IN RE: ROSEWOOD HOTEL GROUP **NPC BN 18-008**

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

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is Rosewood Hotel Group's (Rosewood) breach notification involving an incident that affected its guest reservation system.

Facts

On 19 January 2018, Rosewood Hotel Group (Rosewood) notified the National Privacy Commission (NPC) about a data security issue that affected its guest reservation information maintained on the Sabre Hospitality Solutions (Sabre) system.[1]

Sabre is a service provider utilized by Rosewood and other major hotel brands to process guest reservations.[2] Under Rosewood's contract with Sabre, Sabre is obligated to protect Rosewood's guest data from unauthorized use, access, or disclosure with at least reasonable care and the same measures that Sabre uses to protect its own information.[3] The contract also requires Sabre to remain in compliance with the Payment Card Industry Data Security Standard (PCI DSS).[4]

In December 2017, Sabre informed Rosewood that it discovered that between 29 May 2016 and 11 January 2017 an unauthorized party gained access to Rosewood's guest information by obtaining account credentials from Sabre without its authorization.[5]

---

[1] Letter *from* SGH *to* the National Privacy Commission, 19 January 2018, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2018).
[2] *Id.*
[3] Full Breach Report, 11 April 2022, at 3, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[4] *Id.*
[5] Letter *from* SGH *to* the National Privacy Commission, 19 January 2018, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2018).

Sabre explained that the unauthorized party utilized social engineering techniques to improperly access the system.[6] Sabre's investigation revealed that once the system is accessed, the unauthorized party inappropriately reset the password, and in some instances, changed the email address associated with the credentials.[7] In other instances, the unauthorized party would use the credentials to access a limited set of hotel bookings where some reservations included credit card details as payment information.[8]

According to Sabre, the reservation information affected by the incident involved guests' names and payment card information, including cardholder name, payment card number, expiration date, and security code.[9]

Rosewood stated that none of the affected hotels are in the Philippines, however, approximately nineteen (19) Philippine residents were affected by this incident.[10] Rosewood clarified that the issue occurred on Sabre's systems and did not affect Rosewood's own systems.[11]

Sabre also informed Rosewood that other hotel brands were similarly impacted by this issue.[12]

On 10 March 2022, the NPC, through the Complaints and Investigation Division (CID), ordered Rosewood to submit a Full Breach Report and Supporting Documents in relation to its initial notification.[13] The CID also inquired whether the system affected in the breach notification report in 2017 was related or involved the same system affected in the present breach.[14]

---

[6] Post-Breach Report, 01 June 2022, at 3, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[7] *Id.*
[8] *Id.*
[9] Letter *from* SGH *to* the National Privacy Commission, 19 January 2018, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2018).
[10] *Id*. at 2.
[11] *Id*. at 1.
[12] *Id*.
[13] Order (To Submit Full Breach Report and Supporting Documents), 10 March 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[14] *Id*.

On 28 March 2022, Rosewood, through its counsel, filed for a Motion for Extension of Time to submit a full breach report since Rosewood is domiciled in the United States of America (USA) and the information and documents needed would come from Rosewood.[15]

On 29 March 2022, the CID granted Rosewood's request for an extension of time.[16]

On 11 April 2022, Rosewood submitted its Full Breach Report.[17] Prior to the present breach notification matter, Rosewood explained that there was a similar breach notification report involving the same system in 2017.[18] It clarified that the system involved in the 2017 Report to the NPC was Sabre's SynXis Central Reservation System (CRS), which is also the same system affected in the present breach notification.[19]

Rosewood explained that the cause of the issue described in the 2017 report was a compromised Sabre internal account that enabled an unauthorized party to access Sabre's SynXis CRS.[20] Here, the unauthorized party used social engineering tactics against Sabre.[21] It obtained Rosewood account credentials to access Sabre's SynXis CRS and reset email credentials without authorization from Rosewood.[22]

Rosewood informed the CID that it notified some of the affected data subjects through postal mail.[23] Rosewood also posted notices on its website to notify individuals whose contact information could not be found.[24]

---

[15] Motion for Extension of Time, 28 March 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[16] Resolution (of the Motion for Extension of Time dated 28 March 2022), 29 March 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[17] Full Breach Report, 11 April 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[18] *Id*. at 2.
[19] *Id*. at 1.
[20] *Id*.
[21] *Id.* at 2.
[22] *Id*. at 1.
[23] Full Breach Report, 11 April 2022, at 8, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[24] *Id*. at 9.

On 11 May 2022, the CID issued an Order directing Rosewood to submit a Post-Breach Report containing the proper documentation on the actions it took.[25]

On 01 June 2022, Rosewood submitted its Post-Breach Report.[26]

Rosewood also clarified that only fourteen (14) data subjects are affected in the Philippines instead of nineteen (19) as it initially reported.[27] Rosewood explained that some of the entries appeared to be duplicates.[28]

Rosewood also reported that it revisited its contract with Sabre in order to enhance its security measures against "human dangers" such as social engineering and hacking incidents.[29] The amended contract requires Sabre to ensure that its personnel engaged in processing personal data are dedicated to maintaining confidentiality and must implement suitable technical and organizational safeguards to mitigate risks associated with processing personal data.[30] Lastly, the contract requires Sabre to promptly notify Rosewood upon knowledge of any breaches involving personal data.[31]

Issue

Whether Rosewood conducted proper breach management, including the implementation of reasonable and appropriate security measures.

Discussion

The Commission finds that Rosewood conducted proper breach management and implemented reasonable and appropriate security measures upon knowledge of the incident. Thus, the Commission resolves to close the case.

---

[25] Order (To submit Post-Breach Report), 11 May 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[26] Post-Breach Report, 01 June 2022, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[27] *Id*.
[28] *Id*.
[29] *Id*. at 4.
[30] *Id*.
[31] *Id*. at 2.

Section 20 (a) and (b) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) mandates a Personal Information Controller (PIC) to implement reasonable organizational, physical, and technical measures intended for the protection of personal data:

> Section. 20. *Security of Personal Information.* (a) **The personal information controller must implement reasonable and appropriate organizational, physical and technical measures** intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.
>
> (b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.[32]

Further, Section 17 (D) (3) of NPC Circular 16-03 (Personal Data Breach Management) provides for the PIC's obligation to inform its data subjects of the measures it took to address the breach:

> Section 17. *Notification of the Commission*. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification*. The notification shall include, but not be limited to:
>
> . . .
>
> 3. Measures Taken to Address the Breach
>   a. description of the measures taken or proposed to be taken to address the breach;
>   b. actions being taken to secure or recover the personal data that were compromised;
>   c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;

[32] 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 (a) & (b) (2012). Emphasis supplied.

d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
e. the measures being taken to prevent a recurrence of the incident.[33]

As an immediate response, Rosewood informed relevant payment card companies about the security incident.[34] Sabre also separately provided notice to the credit card companies.[35] Sabre also disabled the impacted accounts and addressed the unauthorized access to its system.[36]

Sabre also hired a cybersecurity expert to conduct a forensic investigation and reported the incident to the law enforcement authorities in the USA.[37]

Rosewood notified the Philippine residents through postal mail.[38] In its submissions, Rosewood attached a copy of its notification to the affected data subjects.[39] The notification included a narration of the security incident and all the measures it took to address the breach.[40] Rosewood also provided its contacts details for data subjects to inquire about any questions they may have regarding the matter.[41]

For affected data subjects that Rosewood could not contact, Rosewood released a statement on its website outlining the details of the incident that occurred.[42]

Rosewood implemented a "call center" staffed by employees tasked with answering calls from data subjects whose data has been compromised.[43] Its employees are available to address any inquiries or

---

[33] *Id.*
[34] Full Breach Report, 11 April 2022, at 6, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[35] Letter *from* SGH *to* the National Privacy Commission, 19 January 2018, at 1, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2018).
[36] Full Breach Report, 11 April 2022, at 6, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[37] *Id.* at 2.
[38] *Id.* at 8.
[39] *Id.* annex 2.
[40] *Id.*
[41] *Id.*
[42] Post-Breach Report, 01 June 2022, annex 9, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022)
[43] Full Breach Report, 11 April 2022, at 9, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).

provide additional information and assistance.[44] The task involves advising affected data subjects to regularly review their account statements and promptly notify their credit card issuer of any suspicious activity.[45]

To prevent the recurrence of the incident, Sabre took steps to improve its information security program like addressing the secure use of the privileged credentials of SynXis CRS.[46] It also enhanced its password policies and procedures and implemented multi-factor authentication for remote access to SynXiS CRS.[47]

Sabre implemented safeguards such as conducting application and code scanning, maintaining appropriate and up-to-date antivirus protection, conducting regular penetration testing of SynXis CRS components, employing enhanced behavior analytics tools, and undergoing third-party information security assessment.[48]

As an organizational measure, Rosewood maintains that it reviewed its internal policies and procedures to assist Rosewood employees with identifying, responding to, and managing data security incidents, including breaches involving personal data.[49] It also reviewed its Data Security Incident Response Plan in response to data security incidents at Sabre and revised the plan.[50]

Based on the foregoing, the actions taken by Rosewood following the incident allowed it to enhance its security measures and are sufficient to close the matter in accordance with the DPA and NPC Circular 16-03.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-008 In re: Rosewood Hotel Group is considered **CLOSED.**

SO ORDERED.

---

[44] *Id*.
[45] *Id*.
[46] *Id.* at 6.
[47] *Id*.
[48] *Id*. at 7.
[49] Full Breach Report, 11 April 2022, at 7, *in* In re: Rosewood Hotel Group, NPC BN 18-008 (NPC 2022).
[50] *Id*.

City of Pasay, Philippines.
18 April 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

SGH
Counsel for Rosewood Hotel Group
Parlade, Hildawa, Eco & Panga Law

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