Republic of the Philippines
NATIONAL PRIVACY COMMISSION

ECA,

Complainant,

NPC 18-103
For: Violation of the Data Privacy Act

-versus-

XXX,

Respondent,

x----------x

DECISION

***NAGA, D.P.C.*:**

This refers to the complaint filed by ECA (Complainant) against XXX. (Respondent) for violation of several provisions of the Data Privacy Act (DPA) due to mishandling of the Complainant's Visa Credit Card and company Identification Card (Company ID).

Facts

On 14 August 2018, the Complainant bought several units of Bluetooth headsets from the Respondent's store branch at Cebu City. She then paid using her Visa Credit Card and presented her Company ID as proof of identity.

During the processing of payment, the Complainant noticed that the Respondent's staff took a picture of her Visa Credit Card and Company ID and sent it to the Respondent's Officer-in-Charge (OIC) through an online messaging system, the Complainant stated:

> But looking to (sic) her, she posed for a moment and looking again to my two cards then (sic) covering the cards to her body and i heard the sounds of her cellphone that she's taken picture of my two cards...To my surprised i saw her phone, she sent picture of my TWO CARDS in the messenger. I asked her again, ms

> what makes (sic) you too long? What's the problem of my card, she said i am waiting for my Boss approval. [1]

The Complainant then cautioned the staff that what she did might constitute a violation of the DPA. After processing the payment, the staff explained what happened in this wise:

> That's the time she answer me, the purpose of taken (sic) picture was to ask approval to our Boss thats (sic) why i also sent (sic) to the messenger which were i communicated to (sic) the messenger.[2]

According to the Complainant, the staff further explained that she just followed the company's procedure. The staff also tried to allay the fear of the Complainant by telling that only the staff and the OIC have access to the Complainant's Visa Credit Card and Company ID.

Complainant alleged that the act of the Respondent's staff caused her stress, loss of time, and inconvenience since she had to report her credit card to the bank. The Complainant is also worried that she might be exposed to identity theft.

Thus, on 22 August 2018, the Complainant filed a complaint with the Commission for violation of the DPA with prayer for damages.

The parties were ordered to appear for discovery conference on 05 December 2018. After the discovery conference, the Respondent was ordered by the investigating officer to submit: 1) an explanation why no data protection officer (DPO) was appointed in their company; 2) a notarized answer to the complaint; 3) corporate papers of XXX; 4) identity of the organization's CEO; and 5) the result of the forensic examination of the mobile phone of the staff and her boss.

On 15 December 2018, the Respondent submitted its answer together with the other required documents, except the result of the

[1] Complaints-Assisted Form, p. 3-4
[2] *Ibid, p. 4*

forensic examination of the mobile phone of the Respondent's staff and her boss and the explanation on why no DPO was appointed in XXX. For the purposes of forensic examination, the Respondent attached a letter to National Bureau of Investigation (NBI) seeking its assistance.

In the answer, the Respondent stated that the acts committed by its staff were not part of company's standard practice considering that they respect the rights of data subjects as provided in the DPA.

The Respondent further averred that the incident was caused by their staff's lack of knowledge on processing credit card transactions, especially if the credit card is not BDO or Eastwest, *to wit:*

> Unfortunately, this incident occurred because the staff involved in this case is not yet very familiar with credit card transactions... She was given a one-on-one instruction on how to process BDO and Eastwest credit cards. The credit card used by complainant in this incident was an HSBC Visa Card and was therefore unsure as to how payment will be processed... The staff saw that an HSBC credit card was given to her and was not sure which POS Terminal to use to swipe the card and not knowing how to better handle the situation, took a picture of the credit card and ID and sent these to her OIC in order to be guided as to what POS Terminal will be used.[3]

Respondent further stated that the processing of Complainant's personal information was conducted to seek guidance from the OIC and not to commit any malicious act. However, the Respondent also acknowledged in the answer that taking photos of credit card and ID and sending those via messenger are risky processes that may cause serious inconvenience and potential damage to their customers.

Respondent then undertook to perform the following activities:

[3] Answer, p. 1

1. On-board a data privacy legal consultant who can guide them in their DPA compliance;

2. Appoint a data protection officer to execute their data privacy program and to whom the customers can direct their data privacy issues and concern;

3. Conduct data privacy awareness training to all their staff who are process owners;

4. Conduct a credit card handling procedure training to all their staff; and

5. Publicly publish an escalation call tree in all their store branches where customers can directly escalate their issues and concerns in their dealings with their staff.

Issue

The sole issue for this Commission's resolution is whether the Respondent committed acts in violation of the DPA.

Discussion

The Complainant's contentions are meritorious.

The DPA, its Implementing Rules and Regulations (IRR), and other issuances of this Commission provide for various obligations and responsibilities for Personal Information Controller (PIC). Among those that are relevant to this case are the following:

1. Adherence to the General Data Privacy Principles in processing of personal information[4];
2. Upholding the Rights of the Data Subjects[5];
3. Securing Personal Information through organizational, physical, and technical measures[6]; and
4. Appointing of a DPO[7].

