The Cathay Pacific Breach: Is Data Protection and Cyber Security Law in Hong Kong about to receive an upgrade?

June 2019

Hogan Lovells

The Cathay Pacific Breach: Is Data Protection and Cyber Security Law in Hong Kong about to receive an upgrade?

Background

On 6 June, 2019, the Privacy Commissioner for Personal Data (the "**PCPD**") issued an enforcement notice against Cathay Pacific Airways (and its affiliate Hong Kong Dragon Airlines) (together, "**Cathay Pacific**") in respect of a data breach concerning unauthorized access to the personal data of some 9.4 million Cathay Pacific customers.

The PCPD's enforcement notice concerns compliance with two aspects of the Personal Data (Privacy) Ordinance (the "**PDPO**"):

- the obligation under Data Protection Principle 4 ("**DPP 4**") to take all practicable steps to ensure that personal data are protected against unauthorized access; and
- the obligation under Data Protection Principle 2(2) ("**DPP 2**") to take all practicable steps to ensure that personal data is kept no longer than necessary for the fulfilment of the purposes for which it has been lawfully collected.

At the time of writing, it was not clear if Cathay Pacific will appeal the enforcement notice.

Key Take-Aways

The scale of the Cathay Pacific data breach, together with the lapse of time between its discovery and reporting, have generated significant publicity in Hong Kong and overseas, and so there is fair speculation that Hong Kong's Legislative Council may follow the lead of many other jurisdictions in introducing a mandatory data breach notification obligation to the PDPO.

Hong Kong's past reforms to the PDPO have been "event driven", the best example being the Octopus Rewards case in 2010, which led to extensive reforms to Hong Kong's direct marketing controls. There is no question that the enforcement action against Cathay Pacific could generate a similar effect in relation to information security management aspects of the PDPO and in a mandatory breach notification obligation. Comprehensive mandatory data breach notification obligations have now been introduced in Australia, the Philippines, Taiwan and South Korea, with Singapore likely to move to introduce such a measure in the near future. The PCPD has published guidance that encourages breach notification, but in line with similar measures in China and Japan, this remains a recommended best practice rather than a mandatory requirement.

The PCPD's enforcement notice may also support class action civil suits in some jurisdictions, and in doing so rekindle the debate in Hong Kong as to whether or not Hong Kong's stalled efforts to implement a class action regime should move forward so as to create more incentive for organizations to implement effective cyber security planning and incident response measures.

In terms of more immediate effects, the Cathay Pacific enforcement notice raises a number of key practical compliance points for organizations:

- the failure of an organization to have completed a data inventory may support a finding of a breach of DPP 4;
- multi-factor authentication may now be a requirement under DPP 4 for remote access to personal data by company employees; and
- DPP 4 compliance may require organizations to take appropriate professional advice on information security matters and ensure that best practices are being followed.

The Incident

According to the Investigation Report accompanying the enforcement notice, the Cathay Pacific breach likely involved more than one party and related to more than one vulnerability in Cathay Pacific's systems. It is also clear that the breaches had been underway

for some time before they were ultimately detected:

- **Which systems were impacted?** The attacks impacted four separate systems: (i) the customer loyalty system, (ii) a shared back-end database used to support web-based applications, (iii) a reporting tool that extracted and complied data from other databases; and (iv) a database used to allow customers to redeem non-air rewards through the Air Miles loyalty scheme.
- **When did Cathay Pacific commence its investigation?** Cathay Pacific's internal investigations were initiated in response to a brute force attack on 13 March, 2018, which locked some 500 Cathay Pacific employees out of their user accounts. The ensuing internal investigation confirmed by 7 May, 2018 that there had been unauthorized access to company data, with a subsequent attack commencing the next day and a further attempted attack initiated in August, 2018.
- **Who was impacted?** Cathay Pacific has concluded that passengers, including members of its Asia Miles reward scheme, totalling some 9.4 million individuals from over 260 jurisdictions.
- **What data was compromised?** The personal data compromised in the attacks varied depending on the system and databases being compromised, but in the majority of cases was limited to passenger names, flight numbers and dates, title and email addresses. In a third of cases, customers' membership numbers were compromised, and in a quarter of cases, addresses were obtained. In nine percent of cases, the customer's passport number was compromised and in six per cent of cases, the individual's identity card number. In 430 cases, individual credit card numbers were compromised, although the vast majority of these had expired. Customer passwords used to access profiles were not compromised through the attacks.
- **When and how did the attacks begin?** Cathay Pacific's investigation revealed two separate groups of attacks. The earliest compromise of its systems took place in 15 October, 2014, around which time stolen user account credentials were used to implement keystroke logging malware on the reporting tool system. Unauthorized access through this malware was stopped on 22 March, 2018. The second group of attackers is understood to have exploited a vulnerability in an internet-facing server to circumvent controls on administrative access to the impacted systems. The earliest known date at which personal data was actually compromised was 7 September, 2016. As noted above, Cathay Pacific's investigators did not conclude there had been unauthorized access to personal data through either means of attack until May, 2018.
- **When did Cathay Pacific start to notify data subjects?** Cathay Pacific notified the PCPD of the breach on 24 October, 2018 and commenced the notification of impacted individuals the next day.

The PCPD's conclusions

It is important to note that the PDPO does not require "data users" (organizations controlling the processing personal data) to notify the PCPD or impacted data subjects after they discover a data security breach. This is the case whether or not the PDPO has actually been breached in the course of the incident.

The PCPD's investigation therefore came to focus primarily on Cathay Pacific's compliance with DPP 4's obligation on data users to take all reasonably practicable steps to protect personal data against unauthorized access and whether Cathay Pacific had failed to meet these requirements in allowing the attacks to succeed.

In reviewing the types of personal data that had been compromised in the attacks, and the purposes for Cathay Pacific holding it, the PCPD also considered Cathay Pacific's obligations under DPP 2 to erase personal data which is no longer needed.

DPP 4 Analysis: Data Security

The PCPD's investigation report cites past appeals to the Administrative Appeals Board (the "**AAB**"), which hears appeals from the PCPD's enforcement notices, noting that DPP 4 compliance is to be judged on a case-by-case basis. The "reasonably practicable steps" that organizations are required to take to protect the personal data they process is to be assessed on the basis of whether or not they are proportionate to the harm that could result from unauthorized access to the specific data in question. Citing the decision in AAB Decision 70/2016, the PCPD considered that DPP 4 does not set a standard of perfection, but does require data users to take all reasonably practicable steps to secure data in the specific circumstances.

The PCPD's DPP 4 analysis came to the following key conclusions:

- A vulnerability scan of the internet-facing server carried out by Cathay Pacific in 2017 had not detected the critical vulnerability, even though: (i) details of this vulnerability had been widely published since 2007 and so was well-known to the industry at this time; and (ii) the scanning tool deployed by Cathay Pacific was equipped in 2013 to detect this particular vulnerability.
- Cathay Pacific's annual scan of the internet-facing server was insufficiently frequent.
- Cathay Pacific's administrator console had been configured to be accessible externally rather than limited to internal network access, and this was found to be deficient.
- Prior to the identification of the vulnerability, only Cathay Pacific's IT support teams were required to use multi-factor authentication to access internal systems remotely (an oversight remedied in July, 2018).
- Cathay Pacific did not encrypt database backup files used to support database migrations carried out between 2016 and 2018.
- Cathay Pacific did not start assembling a personal data inventory until August, 2017, but in any event had not completed this exercise when the unauthorized access was discovered.

Based on these points, the PCPD found that Cathay Pacific was in breach of DPP 4.

DPP 2 Analysis: Data Retention

The PCPD's investigation report notes that Cathay Pacific had policies in place directing that information should not be kept longer than is necessary for the purposes for which it was collected and that information was, in any event, to be purged once the relevant customer's file had been marked inactive for seven consecutive years. Notwithstanding these policies, Cathay Pacific was found to have retained approximately 240,000 Hong Kong Identification Card numbers for thirteen years after it had dispensed with using this data for identity verification purposes. This unnecessary retention was in breach of DPP 2.

The delay in notification

Cathay Pacific notified the PCPD of the security breaches on 24 October, 2018 and started notifying impacted data subjects the next day. These notifications came seven months after the initial attack and five months after Cathay Pacific's internal investigations detected unauthorized access. These notifications were voluntary in nature, given that the PDPO does not include a data breach notification obligation.

Cathay Pacific explained that the delay in notification was due to the highly technical

nature of the investigation and the airline's desire to fully and accurately understand the nature and scope of the breach, and in particular the types of personal data compromised, so as to be in a position to provide a constructive notification to impacted individuals.

The PCPD found that Cathay could have made its notification sooner, although this delay was not in itself a breach of the PDPO.

The Enforcement Notice

Having found Cathay to have breached DPP 2 and 4, the PCPD directed Cathay Pacific to do the following:

1. engage an independent data security expert to overhaul the systems containing personal data to ensure that systems are free from malware and known vulnerabilities;

2. implement effective multi-factor authentication for all remote users of its systems and undertake regular reviews of remote access privileges;

3. implement an appropriate vulnerability scanning program;

4. engage a data security expert to conduct regular reviews on the security of its networks;

5. devise, implement and enforce a clear data retention policy;

6. provide the PCPD with documentary proof of compliance of items 1 through 5 within six months of the date of the enforcement notice; and

7. erase all unnecessary Hong Kong identity card data from its loyalty program systems and provide independent third party certification of this having been done within three months from the date of the enforcement notice.

In its supporting commentary, the PCPD noted the increasing risks posed by data security breaches and recommended that organizations redouble efforts to be accountable for personal data, including efforts by the PCPD to ensure that data protection is a matter of high level governance within organizations (and not just within their IT departments), including as recommended through the PCPD's Privacy Management Programme.

A question of class (actions)?

The PCPD's conclusions and decision to issue an enforcement notice will, no doubt, reignite the discourse around whether Hong Kong should implement a class action regime for consumer cases. In a class action, a representative plaintiff sues on behalf of itself and all the other persons who have a claim in respect of the same (or a similar) alleged wrong, and whose claims raise the same questions of law or fact.

Specialist class action plaintiff lawyers in the U.S. and Europe have been readying themselves for mass claims against Cathay Pacific since the data breach was first announced – the PCPD's findings will only add fuel to that fire.

In May 2012, the Law Reform Commission of Hong Kong (the "**LRC**") published its Report on Class Actions, recommending the introduction, under an incremental approach, of a class action regime, following which the Department of Justice established a cross-sector working group (the "**Working Group**") to study and consider the LRC's recommendations.

As recently as April 17, 2019, the Secretary for Justice stated that it had (at that date) held 25 meetings since its inception while a sub-committee set up under the Working Group had met 30 times.

The Working Group's current position is that time is required for more in-depth analysis, including of the proposed definition of "consumer cases", certification criteria for a class action to be adopted by the Hong Kong Courts, the design of the procedural rules and other ancillary measures.

A draft public consultation document is, so we understand, being compiled, although there is no definitive timetable yet for consultation.

It is unsurprising that the Department of Justice is taking its time on this issue: there are competing public policy considerations. On the one hand, a class action regime would likely enhance access to justice and provide an efficient (and faster) mechanism for dealing with consumer cases. On the other hand, there is a concern about inadvertently creating a more litigious society, such as in the US. The LRC's recommendation of an incremental approach was designed to ameliorate the risk of the latter but the concern is a real one.

The Department of Justice may consider that, in light of the PCPD's findings against Cathay Pacific, data breaches could be a suitable testing ground for a fledgling class action regime in Hong Kong. This may accelerate the Working Group's analysis. There may be good reason to consider data breach class actions as an effective means of encouraging greater compliance by organizations with the PDPO. The PCPD is equipped with limited resources and does not necessarily have the expertise in house to consider the often highly technical matter of compliance with DPP 4. The prospect of class action litigation can support funding of appropriate expertise and ensure higher rates of compliance with this increasingly critical area of the PDPO.

This is definitely a space to watch, with interest. From our extensive experience defending class actions in the U.S. and elsewhere, any movement towards a similar regime would significantly alter Hong Kong's legal landscape. Whether that is for the better or not remains to be seen.

Key Contacts

Mark Parsons

Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Mark Lin

Partner, Hong Kong
T +852 2840 5091
mark.lin@hoganlovells.com

Byron Phillips

Registered Foreign Lawyer, Hong Kong
T +852 2840 5960
byron.phillips@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices

www.hoganlovells.com