x x x In the event that the Commission fails to render its decision within the said period, the CDO shall be deemed automatically lifted. [22]

---

[17] Order, *supra* note 1, at 7.
[18] National Power Corporation Board of Directors v. Commission on Audit, G.R. No. 218052, 26 January 2021.
[19] F-C v.C, A.M. No. RTJ-15-2438, Sept. 15, 2020 (citing Lumiqued v. Exevea, G.R. No. 117565, 18 November 1997). Emphasis supplied.
[20] Order, *supra* note 3, at 4.
[21] Motion to Lift Cease and Desist Order, *supra* note 7, at 2.
[22] NPC Circ. No. 21-02, § 12.

FCC failed to appreciate that the Commission rendered its decision to extend the CDO on 23 February 2021, which is within the thirty-day period provided under Section 12.[23]

Section 12 clearly states that the thirty-day period is computed either from the expiration of the period for FCC to file a Comment or the termination of the clarificatory hearing.[24] The Commission ordered FCC to file a Comment within ten (10) days from receipt of the Order dated 15 October 2020.[25] In its Comment dated 21 January 2021, FCC maintained that it received the Order on 15 January 2021, thus allowing it to file a Comment until 25 January 2021.[26] Hence, the thirty- day period to file FCC's Comment commenced on 25 January 2021 and ended on 24 February 2021.

Considering the foregoing, FCC's contention that the CDO is automatically lifted due to the Commission's alleged failure to render a decision within the thirty-day period is wrong. The Commission rendered its decision to extend the CDO in an Order dated 23 February 2021, which is within the thirty-day period from the expiration of the period given to FCC to issue a Comment.

On the second ground, the basis for which the CDO was issued continues to exist. FCC failed to sufficiently prove that the risk of unauthorized disclosure is no longer present.

To reiterate, Section 13 of NPC Circular No. 16-03 provides:

> **Section 13. When CDO is Extended**. – x x x
>
> The extended CDO shall remain in force and effect until the same is modified or lifted by the Commission **upon showing that the factual or legal basis for which it was issued no longer exists.** [27]

Here, FCC failed to submit evidence to show, much less prove, that these new security measures are already in place and the manner by which these security measures effectively eliminate the risk to the data subjects, as FCC claims in its Motion to Lift CDO.

---

[23] Order, *supra* note 3, at 5.
[24] NPC Circ. No. 21-02, § 12.
[25] Order, *supra* note 1, at 7.
[26] Comment by Familyhan Credit Corporation, 21 January 2021, at 1.
[27] NPC Circ. No. 21-02, § 13. Emphasis supplied.

In the Motion to Lift CDO, FCC reiterated the security features it implemented to address the security breach.[28] The discussion was directly lifted from FCC's Comment dated 25 January 2021.[29] These include the expiration of the link for the borrower-clients' e-signatures, randomization of password and pin code of the General Manager, and limitation of system access to the General Manager.[30] FCC claims that:

> Once the NPC lifts the [CDO] dated 15 October 2020 issued against FCC, the new security features of the [FCC System], which are already in place, will eliminate the risk of unauthorized disclosure.[31]

FCC supposedly introduced new security features to their system. However, it failed to concretely show how these will eliminate the risk of unauthorized disclosure. It is not sufficient for FCC to simply enumerate the security features it introduced and categorically claim that these will eliminate risk once the Extended CDO is lifted. Merely alleging that FCC has implemented new security measures that will eliminate risk does not satisfy the requirement to lift the Extended CDO under Section 13 of NPC Circular No. 16-03. It is incumbent upon FCC to show that the factual or legal basis for which the Extended CDO was issued no longer exists.

FCC did not present anything, either in the Comment dated 25 January 2021 or in the Motion to Lift CDO, to convince the Commission otherwise. In fact, the Motion to Lift CDO also reiterated the Comment that referred to the Affidavits of Undertaking of FCC's General Manager and President.[32] FCC furnished Affidavits of Undertaking to the Commission as part of the Comment dated 25 January 2021.[33] The Motion to Lift CDO[34] and the Comment[35] both state that, as stated in the Affidavits of Undertaking, FCC "**will adopt** methods and protocols to ensure compliance with NPC rules and regulations." Despite a period of almost six (6) months from the time FCC filed the Comment on 25 January 2021, FCC has not presented any details or

---

[28] Motion to Lift Cease and Desist Order, *supra* note 7, at 2.
[29] Comment, *supra* note 2, at 4-5.
[30] Motion to Lift Cease and Desist Order, *supra* note 7, at 2.
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] Comment, *supra* note 2, at 5.

evidence in the Motion to Lift CDO on the supposed methods and protocols it undertook to adopt in its Affidavit of Undertaking.

FCC also failed to conduct the necessary audits to verify that these security measures are effective to eliminate risk. The Commission emphasizes that FCC should have verified the adequacy and efficacy of these security measures against unauthorized disclosure, even while the CDO is in place. There is no need for FCC to wait until the CDO is lifted to demonstrate to the Commission that these security features can actually eliminate the risk of unauthorized disclosure sought to be prevented by the CDO. Absent proof to the contrary, the Commission finds no reason to lift the Extended CDO.

WHEREFORE, premises considered, the Motion to Lift Cease and Desist Order filed by Familyhan Credit Corporation is **DENIED.** The Extended CDO shall **REMAIN IN FORCE AND EFFECT** until the Commission modifies or lifts the same upon showing that the basis for which it was issued no longer exists.

SO ORDERED.

City of Pasay, Philippines.
23 July 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA

Deputy Privacy Commissioner

Copy furnished:

ATTY. JRO
Counsel
Familyhan Credit Corporation

ATTY. AVM
Collaborating Counsel
Familyhan Credit
Corporation

SMA
President
Familyhan Credit Corporation

RA
Vice President
Familyhan Credit Corporation

MRO
Treasurer
Familyhan Credit Corporation

MJR
Corporate Secretary
Familyhan Credit
Corporation

PPM
Director
Familyhan Credit Corporation

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FAMILYHAN CREDIT CORPORATION

Initiated as an Independent NPC Investigation into the Possible Data Privacy Violations Committed by Familyhan Credit Corporation

x----------x

NPC SS 20-001
For: Violation of the Data Privacy Act (DPA) of 2012

RESOLUTION

For Resolution of the Commission are the Motion to Clarify Order submitted by Respondent Familyhan Credit Corporation (Familyhan) and an email request by a collaborating counsel of Familyhan to enter into amicable settlement of this case.

Facts

On 08 April 2021, the Commission conducted a Clarificatory Hearing pursuant to its Order dated 23 February 2021. This was followed by an Order for the submission of several documents as agreed during the hearing. The pertinent excerpt of the dispositive portion stated:

> **WHEREFORE**, all premises considered, the Commission hereby **ORDERS** Respondent Familyhan Credit Corporation to submit the above documents within **FIFTEEN DAYS (15)** from the date of the Clarificatory Hearing.
>
> Failure to comply with this Order shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

Following this, Respondent Familyhan filed a Motion to Clarify Order dated 26 May 2021. They stated thus:

> 5. On 26 May 2021, FCC received through LBC a copy of the Order dated April 2021 which indicates that it is directed to submit the

> documents listed therein within FIFTEEN (15) days from the date of the Clarificatory Hearing.
>
> 6. The FIFTEEN (15) day period to submit the documents listed in the Order dated 08 April 2021 lapsed on 23 April 2021. However, it was only on 26 May 2021, more than a month after the lapse of the fifteen (15) days from the date of the Clarificatory Hearing that FCC received a copy of the said Order;
>
> 7. There was no way before the receipt of the Order dated 08 April 2021 for FCC to determine which documents the Honorable Commission needs to resolve the above-mentioned case;
>
> xxx
>
> 9. It seeks the kind indulgence of the Honorable Commission to allow FCC to submit the documents listed on the Order dated 08 April 2021, fifteen (15) days from receipt of the said Order, which is until 10 June 2021.
>
> 10. The filing of this motion has no intention to disregard the processes of the Honorable Commission nor delay the proceedings or much less frustrate the ends of justice.

On the same day, the Commission, through the Complaints and Investigation Division (CID), received an email from Atty. AVM, collaborating counsel of Respondent Familyhan, stating thus:

> Good afternoon Sir Madam
>
> Relative to the above entitled case, may we request for an appointment with the Commissioner Raymundo Liboro for the possible amicable settlement and resolution of the case.
>
> Your favorable action on the matter will be
>
> appreciated. Very Truly Yours,
>
> Atty. AVM
> Collaborating Counsel-Familyhan Credit Corp.

Discussion

Upon consideration of the allegations stated in the Motion to Clarify Order and in the interest of an exhaustive investigation, the Commission grants the request for Respondent Familyhan to submit

the required documents within fifteen (15) days from receipt of the said Order, which is until 10 June 2021.

The Commission, however, refutes the allegation in paragraph 7 of Respondent Familyhan's Motion which states that "there was no way before the receipt of the Order dated 08 April 2021 for FCC to determine which documents the Honorable Commission needs to resolve the above-mentioned case." The Commission reminds Respondent Familyhan that all of the documents required in its Order were discussed and agreed upon during the Clarificatory Hearing on 08 April 2021. Given this, the additional time granted for the submission of documents will be non-extendible.

As to the email request for an appointment "for the possible amicable settlement and resolution of this case", the Commission denies this request.

The Fact-Finding Report, which serves as the Complaint in this case, details how the personal and sensitive personal information of more than six thousand (6,000) data subjects were accessed by unauthorized persons using simple steps that can be done through a web browser. The Commission's CID was able to confirm the accessibility of the database by following the steps as indicated in the email and in the Facebook group. Based on these, the Report stated:

> In sum, there is sufficient ground to support the finding that FamilyHan violated the following penal provisions of law:
>
> > Section 26 of the DPA. Accessing Personal Information and Sensitive Personal Information Due to Negligence – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than five hundred thousand pesos (Php 500,000.00) but not more than two million pesos (Php 2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.
> >
> > (b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than five hundred thousand pesos (Php

> 500,000.00) but not more than four million pesos (4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.
>
> xxx
>
> Section 30 of the DPA. Concealment of Security Breaches Involving Sensitive Personal Information – The penalty of imprisonment one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php 500,000.00) but not more than One million pesos (Php 1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach.

Such provisions impute criminal liability to the responsible officers of Respondent Familyhan. Due to the seriousness of the allegations and risks poses to the data subjects, it is the Commission itself, through the CID, that instituted action based on certain criteria provided in its Rules of Procedure. NPC Circular No. 16-04 or the Rules of Procedure of the NPC[1] provides the circumstances which merit a *sua sponte* investigation:

> **SECTION 23. *Own initiative*.** – Depending on the nature of the incident, in cases of a possible **serious privacy violation or personal data breach, taking into account the risks of harm to a data subject**, the Commission may investigate on its own initiative the circumstances surrounding the possible violation. Investigations may include on-site examination of systems and procedures. If necessary, the Commission may use its enforcement powers to order cooperation of the personal information controller or other persons, with the investigation or to compel appropriate action to protect the interests of data subjects.

Considering the public interests that the Commission represents, it is therefore not in the position to enter into amicable settlement with a respondent in a *sua sponte* investigation. Such would be a disservice to the data subjects that faced the risks and harm posed by the acts allegedly committed by the respondent in the *sua sponte* investigation.

[1] Dated 15 December 2016.

This is all the more true considering the exception of criminal liability from the scope of the application of the Alternative Dispute Resolution Act of 2004 (ADRA).[2]

Despite the State Policy[3] of the ADRA to "actively promote party autonomy in the resolution of disputes or the freedom of the party to make their own arrangements to resolve their disputes", it explicitly provides an exception:

> Section 6. Exception to the Application of this Act. – The provisions of this Act shall not apply to resolution or settlement of the following: (a) labor disputes covered by Presidential Decree No. 442, otherwise known as the Labor Code of the Philippines, as amended and its Implementing Rules and Regulations; (b) the civil status of persons; (c) the validity of marriage; (d) any ground for legal separation; € the jurisdiction of courts; (f) future legitime; **(g) criminal liability;** and (h) those which by law cannot be compromised.[4]

Lastly, the Commission warns Respondent Familyhan that such requests for amicable settlement in criminal cases may be admissible as evidence of guilt. The Rules of Evidence, which apply suppletorily to the proceedings of the Commission, provide:

> **Rule 130. Rules of Admissibility**
>
> Section 28. Offer of compromise not admissible. – In civil cases, an offer of compromise is not an admission of any liability, and is not admissible in evidence against the offeror.
>
> xxx
>
> **In criminal cases, except those involving quasi-offenses (criminal negligence) or those allowed by law to be compromised, an offer of compromise by the accused may be received in evidence as an implied admission of guilt.**

[2] R.A. 9285. An Act to Institutionalize the Use of An Alternative Dispute Resolution System in the Philippines and to Establish the Office for Alternative Dispute Resolution, and for Other Purposes. Dated 2 April 2004.
[3] *Id.*, at Section 2.
[4] Emphasis supplied.

Respondent Familyhan, therefore, is advised to exercise prudence before it makes such requests without basis in the law.

WHEREFORE, all premises considered, the Commission hereby **ORDERS** Respondent Familyhan Credit Corporation to submit, **within a non-extendible period of FIFTEEN DAYS (15) from its receipt of the Commission Order dated 08 April 2021 or until 10 June 2021**, the documents required therein.

Failure to comply with this shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

Further, the Commission **DENIES** the request of Respondent Familyhan Credit Corporation to enter into amicable settlement for the resolution of this case.

SO ORDERED.

City of Pasay, Philippines;
01 June 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA

Deputy Privacy Commissioner

COPY FURNISHED:

JRO
Counsel
Familyhan Credit Corporation

AVM
Collaborating Counsel

MSV
Counsel
Former Respondents
MTR, VBV, JPV, AA, and
MDA

SMA
President
Familyhan Credit Corporation

RA
Vice President
Familyhan Credit Corporation

MRO
Treasurer
Familyhan Credit Corporation

MJR
Corporate Secretary
Familyhan Credit Corporation

PPM
Director
Familyhan Credit Corporation

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: CATHAY PACIFIC AIRWAYS LIMITED **NPC BN 18-198**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

This Commission resolves the sufficiency of notification of the data subjects and the evidence of such notification submitted by Cathay Pacific Airways Limited (Cathay Pacific) in line with NPC Circular No. 16-03 (Personal Data Breach Management).

Facts

On 18 March 2021, the Commission ordered Cathay Pacific to submit evidence of notification to the affected data subjects in or from the Philippines and explain any discrepancy between its analysis of the number of affected data subjects, exposed passport numbers, and accessed credit card numbers:

> **WHEREFORE,** all premises considered and pursuant to the requirements of Section 18(A) and Section (D) of Circular No. 16- 03, the Commission **ORDERS** Cathay Pacific Airways Limited to submit evidence of notification to the affected data subjects in or from the Philippines and explain any discrepancy from its abovementioned analysis of affected data subjects, exposed passport numbers, and accessed credit card numbers **within fifteen (15) days** from receipt of this Order.
>
> **SO ORDERED.**[1]

On 28 April 2021, Cathay Pacific submitted its response to the Order dated 18 March 2021. It explained the following:

---

[1] Order, 18 March 2021, at 18, *in* In re: Cathay Pacific Airways Limited, NPC BN 18-198.

1. There is no inconsistency between the number of reported notifications and the total number of its affected data subjects. The affected data subjects who were neither notified by email nor by post were notified on 24 October 2018 by general notice posted on the Cathay Pacific website;
2. On 28 October 2018, it completed notification by email its affected data subjects for whom it had email addresses of;
3. On 12 November 2018, it completed notification by post its affected data subjects for whom it had postal addresses of;
4. It no longer retains details of the email notifications that were sent to its affected data subjects. It engaged Acoustics, an email service provider, to send email notifications in 2018. The records, however, have been purged and are therefore no longer available. It attached a screenshot of Acoustics' setting page showing the retention period set for Cathay Pacific's account and its Data Retention Policy, and a screenshot of Acoustics records page showing that the records have been deleted from the system;
5. It committed to submit proof of postal notifications as soon as it receives such from Experian, the printing house it engaged to send out postal notifications.[2]

On 31 May 2021, the Commission, through its Enforcement Division (EnD), sent an Enforcement Letter to Cathay Pacific. It explained to Cathay Pacific that although Acoustics had already purged its records, it remains incumbent upon Cathay Pacific to prove that notification of its affected data subjects took place.[3] It also informed Cathay Pacific that it required further proof that Cathay Pacific posted the general notice on its website.[4] As a result, the Commission, through the EnD, ordered Cathay Pacific to submit the following documents:

> Taking into consideration the foregoing remarks, you are ordered to submit the following within FIFTEEN (15) days from the receipt of this letter:
>
> 1. Evidence of notification to the affected data subjects from Experian;
> 2. Affidavit of the sender attesting to the truth that the notifications were sent through electronic mail to the 64,305 affected data subjects;
> 3. Proof of publication of the general notification in Cathay's Website;

---

[2] Compliance Report *from* BCCS Law *to* National Privacy Commission (28 April 2021), at 1-2.
[3] Enforcement Letter *from* Enforcement Division, National Privacy Commission *to* Cathay Pacific Airways Limited (31 May 2021), at 2.
[4] *Id*, at 2.

4. A corrected version of "Annex A" as there is a distorted page which renders it unreadable.[5]

On 22 June 2021, Cathay Pacific submitted the following compliance documents in response to the Enforcement Letter dated 31 May 2021:

1. Evidence of notification by post to the affected data subjects, for whom it had postal addresses of, in the form of invoices issued by Experian;
2. An affidavit executed by the Head of Customer Experience - Digital, LOA, affirming that Cathay Pacific notified by email its affected data subjects for whom it had email addresses of;
3. Proof of publication of the general notification on its website;
4. Contents of the general notification published on its website and the individual notification sent by email and by post to its affected data subjects; and
5. A corrected version of "Annex A", which refers to its Data Retention Policy.[6]

Discussion

The Commission finds sufficient Cathay Pacific's notification of its affected data subjects and the evidence of such notification that it submitted pursuant to the Order dated 18 March 2021. The Commission also finds Cathay Pacific's explanation on the consistency between the number of reported notifications and the total number of its affected data subjects to be satisfactory.

Section 18 (C) of NPC Circular No. 16-03 provides the necessary contents of the notification to the affected data subjects:

> **SECTION 18.** *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> x x x
>
> C. Content of Notification.

[5] *Id.*
[6] Compliance Report *from* BCCS Law *to* National Privacy Commission (22 June 2021), at 2.

> The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;
> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
> 6. any assistance to be provided to the affected data subjects.
>
> Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.[7]

The contents of the general notice published on the Cathay Pacific website and the individual notifications by post and by email that Cathay Pacific issued satisfy these requirements. These notices contained sufficient information on the nature of the breach incident, the personal data involved, the measures Cathay Pacific took to address the breach and reduce harm or negative consequences of the breach, and the assistance it extended to its affected data subjects.[8]

In its efforts to mitigate the negative consequences of the breach incident, Cathay Pacific offered a twelve-month complimentary identity monitoring services to its affected data subjects to monitor if the affected data subject's personal data are available on public websites, chat rooms, blogs, and non-public places on the internet.[9] It also advised its affected data subjects to change their passwords regularly, check for any suspicious activities, and remain vigilant against phishing and other attempted scams.[10]

Section 18 (D) of NPC Circular No. 16-03 requires a personal information controller (PIC) to establish all reasonable means to ensure that its affected data subjects are notified of the breach incident:

> **SECTION 18.** *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected

---

[7] National Privacy Commission, NPC Circular No. 16-03, "Personal Data Breach Management" [NPC Circ. No. 16-03], § 18
(C) (15 December 2016). Emphasis supplied.
[8] Proof of Publication of General Notice *from* Cathay Pacific Airways Limited (24 October 2018), at 2; Final Individual Notice *from* Cathay Pacific Airways Limited, at 2.
[9] *Id.*
[10] *Id.*

> by a personal data breach, subject to the following procedures:
>
> x x x
>
> D. Form. **Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic.** The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach**: Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[11]

The Commission recognizes that Cathay Pacific took considerable efforts to fulfill the mandatory notification requirement under NPC Circular No. 16-03. Cathay Pacific conducted the notification by email, by post, and by posting a general notice on its website.[12] Despite the large number of individuals affected in the breach incident, Cathay Pacific employed a variety of means to ensure that all its affected data subjects were notified of the breach incident in compliance with Section 18 (D) of NPC Circular No. 16-03.

Cathay Pacific likewise complied with the Commission's Order dated 18 March 2021. It submitted sufficient evidence to prove that it notified its affected data subjects of the breach incident. The Commission deems sufficient the evidence that Cathay Pacific submitted in line with the Order dated 18 March 2021.

Considering the foregoing, the Commission finds that Cathay Pacific complied with the mandatory notification requirement of its affected data subject pursuant to Section 18 of NPC Circular No. 16-03.

---

[11] NPC Circ. No. 16-03, § 18 (D).Emphasis supplied.
[12] BCCS Law, *supra* note 6.

WHEREFORE, premises considered, the Commission hereby finds that Cathay Pacific Airways Limited has sufficiently notified its affected data subjects and complied with the Order dated 18 March 2021. This Commission hereby considers the matter **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
23 September 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

Atty. PRC
Betita, Cabilao, Casuela, Sarmiento Law
Counsel of Cathay Pacific Airways Limited

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: VRP MEDICAL CENTER **NPC BN 18-062**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is a breach notification submitted by VRP Medical Center (VRP) involving a falsified official receipt and statement of account.

Facts

On 27 April 2018, VRP received a letter from Metrocare Health Systems Inc. (Metrocare) verifying availments made by BL, a member of Metrocare.[1] VRP also received a copy of the Official Receipt (OR) and the Statement of Account (SOA) that BL submitted.[2]

Upon checking its system, VRP discovered that BL had no transactions with VRP.[3] It determined that the OR and SOA submitted by BL to Metrocare belonged to two different patients.[4]

VRP compared the falsified OR and SOA submitted by BL to the OR and SOA available on its record. VRP emphasized that the details on the falsified OR were handwritten.[5] It further stated that while the falsified SOA followed VRP's standard format and layout for statements of account, a different font type was used.[6]

VRP stated that "there has been some type of breach over the financial accounts of the real owners of the OR and SOA."[7] VRP stated,

---

[1] Initial Report, 02 May 2018, at 1, *in* In re: VRP Medical Center, NPC BN 18-062 (NPC 2018).
[2] *Id.*
[3] *Id.* at 2.
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] Initial Report, 02 May 2018, at 2, *in* In re: VRP Medical Center, NPC BN 18-062 (NPC 2018).

however, that it will still investigate the matter after obtaining consent from the involved patients.[8]

VRP further stated that it would inform Metrocare that BL had no transactions with VRP.[9]

On 02 May 2018, VRP notified the National Privacy Commission (NPC) of the breach.[10]

On 13 June 2022, the NPC, through its Complaints and Investigation Division (CID), ordered VRP to submit its full report.[11]

On 25 July 2022, VRP submitted its full report.[12]

VRP stated that the possible personal data involved were the patients' names, IDs, and addresses.[13] It explained that these, however, could not be validated because the information was falsified and VRP could not determine the source of the information.[14]

To address the breach, VRP stated that it took the following measures:

- Metrocare has been informed that the member has no transactions with VRP Medical Center after this incident is reported to the NPC.
- All official receipts are being scanned and archived for future references.
- Issuance of receipts are printed and duly signed on by our respective cashiers (with printed name).
- All statement of accounts issued to patients are also signed by our clerks.[15]

Issue

---

[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Order (To submit Full Breach Report), 13 June 2022, at 1 *in* In re: VRP Medical Center, NPC BN 18-062 (NPC 2022).
[12] Full Report, 25 July 2022, *in* In re: VRP Medical Center, NPC BN 18-062 (NPC 2022).
[13] *Id.* at 1.
[14] *Id.*
[15] *Id.*

Whether the incident involves a personal data breach that requires mandatory notification under NPC Circular 16-03 (Personal Data Breach Management).

Discussion

The Commission resolves to close the matter. The incident does not involve a personal data breach. Thus, it is not subject to mandatory breach notification under NPC Circular 16-03.

Section 3 (F) of NPC Circular 16-03 defines a personal data breach as follows:

> Section 3. *Definition of Terms*. For the purpose of this Circular, the following terms are defined, as follows:
>
> . . .
>
> F. "Personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:
>
> 1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
> 2. Integrity breach resulting from alteration of personal data; and/or
> 3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.[16]

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access to personal data transmitted, stored, or otherwise processed.[17]

VRP stated that there may have been a breach over the financial accounts of the real owners of the OR and SOA.[18] VRP, however, explained that this could not be validated given that the information on the documents was falsified.[19]

---

[16] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 3 (F) (15 December 2016).
[17] *Id.*
[18] Full Report, 25 July 2022, Annex 2, *in* In re: VRP Medical Center, NPC BN 18-062 (NPC 2022).

The evidence presented does not show that BL was able to acquire or access the personal data from the OR and SOA on record.

The OR on record and the falsified OR only shared the same official receipt number.[20] Further, as correctly observed by VRP, the details on the falsified OR were handwritten, as opposed to the OR on record wherein the details were typewritten.[21] It must also be noted that the falsified OR does not make any reference to the SOA on record. Thus, the evidence is insufficient to show that BL had access to the personal data stated in the OR on record.

With regard to the SOA, while the SOA on record and the falsified SOA involved the same admission number, they used different templates and contained different entries.[22] VRP also stressed that the falsified SOA used a different font type.[23] Thus, the evidence is likewise insufficient to show that BL had access to the personal data in the SOA on record.

Given that there was no access to personal data, the incident does not involve a personal data breach. There was no accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access to personal data that would require mandatory breach notification.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-062 In re: VRP Medical Center is considered **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
05 June 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

---

[20] Initial Report, 02 May 2018, at 2, *in* In re: VRP Medical Center, NPC BN 18-062 (NPC 2018).
[21] *Id.*
[22] *Id.* Annexes 2-3.
[23] *Id.* at 2.

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

VRG
Data Protection Officer
VRP Medical Center

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FYNAMICS LENDING INC. OPERATING PONDOPESO ONLINE LENDING APPLICATION

x----------x

NPC 19-910

For: Violation of the Data Privacy Act of 2012

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is the Partial Motion for Reconsideration (Partial MR) on the Decision dated 17 December 2020 filed by Respondents KF, JCG, and HAD (Respondents). Respondents are directors of Fynamics Lending Inc. (Fynamics or the "Corporation"), the operators of the PondoPeso Online Lending Application.

Facts

On 17 December 2020, the Commission issued a Decision finding Respondents liable for violation of Section 25 of the Data Privacy Act of 2012 (DPA):

> WHEREFORE, all these premises considered, this Commission hereby:
>
> 1. **FINDS** that Respondent Fynamics Lending Inc. and its Board of Directors, namely, ML, CW, KF, JCG, HAD, as responsible officers, have violated Section 25 of the Data Privacy Act; and
>
> 2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice, recommending the prosecution of the Respondents for the crimes of Unauthorized Processing under Section 25 of the Data Privacy Act, for its further actions.
>
> SO ORDERED.[1]

[1] Decision, 17 December 2020 at 42, *in* In re: Fynamics Lending Corporation.

On 15 February 2021, Respondents received a copy of the Decision. On 02 March 2021, via registered mail, Respondents filed a Partial MR to the Decision arguing the following:

1. The PondoPeso online lending application (OLA) already existed prior to Fynamics' incorporation with the Securities and Exchange Commission (SEC). Respondents were not aware of the existence of PondoPeso before and after the incorporation of Fynamics.[2]

2. Respondents did not issue or execute any document or board resolution approving or ratifying the establishment or creation of PondoPeso after the incorporation of Fynamics. They did not attend meetings of the Board of Directors (BOD) on the online lending business operations or on any corporate matters, including the elections of the members of the BOD of the Corporation.[3]

3. Respondents did not receive any dividends or compensation whatsoever from Fynamics.[4]

4. Assuming for the sake of argument that Respondents are directors of Fynamics, they still cannot be held criminally liable for the acts of the Corporation. There is no proof that Respondents participated, directly or indirectly, in allowing the commission of the violation of the DPA.[5]

5. Respondents cannot be considered to have acted with gross negligence in allowing the commission of the alleged violation of the DPA since Respondents did not know about the business transactions with "PesoPondo and/or AsiaPac." Respondents did not sign the Master Service Agreement (MSA) entered into with AsiaPac Solutions Corporation (AsiaPac).[6]

On 14 July 2021, Respondent KF emailed the Commission. She requested the Commission to either (1) remove her name from the Commission's article on Fynamics or (2) edit the article in such a way

---

[2] Partial Motion for Reconsideration by KF, JCG, HAD ,[Partial MR], 25 February 2021.
[3] *Id.* at 3.
[4] *Id.*
[5] *Id.*
[6] *Id. at 4.*

that the article will not appear in the Google search results of her name.[7] She alleged that, due to the case before the Commission, she could not find a job and continues to suffer from anxiety and depression.[8] In her email, she stated that she is not working with Fynamics and that her name was only used by the Corporation and Emerhub, the company Fynamics engaged for incorporation. She mentioned that Respondents have yet to receive the Commission's decision on the Partial MR.[9] Lastly, in addition to the contents of the Motion for Reconsideration that Respondents filed on 02 March 2021, she alleged the following:

> I am not working with the Fynamics corporation. I and the other Filipino citizens are represented by a separate lawyer. Our goal is to simply get our names out of this case. The recent action made for this is filing for a motion for reconsideration, which is very recent at 2021 and we are yet to receive a decision. The first parts of the hearings in 2020 were primarily focused on the Chinese citizens who are currently running the corporation. Nevertheless, I would also like to mention points on how we are not involved in this:
>
> 1. The NPC required Fynamics to submit proof that we are part of their company or board. They were not able to submit any proof. No board meetings were made where we were present. No signed documents presenting our involvement in any of their decision-making.
> 2. Fynamics' incorporation documents have shown our forged signatures. Everything was forged.
> 3. I did not sign a single document or article involving their company.
> 4. Fynamics cannot present any proof of their relation to us.
> 5. Our names were merely used for the incorporation. We are not receiving any equity or dividend, or salary from the company.
> 6. No proof can be presented to prove that we have any involvement in the violations that the company made. This, according to the law, means we cannot be liable.[10]

Respondent KF attached a copy of the Partial MR, her valid identification cards, and copies of allegedly forged Minutes of a Fynamics' BOD Meetings, board resolutions, Secretary's Certificates, and a Directors' Certificate.

---

[7] Email from KF, respondent director of Fynamics Lending Corporation [Email from KF], 14 July 2021.
[8] *Id.*
[9] *Id.*
[10] *Id.*

Issue

Whether the Partial MR filed by Respondents should be granted.

Discussion

The Commission denies the Partial MR.

The Commission notes that Respondents received the Decision on 15 February 2021. Section 4, Rule 8 of the 2021 Rules of Procedure of the National Privacy Commission (NPC Circular No. 21-01) provides:

> SECTION 4. Appeal. – The decision of the Commission shall become final and executory fifteen (15) calendar days after receipt of a copy by both parties. One motion for reconsideration may be filed, which shall suspend the running of the said period. Any appeal from the Decision shall be to the proper courts, in accordance with law and rules.[11]

Thus, a motion for reconsideration can be filed within the fifteen-day period to appeal. Following this rule, the period to file a motion for reconsideration is until 02 March 2021. The Partial MR was filed by registered mail on 02 March 2021. However, the additional allegations made by Respondent KF in her email were filed only on 14 July 2021.

Although Respondent KF's request and additional allegations in the email were filed out of time, the Commission, in the interest of justice, considers the request and the additional allegations as a supplement to the Partial MR.

Respondents' arguments rely heavily on the allegation that they are not members of Fynamics' BOD. They also stated that even assuming they are directors of the Corporation, they still cannot be held personally liable since they neither, directly or indirectly, participated in the commission of the violation of the DPA nor allowed, by their gross negligence, the commission of the violation of the DPA.

---

[11] National Privacy Commission, NPC Circular No. 21-01, "2021 Rules of Procedure of the National Privacy Commission" [NPC Circ. No. 2021-01], Rule VIII, § 4 (28 January 2021).

These arguments are merely restatements of their arguments in their Answer dated 04 October 2019. Similar to the Answer, Respondents failed to submit evidence to substantiate their allegations. The Commission now discusses the denial of the Partial MR in detail.

Fynamics' Articles of Incorporation and its General Information Sheet for 2018 show that Respondents are members of its Board of Directors.

Respondents, in their Answer and Partial MR, admit to being nominee stockholders for the purpose of incorporating Fynamics with the SEC but deny being members of the BOD.[12] The Articles of Incorporation (AOI), however, shows that Respondents are listed as stockholders, incorporators, and directors of Fynamics. In fact, Respondents were named as three (3) of the five (5) directors of the Corporation.[13] Respondents cannot admit to being incorporators and simultaneously deny being members of the BOD when the AOI clearly provides that they also served as the latter. Further, Fynamics' General Information Sheet (GIS) for 2018 shows that Respondents were incumbent directors of the Corporation at the time of the commission of the violation of the DPA.[14]

Respondents failed to produce evidence to substantiate their allegations and dispute the presumptions in this case.

Respondents made several statements in their attempt to convince the Commission that Respondents are not members of Fynamics' BOD. Having failed to produce any evidence to support these allegations, the statements have no probative value. It is hornbook doctrine that mere allegations do not constitute proof.[15] As held by the Supreme Court in *GSIS v. PGA* et.al., "it is basic in the rule of evidence that bare

---

[12] Verified Answer by KF, JCC, HAD, 04 October 2019, at 2; Partial MR, at 3.
[13] Records, at 166-169.
[14] Records, at 170-177.
[15] Government Services Insurance System v. Prudential Guarantee and Assurance, Inc., Development Bank of The Philippines And Land Bank Of The Philippines G.R. No. 165585, 20 November 2013.

allegations, unsubstantiated by evidence, are not equivalent to proof. In short, mere allegations are not evidence."[16]

Since Respondents failed to provide evidence to support their allegations, the Commission cannot disregard the existing presumptions in this case that Respondents failed to properly dispute or address. According to Rule XII, Section 8 of the 2021 NPC Rules of Procedure, the Rules of Court shall apply in a suppletory character to the Rules of the Commission and whenever practicable and convenient.[17]

Section 3, Rule 131 of the Rules of Court enumerates what are considered disputable presumptions.[18] In *MBTC v. Tobias*, the Supreme Court defined a disputable presumption as:

> species of evidence that may be accepted and acted on when there is no other evidence to uphold the contention for which it stands, or one which may be overcome by other evidence (31A C.J.S., p. 197; People v. de Guzman, G.R. No. 106025, Feb. 9, 1994; Herrera, Remedial Law, Vol. VI, 1999 Edition, pp. 40-41). In fact, Section 3 of Rule 131 provides that the disputable presumptions therein enumerated are satisfactory if uncontradicted but may be contradicted and overcome by other evidence x x x[19]

There are four (4) disputable presumptions present in this case that Respondents failed to properly address. These are (1) the ordinary course of business has been followed;[20] (2) there was a sufficient consideration for a contract;[21] (3) a person intends the ordinary consequences of his or her voluntary act;[22] and (4) evidence wilfully suppressed would be adverse if produced.[23]

First, pursuant to section 3(q) of Rule 131 of the Rules of Court, the operations of Fynamics was conducted following the ordinary course of business. The BOD of Fynamics is composed of ML, CW, and Respondents.[24] Following this presumption, Fynamics' actions when

---

[16] *Id.*
[17] NPC Circ. No. 2021-01, Rule XII, § 8.
[18] Supreme Court of the Philippines, A.M. No. 19-08-15-SC "2019 Amendments to the 1989 Revised Rules on Evidence"
[Rules of Court], Rule 131, § 3 (1 May 2020).
[19] G.R. No. 177780 January 25, 2012 Metropolitan Bank and Trust Co. (Metrobank), represented by RAS v. AOT.
[20] Rules of Court, Rule 131, § 3(q).
[21] *Id.* at Rule 131, § 3(r).
[22] *Id.* at Rule 131, § 3(c).
[23] *Id.* at Rule 131, § 3(e).
[24] Records at 174.

Respondents served as directors are presumed to have been done in the ordinary course of business. Without any of the three (3) Respondents, the BOD would not have the required quorum to validly conduct business. Thus, the failure of Respondents to offer any evidence proving that they are not directors of Fynamics or that they were not included in meetings of the BOD maintains the presumption that Fynamics acted legitimately through its BOD.

As to the allegation of forgery made by Respondent KF in her email,[25] the Commission is not the proper forum to raise these issues. The documents she submitted together with her email can only be construed by the Commission as legitimate unless the forgery of such documents is proven in a court of law. Absent any proof to the contrary, the Commission cannot conclude that all the issuances of the Fynamics' BOD are forged and its entire operations at that time was illegitimate. The Commission notes, however, that despite her claim that her signatures were forged, it does not appear as if she took any action on this very serious matter.

Second, Section 3(r) of Rule 131 provides the disputable presumption that there is a sufficient consideration for a contract.[26] Respondents claimed that they have not received any dividends or compensation from Fynamics as members of its BOD.[27] However, Respondents failed to furnish the Commission with proof to support their claim.

The GIS of Fynamics for the year 2018 shows that Respondents are members of Fynamics' BOD.[28] To serve as a member of the BOD is essentially a contract that requires consent. Under this presumption, there is sufficient consideration for Respondents to agree to being designated as members of Fynamics' BOD.

Moreover, the failure of Respondents to receive dividends or compensation as members of the BOD does not prove that they are not members of Fynamics' BOD. In fact, the Revised Corporation Code provides that members of the BOD shall not receive compensation as directors except reasonable per diems:

---

[25] Email *from* KF.
[26] Rules of Court, Rule 131, § 3(r).
[27] Partial MR, at 3.
[28] Records, at 170-177.

> SEC. 29. Compensation of Directors or Trustees. – **In the absence of any provision in the bylaws fixing their compensation, the directors or trustees shall not receive any compensation in their capacity as such, except for reasonable per diems:** *Provided however,* That the stockholders representing at least a majority of the outstanding capital stock or majority of the members may grant directors or trustees with compensation and approve the amount thereof at a regular or special meeting.
>
> In no case shall the total yearly compensation of directors exceed ten (10%) percent of the net income before income tax of the corporation during the preceding year.
>
> Directors or trustees shall not participate in the determination of their own per diems or compensation.
>
> Corporations vested with public interest shall submit to their shareholders and the Commission, an annual report of the total compensation of each of their directors or trustees.[29]

Even the By-Laws of the Corporation provides for the non-compensation of directors:

> c. The directors shall not receive compensation, as such directors, except for reasonable per diems. Any compensation may be granted to directors by the vote of the stockholders representing at least a majority of the outstanding capital stock at a regular or special stockholders' meeting. In no case shall the total yearly compensation of directors, as such directors, exceed ten (10%) of the net income before income tax of the corporation during the preceding year.[30]

As to dividends, all the stockholders have the right receive dividends when a corporation declares so.[31]

Third, Section 3(c) of Rule 131 provides the presumption that a person intends the ordinary consequences of his or her voluntary act.[32] In the Answer, Respondents categorically admitted to acting as nominee stockholders for the purpose of incorporating Fynamics:

---

[29] An Act Providing for the Revised Corporation Code of the Philippines [Revised Corporation Code of the Philippines], Republic Act No. 11232, §29 (2019). Emphasis supplied.
[30] Compliance *by* Fynamics Lending Corporation., ML, CW and BBS, Annex A, 20 February 2020.
[31] *Id.* at § 42.
[32] Rules of Court, Rule 131, § 3(c).

> On 19 June 2018, [R]espondents acted as nominee stockholders for the incorporation of [R]espondent FYNAMICS LENDING INC. before the Securities Exchange Commission. [33]

They also admitted that they "knew upon incorporation that [Fynamics] would engage in a lending business.".[34] Respondents, as incorporators of Fynamics, voluntarily signed the AOI during the incorporation process. It is clear from the AOI they signed that they are three (3) of the five (5) initial directors of the Corporation.[35] In admitting that they are incorporators of Fynamics, Respondents cannot deny the fact that they are Fynamics' initial directors as well.

Thus, the fact that they voluntarily became nominee stockholders and members of the BOD, as gleaned from the AOI, they should have anticipated the ordinary consequences of their actions which include the obligations and liabilities that come with the position.

Fourth, the Commission ordered Fynamics and the members of the BOD to present evidence on the MSA.[36] This includes any board resolutions relating to the authority of the President to enter into the MSA. Respondents, however, did not submit anything.

Respondents rely on the other respondents to validate whether Respondents have been involved with Fynamics' online lending business.[37] They also alleged that the corporate records of the Corporation or any transaction related to the PondoPeso online lending business would show their non-involvement in any corporate decision.[38] Respondents, however, in alleging that they were not involved with Fynamics, have the burden of proving that they did not serve as members of Fynamics' BOD or participated in the online lending business.

Section 3(e) of Rule 131 of the Rules of Court provides the disputable presumption that evidence wilfully suppressed would be adverse if produced.[39] Respondents should have provided the Commission with the necessary evidence to prove that they are not members of

---

[33] Verified Answer, at 2.
[34] *Id.*
[35] Records, at 165-169.
[36] Order, 01 October 2020, *in* In Re: Fynamics Lending Corporation.
[37] Partial MR, at 3.
[38] *Id.*
[39] Rules of Court, Rule 131, § 3(e).

Fynamics' BOD. In the regular course of business, Respondents, as members of the BOD should be able to request these documents. Assuming that the Corporation would not produce these documents, a request for the documents that was not entertained or a document showing their non-inclusion in company matters despite being members of the board would have helped support their argument. Despite the opportunity to present evidence on these matters, Respondents chose not to do so, leading to the presumption that had the documents been produced, these would have adversely affected Respondents.

Respondents, by their gross negligence as members of Fynamics' BOD, are liable for the violations committed by the Corporation.

Respondents alleged, in the Partial MR, that they "did not process information of the data subjects either in their individual capacity or give their consent to the same."[40] Respondents also alleged that no evidence was presented to show that they participated, directly or indirectly, in allowing the commission of the alleged violation of the DPA.[41] They further alleged that the Commission merely presumed the alleged culpability of Respondents as a result of being listed as directors of Fynamics.[42]

The Commission reiterates that it is an undisputed fact that all Respondents were incumbent members of Fynamics' BOD at the time the violations were committed. The Commission notes that the nature of the DPA violation in this case is tied to the conduct of Fynamics' business as reflected in the MSA they executed with Asiapac. Since the authority of the President to enter into the MSA on behalf of the Corporation is not provided in the By-Laws[43] of Fynamics, it necessarily means that the Fynamics' BOD gave him the authority to do so. Consequently, the directors, including Respondents, should have been aware that the provisions of the MSA contradicted the principles in the DPA.

---

[40] Partial MR at 2.
[41] *Id.* at 4.
[42] *Id.*
[43] Compliance *by* Fynamics Lending Corporation., ML, CW and BBS, Annex A, 20 February 2020.

Moreover, as discussed in the Decision, the failure of the BOD to address the violations, which led to the voluminous cases filed with the Commission, shows gross negligence on their part. Fynamics' counsel stated during the clarificatory hearing on 01 October 2020, that Fynamics was not aware of specific actions that it took against Asiapac on the unlawful processing of personal information.[44]

In the case of *AC vs. Secretary of Justice,* the Supreme Court held that the BOD shall be held criminally liable for violations committed by the corporation when by reason of the latter's negligence to supervise its employees, it has caused the corporation to commit acts in violation of the law:

> Though the entrustee is a corporation, nevertheless, the law specifically makes the officers, employees or other officers or persons responsible for the offense, without prejudice to the civil liabilities of such corporation and/or board of directors, officers, or other officials or employees responsible for the offense. The rationale is that such officers or employees are vested with the authority and responsibility to devise means necessary to ensure compliance with the law and, if they fail to do so, are held criminally accountable; thus, they have a responsible share in the violations of the law.
>
> x x x
>
> A crime is the doing of that which the penal code forbids to be done, or omitting to do what it commands. A necessary part of the definition of every crime is the designation of the author of the crime upon whom the penalty is to be inflicted. When a criminal statute designates an act of a corporation or a crime and prescribes punishment therefor, it creates a criminal offense which, otherwise, would not exist and such can be committed only by the corporation. But when a penal statute does not expressly apply to corporations, it does not create an offense for which a corporation may be punished. On the other hand, if the State, by statute, defines a crime that may be committed by a corporation but prescribes the penalty therefor to be suffered by the officers, directors, or employees of such corporation or other persons responsible for the offense, only such individuals will suffer such penalty. Corporate officers or employees, through whose act, default or omission the corporation commits a crime, are themselves individually guilty of the crime.

---

[44] Transcript of 01 October 2020 Clarificatory Hearing, at 39.

> The principle applies whether or not the crime requires the consciousness of wrongdoing. **It applies to those corporate agents who themselves commit the crime and to those, who, by virtue of their managerial positions or other similar relation to the corporation, could be deemed responsible for its commission, if by virtue of their relationship to the corporation, they had the power to prevent the act.** Moreover, all parties active in promoting a crime, whether agents or not, are principals. Whether such officers or employees are benefited by their delictual acts is not a touchstone of their criminal liability. Benefit is not an operative fact. [45]

The Commission emphasizes that a BOD has the duty of diligence. In *Bernas v. Cinco*, the Supreme Court stated that:

> The board of directors is the directing and controlling body of the corporation. It is a creation of the stockholders and derives its power to control and direct the affairs of the corporation from them. The board of directors, in drawing to itself the power of the corporation, occupies a position of trusteeship in relation to the stockholders, in the sense that the board should exercise not only care and diligence, but utmost good faith in the management of the corporate affairs.[46]

It is the persons behind Fynamics who allowed the harassment of its borrowers through the MSA that surrendered all accountability to its subcontractor. These persons provided the necessary approvals for the PondoPeso application's functionalities and dangerous permissions. They failed to supervise the representations Fynamics made to all its borrowers through the Privacy Policy and the terms and conditions of the PondoPeso application.

Had the PondoPeso application confined itself to the purposes Fynamics itself declared in the Privacy Policy, the collection agents would only have had access to the reference contacts the borrowers willingly provided in their applications.

Due to the existing presumptions, the burden of proof lies with Respondents to prove that they are not members of Fynamics' BOD. However, while Respondents were given several opportunities to dispute the fact that they are members of Fynamics' BOD, they failed to provide any evidence to support their allegations. Had they proven

---

[45] AC v. Secretary of Justice, G.R. No. 164317 (2006). Emphasis supplied.
[46] Bernas v. Cinco, G.R. Nos. 163356-57 (2015).

their non-involvement with Fynamics with sufficient evidence, the discussion on the liability of the BOD would not have applied to them.

The Commission reiterates that, technically, Fynamics' BOD cannot function without Respondents' participation since the required quorum for Fynamics to conduct business cannot be met without any one of them.

Considering the foregoing, Respondents, as members of Fynamics' BOD, are liable for the violations of the Corporation.

Request to remove KF's name in the Commission's article on Fynamics.

The Commission denies the request of Respondent KF to remove her name from the Commission's article. Respondent KF is a member of Fynamics' BOD. She, along with the other directors, are parties to the case filed against the Corporation. If the Commission grants Respondent KF's request to remove her name from the article, then it presupposes that the Commission has granted KF's prayer to drop her as a respondent in the case. Since KF has not been dropped as a respondent in the case, the Commission cannot allow the removal of her name from the article.

WHEREFORE, premises considered**,** the Commission resolves to **DENY** the Partial Motion for Reconsideration filed by Respondents KF, JCG, and HAD. The request to remove KF's name in the Commission's article on Fynamics Lending Inc. is likewise **DENIED.**

The Decision of the Commission dated 17 December 2020 is hereby
AFFIRMED.

SO ORDERED.

City of Pasay, Philippines.
29 July 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

GG & ASSOCIATES
Counsel for Respondents KF, JCG and HAD

GONZALES AND QUISMORIO LAW OFFICES
Counsel for Respondents Fynamics Lending, Inc., ML, CW and BBS.

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FYNAMICS LENDING INC. OPERATING PONDOPESO ONLINE LENDING APPLICATION

x----------x

NPC 19-910
For violation of the Data Privacy Act of 2012

RESOLUTION

AGUIRRE, D.P.C.

For consideration of this Commission is the Motion for Reconsideration filed by Respondent Fynamics Lending Inc., operating the PondoPeso Online Lending Application, and its Board of Directors (Fynamics) of the Decision dated 17 December 2020. In that Decision, this Commission found that the Respondents have violated Section 25 of the Data Privacy Act of 2012 (DPA):

> "WHEREFORE, all these premises considered, this Commission hereby:
>
> 1. **FINDS** that Respondent Fynamics Lending Inc. and its Board of Directors, namely, ML, CW, KF, JCG, HAD, as responsible officers, have violated Section 25 of the Data Privacy Act; and
>
> 2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice, recommending the prosecution of the Respondents for the crimes of Unauthorized Processing under Section 25 of the Data Privacy Act, for its further actions.
>
> SO ORDERED."[1]

Respondent Fynamics prays for the Decision to be reversed and that the instant case be dismissed.

The Facts

[1] Decision dated 17 December 2020.

On 2 March 2021, Respondent Fynamics filed a Motion for Reconsideration. It argued that the Commission erred in resolving that it was afforded procedural due process and that it violated the provisions of the Data Privacy Act.

Respondent Fynamics argued that it was not afforded procedural due process based on the following grounds:

1. The Commission neglected its own Rules of Procedure by not allowing the respondents to participate in a discovery conference; [2]

2. The Fact-Finding Committee circumvented its Rules of Procedure by not adhering to the Exhaustion of Remedies requirement; [3]

3. The conduct of the *sua sponte* investigation was unnecessary as there are existing pending Complaints against Respondent Fynamics; [4]

4. It was not afforded its right to mediate under NPC Circular No. 18-03. [5]

On the substantive matters, Respondent Fynamics argued that the Commission erred in finding that it violated the provisions of the Data Privacy Act, based on the following grounds:

1. Sections 11, 12, 18, 16, 20 and 21 of the DPA cannot be the basis of criminal prosecution. Thus, the Commission can only hold the respondents administratively liable for violation of these provisions;[6] and

2. As regards the alleged violations of Sections 25, 28, 31 and 32, the Respondent officers did not directly participate in any of

---

[2] Motion for Reconsideration dated 2 March 2021, par. 12.
[3] *Id.* at par. 18.
[4] *Id.* at par. 24.
[5] *Id.* at par. 32.
[6] *Id.* at par. 45.

> the complained acts or through gross negligence, allowed the commission of any crime. [7]

Discussion

The Commission denies the Respondent's Motion for Reconsideration.

Ruling on the Procedural Issues

The Commission finds that there are no new material facts alleged by Respondent Fynamics for its consideration and that it merely reiterated the arguments raised in its Answer dated 15 October 2019 and other previous submissions to the Commission. Nevertheless, this Commission will address each of their arguments to further clarify any misconceptions that Respondent Fynamics may continue to have.

Respondent Fynamics gave an interpretation of the *sua sponte* investigation under the NPC Circular No. 16-04,[8] stating thus:

> 7. At the onset, it bears stressing that under Rule II, Section 3 of Rule IV, Section 23 of the Rules of Procedure, a sua sponte investigation is not a special investigation but is similar to the proceeding wherein a Complaint is filed before this Honorable Commission. The main difference lies on the fact that it is the Honorable Commission that initiates a sua sponte investigation.

The latest Rules of Procedure of the Commission indeed clarifies that a *sua sponte* investigation is an investigation initiated by the NPC on its own for possible violation by one or more entities of the Data Privacy Act of 2012.[9]

However, the fact that a *sua sponte* investigation is initiated by the NPC precisely makes it distinct from that of a regular complaint. NPC Circular No. 16-04 provides for the procedure in *sua sponte* investigations, thus:

---

[7] *Id.* at par. 49.
[8] NPC Circular No. 16-03, Rules of Procedure of the National Privacy Commission dated 15 December 2016, Rule IV.
[9] NPC Circular 2021-01, 2021 Rules of Procedure of the National Privacy Commission dated 28 January 2021, Section 4 (p).

> SECTION 24. Uniform procedure. – The investigation shall be in accordance with Rule III of these Rules, provided that the respondent **shall be provided a copy of the fact-finding** report and given an opportunity to submit an answer. In cases where the respondent or respondents fail without justification to submit an answer or appear before the National Privacy Commission when so ordered, the Commission shall render its decision on the basis of available information.[10]

Respondent Fynamics contended that it was not afforded due process as it was not allowed to participate in a discovery conference:

> 14. Worse, the Fact-Finding Committee cited in the Report that "examinations of publicly accessible information and the initial technical evaluation on Fynamics *(sic)* and their online lending application, PondoPeso, show that the company has failed to demonstrate compliance with the DPA".
>
> 15. Apparently, the investigation of the Fact-Finding Committee was conducted without the participation of Respondent Fynamics.
>
> 16. Aptly put, Respondent Fynamics was not allowed to avail of discovery proceedings in the said investigation thereby effectively depriving the said corporation of its right to procure the pertinent pieces of evidence in accordance with Rules of Procedure.
>
> 17. Plainly speaking, the unavailability of this mode of discovery will hamper Respondent Fynamics' preparation of its arguments and evidence to rebut the false accusations against it.

The Commission takes this opportunity to explain the difference between a Discovery Conference under Rule III of NPC Circular No. 16-04 and an investigation under Rule IV of the same Circular.

The procedure for a complaint under Rule III of NPC Circular No. 16- 04 is as follows: The complaint is evaluated by an investigating officer. If the investigating officer finds that on its face the complaint involves a violation of the DPA and based on the allegations, there is a reason to believe that there is a privacy violation or personal data breach, an Order to confer for Discovery is issued by the investigating officer to

---

[10] Section 11, Rule IV, NPC Circular No. 16-04 dated 15 December 2016. Emphasis supplied.

discuss whether discovery of information and of electronically stored information is reasonably likely to be sought in the proceeding.[11] After the discovery conference, a discovery Conference Report is prepared[12] and the respondent is ordered to submit a Responsive Comment to the Complaint together with any supporting documents.[13] The investigating officer, upon his or her discretion, may require the complainant to file a Reply. Such an Order may also require the respondent to file a Rejoinder after receipt of the Reply.[14] The investigating officer shall then investigate the circumstances surrounding the privacy violation or the personal data breach and determine whether additional information, evidence, or investigation is necessary, including the conduct of on-site investigations.[15] Upon termination of the investigation, the investigating officer shall produce a Fact-Finding Report, which shall include the results of the investigation, the evidence gathered, and any recommendations.[16] The report shall be submitted to the Office of the Commissioner.[17] The Commission shall review the evidence presented, including the Fact- Finding Report and supporting documents.[18] It may: (1) promulgate a Decision; or (2) order the conduct of a clarificatory hearing, if in its discretion, additional information is needed to make a Decision.[19] Finally, the Commission shall adjudicate the issues raised in the complaint on the basis of all the evidence presented and its own consideration of the law.[20]

On the other hand, in a *sua sponte* investigation under Rule IV of Circular No. 16-04, the proceedings begin with the conduct of an investigation on a data privacy violation or personal data breach. The investigating officers then create a Fact-Finding Report which serves as a complaint. This Fact-Finding Report is then given to the respondent and the respondent is given an opportunity to submit an Answer, akin to the Responsive Comment under Rule III.[21] It is worth noting that the Responsive Comment under Rule III is only submitted after a Discovery Conference. Under Rule IV,[22] the Responsive

---

[11] *Id. at* Section 13.
[12] *Ibid.*
[13] *Id. at* Section 15.
[14] *Ibid.*
[15] *Id. at* Section 16.
[16] *Id. at* Section 18.
[17] *Ibid.*
[18] *Id. at* Section 21.
[19] *Ibid.*
[20] *Id. at* Section 22.
[21] *Id. at* Section 24.
[22] *Id. at* Rule IV.

Comment or Answer is immediately required from the respondent after it receives the Fact-Finding Report.

The Rules clearly do not intend the two (2) procedures to be exactly the same. The procedure for a *sua sponte* investigation does not include a Discovery Conference because all the information and evidence in the hands of the Commission are already set out in and attached to the Fact-Finding report when it is provided to the respondent. The respondent is given the opportunity to rebut the sufficiency of evidence in its Answer. The Commission then, after reviewing the evidence presented, including the Fact-Finding Report and its supporting documents,[23] may: (1) promulgate a Decision; or (2) order the conduct of a clarificatory hearing first and thereafter promulgate a Decision.[24]

The Commission emphasizes that while Rule IV of NPC Circular No. 16-04 provides that the investigation be in accordance with Rule III, it includes a proviso, "that the respondent shall be provided with a copy of the Fact-Finding Report and given an opportunity to submit an answer."[25] Rule IV does not state that the procedure should be exactly identical to the one described under Rule III. As used in Section 24 of Rule IV, "in accordance with Rule III" simply means as far as practicable taking into consideration and giving effect to the differences between the two (2) procedures.

It is a basic principle in statutory construction that the law must be given a reasonable interpretation and be construed in a manner that avoids absurdity.[26] To accept the construction that Respondents seek to impose upon this Commission would not only result in absurdity as it disregards the clear differences between the ordinary complaints procedure and *sua sponte* investigations but it also ignores another basic rule of statutory construction that a special and specific provision prevails over a general provision irrespective of their relative position in the statute.

In *Batangas City, et.al. v. Pilipinas Shell Petroleum Corporation,* the Supreme Court elaborated on this rule, thus:

---

[23] *Id. at* Sections 21-22.
[24] *Ibid.*
[25] *Id. at* Section 24.
[26] See, Millares v. National Labor Relations Commission, G.R. No. 110524, 29 July 2002; Microsoft Corporation v. Manansala, G.R. No. 166391, 21 October 2015.

> *Generalis specialibus non derogat.* Where there is in the same statute a particular enactment and also a general one which in its most comprehensive sense would include what is embraced in the former, the particular enactment must be operative, and the general enactment must be taken to affect only such cases within its general language as are not within the provisions of the particular enactment.[27]

Since there are specific rules for *sua sponte* proceedings, those rules, which do not require a discovery conference, shall apply to this case.

Respondent Fynamics cannot claim that it was deprived of "its right to procure the pertinent pieces of evidence in accordance with Rules of Procedure"[28] when no Discovery Conference was held for this *sua sponte* investigation. Apart from repeating this claim, however, Respondents have consistently failed to allege what pieces of evidence they were deprived of. It bears repeating that in *sua sponte* investigations, all the evidence in the hands of the Commission are already provided to the Respondents when they are provided with a copy of the Fact-Finding Report and given an opportunity to submit their Answer.

Aside from this, the proceedings in this case show that the Respondents were afforded procedural due process appropriate for a *sua sponte* proceeding and were, in fact, given numerous opportunities to be heard.

As narrated in the Decision, the Respondents were ordered to file an Answer after being served a copy of the Fact-Finding Report together with all of its supporting documents. The Commission issued several Orders for the submission of additional documents to verify the claim of the Respondents and called for a clarificatory hearing. Further, all of the Respondents' Motions for Extension of Time to File and to Reset the Clarificatory Hearing were granted in the interest of an exhaustive investigation.

---

[27] Batangas City, et.al. v. Pilipinas Shell Petroleum Corporation, G.R. No187631, 8 July 2015.
[28] Motion for Reconsideration dated 2 March 2021, par. 16.

Respondent Fynamics further contended that the Commission violated its own Rules of Procedure relating to the exhaustion of remedies:

> 18. *Second,* the Fact-Finding Committee completely circumvented its Rule of Procedure and bypassed Respondent Fynamics and its officers throughout the investigation, which is contrary Section 4 of the Rules of Procedure of the Honorable Commission, which provides that:
>
> > Section 4. Exhaustion of remedies. — No complaint shall be entertained unless:
> >
> > a. the complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same;
> >
> > b. the personal information controller or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the personal information controller within fifteen (15) days from receipt of information from the complaint; and
> >
> > c. the complaint is filed within six (6) months from the occurrence of the claimed privacy violation or personal data breach, or thirty (80) days from the last communiqué with the personal information controller or concerned entity, whichever is earlier.
> >
> > The failure to comply with the requirements of this Section shall cause the matter to be evaluated as a request to the National Privacy Commission for an advisory opinion, and for the National Privacy Commission to take such further action, as necessary. The National Privacy Commission may waive any or all of the requirements of this Section, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject.
>
> 19. Undoubtedly, Respondent Fynamics should have been first informed in writing of their alleged violations and given the

> opportunity to institute appropriate actions to rectify the alleged alleged (sic) findings of the Fact-Finding Committee. [29]

The Respondent's interpretation that the Commission should first reach out to respondents to be "given the opportunity to institute appropriate actions to rectify the alleged criminal violations of the DPA" is purpose-defeating, if not plainly absurd. *Sua sponte* investigations are only conducted under specific premises under the Rules of Procedure, thus:

> Section 23. Own Initiative. – Depending on the nature of the incident**, in cases of a possible serious privacy violation or personal data breach**, taking into account the risks of harm to a data subject, the Commission may investigate on its own initiative the circumstances surrounding the possible violation. If necessary, the Commission may use its enforcement powers to order cooperation of the personal information controller or other persons, with the investigation or to compel appropriate action to protect the interests of data subjects.[30]

As seen with the abovementioned criteria for a *sua sponte* investigation, complaints are only initiated in cases of a possible serious privacy violation or personal data breach. In these actions, the Commission considers evident risks of harm to a data subject. The privacy violation or personal data breach that can be directly acted upon by the Commission is qualified with a degree of seriousness that makes it different from complaints under Rule III. This degree of seriousness is considered in relation to the level of risks posed to the data subjects, and may be manifested in different ways such as the scale of processing or the number of reports received by the Commission.

Thus, in cases of *sua sponte* investigations, it is futile for the Commission to exhaust remedies by communicating with the respondent. The provision on the exhaustion of remedies is meant to provide an opportunity for parties to amicably settle among themselves and rectify the situation. This is only resorted to when the possibility of rectification still exists.

The nature and purpose of *sua sponte* investigations makes such exhaustion of remedies futile because at the point when the

---

[29] Motion for Reconsideration dated 2 March 2021.
[30] NPC Circular No. 16-04 dated 15 December 2016, Rule IV, Section 23. Emphasis supplied.

Commission detects a privacy violation or personal data breach with a degree of seriousness, the opportunity for rectification is no longer available. The requirement of exhaustion of remedies is thus inapplicable to *sua sponte* investigations.

Furthermore, such provision for the exhaustion of remedies is not even an absolute rule that renders all non-conforming complaints invalid. The Commission has previously discussed the purpose for the exhaustion of remedies in the case of NPC 18-038:

> This rule was intended to prevent a deluge of vexatious complaints from those who waited for a long period of time to pass before deciding to lodge a complaint with the NPC, unduly clogging its dockets. Notably, however, the same Section provides that the Commission has the discretion to waive such period for filing upon good cause shown, or if the complaint involves a serious violation or breach of the DPA, taking into account the risk of harm to Complainant.

The Respondent, in its Motion for Reconsideration, raises another argument that the conduct of a *sua sponte* investigation is unnecessary as there are several pending complaints filed against it:

> 24. *Second,* the conduct of sua sponte investigations was totally unnecessary considering the existence of pending complaints against Respondent Fynamics.
>
> 25. Notably, in the Assailed Decision, this Honorable Commission admitted that the sua sponte investigation was conducted in lieu of the several complaints received by the Honorable Commission against Respondent Fynamics.
>
> 26. The Fact-Finding Report further mentioned that there are a "total of 113 complaints as of 31 July 2019" which have been filed with the Honorable Commission against Respondent Fynamics.
>
> 27. Of the 113 complaints, Respondent Fynamics *(sic)* has been made aware only of 54 complaints and have received files, orders, and pleadings only for 54 complaints, which are in different stages of proceedings and some of them have already been subject to a compromise agreement that was approved by the Honorable Commission while some of them are still undergoing mediation proceedings.

> 28. In consideration of due process and fairness, this Honorable Commission should have first allowed the individual complaints against Fynamics *(sic)* to be threshed out by the Complaints and Investigation Division, before creating a fact-finding committee. Unfortunately, in this case, the Fact-Finding Report has effectively prejudged the pending individual complaints.
>
> 29. Under Rules of Procedure, the sua sponte investigation is similar to a complaint filed by a person personally affected by a privacy breach.
>
> 30. This Honorable Commission, through the sua sponte investigation seemingly filed the Complaint on behalf of these affected persons. Thus, the conduct of sua sponte investigation against Fynamics *(sic)* by virtue of the pending complaints somehow makes the sua sponte investigation redundant since the investigation has the same causes of action as the pending complaints.
>
> 31. To be precise, the issues raised, specifically, the violations attributed to Respondent Fynamics are similar to the pending complaints. A possible issue arises when the individual cases are dismissed and the investigation continues for the same cause of action. Therefore, the reasonable approach would be to let the individual complaints run their course and hold the instant case in abeyance.[31]

The Commission addresses these allegations point by point.

Nowhere in the Decision did the Commission "admit that the *sua sponte* investigation was conducted in lieu of the several complaints received by the Honorable Commission against Respondent Fynamics." On the contrary, the Decision explicitly stated that the *sua sponte* investigation is independent and separate from the individual cases by stating that "the pending cases and the case on hand involve different parties, different causes of action with different prayers of relief."

There is also no basis to state that the Commission prejudges individual complaints against respondents when it conducts *sua sponte* investigations. Each individual complaint runs its course according to

---

[31] Motion for Reconsideration dated 2 March 2021.

Rule III and is weighed according to the quantum of evidence required in administrative cases.

The argument that a *sua sponte* investigation is unnecessary because of its similarity with individual complaints is baseless. The discussion above gives a detailed differentiation between the two (2) proceedings, not to mention the plain fact that there is a separate provision for *sua sponte* investigations in the Rules of Procedure. The individual complaints were only cited to demonstrate the seriousness of the possible data privacy violation. The Commission in its Decision emphasized that:

> The citation of allegations from different pending cases illustrate that the effects of the functionalities of Respondent Fynamics' application, the procedures it implemented coupled with its lack of transparency are not imagined but have translated to seriously harmful effects in the lives of their borrowers, all of whom are considered data subjects under the DPA.[32]

On the argument that Respondent Fynamics was not afforded the right to mediate as provided in NPC Circular No. 18-03, the Commission notes that this is not the first time that the Respondents raised the issue of mediation. On 16 September 2019, the Respondents filed an Appearance and Omnibus Motion which included a prayer to refer the case for mediation. On 07 October 2019, the Commission issued a Resolution which included a denial of the prayer of Respondents ML, CW, and BBS for the initiation of mediation proceedings:

> As regards the prayer of the Respondents ML, CW, and BBS for the initiation of a mediation proceeding and the suspension of the proceedings pending the resolution of their Omnibus Motion, the Rule on Alternative Modes of Dispute Resolution under NPC Circular No. 16-04 finds application, thus:
>
> > Section 26. Mediation officer. – The Commission shall assign a mediation officer to assist the complainant and respondent to reach a settlement agreement, **provided that no settlement is allowed for criminal acts.**
>
> The instant case was initiated through a sua sponte investigation of the National Privacy Commission pursuant to

[32] Decision dated 17 December 2020.

> Section 3 of NPC Circular 16-04. The Fact—Finding Report noted certain dangerous permissions in the Android Package (APK) of the Pondo Peso application that are designed to be indispensable for the application to function, as well as the inaccessibility of a Privacy Policy that provides an explanation of this to the user. Based on these, the Fact-Finding report found that "the apparent failure of the company to abide by the directives of the DPA in the protection of data subjects and their personal information constitute violation of the law." Specifically, the Fact-Finding Report recommends criminal prosecution for the company, represented by their board of directors, for violations of Sections 25, 28, 31, and 32 of the Data Privacy Act.
>
> Upon consideration of the allegations in the Fact-Finding Report and the existing rules under NPC Circular No. 16-04, the Commission finds that there is no basis for the Commission to grant the prayer of respondents ML, CW and BBS for the initiation of a mediation proceeding and the suspension of the proceedings pending the resolution of their Omnibus Motion.[33]

While the Rules on Mediation embodied in NPC Circular No. 18-03 did not provide a distinction between cases which can and cannot undergo mediation, NPC Circular No. 16-04 categorically states that *"no settlement is allowed for criminal acts."*

The maxim *interpretare et concordare leges legibus est optimus interpretandi* provides that a statute must be interpreted, not only to be consistent with itself, but also to harmonize with other laws on the same subject matter, as to form a complete, coherent and intelligible system.[34] Applying this concept of harmonization of statutes, the rules of procedure of the NPC do not stand separately from each other. They must be interpreted in a way that would produce a harmonious whole. Thus, considering that the Fact-Finding Report alleged prohibited acts committed by the Respondent which incur criminal liability under the Data Privacy Act, together with the fact that it recommended the criminal prosecution of the Respondents, mediation is not applicable in this case.

Ruling on the Substantive Issues

---

[33] Resolution dated 7 October 2019.

[34] Philippine Economic Zone Authority v, Green Asia Construction & Development Corporation, G.R. No. 188866, 19 October 2011.

Similar to the procedural issues, the Commission finds no new material facts for its reconsideration of the substantial issues. The allegations in the Motion for Reconsideration are a mere rehash of the allegations from the respective Answers filed by the Respondents in the course of the proceedings and were already sufficiently addressed in the Decision.

As regards Respondent Fynamics' contention that there is nothing inherently wrong or illegal with taking a "Dangerous Permission" from the user and that doing so have "corresponding legal, commercial, and operational rationale," the Commission reiterates that it does not question the legality of the "Dangerous Permissions" per se, but looks into their declared purposes in comparison to the actual processing done.

In this case, Respondent Fynamics claimed that the READ_CONTACTS dangerous permission was justified by its need to determine, at the point of the loan application, whether the mobile phone was newly purchased. This is part of their verification process, before approval of the loan. This is determined through the number of entries in the contact list at the moment of application.

While the purpose behind the access of the list of contacts was explained, Respondents have not disputed that it retained the contacts of data subjects and kept the data in a form that allowed them to further process even after the loan applications' approval.

The issue is the retention of these contacts. The excerpts from the cited individual complaints in the Fact-Finding Report pertained to the collection practices made possible because of the retained personal information. Such retention is considered processing of personal information and must be justified under the lawful criteria provided under the DPA. As detailed by the Commission in the Decision, no such lawful criteria is present in this case. Respondent Fynamics failed to prove that their retention of data is supported by consent or any other lawful criteria provided under the Data Privacy Act.

On the contention that the Respondent officers did not directly participate in any of the complained acts or through gross negligence, allowed the commission of any crime, the Data Privacy Act is clear that the liability of the responsible officers in cases where the offender is a corporation does not rely on active participation alone. Gross

negligence is explicitly stated in the Data Privacy Act as a ground for criminal liability.

There is no reason for the Commission to reverse its earlier finding that the Respondent officers are liable for gross negligence. As stated in the Decision:

> The Supreme Court has consistently defined gross negligence as "the negligence characterized by the want of even slight care, or by acting or omitting to act in a situation where there is a duty to act, not inadvertently but willfully and intentionally, with a conscious indifference to the consequences, insofar as other persons may be affected. It is the omission of that care that even inattentive and thoughtless men never fail to give to their own property."[35]
>
> In this case, the Board of Directors of Fynamics did not deny the fact that a Master Service Agreement was entered into between Respondent Fynamics and Asiapac, with the President as the signatory. The Board of Directors should have been aware of the terms in this Agreement, considering that it concerns a vital aspect of their operations as a lending company. Consequently, they should have been aware that the provisions of the Master Service Agreement contradicted the principles in the DPA. It included a provision that sought to surrender its accountability as a Personal Information Controller to Asiapac.[36]

Notwithstanding the provision in the Data Privacy Act that the responsibility to prevent unauthorized processing cannot be subcontracted by Personal Information Controllers, the Commission reiterates that Respondent Fynamics was not entirely powerless under the Master Service Agreement. Respondent Fynamics could have exercised its responsibility under the law through certain provisions in the Master Service Agreement which contained remedies that they should have exercised as the Personal Information Controller after voluminous complaints were filed against it.[37] However, the Respondents failed to prove that they exercised due diligence in protecting the personal data of their borrowers and failed to act upon the unprofessional debt collection practices that have led to the hundreds of complaints filed before the Commission.

---

[35] Fernandez v. Office of the Ombudsman, G.R. No. 193983, 14 March 2012.
[36] Compliance dated 20 February 2020, Annex "C". Emphasis supplied.
[37] Fact-Finding Report, Annex "B". Emphasis in the original.

The Commission emphasizes that the Respondent has not provided any new or material allegations that justify the reversal of the Decision. Having sufficiently addressed all the points raised by Respondent Fynamics in its Motion for Reconsideration through this Resolution and the previously rendered Decision, the Commission finds no basis to overturn its Decision.

WHEREFORE, premises considered**,** the Commission resolves to **DENY** the Motion for Reconsideration filed by Respondent Fynamics Lending, Inc. The Decision of the Commission dated 17 December 2020 is hereby **AFFIRMED**.

SO ORDERED.

City of Pasay, Philippines
11 March 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

GONZALES AND QUISMORIO LAW OFFICES
Counsel for Respondents Fynamics Lending, Inc.,

ML, CW, and BBS

GOROSIN GARCIA & ASSOCIATES
Counsel for Respondents
Kwinnie KF, JCG
and HAD

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FYNAMICS LENDING INC. OPERATING PONDOPESO ONLINE LENDING APPLICATION

x----------x

NPC 19-910
For violation of the Data Privacy Act of 2012

RESOLUTION

On 01 October 2020, the Commission conducted a Clarificatory Hearing pursuant to Section 21 of NPC Circular No. 16-04. Respondent Fynamics Lending, Inc. (Fynamics) and the individual respondents ML, CW, and BBS were represented by Atty. LAQ and Atty. EAT from the Gonzales & Quismorio Law Offices, while the individual respondents KF, JCG and HAD were represented by Atty. FG from the law firm of Gorosin, Garcia & Associates.

During the Clarificatory Hearing, counsels for Fynamics were ordered to submit specific documents to the Commission.[1]

On 16 October 2020, Fynamics filed a Partial Compliance with an attached Memo from Asiapac Solutions Corp. dated 01 October 2019. Fynamics also requested for an extension of thirty (30) days or until 15 November 2020 to produce and submit the other documents required by the Commission. They state in their Partial Compliance that:

> a. Some of the employees and/or custodians of the said documents are no longer in the Philippines and the Respondent is trying its best to communicate and inquire as to where the said documents were placed; and
> b. Some of the employees and/ or custodians of the said documents have severed ties or has resigned from the company and the Respondent is trying to get a hold of the same.[2]

[1] Order dated 01 October 2020.