[4] R.A. No. 10173, §11
[5] *Id.*, §16
[6] *Id.*, §20
[7] NPC Advisory 2017-01 dated 14 March 2017

The Respondent's main argument is anchored on their staff's lack of knowledge and good faith when she took a picture of the Complainant's Visa Credit Card and Company ID. They did not provide explanation for the non-appointment of a DPO, and just enumerated several measures that they are planning to do in order to improve their data privacy compliance.

The Respondent's argument failed to persuade this Commission and finds that the Respondent had unjustifiably disregarded its abovementioned obligations and responsibilities as a PIC.

Respondent failed to adhere to the General Data Privacy Principles of Transparency and violated the Complainant's Right to be Informed

The principle of transparency provides that data subjects must be aware of the nature, purpose, and extent of the processing of his or her personal data.[8] A related provision is the data subject's right to be informed, which states that: "the data subject shall be notified and furnished with information indicated hereunder **before the entry of his or her personal data into the processing system of the personal information controller**, or **at the next practical opportunity**."[9] (Emphasis supplied)

The timing of the provision of the information must be done before the entry of the data subject's personal data to the PIC's system or at the next practical opportunity. The "next practical opportunity" depends upon the surrounding circumstance of the case. However, the timing of the provision of information must always be within a reasonable period to give effect to the data subject's right to be informed.

In this case, the Respondent failed to provide the purpose and justification as to the need of processing the Complainant's personal information through taking pictures of her Visa Credit Card and

[8] DPA IRR, §17.a
[9] *Id.*, §34 (2)

Company ID. It took the Complainant four (4) inquiries before getting a substantial answer from the staff. Further, the needed information was only provided after the processing of payment through the credit card. The timing of the notification was not done before the entry of the Complainant's personal data nor can it be said that it was conducted within a reasonable period given the surrounding circumstances. Indubitably, the Complainant's right to be informed as provided by the DPA was violated.

Respondent disregarded its obligation to secure personal information and responsibility to appoint a DPO

The obligation to comply with the provisions of the DPA, IRR, and other issuances of the Commission primarily rest on the PIC. The Respondent cannot use the fault of its staff to evade its responsibility under the DPA.

The DPA IRR provides that, "the personal information controller and personal information processor **shall take steps to ensure that any natural person acting under their authority and who has access to personal data, does not process them except upon their instructions, or as required by law**."[10] (Emphasis supplied)

Thus, the reasoning provided by the Respondent that the conduct of its personnel was supported by the standard practice of the company must fail. It is its responsibility as PIC to secure personal information of its customers and relay the company's privacy policies and procedures to its personnel, especially to those responsible in processing personal information of customers.

Further, Respondent's gross incompliance of the DPA and other issuances of this Commission made evident on its non-appointment of a DPO, which is one of the elementary ways for

[10] *Id.,* §25 (2)

companies to comply with the DPA.[11] The designation of a DPO is mandatory for all PICs regardless of size and nature of business.[12]

To ensure that the Respondent will make good of its stated undertakings in the submitted answer, this Commission shall require various documentation and/or proof of its compliance in line with the Commission's general power to compel any entity to abide by its orders on matters affecting data privacy.[13]

Complainant is entitled to the award of nominal damages

On the award of damages prayed for, while the Complainant claims that she suffered stress, loss of time, and inconvenience, such bare allegations would not be enough for this Commission to award moral damages without sufficient evidence for the same.[14] Considering the circumstances of this case, it would be appropriate to award nominal damages to the Complainant in recognition of her violated legal right.

As provided by the Supreme Court, in *Santos B. Arreola v. Court of Appeals.:*

> Nominal damage is 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 substantial injury or actual damages whatsoever have been or can be shown.[15]

As established above, the Respondent failed to be transparent in the processing of the Complainant's personal information, which then resulted in the violation the Complainant's right to be informed.

---

[11] *See* The Five Pillars of Data Privacy Compliance and Accountability, NPC Privacy Toolkit (3rd edition)
[12] NPC Advisory 2017-01 dated 14 March 2017
[13] R.A. No. 10173, §7(d)
[14] Kierulf, et.al v. The Court of Appeals et. al., G.R. No. 99301, 13 March 1997
[15] G.R. No. 95641, 22 September 1994

The assessment of nominal damages is left to the discretion of the court/tribunal, according to the circumstances of the case. Taking everything in consideration, this Commission awards nominal damages amounting to Ten Thousand (P10,000.00) Pesos to the Complainant.

WHEREFORE, all these premises considered, this Commission resolves to **AWARD** Complainant, ECA, nominal damages in the amount of Ten Thousand (P10,000.00) Pesos for Respondent XXX's violation of her right to be informed under the Data Privacy Act. Respondent is also **ORDERED** to furnish this Commission the following documents:

1. Proof of its on-boarding a data privacy consultant;
2. Proof of registration with the NPC;
3. Copy of its Data Privacy Manuals and Privacy Notice;
4. Proof of its conduct of data privacy awareness and trainings for its employees;
5. Result of the forensic examination of the NBI on the mobile phone;
6. A sworn undertaking from both the Respondent and its agent regarding the deletion of the photos of the Complainant's credit card and identification card; and
7. Proof of payment of the awarded nominal damages.

The Respondent is **DIRECTED** to accomplish the foregoing within thirty (30) days from receipt of this Decision.

SO ORDERED.

Pasay City, Philippines;
23 July 2020.

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

ECA
Complainant

XXX
Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission