Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: NATIONAL PRIVACY COMMISSION **NPC BN 20-149**

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

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the request for exemption from data subject notification filed by the National Privacy Commission ("PIC") dated 07 August 2020, involving a data breach incident affecting one (1) data subject caused by sending a case assignment to a wrong e-mail address.[1]

The Facts

The Complaints and Investigation Division (CID) of the PIC hired Case Decongestion Officers (CDOs) in its effort to declog its dockets. At the time of the initial case assignments, the CDOs were not yet provided with the Commission-issued (@privacy.gov.ph) e-mail addresses. However, in order to ensure that the CDOs start their work after signing of their contracts, copies of a certain case docket containing the complaint and evaluation form were sent to their personal e-mail addresses.[2]

On 03 August 2020, the supervising lawyer sent an e-mail to pa@gmail.com, the e-mail address registered under the name of the concerned CDO, containing PDF copies of the complaints-assisted form, complaint evaluation, briefing documents for CDOs and word documents, cover memorandum guide, summary sheet guide, and fact-finding report guide.[3]

On 04 August 2020, the breach incident was discovered when the concerned CDO informed the CID that he did not receive the subject e-mail and inquired if the same was sent to

[1] Confidentiality Breach dated August 7, 2020.
[2] *Ibid.*, at p. 2.
[3] *Ibid.*, at p. 2.

pga@gmail.com. In an excel file containing the names and email addresses of CDOs, the e-mail address indicated under the name of the concerned CDO is pa@gmail.com instead of pga@gmail.com, the one indicated in his Personal Data Sheet (PDS).[4] It was then realized that the subject e-mail was sent to the wrong e-mail address.

On the same day, the supervising lawyer recalled the e-mail sent to pa@gmail.com but as of the writing of the Initial Report, no notification has been received from Outlook whether the recall was successful. It was also noted by the PIC that the recall function of Outlook will only work if the recipient has not yet opened the e-mail. The supervising lawyer then sent a notification of the incident to the CID's Officer-in-Charge (OIC).[5]

On 05 August 2020, the OIC met with the Legal and Enforcement Office (LEO) personnel to determine what actions they will take on the breach incident.[6]

On 08 August 2020, the PIC submitted an Initial Report with the subject "Confidentiality Breach dated August 06, 2020 for sending case assignment to wrong email address" stating that one (1) data subject is affected, the complainant in the subject case file. The sensitive personal information involved are the TIN ID No. and the date of issuance of the TIN. Other information of the complainant were also involved that may be used to enable identity fraud, namely, first name, middle initial, last name, home address, e-mail address, mobile number, and signature.[7]

The PIC has taken the following measures to address the breach and actions to secure or recover the personal data that were compromised:

(1) Activation of the recall function of Outlook; and
(2) Sending of letter to the e-mail address pa@gmail.com to ask him to delete the e-mail and refrain from sharing its contents to anyone.[8]

[4] *Ibid.*, at p. 2.
[5] *Ibid.*, at p. 2.
[6] *Ibid.*, at p. 2.
[7] *Ibid.*, at p. 3.
[8] *Ibid.*, at p. 3.

Furthermore, the PIC has performed or proposed the following actions and measures to mitigate possible harm or negative consequences, limit the damage or distress to those affected by the incident, and prevent a recurrence of the incident*:*

(1) To use only Commission-issued (@privacy.gov.ph) e-mail addresses in sending case assignments containing the case files to CDOs;
(2) In case of non-availability of Commission-issued e-mail addresses, to confirm and verify with the CDOs their personal e-mail addresses to be used in receiving case assignments with attached case files;
(3) Double check the sent e-mails to CDOs to fully determine that it was only that of the concerned CDO that was mistakenly sent; and
(4) Remind the employees of CID, especially those in charge of collecting the e-mail addresses of the CDOs to double check their personal e-mail addresses and other contact information they have provided.[9]

Citing Section 19 of NPC Circular 16-03,[10] the PIC requests to be exempted from notifying the data subject considering the personal information involved, the reasonable security measures implemented to ensure the protection of the data subject's personal information, and the notification may only result to unnecessary stress to the data subject. The PIC also claims that the actions it has taken will reduce the risk of harm or that the negative consequence to the data subject will not materialize. In the event of identity fraud committed against the data subject, the PIC also stated that it can be ascertained that it originated from the owner of the e-mail address pa@gmail.com.[11]

Discussion

The Commission resolves to deny the request of the PIC for exemption from data subject notification.