[2] Partial Compliance by Fynamics Lending, Inc. dated 15 October 2020.

The Commission notes the submission of the Partial Compliance. Considering the circumstances raised by Fynamics and in the interest of an exhaustive investigation, the Commission grants the requested extension for submission of the required documents.

WHEREFORE, the Commission **GRANTS** the request for an extension of thirty (30) days or until **15 November 2020** for Fynamics Lending, Inc. to produce and submit the documents specified in the Order dated 01 October 2020. The Partial Compliance filed on 16 October 2020 is **NOTED.**

Failure to comply with this Order shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

SO ORDERED.

City of Pasay,
Philippines 5 November
2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

GONZALES AND QUISMORIO LAW OFFICES
Counsel for Respondents Fynamics Lending, Inc., ML, CW, and BBS

GOROSIN GARCIA & ASSOCIATES
Counsel for Respondents KFJCG and HAD

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: LANDBANK OF THE PHILIPPINES

x----------x

CID BN 18-105
For: Violation of the Data Privacy Act of 2012

RESOLUTION

AGUIRRE, *D.P.C.;*

This resolves a breach notification submitted by Landbank of the Philippines (Landbank) on 06 July 2018 on an incident that allowed an unknown person to open a credit card account using the personal details of a different person.

Facts

On 04 July 2018, MGB submitted a complaint to Landbank for an alleged identity theft.[1] According to Mr. MGB, when he applied for an account with another bank, his name appeared in the "negative file" of the Bankers Association of the Philippines (BAP).[2] MGB later found out that his name was on the delinquent accounts report because of past credit card dues with Landbank.

In the complaint, MGB alleged that his personal details, including his name, birthdate, gender, and tax identification number, were used in the application for the said credit card without his consent.[3]

Upon receipt of the complaint, Landbank's Credit Card Administration Department (CCAD) immediately investigated the incident to validate MGB's claims.[4] Landbank found that there were

---

[1] Records, pp. 3-4; Data Breach Notification dated 6 July 2018.
[2] *Id.* at 4.
[3] *Ibid.*
[4] *Ibid.*

fictitious information stated in the credit card application. These details include the applicant's marital status, cellphone number, business, and home addresses, photograph, and signature.[5]

Thereafter, CCAD requested the deletion of MGB's name in the list of delinquent accounts with the BAP.[6]

In a Resolution dated 12 May 2020, the Commission ordered Landbank to submit a full report on the outcomes of the latter's proposed remedial measures within thirty (30) days from its receipt of the Resolution.

Landbank received the Resolution on 04 February 2021, and on 06 March 2021, submitted a full report on the outcomes of its proposed remedial measures.[7]

Issue

Whether or not Landbank sufficiently addressed the breach incident and implemented measures to prevent similar incidents in the future.

Discussion

Upon review of Landbank's full breach report, the Commission finds that the outlined remedial measures of Landbank comply with R.A. 10173 or the Data Privacy Act of 2012, its Implementing Rules and Regulations, and NPC Circular No. 16-03 on Personal Data Breach Management.

Section 17(D) of NPC Circular No. 16-03 provides for the content of the notification to the Commission:

> A. *Content of Notification*. The notification shall include, but not be limited to:
> 1. Nature of the Breach

[5] *Ibid.*
[6] *Ibid.*
[7] *Letter from Landbank dated 6 March 2021.*

a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
b. a chronology of the events leading up to the loss of control over the personal data;
c. approximate number of data subjects or records involved;
d. description or nature of the personal data breach;
e. description of the likely consequences of the personal data breach; and
f. name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved
   a. description of sensitive personal information involved; and
   b. description of other information involved that may be used to enable identity fraud.
3. Measures Taken to Address the Breach
   a. description of the measures taken or proposed to be taken to address the breach;
   b. actions being taken to secure or recover the personal data that were compromised;
   c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
   d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
   e. the measures being taken to prevent a recurrence of the incident.

The Commission reserves the right to require additional information, if necessary.

In its full breach report, Landbank discussed the actions it had undertaken to mitigate the harm and negative consequences of the reported incident. Aside from the initial investigation by Landbank's CCAD, its Security Department visited the address presented in the Property Valuation and Credit Information Department's (PVCID) Credit Information Report. Based on the information gathered from the visit, Landbank concluded that the complainant was indeed a victim of identity theft:

> To further investigate the claim of the complainant, SD conducted a visit at [ ] on July 20, 2018, the address appearing in

PVCID's Credit Information Report, and the following information were gathered:

A) No MGB and LG resides in the said address.

B) The male tenant in the said address revealed that in several occasions, various letters from different banks pertaining to Credit Cards and Car Loans were sent to the said address using different names as a recipient.

C) As verified with the President of the Homeowner's Association, ALE, no MGB nor LG has been registered as member with their association ever since.

D) Upon verification with the Bureau of Internal Revenue (BIR), Petsburgh Company, listed as the alleged employer of MGB in his application form, was not registered in Paranaque but in Bacoor. Also, when the telephone number as indicated in the application form was contacted, the one who answered the phone does not know any "MGB." As to the mobile number, it can no longer be contacted.

E) Also, the SSS number as indicated in the ID in the Credit Information Report is the number of someone else.

In its report, SD concluded that complainant MGB is a victim of identity theft. [8]

Landbank also reported the said incident to the PNP-Anti Cybercrime Group in a letter dated 06 July 2018.[9]

As a form of assistance to MGB, Landbank's e-Banking Operations Committee (e-BOC) approved the reversal of the outstanding balance of the VISA credit card in Mr. MGB's name amounting to P122,817.21. It further waived the unbooked charges computed up to the reversal date which amounted to P407,477.05.[10]

In a letter dated 06 July 2018, Landbank notified MGB of the measures it undertook to address his complaint.[11]

---

[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.*
[11] *Ibid.*

In the same report, Landbank stated the measures it undertook to prevent the recurrence of the incident:

> To address and prevent the recurrence of the said incident, the Branch Banking Sector issued Revised Internal Control Procedures Affecting Branch Operations 2. Section A (3) states:
>
> (f) Credit Card Applications
>
> All prospective applicants to be endorsed by the Branches should be an existing bank depositor to minimize identity fraud.[12]

The Commission finds that Landbank was able to comply with the requirements of notification when it submitted its full report on 06 March 2021. Moreover, the measures it implemented mitigated the negative consequences of the identity theft incident to the affected data subject. Documents showed that Landbank acted on the breach incident in accordance with the incident response procedure required by NPC Circular No. 16-03.

Lastly, Landbank provided the necessary assistance to the affected data subject when it requested the deletion of MGB's name in the list of delinquent accounts with the BAP, approved the reversal of the outstanding balance of the VISA credit card in MGB's name, and waived the unbooked charges computed up to the reversal date.

WHEREFORE, premises considered, this Commission finds that the submission of Landbank of the Philippines in response to the Resolution dated 12 May 2020 is **SUFFICIENT.** This Commission considers the matter **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
29 April 2021.

---

[12] *Ibid.*

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

ATTY. RMA

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: LAND BANK OF THE PHILIPPINES **CID BN 18-105**

x----------x

RESOLUTION

On 06 July 2018, the Commission received a letter[1] from the Data Protection Officer of Land Bank of the Philippines ("Landbank") regarding an identity theft incident.

In their letter, Landbank relayed an individual's complaint on an alleged identity theft. According to the complaint, someone used his information or identification documents to get money, credit, loans, goods or services without his knowledge or authorization. This individual only found out about the account with Landbank when he applied for an account with another bank and his name appeared in the negative file of the Banker's Association of the Philippines ("BAP") for a past due credit card with Landbank.

In their letter, Landbank narrated the personal data possibly involved:

> [The individual] alleged that his personal details were copied from his records such as the name, birthdate, gender and Tax Identification Number (TIN). However, there are fictitious or inaccurate information that is stated in the credit card application like his marital status, cellphone number, business and home address, photograph, and signature.

Landbank stated that they undertook the following measures to address the alleged identity theft:

> Credit Card Administration Department (CCAD) had immediately asked for investigation with the concerned bank units (Administrative Legal Department and Physical Security Office) to validate the claim of [the individual].

---

[1] Records, pp. 3-4, Letter dated 6 July 2018.

> CCAD requested for the deletion of the name of [the individual] in the reporting of delinquent accounts with the BAP.

Notably, Landbank does not state the results of such actions and has not made manifestations on further findings despite the lapse of almost two (2) years since the initial letter.

Under NPC Circular 16-03,[2] the Commission requires Landbank to submit a full report of the incident that indicates the outcomes of their above-stated remedial measures and the policies adopted to avoid such incidents in the future.

This is pursuant to Section 17 (d)(3) of the same Circular which states that the personal information controller shall notify the Commission of the "actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident" as well as the "the measures being taken to prevent a recurrence of the incident."

WHEREFORE, all premises considered, Landbank is hereby ordered to submit a full report on the outcomes from their stated measures to address the alleged identity theft, with Section 17(d)(3) of NPC Circular 16-03 as guidance, within thirty (30) days from receipt of this resolution.

Pasay City, 12 May 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

[2] NPC Circular 16-03, "Data Breach Management". Dated 15 December 2016.

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JTA
Data Protection Officer

COMPLAINTS AND INVESTIGATION DIVISION;
ENFORCEMENT DIVISION;
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: SUN LIFE OF CANADA (PHILIPPINES), INC. **CID BN 17-019**

x----------x

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the clarification of Sun Life of Canada (Philippines), Inc. ("Sun Life") dated 5 September 2019[1] stating that its Breach Notification Report submitted on 14 October 2017[2] to the National Privacy Commission ("Commission") is already its Full- Breach Report regarding the data breach incident involving ninety- three (93) policy owners and one hundred twelve (112) policies.

The Facts

On 9 October 2017, a Sun Life advisor's five (5) year old child accidentally spilled milk over an envelope containing a Premium Due List.[3] To avoid being reprimanded, the child threw the envelope into the trash bin. The garbage collector collected the bin with the envelope containing the list.[4]

On 12 October 2017, the advisor learned of the incident and immediately sent an e-mail to Sun Life's Compliance team.[5] However, the advisor was unable to recover the list from the garbage collector.[6]

On 14 October 2017, Sun Life submitted to the Commission a Breach Notification Report[7] narrating the incident. It also provided that the personal data involved in the incident are the following:

---

[1] Breach Notification Report of Sun Life Canada (Philippines), Inc. dated 5 September 2019.
[2] Breach Notification (NPC-SLOCPI-2017-02) dated 14 October 2017.
[3] *Ibid.*
[4] *Ibid.*
[5] *Ibid.*
[6] *Ibid.*
[7] *Ibid.*

1. Policy Number;
2. Client Name (Policy Owner/Insured);
3. Policy Name;
4. Face Amount;
5. Premium Due Date;
6. Premium Amount;
7. Issue Date; and
8. Status of the Policy.[8]

Sun Life has also undertaken the following measures to address the breach:

1. Monitor the policies for any unusual activity; and
2. To avoid recurrence of the incident, the advisor agreed to keep her files organized and secured when unattended.[9]

In view of the foregoing, Sun Life requested to be exempted from notifying its policyholders of the incident based on the following grounds:

1. The information contained in the policy/premium list does not contain sensitive personal information or information that may be used to enable identity fraud;
2. It is unlikely that the incident will give rise to a real risk of harm to the rights and freedoms of the policyholders in view of the controls in place in policy amendment, withdrawal or cancellation; and
3. A notification would not be in the best interest of the affected policyholders and may cause undue alarm.[10]

On 29 July 2019, the Commission issued a Resolution[11] granting the request for exemption from notifying the affected data subjects, and ordering Sun Life to submit a full report on its breach management within thirty (30) days from receipt of the Resolution.

---

[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.*
[11] Resolution In Re: Breach Notification Report of Sun Life of Canada (Philippines), Inc. dated 29 July 2019.

On 5 September 2019, Sun Life submitted a letter[12] clarifying to the Commission that the report it submitted on 14 October 2017 was not a preliminary report, but its final breach report. It again furnished the Commission with the report and reiterated the breach management actions it has undertaken. It also informed the Commission that it has not received any concern relating to the incident.

On 10 August 2020, the Enforcement Division issued its findings on the breach report, stating:

> Upon assessment of the breach report, this Division found that the measures undertaken and the notification sent complies with R.A. 10173 or the Data Privacy Act, its Implementing Rules and Regulations, and specifically NPC Circular 16-03 on Personal Data Breach Management (Circular).
>
> Taking into consideration the actions taken by Sun Life immediately after the breach and its remedial measures, this Division assessed that Sun Life acted on the breach incident in accordance with the incident response procedure required by the Circular.

Discussion

The Commission hereby finds the Breach Notification Report dated 14 October 2017 of Sun Life sufficient and considers this matter closed.

Section 17(D) of NPC Circular 16-03[13] provides that the Notification shall include, but not be limited to:

1. Nature of the Breach
    a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
    b. a chronology of the events leading up to the loss of control over the personal data;
    c. approximate number of data subjects or records involved;
    d. description or nature of the personal data breach;

[12] *Supra* note 1.
[13] Personal Data Management Breach dated 15 December 2016.

e. description of the likely consequences of the personal data breach; and
f. name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved
   a. description of sensitive personal information involved; and
   b. description of other information involved that may be used to enable identity fraud.

3. Measures Taken to Address the Breach
   a. description of the measures taken or proposed to be taken to address the breach;
   b. actions being taken to secure or recover the personal data that were compromised;
   c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
   d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
   e. the measures being taken to prevent a recurrence of the incident.

   The Commission reserves the right to require additional information, if necessary.

In the Breach Notification Report of Sun Life dated 14 October 2017,[14] it has already indicated the Nature of the Breach, the Personal Data Involved, and the Measures Taken to Address the Breach. The Commission has also not required additional information from Sun Life.

WHEREFORE, premises considered, the instant case, CID BN 17- 019, *In Re: Sun Life of Canada (Philippines), Inc.*, is hereby **CLOSED**.

SO ORDERED.

Pasay City, Philippines;
20 August 2020

[14] *Supra* note 2.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JSC
Data Protection Officer

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

JBD,

Complainant,

- versus -

JI and VVV,

Respondents.

CID 18-D-012

For: Violation of Data Privacy Act of 2012

x----------x

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to Complainant's Motion for Extension to Comply with the Order of the National Privacy Commission ("Commission") filed on 04 August 2020 by the Complainant[1] and Respondent VVV's Manifestation and Motion dated 29 July 2020.[2]

The Facts

The Commission issued an Order dated 21 May 2020[3] directing the Complainant to submit a Certified True Copy of the Position Paper containing the SSS documents filed with the Professional Regulatory Commission (PRC), and documents to substantiate the allegations made in paragraph 10 of the Verified Reply dated 13 August 2018 which refers to the findings of the SSS Fraud and Legal Department.

On 04 August 2020, Complainant filed a Motion for Extension to Comply with the said Order citing the lockdown of the PRC's Legal Division from 20 July 2020 to 27 July 2020, and the present classification of the National Capital Region (NCR) as an area placed under Modified Enhanced Community Quarantine (MECQ). Complainant specifically requests that he be given until 02 September 2020 to comply with the said Order.[4]

---

[1] Motion for Extension to comply with NPC Order filed on 4 August 2020.
[2] Motion and Manifestation dated 29 July 2020.
[3] NPC Order dated 21 May 2020.
[4] Motion for Extension to Comply with NPC Order filed on 4 August 2020, pp. 1-2.

On the other hand, Respondent VVV filed his Manifestation and Motion dated 29 July 2020 requesting the Commission to order the Complainant to furnish him a copy of the Verified Reply and allow him to file a Rejoinder. Respondent VVV claims that under Section 15 of NPC Circular 16-04, the respondent may file a Rejoinder after receipt of the Reply from the complainant. Respondent VVV also moved that his other prayers be granted, namely, to (a) note their manifestation; (b) hold in abeyance any clarificatory hearing pending the consideration of his Manifestation and Motion; and (c) note his counsel's entry of appearance.[5]

Discussion

The Commission grants Complainant's Motion for Extension to Comply with the Commission's Order as well as Respondent VVV's Manifestation and Motion.

As to Respondent VVV's Manifestation and Motion for them to file their Rejoinder, Section 15 of NPC Circular 16-04 is applicable. The said section provides that:

> Following the receipt of the Discovery Conference Report, the investigating officer shall issue an Order directing the respondent or respondents, as the case may be, to submit within ten (10) days from receipt thereof, a responsive Comment to the Complaint, together with any supporting documents the respondent or respondents may have, including the affidavits of any of the respondents' witnesses, if any. **The investigating officer, upon his or her discretion, may require the complainant to file a Reply within ten (10) days after receipt of the Order requiring the filing of a Reply. Such an Order may also require the respondent to file a Rejoinder within ten (10) days after receipt of the Reply**.[6]

Considering the above-quoted provision, the filing of both Reply and Rejoinder is dependent upon the discretion of the investigating officer. As provided therefor, the investigating officer may issue an Order requiring complainant to file a Reply and in the same Order, the respondent may also be required to file a Rejoinder within the said periods. Being discretionary, the investigating officer may therefore choose not to require both the complainant to file a Reply and the respondent to file a Rejoinder if he or she deems it not necessary. It follows that the investigating

[5] Manifestation and Motion dated 29 July 2020, p. 2.
[6] Emphasis supplied.

officer may also require the complainant to file a Reply without requiring the respondent to file a Rejoinder.

In the Order dated 12 July 2018,[7] while the Commission had required Complainant to file a Reply, there was however no Order requiring Respondent to file a Rejoinder. The said Order merely provided that:

> Respondents are hereby ordered to file their Responsive Comment within ten (10) days from 12 July 2018 or until 22 July 2018. **Complainant is also given ten (10) days from receipt of the Responsive Comment to file his Reply**.[8]

There was also no showing that a separate Order was issued requiring the filing of a Rejoinder. Thus, Respondent VVV's assertion that he can file a Rejoinder after a Reply pursuant to NPC Circular 16-04 is erroneous. Under the said Circular, the investigating officer must first require the respondent to file a Rejoinder.

Be that as it may, in the interest of justice and due process, the Commission grants the Motion of Respondent VVV that Complainant be ordered to furnish him a copy of his Verified Reply and that he be allowed to file his Rejoinder. His other prayers are also found reasonable in light of the facts of the case.

As to the Motion for Extension to Comply with the Commission's Order filed by the Complainant, the same is justified in view of the limitations brought about by the present COVID-19 pandemic and the reversion of the NCR to MECQ.

WHEREFORE, premises considered, Complainant's Motion for Extension to Comply with the Commission's Order until 02 September 2020 is hereby **GRANTED**. Complainant is **ORDERED** to furnish the Respondents a copy his Verified Reply within ten
(10) days from receipt of this Resolution.

Respondent VVV's Motion to Order the Complainant to furnish him a copy of the Verified Reply and his prayers for the Commission to (a) Note his Manifestation; (b) Hold in abeyance any clarificatory hearing pending the consideration of his Manifestation, and (c) Note his counsel's entry of appearance, are

---

[7] Order dated 12 July 2018.
[8] Emphasis supplied.

hereby **GRANTED**. Respondent is also **ORDERED** to submit his Rejoinder within ten (10) days from receipt of the Verified Reply.

SO ORDERED.

Pasay City, Philippines;
06 August 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JBD
Complainant

VVV
Respondent

JI
Respondent

BACCAY HUSSIN & VISCONDE
Represented by Atty. KLR

IN RE: POPULUS LENDING CORPORATION (PESOPOP) AND ITS RESPONSIBLE OFFICERS

NPC SS 21-008

INITIATED AS A *SUA SPONTE* NPC INVESTIGATION INTO THE POSSIBLE DATA PRIVACY VIOLATIONS COMMITTED BY POPULUS LENDING CORPORATION (PESOPOP)

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

This refers to the Temporary Ban on the processing of personal data issued against Populus Lending Corporation, the owners and operator of the online lending application, Pesopop, and its responsible officers (Pesopop) in an Order dated 12 August 2021.

Facts

On 12 August 2021, the Commission issued an Order imposing a Temporary Ban on the processing of personal data against Pesopop in relation to its online lending application:

> **WHEREFORE**, all these premises considered, this Commission **GRANTS** the Application for Temporary Ban on the processing of personal data filed by the Complaints and Investigation Division (CID) of the National Privacy Commission. A **TEMPORARY BAN ON PROCESSING OF PERSONAL DATA**
> is hereby issued against Respondent Populus Lending Corporation, as the operator of the online lending application, Pesopop.

Further, pursuant to the **TEMPORARY BAN**, Respondent Populus Lending Corporation shall:

1. Immediately take down its online lending application, Pesopop, to ensure that it is no longer available for download, installation or use by data subjects; and

2. Stop personal data processing activities, including those activities outsourced to third parties, where the processing operations involves use of information from the phonebook, directory, and contact list of data subjects, disclosure of false or unwarranted information, and other unduly intrusive personal data processing methods.

The **TEMPORARY BAN ON PROCESSING OF PERSONAL DATA** shall remain in effect until the final resolution of the *sua sponte* investigation against Respondent and its responsible officers.

Let copies of this Order be furnished to the National Telecommunications Commission for their appropriate action, and Google LLC, which operates the Google Play Store for its compliance in accordance with the terms and conditions of its platform.

Furthermore, Respondent Populus Lending Corporation and its responsible officers are **ORDERED, within ten (10) days** from receipt of this Order, to file a **COMMENT** on the allegations in the attached Fact-Finding Report, pursuant to Section 6 of Rule X of NPC Circular No. 2021-01 (2021 NPC Rules of Procedure).

In case of failure by the Respondent and its responsible officers to file a Comment, this case shall be deemed submitted for resolution based on the evidence on record.

The proceedings before the Commission based on the Fact-Finding Report of the CID, which serves as the Complaint against Respondent Populus Lending Corporation and its responsible officers, will now resume, pursuant to Section 2, Rule IX of the 2021 NPC Rules of Procedure.

SO ORDERED.[1]

[1] Order, 12 August 2021, at 11, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

On 03 September 2021, Pesopop, through its counsel Zosa & Quijano Law Offices, filed a Notice of Entry of Appearance with Motion for Reconsideration.[2]

In its Motion for Reconsideration, Pesopop manifested that it shall be deemed as its Comment on the allegation in the Fact-Finding Report in compliance with the Order dated 12 August 2021.[3] Pesopop prayed:

> **WHEREFORE**, premises considered, the respondents respectfully prays that this Honorable Commission to:
>
> 1. **Note** the entry of appearance of the undersigned counsel;
> 2. **GRANT** the instant motion **RECONSIDER AND SET-ASIDE** the order dated 12 August 2021; and
> 3. **ISSUE** a new order cancelling the temporary ban for being void ab initio;
> 4. **DISMISS** the complaint as regards the individual respondents for lack of participation and evidence of direct participation;
> 5. **ALLOW** respondent Pesopop reasonable time to comply and amend its data privacy terms and conditions to conform to the Data Privacy Act of 2021, rules and regulations and all issuance of this Honorable Commission.
>
> Other reliefs, just and equitable under the premises are likewise prayed for.[4]

On 17 September 2021, the Commission issued an Order directing Pesopop to appear in a Clarificatory Hearing scheduled on 28 September 2021.[5] During the Clarificatory Hearing, the Commission ordered Pesopop to submit the following compliance documents:

1. Revised Privacy Policy of Pesopop;
2. Revised Terms and Conditions or Terms of Service of Pesopop;
3. Revised Pesopop application;
4. Company Profile and a discussion of the business model of the Corporation;
5. An explanation of the discrepancy between Counsel's representations in the Motion for Reconsideration on

---

[2] Notice of Appearance with Motion for Reconsideration, 03 September 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[3] *Id.* at 6.
[4] *Id.* at 7.
[5] Order, 17 September 2021, at 5, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

the access to the phone contact list and the Privacy Policy dated 10 September 2021;

6. A technical explanation on the purpose of the code "android.permission.READ_CONTACTS", which if enabled, gives the application permission to read the user's contacts data;
7. Collection Policy of the corporation;
8. An Agreement between the corporation and its third party collection partners or agents;
9. An Agreement between the corporation and its third-party payment partners;
10. An explanation behind the drafting process of the Privacy Policy dated 10 September 2021;
11. Privacy Manual; and
12. Employee Manual, particularly on the provisions governing its employees' conduct of collecting debt and collection and usage of personal information.[6]

The counsel of Pesopop manifested that he requires fifteen (15) days from 28 September 2020 to submit the compliance documents.[7] Based on the counsel's representations, the Commission issued an Order directing Pesopop to submit the compliance documents within a non- extendible period of fifteen (15) days from receipt of the Order.[8]

On 20 October 2021, Pesopop filed a Motion to Admit With Compliance (to the Order dated 28 September 2021).[9] It manifested that it received the Order dated 28 September 2020 on 01 October 2021.[10] It stated that the fifteen-day period was insufficient and that it needed more time to collate the compliance documents. [11] It also submitted some of its compliance documents pursuant to the Order dated 28 September 2020.[12]

On 29 October 2021, the Enforcement Division (EnD) of the National Privacy Commission (NPC) determined that version 1.5.4 of the online lending application was available for download from Google Play, and

---

[6] Order, 28 September 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[7] T.S.N., *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021) (pending).
[8] Order, 28 September 2021, at 2, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008, (NPC 2021).
[9] Motion to Admit with Compliance, 20 October 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[10] *Id.* at 1.
[11] *Id.* at 1.
[12] *Id.* at 1.

download links to the online lending application were available on its official Facebook page though the "Use App" button, its website through the "Get it on Google Play" and "Download Pesopop now" buttons, and a QR Code.[13]

On 08 November 2021, the EnD sent a letter to Pesopop in relation to the availability of the online lending application despite the pendency of the Temporary Ban.[14] The letter required Pesopop to explain within ten (10) days from its receipt of the letter the availability of the online lending application, and ordered it to immediately ensure that the online lending application is no longer available for download, installation, or use by the data subjects in any manner until the Temporary Ban is lifted.[15]

On 15 November 2021, Pesopop, through counsel, replied to the EnD.[16] It informed the EnD that it filed its Motion for Reconsideration to the Order dated 12 August 2021, and that its Motion for Reconsideration shall be treated as its Motion to Lift the Temporary Ban. [17] It also reiterated that the Temporary Ban is *void ab initio* since "it was filed *motu proprio* and that the same was issued without the required bond."[18]

On 25 November 2021, the EnD issued a second letter to Pesopop pointing out that the online lending application was once again available on Google Play and ordered Pesopop to immediately ensure that the online lending application is no longer available for download. [19] It also explained that the filing of the Motion of Reconsideration does not in any way lift or suspend the effectivity of the Temporary Ban.[20]

---

[13] Enforcement Division Memorandum, 03 November 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[14] Letter *from* Enforcement Division, National Privacy Commission, Compliance With Order dated 12 August 2021 in NPC SS 21-008 entitled "In re: Populus Lending Corporation (Pesopop) and its Responsible Officers" *to* Zosa & Quijano Law Offices (08 November 2021).
[15] *Id.* at 2.
[16] Letter *from* Zosa & Quijano Law Offices, Reply to letter dated 8 November 2021 *to* Enforcement Division, National Privacy Commission (15 November 2021).
[17] *Id.*
[18] *Id.*
[19] Letter *from* Enforcement Division, National Privacy Commission, Compliance With Order dated 12 August 2021 in NPC SS 21-008 entitled "In re: Populus Lending Corporation (Pesopop) and its Responsible Officers" *to* Zosa & Quijano Law Offices (25 November 2021).
[20] *Id.*

On 26 November 2021, the EnD verified that the online lending application was taken down from Google Play.[21]

On 06 December 2021, the EnD determined that version 1.5.5 of the online lending application was once again available for download from Google Play Store.[22]

On 28 December 2021, the EnD issued a third letter to Pesopop, which stated that version 1.5.5 of the online lending application was once again available for download on Google Play Store.[23] Again, the EnD ordered Pesopop to immediately take down the online lending application from Google Play and ensure that it is no longer available for download, installation, or use by the data subjects.[24]

On 02 January 2022, Pesopop replied to the EnD and informed the EnD that it already removed the online lending application from Google Play.[25] It explained that it had no intention to violate the Order dated 12 August 2021.[26] It reiterated that the Temporary Ban is *void ab initio* and claimed that it exposes the Commission to liability for damages if the Temporary Ban is not lifted.[27] It also prayed for the resolution of the pending Motion for Reconsideration.[28]

Discussion

The Commission recognizes that the Motion for Reconsideration shall serve as Pesopop's Comment to the Fact-Finding Report in compliance with the Order dated 12 August 2021, and its Motion to Lift the Temporary Ban.

Be as it may, the Commission denies the Motion to Lift and maintains the Temporary Ban on Pesopop's processing of personal data.

---

[21] Enforcement Division Memorandum, 26 November 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[22] *Id.*
[23] Letter *from* Enforcement Division, National Privacy Commission, Compliance With Order dated 12 August 2021 in NPC SS 21-008 entitled "In re: Populus Lending Corporation (Pesopop) and its Responsible Officers" *to* Zosa & Quijano Law Offices (28 December 2021).
[24] *Id.* at 2.
[25] Letter *from* Zosa & Quijano Law Offices, Compliance to letter dated 28 December 2021 *to* Enforcement Division, National Privacy Commission (02 January 2022).
[26] *Id.*
[27] *Id.*
[28] *Id.*

At the onset, the Commission notes that the period to submit the compliance documents lapsed on 15 October 2021. The Commission stresses that counsel himself requested a fifteen-day period counted from the Clarificatory Hearing on 28 September 2021 to submit the necessary compliance documents. In fact, the Commission already gave Pesopop significant time to submit the compliance documents by 15 October 2021 or fifteen (15) days from 01 October 2021, which is the date of Pesopop's receipt of the Order dated 28 September 2021. Despite the additional period given to Pesopop, it still belatedly submitted its compliance documents on 20 October 2021 when the period to submit had already lapsed.[29]

Nevertheless, in the interest of fully assessing the issue at hand, the Commission admits and considered Pesopop's compliance documents in its resolution to lift or maintain the Temporary Ban imposed in the Order dated 12 August 2021.

The Temporary Ban imposed on Pesopop is valid.

Contrary to Pesopop's assertions in its Motion for Reconsideration and its 02 January 2022 letter, the Temporary Ban is not *void ab initio*. Pesopop maintains that the Temporary Ban is unwarranted because the Commission failed to satisfy the second and third requisites enumerated in Rule IX Section 3 of NPC Circular No. 20-01 or the 2021 NPC Rules of Procedure. For reference, the requisites are:

> Section 3. Requisites for temporary ban. – A temporary ban on processing of personal data may be granted only when:
>
> 1. it is necessary in order to preserve the rights of the complainant or to protect national security or public interest, or if it is necessary to preserve and protect the rights of data subjects;
> 2. the motion shows facts entitling the complainant to the relief demanded;
> 3. unless exempted from the payment of filing fees as provided for in these Rules, the complainant shall file with the NPC a bond in an amount to be fixed by the

[29] Motion to Admit with Compliance, 20 October 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

investigating officer executed in favor of the party or person so banned from processing personal data; and

4. the parties are heard in a summary hearing.[30]

The requisites have been explained in the Order dated 12 August 2021. In response to Pesopop's assertions in the Motion for Reconsideration, the Commission shall recapitulate why the second and third requisites have been satisfied.

As discussed in the Order dated 12 August 2021, the Fact-Finding Report with Application for the Issuance of a Temporary Ban (FFR) filed by the Complaints and Investigation Division (CID) of the NPC prayed for the imposition of a Temporary Ban against Pesopop.[31] It alleged that undisclosed permissions that violate the right of the data subjects to be informed exist and merit the issuance of a temporary ban.[32] Thus, the second requisite is satisfied.

Further, the Commission reiterates that the CID of the NPC initiated the Complaint through a *sua sponte* investigation under Rule X of the 2021 NPC Rules of Procedure.[33] As such, the NPC, as a government agency, is exempt from filing fees and consequently, the bond for the application of Temporary Ban as stated in Rule II Section 4 (a) of the 2021 NPC Rules of Procedure. [34] Thus, the third requisite is also satisfied.

Pesopop's claim that the Order imposing the Temporary Ban was issued without authority is patently wrong. The Temporary Ban imposed on Pesopop's processing of personal data is valid.

Pesopop has not sufficiently addressed the reasons for the issuance of the Temporary Ban.

---

[30] National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], rule III, § 5 (28 January 2021).
[31] Order, 12 August 2021, at 11, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[32] Order, 12 August 2021, at 6–9, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[33] NPC 2021 Rules of Procedure, rule X.
[34] NPC 2021 Rules of Procedure, rule II § 4 (a).

Considering that the Order dated 12 August 2021 already discussed the existence of facts and circumstances necessitating the issuance of a Temporary Ban, Pesopop now has the burden to prove that the Temporary Ban imposed on the processing of personal data is no longer necessary. As such, it must show that the reasons behind the imposition of the Temporary Ban as stated in the Order dated 12 August 2021 no longer exist. This is determined based on its actions and submissions to the Commission.

In the Order dated 12 August 2021, the Commission directed Pesopop to immediately take down its online lending application to ensure that it is no longer available for download, installation, or use by its data subjects and to stop personal data processing activities. [35] Pesopop, however, violated the Temporary Ban when it made versions 1.5.4 and
1.5.5 of its online lending application available several times on Google Play, its official Facebook page, its website, and through a QR Code. By making the online lending application available for download, it appears that Pesopop continued personal data processing activities while the Temporary Ban issued by the Commission was in effect.

Pesopop indeed removed its online lending application from Google Play following the Order dated 12 August 2021. It, however, disregarded the Temporary Ban when it made the online lending application available for download three separate instances. It only took down the online lending application from Google Play whenever it would receive orders from the EnD to do so.

In effect, Pesopop never complied with the Order dated 12 August 2021, as verified by the EnD.[36] Even if Pesopop took down the online lending application whenever it received an order to do so from the EnD, the fact remains that the online lending application should not have been available for download, to begin with. Aside from the fact that Pesopop never presented any evidence to show their compliance with the Order dated 12 August 2021, the fact that it made the application available several times shows that it violated the Temporary Ban.

---

[35] Order, 12 August 2021, at 11, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[36] Enforcement Division Memorandum, 26 November 2021, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).

Further, in its Motion for Reconsideration, Pesopop represented that it "undertakes to immediately make a complete and thorough review and amendment of its existing data privacy terms and conditions and will revise the same to conform to the [DPA]."[37] It, however, appears from Pesopop's submissions that it does not intend to abide by its statements.

Despite the additional time given by the Commission and the delay in Pesopop's submission of its compliance documents, the EnD determined that Pesopop did not submit all the documents and information required upon it following the Order dated 28 September 2021.

As verified by the EnD, Pesopop did not submit the following:

1. An explanation of the discrepancy between Counsel's representations in the Motion for Reconsideration on the access to the phone contact list and the Privacy Policy dated 10 September 2021;
2. A technical explanation on the purpose of the code "android.permission.READ_CONTACTS", which if enabled, gives the application permission to read the user's contacts data; and
3. An Agreement between the corporation and its third party collection partners or agents;

In its Motion for Reconsideration, Pesopop, through its Counsel, claimed that the "inclusion of requesting for the phone contact list as part of the registration to apply for loan in PesosPop was purely unintentional and a result of an inadvertent and honest mistakes."[38] Instead of explaining the discrepancy between Counsel's representations in the Motion for Reconsideration on the access to the phone contact list and what its Privacy Policy dated 10 September 2021 states, Pesopop explained the necessity of the online lending application's access to its users' contact lists.[39] Suffice to say, Pesopop's explanation was unresponsive.

---

[37] Notice of Appearance with Motion for Reconsideration, 03 September 2021, at 5, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[38] Notice of Appearance with Motion for Reconsideration, 03 September 2021, at 3, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[39] Enforcement Division Memorandum, 12 January 2022, at 5, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022).

The EnD also raised the glaring deficiencies in Pesopop's Revised Privacy Policy. It observed that the Revised Privacy Policy does not fully abide by Section 16 of the DPA. For reference, Section 16 of the DPA states:

> Section 16. *Rights of the Data Subject.* – The data subject is entitled to:
>
> (a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;
> (b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:
> (1) Description of the personal information to be entered into the system;
> (2) Purposes for which they are being or are to be processed;
> (3) Scope and method of the personal information processing;
> (4) The recipients or classes of recipients to whom they are or may be disclosed;
> (5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
> (6) The identity and contact details of the personal information controller or its representative;
> (7) The period for which the information will be stored; and
> (8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.[40]

The EnD determined the following:

> [T]he revised Privacy Policy failed to:
>
> 1. discuss any methods utilized for automated access and the logic involved;
>
> 2. provide its contact details for except for an e-mail address: pesopop.cs@cashrocket.com.ph, which the users can use if they want to request for an update of information;
>
> 3. specify the retention period for data collected, except for generic terms stated like:

---

[40] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 16 (2012).

a. "Storage time will not exceed your usage time." and
b. "We will only keep your information for as long as we are either required to by law or as is relevant and material for the purposes for which it was collected."; and

4. discuss the existence of rights of data subjects, except the right to update their personal data or the right to rectify.

Upon comparison of the Privacy Policies in the different versions of the app, it can be observed that the respondent made several changes from the Privacy Policy in the 1.5.1 version (the one investigated by CID) and Policies in the later versions, which are all the same. Despite the changes, however, the revised Privacy Policy still lacks the required information mandated by the DPA and its IRR.

