Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: BATANGAS BAY CARRIERS, INC. **NPC BN 20-157**

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

RESOLUTION

***AGUIRRE*, D.P.C.:**

This Resolution refers to the request for Postponement of Notification to affected data subjects of Batangas Bay Carriers, Inc. (Batangas Bay), a subsidiary of Magsaysay Shipping & Logistics, dated 01 September 2020,[1] involving a personal data breach caused by a ransomware attack.[2]

The Facts

On 26 August 2020, some users reported that their files stored in the company's shared network drive could not be opened. This was reported to the IT Servicedesk and upon checking, they discovered that the files have been encrypted and the file extensions have been changed to *.ROGER*. The research showed that the incident was caused by a certain strain of ransomware virus. Around the same time, they realized that other servers at the Time Plaza Data Center, which hosts other systems, applications or databases, were infected by the same ransomware virus.[3]

On 01 September 2020, Batangas Bay was able to determine that the availability of personal data in its payroll database was compromised due to encryption as a result of the ransomware attack. In its report, the officers stated that they remain hopeful that the data's availability can be restored through decryption without paying a ransom.[4]

As it was unclear what vulnerabilities in the data processing system allowed the breach, Batangas Bay engaged cybersecurity experts to learn more about the incident during the investigation.[5]

---

[1] Possible availability breach due to ransomware affecting Payroll Database dated 1 September 2020.
[2] *Ibid*., at p. 2.
[3] *Ibid*., at pp. 1-2.
[4] *Ibid*., at p. 2.
[5] *Ibid*., at p. 2.

As to the number of individuals or personal records affected, the officers of Batangas Bay claim that it is yet to be determined. Nonetheless, they believe the number to be more than one hundred (100) individuals.[6]

Batangas Bay believes that the most likely consequence of this incident is data loss arising from an inability to decrypt the affected files since the security incident involves a ransomware. In the report, the officers state that there is no indication that personal data has been acquired by unauthorized persons. However, they expect that the data loss will be minimal and temporary as it backs up data constantly and the same are intact.[7]

The report indicated the following as the personal data possibly involved in this breach: name, birthday, age, marital status, number of dependents, home address, salary and allowance, government ID numbers, bank account numbers, contact numbers, and employment information.[8]

Batangas Bay reports that it has undertaken the following measures to address the breach:

(1) All servers were shut down to contain the virus and allow the IT team to inspect each server;
(2) An incident advisory was sent to all users and management on 27 August 2020, and all units were advised to apply business continuity plans and workarounds while the servers or systems are down;
(3) Security patches for the ransomware were applied to non-affected servers;
(4) Cybersecurity vendors were tapped to assist on the containment, clean-up, and possible decryption of affected files; and
(5) The network traffic from and to the network was stopped, thus disconnecting the internet access in Times Plaza on 27 August 2020. The internet connection was diverted to Antonino building, the back-up center. This enabled the cybersecurity vendor and IT to monitor the link, and determine any suspicious and virus-related activities.[9]

[6] *Ibid*., at p. 2.
[7] *Ibid*., at p. 2.
[8] *Ibid*., at p. 2.
[9] *Ibid*., at p. 2.

However, Batangas Bay stated that it has yet to notify the affected data subjects since it still needs to determine precisely who were affected, and that it is not reasonably possible to notify them all individually within a span of seventy two (72) hours.[10] It also claims that it has no reason to believe at the time that any data has been acquired by an unauthorized person or that the breach is likely to give rise to a real risk of serious harm to the affected data subjects.[11]

Hence, the instant request for postponement of notification of data subjects until such time that it has ascertained the identities of the affected data subjects.[12]

Discussion

This Commission denies the herein request for postponement of notification to data subjects of Batangas Bay in accordance with NPC Circular No. 16-03 (Personal Data Breach Management).

At the outset, it should be emphasized that notification of data subjects of data breaches is the general rule. Under Section 18(A) of NPC Circular No. 16-03, it 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.[13]

The exemption or postponement will only be allowed in exceptional circumstances under Section 18(B) of NPC Circular No. 16-03, which provides that:

---

[10] *Ibid.*, at p. 2.
[11] *Ibid.*, at p. 1.
[12] *Ibid.*, at p. 2.
[13] Emphasis supplied.

> **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.[14]

The report of Batangas Bay does not contain any narration of a "criminal investigation related to a serious breach that may hinder the progress thereof, taking into account circumstances provided in Section 13 of the said Circular, and other risks posed by the personal data breach" in order for the Commission to consider its request for postponement. Following this, the instant request for postponement is not proper and must be denied.

The Commission notes that Batangas Bay also asserts that it has yet to determine the identities of the affected data subjects, as the ground for their request for postponement of notification of data subjects. This is not plausible as Batangas Bay has categorically reported that it has ascertained that the subject ransomware attack affected the availability of personal data in the company's payroll database. Considering that the affected database is the payroll system, it should be able to readily identify the data subjects as the persons therein are its own employees.

Batangas Bay's report and request also contains a contention that, since the security incident involves ransomware, it has no reason to believe that any data has been acquired by an unauthorized person or that the breach is likely to give rise to a real risk of serious harm to the affected data subjects.

On this issue, the Commission finds that no evidence was presented to support this claim. It is a basic rule of evidence and procedure that the Commission cannot simply rely on bare allegations and must look at the available evidence on record to

[14] Emphasis supplied.

see whether these are sufficient to overcome the presumption that notification is in the best interest of the data subjects.

The Commission also notes that Batangas Bay seems to connect the fact that the security incident involved ransomware with the lack of any indication that personal data has been acquired by unauthorized persons.

Section 11 of NPC Circular 16-03 states the conditions for notification, thus:

> **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:
>
> 1. 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.
>
> 2. There is reason to believe that the information may have been acquired by an unauthorized person; and
>
> 3. 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.

Certain misconceptions about Section 11(2) of NPC Circular 16-03 (Section 11(2)) must be clarified. 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."

This liberal interpretation of the conditions necessitating mandatory breach notification is rooted in Section 20(f) of the DPA itself, which provides:

> 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.[15]

The infection of the system by a ransomware should be sufficient to form a reasonable belief for the personal information controllers.

Ransomware is defined as "a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it… Typically, these alerts state that the user's systems have been locked or that the user's files have been encrypted. Users are told that unless a ransom is paid, access will not be restored."[16] While ransomwares primarily cause availability breaches, it is different from other availability breaches because a malefactor intentionally causes them. This is unlike other types of availability breaches that are caused by accidents or system glitches. In these cases, the total exercise of control over the data is removed from the personal information controller and is taken by the malefactor. Without this control, the personal information controller will be unable to exercise its obligations in processing

[15] Emphasis supplied.
[16] UC Berkeley Information Security Office (n.d).*Frequently Asked Questions- Ransomware.* Retrieved from https://security.berkeley.edu/faq/ransomware/.

the personal data according to the provisions of the DPA. Recent ransomware attacks have also shown a capability to release the encrypted data over the internet upon non-payment of the ransom, potentially leading to a confidentiality breach contemplated in Section 11(2). For the protection of the data subjects, such incidents must be notified both to the Commission and the affected data subjects.

This construction of Section 11(2) is guided by the Interpretation Clause in the DPA which states:

> Section. 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.

WHEREFORE, premises considered, the request for Postponement of Notification to Data Subjects filed by Batangas Bay Carriers, Inc. is hereby **DENIED.**

Batangas Bay Carriers, Inc. is **ORDERED** to 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 **within fifteen (15) days** from receipt of this Resolution.

SO ORDERED.

Pasay City, Philippines;
21 September 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:

CRD
Data Protection Officer

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