IN RE: TRAVELSERVICES, INC. **NPC BN 20-167**

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

RESOLUTION

NAGA, *P.C.;*

Before the Commission are TravelServices, Inc.'s (TravelServices) Compliance and Motion for Partial Reconsideration dated 09 February 2021[1] to the Resolution issued by the Commission dated 21 September 2020.[2]

Facts

On 21 September 2020, the Commission issued an Order with the following dispositive portion:

> **WHEREFORE**, premises considered, the request for Postponement of Notification to Data Subjects filed by TravelServices, Inc. is hereby **DENIED.** TravelServices, 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.
>
> **SO ORDERED.**[3]

[1] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc.
[2] In Re: TravelServices, Inc., NPC BN 20-167, Resolution dated 21 September 2020.
[3] *Id.*

Accordingly, TravelServices submitted its Compliance and Motion for Partial Reconsideration dated 09 February 2021 and stated that it received the above Resolution on 25 January 2021.[4]

In Compliance to the Commission's order to submit its Full Breach Report, TravelServices provided the details on the nature of the breach stating that its server, holding TravelServices' clients and suppliers' information, has been infected by a ransomware virus which resulted to the encryption of files and change of file extensions to ".R," which made them inaccessible without a decryption key.[5] According to TravelServices, the incident resulted to the temporary inaccessibility of approximately fifty thousand (50,000) or more booking transactions, and that the incident has resorted them to manually input the ticket details and payment requests to suppliers.[6]

TravelServices also enumerated the personal data possibly involved in the ransomware attack, which include the following:

- First and last names of clients (no middle names).
- Booking details, i.e., ticket numbers, destinations, flight schedules, and the like.
- Email addresses (not applicable to all data subjects).
- Telephone numbers (not applicable to all data subjects).[7]

As to the measures taken to address the breach, TravelServices provided the following details:

- All servers were shut down to contain the virus and to allow IT to conduct a check on each server.
- 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 were down.
- Security patches for the ransomware were applied to non-affected servers.
- Cybersecurity experts from the ePLDT Cyber Security were engaged to assist in the containment, clean-up, and possible decryption of affected files. The experts also conducted a

[4] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 1.
[5] Full breach report dated 09 February 2021 of TravelServices, Inc., at pp. 1-2.
[6] *Id.*
[7] *Id.*, at p. 2.

> forensic investigation to determine the methodology and behavior of the ransomware virus that infected the server.
> - All the affected data was restored from backups by September 8, 2020.
> - To prevent recurrence of the incident, [it] engaged experts to conduct a vulnerability assessment and penetration test on all systems in order to identify our risks of further exposure to cyberattacks and other security incidents and determine possible measures to mitigate or avoid them. [It] also plan[s] to deploy advanced endpoint detection and response tools to all workstations and servers in the first quarter of 2021.[8]

Further, TravelServices stated that it initially requested for the postponement from the notification required since it could not ascertain the identities of the affected data subjects and that no personal data had been acquired or accessed by unauthorized persons.[9]

However, upon investigation, TravelServices alleged that the incident did not show sensitive personal information or other information that may be used to enable identity fraud.[10] TravelServices further averred that there were no data subjects that "were harmed or could have been harmed as a consequence of the incident."[11] Thus, TravelServices claimed that there is no need to notify the affected data subjects regarding the "temporary availability breach" incident in this case.[12]

Lastly, TravelServices stated that if notification is done, "it will be impossible for [TravelServices] to notify all the data subjects directly, as [it] generally do not collect and record postal addresses, and not all clients provide their email addresses or phone numbers when transacting with [TravelServices]."[13]

On the other hand, TravelServices also filed its Motion for Partial Reconsideration to the Resolution issued by the Commission dated 21 September 2020.[14]

---

[8] *Id.*
[9] Full breach report dated 09 February 2021 of TravelServices, Inc., at p. 3.
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Full breach report dated 09 February 2021 of TravelServices, Inc., at p. 3.
[14] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc.

According to TravelServices, the Forensic Investigation Report from the cyber security experts it engaged to address the incident determined that "the security incident did not provide unauthorized persons any opportunity to access, obtain, or disclose any of the data affected by the ransomware virus."[15] TravelServices claimed that these findings confirmed its initial assessment that "there was no reason to believe that the data had been acquired by unauthorized person or that the incident/breach was likely to give rise to a real risk of serious harm to the affected data subjects."[16]

Moreover, TravelServices reiterated that if individual notification must be done directly to the affected data subjects, the same will be impossible as TravelServices generally does not collect and record postal addresses, and that not all of its clients provide their email addresses or phone numbers with TravelServices when transacting.[17]

Further, TravelServices stated that the instant case does not warrant notification to the affected data subjects.[18] It claimed that the three (3) requisites for the mandatory notification requirement under Section 11 of NPC Circular No. 16-03 are not present.[19]

TravelServices argued that none of the personal data involved in the incident are considered sensitive personal information or other information that may be used to enable identity fraud.[20] It also stated that there is no reason to believe that the information herein were acquired by an unauthorized person considering that according to the forensic investigation conducted by a reputable third-party cybersecurity experts, "*there was no malicious executable files dropped on the victim machine*" and "*there were no outbound connections to any known malicious hosts that were seen in the packet capture as signs of command and control of the miscreant.*"[21]

---

[15] *Id.,* at p. 2.
[16] *Id.*
[17] *Id.*
[18] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 2.
[19] *Id.,* at p. 3.
[20] *Id.*
[21] *Id.*

Lastly, TravelServices submitted that no harm was inflicted to data subjects as a consequence of the security incident.[22] According to TravelServices, the only "harm" herein was the temporary inconvenience to its staff when the latter "had to input data manually while the travel management system was offline."[23]

Issue

Whether to grant the Motion for Partial Reconsideration filed by TravelServices dated 09 February 2021.

Discussion

The Commission notes the Compliance of TravelServices dated 09 February 2021. Further, the Commission denies the Motion for Partial Reconsideration filed by TravelServices.

The incident falls under the mandatory breach notification requirement.

Section 20(f) of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA) states:

> SEC. 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[.]**[24] (Emphasis supplied)

---

[22] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 3.
[23] *Id.*
[24] 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, chapter V, § 20(f) (2012).

In relation thereto, Rule V, Section 11 of NPC Circular No. 16-03 provides:

> **Sec. 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**.[25] (Emphasis supplied)

In its full breach report, TravelServices stated that the personal data possibly involved are:

> - First and last names of clients (no middle names).
> - Booking details, i.e., ticket numbers, destinations, flight schedules, and the like.
> - Email addresses (not applicable to all data subjects).
> - Telephone numbers (not applicable to all data subjects).[26]

In this case, the first element of mandatory breach notification is present since the breach incident under the circumstances involves information that may be used to enable identity fraud such as the data subjects' names, email addresses, and telephone numbers.

---

[25] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 11 (15 December 2016) (NPC Circular 16-03).
[26] Full breach report dated 09 February 2021 of TravelServices, Inc., at p. 2.

Given that these information were the subject of a ransomware attack, their unauthorized acquisition may result to identity fraud, identity theft, and phishing activities, when used in a manner that could expose the affected data subjects to harassment, discrimination, or other risks of real and serious harm. Thus, the first requisite is present.

As to the second requisite, the forensic investigation conducted by a reputable third-party cybersecurity experts stated that "*there was no malicious executable files dropped on the victim machine*" and "*there were no outbound connections to any known malicious hosts that were seen in the packet capture as signs of command and control of the miscreant.*"[27]

However, as previously held by the Commission in its Resolution dated 21 September 2020:

> 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."[28]

Thus, the second requisite is present in this case considering that due to the ransomware attack, TravelServices has lost control over the information of its clients. Such is deemed a reason to believe that the information may have been acquired by an unauthorized person.

Lastly, TravelServices stated that no harm was inflicted to data subjects as a consequence of the security incident, that the only "harm" herein was the temporary inconvenience to its staff when the latter "had to input data manually while the travel management system was offline."[29]

---

[27] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 3.
[28] In Re: TravelServices, Inc., NPC BN 20-167, Resolution dated 21 September 2020.
[29] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 3.

However, mere temporary inconvenience to TravelServices' staff in manually inputting the booking records of approximately fifty thousand (50,000) or more individuals is not the "harm" contemplated under Section 11(c) of NPC Circular 16-03. The serious harm being considered in the said provision means that negative consequences such as identity fraud or theft may give rise due to the ransomware attack.[30] In this case, since TravelServices has lost control over the personal data due to ransomware attack, there already arose a belief that a real risk of serious harm to any affected data subjects may occur, which TravelServices failed to sufficiently prove. Thus, the third requisite is present.

Considering that all the requisites for mandatory breach notification are present in this case, the Commission deems it necessary to require TravelServices to notify the affected data subjects of the security incident. Such notification will enable the affected data subjects to take necessary actions "to protect themselves against the possible effects of the breach."[31]

TravelServices cannot excuse itself from its obligation to notify the affected data subjects by stating that TravelServices "generally do not collect and record postal addresses" and that "not all clients provide their email addresses or phone numbers when transacting with [it]."[32] In addition to its obligation to individually notify the affected data subjects, TravelServices may also notify them using alternative means of notification, or any other means wherein the data subjects are informed in an equally effective manner.[33]

WHEREFORE, premises considered, this Commission resolves to:

1. **DENY** the Motion for Partial Reconsideration dated 09 February 2021 filed by TravelServices, Inc. (TravelServices);

2. **DIRECT** TravelServices to individually **NOTIFY** the affected data subjects and **SUBMIT** proof of notification to the

[30] NPC Circular 16-03, § 11.
[31] *Id.*, § 18(A).
[32] Compliance and Motion for Partial Reconsideration dated 09 February 2021 of TravelServices, Inc., at p. 2.
[33] NPC Circular 16-03, rule V, § 18(D).

Compliance and Monitoring Division (CMD) within **fifteen (15) days** from receipt of this Resolution;

3. **DIRECT** TravelServices to **SUBMIT** proof of notification to the affected data subjects through alternative means to the CMD within **five (5) days** from receipt of this Resolution;

4. **DIRECT** CMD to issue the appropriate orders necessary to evaluate and monitor the completeness of TravelServices' Compliance and assess its breach management pursuant to NPC Circular 16-03 (Personal Data Breach Management).

SO ORDERED.

City of Pasay, Philippines.
13 November 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

GGB
Data Protection Officer

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