Further, the policy also failed to provide details on its use of profiling, automated processing, automated decision-making, or credit rating or scoring, and the categories of data considered in deciding whether to approve or disapprove a loan application.[17] Despite informing its users that it will use the information it collects to prevent fraud, credit risk evaluation management, debt collection, identity verification, and anti- money laundering, activities that obviously involves profiling, credit rating or scoring.[41]

Based on the EnD's assessment, Pesopop also does not comply with the provisions of NPC Circular No. 20-01 (Guidelines on the Processing of Personal Data for Loan-Related Transactions), particularly Section 3 of NPC Circular No. 20-01, which states:

Section 3. *Guidelines*. The processing of personal data for evaluating loan applications, granting loans, collection of loans, and closure of loan accounts shall be subject to the following general guidelines:

A. Borrowers shall be provided all the details required under Section 16 (b) of the DPA and Section 34 (a)(2) of its IRR, in a clear language and in the most appropriate format.

. . .

[41] Enforcement Division Memorandum, 12 January 2022, at 3 - 4, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022) (pending).

D. Where online apps are used for loan processing activities, LCs, FCs, and other persons acting as such shall be prohibited from requiring unnecessary permissions that involve personal and sensitive personal information.

1. Application permissions shall only be allowed when suitable, necessary, and not excessive for the purpose of KYC, determining creditworthiness, preventing fraud, and collecting the debt in accordance with applicable provisions of law.

2. When such purpose has already been achieved, such online apps shall prompt the data subject to turn off or disallow these permissions.

3. Where an online app requires access to the borrower's phone camera to take a photo of the borrower and/or the photo gallery to choose a photo for the exclusive purpose of KYC and preventing fraud at the beginning of the loan application, permission for such access may be allowed at that stage in the loan application process.

   Where the photo has already been taken and saved in the application, the application should already turn off such permission by default, or at the very least, prompt the borrowers through appropriate means, i.e. just-in-time, pop-up notices, etc. that they may already turn off or disallow such permission as the same is no longer necessary for the operation of the application. In no way shall the borrower's photo be used to harass or embarrass the borrower in order to collect a delinquent loan.

4. Access to contact details in whatever form, such as but not limited to phone contact list or e-mail lists, the harvesting of social media contacts, and/or copying or otherwise saving these contacts for use in debt collection or to harass in any way the borrower or his/her contacts, are prohibited. In all instances, online lending apps must have a separate interface where borrowers can provide character references and/or co-makers of their own choosing.[42]

The EnD determined that Pesopop's submissions show that the online lending application still contains the undisclosed permissions identified in the FFR:

---

[42] National Privacy Commission, Guidelines on the Processing of Personal Data for Loan-Related Transactions, Circular No. 01, Series of 2020 [NPC Circ. No. 20-01], § 3 (A), (D) (28 January 2021).

> Based on the screenshots of the revised application submitted by Populus Lending Corporation, it can be deduced that the same dangerous permissions (Phone, Location, Storage and Camera) are still present.
>
> The 'Notice' found in the application shows that the Contact list is one of the permissions needed to start the loan application. However, it was not shown in the screenshots the specific part where the application asks for the Contacts permission during the collection of information or loan application process.
>
> It can also be seen that Step 4, where the app asks for contact references based on the simulation of other versions, is missing in the attached screenshots as Step 5 is shown after Step 3. Thus, it cannot be verified whether the revised app offered a separate interface where borrowers can provide character references and/or co-makers of their own choosing as required by the NPC Circular 20-01.
>
> Further, the Division cannot verify if the revised application, which requires access to camera, turn off such permission by default, or at the very least, prompt the borrowers through appropriate means, i.e. just-in-time, pop-up notices, etc. that they may already turn off or disallow such permission as the same is no longer necessary for the operation of the application, after use during loan application or account creation. [43]

The EnD also elaborated on the online lending application's access to the users' contacts list:

> Consequently, it can be assessed, based on the statement made in their revised Privacy Policy, that the Revised Application indeed still have access to the contacts of the user's phone, as stated:
>
> > **We will request you to 'Read Contacts' permission. If you agree to the authorization, we will scan and upload the contact list information to https://api.pesopop.com:18062 using the most secured data transfer protocol (HTTPS).** We will store your personal information through DES and AES encryption.
> >
> > Storage time will not exceed your usage time.

[43] Enforcement Division Memorandum, 12 January 2022, at 5, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2022) (pending).

> We will request contact list limited to five (5) phone contacts for character reference purpose and identity verification. **By giving us your home and/or mobile phone number, we have your permission to contact you or the phone contacts you provided us.** This shall allow us to use text messaging, artificial or prerecorded voice messages, and automatic dialing technology, for all purposes not prohibited by applicable law. We may also send an email to any address where we reasonably believe we can contact you (include the contact list). Some of the purposes for calls and messages include suspected fraud or identity theft; obtaining information; transactions on or servicing of your account; and collecting on your account or collecting the delinquent account.

However, it was not shown in the Revised Application screenshots submitted, the supposed 'Step 4' where users will choose character reference from their phone contact list.
But, it should be noted that the app versions 1.5.4 and the 1.5.5. currently available in Google Play Store, have these features.

. . .

Clearly, the app's access to the phone contacts, though limited to five (5) contacts for character reference is a violation of the said circular, especially that the contact lists are not only for purpose of character verification but will also be used to contact them for debt collection as stated in the revised Privacy Policy:

> By giving us your home and/or mobile phone number, we have your permission **to contact you or the phone contacts you provided us.** This shall allow us to use text messaging, artificial or prerecorded voice messages, and automatic dialing technology, for all purposes not prohibited by applicable law. **We may also send an email to any address where we reasonably believe we can contact you (include the contact list).** Some of the **purposes for calls and messages include suspected fraud or identity theft; obtaining information; transactions on or servicing of your account; and collecting on your account or collecting the delinquent account.**[44]

In its Motion for Reconsideration, Pesopop represented that it "do[es] not have any intention to violate any data privacy law, rules and regulations, issuances and will always consider the privacy rights of

---

[44] Enforcement Division Memorandum, 12 January 2022, at 6 – 7, *in re: Populus Lending Corporation and Its Responsible Officers*, NPC SS 21-008 (NPC 2022). Emphasis supplied.

its customer supreme."[45] Pesopop, however, continued to make the online lending application available for download during the Temporary Ban and it has not rectified its operations to comply with the DPA, its IRR, and the issuances of the Commission. As such, it has not sufficiently shown to satisfaction of the Commission that lifting the Temporary Ban imposed in the Order dated 12 August 2021 is warranted. It also appears from Pesopop's actions that it had no intention to comply with the Order dated 12 August 2021 to justify the lifting of the Temporary Ban imposed on its processing of personal data.

Given all these, the Commission finds that Pesopop violated the Temporary Ban imposed in the Order dated 12 August 2021. Rule IX Section 8 of NPC Circular No. 21-01 or the 2021 Rules of Procedure states:

> Section 8. *Duration of temporary ban.* – When issued, **the temporary ban on processing of personal data shall remain in effect until the final resolution of the main case**, or upon further orders by the Commission or other lawful authority.[46]

Considering the foregoing, the Commission finds no reason to lift the Temporary Ban.

WHEREFORE, premises considered, the Commission **ADMITS** the compliance documents submitted by Populus Lending Corporation and its responsible officers.

The Commission **DENIES** the Motion for Reconsideration, and **MAINTAINS** the Temporary Ban on the processing of personal data issued against Populus Lending Corporation and its responsible officers.

Further, the Commission orders Populus Lending Corporation and its responsible officers and the Complaints and Investigation Division of the National Privacy Commission to **SUBMIT within ten (10) days from the receipt of this Order** their respective Memoranda on their respective arguments on the facts and issues for the resolution of this Commission.

---

[45] Notice of Appearance with Motion for Reconsideration, 03 September 2021, at 5, *in* In re: Populus Lending Corporation and its Responsible Officers, NPC SS 21-008 (NPC 2021).
[46] NPC 2021 Rules of Procedure, rule IX § 8 (28 January 2021). Emphasis supplied.

SO ORDERED.

City of Pasay, Philippines.
27 January 2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

ZOSA & QUIJANO LAW OFFICES
Counsel for Populus Lending Corporation and its Responsible Officers

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: ASIAN HOSPITAL AND MEDICAL CENTER **NPC BN 18-021**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is a breach notification submitted by Asian Hospital and Medical Center (AHMC) involving the access of a patient's chart by third persons.

Facts

On 15 February 2018, the data subject was admitted as a patient at AHMC.[1] During the duration of her admission, AHMC's Guest Services Department received numerous inquiries about her.[2]

On 16 February 2018, a group of people, some introducing themselves as police and military personnel, came to the nurses' station asking for the patient's whereabouts.[3] The hospital's security team, assisted by the police, later escorted the group outside of the hospital to prevent any further commotion.[4]

On the same day, the Manager of the General Nursing Unit (GNU) informed AHMC's Data Protection Officer (DPO) of a possible data breach.[5] The GNU Manager narrated that he received an unverified report concerning a photo of AHMC's Hospital Information System (HIS) that shows the patient's name, age, date of birth, and medical diagnosis.[6] The DPO informed the GNU Manager that he will initiate

---

[1] Initial Report, 22 February 2018, at 2, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*

an investigation on the alleged breach in accordance with AHMC's Data Privacy Breach Protocol.[7]

AHMC's Medical Informatics Team (MID) initiated the extraction of the names of the personnel who viewed the patient's chart.[8] The MID submitted two reports, which are those who searched the patient's name (search log) and those who accessed the patient's chart (view log).[9]

On 17 February 2018, the patient was discharged from the HIS and was physically discharged from the hospital the following day.[10]

As part of the investigation, on 19 February 2018, the DPO conducted interviews with the GNU Manager and the Medical Information Services Manager.[11]

After the initial investigation, AHMC discovered that a photo of the patient's personal data was already posted in a Facebook group of what appears to be composed of the patient's creditors.[12] At this point, AHMC stated that it "has established reasonable belief and determination that a personal data breach indeed transpired."[13] As a result, AHMC conducted a full investigation on how an unauthorized person took a photo of its HIS.[14]

On 22 February 2018, AHMC notified the patient through mail sent to her home address.[15]

On 22 February 2018, AHMC notified the National Privacy Commission (NPC) of the breach.[16]

---

[7] Initial Report, 22 February 2018, at 2, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Initial Report, 22 February 2018, at 2, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[14] *Id.*
[15] *Id.* at 4.
[16] *Id.* at 2.

On 06 October 2020, the NPC, through its Complaints and Investigation Division (CID) issued an Order requiring AHMC to submit its Full Breach Report within fifteen (15) days from receipt.[17]

On 19 October 2020, AHMC submitted its compliance,[18] together with the following documents: (1) a copy of its initial report;[19] (2) a summary of employees who underwent the internal investigation or "dialogue";[20] (3) its security incident report;[21] and (4) the remedial measures taken to address the incident and prevent its recurrence.[22]

In its compliance, it stated that it issued show cause memoranda and conducted a dialogue session with all personnel whose names were recorded in the search log and view log based on the report of the MID.[23] AHMC also reviewed the closed-circuit television (CCTV) camera footage.[24]

AHMC, through its investigation, determined that a member of the hospital staff took a photo of the patient's chart from AHMC's desktop using her mobile phone and forwarded the photo to a Facebook messenger group chat.[25]

As a result, AHMC imposed sanctions on all its personnel who violated the hospital's policy and procedure under the hospital's Code of Ethics.[26]

AHMC also stated that it took remedial measures to address the incident and prevent its recurrence and attached proof, including:

1. Strengthened and improved hospital policies and reiteration of protocols to all AHMC end users.
    i. Information security (PL-MID-004)

---

[17] Order, 06 October 2020, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[18] Response Letter dated 19 October 2020, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[19] Compliance, 19 October 2020, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[20] *Id.* Annex A.
[21] *Id.* Annex B.
[22] *Id.* Annex C.
[23] Response Letter dated 19 October 2020, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[24] *Id.*
[25] *Id.*
[26] *Id.*

ii. Access Matrix Security (PL-MID-002)

2. Reinforced Violations on Computer, Information Security & Data Privacy under the Hospital's Code of Ethics.
3. Integration of Data Privacy Act trainings for all newly hired employees under the "Safety Culture Program."
4. Confidentiality agreement[s] were ensued between AHMC and hospital staff, doctors, outsourced personnel and consultant and third party vendors.
5. Data Privacy Initiatives such as "Think Before You Click", as a social media reminder for all hospital employees, patients and visitors.
6. Integration of Data Privacy Act video materials in all AHMC's Devant LED Informercial platform.[27]

Issue

Whether AHMC conducted proper breach management, including the implementation of reasonable and appropriate security measures and notification of the affected data subject.

Discussion

The Commission finds that AHMC conducted proper breach management and implemented reasonable and appropriate security measures in addressing the breach. AHMC has also sufficiently notified the patient. Thus, the Commission resolves to close the matter.

Section 20 (a) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) provides that a Personal Information Controller (PIC) should implement reasonable and appropriate measures to protect personal information:

> Section 20. *Security of Personal Information.*
>
> (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[28]

---

[27] *Id.*
[28] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (a) (2012).

Similarly, Section 17 (D) of NPC Circular 16-03 (Personal Data Breach Management) provides a PIC with the obligation to notify the NPC of a personal data breach.[29] The provision also outlines the content of notification specifically the measures that a PIC took to address the breach:

> Section 17. *Notification of the Commission*. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification*. The notification shall include, but not be limited to:
>
> . . .
>
> 3. Measures Taken to Address the Breach
>
> a. description of the measures taken or proposed to be taken to address the breach;
>
> b. actions being taken to secure or recover the personal data that were compromised;
>
> c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
>
> d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
>
> e. the measures being taken to prevent a recurrence of the incident.[30]

As early as its Initial Report, AHMC narrated the measures it took to address the breach following Section 20 (a) of the DPA and Section 17
(D) (3) of NPC Circular 16-03.

Upon receiving a report of a potential data breach, AHMC initiated its Data Privacy Breach Protocol.[31] This included the extraction of the names of the personnel who accessed the patient's chart on the HIS and the conduct of interviews and dialogues with the involved personnel.[32]

---

[29] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §17 (D)(3) (15 December 2016).
[30] *Id.*
[31] Initial Report, 22 February 2018, at 2, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[32] *Id.*

As part of its remedial measures, AHMC stated that it strengthened and improved the hospital's policies, specifically its Information Security Policy and Access Matrix Security Policy, and re-trained all its employees and medical staff on these policies. [33]

Further, AHMC reinforced its provisions on "Violations on Computer, Information Security, and Data Privacy" under the hospital's Code of Ethics.[34] This included the imposition of the penalty of dismissal on the first offense for the following violations:

Computer, Information Security and Data Privacy[35]

. . .

VIOLATIONS on Computer, Information Security and Data Privacy	**PENALTIES**			
	1st Offense	2nd Offense	3rd Offense	4th Offense
1. **Willful non-observance of Computer Information Security and Data Privacy Policy, resulting in disruption of Hospital's operations, procedure, activities, and breach of information.**	**Dismissal**			
2. **Unauthorized Disclosure of Personal Information and Sensitive Personal Information of data subjects to co-employees, relatives, friends**	**Dismissal**			

[33] Compliance, 19 October 2020, Annex C, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[34] *Id.*
[35] *Id.*

and the like that will lead to Personal Data Breach. **3. Concealment of knowledge on Incidents of breach information.**	**Dismissal**			

In addition, AHMC integrated data privacy trainings for all newly hired employees in its Safety Culture Program which aims "to provide awareness and preventive action in response to possible hazard to individual and hospital-wide safety."[36]

AHMC also reiterated its confidentiality agreements between AHMC and its staff, doctors, outsourced personnel, consultants, and third- party vendors.[37] In its confidentiality agreements, AHMC explained that it has "a legal and ethical responsibility to safeguard the privacy of all patients and protect information that is identified as confidential."[38]

Further, AHMC submitted its Data Protection Vendor Consent Form, prepared by Metro Pacific Hospital Holdings, Inc. Hospital Group, which requires its suppliers to consent before AHMC processes personal data in relation to supplier registration and accreditation.[39]

Finally, AHMC created data privacy initiatives, such as "Think Before You Click," a reminder on using social media shared with all hospital employees, patients, and visitors.[40] It also included data privacy video materials on its LED informercial platform. [41]

It is the obligation of the PIC, such as AHMC, to ensure that it promptly and properly notifies its affected data subjects of the

---

[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Compliance, 19 October 2020, Annex C, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[40] *Id.*
[41] *Id.*

breach.[42] The Commission has consistently emphasized that the purpose of the notification to the data subjects is to allow them to take the necessary precautions or other measures to protect themselves against its possible effects.[43]

In this case, AHMC notified the patient through mail.[44] It submitted a copy of the letter and a 2GO Express receipt as proof of mailing to the patient's home address.[45]

In its letter, AHMC provided a narration of how the breach occurred, the personal data involved, and the results of its initial investigation.[46]

AHMC also enumerated the measures it undertook upon receiving information pertaining to the breach.[47] It also informed the patient that it will be issuing show cause memoranda to the responsible personnel and improve the security safeguards to its HIS. [48]

Further, AHMC provided the patient with the contact details of its DPO and Risk Management Manager in case she needed any assistance or further information in relation to the breach.[49]

Given the foregoing, the Commission finds that the measures undertaken by AHMC have sufficiently addressed the incident and prevented its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-021 In re: Asian Hospital and Medical Center is **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.

---

[42] NPC Circ. No. 16-03, § 18 (A).
[43] *Id.*
[44] Initial Report, 22 February 2018, at 2, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[45] *Id.*
[46] Letter Re: Data Privacy Breach, 22 February 2018, at 1, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[47] *Id.* at 2.
[48] *Id.* at 2-3.
[49] *Id.* at 2.

13 November 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

JC
Assistant Manager, Data Privacy and Regulatory Compliance
Asian Hospital and Medical Center

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: E-SCIENCE CORPORATION **NPC BN 20-124**

x----------x

RESOLUTION

AGUIRRE, D.P.C.:

For the Commission's resolution is the Request for Exemption to Notify the Data Subjects from E-Science Corporation ("E-Science") dated 28 August 2020 involving a data breach incident affecting approximately four thousand (4,000) test records of data subjects.[1]

The Facts

On 6 August 2020, this Commission issued a Resolution[2] with the following disposition, *to wit*:

> **WHEREFORE,** premises considered, E-Science Corporation is **ORDERED** to **1) SUBMIT** with dispatch a Full Report of the Personal Data Breach as required under Section 17(C) of NPC Circular No. 16-03; and **2) SHOW CAUSE** in writing why it should not be liable for failure to submit a Full Report within the required period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.
>
> Furthermore, the Commission **GRANTS** the request for Postponement of Notification to Data Subjects of E-Science Corporation and directs them to submit proof of compliance thereof within fifteen (15) days from submission of their Full Breach Report. Pending their verification of the full list of affected data subjects, E- Science Corporation is enjoined to use alternative means of notification under Section 18(d) of NPC Circular No. 16- 03.

However, instead of submitting a proof of compliance on the required Notification to Data Subjects, E-Science submitted a Request for Exemption to Notify the Data Subjects.[3] Citing Section 11 of NPC Circular 16-03, it contended that after full investigation, it has confirmed that the incident was only limited to names, e-mail

---

[1] Exemption Request to Notify the Data Subjects for NPC BN 20-124 submitted by E-Science Corporation dated 18 August 2020.

[2] Resolution dated 6 August 2020, *In re: E-Science Corporation*, NPC BN 20-124.

[3] *Supra* note 1.

addresses and testing logs. It claimed that no sensitive, personal or biometric data were involved. It also found that there was no PIN, password, birthday, account number, telephone number, or any data involved that could put the individual at risk.[4]

E-Science also stated that it has undertaken subsequent measures to ensure that the risk of harm or negative consequence to the data subjects will not materialize.[5]

Discussion

This Commission denies E-Science's Request for Exemption to Notify the Data Subjects.

Section 11 of NPC Circular 16-03 provides that:

> Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:
>
> A. **The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.** For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> B. **There is reason to believe that the information may have been acquired by an unauthorized person**; and
>
> C. **The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.**[6]

In its Request for Exemption to Notify the Data Subjects,[7] E-Science has stated that after its full investigation, it has confirmed that only names, e-mail addresses and testing logs were involved in the subject breach incident.

---

[4] *Ibid.*
[5] *Ibid.*
[6] Emphasis supplied.
[7] *Supra* note 1.

This Commission takes this opportunity to stress that information that may be used to enable identity fraud under Section 11 (A) is not limited to the categories of information listed therein, such as data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

Contrary to Respondent's claim, names and e-mail addresses are information that may be used to enable identity fraud. An e-mail address is considered personal information and an unauthorized acquisition thereof could easily trace the identity of the data subject through the conduct of *"Phishing"* attacks to obtain more information about the user which would then be used to access important accounts resulting to identity theft and financial loss.[8]

Republic Act No. 10175, otherwise known as the *Cybercrime Prevention Act* of 2012, provides that computer-related identity theft is a cybercrime offense. Section 4(b)(3) thereof states that:

> **Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right**: Provided, That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.[9]

In the case of *Disini, et al. v. Secretary of Justice, et. al.,*[10] the Supreme Court recognized that the use of identifying information regarding a person could perpetrate the commission of identity theft. The Court had this to say on the crime of Identity Theft:

> The usual identifying information regarding a person includes his name, his citizenship, his residence address, his contact number, his place and date of birth, the name of his spouse if any, his occupation, and similar data. **The law punishes those who acquire or use such identifying information without right, implicitly to cause damage.**

---

[8] *What is Phishing?* Accessed from https://www.phishing.org/what-is-phishing, last September 11, 2020.

[9] Emphasis supplied.

[10] GR No. 203335, February 11, 2014.

Theft of identity information must be intended for an illegitimate purpose.[11]

In this case, since names, e-mail addresses and testing logs were confirmed to be involved, identity theft could therefore be committed using those information.

Aside from this, determining whether the compromised information may enable identity fraud requires a consideration of circumstances other than the nature of the personal information, such as the manner of disclosure and to whom the information was disclosed. In this case, the names and email addresses of its data subjects were not just disclosed accidentally but taken intentionally. In both its Initial Report[12] and Full-Breach Report,[13] E-Science reported that a hacker was able to access one of its online databases and a ransomware was implanted therein. It recognized that one of the likely consequences of the incident is that the hacker may contact the data subjects directly and send them malicious e-mails. Such reported circumstances surrounding the security incident gives rise to a real risk of serious harm to any affected data subject, such as the commission of identity theft through *Phishing* activities.[14]

Another justification relied upon by E-Science in its Request for Exemption to Notify the Data Subjects is that it has undertaken subsequent measures to ensure that the risk of harm or negative consequence to the data subjects will not materialize. The Commission notes, however, that the measures it has undertaken[15] do not address the abovementioned risks that *Phishing* activities may pose to its data subjects. Such risks may only be addressed through the prompt notification of the affected data subjects regarding the circumstances of the breach so that they can take the necessary precautions.

In view of the foregoing and having met all the conditions for mandatory breach notification under Section 11 of NPC Circular 16- 03, E-Science should have promptly notified the affected data subjects the moment it has confirmed that the names, e-mail addresses and testing logs of the affected data subjects were indeed

---

[11] Emphasis supplied.
[12] Initial Breach Report dated 2 July 2020.
[13] Full Breach Report dated 18 August 2020.
[14] *Ibid.*
[15] See, Initial Breach Report dated 2 July 2020 and Full Breach Report dated 18 August 2020.

involved in the subject breach incident. Its contention that no sensitive, personal or biometric data were involved, or its finding that there was no PIN, password, birthday, account number, telephone number, or any data involved which could put the individual at risk, is of no merit. Its mere confirmation that names, e-mail addresses and testing logs of the data subjects were involved in the breach incident, and the fact that the same was caused by a hacker, are sufficient to require E-Science to notify the affected data subjects. Further, E-Science cannot renege on its obligation to notify the data subjects by simply stating that no sensitive personal information was involved in the data breach incident when it has, at the onset, recognized that there was a need for such notification when it reported the likelihood that the hacker may directly contact and provide malicious e-mails to the affected data subjects. This recognition of the risks posed to its data subjects should have already been enough to move E-Science to immediately notify its data subjects.

Lastly, this Commission granted the Request for Postponement of E-Science on the premise that it will have to conduct further investigation in order to prevent sending the notification to unaffected data subjects. Thus, considering that it has already completed its full investigation on the incident, E-Science should now be prepared to proceed with the required notification of the data subjects without further delay.

WHEREFORE, premises considered, the Request for Exemption to Notify the Data Subjects of E-Science Corporation is hereby **DENIED**. E-Science Corporation is **ORDERED** to submit proof of compliance on the Notification of the Data Subjects within five (5) days from receipt of this Resolution

SO ORDERED.

Pasay City, Philippines
10 September 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JYP
Data Protection Officer
E-Science Corporation

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: PJ LHUILLIER INCORPORATED **NPC BN 19-002**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is PJ Lhuillier Incorporated's (PJLI) breach notification and management in compliance with NPC Circular 16-03 (Personal Data Breach Management).

Facts

On 18 January 2019, PJLI reported a confidentiality breach involving its email marketing tool platform server.[1] PJLI stated that the server is used to send marketing emails to a subset of its clients and operates on an isolated network with its own ISP connection.[2]

According to PJLI, on 10 January 2019, an employee received a spam email and alerted PJLI's Information Security Department.[3] On the same date, PJLI discovered that the spam email had been sent using their Email Marketing Tool Platform.[4]

PJLI initially reported the breach as a series of spam emails, but further investigation traced them back to the email blast server.[5] The investigation allegedly revealed that "a non-standard email blast campaign job has been defined."[6] An Incident Response (IR) investigation subsequently identified a vulnerability in the web

---

[1] Initial Report, 18 January 2019, at 1, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).
[2] *Id.*
[3] Supporting Details June 2021 Updates for NPC, 18 June 2021, at 1, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[4] *Id.*
[5] Initial Report, 18 January 2019, at 1, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).
[6] *Id.*

application used for email blasts, which PJLI claims was exploited to gain unauthorized access to the server.[7]

The IR team conducted an examination of the server logs to check for other potential malicious activities exploiting the same vulnerability.[8] Based on its findings, in addition to the server being used to send spam emails, there were unauthorized attempts to export recipient lists from an undetermined number of contact lists.[9]

PJLI reported that the extent of exposed "Personally Identifiable Information (PII)" varies.[10] Some campaigns allegedly involved only the exposure of email addresses or mobile numbers, while others potentially included information such as names, birthdates, and income details.[11]

In response to the breach, PJLI claimed that it took the following steps:

(1) Removed the server from the network;

(2) Engaged a third-party for an IR investigation and validation of internal results;

(3) Revisited the regular vulnerability scans performed on the server, noting that the CVE used was not detected in previous scans;

(4) Continued the process of de-duplicating records; and

(5) Prepared notifications for affected data subjects.[12]

On 23 January 2019, PJLI submitted a supplemental report with the subject, "Data Breach Notification - Email Marketing Tool Platform Web App Report."[13] In the report, PJLI reiterated that the breach involved the exploitation of a vulnerability within the Interspire Email Marketing Web Application.[14] This vulnerability allegedly allowed unauthorized parties to bypass authentication of the web application, gain access to, and subsequently download recipient mailing lists originally compiled for marketing email campaigns.[15]

---

[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Initial Report, 18 January 2019, at 1, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).
[12] *Id.*
[13] Supplemental Report, 23 January 2019, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).
[14] *Id.* at 1.
[15] *Id.*

PJLI reiterated that the investigation suggests that the compromised "personally identifiable information (PII)" may include the following:
(a) Email addresses; (b) Full names; (c) Birthdates; (d) Mobile numbers; and (e) Income ranges.[16]

PJLI claimed that it immediately disconnected the system upon discovery of the breach on 15 January 2019.[17] Further, PJLI engaged Red Rock Security, a third-party Information Security firm, to assist in preparing the incident report.[18]

PJLI provided the sequence of events from the initial report of a spam email to the submission of the initial report:[19]

January 10, 2019	Report of SPAM in a foreign language. Processed as per SOP as SPAM.
January 10, 2019	Discovery that SPAM source was the departmental web application used for marketing email blasts.
January 11, 2019	System configuration was updated to prevent its use to send out relays.
January 13, 2019	Recurrence of spamming relay. Campaign used to send out spam was disabled. Contacted business units to determine who created the campaign.
January 14, 2019	Changed password of account of server.
January 15, 2019	• Relaying persisted. Called in 3rd Party IR assistance to review collected evidence and initial internal investigation. • Confirmation of exploit used to send relay. Algerian IP 105.111.116.105 connected via Bing.com. This was then followed by a connection from AWS Germany 35.157.92.39 which loaded the spamming campaign. • Compromised Web application was immediately shut down. • Conducted log analysis to see if there were other activities aside from the relaying incident.
January 15, 2019	Confirmation of unauthorized downloads.

[16] *Id.*
[17] *Id.*
[18] Compliance, 18 June 2021, *Supporting Details June 2021 Updates for NPC*, in In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[19] Supplemental Report, 23 January 2019, at 1-2, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).

	August 5, 2018 7:03 AM 11:30 PM 144.217.241.249 Canada	August 12, 2018 7:56 PM 3:56 AM 105. 157.205.190 Morocco
	Please refer to attached 3rd Party for additional details.	
January 16, 2019	Activation of PJLI Data Breach Team / Corporate Crisis Team	
January 17, 2019	Reported to PJLI Management Committee and Board of Directors	
January 18, 2019	Initial meeting with the NPC to discuss the incident and ask for guidance regarding the next steps.	
January 18, 2019	Submission of initial report. Start of client notification-related activities. Sourced out email marketing tool after NPC meeting since our email marketing web app was disabled.	

PJLI initially claimed that according to the investigation, a total of nine hundred thirteen thousand three hundred seventy-one (913,371) data subjects were possibly affected.[20] PJLI alleged that the compromised "contact lists can be commoditized and sold [to be used] for malicious activities such as spam campaigns, phishing attacks, and similar threats."[21]

PJLI claimed that it took several measures to address the incident.[22] The email marketing web application involved was removed from the network, and logs were reviewed to identify other indicators of compromise to make sure that the incident was limited to the web application.[23]

To secure or recover the compromised personal data, PJLI stated that it "notified possibly affected data subjects" and "provided reminders on how to minimize [the risks of] password guessing attacks, phishing, and the likes."[24] Additionally, PJLI alleged that it has taken steps to mitigate possible harm and limit the damage and distress to those affected by the incident by providing contact details for feedback or

---

[20] *Id.* at 2.
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*

inquiries and confirming that the incident was isolated to the email marketing web app with no transactional data exposed.[25]

To prevent a recurrence of the incident, PJLI states that it has discontinued the use of the email marketing web app and permanently removed it from their list of solutions.[26] It also engaged a third party to perform an independent vulnerability assessment to validate internal test results conducted regularly.[27] Further, PJLI reported the Common Vulnerabilities and Exposures (CVE) System used in the exploit to the Pen Testing Tool provider to ensure it can be detected in future versions.[28] It also claimed that it "[a]ugment[ed] existing information security controls by implementing a security operations center" and "deploying a Security Analytics and Intelligence solution to further improve proactive responses to security attacks as per their approved 2019 plans."[29]

On 10 May 2021, the NPC, through the Complaints and Investigation Division (CID), directed PJLI to submit additional details on the incident within fifteen (15) days from the receipt of the Order.[30] The CID instructed PJLI to submit the following:

> a. A copy of the notification to the affected data subjects, as well as the manner of sending the same and proof of receipt thereof;
>
> b. Proof of actions taken to mitigate the harm or negative consequences and limit the damage and distress of the affected data subjects;
>
> c. Full Investigation Report of the Company resulting from its own internal investigation on the breach incident;
>
> d. Detailed Investigation Report of the third-party service provider;
>
> e. Results of the vulnerability assessments and penetration tests conducted by third-party service providers;
>
> f. Results of the vulnerability assessments/scans and penetration tests conducted by the Company; and

---

[25] Supplemental Report, 23 January 2019, at 2, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).
[26] *Id.*
[27] *Id.* at 3.
[28] *Id.*
[29] *Id.*
[30] Order, 10 May 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).

g. Network diagram/Topography at the time of the incident.[31]

On 18 June 2021, PJLI submitted its Compliance which included a Response to the Order dated 10 May 2021, and annexes containing the details of the incident as directed by the CID.[32] In contrast to its initial submissions, PJLI reported in its Compliance report that the number of affected data subjects totaled 912,015.[33]

PJLI included an incident report[34] and a 3rd Party Host Analysis Report of the incident[35] in its Compliance. PJLI stated that they use the Interspire Email Marketer version 6.1.2, which they installed on 22 July 2014, as their email marketing tool.[36] A vulnerability identified in this email marketing tool, titled "CVE-2017-14322," allows remote attackers to bypass authentication and gain administrative access.[37] This issue affects versions of Interspire Email Marketer prior to 6.1.6.[38]

As part of its Compliance, PJLI also submitted a copy of the notification template sent to the affected data subjects:

> Dear Valued Client,
>
> We are writing to inform you of a security incident which may have affected your personal data stored in one of our email marketing tool servers.
>
> On January 15, 2019, we detected attempts to use one of our email servers as a relay to send out spam to other domains. Follow-up investigation resulted in the discovery of unauthorized downloading of contact lists used as recipients for email campaigns. These unauthorized downloads took place on August 5, 8, and 12, 2018. Your personal information (name, birth date, email address, mobile number and in some cases, income information) may have been exposed in this incident. Upon discovery, remedial actions were taken to reduce the harm. The server was immediately disconnected from the network after confirmation of breach. The incident was likewise reported to the National Privacy Commission.

---

[31] *Id.* at 2.
[32] Compliance, 18 June 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[33] *Id. PJLI response to NPC 19 002 Received June 4 2021.*
[34] *Id. IR011-011019 Report.*
[35] *Id. 3rd Party Incident Review Report.*
[36] *Id.*
[37] Technical Report, 30 June 2021, at 1, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[38] *Id.*

> We value your patronage and respect the privacy of your personal information, and we are committed in our role in keeping your personal data safe and secure. As a precautionary measure, please observe the following steps in order to fully protect your user information:
>
> - Immediately change the passwords of all user accounts in which personal information details or portions of it are used as passwords.
> - Do not use the same password across multiple accounts. Use strong passwords. Change passwords regularly.
> - Regularly check your accounts for suspicious transactions.
> - Take advantage of available two-factor authentication features of applications that you use. For example. you can configure your account to require a one-time passcode (sent to your phone or other email) in addition to your password before you can access.
> - Be very cautious about providing personal information which will require you to click on links or download attachments contained in email, SMS or private messages. Take time to validate these requests for personal information through other communications channels (e.g. contact numbers in billing notices) with your online services providers.
>
> For any inquiries, please contact our Data Protection Officer thru the email emailprivacy@pjlhuillier.com or SMS only numbers 09188122737 or 09178122737. We will do our best to provide feedback to you as soon as possible.
>
> We undertake to provide more information to you as soon as they become available.[39]

Additionally, PJLI submitted the results of an internal vulnerability assessment test covering the affected server, [40] as well as a network diagram depicting the state of the network at the time of the incident.[41] PJLI has also provided evidence of the implementation of both organizational[42] and technical measures[43] within the organization.

As to PJLI's organizational measures, it attached proof that it observes Privacy Awareness Week (PAW) and Information Security Month.[44] PJLI also hosted activities such as "Defend the Flag" competitions in order to improve the skills of its information security team and "Catch

---

[39] Compliance, 18 June 2021, *Notification to Affected Data Subjects*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[40] *Id. IR011-011019 Report.*
[41] *Id. Network Diagram During Time of Incident.*
[42] *Id. Proof of Implementation – Organizational.*
[43] *Id. Proof of Implementation – Technical.*
[44] *Id. Proof of Implementation – Organizational.*

the Phish Quiz/Test" which aims to educate employees about phishing threats and how to identify them.[45]

PJLI also included proof of its technical measures.[46] It has a Host-based Intrusion Protection System (HIPS)[47] that analyzes detailed activities on monitored hosts, identifying malicious processes or users and accessing data files and system processes to monitor attack outcomes.[48]

PJLI also uses a Security Information and Event Management (SIEM) system[49] to collect, categorize, and analyze log and event data from applications, security devices, and host systems, generating alerts and threat levels based on predefined rules.[50] Additionally, Honeypot monitoring is in place,[51] using deception technology to lure cybercriminals into exploiting vulnerabilities, allowing the security team to study attacker behaviors and improve security policies.[52]

Moreover, PJLI employs Akamai Enterprise Threat Protector,[53] a cloud-based secure web gateway, later transitioned to Cloudflare in 2020,[54] ensuring safe internet connections for users and devices.[55] It also has a Sophos Web Appliance[56] to block web threats at the source, enforce acceptable use policies, and safeguard against data loss.[57] PJLI also has Imperva Database Firewall,[58] a database firewall that monitors databases to protect against attacks targeting sensitive information.[59] In 2020, PJLI installed anti-exploit/ransomware software,[60] adding an extra layer of security by blocking attacker techniques, including new

---

[45] Compliance, 18 June 2021, *Proof of Implementation - Organizational*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[46] *Id. Proof of Implementation – Technical.*
[47] *Id. Proof of controls prior to incident.*
[48] Technical Report, 30 June 2021, at 2, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[49] Compliance, 18 June 2021, at *Proof of controls prior to incident*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[50] Technical Report, 30 June 2021, at 2, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[51] Compliance, 18 June 2021, *Proof of controls prior to incident*, *in* In re: PJ Lhuillier, Inc., NPC BN 19- 002 (NPC 2021).
[52] Technical Report, 30 June 2021, at 2, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[53] Compliance, 18 June 2021, *Proof of controls prior to incident*, *in* In re: PJ Lhuillier, Inc., NPC BN 19- 002 (NPC 2021).
[54] *Id. Proof of Implementation – Technical.*
[55] Technical Report, 30 June 2021, at 3, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[56] Compliance, 18 June 2021, *Proof of controls prior to incident*, *in* In re: PJ Lhuillier, Inc., NPC BN 19- 002 (NPC 2021).
[57] Technical Report, 30 June 2021, at 3, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[58] Compliance, 18 June 2021, *Proof of Implementation - Technical*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[59] Technical Report, 30 June 2021, at 3, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[60] Compliance, 18 June 2021, *Proof of Implementation - Technical*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).

exploits and ransomware that threaten to block access to data unless a ransom is paid.[61]

On 24 September 2021, the CID directed PJLI to clarify the following statements made by the latter in its submissions:

> 1. At the time of the contract with Web Solutions Inc, the latest version of Interspire Email Marketer available is version 6.1.4, Why did PJLI chose the prior version of 6.1.2?
>
> 2. As to the number of affected data subjects, clarify the breakdown of the nine hundred twelve thousand and fifteen (912,015).
>
> 3. On 10 lanuary 2019, PJLI updated its CLAM AV. When was the last update of Clam AV prior to this date, as well as the frequency of updates?
>
> 4. The vulnerability assessment was noted to have a change as to frequency, what brought about the change?
>
> 5. Upon investigation, what caused the non-detection of the published vulnerability?
>
> 6. Attach proof of receipt/ sending of the notification to the data subjects[62]

On 29 September 2021 PJLI submitted its response.[63] It claimed that at the time of deployment, its vendor recommended version 6.1.2 of Interspire Email Marketer as the stated and stable version.[64] PJLI also attached a breakdown of the 912,015 affected data subjects:[65]

912,015	Represents master list of recipients for email notifications. Since investigation was still ongoing at this point, PJLI decided to notify all clients in its email database list to ensure that we can comply with the prescribed notification deadline of within 72 hours.
10,697	Represents subset of records created after August 13 which was after the reported breach.

---

[61] Technical Report, 30 June 2021, at 3, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[62] Additional Questions from CID, 24 September 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[63] PJLI Response dated 29 September 2021, 29 September 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[64] *Id.* at 1.
[65] *Id.*

901, 318	Represents records which were possibly included in the breach
121,059	Hard bounced emails as reported by mailchimp.com
780,259	Emails not included in the hard bounced list which means they were notified accordingly
Breakdown using email address as the main identifier	
260,190	number of records containing email details only
1,761	number of records containing email and name details only
70,171	number of records containing email, name, and bday
71,485	number of records containing email, name, bday and possibly other PIIs such as of age, gender, educational attainment, civil status or income bracket value estimates
377,495	number of records containing email, and possibly other PIIs such as of age, gender, educational attainment, civil status or income bracket value estimates

As part of its response, PJLI included an Email Campaign Report as proof of sending the notification to the affected data subjects:[66]

Email Campaign Report	
Title:	Privacy Notice
Subject Line:	Notice from Cebuana Lhuillier Data Privacy Officer
Delivery Date/Time:	Sat, Jan 19, 2019 8:00 am
Overall Stats	
Total Recipients:	912,015
Successful Deliveries:	787,335
Bounces:	124,680 (13.7%)
Recipients Who Opened:	119,635 (15.2%)
Total Opens:	177,468
Last Open Date:	6/16/21 9:33AM
Total Unsubs:	1,062

On 1 October 2021, the CID directed PJLI to clarify the number of affected data subjects.[67] The CID noted that nine hundred one thousand three hundred eighteen (901,318) records were compromised.[68] There, however, was a discrepancy of one hundred

[66] *Id.* at 2.
[67] Order, 01 October 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[68] *Id.*

twenty thousand two hundred sixteen (120,216) records in the breakdown of compromised personal data.[69] Thus, CID directed PJLI to clarify the specific personal data compromised for the one hundred twenty thousand two hundred sixteen (120,216) data subjects identified in the discrepancy.[70]

The CID also observed that one hundred twenty-four thousand six hundred eighty (124,680) notifications to affected data subjects bounced, meaning those individuals did not receive the notification.[71] Since not only email addresses but other personal data were compromised, the CID requested details on how PJLI notified these data subjects and the specific personal data compromised.[72]

PJLI clarified that there was a line item that was mistakenly omitted in the breakdown included in their previous submission.[73] Thus, PJLI attached an updated breakdown of affected data subjects:[74]

901,318	Total records on or before 13 August 2018
BREAKDOWN	
260,190	Email Only
1,761	Email and name
70,171	Email, name and birthday
71,485	Email, name, birthday and other PIIs such as the age, gender, mobile number, educational attainment, civil status and income bracket values
377,495	Email and other PIIs such as the age, gender, mobile number, educational attainment, civil status and income bracket values
120,216	Email and other PIIs possibly with Age, Town, City, Civil Status, Gender, NumChild, Education, House, source fund

For the one hundred twenty-four thousand six hundred eighty (124,680) data subjects whose notifications bounced, PJLI indicated that there were no other means of notification because there were no mobile numbers or complete addresses available for use.[75] Regarding the specific personal data compromised, PJLI claimed that thirteen

[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] PJLI Response dated 06 October 2021, at 1, 06 October 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[74] *Id.*
[75] *Id.*

thousand six hundred eight (13,608) involved only email addresses while one hundred eleven thousand seventy-two (111,072) included email addresses, age, town, city, civil status, gender, number of children, education, house, and source of funds.[76]

Issue

Whether PJLI notified its affected data subjects, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. PJLI's submissions show that it properly notified its affected data subjects, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

It is the obligation of a Personal Information Controller (PIC), such as PJLI, to ensure that affected data subjects of the breach are promptly and properly notified.[77] The Commission has consistently emphasized that the purpose of the required notification to the data subjects of a breach is to allow them to take the necessary precautions or other measures to protect themselves against its possible effects.[78]

Section 18 of NPC Circular 16-03 provides the requirements as to the content and form of the notification of data subjects:

> Section 18. *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> C. *Content of Notification*. The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;

---

[76] *Id.*
[77] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).
[78] NPC Circ. No. 16-03, § 18 (A).

4. measures taken to reduce the harm or negative consequences of the breach;
5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. any assistance to be provided to the affected data subjects.

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.

D. *Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.

The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[79]

In this case, PJLI notified the affected data subjects about the security incident through a letter sent by email.[80]

PJLI identified the nature of the breach by informing the recipients of a security incident involving unauthorized attempts to use their email server to send spam and unauthorized downloading of contact lists.[81] This fulfilled the requirement to describe the nature of the breach. [82]

---

[79] NPC Circ. No. 16-03, § 18 (C) & (D).
[80] Compliance, 18 June 2021, *Notification to Affected Data Subjects*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[81] *Id.*
[82] NPC Circ. No. 16-03, § 18 (C).

The notification specified the types of personal data that may have been exposed, including name, birth date, email address, mobile number, and, in some cases, income information.[83]

The notification also outlined the immediate actions taken to address the breach, such as disconnecting the affected server from the network and reporting the incident to the National Privacy Commission.[84] Additionally, the notification described the steps PJLI took to reduce harm, including server disconnection and actions to prevent further unauthorized access.[85]

PJLI provided the Data Protection Officer's (DPO) contact information, including an email address and phone numbers, allowing data subjects to obtain additional information regarding the breach.[86] This satisfied the requirement to include contact information of a representative from whom more information could be obtained.[87] The notification also included practical advice for data subjects to protect their information, such as changing passwords, using strong passwords, enabling two-factor authentication, and being cautious about phishing attempts.[88]

In addition, PJLI took measures to sufficiently address the breach and adopted measures to prevent its recurrence.

Section 20 of the DPA provides that PICs must implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any unlawful disclosure:

> Section 20. *Security of Personal Information.* (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any

---

[83] Compliance, 18 June 2021, *Notification to Affected Data Subjects*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] NPC Circ. No. 16-03, § 18 (C).
[88] Compliance, 18 June 2021, *Notification to Affected Data Subjects*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).

> accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[89]

As part of its organizational measures, PJLI took several significant steps to ensure data protection and security. PJLI designated a DPO whose name and business contact information are registered with the NPC. Further, PJLI established a Data Breach Management and Corporate Crisis Team.

Additionally, PJLI engaged in various activities to bolster its data security practices. It participated in and hosted a "Defend the Flag" competition designed to enhance the skills of its information security team by simulating real-world cyber-attack scenarios.[90] PJLI developed the "Catch the Phish Quiz/Test," an initiative aimed at educating employees about phishing threats and how to identify and avoid them.[91]

Moreover, PJLI's Information and Communication Technology (ICT) service provider, Networld Capital Ventures Incorporated (NCVI), is certified to be compliant with the requirements of ISO 27001:2013, a globally recognized standard for information security management systems.

As to its technical security measures, PJLI employed multiple vulnerability assessment and penetration test providers to ensure comprehensive detection and mitigation of all potential vulnerabilities in their system. This includes a Host-based Intrusion Protection System (HIPS) to monitor host activities and identify malicious processes,[92] and a Security Information and Event Management (SIEM) system to analyze log data and generate alerts based on predefined rules.[93] PJLI also uses Honeypot monitoring to study attacker behaviors,[94] Akamai Enterprise Threat Protector (transitioned to Cloudflare in 2020) for secure web connections,[95] and a Sophos Web

---

[89] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (a) (2012).
[90] Compliance, 18 June 2021, *Proof of Implementation - Organizational*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[91] *Id.*
[92] *Id. Proof of controls prior to incident.*
[93] *Id.*
[94] *Id.*
[95] *Id.*

Appliance to block web threats and enforce acceptable use policies.[96] Additionally, they employ the Imperva Database Firewall to protect databases[97] and have installed anti-exploit/ransomware software to block new exploits and ransomware threats.[98]

Given the foregoing, the Commission finds that the measures undertaken by PJLI have sufficiently addressed the incident and prevented its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 19-002 In re: PJ Lhuillier Incorporated is **CLOSED**.

SO ORDERED.

City of Pasay, Philippines. 16 May 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

---

[96] Compliance, 18 June 2021, *Proof of controls prior to incident*, *in* In re: PJ Lhuillier, Inc., NPC BN 19- 002 (NPC 2021).
[97] *Id. Proof of Implementation – Technical.*
[98] Technical Report, 30 June 2021, at 3, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).

Copy furnished:

APM
Data Protection Officer
PJ Lhuillier Incorporated

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: OFFICE WAREHOUSE INC. **NPC BN 18-144**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is a breach notification submitted by Office Warehouse, Inc. (OWI) involving the inadvertent disclosure of email addresses of its CLP Points Plus+ Cardholders.

Facts

On 02 August 2018, OWI notified the National Privacy Commission (NPC) of a breach:

> This is to report a data breach involving approximately 1,900 email addresses of customers of Office Warehouse, Inc. (the "Company.")
>
> The incident happened when one of the staff of the Company unintentionally sent an email message to its customers without hiding, thus, exposing the email address of a certain customers to more or less 50 other customers. The delivery of email message was made per batch to at least 50 email users. The management was informed of the incident on July 30, 2018 at about 7:30 pm. The personal information involved in the incident are only email addresses.
>
> We are conducting further investigation on this incident and we will inform the Commission of the results thereof[.][1]

On 26 October 2020, the NPC, through its Complaints and Investigation Division (CID), issued an Order directing OWI to submit a Full Report within fifteen (15) days from receipt.[2]

---

[1] Personal Data Breach Notification from Office Warehouse, Inc., 02 August 2018, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2018).
[2] Order, 26 October 2020, at 1-2, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).

On 13 November 2020, OWI submitted its compliance[3] and a copy of the emails that exposed its customers' email addresses.[4]

OWI reiterated substantially the same narration it provided in its initial notification. On 27 July 2018, OWI sent a marketing email to approximately one thousand nine hundred (1,900) customers' email addresses to remind them of the "Office Warehouse CLP Privacy Policy."[5] The emails were sent to CLP Points Plus+ Cardholders in thirty-seven (37) batches.[6] OWI's staff, however, claimed that it "unintentionally" sent the emails without using the blind carbon copy (BCC) function and exposed the email addresses of at least fifty (50) cardholders to other recipients of the same email.[7]

OWI stated that the email content did not involve information "that may lead to the identification of its members."[8] OWI added that "[t]he event was caused by a [sic] human error by one of [its] staff and [OWI] sent an apology letter to those recipients who responded via [] and [] email."[9]

On measures implemented to address the breach, OWI reported that it sent an apology letter to those recipients who responded to their marketing email.[10] OWI also stated that it reported and discussed the breach incident with its Data Protection Officer (DPO) and the OWI management.[11]

OWI also reported that it recalled all the emails sent without using the BCC function on 30 July 2018.[12] It identified that some of the emails were not successfully sent because (1) the email bounced back (Mailer Daemon), as the email inbox is full, the email address does not exist, or the email server is unavailable;[13] (2) the email was blocked by

---

[3] Data Breach Report Form, 13 November 2020, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[4] Data Breach Report Form, 13 November 2020, Email List_CLP Jul 2018, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[5] *Id.* at 1.
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] Data Breach Report Form, 13 November 2020, at 2, *in* In re: Office Warehouse, Inc., NPC BN 18- 144 (NPC 2020).
[11] *Id.*
[12] *Id.*
[13] *Id.*

Google, Yahoo and Global spam filters;[14] or (3) the email was deleted on the server due to queue status.[15] Thus, it reviewed emails in the deferred queue of Office Warehouse's server, checked "Global spam filters" of Gmail, Yahoo, and other mail addresses, and identified the number of active email addresses to whom the email was successfully sent.[16] Finally, OWI reported it "[r]eplied to the affected email recipient[s] to get updates on the action taken."[17]

On 24 September 2021, the CID directed OWI to submit additional information on the actions it reported to have been taken within five
(5) days from receipt of the directive.[18] Specifically, the CID required the following:

1. A Full Investigation Report containing a description on the breach, its discovery, and root causes;[19]
2. Details of the incident response team's actions and decisions, specifically if certain emails were deleted, proof of deletion, if any, and the rationale behind such actions;[20]
3. The outcomes of breach management and any difficulties, including: the status of the recalled emails, review of emails in the deferred queue of OWI's server, check on global spam filters, identification of active email addresses involved, and updates provided to the affected email recipients;[21]
4. Compliance with notification requirements, including clarification on the number of affected data subjects, copies of the notification sent, proof of notification, copies of the apology letter to those recipients who responded to the original email, and proof of assistance provided to the data subjects;[22] and
5. Measures implemented post-incident to prevent future breaches, including updates to policies, employee training, and proof of these actions.[23]

On 22 October 2021, OWI submitted its compliance with supporting documents.[24]

---

[14] *Id.*
[15] *Id.*
[16] Data Breach Report Form, 13 November 2020, at 2, *in* In re: Office Warehouse, Inc., NPC BN 18- 144 (NPC 2020).
[17] *Id.*
[18] Complaints and Investigation Division Email, 13 November 2020, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] Compliance, 22 October 2021, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2021).

OWI re-submitted its Data Breach Report Form dated 13 November 2020 to comply with the CID's directive to submit a Full Investigation Report.[25] OWI also stated that its Information Technology (IT) Team worked with its Marketing Staff "for email callback to reduce the bulk email sending that has been successfully done."[26]

OWI also submitted a breakdown of the number of recipients per email batch,[27] a copy of one of the emails sent without using the BCC function,[28] and a copy of the apology emails sent to the four (4) recipients who called out the incident.[29]

In response to one of the customers who emailed to point out OWI's failure to use the BCC function, OWI stated:

> Hello [OWI customer],
>
> Office Warehouse data privacy team, values your privacy and deeply regrets that this incident occurred. Our team has taken immediate actions to address your concern. Rest assured that the security and privacy of your personal data is of an utmost important to us and we are continually improving our systems and business processes to better serve you.
>
> Thank you for your understanding.
>
> Sincerely,
> Data Privacy Team
> Office Warehouse,
> Inc.[30]

OWI sent a similar response to the three (3) other recipients who pointed out the incident.[31] OWI assured them that it took immediate actions to address the incident and offered assistance for any other concerns.[32]

---

[25] *Id.* Annex 1.
[26] *Id.*
[27] *Id.* Annex 2.
[28] *Id.* Annex 3
[29] *Id.* Annex 4-5.
[30] Compliance, 22 October 2021, Annex 4, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2021).
[31] *Id.* Annex 5.
[32] *Id.*

OWI also explained in its compliance that it merely stated that it sent an apology to its data subjects and claimed the data subjects did not request further help.[33]

OWI submitted copies of the following: an internal memorandum reminding its employees on Email Policy and Etiquette (with translations in both English and Filipino),[34] its Privacy Awareness training material,[35] and its Email Etiquette Training slides presented during a Data Privacy Orientation conducted in 2018 for employees.[36]

On 25 January 2022, OWI resubmitted its compliance dated 22 October 2021.[37]

Issue

Whether OWI sufficiently addressed the breach and implemented security measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. The incident does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03 (Personal Data Breach Management). Nevertheless, OWI sufficiently addressed the breach and implemented security measures to prevent its recurrence.

Section 11 of NPC Circular 16-03 on mandatory breach notification provides:

> Section 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include,

---

[33] Compliance, 22 October 2021, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2021).
[34] *Id.* Annex 6.
[35] *Id.* Annex 7.
[36] *Id.* Annex 8.
[37] Email Re: NPCBN 18-144, 25 January 2022, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2022).

but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

B. There is reason to believe that the information may have been acquired by an unauthorized person; and

C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[38]

Following this, the requisites for mandatory breach notification to the Commission are:

1. The breach involves sensitive personal information, or information that may, under the circumstances, be used to enable identity fraud;[39]
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[40]

The first requisite is absent in this case. The nature of the information involved is neither sensitive personal information nor other information that, under the circumstances, may enable identity fraud.

The first requisite of mandatory breach notification under Section 11 of NPC Circular 16-03 should be read together with Section 20 (f) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA). Section 20 (f) expressly requires the consideration of the specific circumstances of a breach in determining whether other information involved in the breach may enable identity fraud:

> Section 20. *Security of Personal Information.*
>
> . . .

---

[38] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).

[39] NPC BN 18-158, 13 November 2023, at 10 (NPC 2023) (unreported).

[40] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does Initiated as a Sua Sponte NPC Investigation on Possible Data Privacy Violations Committed in Relation to the Alleged Hack and Breach of the Commission on Elections System or Servers, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-SS-22-001-and-NPC-SS-22- 008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 31 January 2024).

> (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or **other information that may, under the circumstances, be used to enable identity fraud** are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.[41]

The Commission previously held that a data subject's name and email may be considered under other information that may enable identity fraud.[42] The Commission explained:

> This Commission takes this opportunity to stress that information that may be used to enable identity fraud under Section 11 (A) is not limited to the categories of information listed therein, such as data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> **Contrary to Respondent's claim, names and e-mail addresses are information that may be used to enable identity fraud. An e-mail address is considered personal information and an unauthorized acquisition thereof could easily trace the identity of the data subject through the conduct of "Phishing" attacks to obtain more information about the user which would then be used to access important accounts resulting to identity theft and financial loss.**[43]

In that case, the Commission, after considering the circumstances, determined that the names and email addresses of the data subjects are information that may be used to enable identity fraud.[44] The PIC

---

[41] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (f) (2012). Emphasis supplied.

[42] NPC BN 20-124, 10 September 2020, at 3 (NPC 2020) (unreported).

[43] *Id.* Emphasis supplied.

[44] *Id.* at 4.

reported that a hacker accessed and implanted ransomware in an online database.[45] Because of these particular circumstances, the Commission concluded that the hacker may contact and send malicious emails directly to the data subjects.[46]

Here, however, the inadvertent disclosure of the CLP Points Plus+ Cardholders' email addresses would not have enabled identity fraud.

In its initial report, OWI stated that "the personal information involved in the incident are only email addresses."[47] Later, in its compliance dated 13 November 2020, OWI reiterated that the email content did not involve information "that may lead to the identification of its members,"[48] and that the disclosed information was limited to email addresses only.[49] As proof, it also submitted a copy of the emails that exposed its customers' email addresses.[50]

OWI also explained in its submissions that the incident was "[c]aused by a [sic] human error by one of [its] staff"[51] when they "unintentionally" sent the emails without using the BCC function.[52]

Given the specific circumstances of this case, email addresses alone do not provide adequate means of committing identity fraud. As such, the email addresses of the data subjects cannot be considered as other information that may enable identity fraud.

The second requisite is present in this case. There was acquisition of the information by an unauthorized person.

The Commission previously held that a loss of control over personal data held in custody is enough for a personal information controller (PIC) to have "reason to believe that the information may have been acquired by an unauthorized person."[53]

---

[45] *Id.*
[46] *Id.*
[47] Personal Data Breach Notification from Office Warehouse, Inc., 02 August 2018, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2018).
[48] Data Breach Report Form, 13 November 2020, at 1, *in* In re: Office Warehouse, Inc., NPC BN 18- 144 (NPC 2020).
[49] *Id.*
[50] Data Breach Report Form, 13 November 2020, Email List_CLP Jul 2018, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2020).
[51] *Id.* at 1.
[52] *Id.*
[53] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).

In this case, OWI admitted that the marketing email was sent to thirty- seven (37) batches of CLP Points Plus+ Cardholders at a time without using the BCC function,[54] which made the other recipients' email addresses visible. Further, OWI submitted a copy of the apology emails sent to the four (4) recipients who responded to the email to point out the incident.[55] The foregoing shows that there is not just a reasonable belief but certainty that an unauthorized person acquired the information involved in the breach.[56]

The third requisite is also absent. There is no real risk of serious harm in this case.

The Commission takes this opportunity to discuss the factors considered in determining the presence of the third requisite of mandatory breach notification. Section 11 (C) of NPC Circular 16-03 provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> . . .
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[57]

For this purpose, the phrase "likely to give rise to a real risk" in Section 11 (C) means that a link exists between the breach and the possible resulting harm to any affected data subject.[58] The risk must be apparent and not the product of mere speculation.[59] Serious harm

---

[54] Data Breach Report Form, 13 November 2020, at 1, *in* In re: Office Warehouse, Inc., NPC BN 18- 144 (NPC 2020).
[55] Compliance, 22 October 2021, Annex 4-5, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2021).
[56] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).
[57] NPC Circ. No. 16-03, § 11.
[58] In re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8, available at https://privacy.gov.ph/wp-content/uploads/2024/06/NPC-BN-17-028-_-18-180- 2023.05.11-Resolution-FinalP.pdf (last accessed 30 March 2024).
[59] *Id.*

means that the consequences and effects to any affected data subject are significant based on the surrounding circumstances of the breach.[60]

In determining whether the unauthorized acquisition is likely to give rise to real risk of serious harm, a PIC or the Commission may consider several factors, such as: the nature and amount of information involved in the breach, the period of time that has lapsed since the breach, objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.[61]

In this case, the objective of the unauthorized acquisition was not for some malicious or fraudulent purpose. As previously established, the disclosure of the email addresses was due to the OWI staff's inadvertent failure to use the BCC function.[62] Further, the nature and amount of information involved was limited to the email addresses of CLP Points Plus+ Cardholders.[63] This limited information did not provide the recipients with access to other details that would enable identity fraud. Thus, further exposure or misuse of the information is unlikely.

Finally, OWI implemented sufficient security measures to address the breach and prevent its recurrence. It recalled all the emails sent without using the BCC function on 30 July 2018.[64] OWI also sent apology emails to the four (4) recipients who called out the incident[65] and offered assistance for any other concern that may arise.[66] After the breach, OWI sent out an internal memorandum to remind employees on Email Policy and Etiquette.[67] It also conducted data privacy awareness training[68] and email etiquette[69] orientation for its employees.

---

[60] *Id.*
[61] *Id.*
[62] Data Breach Report Form, 13 November 2020, at 1, *in* In re: Office Warehouse, Inc., NPC BN 18- 144 (NPC 2020).
[63] *Id.*
[64] *Id.* at 2.
[65] Compliance, 22 October 2021, Annex 4-5, *in* In re: Office Warehouse, Inc., NPC BN 18-144 (NPC 2021).
[66] *Id.* Annex 5.
[67] *Id.* Annex 6.
[68] *Id.* Annex 7.
[69] *Id.* Annex 8.

Given the foregoing factors and the remedial measures taken by OWI, the unauthorized acquisition did not give rise to a real risk of serious harm to any affected data subject. Thus, the third requisite is absent.

Considering that the first and third requisites are absent, the matter does not fall under mandatory breach notification. Nevertheless, OWI conducted proper breach management. The measures implemented by OWI are sufficient to address the breach and to prevent its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-144 In re: Office Warehouse, Inc. is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
21 March 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

NRZ
Data Protection Officer
Office Warehouse, Inc.

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: RAREJOB ENGLISH ASSESSMENT, INC. (FORMERLY GOLA ENGLISH TUTORIAL, INC.)

NPC BN 18-131

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is a breach involving unauthorized access to Google Form responses of the applicants of Rarejob English Assessment, Inc. (formerly, GOLA English Tutorial, Inc.) (REA).

Facts

On 20 July 2018, GOLA English Tutorial, Inc. (GOLA) notified the National Privacy Commission (NPC) of a breach involving personal information:

> GOLA hires tutors whose application/s are processed via Google Forms, an external party application.
>
> As a first step of our application process, we require applicants to fill out the online form via Google Forms for information pertinent to their application.
>
> Unfortunately, the privacy setting implemented for the online form allowed all applicants who completed their application to view other tutor applicants' responses.
>
> Once the tutor applicant completed filling out the online form, he /she was redirected to a page which confirmed his/her application and provided for an option to "view other responses." As such, the personal information accomplished by the other tutor applicants became viewable to other tutor applicants by clicking the "view other responses" link.[1]

---

[1] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly, GOLA English Tutorial, Inc., 27 July 2018, at 1, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).

GOLA explained that one (1) applicant was able to view the personal information of the other applicants.[2] The same applicant notified GOLA about the breach.[3] GOLA reported that there were at least two hundred forty-six (246) applicants affected.[4]

The information involved were the following: complete name, current address, mobile phone number, email address, educational attainment, and name of their school.[5] GOLA's Google Form also asked the applicant whether they had teaching experience and if so, what the name of their previous workplace was, how they found out about GOLA, and whether they were amenable to working full-time.[6]

GOLA reported that it immediately disabled the feature that allowed others to view the applicants' personal information.[7] It also stated that it would individually inform the affected applicants of the breach and the mitigating measures taken through the email address they provided.[8]

On measures to prevent recurrence of the incident, GOLA stated that it would use e-mail instead of an external third party for the tutor- application process.[9] It also stated it would "proceed with appointing a Data Protection Officer and completing [its] registration with the NPC in parallel with the completion of [GOLA's] post-incorporation requirements."[10]

On 14 February 2022, the NPC, through its Complaints and Investigation Division (CID), issued an Order directing GOLA to submit its Post-Breach Report on the incident through e-mail within fifteen (15) days from receipt.[11] The Order, which was sent via email, bounced back. [12]

---

[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.* at 1-2.
[6] *Id.*
[7] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc., 27 July 2018, at 2, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Order, 14 February 2022, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2022).
[12] Failed Delivery Email from Microsoft Outlook, 15 February 2022, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2022).

On 15 February 2023, the CID issued another Order directing GOLA, now REA, to submit a Post-Breach Report within five (5) days from receipt.[13]

On 20 February 2023, REA requested for an additional fifteen (15) days, or until 07 March 2023, to file its Post-Breach Report.[14] It clarified that the request was not intended to cause delay, but rather "it foresees its inability to comply with [the Order] within the 5-day period due to the limited mobility of its staff still presented by the COVID-19 pandemic."[15]

On 21 February 2023, the CID issued a Resolution granting REA's request for extension of time:

> In view of the abovementioned circumstances, the Commission deems it proper to afford the PIC an opportunity to comply with the Order dated 15 February 2023. Thus, in line with principle of due process and considering as the granting of such request will not prejudice the conduct of the investigation, we grant the request for extension of time.
>
> WHEREFORE, premises considered, **Rarejob English Assessment, Inc.** (formerly Gola English Tutorial, Inc.) request for an extension of time is hereby **GRANTED. Rarejob English Assessment, Inc.** (formerly Gola English Tutorial, Inc.) is given an additional period of fifteen (15) calendar days from the date of this Order, or until **07 March 2023** to submit its compliance.
>
> **SO ORDERED.**[16]

On 07 March 2023, REA submitted its Compliance.[17] REA reiterated substantially the same narration it provided in its initial notification.

In 2018, REA processed the application of tutors through Google Forms, an external party application.[18] The settings implemented for the Google Form, however, allowed all applicants who completed it to

---

[13] Order, 15 February 2023, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[14] Letter Re: Data Breach Notification filed by Rarejob English Assessment, Inc., 20 February 2023,
in In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2023).
[15] Letter Re: Data Breach Notification filed by Rarejob English Assessment, Inc., 20 February 2023, at 2, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2023).
[16] Resolution, 21 February 2023, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[17] Compliance, 07 March 2023, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[18] *Id.* at 1.

view other applicants' responses.[19] On 19 July 2018, one (1) applicant notified REA that "he was able to view the personal information of the other applicants."[20] On 20 July 2018, or the following day, REA sent its Data Breach Notification to the NPC through complaints@privacy.gov.ph.[21] REA also submitted the same to reports@privacy.gov.ph on 23 July 2018.[22] REA reported that "[t]o date, there have been no further complaints or matters arising from [the] incident."[23]

REA explained that it immediately disabled the feature that allowed the applicants to see other responses.[24] REA provided that the settings implemented "allowed only the viewing of data," and as such, "no actions were taken to recover the data."[25] REA added that an investigation was conducted, but that it was "on a purely internal basis and no physical investigation report was prepared."[26]

REA also claimed that it notified the two hundred forty-six (246) affected data subjects of the breach and mitigating measures taken through their respective e-mail addresses.[27] The e-mail notification, however, could no longer be recovered for submission "due to the deletion of the 'gola.com.ph' domain after the corporation changed its name to REA in 2021."[28] It also stated that other than notification, no additional assistance was provided to the affected data subjects "because no data was taken."[29]

To prevent the recurrence of the incident, REA reported that it shifted to the use of email correspondence in the tutor application process rather than using an external party.[30] It allowed "only one person in the relevant department to take charge of the said process."[31] REA also stated that it "called the attention of the relevant employees" and "reinforced the need to be hyper-aware of the Data Privacy Act's

---

[19] *Id.*
[20] *Id.* at 1-2.
[21] *Id.* at 2.
[22] *Id.*
[23] Compliance, 07 March 2023, at 2, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[24] *Id.*
[25] *Id.*
[26] *Id.* at 3.
[27] *Id.*
[28] *Id.*
[29] Compliance, 07 March 2023, at 3, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[30] *Id.*
[31] *Id.*

requirements."[32] Finally, it stated that it was still "in the process of appointing a suitable [DPO]."[33]

Issue

Whether the matter falls under mandatory breach notification and whether REA sufficiently addressed the breach and implemented security measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. The incident does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03 (Personal Data Breach Management). Nevertheless, REA sufficiently addressed the breach and implemented security measures to prevent its recurrence.

Section 11 of NPC Circular 16-03 on mandatory breach notification provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
> B. There is reason to believe that the information may have been acquired by an unauthorized person; and
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[34]

---

[32] *Id.*
[33] *Id.*
[34] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).

Following this, the requisites for mandatory breach notification to the Commission are:

1. The breach involves sensitive personal information, or information that may, under the circumstances, be used to enable identity fraud;[35]
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[36]

The first requisite is absent in this case. The nature of the information involved is not sensitive personal information and cannot, under the circumstances, enable identity fraud.

REA admitted that the personal data involved in the breach included, among others, the applicants' educational attainment and the name of their school.[37] Under Section 3 (l) of Republic Act No. 10173 or the Data Privacy Act (DPA), personal information about an individual's education is considered sensitive personal information.[38]

In *RCJ v. DL*, however, the Commission explained that not all information related to education should automatically be considered sensitive personal information:

> In construing Section (3) (l) of the DPA as a whole and considering the company of words in this Section, the information enumerated, which includes "education", may be used to profile an individual. Thus, to harmonize and give effect to the provision as a whole, only information about education which can profile a particular individual falls within the definition of sensitive personal information.
>
> Granular or detailed information relating to the education of an individual can be used to profile that particular individual. For

---

[35] NPC BN 18-158, 13 November 2023, at 10 (NPC 2023) (unreported).
[36] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does Initiated as a Sua Sponte NPC Investigation on Possible Data Privacy Violations Committed in Relation to the Alleged Hack and Breach of the Commission on Elections System or Servers, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://privacy.gov.ph/wp-content/uploads/2024/05/NPC-SS-22-001-and-NPC-SS-22-008- 2022.09.22-In-re-COMELEC-Decision-FinalP.pdf (last accessed 28 May 2024).
[37] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc., 27 July 2018, at 1-2, *in* In re: Rarejob English Assessment, Inc., NPC BN 18- 131 (NPC 2018).
[38] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (l) (2012).

> instance, transcript of records containing a comprehensive breakdown of a student's grades and other definitive administrative information, such as a student identification number, can be used to personally identify the student.[39]

In that case, the Commission determined that the petitioner's transcript of records, which included a detailed breakdown of his grades, was considered sensitive personal information since the information can profile him.[40] Thus, the processing in relation to the information about his education should be in accordance with Section 13 of the DPA.[41]

Here, the educational attainment and name of the school of REA's applicants are general in nature and cannot be used to profile a particular applicant or enable identity fraud. As such, it cannot be considered as sensitive personal information under Section 3 (l) of the DPA.

Further, the applicants' personal information—their name, address, mobile phone number, and name of their previous workplace—cannot be considered as other information that may, under the circumstances, be used to enable identity fraud.[42]

The first requisite of mandatory breach notification should be read together with Section 20 (f) of the DPA. Section 20 (f) expressly requires the consideration of the specific circumstances of a breach in determining whether other information involved in the breach may enable identity fraud:

> Section 20. *Security of Personal Information.*
>
> . . .
>
> (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or **other information that may, under the circumstances, be used to enable identity fraud** are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real

---

[39] RCJ v. DL, NPC BN 22-012, 10 November 2022, at 7, *available at* https://privacy.gov.ph/wp- content/uploads/2023/08/NPC-22-012-2022.11.10-RJC-v.-DL-Decision.pdf (last accessed 28 May 2024).

[40] *Id.* at 8.

[41] *Id.*

[42] NPC Circ. No. 16-03, § 11.

> risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.[43]

While the Commission previously held that a data subject's name and email may be considered under "other information that may enable identity fraud,"[44] that decision took into consideration the unique circumstances of the case. The Commission explained:

> This Commission takes this opportunity to stress that information that may be used to enable identity fraud under Section 11 (A) is not limited to the categories of information listed therein, such as data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> **Contrary to Respondent's claim, names and e-mail addresses are information that may be used to enable identity fraud. An e-mail address is considered personal information and an unauthorized acquisition thereof could easily trace the identity of the data subject through the conduct of "Phishing" attacks to obtain more information about the user which would then be used to access important accounts resulting to identity theft and financial loss.**[45]

In that case, the Commission, after considering the circumstances, determined that the names and email addresses of the data subjects are information that may be used to enable identity fraud.[46] The PIC reported that a hacker accessed and implanted ransomware in an online database.[47] Because of these circumstances, the Commission concluded that the hacker may contact and send malicious emails directly to the data subjects.[48]

---

[43] Data Privacy Act of 2012, § 20 (f). Emphasis supplied.
[44] NPC BN 20-124, 10 September 2020, at 3 (NPC 2020) (unreported).
[45] *Id.* Emphasis supplied.
[46] *Id.* at 4.
[47] *Id.*
[48] *Id.*

Here, the disclosure of the applicants' information would not have enabled identity fraud.

The applicant was able to view the other responses due to REA's inadvertent failure to turn off the "view other responses" function.[49] There is no showing that the applicant who notified REA deliberately intended to obtain the other applicants' information, as he was the one who reported the incident to REA.[50] Further, REA noted in its Post- Breach Report that "[t]o date, there have been no further complaints or matters arising from [the] incident."[51] Given the specific circumstances of the matter, the personal information involved could not have been used to commit identity fraud. As such, the personal information of the data subjects cannot be considered as other information that, under the circumstances, may enable identity fraud.

The second requisite is present in this case. There was acquisition of the information by an unauthorized person.

The Commission previously held that a loss of control over personal data held in custody is enough for a personal information controller (PIC) to have "reason to believe that the information may have been acquired by an unauthorized person."[52]

REA admitted in its Post-Breach Report that one (1) applicant notified REA that "he was able to view the personal information of the other applicants."[53] This shows that there is not just a reasonable belief but certainty that an unauthorized person acquired the information involved in the breach.[54]

The third requisite is also absent. There is no real risk of serious harm in this case.

---

[49] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly, GOLA English Tutorial, Inc., 27 July 2018, at 1, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).
[50] Compliance, 07 March 2023, at 1-2, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[51] *Id.* at 2.
[52] In re: Batangas Bay Carriers, Inc., NPC BN 20-157, 21 September 2020, at 5, *available at* https://www.privacy.gov.ph/wp-content/uploads/2022/01/Resolution-NPC-BN-20-157-In-re- Batangas-Bay_Sep-21.pdf (last accessed 11 July 2024).
[53] Compliance, 07 March 2023, at 1-2, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[54] In re: Batangas Bay Carriers, Inc., NPC BN 20-157, at 5.

