IN RE: CEBU AIR, INC. **NPC BN 18-075**

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

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is a breach notification report submitted by Cebu Air, Inc. (Cebu Pacific) in compliance with the Order dated 06 January 2021.

Facts

On 18 May 2018, Cebu Pacific, owner of Cebu Pacific Airlines, received reports from two (2) passengers that they were each presented with the booking information of four (4) other passengers after making their own booking on www.cebupacificair.com.[1]

On 21 May 2018, Cebu Pacific notified the Commission of the breach.[2] According to Cebu Pacific, it believed the incident happened after releasing "the latest version of its Web-based Booking Manager on 18 May 2018" earlier that day.[3] The information involved the following details: Booking Reference Number, Date Booked, Status of Booking, Originating and Destination airports, Date of Departure, and Flight Number, Originating and Destination Airports, Date of Return, Flight Number, Name of the Passengers.[4]

Nonetheless, Cebu Pacific explained:

---

[1] Breach Notification Report – 18 May 2018 Event, 21 May 2018, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[2] *Id.*
[3] *Id.* at 1.
[4] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> No personal information (e.g., passport number, credit card information, passwords, birthday, or email address) was shown immediately other than the name of the guests, the combination of the four elements above was assessed as providing an opportunity for fraudulent changes to existing bookings. However, the combined information can enable a person to modify the booking of those guests associated with the Booking Details.[5]

On 25 May 2018, Cebu Pacific submitted its Full Breach Report.[6] Cebu Pacific reiterated its earlier statement that no other personal information, such as passport number, credit card information, passwords, birthday, or email addresses, was exposed:

> No personal information (e.g., passport number, credit card information, passwords, birthday, or email address) was shown immediately other than the name of the passengers. However, the combination of the four elements above was assessed as providing an opportunity for fraudulent modification of existing bookings associated with the exposed details.[7]

According to Cebu Pacific, its Data Protection Officer (DPO) learned about the incident at 1:00 p.m. of the same date as the breach and immediately reached out to the systems owner, systems support team, and technical support team.[8] The teams verified that the released version of the website contained a bug.[9] The DPO held a conference with the teams to identify extent of the breach and remediation measures.[10]

According to Cebu Pacific, the teams identified "critical factors that should be considered in relation to the confidentiality breach"[11] during the meeting:

> a. Unauthorized disclosure of booking details only happened when an "anonymous guest" created a new booking. 'Anonymous guest' refers to a person who makes a booking

---

[5] *Id.*
[6] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[7] *Id.* at 2.
[8] *Id.*
[9] *Id.*
[10] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

without an existing account in the Corporation's booking management system.

b. Not all anonymous guests who created a new booking were shown the booking details of other passengers.
c. An anonymous guest could not view the same booking information after leaving the booking page. The same held true even if the anonymous guest saved the Uniform Resource Identifier (URI) pertaining to the booking details.[12]

Cebu Pacific determined that while the web booking system was online between 9:15 a.m. and 3:30 p.m., six hundred seventy-four (674) bookings were modified.[13] Cebu Pacific stated "these were the only bookings where possible fraudulent activity could have occurred."[14]

At 3:30 p.m., Cebu Pacific reported that it had also "rolled back the latest version of its web-based Booking Manager, so as to prevent any further exposure."[15]

Cebu Pacific reported that by the time it rolled back the latest version of their website, six hundred seventy-eight (678) bookings were already modified or changed.[16] It reported that it released an email, through its Contact Center, to the contact persons of each of the six hundred seventy-eight (678) bookings that were modified when the website was live, to verify the authenticity of the change in their respective bookings.[17] Cebu Pacific included a template of the email in its Full Breach Report, which had contained a Reference code to validate the recipient of the email.[18] The email states:

> **Manage Booking Notification**
> Today at 7:08
>
> Hi [redacted],
>
> We noticed that there was a change made to your booking on May 18, 2018. This is for your flight with booking reference ABC123.

---

[12] *Id.*
[13] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[14] *Id.* at 3.
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.* at 5.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> If this was you, please disregard this email. No further action is needed.
>
> If this wasn't you, please contact us by replying to this email.
>
> Sincerely,
> **Your Cebu Pacific Team**
>
> . . .
>
> **Note:**
> "*Please do not delete or modify below Reference code to receive your response.*"[19]

After the conference with the systems owner, the systems support team, and technical support team on 18 May 2018, Cebu Pacific reported that it resolved to take the following actions:

> 2.3 Long-Term Remediation — the Corporation further proposed the following actions:
>
> 2.3.1 Send confirmatory notification to every changed booking;
> 2.3.2 Require log-on before allowing any change to a booking; and
> 2.3.3 Review the development and production release processes for increased robustness.[20]

On 19 May 2018, Cebu Pacific called a Disruption Management Team (DMT) Conference to investigate its logs.[21] The purpose of the DMT is "to deal with all unusual events like aviation security, hazardous weather, Information Systems issues, and other similar events."[22] Cebu Pacific reported, however, that it could not identify exactly how many records were exposed:

> Despite these efforts. the Corporation could not exactly determine how many records were exposed other than the eight booking details reported by the two passengers. The failure mode identified indicated that there could have been more than eight such records exposed, but given the nature of the information exposed (as detailed in Section 1 of this Breach Notification Report), the identified fraud risk extended only to

---

[19] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 5, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[20] *Id.* at 3.
[21] *Id.* at 2.
[22] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> the 678 bookings, where a change was executed during the existence of the website bug.[23]

Cebu Pacific determined that based on updated information, "there were only 332 booking changes executed by the anonymous guests and that 346 ("Others") booking changes were effects of system updates."[24]

Cebu Pacific reported that it "constantly monitored customer communication channels for the 332 booking changes."[25] As of 24 May 2018, or before its submission of the Full Breach Report, Cebu Pacific claimed it did not receive "any confirmed fraudulent booking modification either through its Contact Center or customer emails."[26]

Cebu Pacific also reported that it also reviewed documentation "relevant to the system development policies and practices in the business and operations areas" during the DMT Conference.[27] Cebu Pacific explained:

> When the Corporation's review of the system development policies and practices concluded, the teams agreed to incorporate two additional preventive controls: (i) Add severity ranking to the release prioritization level to show increased rigor as early as the testing phase before releasing any system update; and (ii) Add another approver with executive authority when promoting code to the production environment.[28]

Cebu Pacific concluded that it would take the following measures to minimize if not eliminate further damage that may arise from the breach:

> 5.1 Notify Contact when a Booking ls Changed
>
> The Corporation will notify the contact of any booking that will be changed. As a detective control, this approach will enable the Corporation to identify when a fraud is made on a booking and execute the appropriate course of action to protect its passengers.

---

[23] *Id.* at 3.
[24] *Id.*
[25] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[26] *Id.* at 4.
[27] *Id.*
[28] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> 5.2 System Development Policies, Practices, and Processes
>
> The Corporation will implement the controls it identified in its review as described in Section 3.5 of this report.
>
> 5.2.1 Add severity ranking to the release prioritization level. The severity ranking will enable the Corporation to evaluate whether a particular bug can be an acceptable risk when a system update is released
>
> 5.2.2 Add another approver with executive authority. This will enable the Corporation to strengthen the accountability culture in its system development area.[29]

On 07 January 2022, the Commission, through the Complaints and Investigation Division (CID) issued an Order to Cebu Pacific via email, directing to submit a Post Breach Report and supporting documents within fifteen (15) days from receipt:

> This Commission finds the breach notification report lacking details to fully appreciate and determine the compliance of Cebu Pacific with the Data Privacy Act and the issuances of this Commission.
>
> Thus, pursuant to Section 9, Rule IV of the NPC Circular No. 16-03 on Personal Data Breach Management, you are hereby required to submit a Post Breach Report detailing the incident that prompted the notification to the Commission, **provide documentation/ reports as to determination of the extent and number of data subjects affected, the security measures conducted before, during and after the security incident and remedial measures taken to address the incident and prevent its recurrence.**
>
> You are hereby given a period of fifteen (15) days from receipt hereof to submit your compliance through email at complaints@privacy.gov.ph.
>
> SO ORDERED. Pasay City. 06 January 2021 [sic].[30]

[29] *Id.* at 6.
[30] Order, 06 January 2021 [sic], at 1, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Cebu Pacific submitted a Post-Data Breach report dated 19 January 2022 to comply with the CID's Order.[31] Cebu Pacific reiterated its findings in its Full Breach Report, and re-attached it as Annex A.[32]

Cebu Pacific explained further that "[a]part from the eight (8) records reported by the two (2) passengers, however, [it] was unable to determine whether other records were similarly exposed due to safety features built into the system meant to enhance data privacy."[33] It reported monitoring its channels until 25 May 2018. It also reported that it engaged a data breach monitoring service "to investigate the dark web"[34] Cebu Pacific stated that it was able to validate "that no [personal information] appeared in the dark web."[35]

The CID recommended to close the matter based on its assessment,[36] because it does not fall within mandatory notification under NPC Circular 16-03 (Personal Data Breach Management):

> In this case, it appears that only the name and other flight details were compromised. Clearly, the personal data affected in this breach incident only involved personal information. Cebu Pacific reiterated that passport numbers, credit card information, passwords, birthdays, or email addresses were not compromised.
> While it may be true that the incident involved an unauthorized disclosure of passenger flight details to another passenger, with the limited information involved, we cannot think that they may be used to enable identity theft or identity fraud or pose a real risk of serious harm to the data subjects.
>
> **At most, Cebu Pacific specified the possible effect of the incident as to providing an opportunity to change the existing booking details. But which may not be easily possible since confirmation for such change and account log-in are required.**
>
> Although there is reason to believe that the information may have been acquired by unauthorized individuals, we determine that the limited personal data affected by the subject breach cannot be used to enable identity fraud and the incident may not

---

[31] Post-Data Breach Report for May 2018 Case, 19 January 2022, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[32] *Id.* at 6.
[33] *Id.* at 2.
[34] *Id.*
[35] *Id.*
[36] Final Breach Notification Evaluation Report, 13 November 2022, at 9, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2022).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> likely lead to a risk of serious harm and damage to affected data subjects.
>
> Thus, with only one (1) out of three elements for a mandatory breach notification present in this case, it is hereby determined that notification, in this case, is not required.[37]

The CID concluded that the breach posed only minor risks to data subjects, and the Personal Information Controller (PIC) implemented reasonable and appropriate measures to address the incident.[38] According to the CID, there was also no possible violation of the Data Privacy Act (DPA),[39] and as such, notification was not required.[40]

Issue

Whether Cebu Pacific notified its data subjects, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. Cebu Pacific showed that it notified its data subjects and implemented sufficient security measures to address the breach incident, which prevented the real risk of serious harm from materializing.

Contrary to the CID's assessment, however, this matter falls under mandatory breach notification.

Section 11 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.
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity

[37] *Id.* at 8.
[38] *Id.* at 9.
[39] *Id.*
[40] *Id.* at 8.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> 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]

Following this, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
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.[42]

The first requisite is present in this case. The information involved may enable identity fraud.

Cebu Pacific admitted that the exposed information may be and may have been used to fraudulently modify bookings.[43] It reported that it reached out to the six hundred seventy eight (678) affected passengers to "verify the authenticity of the change in their booking" on the same date as the incident.[44] After investigation, it determined on 21 May 2018 or three (3) days after the breach, three hundred thirty-two (332) booking changes were executed by anonymous guests, while three hundred forty-six (346) others were the effects of system updates.[45]

---

[41] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).
[42] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-SS-22-001-and-NPC-SS-22-008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 22 February 2023).
[43] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[44] *Id.* at 3.
[45] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Cebu Pacific reiterated that the exposed personal information did not involve "passport numbers, credit card information, passwords, birthdays, or email addresses."[46]

Further, after the breach, Cebu Pacific constantly monitored its customer communication channels for the three hundred thirty-two (332) anonymous booking changes.[47] Cebu Pacific also reported that it had implemented a log-in requirement for modifications to bookings made within this period.[48]

As of 24 May 2018, Cebu Pacific reported that it had continued to monitor its channels until 25 May 2018[49] and that it did not receive any confirmed fraudulent booking modification.[50]

Nonetheless, the risk that the compromised information will be used for identity fraud is still only lessened, not eliminated, and this was admitted by Cebu Pacific itself.[51] The first requisite is satisfied by the fact that the compromised information enables an unauthorized person to fraudulently modify a passenger's booking as if it were the unauthorized person's own booking.

The second requisite is also present in this case. There was acquisition by an unauthorized person.

The Commission has held that a loss of control over personal data held in custody should be enough for a PIC to have "reason to believe that the information may have been acquired by an unauthorized person."[52]

---

[46] Post-Data Breach Report for May 2018 Case, 19 January 2022, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2022).
[47] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[48] Post-Data Breach Report for May 2018 Case, 19 January 2022, at 3, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2022).
[49] *Id.* at 2.
[50] *Id.*
[51] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[52] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

In this case, Cebu Pacific admitted that two (2) passengers reported having seen others' booking details and names.[53] Further, it admitted in its Full Breach Report that it could not ascertain the exact number of exposed records, and that "[t]here is a possibility that thousands of records could have been exposed to other passengers."[54] The mere viewing of such personal information by the two passengers and other unidentified, unauthorized persons should be sufficient to form a reasonable belief for the PIC.[55]

Given the totality of the circumstances, including the possibility of fraudulent changes being made to the booking of data subjects, the third requisite of real risk of serious harm to the data subject was also present in this case. Nevertheless, the security measures implemented by Cebu Pacific prevented the materialization of such risk of serious harm to the affected data subjects.

Cebu Pacific reported rolling back the released version containing a bug.[56] In its Full Breach Report, Cebu Pacific explained that "this will remove the identified vulnerability which caused the personal breach" and "will prevent any other possible exploit that could threaten the Corporation's further exposure."[57] In total, the released version was up for six (6) hours and fifteen (15) minutes before Cebu Pacific shut it down as a preventive measure.

Cebu Pacific also reported that it constantly and continuously monitored the three hundred thirty-eight (338) booking modifications made during the time the web-based Booking Manager was live.[58] The monitoring continued up to 25 May 2018.

---

[53] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 1, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[54] *Id.* at 2.
[55] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).
[56] Post-Data Breach Report for May 2018 Case, 19 January 2022, at 1, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2022).
[57] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[58] Post-Data Breach Report for May 2018 Case, 19 January 2022, at 2, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2022).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Cebu Pacific also reported implementing a log-in requirement prior to booking modification[59] and sending of email notification to the passenger for validation thereof.[60]

Further, Cebu Pacific reported the addition of preventive controls with respect to releasing system updates.[61] In its Full Breach Report, it explained:

> When the Corporation's review of the system development policies and practices concluded, the teams agreed to incorporate two additional preventive controls: (i) Add severity ranking to the release prioritization level to show increased rigor as early as the testing phase before releasing any system update; and (ii) Add another approver with executive authority when promoting code to the production environment.[62]

Finally, Cebu Pacific also sent emails to its affected data subjects, which gives notice to the recipient that a change was made to their booking on 18 May 2018 (the date of the incident) between 9:15 a.m. and 3:30 p.m.[63] The email states that if there were any unauthorized changes made to the booking, the recipient could contact Cebu Pacific by replying to the same email thread.[64] As such, the email enabled the data subjects to take measures to protect themselves from the consequences of the breach by contacting Cebu Pacific regarding any unauthorized changes.

To reiterate, the first two requisites of mandatory breach notification are present because the nature of the information involved in the breach enables identity fraud and Cebu Pacific admitted there may have been unauthorized acquisition of the information.[65] Nonetheless, the third requisite of real risk of harm to the data subjects did not materialize due to the security measures implemented by Cebu Pacific immediately after the breach. The security measures of the log-in requirement, email notification for validation, email notification to the three hundred thirty-eight (338) passengers whose bookings were affected on 18 May 2018, and constant monitoring until 25 May 2018

---

[59] *Id.*
[60] *Id.* at 3.
[61] *Id.*
[62] *Id.*
[63] Full Breach Report – 18 May 2018 Event, 25 May 2018, at 5, *in* In re: Cebu Pacific, NPC BN 18-075 (NPC 2018).
[64] *Id.*
[65] *Id.* at 1.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

enabled the data subjects to take measures to protect themselves if there were any unauthorized modifications to their booking.

Given the foregoing, the Commission finds that Cebu Pacific's Post-Data Breach Report and Full Breach Report show that it was able to sufficiently notify its affected data subject, address the breach, and implement security measures to prevent its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-075 In re: Cebu Pacific is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
22 February 2023.

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:

RAE
Data Protection Officer
Cebu Air, Inc.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

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

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228