Republic of the Philippines
NATIONAL PRIVACY COMMISSION

CCMC,

Complainant,

CID 18-K-200
For: Violation of the Data Privacy Act of 2012

-versus-

QXXX FINANCING CO., INC.,

Respondent.

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

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission are the submissions of QXXX Financing Co., Inc. in response to the Commission's Decision dated 17 January 2020. This case involves an "Early Payment Reminder"" sent by Respondent via email where the names and email addresses of all one hundred thirty-six (136) recipients were visible to all the recipients.

Facts

On 17 January 2020, the Commissioner rendered a Decision on this case, thus:

> "**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 the procedures by the DPO and his team.
>
> **SO ORDERED."**[1]

[1] NPC Decision dated 17 January 2020.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

On 16 September 2020, the Commission received QXXX's Privacy Manual.[2] After assessing the Privacy Manual, the Commission found that while it included a section on Security Management, it did not include the required provisions in NPC Circular No. 16-03[3] that will ensure the following:

> a. Implementation of an Incident Response Procedure intended to contain a security incident or personal data breach and restore integrity to the information and communication system.
>
> b. Steps to be undertaken to mitigate possible harm and negative consequences to a data subject in the event of a personal data breach.

The Commission found that the submitted document only discussed in general that QXXX will recover and restore the affected data but lacked concrete steps to mitigate or contain the breach to prevent greater harm. Moreover, the Commission found that there was no discussion regarding the steps that QXXX would undertake to mitigate possible harm to data subjects.

Consequently, the Commission, through the Enforcement Division (EnD), sent an Enforcement Letter to QXXX directing it to submit a Security Incident Management Policy that augmented the identified deficiencies within fifteen (15) days from the receipt of the letter.[4] In a letter dated 09 November 2020, which was received by the Commission on 16 November 2020, the Respondent sent its complete Security Incident Management Policy to comply with the aforementioned directive.[5]

Issue

Whether or not QXXX implemented sufficient measures to manage data privacy breach incidents

---

[2] Letter from QXXX Financing Co. Inc. dated 14 September 2020.
[3] Section 4, NPC Circular No. 16-03. Personal Data Breach Management, dated 15 December 2016.
[4] Enforcement Letter dated 22 October 2020.
[5] Letter from QXXX Financing Co. Inc. dated 9 November 2020.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Discussion

Rule II, Section 4 of NPC Circular No. 16-03 states that personal information controllers should implement policies and procedures to manage security incidents:

> **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:
>
> A. Creation of a data breach response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;
> 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;
> C. Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system;
> D. Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and
> E. Compliance with the Act, its IRR, and all related issuances by the Commission pertaining to personal data breach notification.

The Commission finds that the Data Privacy Security Incident Management Policy (SIMP) submitted by QXXX has substantially complied with the Decision dated 17 January 2020 and NPC Circular No. 16-03 on Personal Data Breach Management.

In its SIMP, QXXX outlined eight (8) steps that it will follow in cases of security incidents and data breaches.[6] These are:

[6] QXXX Financing Co., Inc.'s Security Incident Management Policy.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

(1) Reporting – Any person, whether connected to QXXX or not, should report an incident or breach to the QXXX DPO within two (2) hours from discovery;[7]

(2) Categorization - A member of the Breach Response Team (BRT) shall categorize the event whether it is a security incident, a personal data breach, or non-urgent matter;[8]

(3) Investigation and Identification – If the event is categorized as either a security incident or a personal data breach, the BRT should investigate it to discover the nature and circumstances of the incident or breach, the data processing systems involved and the persons responsible, involved and affected, as well as their contact details;[9]

(4) Reporting and Notification – If the incident or the breach falls under the mandatory breach notification of NPC Circular No. 16-03, QXXX shall notify the Commission within seventy-two (72) hours from the discovery of the incident. Aside from notifying the Commission, QXXX shall also notify the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred;[10]

(5) Containment and eradication – The BRT shall conduct steps to stop the cause of the incident or the breach and its effects;[11]

(6) Recovery – The BRT shall restore the system or application to a working state and disclose details of the incident to affected users, if necessary;[12]

(7) Feedback – The BRT shall categorize the Security Incident or Personal Data Breach based on the actions taken;[13] and

---

[7] *Id.* at 6.
[8] *Ibid.*
[9] *Id.* at 7.
[10] *Ibid.*
[11] *Id.* at 8.
[12] *Id.* at 9.
[13] *Ibid.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

(8) Learning – The BRT should discuss the lessons learned and may document lessons to prevent similar incidents from occurring again.[14]

In its Mitigation Response Plan,[15] QXXX enumerated specific examples of how it plans to contain an incident:

> Step 5 - Containment and Eradication
>
> The BRT shall conduct steps to stop the cause of the Security Incident or Personal Data Breach and its effects. The BRT is responsible to contain the Security Incident or Personal Data Breach so that it does not spread and cause further damage. Steps that may be taken are:
>
> - Disconnect the affected devices from *(sic)* the internet or intranet
> - Commence short-term and long-tern containment strategies
> - Ensure that there is a backup system to help us in the restoration process
> - Update and patch the system
> - Review remote access protocols
> - Change user and administrative access credentials
> - Secure passwords
>
> The QXXX DPO shall address the Concern. The DPO shall facilitate all forms of resolutions by ensuring that the support provided by the QXXX BRT responsively and effectively addresses the Concern without causing new Concerns.
>
> Step 6 – Recovery
>
> The BRT, in coordination with relevant QXXX I.T. personnel, shall endeavor to restore the system or application to a working state and take necessary actions to recover affected records, systems and other matters affected by the Security Incident. The following tasks may be conducted:
>
> - restoring system data to a known good state
> - repairing or rebuilding the system or application that was compromised

[14] *Ibid.*
[15] *Id.*at 8.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

- validating that the problem that caused the incident has been addressed
- communicating to users that the system is back online
- disclosing the incident to affected *(sic)* users if necessary
- taking any appropriate administrative action related to the incident[16]

The Commission acknowledges that these policies and procedures comply with NPC Circular No. 16-03 and can help mitigate the possible harm to a data subject. Moreover, these clear policies on security incidents will help avoid delays in notification to the Commission and the affected data subjects.

WHEREFORE, premises considered, this Commission finds that the submission of QXXX Financial Co., Inc. in response to the Decision dated 17 January 2020 is **SUFFICIENT.** This Commission considers the matter **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
29 April 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

[16] *Ibid.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

CCMC
Complainant

JNB
Data Protection Officer of Respondent

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

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228