Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: TRAVELPEOPLE LTD., INC. **NPC BN 20-170**

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

RESOLUTION

LIBORO, P.C.:

This Resolution refers to the request for postponement of Notification to affected data subjects filed by TravelPeople Ltd., Inc. ("TPLI") of the Magsaysay Group of Companies dated 02 September 2020,[1] involving a personal data breach caused by a ransomware attack in the company's system.

The Facts

In its Initial Report filed with the Commission, TPLI stated that in the morning of 26 August 2020, the company was advised by its in-house IT that there was a problem with the Magsaysay network which currently houses its systems which resulted in difficulties in connection. It was later found that the Travel Management Systems of the company, the system that holds information of its clients and suppliers, were affected by a strain of ransomware virus. As a result, the company have to manually input details of ticket issued, requests for cash advance, and requests for payment to its suppliers.

According to the Initial Report Submitted by TPLI, it has established that no personal data or records have been exposed to the public. It is unclear at this time what vulnerabilities in the data processing system allowed the breach. Further investigation is being conducted by the cybersecurity experts they engaged.

According to the company, as the security incident involves ransomware, there is no indication that personal data has been acquired by unauthorized persons. They believe the most likely consequence of this incident is data loss arising from an inability to

[1] Notification: Personal Data Breach for the National Privacy Commission dated 02 September 2020.

decrypt the affected files. However, they expect the data loss to be minimal and temporary, as they back up their data constantly, and the backups are still intact.

Records also shows that the total number of data subjects who may be affected, as well as the personal information involved were not indicated in the report.

According to its Initial Report, the following were measures taken to address the breach:

i. All servers were shut down to contain the virus and to allow IT to conduct check each server.
ii. An incident advisory was sent to all users and to management on August 26, 2020. All units were advised to apply their Business Continuity Plans and workarounds while the servers/systems are down.
iii. Security patches for the ransomware was applied to non-affected servers.
iv. Cybersecurity vendors were tapped to assist on the containment, clean-up, and possible decryption of affected files.

While an incident advisory was sent to all users and to the management, they have yet to notify the affected data subjects at this time, as they have yet to determine precisely who were affected.

If notification is necessary in the determination of the Commission, TPLI request for a postponement in notifying the affected data subjects until such time as they have ascertained the identities of the affected data subjects.

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.

Discussion

This Commission denies the herein request for postponement of notification to data subjects of TPLI 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.[2]

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

> **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.[3]

The Initial Report submitted by TPLI 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

[2] Emphasis supplied.
[3] Emphasis supplied.

Commission to consider its request for postponement of notification to data subjects. Thus, a request for postponement is not proper and must be denied.

The company's Initial Report and request also contains a contention that since the that the security incident involves ransomware and that there is no indication that personal data has been acquired by unauthorized persons, no evidence was submitted to support this. On this issue, the Commission finds that no evidence was presented to support this claim.

Furthermore, this Commission wants to clarify the obvious misconception of TPLI that since the security incident involved ransomware, there is no reason to believe that the information may have been accessed 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.

It should be noted that 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.[4]

In the previous Resolutions[5] issued by this Commission, it was held that:

> 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,

[4] Emphasis supplied.
[5] NPC BN 20-157, NPC BN 20-158, NPC BN 20-159, NPC BN 20-160, NPC BN 20-161, NPC BN 20-162, NPC BN 20-163, NPC BN 20-164, NPC BN 20-165.

> access will not be restored."[6] 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 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 TravelPeople Ltd., Inc. is hereby **DENIED.** TravelPeople Ltd., Inc. is **ORDERED** to comply with the following **within fifteen (15) days from receipt of this Resolution**:

1. **SUBMIT** full breach report with the complete information required under NPC Circular 16-03 which includes among others, the nature of personal data involved and a determination of the affected data subjects; and

2. **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.

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

SO ORDERED.

Pasay City, Philippines;
21 September 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

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

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

Copy furnished:

N.K.D.
Data Protection Officer
TravelPeople Ltd., Inc.

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