The Commission takes this opportunity to discuss the factors considered in determining the presence of the third requisite of mandatory breach notification. Section 11 (C) of NPC Circular 16-03 provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> . . .
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[55]

For this purpose, the phrase "likely to give rise to a real risk" in Section 11 (C) means that a link exists between the breach and the possible resulting harm to any affected data subject.[56] The risk must be apparent and not the product of mere speculation.[57] Serious harm means that the consequences and effects to any affected data subject are significant based on the surrounding circumstances of the breach.[58]

In determining whether the unauthorized acquisition is likely to give rise to a real risk of serious harm, a PIC or the Commission may consider several factors, such as: the nature and amount of information involved in the breach, the period of time that has lapsed since the breach, objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.[59]

In this case, as previously established, the unauthorized acquisition was due to REA's inadvertent failure to turn off the "view other responses" function.[60] There is no showing that the tutor-applicant who notified REA deliberately intended to obtain the other applicants'

---

[55] NPC Circ. No. 16-03, § 11.
[56] In re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8, *available at* https://privacy.gov.ph/wp-content/uploads/2024/05/NPC-BN-17-028-_-NPC-BN- 18-180-2023.05.11-In-re-Easytrip-Reso-Final.pdf (last accessed 28 May 2024).
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly, GOLA English Tutorial, Inc., 27 July 2018, at 1, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).

information, as he even reported it to REA.[61] Thus, the objective of the unauthorized acquisition was not for malicious or fraudulent purposes. Further, REA reported that it immediately disabled the feature that allowed the personal information of the applicants to be viewed by others.[62] As such, further exposure or misuse of the information is unlikely.

Finally, Section 20 of the DPA provides that Personal Information Controllers (PICs) must implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any unlawful disclosure:

> Section 20. *Security of Personal Information*. (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[63]

In this case, REA implemented sufficient security measures on the information to address the breach and prevent its recurrence. REA reported that it shifted to the use of email correspondence in the tutor application process rather than using an external party application like Google forms.[64] Further, it designated only one person to take charge of the new email application process.[65] REA also reminded its employees and "reinforced the need to be hyper-aware of the Data Privacy Act's requirements."[66]

Given the foregoing factors, the unauthorized acquisition did not give rise to a real risk of serious harm to any affected data subject. Thus, the third requisite is absent.

Considering that the first and third requisites are absent, the matter does not fall under mandatory breach notification. Nevertheless, REA conducted proper breach management, including the implementation of reasonable and appropriate security measures. The measures

---

[61] Compliance, 07 March 2023, at 1-2, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[62] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc., 27 July 2018, at 2, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).
[63] Data Privacy Act of 2012, § 20 (a).
[64] Compliance, 07 March 2023, at 3, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[65] *Id.*
[66] *Id.*

implemented by REA are sufficient to address the breach and to prevent its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-131 In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.) is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
16 May 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

PVO
Representative
Rarejob English Assessment, Inc.

AOT
Counsel for Rarejob English Assessment, Inc.
De Guzman San Diego Mejia & Hernandez Law Offices (GSMH Law)

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FYNAMICS LENDING INC. OPERATING PONDOPESO ONLINE LENDING APPLICATION
x----------x

NPC 19-910
For violation of the Data Privacy Act of 2012

RESOLUTION

On 05 November 2020, the Commission issued an Order granting the request by Respondent Fynamics Lending, Inc. (Respondent) for a thirty (30) day extension or until 15 November 2020 to submit the documents requested following the Clarificatory Hearing held on 01 October 2020.

On 15 November 2020, Respondent filed a Motion for Additional Time to File Compliance, requesting for another extension of ten (10) days within which to comply with the 01 October 2020 Order of the Commission. They state in their Motion:

> 3. The Respondent respectfully manifest (sic) that while it endeavored to secure the required documents, it was experiencing difficulty due to the resignation and layoffs of its former employees. Moreover, its efforts were hampered by the series of typhoons which affected Metro Manila.

Considering the circumstances raised by Respondent and in the interest of an exhaustive investigation, the Commission grants the requested additional time to submit the required documents.

WHEREFORE, the Commission **GRANTS** a final and non-extendible extension of ten (10) days or until **25 November 2020** for Fynamics Lending, Inc. to produce and submit the documents specified in the Order dated 01 October 2020.

Failure to comply with this Order shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

SO ORDERED.
City of Pasay, Philippines
19 November 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

GONZALES AND QUISMORIO LAW OFFICES
Counsel for Respondents Fynamics Lending, Inc., ML, CW, and BBS

GOROSIN GARCIA & ASSOCIATES
Counsel for Respondents KF, JCG and HAD

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FYNAMICS LENDING INC. OPERATING PONDOPESO ONLINE LENDING APPLICATION

NPC No. 19-910
For violation of the Data Privacy Act of 2012

x----------x

RESOLUTION

On 10 February 2020, the Commission received a Motion for Extension of Time to File Compliance (hereafter, "Motion") by respondent Fynamics Lending Inc. and some of its directors, ML, CW, and BBS (hereafter "the Respondents").

In their Motion, the Respondents state:

> 3. The Respondents, in collaboration with their undersigned counsel, are currently preparing and gathering documents to support specific allegations in the Answer, in compliance with the Order.
>
> 4. However, the efforts to comply with the Order are being beset by communication and logistics issues arising from the ongoing outbreak in China caused by the 2019 Novel Coronavirus and by time-consuming presentation and review of documents.

The Commission emphasizes that the period of time it granted the Respondents in its Order dated 8 January 2020 was based on the nature of documents it required to be submitted. The allegations in their Answer show that these are documents that would have been readily available and already in the possession of the Respondents, thus:

> 18. It is not true that Fynamics and its directors/officers have "knowledge of the practices of its agents or other people clothed with the authority to collect outstanding loans" because, in fact, the collection agents who committed debt-shaming practices did so without the knowledge of Fynamics and its directors/officers. It then follows that without any knowledge of Fynamics and its officers, the respondents could not have consented to the acts of the collection agents, whether expressly or impliedly.[1]

[1] Answer dated 15 October 2019, par. 18.

> 19. Fynamics recognizes that even if the collection of loan repayments was outsourced to a third-party service provider, it was not amiss in its duty to ensure that the third-party service provider/processor and the collection agents under its employ comply with the DPA and the basic principles of personal data protection. In particular, collection agents are supposed to use only a provided computer software to contact the user/borrower or third parties. They were not allowed to use their personal phones to contact the user or other parties, which is what these collection agents did.[2]

The Commission finds the Respondents' Motion to be unclear about how the outbreak in China caused by the 2019 Novel Coronavirus affects their possession and submission of the required documents to the Commission within the prescribed period.

Nevertheless, in the interest of conducting an exhaustive investigation and finding that the Motion was filed within the allowable period of time, the Commission grants the Motion for additional time as prayed for by the respondents.

WHEREFORE, the Commission hereby **GRANTS** the Motion for Extension of Time to File Compliance by respondents Fynamics Lending Inc. and the individual respondents ML, CW, and BBS, allowing the submission of Compliance until 20 February 2020.

Failure to comply with this Order shall cause the Commission to adjudicate the issues on the basis of the evidence on record.

SO ORDERED.

City of Pasay, Philippines
20 February 2020

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

---

[2] Answer dated 15 October 2019, par. 19.

WE CONCUR:

Sgd.

JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Sgd.

RAYMUND E. LIBORO
Privacy Commissioner

COPY FURNISHED:

ROMULA MABANTA BUENAVENTURA SAYOC & DE LOS ANGELES
Counsel for Fynamics Lending Inc., ML, CW, and BBS.

GOROSIN GARCIA & ASSOCIATES
Counsel for Respondents KF, JCG and HAD

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: FYNAMICS LENDING INC. OPERATING PONDOPESO ONLINE LENDING APPLICATION

NPC No. 19-910
For violation of the Data Privacy Act of 2012

x----------x

RESOLUTION

On 30 August 2019, the Commission issued an Order requiring Fynamics Lending Inc. and its responsible officers to submit their respective Answers to the allegations in the Fact-Finding Report within ten (10) days from receipt thereof.

Consequently, upon receipt of the said order on 5 September 2019, individual respondents KF, JCG and HAD, through counsel, submitted their Appearance and Motion for Extension to file Answer and prayed that the Commission grant an additional period of ten (10) days from 16 September 2019, or until 26 September 2019, within which to file their responsive pleading.

For their part, respondents Fynamics Lending Inc., ML, CW, and BBS, through counsel, submitted on 16 September 2019 their Appearance and Omnibus Motion. They cited the fact that the last day of the 10-day period fell on a Sunday, moving the deadline to the next working day or 16 September 2019. The respondents prayed that the proceedings be suspended pending the resolution of the instant Omnibus Motion and that mediation proceedings be initiated. It was also prayed that the Commission grant the respondents an additional period of fifteen (15) days from 15 September 2019, or until 30 September 2019, to file their responsive pleading.

On 26 September 2019, respondents KF, JCG and HAD, through counsel, another Motion for Additional Time to File Verified Answer and moved for an additional period of ten (10) days from 26 September 2019 or until 06 October 2019 within which to file their responsive pleading.

On 27 September 2019, counsel for respondent Fynamics Lending Inc., the Gonzales & Quismorio Law Offices, filed their Withdrawal of Appearance with the conformity of respondent ML as the respondent corporation's President.

On 30 September 2019, respondent Fynamics Lending Inc., through counsel Romulo Mabanta Buenaventura Sayoc & de los Angeles filed an Entry of Appearance with Motion for Further Extension of Time to File Answer, citing the fact that new counsel has just been engaged. Respondent Fynamics Lending, Inc. moved for an additional period of fifteen (15) days from 30 September 2019 or until 15 October 2019 within which the file their answer.

Upon consideration of the requests of the respondents for additional time to file their Answers, all duly filed within the allowable period of time and not prejudicial to the plaintiff's substantive rights, the Commission grants such motions for additional time as prayed for by the respondents.

As regards the prayer of respondents ML, CW, and BBS for the initiation of a mediation proceeding and the suspension of the proceedings pending the resolution of their Omnibus Motion, the Rule on Alternative Modes of Dispute Resolution under NPC Circular No. 16-04 finds application, thus:

> Section 26. Mediation officer. - The Commission shall assign a mediation officer to assist the complainant and respondent to reach a settlement agreement, **provided that no settlement is allowed for criminal acts**.[1] xxx

The instant case was initiated through a *sua sponte* investigation of the National Privacy Commission pursuant to Section 3 of NPC Circular No. 16-04. The Fact-Finding Report noted certain dangerous permissions in the Android Package (APK) of the PondoPeso application that are designed to be indispensable for the application to function,[2] as well as the inaccessibility of a Privacy Policy that provides an explanation of this to the user.[3] Based on these, the Fact-Finding report found that "the apparent failure of the company to abide by the directives of the DPA in the protection of data subjects and their personal information constitute violations of the law."[4] Specifically, the Fact-Finding Report recommends

---

[1] Section 26, emphasis mine.
[2] Fact-Finding Report, p. 11.
[3] *Id.*, at p. 14.
[4] *Id.*, at p. 15.

criminal prosecution for the company, represented by their board of directors, for violations of Sections 25, 28, 31, and 32 of the Data Privacy Act.

Upon consideration of the allegations in the Fact-Finding Report and the existing rules under NPC Circular No. 16-04, the Commission finds that there is no basis for the Commission to grant the prayer of respondents ML, CW, and BBS for the initiation of a mediation proceeding and the suspension of the proceedings pending the resolution of their Omnibus Motion.

WHEREFORE**,** all premises considered, the Commission resolves to:

(1) **GRANT** the Motion for Further Extension of Time to File Answer by Respondent Fynamics Lending Inc., allowing the submission of an Answer until 15 October 2019;
(2) **GRANT** the Motion for Additional Time to File Verified Answer by respondents KF, JCG and HAD, allowing the submission of an Answer until 06 October 2019;
(3) **GRANT** the prayer for an additional period to file their Answer in the Omnibus Motion by respondents ML, CW, and BBS, allowing the submission of an Answer until 30 September 2019; and
(4) **DENY** the prayer for the initiation of a mediation proceeding and the suspension of the proceedings pending the resolution of the Omnibus Motion by respondents ML, CW, and BBS

SO ORDERED.

City of Pasay, Philippines
7 October 2019

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
IVY D. PATDU

Sgd.
RAYMUND ENRIQUEZ LIBORO

Deputy Privacy Commissioner

Privacy Commissioner

COPY FURNISHED:

GONZALES & QUISMORIO LAW OFFICES
Counsel for Respondents
ML, CW, and BBS

GOROSIN GARCIA & ASSOCIATES
Counsel for Respondents KF,
JCG and HAD

ROMULA MABANTA
BUENAVENTURA SAYOC &
DE LOS ANGELES
Counsel for Fynamics Lending Inc.

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: WESTERN UNION SERVICES (PHILIPPINES), INC.

NPC BN 18-151

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is Western Union Services (Philippines), Inc.'s (WUSPI) breach notification and management in compliance with NPC Circular 16-03 (Personal Data Breach Management).

Facts

On 8 August 2018, WUSPI notified the National Privacy Commission (NPC) about a data breach that took place on 5 August 2018.[1] It involved one data subject from the Philippines whose personal data was disclosed to twenty-seven (27) individuals overseas.[2] The information was in electronic format and consisted of the data subject's name, address, primary phone number, email address, date of birth, occupation, the names of transaction counterparties, the relationship to the data subject and the transaction purpose.[3]

In its initial notification, WUSPI, on behalf of Western Union (WU) indicated the names of the Head of the Organization and the Data Protection Officer (DPO) as the responsible officers.[4]

WUSPI stated that WU runs a call cent[er] in the Philippines known as the Asia Pacific Regional Operations Cent[er] (AROC).[5] AROC utilizes a template Reinstatement Form to request information from

---

[1] Mandatory Breach Notification Letter, 08 August 2018, at 1, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).

[2] *Id.*

[3] *Id.*

[4] *Id.* at 1-2.

[5] *Id.* at 2.

individuals regarding certain transactions.[6] The data subject, being one of the clients, completed this form and sent it to WU.[7] WUSPI's employee, however, mistakenly sent the completed form to twenty- seven (27) other individuals.[8]

In response to the breach, WUSPI claimed that it took the following measures:

- [It] contacted the recipients to delete the email and [data subject's] personal data;
- Internal measures were undertaken to address the issue with [its] staff to avoid recurrence of the incident; [and]
- [It] contact[ed] the affected data subject to notify her of the incident.[9]

WUSPI concluded its initial notification by stating that it is conducting further investigations to determine if any other individuals were affected by the breach.[10]

WUSPI also noted in its notification that it was "in the process of registering with the NPC and is one of the entities subject of a pending Request for Group DPO filed with the NPC on 27 February 2018 and refiled on 14 May 2018."[11]

On 15 October 2020, the NPC, through the Complaints and Investigation Division (CID), directed WUSPI to "submit a post-breach report detailing the results of the investigation conducted as well as the remedial measures taken to notify the affected data subjects, address the incident and prevent its recurrence" within fifteen (15) days from the receipt of the Order.[12]

On 28 March 2022, the CID issued another Order directing WUSPI, pursuant to Section 17(D) of NPC Circular 16-03, to submit a Full

---

[6] *Id.*
[7] Mandatory Breach Notification Letter, 08 August 2018, at 2, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.* at 1.
[12] Order, 15 October 2020, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2020).

Report detailing the incident within fifteen (15) days from receipt of the Order.[13]

On 08 August 2022, WUSPI sent a letter requesting an extension of time to submit its response.[14] In this letter, WUSPI explained that there was a delay in receiving the Order because it had been sent to the previous DPO, who left WU near the end of 2018.[15] The DPO who succeeded him also left WU on 3 June 2022.[16] Consequently, the current DPO was only able to register on 4 August 2022.[17] Given these circumstances, WUSPI's DPO requested an extension of time to submit a response.[18] She also stated that a response to the Order would be submitted within fifteen (15) days of receiving a copy of the incident report that WU submitted to the NPC.[19]

On 30 August 2022, the CID granted the request for extension.[20]

On 07 September 2022, WUSPI submitted its Compliance, including a full report detailing the incident as directed by the CID.[21] In its Report, WUSPI reiterated the details indicated in its initial notification to the Commission.[22] In its Report, WUSPI reiterated the details indicated in its initial notification, stating that the breach was caused by human error.[23] It claimed that WU employees are trained to send the blank Reinstatement Form template, which is stored on WU's SharePoint site, to customers upon request.[24] In this particular incident, however, instead of following the standard procedure to access the shared storage site, the employee mistakenly sent the Completed Reinstatement Form.[25]

---

[13] Order, 28 March 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[14] Request for Extension, 08 August 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] Order, 30 August 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[21] Compliance, 07 September 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18- 151 (NPC 2022).
[22] *Id.*
[23] *Id.* at 2.
[24] *Id.*
[25] *Id.*

WUSPI added a chronology of the events that led to the loss of control over the data subject's personal data:

> Prior to July 30, 2018: The Western Union customer the [sic] completed the Reinstatement Form and sent the Completed Reinstatement Form to AROC
>
> July 30, 2018: An AROC employee mistakenly sent the Completed Reinstatement Form to 27 other customers.
>
> Between July 30 and August 2, 2018: One of the 27 customers to whom the Completed Reinstatement Form was sent notified AROC that the Completed Reinstatement Form [of] the customer had received contained information about another customer.
>
> Between July 30 and August 2, 2018: Western Union determined that in addition to the customer that reported receiving the populated Restatement Form, 26 other customers had received the same populated Form. Western Union emailed each of the 27 customers and requested that they delete the email that contained the data subject's personal information.
>
> August 3, 2018: Western Union's Data Protection Officer, WLT, was notified that a potential data privacy incident had occurred.
>
> August 5, 2018: Western Union's Data Protection Officer, WLT, determined that a reportable privacy incident had occurred.
>
> August 8, 2018: Following investigation into the incident, WLT submitted the incident notification to the NPC and sent the customer notification letter to the affected data subject.[26]

WUSPI asserted that the scope of disclosed data was limited, as only the personal data of one customer was inadvertently disclosed, and the categories of personal data were minimal.[27] It also alleged that "the completed reinstatement form did not contain any sensitive personal data, banking or funds source information, or the affected individual's national identification number."[28]

WUSPI claimed that the number of recipients was also limited, with the form being shared with only twenty-seven (27) individuals.[29] WUSPI contacted these individuals and instructed them to delete the

---

[26] *Id.*
[27] Compliance, 07 September 2022, at 3, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[28] *Id.*
[29] *Id.*

form.[30] WUSPI maintained that the recipients were not malicious actors but were customers seeking reinstatement of their own accounts.[31] According to WUSPI, since it is aware which customers received the data, any illegitimate use of the personal data could be traced back to those customers.[32]

Further, WUSPI contended that no systems or databases were compromised due to this incident.[33] The breach was caused solely by human error, and no system vulnerabilities were identified during the investigation that required remediation.[34] Additionally, WUSPI alleged that this incident occurred in July 2018, and it "has no knowledge of any illegitimate uses of the data subject's information since that time."[35]

WUSPI alleged that several safeguards had been in place to minimize the impact of the personal data breach and to prevent future incidents.[36]

WUSPI stated that after discovering the breach, it promptly sent emails to the twenty-six (26) customers as well as the one customer who had notified WUSPI of receiving the Completed Reinstatement Form.[37] Through these emails, WUSPI informed the customers about the error and instructed them to delete the form from their email accounts immediately.[38] WUSPI also alleged that it notified the individual whose personal data had been inadvertently disclosed, even though they assessed that the risk of harm was low.[39]

As part of its Compliance, WUSPI submitted a copy of the letter notice sent to the affected data subject,[40] along with a copy of the airway bill from the courier as proof of notification:[41]

---

[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] Compliance, 07 September 2022, at 3, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Compliance, 07 September 2022, at 3-4, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[40] Notification to Affected Data Subject, 08 August 2018, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).
[41] Courier Receipt, 08 August 2018, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18- 151 (NPC 2018).

> Dear [ ],
>
> I write on behalf of WU, regarding an incident involving personal data you provided recently in your reinstatement request for transaction with money transfer control number (MTCN) – [ ] - 7823.
>
> We regret to inform you that your data was inadvertently exposed in this Incident. The exposure included your full name, primary phone number, address, date of birth, occupation, email address, 455 and the names of your blood relatives from whom you received or to whom you sent money (and purpose for those transactions).
>
> Nature of the Breach.
> - You completed a reinstatement form and sent this to WU. The completed reinstatement form containing your information was mistakenly sent to 27 other individuals.
>
> Measures taken to Address the Breach.
> - Internal measures were undertaken to address the issue with our staff to avoid a recurrence of the incident.
>
> Measures taken to reduce the harm or negative consequences of the breach.
> - We have contacted the recipients to delete the email and your personal data.
>
> Do not hesitate to contact me for further information:
>
> Data Protection Officer WLT
>
> [Contact details]

WUSPI also claimed that disciplinary action had been taken against the employee who did not follow standard procedures.[42] It reminded the employee of the correct processes and issued a written disciplinary warning to prevent similar incidents from occurring in the future.[43] WUSPI contended that following the incident, the team in charge of sending reinstatement forms was reminded of the importance of adhering to the established processes.[44]

---

[42] Compliance, 07 September 2022, at 4, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[43] *Id.*
[44] *Id.*

WUSPI maintained that an internal privacy policy had been in force at the time of the incident, which contained several provisions on the protection of personal information.[45] The policy included clauses such as collecting only necessary personal information,[46] using personal information for specific pre-defined purposes,[47] maintaining a comprehensive privacy and data protection training program,[48] implementing appropriate administrative, technical, physical, and organizational measures to protect personal information,[49] sharing only the minimum necessary personal information in a secure manner,[50] and enforcing disciplinary action for policy violations.[51]

WUSPI also attached its Information Classification Policy in its Compliance, which classified customer information as confidential and required all employees to protect this information, including providing heightened protections for confidential information.[52] In accordance with this policy, WUSPI required employees and departments to provide necessary information to demonstrate adherence and compliance which will be verified and documented by the Chief Privacy Officer (CPO) and the Chief Information Security Officer through Privacy Impact Assessments or Information Security Assessments.[53] Any violation of this Policy must be reported to the CPO or the Privacy Office, which will investigate and coordinate with relevant departments like HR, Legal, and Information Security to address and resolve any allegations of non-compliance.[54]

WUSPI claimed that it conducts mandatory global privacy training for all employees annually.[55] The training covered various aspects of data privacy and security, including the importance of data privacy laws, key privacy concepts, defining personal data, and handling individual data rights.[56] According to WUSPI, employees were also trained to

---

[45] *Id.*
[46] 2018 Privacy Policy, 17 May 2018, at 6, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).
[47] *Id.*
[48] *Id.* at 7.
[49] *Id.* at 8.
[50] *Id.*
[51] *Id.* at 10.
[52] Information Classification Policy, 24 June 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[53] *Id.* at 14.
[54] *Id.*
[55] Compliance, 07 September 2022, at 6, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[56] Privacy Training Continuing Education Visual Aid, 07 September 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).

recognize and manage privacy incidents in order to ensure compliance with relevant privacy laws and regulations.[57]

In addition, WUSPI alleged that it has a mandatory Corporate Information Security Program applicable globally to WU and its subsidiaries.[58] The program provided a framework for risk-based IT security measures.[59] WUSPI claimed that this program was designed to maintain the confidentiality of organizational information, safeguard against potential threats and hazards, ensure the availability and integrity of WU's data, and prevent unauthorized or illegal access to or use of its information assets.[60]

Issue

Whether WUSPI notified the affected data subject, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. WUSPI's submissions show that it properly notified its affected data subject, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

It is the responsibility of a Personal Information Controller (PIC), such as WUSPI, to ensure that affected data subjects of the breach are promptly and properly notified about the breach.[61] The Commission has consistently emphasized that the purpose of notifying data subjects of a breach is to enable them to take necessary precautions or other actions to protect themselves from potential consequences.[62]

Section 18 of NPC Circular 16-03 provides the requirements on the content and form of the notification of data subjects:

---

[57] *Id.*
[58] Compliance, 07 September 2022, at 6, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[59] *Id.*
[60] *Id.*
[61] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).
[62] *Id.* § 18 (A).

Section 18. *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:

. . .

C. *Content of Notification*. The notification shall include, but not be limited to:

1. nature of the breach;
2. personal data possibly involved;
3. measures taken to address the breach;
4. measures taken to reduce the harm or negative consequences of the breach;
5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. any assistance to be provided to the affected data subjects.

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.

D. *Form*. Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.

The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[63]

[63] NPC Circ. No. 16-03, § 18 (C) & (D).

Here, WUSPI notified the affected data subject about the incident through a letter sent by courier.[64] This aligns with the requirements set forth in Section 18(D) since it provides a direct and secure way to inform the affected individual while taking necessary precautions to protect her personal data from further unnecessary disclosure.

On the content of the notification, WUSPI identified the nature of the breach by informing the affected data subject that the completed reinstatement form containing the data subject's information was mistakenly sent to twenty-seven (27) other individuals.[65]

The notification specified the types of personal data that may have been exposed, including the full name, primary phone number, address, date of birth, occupation, email address, and the names of blood relatives involved in money transactions.[66]

The notification also outlined the immediate actions taken to address the breach, such as implementing internal measures to prevent recurrence and contacting the recipients to delete the email and personal data.[67]

WUSPI provided the DPO's contact information, including an email address and phone numbers, allowing data subjects to obtain additional information regarding the breach.[68] This satisfied the requirement to include contact information of a representative from whom more information could be obtained.[69]

In addition, WUSPI took measures to sufficiently address the breach and adopted measures to prevent its recurrence.[70]

Section 20 of Republic Act No. 10173 or the Data Privacy Act (DPA) provides that PICs must implement reasonable and appropriate

---

[64] Notification to Affected Data Subject, 08 August 2018, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] NPC Circ. No. 16-03, § 18 (C).
[70] Compliance, 07 September 2022, at 4, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).

organizational, physical, and technical measures intended for the protection of personal information against any unlawful disclosure:

> Section 20. *Security of Personal Information.* (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[71]

Disciplinary action was taken against the employee who failed to follow standard procedures, including a reminder of the correct processes and a written disciplinary warning.[72] The team responsible for sending reinstatement forms was reminded of the importance of adhering to established procedures.[73]

Even prior to the incident, WUSPI had an internal privacy policy, which included provisions for the protection of personal information.[74] This policy outlined practices such as collecting only necessary personal information, using it for specific pre-defined purposes, maintaining comprehensive privacy and data protection training programs, and enforcing appropriate security measures.[75]

WUSPI also has an Information Classification Policy, which stated that customer information is confidential and required heightened protections.[76] Moreover, WUSPI claimed that it conducted mandatory global privacy training for all employees annually, covering various aspects of data privacy and security.[77] In addition, WUSPI's Corporate Information Security Program provided a framework for risk-based IT security measures to maintain confidentiality, safeguard data, and prevent unauthorized access.[78]

---

[71] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (a) (2012).
[72] Compliance, 07 September 2022, at 4, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[73] *Id.*
[74] *Id.*
[75] 2018 Privacy Policy, 17 May 2018, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18- 151 (NPC 2018).
[76] Information Classification Policy, 03 April 2007, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[77] Privacy Training Continuing Education Visual Aid, 07 September 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[78] Compliance, 07 September 2022, at 6, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).

Given the foregoing, the Commission finds that WUSPI properly notified its affected data subjects and implemented sufficient measures to address the breach and prevent its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-151 In re: Western Union Services (Philippines), Inc. is **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
05 June 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

APG
Data Protection Officer
Western Union Services (Philippines), Inc.

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: TELETECH CUSTOMER CARE MANAGEMENT PHILIPPINES, INC. **NPC 21-214**

x----------x

RESOLUTION

NAGA, P.C.:

This Resolution refers to the Compliance dated 17 May 2022 of Teletech Customer Care Management Philippines, Inc. (TTEC) to the Order dated 17 March 2022.

Facts

On 17 March 2022, the Commission issued an Order to TTEC with the following dispositive portion:

> **WHEREFORE**, premises considered, Teletech Customer Care Management Philippines, Inc. (TTEC) is **ORDERED** to comply with the following **within a non-extendible period of fifteen (15) days upon receipt of the Order to:**
>
> **(1) NOTIFY** the affected data subjects.
>
> For the **current** employees, they shall be notified pursuant to Section 18(D) of the NPC Circular No. 16-03. The notification shall be done individually using secure means of communication, **through email**. TTEC shall submit proof of compliance, including the proof of receipt of the data subjects of such notification.
>
> For the **former** employees, they shall be notified through alternative means pursuant to Section 18(D) of the NPC Circular No. 16-03, through the publication of the notice on the following media: (a) TTEC's website; and (b) advertisement spaces to be procured from newspapers of

national circulation (i.e., Philippine Daily Inquirer or Manila Bulletin), and regional circulation in key cities or provinces wherein TTEC has an office or contact center. TTEC shall also provide to the Commission proof of compliance, including proof of notification/publication;

The proof of notification must be supported by appropriate affidavits, as applicable, including evidence that TTEC has procured advertisement spaces in newspapers of national circulation, and newspapers of regional circulation in all the cities or provinces wherein TTEC has an office or contact center;

(2) SUBMIT its Full Breach Report pursuant to Section 9 and Section 17(D) of NPC Circular No. 16-03; and

(3) ADDRESS the directive contained in the Order dated 13 January 2022 to show cause in writing on why it should not be subjected to contempt proceedings, as permitted by law, before the appropriate court, and other actions as may be available to the Commission, for its failure to submit its Full Breach Report within the prescribed period.

The Complaints and Investigation Division (CID) and the Compliance and Monitoring Division (CMD) of the National Privacy Commission are hereby **ORDERED** to conduct the appropriate investigation on TTEC's possible violations of the DPA.

SO ORDERED.[1]

In compliance with the Order dated 17 March 2022, TTEC submitted a Manifestation and Motion dated 17 May 2022 attaching therein the Affidavit of Publication issued by Manila Bulletin [2] and Panay News,[3] an Authorization to Sunstar Publishing, Inc. issued by TTEC to complete the publication in Batangas, Laguna, Cebu, and Dumaguete,[4] and its Full Breach Report.[5]

---

[1] In re: Teletech Customer Care Management Philippines, Inc., NPC BN 18-205, Order dated 17 March 2022

[2] Manifestation and Motion dated 17 May 2022 of Teletech Customer Care Management Philippines, Inc., in Annex "A"

[3] *Id.*, in Annex "B"

[4] *Id.*, Annex "C"

[5] *Id.*, Annex "D"

In its Compliance, TTEC stated that it should not be subjected to contempt proceedings since it was able to timely notify the Commission of the data breach and exerted its effort to comply with the directives of the Commission by supplementing its initial data breach report, which contains relevant information available to TTEC.[6]

Thus, TTEC prayed for the Commission to issue an order: (1) making of record TTEC's partial compliance with the Order dated 17 March 2022; and (2) granting an additional reasonable period to file its full compliance with the Order dated 17 March 2022.[7]

On 23 May 2022, TTEC submitted a Supplement to the Manifestation and Motion dated 17 May 2022, attaching therein (1) affidavits of publication issued by Sunstar Bacolod[8] and Cebu[9] and
(2) TTEC's Service Agreement on its purchase with Epiq Corporate Services, Inc. for the sending of breach notice via email and setting up a call center to answer concerns from the affected data subjects.[10]

On 29 June 2022, TTEC submitted its Second Supplement to the Manifestation and Motion dated 17 May 2022 with the following attachments:

> 3.1. Proof of publication of the data breach notice in regional newspapers in Batangas and Laguna, Cebu City, and Dumaguete City as Annex "A-Series";
>
> 3.2. Proof of posting of the data breach notice on TTEC's website as
> Annex "B"; and
>
> 3.3 Proof of individual notification to TTEC employees through email made by TTEC's service provider, Epiq Corporate Services, Inc., and of receipt of such email notification as Annex "C-Series".[11]

---

[6] Manifestation and Motion dated 17 May 2022 of Teletech Customer Care Management Philippines, Inc., at p. 3.
[7] *Id.* at p. 3.
[8] Supplement to the Manifestation and Motion dated 23 May 2022 from TTEC, in Annex "A"
[9] *Id.*, in Annex "B"
[10] *Id.*, in Annex "C"
[11] Second Supplement to the Manifestation and Motion dated 17 May 2022 (Re: Order dated 17 March 2022) dated 29 June 2022 of Teletech Customer Care Management Philippines, Inc.,

On 14 July 2022, the Commission issued a Resolution denying the Manifestation and Motion dated 17 May 2022 filed by TTEC.[12] In denying TTEC's request for an additional period to comply with the 17 March 2022 Order, the Commission stated that "the request has become moot since TTEC claims that its latest submission [Second Supplement to the Manifestation and Motion] [completes] its compliance" with the Commission's Order. [13] Further, the Commission denied the request for an extension since TTEC has not provided sufficient ground for its request for extension to be granted by the Commission.[14]

The Commission also stated that "even though TTEC claims that it has already fully complied with the Commission's Directives", the submissions are fragmentary and delayed. [15] Finally, "the Commission has accommodated TTEC's numerous requests for extension to comply with its obligations as a personal information controller (PIC), particularly with regard to data breach notification proceedings."[16]

On 12 October 2022, the Commission, through its Enforcement Division (EnD), issued a Compliance Letter requiring TTEC to submit a viewable excel file of its email report with regard to the proof of notification. [17] Subsequently, TTEC submitted its compliance on 19 October 2022, attaching therein a portable data format (pdf) file that contains proof of e-mail notification to its current employees.[18]

Issue

Whether TTEC is compliant with the Order of the Commission dated 17 March 2022.

---

[12] In re: Teletech Customer Care Management Philippines, Inc., NPC BN 21-214, Resolution dated 14 July 2022, at p. 10.

[13] *Id.*, at p. 5.

[14] *Id.*, at p. 5.

[15] *Id.*, at p. 10.

[16] In re: Teletech Customer Care Management Philippines, Inc., NPC BN 21-214, Resolution dated 14 July 2022, at p. 5.

[17] In re: Teletech Customer Care Management Philippines, Inc., NPC BN 18-205, Order dated 12 October 2022

[18] Electronic mail dated 19 October 2022 from Teletech Customer Care Management Philippines, Inc.

Discussion

The Commission finds that TTEC has sufficiently complied with the Order dated 17 March 2022.

I. TTEC sufficiently notified the data subjects affected by the breach.

Rule V, Section 18(D) of the NPC Circular No. 16-03 (Personal Data Breach Management) provides:

> D. *Form*. **Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic.** The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: Provided, that **where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner**: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[19] (Emphasis supplied)

In an Order dated 17 March 2022, the Commission ordered TTEC to notify the affected data subjects composing of its (1) current employees, using secure means of communication, through email; and (2) former employees through alternative means of communication.[20]

---

[19] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18(D) (15 December 2016) (NPC Circular 16-03).
[20] In re: Teletech Customer Care Management Philippines, Inc., NPC BN 21-214, Order dated 17 March 2022, at p. 16.

It complying with the said Order, TTEC sufficiently showed that it complied with the notification requirement through alternative means of communication.[21] In the said compliance, TTEC attached notices to the affected data subjects through publications from Panay News, [22] SunStar Bacolod, [23] SunStar Pampanga, [24] SunStar Business Section,[25] Manila Bulletin,[26] and on TTEC's website.[27]

On the other hand, TTEC provided an excel file to the Commission containing proof of e-mail notifications sent to its twelve thousand eight hundred sixty-six (12,866) current employees sent via email on 19 October 2022.[28]

Further, Section 18(C) of NPC Circular No. 16-03 provides for the content of notification to be sent to the affected data subjects:

> C. *Content of Notification.* The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;
> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
> 6. any assistance to be provided to the affected data subjects.
>
> Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.[29]

---

[21] Compliance and Manifestation dated 28 February 2022 of Teletech Customer Care Management Philippines, Inc.
[22] *Id.* Annex "A"
[23] *Id.*
[24] *Id.*"
[25] Compliance and Manifestation dated 28 February 2022 of Teletech Customer Care Management Philippines, Inc., Annex "A"
[26] *Id.*
[27] *Id.*
[28] Electronic mail dated 19 October 2022 from Teletech Customer Care Management Philippines, Inc.
[29] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18 (C) (15 December 2016) (NPC Circular 16-03).

TTEC's notices to its current and former employees contained the aforementioned contents of notification. Such notifications also stated that TTEC encourages the data subjects affected by the breach to "actively monitor and review [their] credit report and credit card, bank, and other financial statements for any unauthorized activity."[30] Further, affidavits of the publishers were submitted by TTEC to show proof of publication in various newspapers.[31]

Based on the foregoing, the Commission finds that TTEC has sufficiently complied with the Order dated 17 March 2022 by submitting its proof of notification to the affected data subjects. Thus, the notices sent to the current and former employees of TTEC satisfactorily complied with Section 18(C) and (D) of NPC Circular No. 16-03.

II. The Data Breach Report submitted by TTEC sufficiently complied with Section 17 (D) in relation to Section 9 of NPC Circular No. 16-03.

In the Orders dated 13 January 2022[32] and 17 March 2022[33],TTEC was ordered by the Commission to submit its Full Breach Report pursuant to Section 17 (D) in relation to Section 9 of NPC Circular No. 16-03, *thus*:

> **SECTION 9.** *Documentation.* All actions taken by a personal information controller or personal information processor shall be properly documented. Reports should include:
>
> A. Description of the personal data breach, its root cause and circumstances regarding its discovery;
> B. Actions and decisions of the incident response team;
> C. Outcome of the breach management, and difficulties encountered; and
> D. Compliance with notification requirements and assistance provided to affected data subjects.

[30] Compliance and Manifestation dated 28 February 2022 of Teletech Customer Care Management Philippines, Inc., Annex "A"
[31] Manifestion and Motion dated 17 May 2022 of Teletech Customer Care Management Philippines, Inc.
[32] In re: Teletech Customer Care Management Philippines, Inc., NPC BN 21-214, Order dated 13 January 2022, at p. 10.
[33] In re: Teletech Customer Care Management Philippines, Inc., NPC BN 21-214, Order dated 17 March 2022, at p. 16.

> A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor.[34]

Rule V Section 17(D) of NPC Circular No. 16-03 states:

> *D. Content of Notification.* The notification shall include, but not be limited to:
>
> 1. Nature of the Breach
> a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
> b. a chronology of the events leading up to the loss of control over the personal data;
> c. approximate number of data subjects or records involved;
> d. description or nature of the personal data breach;
> e. description of the likely consequences of the personal data breach; and
> f. name and contact details of the data protection officer or any other accountable persons.
> 2. Personal Data Possibly Involved
> a. description of sensitive personal information involved; and
> b. description of other information involved that may be used to enable identity fraud.
> 3. Measures Taken to Address the Breach
> a. description of the measures taken or proposed to be taken to address the breach;
> b. actions being taken to secure or recover the personal data that were compromised;
> c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
> d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
> e. the measures being taken to prevent a recurrence of the incident.
>
> The Commission reserves the right to require additional information, if necessary.[35]

[34] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule IV, § 9 (15 December 2016) (NPC Circular 16-03).
[35] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule IV, § 17(D) (15 December 2016) (NPC Circular 16-03).

In the 17 March 2022 Order, the Commission stated that "TTEC's three-page Report lacks clear and full details on the personal data breach."[36] The Commission also stated that the breach report of TTEC has "no actual description or narrative that refers or discusses the personal data breach itself."[37]

In its submissions, TTEC was able to provide the description of the personal data involved wherein "the unauthorized actor was able to exfiltrate several spreadsheets containing personal data of current and former employees."[38] TTEC has also identified the root cause of the breach in which "the unauthorized entry was the result of a phishing attack on an enterprise domain administrator who has access across various domains within TTEC environment."[39]

With regard to the actions and decisions of the incident teams, TTEC engaged with Arete Incident Response "to conduct a forensic investigation in connection with incident, identify incidents of compromise and assist with their eradication from the TTEC environment."[40] After the investigation, there is no evidence that unauthorized parties remained in TTEC's environment after the initial attack.[41]

Further, with the outcome of the breach management, TTEC was able to determine the total number of affected current and former employees.[42]

In sum, the submitted report of TTEC containing the description of the personal data involved, identifying the root cause of the breach, and the actions and decisions of the incident teams are compliant with the directives of the Commission pursuant to NPC Circular 16- 03 Section 17 (D) in relation to Section 9.

---

[36] In re: Teletech Customer Care Management Philippines, Inc., NPC BN 21-214, Order dated 17 March 2022, at p. 14.
[37] *Id.*
[38] Manifestation and Motion dated 17 May 2022 of Teletech Customer Care Management Philippines, Inc., in Annex "D"
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] Manifestation and Motion dated 17 May 2022 of Teletech Customer Care Management Philippines, Inc., in Annex "D"

III. TTEC has sufficiently shown proof of security measures it implemented to mitigate the breach

The Commission ordered TTEC to submit proof of security measures it implemented to address the breach.[43]

In compliance with the said Order, TTEC submitted its Manifestation and Compliance dated 25 January 2022 attaching therein proof of security measures to address the breach.[44]

In the said submission, TTEC stated that:

> "(a) Threat hunted incidents of compromise (IOCs) to contain and block potential malicious activity;
>
> (b) Added the TTEC incident specific IOCs, captured through the investigation, and other IOCs indicative of known cyber security ransomware threat actors to EDRs' and firewalls' blacklist; audited whitelists to make sure that known IOCs are not included there to supersede the blacklists;
>
> (c) Conducted an audit of all firewall domains;
>
> (d) Conducted an audit of Active Directory; and
>
> (f) *[sic]* Geo-blocked for connectivity in all countries where TTEC does not have business activity."[45]

TTEC also attached an ADAssessor Executive Summary showing data on the vulnerability status of TTEC's system.[46]

Thus, the Commission finds that TTEC's submitted Full Breach Report and proof of security measures are sufficient and compliant with the Orders of the Commission. Finally, the Commission finds that TTEC has sufficiently notified the affected data subjects in accordance with NPC Circular No. 16-03.

---

[43] In re: Teletech Customer Care Management Philippines, Inc., NPC BN 21-214, Order dated 13 January 2022, at p. 10.
[44] Manifestation and Compliance dated 25 January 2022 of Teletech Customer Care Management Philippines, Inc., in Annex "C"
[45] *Id.*
[46] *Id.*

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 21-214 "In re: Teletech Customer Care Management" is hereby considered **CLOSED**.

SO ORDERED.

Pasay City, Philippines.
26 January 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy Furnished:

SB
Data Protection Officer

DP
Counsel

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT DIVISON
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: TRAVELSERVICES, INC. **NPC BN 20-167**

x----------x

RESOLUTION

NAGA, *P.C.;*

Before the Commission are TravelServices, Inc.'s (TravelServices) Compliance and Motion for Partial Reconsideration dated 09 February 2021[1] to the Resolution issued by the Commission dated 21 September 2020.[2]

Facts

On 21 September 2020, the Commission issued an Order with the following dispositive portion:

> **WHEREFORE**, premises considered, the request for Postponement of Notification to Data Subjects filed by TravelServices, Inc. is hereby **DENIED.** TravelServices, Inc. is **ORDERED** to comply with the following **within fifteen (15) days from receipt of this Resolution:**
>
> 1. **SUBMIT** full breach report with the complete information required under NPC Circular 16-03 which includes among others, the nature of personal data involved and a determination of the affected data subjects; and
>
> 2. **NOTIFY** the affected data subjects of the breach incident in accordance with the provisions of NPC Circular 16-03 and to **SUBMIT** proof of compliance thereto.
>
> **SO ORDERED.**[3]

---

[1] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc.

[2] In Re: TravelServices, Inc., NPC BN 20-167, Resolution dated 21 September 2020.

[3] *Id.*

Accordingly, TravelServices submitted its Compliance and Motion for Partial Reconsideration dated 09 February 2021 and stated that it received the above Resolution on 25 January 2021.[4]

In Compliance to the Commission's order to submit its Full Breach Report, TravelServices provided the details on the nature of the breach stating that its server, holding TravelServices' clients and suppliers' information, has been infected by a ransomware virus which resulted to the encryption of files and change of file extensions to ".R," which made them inaccessible without a decryption key.[5] According to TravelServices, the incident resulted to the temporary inaccessibility of approximately fifty thousand (50,000) or more booking transactions, and that the incident has resorted them to manually input the ticket details and payment requests to suppliers.[6]

TravelServices also enumerated the personal data possibly involved in the ransomware attack, which include the following:

- First and last names of clients (no middle names).
- Booking details, i.e., ticket numbers, destinations, flight schedules, and the like.
- Email addresses (not applicable to all data subjects).
- Telephone numbers (not applicable to all data subjects).[7]

As to the measures taken to address the breach, TravelServices provided the following details:

- All servers were shut down to contain the virus and to allow IT to conduct a check on each server.
- An incident advisory was sent to all users and to management on August 26, 2020. All units were advised to apply their Business Continuity Plans and workarounds while the servers/systems were down.
- Security patches for the ransomware were applied to non- affected servers.
- Cybersecurity experts from the ePLDT Cyber Security were engaged to assist in the containment, clean-up, and possible decryption of affected files. The experts also conducted a

---

[4] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 1.
[5] Full breach report dated 09 February 2021 of TravelServices, Inc., at pp. 1-2.
[6] *Id.*
[7] *Id.*, at p. 2.

> forensic investigation to determine the methodology and behavior of the ransomware virus that infected the server.
> - All the affected data was restored from backups by September 8, 2020.
> - To prevent recurrence of the incident, [it] engaged experts to conduct a vulnerability assessment and penetration test on all systems in order to identify our risks of further exposure to cyberattacks and other security incidents and determine possible measures to mitigate or avoid them. [It] also plan[s] to deploy advanced endpoint detection and response tools to all workstations and servers in the first quarter of 2021.[8]

Further, TravelServices stated that it initially requested for the postponement from the notification required since it could not ascertain the identities of the affected data subjects and that no personal data had been acquired or accessed by unauthorized persons.[9]

However, upon investigation, TravelServices alleged that the incident did not show sensitive personal information or other information that may be used to enable identity fraud.[10] TravelServices further averred that there were no data subjects that "were harmed or could have been harmed as a consequence of the incident."[11] Thus, TravelServices claimed that there is no need to notify the affected data subjects regarding the "temporary availability breach" incident in this case.[12]

Lastly, TravelServices stated that if notification is done, "it will be impossible for [TravelServices] to notify all the data subjects directly, as [it] generally do not collect and record postal addresses, and not all clients provide their email addresses or phone numbers when transacting with [TravelServices]."[13]

On the other hand, TravelServices also filed its Motion for Partial Reconsideration to the Resolution issued by the Commission dated 21 September 2020.[14]

---

[8] *Id.*
[9] Full breach report dated 09 February 2021 of TravelServices, Inc., at p. 3.
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Full breach report dated 09 February 2021 of TravelServices, Inc., at p. 3.
[14] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc.

According to TravelServices, the Forensic Investigation Report from the cyber security experts it engaged to address the incident determined that "the security incident did not provide unauthorized persons any opportunity to access, obtain, or disclose any of the data affected by the ransomware virus."[15] TravelServices claimed that these findings confirmed its initial assessment that "there was no reason to believe that the data had been acquired by unauthorized person or that the incident/breach was likely to give rise to a real risk of serious harm to the affected data subjects."[16]

Moreover, TravelServices reiterated that if individual notification must be done directly to the affected data subjects, the same will be impossible as TravelServices generally does not collect and record postal addresses, and that not all of its clients provide their email addresses or phone numbers with TravelServices when transacting.[17]

Further, TravelServices stated that the instant case does not warrant notification to the affected data subjects.[18] It claimed that the three (3) requisites for the mandatory notification requirement under Section 11 of NPC Circular No. 16-03 are not present.[19]

TravelServices argued that none of the personal data involved in the incident are considered sensitive personal information or other information that may be used to enable identity fraud.[20] It also stated that there is no reason to believe that the information herein were acquired by an unauthorized person considering that according to the forensic investigation conducted by a reputable third-party cybersecurity experts, *"there was no malicious executable files dropped on the victim machine"* and *"there were no outbound connections to any known malicious hosts that were seen in the packet capture as signs of command and control of the miscreant."*[21]

---

[15] *Id.*, at p. 2.
[16] *Id.*
[17] *Id.*
[18] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 2.
[19] *Id.*, at p. 3.
[20] *Id.*
[21] *Id.*

Lastly, TravelServices submitted that no harm was inflicted to data subjects as a consequence of the security incident.[22] According to TravelServices, the only "harm" herein was the temporary inconvenience to its staff when the latter "had to input data manually while the travel management system was offline."[23]

Issue

Whether to grant the Motion for Partial Reconsideration filed by TravelServices dated 09 February 2021.

Discussion

The Commission notes the Compliance of TravelServices dated 09 February 2021. Further, the Commission denies the Motion for Partial Reconsideration filed by TravelServices.

The incident falls under the mandatory breach notification requirement.

Section 20(f) of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA) states:

> SEC. 20. Security of Personal Information.-
>
> ...
>
> (f) The personal information controller shall **promptly notify the** Commission and **affected data subjects when** sensitive personal information or **other information that may**, under the circumstances, **be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person,** and **the personal information controller** or the Commission believes **that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject[.]**[24] (Emphasis supplied)

---

[22] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 3.

[23] *Id.*

[24] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter V, § 20(f) (2012).

In relation thereto, Rule V, Section 11 of NPC Circular No. 16-03 provides:

> **Sec. 11. *When notification is required.*** Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:
>
> A. The personal data involves sensitive personal information or **any other information that may be used to enable identity fraud.** For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
> B. There is **reason to believe that the information may have been acquired by an unauthorized person**; and
> C. The personal information controller or the Commission believes that the unauthorized acquisition is **likely to give rise to a real risk of serious harm to any affected data subject**.[25] (Emphasis supplied)

In its full breach report, TravelServices stated that the personal data possibly involved are:

- First and last names of clients (no middle names).
- Booking details, i.e., ticket numbers, destinations, flight schedules, and the like.
- Email addresses (not applicable to all data subjects).
- Telephone numbers (not applicable to all data subjects).[26]

In this case, the first element of mandatory breach notification is present since the breach incident under the circumstances involves information that may be used to enable identity fraud such as the data subjects' names, email addresses, and telephone numbers.

---

[25] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V,
§ 11 (15 December 2016) (NPC Circular 16-03).
[26] Full breach report dated 09 February 2021 of TravelServices, Inc., at p. 2.

Given that these information were the subject of a ransomware attack, their unauthorized acquisition may result to identity fraud, identity theft, and phishing activities, when used in a manner that could expose the affected data subjects to harassment, discrimination, or other risks of real and serious harm. Thus, the first requisite is present.

As to the second requisite, the forensic investigation conducted by a reputable third-party cybersecurity experts stated that "*there was no malicious executable files dropped on the victim machine*" and "*there were no outbound connections to any known malicious hosts that were seen in the packet capture as signs of command and control of the miscreant.*"[27]

However, as previously held by the Commission in its Resolution dated 21 September 2020:

> It should be noted that a loss of control over personal data held in custody should be enough for a personal information controller to have "reason to believe that the information may have been acquired by an unauthorized person." An indication of exfiltration of data is not a requirement in Section 11(b). Absolute certainty of acquisition by an unauthorized person is not required by either the Circular or the Data Privacy Act (DPA), considering that the condition only provides for a determination based on the existing circumstances that can give a "reason to believe."[28]

Thus, the second requisite is present in this case considering that due to the ransomware attack, TravelServices has lost control over the information of its clients. Such is deemed a reason to believe that the information may have been acquired by an unauthorized person.

Lastly, TravelServices stated that no harm was inflicted to data subjects as a consequence of the security incident, that the only "harm" herein was the temporary inconvenience to its staff when the latter "had to input data manually while the travel management system was offline."[29]

---

[27] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 3.
[28] In Re: TravelServices, Inc., NPC BN 20-167, Resolution dated 21 September 2020.
[29] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 3.

However, mere temporary inconvenience to TravelServices' staff in manually inputting the booking records of approximately fifty thousand (50,000) or more individuals is not the "harm" contemplated under Section 11(c) of NPC Circular 16-03. The serious harm being considered in the said provision means that negative consequences such as identity fraud or theft may give rise due to the ransomware attack.[30] In this case, since TravelServices has lost control over the personal data due to ransomware attack, there already arose a belief that a real risk of serious harm to any affected data subjects may occur, which TravelServices failed to sufficiently prove. Thus, the third requisite is present.

Considering that all the requisites for mandatory breach notification are present in this case, the Commission deems it necessary to require TravelServices to notify the affected data subjects of the security incident. Such notification will enable the affected data subjects to take necessary actions "to protect themselves against the possible effects of the breach."[31]

TravelServices cannot excuse itself from its obligation to notify the affected data subjects by stating that TravelServices "generally do not collect and record postal addresses" and that "not all clients provide their email addresses or phone numbers when transacting with [it]."[32] In addition to its obligation to individually notify the affected data subjects, TravelServices may also notify them using alternative means of notification, or any other means wherein the data subjects are informed in an equally effective manner.[33]

WHEREFORE, premises considered, this Commission resolves to:

1. **DENY** the Motion for Partial Reconsideration dated 09 February 2021 filed by TravelServices, Inc. (TravelServices);

2. **DIRECT** TravelServices to individually **NOTIFY** the affected data subjects and **SUBMIT** proof of notification to the

---

[30] NPC Circular 16-03, § 11.
[31] *Id.*, § 18(A).
[32] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 2.
[33] NPC Circular 16-03, rule V, § 18(D).

Compliance and Monitoring Division (CMD) within **fifteen (15) days** from receipt of this Resolution;

3. **DIRECT** TravelServices to **SUBMIT** proof of notification to the affected data subjects through alternative means to the CMD within **five (5) days** from receipt of this Resolution;

4. **DIRECT** CMD to issue the appropriate orders necessary to evaluate and monitor the completeness of TravelServices' Compliance and assess its breach management pursuant to NPC Circular 16-03 (Personal Data Breach Management).

SO ORDERED.

City of Pasay, Philippines.
13 November 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

GGB
Data Protection Officer

COMPLIANCE AND MONITORING DIVISION COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION GENERAL RECORDS UNIT
National Privacy Commission

IN RE: COCA-COLA FEMSA PHILIPPINES, INC.
(now Coca-Cola Beverages Philippines, Inc.) x----------x

NPC BN 18-202

RESOLUTION

NAGA, *P.C.;*

Before the Commission is the Compliance[1] of Coca-Cola FEMSA Philippines, Inc. (CCFPI) (now Coca-Cola Beverages Philippines, Inc.) with the Order of the National Privacy Commission (NPC) through its Complaints and Investigation Division (CID) dated 06 October 2020.[2]

Facts

On 25 October 2018, CCFPI filed its initial breach report before the NPC regarding a data breach involving the Annual Physical Examination (APE) results of its thirty-nine (39) employees.[3] According to CCFPI, it engaged the services of ActiveOne Health, Inc. (ActiveOne), an occupational health services provider, for the periodic medical assessment of CCFPI's employees "to detect in time health risk factors and present ailments derived from the employees' work environment and lifestyle."[4]

In its initial report, CCFPI stated that:

> "ActiveOne provides delivery of the APE through onsite and offsite facilities using its network adjacent to CCFPI's sites. It is also obligated to collect, store and report on employee-patient information and the data collected must be in a format that is transferrable to CCFPI or their future clinical providers taking into account the best practices in the handling of data especially with respect to confidentiality. Moreover, records should be

[1] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc.
[2] *In re: Coca-Cola FEMSA Philippines, Inc.*, NPC BN 18-202, Order dated 06 October 2020.
[3] Breach Notification dated 25 October 2018 of Coca-Cola FEMSA Philippines, Inc., at p. 1.
[4] *Id.*, at p. 2.

> coded (using unique identifiers and illness using ICD codes) and entered into an electronic system."[5]

On 24 October 2018, ActiveOne notified CCFPI that some employees of the latter's Carlatan Sales Office requested for their APE results.[6] However, one of ActiveOne's nurses accidentally sent to twenty-five (25) recipients, who are also CCFPI employees, the Microsoft Excel file of the summary of APE results of its 39 employees.[7] The following day, the said nurse tried to recall her email, but failed to successfully recall all of them.[8]

According to CCFPI, there would be a likelihood of unauthorized disclosure of medical conditions of the thirty-nine (39) affected data subjects[9] whose personal data involve their employee numbers, names of the data subjects, personnel areas, company positions, gender, birth date, age, results of laboratory tests, medical check-up remarks and recommendations, and prescribed medications.[10] CCFPI stated that it intended to notify the affected data subjects within the prescribed period.[11]

Lastly, CCFPI's initial report contained statements on the safeguards it implemented to minimize or mitigate the impact of the incident which provide the following:

1. Clinic Operations Manual which provides for the standard APE procedure on the proper disposition and securing the confidentiality of the APE results.
2. ActiveOne's Academy On-boarding Orientation regarding CCFPU Processes which is provided to and required all of its Nurses and Doctors.
3. ActiveOne's Memorandum dated 05 October 2018 addressed to its Nurses and Doctors assigned to CCFPI concerning the Procedure for the Release of Records including APE results.
4. Soon after CCFPI was notified of the breach incident on 24 October 2018, CCFPI recalled the subject email communication of Nurse A and copies thereof were successfully deleted on the recipients' mailboxes.[12]

---

[5] *Id.*
[6] *Id.*
[7] Breach Notification dated 25 October 2018 of Coca-Cola FEMSA Philippines, Inc., at p. 2.
[8] *Id.*
[9] *Id.*, at p. 3.
[10] *Id.*, at pp. 3-4.
[11] Breach Notification dated 25 October 2018 of Coca-Cola FEMSA Philippines, Inc., at p. 4.
[12] *Id.*, at p. 3.

Moreover, CCFPI also stated its proposed measures to be taken to address the breach which are:

1. Subject Nurse A to disciplinary action under ActiveOne's Employee Discipline Policy.
2. Continuing education for all ActiveOne's Onsite Personnel on Data Privacy Law and ActiveOne's Internal Policies on Medical Data Confidentiality.
3. Include in ActiveOne's Clinic Process Manual a procedure on safeguarding electronic data by encryption.[13]

On 06 October 2020, the NPC's Complaints and Investigation Division (CID) issued an Order requiring CCFPI to submit a Full Report which contains the details provided under Rule V, Section 17 (D) of NPC Circular No. 16-03 (Personal Data Breach Management).[14]

On 18 November 2020, CCFPI moved for a 15-day extension for the submission of its Full Report stating that it is encountering difficulties in coordinating with ActiveOne due to the pandemic[15] which the CID granted in its 20 November 2020 Resolution.[16]

In compliance therewith, CCFPI, now Coca-Cola Beverages Philippines, Inc. (CCBPI) submitted its Full Report dated 03 December 2020 attaching therein documents to substantiate security measures it implemented to address the breach.[17]

Issue

Whether CCBPI sufficiently complied with the Order of NPC dated 06 October 2020.

Discussion

CCBPI sufficiently complied with the Order of NPC dated 06 October 2020. The Commission therefore resolves to close the instant case.

---

[13] *Id.*, at p. 4.
[14] *In re: Coca-Cola FEMSA Philippines, Inc.*, NPC BN 18-202, Order dated 06 October 2020, at pp. 1-2.
[15] Motion for Extension dated 18 November 2020 of Coca-Cola FEMSA Philippines, Inc.
[16] *In re: Coca-Cola FEMSA Philippines, Inc.*, NPC BN 18-202, Resolution dated 20 November 2020.
[17] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc.

I. The incident falls under the mandatory breach notification requirement.

Rule V, Section 11 of NPC Circular No. 16-03 provides:

> **Sec. 11. *When notification is required.*** Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:
>
> A. **The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.** For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
> B. There is **reason to believe that the information may have been acquired by an unauthorized person**; and
> C. The personal information controller or the Commission believes that the unauthorized acquisition is **likely to give rise to a real risk of serious harm to any affected data subject**.[18] (Emphasis supplied)

In its initial breach report, CCFPI stated that a nurse from ActiveOne accidentally sent the MS Excel file of the summary of APE results of 39 employees to 25 employees of CCFPI[19] which contained the employee numbers, names of the data subjects, personnel areas, company positions, gender, birthdate, age, results of laboratory tests (i.e. chest x-ray, fecalysis, complete blood count, urinalysis, dental examination, and blood chemistry), medical check-up remarks and recommendations, and prescribed medications.[20]

---

[18] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V,
§ 11 (15 December 2016) (NPC Circular 16-03).
[19] Breach Notification dated 25 October 2018 of Coca-Cola FEMSA Philippines, Inc., at p. 2.
[20] *Id.*, at pp. 3-4.

As defined under the Data Privacy Act of 2012 (DPA), sensitive personal information refers to personal information:

> (1) About an individual's race, ethnic origin, marital status, **age,** color, and religious, philosophical or political affiliations;
>
> (2) About an **individual's health**, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;[21] (Emphasis supplied)
>
> ...

Based on the definition, the APE results contained not only the names of the affected data subjects, but also sensitive personal information such as their birthdates, age, gender, and the results of laboratory tests, medical check-up remarks and recommendations, and prescribed medications. [22]

Further, the employee numbers, names of the data subjects, personnel areas, and company positions,[23] are considered other information that may be used to enable identity fraud, such as when a fraudster would identify himself or herself as an employee of CCFPI and whose medical records can be used to avail health care services or products that are covered by company medical programs. Thus, the first requisite of Section 11 of the Circular No. 16-03 is present in this case.

Moreover, CCFPI reported that such APE results were accidentally sent to different recipients other than the affected data subjects.[24] Even though the APE results were sent to employees of CCFPI, the said recipients were unauthorized to acquire the same. Thus, the second requisite is present considering that APE results were acquired by unauthorized persons.

---

[21] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter I, § 3(l) (2012).
[22] Breach Notification dated 25 October 2018 of Coca-Cola FEMSA Philippines, Inc., at pp. 3-4.
[23] *Id.*
[24] *Id.*, at p. 2.

Lastly, CCFPI stated in its initial report that there would be a likelihood of unauthorized disclosure of medical conditions of the affected data subjects.[25] The fact that the email containing the APE results was sent to other CCFPI employees and that the nurse who accidentally sent the same failed to recall such email, the incident may therefore give rise to a real risk of serious harm to the affected data subjects such as identity theft or fraud especially when claiming health care benefits. Thus, the third requisite is present in this case.

Considering that all the requisites under Section 11 of NPC Circular 16-03 are present in this case, CCFPI, as personal information controller, is mandated to notify the affected data subjects to allow them to take "the necessary precautions or other measures to protect themselves against the possible effects of the breach."[26]

However, CCFPI, now CCBPI, already implemented security measures to mitigate the harm and has notified the affected data subjects regarding the incident.

II. CCBPI has security measures in place to mitigate the breach and the recurrence of the incident; CCBPI sufficiently notified the affected data subjects of the breach.

In an Order dated 06 October 2020, the CID required CCFPI to submit a Full Report which contains the details provided under Rule V, Section 17 (D) of NPC Circular No. 16-03.[27] Among those required to submit are the description of the measures taken to address the breach and to recover the personal data that were compromised, actions performed to mitigate the possible harm and those taken to inform the affected data subjects of the breach, and the measures taken to prevent recurrence of the incident.[28]

---

[25] *Id.*, at p. 3.
[26] NPC Circular 16-03, rule V, § 18(A).
[27] *In re: Coca-Cola FEMSA Philippines, Inc.*, NPC BN 18-202, Order dated 06 October 2020, at pp. 1-2.
[28] *Id.*

In its Full Report dated 03 December 2020, CCBPI submitted necessary documents as proof of its compliance.[29]

According to CCBPI's Full Report, there were forty (40) employees whose APE results were inadvertently sent to 25 email recipients who are also employees of CCBPI,[30] causing a disclosure of a total number of six hundred forty (640) personal records.[31]

To minimize or mitigate the harm, it was reported that ActiveOne issued a Memorandum addressed to its nurses and doctors assigned to CCBPI about the process of releasing the records including APE results.[32] CCBPI also attached an affidavit of its former Data Protection Officer stating that "[u]pon receiving the report, [CCFPI] recalled the subject email communication of said nurse and copies thereof were successfully deleted from the recipients' mailboxes."[33]

CCBPI also submitted the affidavits executed by the affected data subjects stating that "[they] did not experience any negative effect or untoward incident due to the mistake committed by the ActiveOne nurse in sending the results of [their] to unintended recipients."[34]

Moreover, as to the measures taken to address the breach, CCBPI reported that ActiveOne subjected the concerned nurse to disciplinary action,[35] and that upon report of the breach, a subsequent investigation was conducted by ActiveOne's management.[36]

CCBPI also reported that ActiveOne conducts continuing education for all its personnel regarding DPA and ActiveOne's internal policies on Medical Data Confidentiality.[37] Further, ActiveOne, as a subsidiary of RellianceCARE, Inc., included in its Data Privacy Manual policies on the technical security measures procedure which include the use of systems to be used as monitoring security for breaches, the evaluation

---

[29] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc.
[30] *Id.*, at p. 1.
[31] *Id.*, at p. 2.
[32] *Id.*, referred to as Annex "A."
[33] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc., at p. 3; referred to
as Annex "B."
[34] *Id.*, at p. 2; referred to as Annexes "C" to "C-37."
[35] *Id.*, at p. 4.
[36] *Id.*
[37] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc., at p. 4.

of software applications prior to their installation in their computers or devices, the conduct of vulnerability assessments and penetration testing, and the encryption and authentication procedures it will implement to control and limit access to personal data.[38]

ActiveOne's Data Privacy Manual also provides policies on the physical security measures which contain procedures on data formatting, personal data storage, accessing by company personnel, monitoring and limitation of access to the storage facility, modes of transfer, retention, and disposal of personal data.[39]

To prevent the recurrence of the breach, CCBPI published its own Privacy Manual which contains provisions on security measures it shall implement in order to maintain the availability, integrity, and confidentiality of personal data.[40] As part of its "organizational security measures," CCBPI shall appoint its Data Protection Officer, conduct trainings and seminars regarding data privacy and security, and conduct of the Privacy Impact Assessment (PIA), among others.[41]

Also, as part of its "physical security measures," CCBPI provided procedures on the storage, access, monitoring, and transfer of personal data, among others.[42]

CCBPI's Privacy Manual also contains provisions on the creation of a data breach response team to endure immediate response and appropriate action in case of personal data breach.[43] CCBPI also stated it shall regularly conduct a PIA to identify the risks in the processing system.[44] Lastly, the Privacy Manual of CCBPI also contains a procedure for recovery and restoration of personal data, a notification protocol to the company's management, NPC and the data subjects, and a procedure on the documentation and report of security incidents or personal data breach.[45]

---

[38] *Id.*, referred to as Annex "E," at pp. 24-26.
[39] *Id.*, at pp. 20-23.
[40] *Id.*, at p. 5; referred to as Annex "G," at p. 12.
[41] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc., at p. 5; referred to
as Annex "G," at pp. 12-13.
[42] *Id.*, at pp. 13-15.
[43] *Id.*, at p. 18.
[44] *Id.*, at p. 19.
[45] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines. Inc., at p. 5; referred to
as Annex "G," at pp. 19-20.

Furthermore, CCBPI attached in its Full Report screenshots of a communication released by its Office of Internal Control regarding data labels and electronic mail classification,[46] and of the "Drops of Knowledge"[47] which the CCBPI launched containing Data Privacy trainings used as a mandatory compliance requirement for all CCBPI associates.[48]

Finally, as to the actions taken to inform the affected data subjects, CCBPI was able to promptly notify the 40 employees affected by the breach, as proven by notification letters dated 25 October 2018 sent to them.[49] In the said notification letters, CCBPI explained how the breach occurred, the safeguards it took to minimize or mitigate the risk of the incident, and the actions it implemented and will implement "to decrease the likelihood of a similar incident from happening again."[50] Such action taken to notify the affected data subjects is deemed by the Commission as sufficiently compliant with the mandatory notification requirement and the contents thereof under NPC Circular 16-03.

It is in these types of cases where sensitive personal information and other information that, under the circumstances, may enable identity fraud are involved, the Commission repeatedly reminds the personal information controllers (PICs) and processors (PIPs) of their obligation under the DPA to promptly notify the affected data subjects of a personal data breach[51] in order for them to take necessary actions "to protect themselves against the possible effects of the breach."[52]

Following the principle of proportionality under the DPA and its Implementing Rules and Regulations, the "processing of information

---

[46] *Id.*, referred to as Annex "H."
[47] *Id.*, referred to as Annex "I."
[48] *Id.*
[49] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc., at p. 4; referred to
as Annexes "F" to "F-39."
[50] *Id.*
[51] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter V, § 20 (f) (2012).
[52] NPC Circular 16-03, rule V, § 18(A).

shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose."[53]

Necessarily, to avoid further recurrence of this incident as well as to comply with the proportionality principle, CCBPI's access to its employees' periodic medical assessment should be limited to the physician's evaluation of whether an employee is "fit to work" instead of providing the specific laboratory results of the APE. Such evaluation may be seen in a medical certificate issued to the employees upon their request, as to ensure the confidentiality of the medical records of CCBPI's employees.

WHEREFORE, premises considered, this Commission resolves that the matter on NPC BN 18-202 "In re: Coca-Cola FEMSA Philippines, Inc." is hereby considered **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
19 October 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

---

[53] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter III, § 11 (2012); *see also* Implementing Rules and Regulations of the Data Privacy Act of 2012, rule IV, § 18(c) (2016).

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

EB
Data Protection Officer

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: HC CONSUMER FINANCE PHILIPPINES, INC. **NPC BN 18-199**

x----------x

RESOLUTION

NAGA, P.C.:

This Resolution refers to the Breach Notification dated 23 October 2018 of HC Consumer Finance Philippines, Inc. (HC).

Facts

On 23 October 2018, HC Consumer Finance Philippines, Inc. notified the National Privacy Commission (Commission) through a letter regarding a breach incident involving its sales agent, FM (FM). [1] In its report, HC stated that FM processed the loan application of RBB (RBB) at AVR Full Hauz Furniture Inc. – Roxas City which was subsequently approved. On 10 September 2018, FM resigned from HC.[2]

Thereafter, on 14 September 2018, HC's Investigation Security Support Team detected a possible identity theft.[3] The investigation was prompted by a report filed by RBB regarding the loan collection efforts of HC. [4] In its investigation, it showed that RBB did not continue with her approved loan application instead FM had "colluded with another person to continue" the said loan application.[5] Accordingly, an "unidentified individual claimed the

[1] Letter dated 23 October 2018 "Identity Theft dated May 01, 2018 of Data Breach Notification No. 2018-003" from HC Consumer Finance Philippines, Inc.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] Letter dated 23 October 2018 "Identity Theft dated May 01, 2018 of Data Breach Notification No. 2018-003" from HC Consumer Finance Philippines, Inc.

commodity subject of the loan" and someone is paying for the installments of the loan amount.[6] HC has also concluded that the incident was an identity theft.[7]

In its report, HC stated that FM was already reported in the Human Resource-Employee Relation and that he is ineligible for rehire.[8] It also stated that it is assessing the incident and filing a criminal complaint against FM.[9] Further, to address the breach, HC stated that their retailers were being oriented to verify by matching the clients' faces and names with the documents presented before releasing the commodity of the loan.[10] As an additional measure to prevent any fraud, a photo of the client holding the welcome kit and the commodity is being taken.[11] Lastly, HC's Back Office Team was tasked to cross-check the photo with the documents submitted.[12]

On 26 October 2020, the Commission, through its Complaints and Investigation Division (CID), issued an Order directing HC to submit its "Full Report expounding the details of the incident with emphasis supplied on the lacking information from the initial notification" dated 23 October 2018.[13]

On 04 November 2020, HC submitted its compliance to the Order dated 26 October 2020.[14] In its Updated Report on Identity Theft, HC stated that it called RBB on 14 September 2018 to collect the loan, however, the latter insisted that she does not have any loan and that despite the approval of the loan, RBB backed out of the loan application and paid in full amount in cash for the videoke set she purchased.[15]

---

[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] Letter dated 23 October 2018 "Identity Theft dated May 01, 2018 of Data Breach Notification No. 2018-003" from HC Consumer Finance Philippines, Inc.
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Order dated 26 October 2020
[14] Letter dated 04 November 2020 "Updated Report on Identity Theft (NPC BN-199)" from HC Consumer Finance Philippines, Inc.
[15] *Id.*

Further, HC stated that based on its internal investigation it "showed that the sales agent continued processing the loan and released the commodity covered by such loan to an unknown person, in clear violation of the client's authorization and Home Credit policies and procedure.[16]

HC also stated there is one data subject and the personal information involved in the incident are "name, address, mobile number, marital status, age, educational attainment, National Senior Citizens Card and voter's ID" which were collected in compliance with the Know-Your -Customer (KYC) rules provided by the Bangko Sentral ng Pilipinas.[17]

HC also claimed that it already notified the affected data subject, and her contact information was already deleted.[18] It also claimed that there was no loss of control over the personal data involved and that there was no disclosure to an unauthorized person.[19]

On 23 April 2022, the NPC CID issued an Order directing HC to submit a Post-Breach Report.[20]

On 11 May 2022, HC submitted its compliance to the Order dated 23 April 2022.[21] In its submission, HC attached a copy of its Contract Receiving, Registration and Archiving Work Instruction, Data Privacy Manual and Partner Privacy Manual, Access Control Management Manual, Policy on IT Security Management, Policy on IT Acceptable Use, a copy of its 2021 Annual Data Privacy Training, notification issued to the affected data subject, and a screenshot photo to proof that the information of RBB was indeed deleted in HC's system.[22]

---

[16] *Id.*
[17] *Id.*
[18] Letter dated 04 November 2020 "Updated Report on Identity Theft (NPC BN-199)" from
HC Consumer Finance Philippines, Inc.
[19] *Id.*
[20] Order dated 23 April 2022
[21] Electronic Mail from HC Consumer Finance Philippines, Inc. dated 11 May 2022
[22] *Id.*

On 12 July 2022, the NPC CID issued an Order directing HC to submit its Supplemental Post-Breach Report.[23]

On 01 August 2022, HC Submitted its Compliance to the Order dated 12 July 2022. [24] HC has submitted its proof of the implementation of the remedial measures it took after the incident such as its retailer's orientation on verifying the client's face and its submitted documents, photo of its clients holding the welcome kit and commodity of the loan, and its Back Office Team in cross- checking the documents submitted and the photo of the client holding the commodity.[25] Lastly, HC has submitted its proof of sending of data subject notification.[26]

Issue

Whether HC has sufficiently addressed the breach and implemented appropriate measures pursuant to NPC Circular 16- 03 (Personal Data Breach Management).

Discussion

The Commission deems it proper to close and terminate the case.

HC complied with the directives of the Commission. It has implemented sufficient security measures to address the incident and notified the affected data subject.

As to the security measures it implemented, HC's agents were reoriented to verify the client's face by matching the submitted documents before releasing the subject commodity of approved loans. The photos of the clients holding the welcome kit and the

[23] Order dated 12 July 2022
[24] Letter dated 01 August 2022 "Supplemental Post-Breach Report on NPC BN 18-199" from HC Consumer Finance Philippines, Inc.
[25] *Id.*
[26] *Id.*

commodity were also taken as additional measures to prevent any other fraudulent schemes.[27]

Further, HC has notified the affected data subject following Rule V, Section 18 (C) and (D) NPC Circular 16-03.

> **SECTION 18.** ***Notification of Data Subjects***. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> *C. Content of Notification.* The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;
> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
> 6. any assistance to be provided to the affected data subjects.
>
> Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.
>
> *D. Form*. **Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach**: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are

[27] *Id.*

> informed in an equally effective manner: *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach. [28] (Emphasis Supplied)

In its data subject notification sent through a letter via the registered mailing address of the affected data subject, HC informed RBB of the incident as a precautionary measure. [29] It also stated in its notification that the latter's data such as "date of birth, home address, permanent address, email, landline, mobile number, and identity contact numbers" were involved in the incident.[30]

Furthermore, HC has deleted the contact information of RBB to prevent any further notification regarding the loan. To mitigate any potential harm that might arise from the incident, HC also reminded RBB to take necessary precautions in addition to the measures it will implement.[31]

Additionally, HC provided its Customer Service Hotline and an email address to report any unauthorized or suspicious activity involving the personal data of RBB.[32] However, HC stated in its Supplemental Post Breach Report dated 01 August 2022, that it did not receive any inquiries or responses from RBB. [33]

As to the notification to the Commission, HC submitted its full breach report dated 04 November 2020. Rule V, Section 17 (D) of the NPC Circular 16-03 provides:

> *D. Content of Notification.* The notification shall include, but not be limited to:
>
> 1. Nature of the Breach

[28] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18 (C) (D) (15 December 2016) (NPC Circular 16-03).
[29] Letter dated 23 October 2018, from HC Consumer Finance Philippines, Inc. (Data Subject Notification) Annex (I)
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] Letter dated 01 August 2022 "Supplemental Post-Breach Report on NPC BN 18-199" from HC Consumer Finance Philippines, Inc.

a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
b. a chronology of the events leading up to the loss of control over the personal data;
c. approximate number of data subjects or records involved;
d. description or nature of the personal data breach;
e. description of the likely consequences of the personal data breach; and
f. name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved
    a. description of sensitive personal information involved; and
    b. description of other information involved that may be used to enable identity fraud.
3. Measures Taken to Address the Breach
    a. description of the measures taken or proposed to be taken to address the breach;
    b. actions being taken to secure or recover the personal data that were compromised;
    c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
    d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
    e. the measures being taken to prevent a recurrence of the incident.

The Commission reserves the right to require additional information, if necessary.[34]

In the submitted Full Breach Report dated 04 November 2020, HC classified the incident as a personal data breach arising from a violation of its policies and procedures. [35] It also reiterated the chronological event of the incident and stating on how the breach transpired and claimed that only RBB, was affected by the incident.[36]

[34] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 17(D) (15 December 2016) (NPC Circular 16-03).
[35] Letter dated 04 November 2020 "Updated Report on Identity Theft (NPC BN-199)" from HC Consumer Finance Philippines, Inc.
[36] *Id.*

HC asserted that there is no indication of loss of control over the personal data and disclosure to an unauthorized person.[37] It stated that it has also "absorbed the financial impact of the fraud by cancelling collections activities and writing off the debt" as a result of the unauthorized processing of the loan.[38]

In addition, HC also provided in its report the measures it took to address the breach, including the conduct of orientation on verifying the identities of its clients with its submitted documents before releasing the commodity.[39] It also stated that it provided data subject assistance by notifying RBB of the incident, deleting the contact information to prevent any further notification regarding the loan, and to report any suspicious activity which may involves her personal data.[40]

Subsequently, HC also submitted its Supplemental Post-Breach Report dated 01 August 2022. [41] It provided the proof of implemented measures it undertook after the incident including orientation on its employees in verifying the identities of its clients, proof of data subject and notification, and other related documents in addressing the breach incident. [42] HC also submitted the presentation of trainings it provided to its employees in verifying the identity of its customers and manual of procedures on reporting data breach incidents.[43]

Moreover, HC stated that there was a same investigation report from their Anti-Fraud Department and Compliance Department.[44] It further stated that it treated the incident as a case of internal fraud,

---

[37] *Id.*
[38] *Id.*
[39] Letter dated 04 November 2020 "Updated Report on Identity Theft (NPC BN-199)" from
HC Consumer Finance Philippines, Inc.
[40] *Id.*
[41] Letter dated 01 August 2022 "Supplemental Post-Breach Report on NPC BN 18-199" from
HC Consumer Finance Philippines, Inc.
[42] *Id.* (Annex A and Annex H)
[43] *Id.* (Annex A and Annex H)
[44] *Id.*

considering that there is similar finding with its Investigation Security Support.[45]

Thus, HC has sufficiently complied with the notification requirements pursuant to NPC Circular No. 16-03 in compliance with the directives of the Commission as indicated in its Orders dated 26 October 2020, 23 April 2022, and 12 July 2022.

Considering the foregoing, the Commission finds that since HC has already complied with the directives of the Commission and has already complied with NPC Circular 16-03 (Personal Data Breach Management), it deems it proper to close and terminate the case.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-199 "In re: HC Consumer Finance Philippines, Inc. is hereby considered **CLOSED**.

SO ORDERED.

Pasay City, Philippines.
17 August 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

[45] Letter dated 01 August 2022 "Supplemental Post-Breach Report on NPC BN 18-199" from HC Consumer Finance Philippines, Inc.

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy Furnished:

RBP
Data Protection Officer
HC CONSUMER FINANCE PHILIPPINES, INC.

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISON
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: ELS LANGUAGE SERVICES, INC.

NPC BN 18-194

x----------x

RESOLUTION

NAGA, *P.C.;*

Before the Commission is the Compliance submitted by ELS Language Services, Inc. (ELS) dated 28 October 2020 in accordance with the Order dated 13 October 2020.

Facts

ELS is a company organized and existing in the United States of America which provides English language training and instructions.[1] On 04 October 2018, it appointed ACCRLAW and/or any of its lawyers as its Attorney-In-Fact, through a Special Power of Attorney executed by PHW, its Vice President, General Counsel, and Secretary.[2]

On 11 October 2018, ELS, through ACCRALAW, notified the Commission that a possible security incident involving one (1) of its customers in the Philippines had occurred, attaching therein a letter dated 04 October 2018, detailing said incident.[3]

In its letter, ELS narrated that it learned from the Federal Bureau of Investigation (FBI) that a former employee of ELS Santa Monica, in California, United States, has been arrested and charged in connection with a conspiracy to launder funds derived from Business Email Compromise fraud schemes.[4]

---

[1] Electronic Mail dated 11 October 2018 from ELS Language Services, Inc.
[2] Special Power of Attorney, Attachment to Electronic Mail dated 11 October 2018 from ELS Language Services, Inc.
[3] Electronic Mail dated 11 October 2018 from ELS Language Services Inc.
[4] ELS Letter to NPC, Attachment to Electronic Mail dated 11 October 2018 from ELS Language Services, Inc.

ELS alleged that the incident probably occurred between April 2017 and 22 August 2018, the period during which the former employee was working for it and was responsible for processing credit card information.[5] Nonetheless, the latest information ELS received from the FBI revealed that no information from any Philippine resident was affected or involved in the incident.[6]

However, during the period in question, ELS processed credit card payments made by approximately three thousand five hundred (3,500) customers that involve student records, including: customer's first and last name, passport number, photograph, email address, mailing address, billing address, and credit or debit card information as well as its security code.[7]

According to ELS, it is cooperating with the FBI and other law enforcement agencies while also conducting its own investigation "to identify the customers and personal data categories affected by the incident and to determine how it might improve their practices to prevent similar instances in the future."[8]

Thus, on 10 September 2018, ELS was able to notify the potentially affected data subjects through mail.[9] ELS recommended therein that they contact their bank or credit card provider promptly to dispute charges they feel may have been unauthorized, inform them of an FBI investigation of criminal activity, and request immediate re-issuance of their credit card.[10]

In addition, ELS informed them that it is prepared to offer twelve (12) months of free credit monitoring and fraud detection to potentially affected customers who suspect fraudulent activity on their credit card or bank account.[11]

---

[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] ELS Letter to NPC, Attachment to Electronic Mail dated 11 October 2018 from ELS Language Services, Inc.
[9] Personal Data Breach Report of ELS Language Services, Inc., dated 28 October 2020.
[10] ELS Letter to NPC, Attachment to Electronic Mail dated 11 October 2018 from ELS Language Services, Inc.
[11] *Id.*

On 13 October 2020, the Commission, through its Complaints and Investigation Division, ordered ELS to submit a Full Breach Report, describing the nature of the breach, personal data possibly affected, and measures taken to address the breach.[12]

On 28 October 2020, ELS submitted its Personal Data Breach Report in compliance with the abovementioned Order, reiterating its previous submissions and expounding on the measures it took to address the breach, namely:

> a. ELS implemented a number of measures in response to the breach to secure credit card information across its enterprise, including in store audits, purging of all credit card data and re- examination of all background check procedures;
>
> b. Law enforcement was notified and the U.S. Attorney's office was involved in the prosecution of the individual responsible for the theft;
>
> c. Affected individuals were offered 12 months of free credit monitoring and provided detailed instruction on how to monitor credit reporting and how to report criminal activity to law enforcement.
>
> d. Affected individuals were notified by mail on September 10, 2018;
>
> e. As a result of this incident credit card processing has been outsourced to eliminate the risk or physical/electronic access. Additionally, access to sensitive student information is based upon least-privilege and need-to-know. ELS continues to monitor need to for additional control measures as necessary.[13]

Issue

Whether ELS has sufficiently complied with the Commission's Order
dated 13 October 2020.

Discussion

---

[12] In re: ELS Language Services, Inc., NPC BN 18-194, Order to Submit Full Breach Report, 13 October 2020.
[13] Personal Data Breach Report of ELS Language Services, Inc., dated 28 October 2020.

The Commission finds that ELS has sufficiently complied with the Order dated 13 October 2020. As such, the Commission resolves to terminate the investigation and consider the matter closed.

Section 18 (D), NPC Circular 16-03 provides how notification shall be made, to wit:

> **Section 18. *Notification of Data Subjects.***
>
> D. *Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach:** Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[14]

Whenever a personal data breach occurs, the personal information controller (PIC), shall identify the data subjects who are affected by the breach and shall notify all of them individually using secure means of communication.[15]

In this case, despite the FBI's finding that no resident of the Philippines was on the list of individuals whose credit card information was compromised, ELS still notified the potentially affected customers through mail on 10 September 2018 as a precautionary measure because at the time of the incident, ELS processed credit card payments made by approximately three thousand five hundred (3,500) customers.[16]

---

[14] National Privacy Commission, Personal Data Breach Management, NPC Circular 2016-03, rule V, § 18 (D) (15 December 2016) (NPC Circular 16-03).

[15] RPR vs. Edukasyon.ph, NPC 19-438, Resolution dated 22 September 2022, at p. 4.

[16] ELS Letter to NPC, Attachment to Electronic Mail dated 11 October 2018 from ELS Language Services, Inc.

On this note, the Commission emphasizes the importance of ensuring that affected data subjects receive timely notification, viz:

> The purpose of the requirement to notify data subjects of a breach incident is to give them the opportunity to take the necessary precautions or such other measures to protect themselves against possible effects of the breach. Personal information controllers (PICs) are likewise required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. A delay in notification can cause harm to affected data subjects as they cannot protect themselves from the consequences of the breach.[17]

Moreover, to further comply with the Commission's Order dated 13 October 2020, ELS undertook the following measures to protect the personal information of its potentially affected data subjects, to wit:

> 1. It audited its stores, purged credit card data and re-examined its background check procedures;
> 2. It notified the law enforcement and the US Attorney's Office was involved in the prosecution of the individual responsible for the theft;
> 3. Affected individuals were offered 12 months of free credit monitoring and provided instruction on how to monitor credit reporting and how to report criminal activity to law enforcement;
> 4. Affected individuals were notified by mail on September 10, 2018;
> 5. Credit card processing was outsourced to eliminate the risk of physical/electronic access;
> 6. It also cooperated with the FBI and other law enforcement agencies in the investigation and conducted its own investigation to identify individuals affected by the incident and to determine how it can improve its operation to prevent similar recurrence;
> 7. Notified this Commission;
> 8. Designation of a Data Protection Officer (DPO), RT.[18]

In this regard, Section 20 (a) of the Data Privacy Act of 2012 provides:

> Sec. 20. *Security of Personal Information.*
> (a) The personal information controller must implement reasonable and appropriate organizational, physical, and

---

[17] In Re BPI Philam Life Assurance Corporation, NPC BN 21-054, Order dated 15 April 2021, at p. 3.
[18] Final Breach Notification Evaluation Report, 12 December 2022, at 6, in In Re ELS Language Services, Inc., NPC BN 18-194 (NPC 2018).

> technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[19]

Furthermore, as also emphasized in Section 4 (B) of NPC Circular 16- 03:

> **SECTION 4. *Security Incident Management Policy.*** A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:
>
> B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident.[20]

The implementation of the abovementioned measures after the security incident had occurred, as well as the notification made by ELS on its own initiative, demonstrated its diligence and commitment to protect the rights of its data subjects and abide by the DPA and its existing rules and regulations.

These are reasonable and appropriate remediation measures to address and correct the incident which can otherwise lead to issues arising from the use of personal data by any person not authorized to access it.

Hence, ELS was able to mitigate the risks caused by the incident through its existing security measures and the notification it sent to the potentially affected data subjects.

In view of the foregoing, the Commission holds that ELS Language Services Inc. had sufficiently notified the potentially affected data

---

[19] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, Chapter V, § 20 (a) (2012) (Data Privacy Act of 2012).

[20] NPC Circular 16-03, rule II, § 4 (B).

subjects and it has implemented reasonable and appropriate security measures to prevent a recurrence of the incident.

WHEREFORE, premises considered, the Commission resolves that the matter of NPC BN 18-194 "In re ELS Language Services, Inc." is hereby **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
17 August 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

RT
Chief Operating Officer & Data Protection Officer

JMG
MML
Attorney-In-Fact for ELS Language Services, Inc.

COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

SPOUSES LTG AND CIG,

Complainant,

NPC 21-095
For: Violation of the Data Privacy Act of 2012

- versus -

LSR,

Respondent.

x----------x

RESOLUTION

NAGA, P.C.:

Before this Commission is the Motion for Reconsideration dated 25 October 2022 filed by Spouses LTG and CIG (Complainants) on the Decision dated 28 July 2022 which dismissed their Complaint against LSR (Respondent) for lack of merit.

Facts

The Commission issued a Decision dated 28 July 2022, dismissing the Complaint filed by the Complainants, with the following dispositive portion:

> **WHEREFORE,** premises considered, the Complainants filed by SPOUSES LTG and CIG against LSR is hereby **DISMISSED** for lack of merit.
>
> **SO ORDERED.**[1]

[1] Spouses LTG and CIG v. LSR, NPC 21-095, Decision dated 28 July 2022 at p. 22.

On 13 October 2022, Complainants received the Decision through electronic mail.[2] Subsequently, Complainants filed their Motion for Reconsideration (MR) dated 25 October 2022.[3]

In their MR, Complainants stated that the Respondent's act of issuing the subject certification does not fall under the exception of Section 13(f) of Data Privacy Act of 2012 (DPA).[4] According to Complainants, Respondent has the burden of proof to show that her act of issuing the subject certification to JMB (JMB) is an exception to the strict provision, which Respondent failed to do.[5]

Complainants emphasized that to fall under the exception in Section 13(f) of DPA, there must be an ongoing court proceeding at the time the processing of the sensitive personal information was done.[6] With this, Complainants argued that there was no ongoing court proceeding when the Respondent issued the subject certification to JMB.[7]

Moreover, Complainants cited Section 38 of DPA which provides that when there is doubt in the interpretation thereof shall be "liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed."[8]

Complainants also alleged that Respondent cannot hide behind the presumption of regularity in the exercise of her function.[9] Since Respondent is the "keeper of records containing people's sensitive personal information, x x x [R]espondent should have been mindful of the rights and interests of complainants whose personal information shall be processed."[10]

---

[2] Motion for Reconsideration dated 25 October 2022 of Spouses LTG and CIG, ¶1.
[3] Motion for Reconsideration dated 25 October 2022 of Spouses LTG and CIG.
[4] *Id.*, at p. 2
[5] *Id.*, at p. 2
[6] *Id.*, at p. 2
[7] Motion for Reconsideration dated 25 October 2022 of Spouses LTG and CIG, ¶5.
[8] *Id.*, ¶6.
[9] *Id.*, ¶7.
[10] *Id.*

Lastly, Complainants stated that if sensitive personal information shall be used in a court proceeding, "a proper *subpoena duces tecum* shall have been issued by a proper Court."[11]

Thus, Complainants prayed that the Commission reconsider and set aside its Decision dated 28 July 2022 dismissing the instant complaint, and to find Respondent guilty of having violated the provisions of
R.A. 10173 or the DPA.[12] Complainants also prayed for the imposition of appropriate penalty and order Respondent to indemnify them for damages as may be provided for by the DPA.[13]

On 10 November 2022, the Commission issued an Order requiring Respondent to comment on the MR filed by the Complainants.[14]

On 29 December 2022, Respondent filed its Comment/Opposition to the Complainant's Motion for Reconsideration.[15]

In its Comment, Respondent argued that the grounds in Complainants' MR is a mere rehash of their arguments and that the "Complainants failed to raise new matters substantially plausible or compellingly persuasive to warrant its desired course of action."[16]

Respondent countered that the case falls under the exception set forth by the DPA where consent of the Complainants is not necessary.[17] Respondent cited the case of EA and TA v. EJ, EE and HC, where this Commission ruled that "processing, as necessary for the establishment of legal claims" does not require an existing court proceeding.[18]

In addition, Respondent did not agree with the Complainants' argument that the former cannot hide behind the presumption of regularity in the exercise of her function.[19] Respondent added that this

---

[11] Motion for Reconsideration dated 25 October 2022 of Spouses LTG and CIG, ¶7.
[12] *Id.*, at pp. 4-5.
[13] *Id.*, at p. 5.
[14] Spouses LTG and CIG v. LSR, NPC 21-095, Order dated 10 November 2022 at p. 3.
[15] Comment/Opposition dated 29 December 2022 of LSR.
[16] *Id.*, at p. 2.
[17] *Id.*, at p. 3.
[18] EA and TA v. EJ, EE and HC, Resolution dated 15 July 2019.
[19] Comment/Opposition dated 29 December 2022, at p. 6.

argument of Complainant was already discussed in the Decision of the Commission dated 28 July 2022.[20]

Lastly, Respondent argued that her action does not exhibit irregularities that would overthrow the presumption of regularity, and the Complainants failed to provide clear and convincing evidence to overcome this presumption.[21]

Thus, Respondent prayed that the Commission deny Complainants' MR.[22]

Issue

Whether the Motion for Reconsideration filed by the Complainants should be granted.

Discussion

The Commission resolves to deny the Motion for Reconsideration filed by the Complainants.

Complainants alleged that in order for the processing should be necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, as provided in Section 13(f) of DPA, there must be an ongoing court proceeding at the time processing of the sensitive personal information was done.[23] Section 13(f) of DPA provides:

> SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> xxx
>
> (f) The processing concerns such personal information as is **necessary** for the protection of lawful rights and interests of

[20] *Id.*, at. p. 6.
[21] *Id.*, at. p. 6.
[22] *Id.*, at p. 7.
[23] Motion for Reconsideration dated 25 October 2022 of Spouses LTG and CIG, at p. 2.

> natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.[24]

Complainants stated that when JMB requested the subject certification there was no case filed.[25] Hence, Complainants believe that the instant case does not fall under the exception provided in Section 13(f) of the DPA.[26]

In the case of *EA and TA vs. EJ et. al,* this Commission ruled that the application of Section 13(f) of the DPA does not require existing court proceedings.[27] This Commission held that:

> On this matter, it must be clarified that the Data Privacy Act makes a distinction between the three instances where Section 13(f) is applicable, namely: (a) The processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings; (b) The processing is necessary for the establishment, exercise or defense of legal claims; or (c) The processing concerns personal information that is provided to government or public authority.
>
> xxx
>
> After all, the very idea of "establishment ... of legal claims" presupposes that there is still no pending case since a case will only be filed once the required legal claims have already been established.
>
> In addition, the use of the qualifier "necessary" in the law should be understood to apply not just to the "protection of lawful rights and interests of...persons in court proceedings" but also to the "establishment... of legal claims."
>
> The DPA should not be seen as curtailing the practice of law in litigation. Considering that it is almost impossible for Congress to determine beforehand what specific data is "necessary" or may or may not be collected by lawyers for purposes of building a case, applying the qualifier "necessary" to the second instance in Section 13(f) therefore, serves to limit the potentially broad

---

[24] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter III, § 13(f) (2012).

[25] Motion for Reconsideration dated 25 October 2022 of Spouses LTG and CIG, at p. 3.

[26] *Id.*, at p. 2.

[27] EA and TA vs. EJ, EE, and HC, NPC 17-018, Decision dated 15 July 2019, at p. 8.

> concept of "establishment of legal claims" consistent with the general principles of legitimate purpose and proportionality.
>
> As regards legitimate purpose, the Implementing Rules and Regulations (IRR) of the Data Privacy Act provides that the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. This means that the processing done for the establishment of a legal claim should not in any manner be outside the limitations provided by law. The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.[28]

Based on the foregoing, the Respondent's act of issuing the subject certification is within the ambit of Section 13(f) of DPA.

To reiterate, JMB' purpose for requesting the subject Certification is to attach the same to the civil case he filed against the Complainants. The issuance of a Certification containing the marriage details of the Complainants is necessary for the establishment, exercise, or defense of legal claims in the civil case against them. Thus, such issuance of the Certification by the Respondent is considered valid processing even though a court proceeding has yet to be filed by JMB.

Moreover, Complainants noted that the crux of the DPA is for the protection and safeguarding of a person's sensitive personal information.[29] With this, they stated that when there is doubt in the interpretation of the provisions of DPA, it shall be liberally interpreted in favor of the data subject.[30] Complainant cited Section 38 of DPA which provides:

> SEC. 38. Interpretation. – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.[31]

---

[28] *Id.*, at p. 7.

[29] Motion for Reconsideration dated 25 October 2022 of Spouses LTG and CIG, at p. 3.

[30] *Id.*

[31] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter IX, § 38 (2012).

The Supreme Court held that the cardinal rule in statutory construction is that when the law is clear and free from any doubt or ambiguity, there is no room for construction or interpretation.[32] There is only room for application.[33]

Complainants argued that Respondent cannot hide behind the presumption of regularity in the exercise of her functions.[34] Further, Complainants alleged that as keeper of the records containing sensitive personal information of data subjects, Respondent should have been mindful of the rights and interests of the former whose personal information shall be processed.[35] They added that Respondent may only issue the subject Certification when there is a proper subpoena *duces tecum*.[36]

To reiterate the previous discussion of this Commission in the Decision dated 28 July 2022:

> Respondent's actions do not exhibit irregularities that would overthrow the presumption of regularity and Complainants failed to provide clear and convincing evidence to overcome this presumption. Thus, the presumption of regularity of official acts must stand. Respondent cannot be faulted for issuing the Certification.[37]

In the instant case, the Complainants failed to provide clear and convincing evidence in its Motion for Reconsideration that would overthrow the presumption of regularity.

Moreover, the Complainants' argument that the subject Certification may only be issued when there is a proper subpoena *duces tecum* does not hold water.

As defined by the Rules of Court, [s]ubpoena *duces tecum* is a court process directed to a person requiring him or her "to bring with him

---

[32] CSB vs. DTB, G.R. No. 186400, 20 October 2010.
[33] *Id.*
[34] Motion for Reconsideration dated 25 October 2022 of Spouses LTG and CIG, at p. 4.
[35] *Id.*
[36] *Id.*
[37] Spouses LTG and CIG v. LSR, NPC 21-095, Decision dated 28 July 2022, at p. 17.

or her any books, documents, or other things under his or her control."[38]

The processing of sensitive personal information is lawful for the establishment, exercise or defense of legal claims which does not require court proceedings under Section 13(f) of the DPA. Thus, given that an existing case is not required, thenthe issuance of a subpoena *duces tecum* by the proper court is likewise not required to process sensitive personal information under Section 13 (f) of the DPA for the same reasons.

Overall, an examination of the issues raised in the Motion for Reconsideration reveals that the same are a mere rehash of the issues raised in the Complaint and Memorandum of the Complainants and which were already exhaustively passed upon, duly considered, and resolved by this Commission in its Decision dated 28 July 2022.

WHEREFORE, premises considered, this Commission resolves to **DENY** the Motion for Reconsideration dated 25 October 2022 filed by Complainants Spouses LTG and CIG. The Decision dated 28 July 2022 is hereby **AFFIRMED.**

SO ORDERED.

City of Pasay,
Philippines.
19 January 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE

[38] Amendments to the 1997 Rules of Civil Procedure [Rules of Court], A.M. No. 19-10-20-SC 2019, Rule 21, § 1 (2019).

Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

SPOUSES LTG and
CIG
Complainant

ACF
Counsel for Complainants

LSR
Respondent

DMP
Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

TGM,

Complainant,

-versus-

EDM, EAS, and MCN,

Respondents.

x----------x

NPC 18-G-077

For: Violation of the Data Privacy Act

RESOLUTION

NAGA, *P.C.;*

Before the Commission is a Motion for Reconsideration dated 10 June 2021 (Motion) filed by TGM (TGM).[1]

Facts

The Commission issued a Decision dated 15 April 2021 dismissing the Complaint filed by TGM against EDM, EAS, and MCN (Respondents).[2] The said Decision disposed of as follows:

> **WHEREFORE**, all the above premises considered, the Complaint is hereby **DISMISSED** for lack of merit**.**
>
> This is without prejudice to the filing of appropriate civil, criminal, or administrative cases against Respondent before any other forum or tribunal, if any.[3]

---

[1] Motion for Reconsideration dated 10 June 2021 of TGM.
[2] NPC 18-077 (*unreported*), Decision dated 15 April 2021.
[3] *Id.*, at p. 11.

TGM filed her Motion dated 10 June 2021, reiterating the arguments alleged in her Complaint. In her Motion, TGM argued that "[t]he share capital account is classified as sensitive personal information" hence, "[l]egitimate [r]easons" rule does not apply.[4] TGM stated that Section 3(l) of the Data Privacy Act of 2012 (DPA) is not exclusive, emphasizing on the phrase "**but not limited to**," under paragraph 3 of the said provision.[5]

TGM further argued that the Commission "extended the meaning of "health records" to medical records kept by publicly-listed corporation notwithstanding the original tenor of Section 3(l) referring to health records issued by "government agencies" citing Advisory Opinion No. 2019-010.[6]

Moreover, TGM stated that the parties sufficiently established in their pleadings that shared capital accounts are sensitive personal information.[7] According to TGM, the pleadings submitted to the Commission stated that the share capital account contains sensitive personal information, including deposits, withdrawals, and other loan details.[8] Thus, she argued that the share capital account should be considered as a financial record that is confidential and sensitive information.[9]

TGM concluded that the "legitimate interests" rule is not applicable in this case as its applicability is limited to the processing of personal information pursuant to Section 12 of the DPA.[10]

Lastly, TGM stated in her Motion that Respondents violated her right to be informed of the processing of her information, which is tantamount to unauthorized processing of information under Section 25 of the DPA.[11]

---

[4] Motion for Reconsideration dated 10 June 2021 of TGM, at p. 2.
[5] *Id.*, at p. 3.
[6] *Id.*
[7] *Id.*
[8] Motion for Reconsideration dated 10 June 2021 of TGM, at pp. 3-4.
[9] *Id.*, at p. 4.
[10] *Id.*
[11] *Id.*, at p. 5.

Therefore, TGM prayed for the Commission to reverse and set aside the Decision dated 15 April 2021, and to issue a new one recommending the case for prosecution for violating Section 25 (b) of the DPA.[12]

On 17 January 2023, TGM filed an Urgent Motion for Reconsideration with a prayer that the "Certification (of Finality) dated 22 June 2022 be recalled" and that the "Motion for Reconsideration" be granted.[13]

Issue

Whether the Motion for Reconsideration dated 10 June 2021 filed by TGM be granted.

Discussion

The Commission resolves to deny the Motion.

I. Share capital account is not sensitive personal information as defined under the DPA.

Personal information is considered sensitive personal information if it falls under the exclusive enumeration set forth by Section 3(l) of the DPA.

In this case, TGM alleged that the enumerations under Section 3(l) of the DPA is not exclusive emphasizing that par. 3 of the said provision contains the phrase "**but not limited to**."[14]

Section 3(l) par. 3 states that-

> (l) *Sensitive personal information* refers to personal information:
>
> x x x

[12] Motion for Reconsideration dated 10 June 2021 of TGM.
[13] Urgent Motion to Resolve Motion for Reconsideration dated 10 June 2021 and To Recall Certificate of Finality dated 17 January 2023 of TGM.
[14] NPC 18-077 (*unreported*), Decision dated 15 April 2021, at p. 9.

> (3) Issued by government agencies peculiar to an individual which includes, **but not limited to,** social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns."[15] (Emphasis supplied)
>
> x x x

As defined, a "share capital account" shall refer to "the money paid or required to be paid by the members for the conduct of the operations of the cooperative."[16]

Based on the above definition, "share capital account" is not among the enumeration of sensitive personal information under Section 3 (l)
(3) of the DPA.[17] The said provision, if read in its entirety, is interpreted to only include sensitive personal information issued by government agencies. In this case of MC v. VP, the Supreme Court held that:

> It is an elementary rule of statutory construction that the express mention of one person, thing, act, or consequence excludes all others. This rule is expressed in the familiar maxim *"expressio unius est exclusio alterius."* **Where a statute**, by its terms, **is expressly limited to certain matters, it may not, by interpretation or construction, be extended to others.** The rule proceeds from the premise that the **legislature would not have made specified enumerations in a statute had the intention been not** to restrict its meaning and **to confine its terms to those expressly mentioned.[18]** (Emphasis supplied)

Moreover, the phrase "**but not limited to**" specifically refers only to sensitive personal information issued by government agencies which are peculiar to an individual under Section 3 (l) (3) of the DPA. In another case, the Supreme Court explained the maxim *noscitur a sociis,* to wit:

---

[15] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter I, § 3 (2012).
[16] Rules and Regulation Implementing Certain Provisions of the Philippine Cooperative Code of 2008, Republic Act No. 9520, § 2(m) (2015).
[17] NPC 18-077 (*unreported*), Decision dated 15 April 2021, at p. 9.
[18] Martin Centeno v. Hon. Victoria Villalon-Pornillos, G.R. No. 113092, 01 September 1994.

> Moreover, the maxim *noscitur a sociis*, where a particular word or phrase is ambiguous in itself or is equally susceptible of various meanings, its correct construcphone ltion may be made clear and specific **by considering the company of words in which it is founded or with which it is associated.** This is because a word or **phrase in a statute is always used in association with other words or phrases, and its meaning may, thus, be modified or restricted by the latter**.[19] (Emphasis supplied)

Applying the maxim *noscitur a sociis,* reference should be made to the words associated to the phrase "**but not limited to**" which shall refer to sensitive personal information issued by government agencies which are peculiar to an individual such as social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns.[20] Thus, the "share capital account" as claimed by TGM to be sensitive personal information, is not covered by Section 3(l)(3) of the DPA since it is not among the enumerated government-issue personal information peculiar to an individual.

Further, TGM cited in her Motion the Commission's Advisory Opinion 2019-010 which extends the meaning of "health records"to medical records kept by a publicly-listed corporation.[21] However, advisory opinions, like herein alleged, only serves as guidance to a requesting party and the general public, "but shall not be used in the nature of a standing rule binding on the [Commission] when evaluating other cases regardless of the similarity of the facts and circumstances."[22] In other words, advisory opinions issued by the Commission is merely an explanation of certain provisions, and not an extension of the DPA.

II. Respondents did not violate Section 25 of the DPA for Unauthorized Processing of Personal and Sensitive Personal Information. The processing of share capital account has lawful basis.

---

[19] Francisco I. Chavez v. Judicial and Bar Council, G.R. No. 202242, 17 July 2012
[20] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter I, § 3 (2012).
[21] Motion for Reconsideration dated 10 June 2021 of TGM, at p. 3.
[22] National Privacy Commission, Rules of procedure on requests for Advisory Opinions, NPC Circular 18-01, rule I, § 2 (10 September 2018) (NPC Circular 18-01).

TGM stated that Respondents violated her right to be informed of the processing of her information under Section 16(a) of the DPA which is a violation of Section 25 for Unauthorized Processing of Personal and Sensitive Personal Information.[23]

In establishing whether there is a violation of Section 25 of the DPA, the following requisites must be present:

> 1. The accused processed information of the data subject;
> 2. The information processed is classified as personal or sensitive personal information.
> 3. The processing of personal information or sensitive personal information was without the consent of the data subject, or not authorized under the DPA or any existing law.

The first requisite is present in this case since there was processing of personal information in this case when the Respondents attached the share capital account to the letter submitted to the Philippine Long Distance Telephone (PLDT) Employees Credit Cooperative (PECCI) Chairperson to defer TGM in the general election. The act of attaching the share capital account is considered processing under the DPA.

The second requisite is also present considering that the share capital account contained Complainant's name,[24] which under the DPA is a personal information.

However, the third requisite is lacking in this case.

TGM stated that the Respondents processed her personal information without her consent.[25] Under Section 12 of the DPA, the processing of personal information is permitted whenever there is lawful basis, and when at least one of the criteria for lawful processing is present.[26] Among the conditions is when the data subject has given his or her consent. However, the Commmission emphasizes that under the DPA,

---

[23] Motion for Reconsideration dated 10 June 2021 of TGM, at p. 5.
[24] Complaint-Affidavit dated 25 July 2018 of TGM, referred to as Annex "A-1"
[25] Motion for Reconsideration dated 10 June 2021 of TGM, at p. 5.
[26] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter III, § 12 (2012).

consent is not the only lawful basis for processing personal information.

In this case, the processing of the share capital account is valid as there exists legitimate interest pursuant to Section 12(f) of the DPA, which provides:

> (f) The processing is necessary for the purposes of the **legitimate interests** pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[27]

The Commission has laid down the following conditions to determine whether the processing is based on legitimate interest:

1. The legitimate interest is established;
2. The processing is necessary to fulfill the legitimate interest that is established; and,
3. The interest is legitimate or lawful and it does not override fundamental rights and freedoms of data subjects.[28]

In this case, Respondents had legitimate interest in sharing TGM's share capital account to the PECCI Chairperson in order to dispute the accuracy of TGM's records in relation to her deferment in the general election.[29] In order to fulfill this purpose, the Respondents attached to the letter-request forwarded to PECCI the deferred share capital account of TGM to disregard the good standing status granted to her, which may have been done erroneously.[30] Unfortunately, the letter-request was not acted upon, enabling TGM to run for the Director position.[31]

Thus, it cannot be denied that the Respondents' processing of the share capital account was done with legitimate interest, which is to challenge the veracity of TGM's records given the possibility that the same was granted erroneously.

---

[27] *Id.*, § 12(f).
[28] MAF v. Shopee Philippines, Inc., Decision dated 22 September 2022.
[29] NPC 18-077 (*unreported*), Decision dated 15 April 2021, at p. 10.
[30] *Id.*
[31] *Id.*, at p. 2.

Further, considering that the interest is legitimate herein, the processing of TGM's personal information does not override her rights as a data subject. TGM failed to prove that her rights as data subject have been violated by the Respondents.

Lastly, TGM did not provide any new or material allegations in her Motion to warrant the reversal of the Commission's Decision dated 15 April 2021. Hence, Respondents should not be held liable for violating Section 25 of the DPA.

Thus, the Commission deems it proper to deny the Motion filed by TGM for failure to establish by substantial evidence her allegations against the Respondents.

WHEREFORE, all the above premises considered, this Commission hereby resolves to **DENY** the Motion for Reconsideration filed by TGM. The Decision of the Commission dated 15 April 2021 is hereby **AFFIRMED**.

SO ORDERED.

City of Pasay,
Philippines.
22 February 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

TGM
Complainant

MMBZ LAW FIRM
Complainant's Counsel

EDM
Respondent

EAS
Respondent

MCN
Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

NATIONAL
PRIVACY
COMMISSION

Address

25th-27th Floors, The Upper Class Tower,
Quezon Ave. Corner Scout Reyes Street, Quezon City 1103

Telephone

+632 5322 1322

Social Media

privacy.gov.ph

PrivacyPH