Under Section 11 of NPC Circular No. 16-03,[12] 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:

[9] *Ibid.*, at pp. 3-4.
[10] Personal Data Breach Management, 15 December 2016.
[11] *Ibid.*, at p. 4.
[12] *Supra* note 10.

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**.[13]

In this case, the sensitive personal information involved is the TIN ID No. as well as its date of issuance. Other personal information of the data subject are also involved, namely, the first name, middle initial, last name, home address, e-mail address, mobile number, and signature. These are personal information that may be used to enable identity fraud. As these personal information were included in the subject e-mail sent to an unintended recipient and that the recall function was not found to be successful, there is already reason to believe that the information may have been acquired by an unauthorized person and such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The PIC is therefore obliged to notify the affected data subject of the breach incident in accordance with Section 18(A) of the same Circular, which 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.[14]

[13] Emphasis supplied.
[14] Emphasis supplied.

Instead of notifying the data subject, however, the PIC requested for an exemption from notification requirements under Section 19 of the same Circular which provides that:

> The following additional factors shall be considered in determining whether the Commission may exempt a personal information controller from notification:
>
> A. Security measures that have been implemented and applied to the personal data at the time the personal data breach was reasonably believed to have occurred, **including measures that would prevent use of the personal data by any person not authorized to access it**;
> B. Subsequent measures that have been taken by the personal information controller or personal information processor to **ensure that the risk of harm or negative consequence to the data subjects will not materialize**;
> C. Age or legal capacity of affected data subjects: *Provided*, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives.
>
> In evaluating if notification is unwarranted, the Commission may take into account the compliance by the personal information controller with the law and existence of good faith in the acquisition of personal data.[15]

While the PIC recalled the e-mail sent to the wrong e-mail address, no notification was however received from Outlook to show that the recall was successful. In fact, the PIC even noted that the recall function of Outlook will only work if the recipient has not yet opened the e-mail. Considering that no such notification from Outlook was received, it cannot therefore be ascertained whether such measure taken by the PIC will prevent the use of the personal data by the unintended recipient of the subject e-mail – a person who is not authorized to access it.

Moreover, while one of the measures taken by the PIC to address the breach was sending a letter to the e-mail address of the unintended recipient asking him to delete the subject e-mail and refrain from sharing its contents, there is nothing on record to show that the unintended recipient replied and agreed to such request. Given these, there is no assurance that the risk of harm or negative consequence to the affected data subject will not materialize.

[15] Emphasis supplied.

Lastly, the assertion of the PIC that the notification may only result in unnecessary stress to the data subject is unsubstantiated. The personal information involved in the incident contains sensitive personal information and those that can enable identity fraud. Despite this, the security measures it implemented are prospective and does not protect the data subject from the risk he was already exposed to. Merely stating the grounds for exemption without any justification is not sufficient.

In view of the foregoing, the PIC cannot therefore rely on Section 19 of NPC Circular 16-03 to be exempted from notifying the data subject on the data breach incident. It is worth noting that under Section 18(A) of the that Circular, it provides that the notification shall be undertaken in such 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. If the PIC will be exempted from the required notification, the affected data subject will not be able to take such the necessary precautions or measures to protect himself from the possible adverse effects of the breach. This is all the more true considering that the security measures undertaken by the PIC are inadequate to protect the data subject from the unauthorized use of his exposed data.

WHEREFORE, premises considered, the request for exemption from data subject notification filed by the National Privacy Commission is hereby **DENIED.**

The National Privacy Commission is **ORDERED** to notify the affected data subject of the breach incident in accordance with the provisions of NPC Circular 16-03 and to **SUBMIT** proof of compliance thereto within fifteen (15) days of receipt of this Resolution.

SO ORDERED.

Pasay City, Philippines;
20 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:

JRYR
Data Protection Officer
National Privacy Commission

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission