Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: CATHAY PACIFIC AIRWAYS LIMITED **NPC BN NO. 18-198**

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

ORDER

AGUIRRE, D.P.C.:

This Order refers to a breach notification report sent by Cathay Pacific Airways Limited (Cathay) involving one hundred two thousand two hundred nine (102,209) data subjects in the Philippines that were affected; roughly thirty-five thousand seven hundred (35,700) passport numbers from the Philippines that were exposed, and around one hundred forty-four (144) credit card numbers from the Philippines that were accessed.[1]

The Facts

Cathay is an airline company based in Hong Kong Special Administrative Region (HK SAR). As such, Cathay collects personal data of its passengers connected to its services.

The systems connected with the collection of data are composed of: (1) a customer loyalty system (System A) which is used for processing and recording membership of members of Asia Miles, Marco Polo Club and Registered Users; (2) a platform used to support various web-based applications (System B) which is a shared back-end database primarily used to support web-based applications; (3) a reporting tool (System C) that queries the customer information systems data warehouse; and (4) an Asia Miles redemption system (System D) which is a transient database allowing Asia Miles members to redeem non-air awards.[2] The personal data collected in the systems include the passenger name, phone number, address, email address, date of birth, nationality, passport number, identification number, frequent flyer

[1] "Data Breach Notification" dated 25 October 2018.
[2] Report on the measures taken to address the breach dated 15 November 2018, p. 4.

membership number, customer service remarks, and historical travel information depending on the system.[3]

Among Cathay's wholly owned subsidiaries are Hong Kong Dragon Airlines Limited (HK Dragon) and Asia Miles Limited (Asia Miles Ltd). Cathay manages and provides IT support services to HK Dragon and in effect, the personal data of HK Dragon's passengers also resides in Cathay's information systems. Asia Miles Ltd manages and operates Asia Miles, a program provided for the frequent flyer members of Cathay. Together with Cathay, its subsidiaries are also headquartered in HK SAR and their information systems reside within the said territory.[4]

On 13 March 2018, Cathay noted a suspicious activity on its network caused by a brute force attack[5] resulting in approximately five hundred (500) staff users being locked out of their accounts and which affected Cathay, HK Dragon and Asia Miles Ltd. [6]

Based on the examination of the source of the traffic, it was found that a server outside the Philippines was at issue. [7] Upon becoming aware that any of its database was potentially affected, Cathay commenced investigations into the nature of the personal data contained in each database and the purpose of use for that data.[8]

Cathay reported that it engaged a leading cybersecurity firm (CS FIRM) to assist in the investigation, conduct dark web searches for stolen personal data, advise on defensive and containment measures to take, and conduct of a full sweep of its entire environment.[9] Cathay stated that it also worked with other third parties including hosting and managed security providers, experienced counsel with data privacy and cybersecurity experts to coordinate and direct these efforts.[10]

---

[3] Report on the measures taken to address the breach dated 15 November 2018.
[4] Data Breach Notification dated 25 October 2018.
[5] A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing a combination correctly. Technical Report dated 30 October 2020.
[6] Technical Report dated 30 October 2020, p. 1.
[7] *Id.* at *Note 2*.
[8] Report on the measures taken to address the breach dated 15 November 2018, p. 11.
[9] *Id.* at *Note 2*.
[10] *Ibid.*

During the investigation on the nature and scope of the attack and what personal data may have been compromised, Cathay was subjected to continued attacker activities, such as continued remote access to the environment, lateral movement through its networks and installation of additional malware and utilities.[11] It was determined that the systems affected by the incident are System A, System B, System C and System D. [12]

The CS FIRM identified two (2) attackers in the environment. The key activities are as follows:

1. On 31 March 2018, an attacker activity was detected in relation to System C where two database extracts may have been created and accessed by the attacker.

2. On 04 April 2018, CS FIRM discovered that archives had been placed on a server that contained the database backup of the System B and may have been a subject of attacker activity.

3. On 04 May 2018, the attacker remotely accessed Cathay's environment and exfiltrated files identified as partial database backups for the System A.

4. On 06 May 2018, an additional malware was uncovered relating to System C.

5. On 08 May 2018, the attacker accessed the administration console of the System D website to view customer redemption and transaction data and export a database backup.[13]

A total of forty-one (41) user accounts were stolen during the attack. This included accounts that have administrator rights[14] on its systems. Cathay stated that the attackers used malware that was unique with previously unknown signatures and therefore was not detected by Cathay's up-to-date anti-virus system. The attackers also took steps to

---

[11] Report on the measures taken to address the breach dated 15 November 2018, p. 11.
[12] *Ibid.,* at p. 4.
[13] *Ibid.,* at p. 12.
[14] Having administrator rights (sometimes shortened to admin rights) means a user has privileges to perform most, if not all, functions within an operating system on a computer. These privileges can include such tasks as installing software and hardware drivers, changing system settings, installing system updates. They can also create user accounts and change their passwords.

avoid detection, deployed counter forensics, and hid the malware they were using.

By mid-October 2018, it was revealed that the passengers' personal data of Cathay, HK Dragon and Asia Miles Ltd were affected.

Based on Cathay's analysis, a total of one hundred two thousand two hundred nine (102,209) data subjects in the Philippines were affected; roughly thirty-five thousand seven hundred (35,700) passport numbers from the Philippines were exposed and around one hundred forty-four (144) credit card numbers from the Philippines were accessed. These personal data compromised are not cumulative as there may be individuals who fall into all three categories.[15]

On 25 October 2018, Cathay submitted its breach notification report[16] through its counsel, BCCS Office (BCCSLAW) to the National Privacy Commission. Cathay stated that it "has very recently established the types of personal data involved and the number of data subjects in the Philippines whose personal data may have been accessed."[17]

Cathay claimed that no data subject's travel or loyalty profile was accessed in full, no passwords were compromised, and that Cathay found no evidence that any of the personal data has been released.

On 29 October 2018, the Complaints and Investigation Division (CID) ordered Cathay to submit: (1) further information on the measures it had taken to address the breach, which Cathay complied with on 15 November 2018; and (2) an explanation for the failure to timely notify this Commission, which Cathay complied with on 20 November 2018.

In its email dated 15 November 2019, Cathay explained that it had to first fully understand the nature of the personal data affected to provide a meaningful notification to the affected data subjects. It argued that it applied the findings from its data analysis to be able to implement breach notifications in accordance with various legal requirements and prepare a disclosure plan for communications with the affected data subjects, regulators and stakeholders.

---

[15] Data Breach Notification dated 25 October 2018, p. 3.
[16] *Ibid.*
[17] *Id.*, at p. 2.

On 20 November 2018, Cathay sent another response to the Order dated 29 October 2018 issued by this Commission through the CID. With its recognition of the importance of timely notification with the Commission, Cathay claimed that it reacted promptly upon discovering suspicious activity relative to the breach that occurred within its system. It denied delay in notifying regulators as well as the affected data subjects, arguing that it provided notification as soon as practically possible.

In an Order,[18] the CID required Cathay to submit, within fifteen (15) days from receipt, additional documents and/or details regarding the details on how the third-party actor gained entry and the vulnerability of the data processing system that led to it, as well as the security measures in place; and an update on the physical, organizational and technical measures undertaken after the incident. The CID also required Cathay to specify the period and reason for the retention of the personal data including the travel information and expired credit card numbers of the data subjects affected.

On 31 December 2020, Cathay, through its counsel, BCCSLAW, submitted an extension request on the matter, *to wit:*

> x x x While Cathay is exerting best efforts to respond to the Order by the deadline, it anticipates its inability to do so because of difficulties in quickly gathering the required information from the relevant personnel during this holiday season.
>
> Considering that the information and details needed to completely respond to the Order are still being gathered at this time, Cathay respectfully requests to be granted an extension of fifteen (15) days from 2 January 2021, or until 17 January 2021, to respond to the Order.

In its Resolution,[19] the CID granted Cathay's Motion for an Extension of fifteen (15) days from 2 January 2021, or until 17 January 2021, to respond to the said Order.

---

[18] NPC Order dated 16 December 2020.
[19] NPC Resolution dated 05 January 2021.

In its Response, Cathay alleged that based on the tools, tactics and procedures used, the incident was caused by unauthorized access believed to have been conducted by two groups of attackers, *to wit:*

- Group One: The earliest evidence of activity by what is suspected as Group One occurred on 15 October 2014. The last known activity by Group One was on 22 March 2018. It was found that a keylogger malware[20] had been installed on the BRIO server to harvest user account credentials. Using the stolen but valid user account credentials, the attackers accessed Cathay's IT System via its VPN (bypassing the VPN restriction) and the personal data contained therein Group One also moved laterally through the network and placed credential dumping tools in order to extract domain credentials. Group One used the BRIO server to access Cathay's customer information system (**CIS**).

- Group Two: The earliest evidence of activity by what is suspected to be Group Two occurred on 10 August 2017 and the last known activity by Group Two was on 11 May 2018. Group Two exploited a vulnerability of an internet facing server, which enabled them to bypass authentication and gain administrative access. This also enabled Group Two to move laterally within Cathay's environment and install malware and credential harvesting tools. Group Two accessed database backup files of CLS and EBSP, and also accessed iRedeem. In addition, on 28 August 2018, Cathay's IT team detected and prevented an attempted attack which is suspected to have been carried out by Group Two. [21]

Cathay alleged that prior to the incident, the following security measures were taken to ensure personal data was protected against unauthorized or accidental access, processing, erasure, loss, or use, including to prevent its network from attacks:

- Cathay's network was protected from the Internet by 3-leg firewalls;

---

[20] Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored.
[21] CATHAY's Response dated 15 January 2021.

- Cathay's B2C commercial websites were protected by Content Delivery Network with Web Application Firewall (WAF) capabilities;

- Two-Factor Authentication was implemented for privileged IT Support staff;

- Forward proxy and reverse proxy were used to remove malicious outbound and inbound web-based traffic;

- Direct access to customer information systems data warehouse (accessible via the System C server) was granted to authorized users only; and

- A firewall was used to segregate Cathay's network from its service providers' networks. [22]

After the incident, Cathay stated in its Report that it adopted administrative and technical security measures to protect personal data contained in its information systems from any unauthorized or accidental access, processing or use, *to wit:*

1. Information Security Policies and Standards
   Cathay enforces security requirements for staff and all subcontractors, service providers, or agents who have access to Cathay's data.

xxx

2. Security Incident & Response
   All IT incidents are managed in accordance with appropriate incident response procedures. Cathay has a defined incident response procedure to handle security incidents.

   Cathay monitors and alerts suspicious security events and subscribes to incident response services from renowned security service providers to handle specific situations and get intelligence on potential and actual attacks;

3. Human resource security
   Cathay has clearly defined roles and responsibilities for employees. Screening is carried out before employment

[22] CATHAY's Response dated 15 January 2021, p. 5.

with terms and conditions of employment applied appropriately;

Cathay implements phishing simulation exercises to measure the security awareness of employees and a regular security awareness program to train new joiners and existing personnel about their IT security obligations. This program includes training about security practices and a security incident reporting channel;

4. Disaster Recovery
   Cathay implements appropriate disaster recovery and business resumption plans. Cathay reviews both business continuity plans and risk assessments regularly. Business continuity and disaster recovery plans are tested and updated regularly to ensure that they are up to date and effective;

5. Compliance
   IT security policies and standards are monitored and maintained on a regular basis to ensure compliance.

   Cathay has conducted regular internal and external audits and security testing to ensure continuous compliance and effectiveness of security controls and processes over Cathay's data;

Technical measures

1. Operations Security
   Cathay has policies on how to classify information assets and security measures according to their classification.

   Cathay issues guidelines on configuration hardening to secure the system and get updates on an ongoing basis.

   Cathay implements an event monitoring and correlation tool that provides real time analysis and alerting of security issues and has monitoring and auditing facilities for any changes to accounts with privileged access to systems and databases.

   Cathay installs and maintains appropriate anti-malware solutions on different channels: servers, workstations, inbound and outbound emails, internal email, and web browsing. All solutions are updated on a timely basis to ensure they can protect Cathay's systems effectively.

Cathay implements regular security testing on its information systems. All new systems are subject to such testing.

Periodic security scans and tests are conducted to assess the security posture of information systems; all new systems are security tested. All major systems are regularly patched to ensure system integrity and prevent attacks.

Encrypted removal storage devices and network storage are provided to protect sensitive information during storage and transmission.

When media are to be disposed of or reused, procedures are implemented to prevent any subsequent retrieval of any sensitive data stored in them.

2. Network Security
   Cathay maintains network security controls, including web application firewalls, denial of service protection, host-based & network-based firewalls, intrusion detection and prevention systems, network surveillance system, network segmentation, virtual private networks, secure web proxies, secure wireless networks, secure routing and access control lists to protect against malicious attacks.

   Cathay's network is protected from the public network by multiple layers of firewalls and split into difference areas or zones. This zoning allows granular control of the data that can pass between these zones.

   xxx

   Cathay implements services to handle fraudulent actions by preemptively identifying possible attacks and fraudulent sites and to take down suspicious web sites in due course.

   Cathay uses authorized public certificate authority for certificate management lifecycle. Secure algorithms and protocols are used. Cathay has internal certificate authority, with the use of hardware security module for internal certificate management.

   Cathay enforces security controls to prevent incoming virus, spam and phishing emails and protect against spoofing emails.

3. Access Control

All Cathay's employees are assigned unique user IDs to authenticate to the system to ensure accountability

Cathay has established a password policy that prohibits sharing of passwords, governs what to do if a password is disclosed, and requires passwords to be changed on a regular basis and default passwords to be altered. All passwords must fulfil the minimum requirements and are stored in hashes.

Unattended workstations on company premises are protected from unauthorized access by a password-protected screensaver.

Access rights to information are granted based on a "need-to-know" basis and in accordance with "least privilege" principles.

Privileged accounts are managed through the Privilege Identity Management System. All access to privileged accounts is logged and justified. Automatic reset of password of privilege accounts is enforced.

Identity Management System is used to provide and remove staff accounts from the system automatically to ensure prompt access removal.

Cathay has standard operating procedures to define user roles and their privileges, how access is granted, changed and terminated; addresses appropriate segregation of duties; and defines the logging/monitoring requirements and mechanisms.

Cathay has procedures in place to ensure that all requested changes are authorized and obsolete access rights for the centralized identity store are revoked appropriately

Cathay has a Data Loss Prevention solution for selected users that detects potential data breaches/data exfiltration transmissions and prevents such transmissions by monitoring, detecting and blocking

Physical security

Cathay maintains physical security systems at all company sites where there are information systems that use, process,

> transmit or store Cathay's data. Access to data centers is restricted to authorized personnel only.
>
> Physical access controls have been implemented for all such sites to prohibit unauthorized access. Access to all company sites is monitored 24x7 by security personnel and surveillance cameras. All access tokens or keys must be returned when a staff member is leaving Cathay. Visitor access to such sites is pre-registered and requires approval. Visitors are to be escorted.
>
> Cathay uses uninterrupted power supplies to ensure power availability to data centers and employs environmental devices to ensure a stable and sustainable operating environment for the computing facilities. Cathay has contingency plans defined and tested to ensure that core services are not disrupted by incidents. [23]

Aside from conducting an immediate investigation on the brute force attack resulting in staff users being locked out of their accounts, Cathay stated in its report dated 15 November 2018 that it performed the following actions to address the breach:

1. Upon becoming aware that any particular database was potentially impacted, Cathay commenced investigations into the nature of the personal data contained in each impacted database and the purpose of use for that data;

2. Cathay engaged a leading cybersecurity firm, CS FIRM, to assist in the investigation;

3. CS FIRM was also engaged to conduct searches of the dark web and assess whether the compromised personal data appeared in Chinese underground markets or in English speaking darknet community to identify possible misuse of the personal data accessed which normally involves monetizing such information;

4. Cathay also began working with other third parties including hosting and managed security providers, experienced counsel

[23] Administrative and Technical Measures. Attachment 1, CATHAY's Response dated 15 January 2021.

with data privacy and cybersecurity expertise to coordinate and direct these efforts;

5. In relation to the personal data compromised, Cathay applied the process of reconstruction, consolidation, de-duplication and made a detailed analysis of the incident to determine the scope of data accessed, as well as the number of affected data subjects;

6. Cathay offered various service channels to assist the data subjects who are affected by the incident such as a dedicated sub-page of Cathay's website Cathaypacific.com and an enquiry mechanism therein, a dedicated customer call center with a toll-free number for Hong Kong and other countries, including the Philippines, and a dedicated email address at [ ];

7. Cathay notified the regulators of different jurisdictions about the incident including coordination with the Cyber Security and Technology Crime Bureau of the Hong Kong Police on the investigation of the incident; and

8. Cathay sent notifications to all affected data subjects via email, post and general/substitute notice.

In its Report dated 15 November 2018, Cathay reported the following measures undertaken to prevent the incident from recurring: [24]

1. Cathay worked with a forensic investigation firm, as well as other cybersecurity experts; and

2. Cathay narrated its IT security program upgrade that commenced from 2014 under the overall infrastructure upgrade program;

3. Cathay enforced a comprehensive framework of data protection policies, manuals and guidelines, ensuring the fair, lawful and secure processing of personal data;

4. Cathay established a robust data protection organization;

[24] Report on the measures taken to address the breach dated 15 November 2018.

5. Cathay implemented a Privacy Impact Assessment (PIA) process;

6. Cathay maintains a Record of Processing Activities (RPA). Cathay has a designated Data Governance team responsible for the management and ongoing maintenance of the RPA;

7. Cathay has established a supplier management process;

8. Cathay regularly reviews and enhances its cybersecurity policies and processes;

9. Cathay has further enhanced its Personal Data Incident response protocols;

10. Cathay has in place training programs for its employees to strengthen their security awareness;

11. Cathay has enhanced its user, vendor, endpoint, network life cycle control framework;

12. To further enhance its data security, Cathay has enhanced its:
    a. Enterprise-wide encryption program;
    b. Enterprise test data management framework;

13. Cathay has reviewed its identity management coverage;

14. Cathay has reviewed its remote access security and established a policy to govern the remote access lifestyle;

15. Cathay has further enhanced its network segmentation;

16. Cathay is implementing unified cloud security platform for managing the security of its overall SaaS infrastructure. Additionally, Cathay has reviewed protection of application API's to prevent security attacks and abuse;

17. Cathay has subscribed to threat intelligence feeds providing up-to-date information on the latest cybersecurity threats;

18. Cathay is extending the coverage of its data loss prevention program;

19. Cathay has completed PCI DSS (Payment Card Industry Data Security Standard) Attestation of Compliance audits; and

20. Remediation measures had been taken to enhance the security and monitoring of its environment, including:[25]
    a. Enhancing visibility;
    b. Rebuilding its systems;
    c. Blocking of threat actors;
    d. Resetting passwords and monitoring changes;
    e. Provision of authentication;
    f. Upgrading user directory; and
    g. Restriction and segmentation of network traffic.

Discussion

Upon careful examination of the reports and documents submitted by Cathay, the Commission finds the absence of any proof of the said notification to the affected data subjects. NPC Circular No. 16-03[26] requires that all actions made by a personal information controller should be property documented. This includes compliance with the notification requirements and assistance to affected data subjects:

> **SECTION 9.** ***Documentation.*** All actions taken by a personal information controller or personal information processor shall be properly documented. Reports should include:
>
> A. Description of the personal data breach, its root cause and circumstances regarding its discovery;
>
> B. Actions and decisions of the incident response team;
>
> C. Outcome of the breach management, and difficulties encountered; and

[25] Administrative and Technical Measures. Attachment 1, CATHAY's Response dated 15 January 2021.
[26] National Privacy Commission, Personal Data Breach Management, Circular No. 16-03 (December 15, 2016).

> D. Compliance with notification requirements and assistance provided to affected data subjects.
>
> A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor.

As to the manner of notification to the affected data subjects, Section 18(A) of NPC Circular No. 16-03 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.[27]

Moreover, Section 18(D) of same Circular provides that:

> Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach**: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish means

[27] National Privacy Commission, Personal Data Breach Management, Circular No. 16-03 (December 15, 2016). Emphasis supplied.

> through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[28]

The Commission, in its Resolution for NPC BN 20-161, emphasized the importance of ensuring that affected data subjects receive timely notification:

> It is noteworthy that the avowed purpose of the required notification to data subjects of a breach incident is for them to take the necessary precautions or other measures to protect themselves against possible effects of the breach. Moreover, personal information controllers (PICs) are required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. It therefore follows that PICs should guarantee that the notification they sent to data subjects has been received. Otherwise, it defeats the very purpose of notification of data subjects.[29]

Notification of the affected data subjects in cases of personal data breach is an essential obligation in data privacy protection. Section 20(f) of the DPA of 2012[30] states that:

> SEC. 20. *Security of Personal Information.* –
>
> xxx
>
> (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. 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.

---

[28] *Id.* Emphasis supplied.
[29] NPC BN 20-161, 17 December 2021.
[30] 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], Republic Act No. 10173 (2012).

The Commission notes that Cathay failed to provide proof of notification to affected data subjects and their receipt thereof and merely stated the following in its Notice of Information Security Breach:[31]

> **I. Measures Taken to Address the Breach**
>
> x x x
>
> **d. Action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification.**
>
> Notification of all affected data subjects, including all affected data subjects in the Philippines, was done via three channels:
>
> (i) **By email**: for the affected data subjects who are Marco Polo Club members, Asia Miles members and Registered Users of Cathay (the "**Member Group**"), where Cathay had an email address in its records.
>
> (ii) **By post**: for the affected data subjects who are part of the Member Group, where Cathay had a postal address (and did not have an email address) in its records and for the affected data subjects located in the US where notification by post is required by law.
>
> **(iii) By general/ substitute notice**: for affected data subjects that do not fall within categories (i) and (ii) above. A general notice was placed on the website https://infosecurity.cathaypacific.com ("**Website**") to notify the affected data subjects in Hong Kong and the rest of the world (excluding the US) who Cathay was unable to contact. For the US, a substitute notice was placed on the Website in accordance with the legal requirements of the various US states to notify the affected data subjects for whom Cathay did not have contact details. The US substitute notice is a US specific notice which consists of elements required by the laws of the various US states.
>
> On 25 October 2018, Cathay commenced sending the personalised email notifications to the Member Group. Cathay completed sending the personalised email

[31] E-mail from PRC & KRI," Re: Notice of Information Security Breach: Cathay Pacific Airways Ltd (Hong Kong) Ref. No. CID BN No. 18-198." dated 15 November 2018.

> notifications to the Member Group on 28 October 2018. 3,252,559 email notifications were sent to the Member Group.
>
> On 2 November 2018, Cathay commenced the dispatch of 74,792 postal mail notifications to the affected data subjects in the Member Group for whom Cathay does not have an email address and as required by US state laws. This batch of physical letters was dispatched on 8 November 2018. A further batch of 265,511 postal mail notifications was dispatched on 12 November 2018 to the affected data subjects with invalid email addresses.
>
> Remaining data subjects have been notified either via the substitute notice (US) or via the general notice on the Website which went live on 24 October 2018, shortly after the Hong Kong Stock Exchange announcement.
>
> Of those notified by email or post, there are approximately 64,035 data subjects believed to be in or from Philippines who Cathay contacted by email and approximately 5,024 data subjects who have postal addresses in the Philippines that Cathay contacted by mail.

The Commission notes that Cathay did not provide proof of its reported notification of sixty-four thousand thirty-five (64, 035) data subjects believed to be from the Philippines by email and five thousand twenty-four (5, 024) data subjects who have postal addresses in the Philippines by mail. There is also no explanation on the discrepancy between these numbers and Cathay's analysis of a total of one hundred two thousand two hundred nine (102,209) affected data subjects in the Philippines; roughly thirty-five thousand seven hundred (35,700) exposed passport numbers from the Philippines and around one hundred forty-four (144) accessed credit card numbers from the Philippines.[32]

WHEREFORE, all premises considered and pursuant to the requirements of Section 18(A) and Section (D) of Circular No. 16-03**,** the Commission **ORDERS** Cathay Pacific Airways Limited to submit evidence of notification to the affected data subjects in or from the Philippines and explain any discrepancy from its abovementioned

[32] Data Breach Notification dated 25 October 2018, p. 3

analysis of affected data subjects, exposed passport numbers, and accessed credit card numbers, **within fifteen (15) days** from receipt of this Order.

SO ORDERED.
City of Pasay, Philippines;
18 March 2021.

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:

ATTY. PRC
Betita, Cabilao, Casuela, Sarmiento Law
Representative of Cathay Pacific Airways Limited

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