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