Written submission by
Cathay Pacific Airways Limited
for the
Joint Meeting on Wednesday, 14 November, 2018
of the
Panel on Constitutional Affairs,
Panel on Information Technology and Broadcasting,
Panel on Security

The Legislative Council ("**LegCo**") has requested Cathay Pacific Airways Limited ("**Cathay**") to attend a joint meeting of the Panel on Constitutional Affairs, Panel on Information Technology and Broadcasting and the Panel on Security on Wednesday, 14 November, 2018. The request also invited a written submission for the joint meeting to be provided on or before noon, 12 November 2018. The written submission is set out below.

On 24 October 2018, Cathay notified the Privacy Commissioner for Personal Data, the Hong Kong Police and the Hong Kong Stock Exchange, and shortly thereafter, other applicable regulators and affected passengers, of unauthorised access to certain IT systems of Cathay that affected the personal data of certain passengers in Hong Kong and elsewhere around the world.

Before setting out the details of what happened and what actions have been taken, Cathay wishes to publicly express its great regret over this incident and to extend its sincere apologies to those passengers affected. Cathay attaches great importance to its relationship with the people of Hong Kong and is committed to improving itself so that we can continue to earn their confidence and their trust.

Throughout our investigation of this incident, our foremost objective and primary motivation has been to support our affected passengers by providing accurate and meaningful information to them. Cathay respects the fact that all personal data needs to be protected and is important to the individual and we take our passengers' concerns caused by this incident very seriously. The investigation was complex, longer than what we would have wished and we would have liked to have been able to provide this information sooner.

What happened?

Cathay and our affected passengers are victims of a cybercrime carried out by sophisticated attacker(s). Upon discovery we immediately launched a comprehensive investigation with the help of external experts to determine what occurred and what information was affected. Very early in the investigation, Cathay verified that its operations and flight safety systems were not impacted and flight safety was never compromised. The investigation continued focussing on three objectives: (i) investigation, containment and remediation; (ii) confirming which data had been accessed and whether it could be read by the attacker(s); and (iii) determining the types of personal data that pertain to each affected passenger and notification. Once we met these objectives, we notified affected passengers and relevant authorities.

Who was affected and what information was accessed?

The affected passengers include members of the Asia Miles programme and the Marco Polo Club, as well as non-member passengers who travelled on Cathay or Cathay Dragon services. Our investigation revealed that approximately 9.4 million passengers globally were affected by this incident.

Types of personal data that were found to be accessed include passenger name, nationality, date of birth, phone number, email address, postal address, travel document and/or passport number, identity card number, frequent flyer membership number, customer service remarks, and/or historical travel information. The combination and number of personal data accessed varied by affected passenger. Our analysis revealed that, for the majority of affected passengers, the data accessed was limited to either passenger name and phone number or passenger name and email.

Our investigation also revealed that, although our systems designed to process payment information appropriately masked credit card details, a very small number of mostly expired credit card numbers were accessed by the attacker(s) because they had been improperly entered into a field not intended for credit card data. In no case was the credit card data complete.

No passenger's travel or loyalty profile was accessed in full, and no passenger passwords were compromised.

During our investigation, Cathay has employed cybersecurity experts to search the dark web and other sites. On the basis of such searches to date, we have found no evidence that any of the stolen data has appeared in these forums. Cathay will continue these searches.

Supporting our passengers

Cathay believes that it was important to fully and accurately understand the scope and specific details of the personal data that had been taken from each affected passenger so as to be able to provide a meaningful, individualised notification to them.

Cathay put in place a comprehensive global notification and customer care plan in the form of individual notification letters via email or post, identifying for each passenger which types of data relating to them had been taken. A more general notice for passengers who could not be contacted individually was placed on the dedicated webpage set up by Cathay at infosecurity.cathaypacific.com.

In addition to the individualised notifications, Cathay set up various customer care channels to assist passengers who were affected by the crime, including establishing a dedicated customer call centre with a toll free number for Hong Kong passengers and a dedicated email address (infosecurity@cathaypacific.com) for passengers to enquire specifically about the data theft.

The statistics below set out the global take up by affected passengers of these customer care channels:

Service channel	Statistics to midnight 12 November 2018
Website	181,700 page views
Call centre enquiries	5,031 calls received
Enquiry mechanism on the Website	19,005 enquiries received
Emails received by infosecurity@cathaypacific.com	5,622 emails received

Cathay also continues to offer affected passengers the option of enrolling at no-cost in IdentityWorks, an ID monitoring service offered by Experian in countries where it is possible to offer the service, which includes Hong Kong. As at midnight 12 November 2018, approximately 50,271 passengers had enrolled.

Experian works with many leading companies, financial institutions and government agencies around the world and our research indicated that their ability to search the web (including the dark web) for evidence of unauthorized personal data usage is valuable for affected passengers. This service is optional and each passenger can choose which types of personal data they wish to input for monitoring purposes. Experian was involved in a security incident in 2015, but Experian's consumer credit database was not accessed. In Experian's continued efforts to improve security, they embarked on a global cybersecurity initiative to bolster global security and implemented standards to identify, protect, detect and respond to cybersecurity threats. Experian continues to meet all global data protection and security standards.

Cathay IT security

Cathay recognises the critical importance of IT security. Over the past three years, we have spent over HK$1 billion on IT infrastructure and security. Cathay has a dedicated team of IT security specialists who were specifically not impacted in the 2017 organisational re-design. They are responsible for overseeing IT security and their work and expertise is complemented by leading industry experts. Cathay is cognizant that changes in the cybersecurity threat landscape continue to evolve at pace as the sophistication of the attackers improves. Our plans, which include growing our team of IT security specialists, will necessarily evolve in response to this challenging environment.

Why has the investigation taken so long?

Our investigation and response to this incident involved three sequential and overlapping phases: (i) investigation, containment and remediation; (ii) confirming which data had been accessed and whether it could be read by the attacker(s); and (iii) determining the types of personal data that pertain to each affected passenger and notification.

The first phase commenced in March 2018 when Cathay first detected suspicious activity on its network and took immediate action to understand the incident and to contain it. Cathay did this with the assistance of a leading global cybersecurity firm. During this phase of the investigation, Cathay was subject to further attacks which were at their most intense in March, April and May but continued thereafter. These ongoing attacks meant that internal and external IT security resources had to remain focused on containment and prevention. Remediation activities began as part of this effort and continued throughout. Even as the number of successful attacks diminished, we remained concerned that new attacks could be mounted.

These ongoing attacks also expanded the scope of potentially accessed data, making the challenge of understanding it more lengthy and complex in phase two of the investigation.

During the second phase, the two big issues were: which passenger data had been accessed or exfiltrated and, since the affected databases were only partially accessed, whether the data in question could be reconstructed outside Cathay's IT systems in a readable format useable to the attacker(s). Conclusions on these issues proved difficult and time-consuming and were only reached in mid-August.

During the third phase, the emphasis shifted to identifying the compromised data types for each affected passenger. Cathay wanted to be able to give a single, accurate and meaningful notification to each affected passenger, rather than to provide an overly broad and non-specific notice. It was not until 24 October that Cathay had completed the identification of the personal data that pertained to each individual passenger. In parallel, arrangements were made to allow Cathay to respond promptly to passenger enquiries (see Supporting our passengers above). On 24 October 2018, disclosures and notifications began and we commenced notifying the affected passengers from 25 October 2018.

In summary, the nature of this attack involved a number of complex systems that took significant time to analyse. An enormous amount of work was involved in the investigation, which was highly technical. The process by which the stolen data could be identified, processed, and linked to a specific passenger also contributed to the length of time involved between initial discovery and public disclosure.

……

In closing, Cathay would like to apologise again to our passengers for the incident and any concerns that it has caused. We take our responsibilities with respect to our passengers' personal data very seriously and we acknowledge that there many lessons that we can and will learn from this event.

Cathay Pacific Airways Limited
November 2018