For discussion on
14 November 2018

Joint Meeting of the Legislative Council
Panel on Constitutional Affairs,
Panel on Information Technology and Broadcasting and
Panel on Security

The Incident of Leakage of Passengers' Personal Data by Cathay Pacific Airways and Issues relating to Protection of Personal Data and Cyber Security

Purpose

This paper briefs Members on the follow-up actions taken by the relevant government departments and the Office of the Privacy Commissioner for Personal Data ("PCPD") in response to the incident of leakage of passengers' personal data by Cathay Pacific Airways Limited ("Cathay Pacific").

Work on Personal Data Protection

2. Cathay Pacific announced the incident of leakage of passengers' personal data in the evening of 24 October 2018. The PCPD issued a media statement the next day (25 October) to express its serious concern over the incident and its decision of initiating a compliance check. The PCPD also advised Cathay Pacific to notify affected clients as soon as possible, and to take remedial measures with details explained immediately. The PCPD wrote on the same day to Cathay Pacific to request for detailed information on the incident on or before 5 November 2018 and urged the company to enhance its information security measures. Besides, the PCPD issued another statement on the day to remind members of the public via the media that if they detected any abnormalities with their personal accounts at Cathay Pacific or credit card accounts, they should take the initiative to contact

Cathay Pacific and relevant financial institutions for follow-up, and they should also change account passwords for the accounts and enable two-factor authentication as soon as possible to protect their own personal data. In response to public and media enquiries, the PCPD also appealed to various sectors of the community to contact the PCPD and seek legal assistance if they could prove that they suffered damages caused by the incident and would like to file a claim.

3. The PCPD received a reply from Cathay Pacific on 5 November, and the Privacy Commissioner for Personal Data was of the view that there were reasonable grounds to believe that there might be a contravention by the company of requirements under the Personal Data (Privacy) Ordinance ("PDPO"). In a media statement issued on the same day, the PCPD announced its decision to commence a compliance investigation against Cathay Pacific and its wholly owned subsidiary, Hong Kong Dragon Airlines Limited, pursuant to section 38(b) of the PDPO.

4. As at 5 pm on 8 November, the PCPD received 131 enquiries and 101 complaints, as categorised below:

Enquiries

Nature of enquiries	**Number of enquiries (a single enquiry may be of multiple nature)**
Expressed concern about the Cathay Pacific incident (mainly about inadequate security measures)	72
Enquired what they as Cathay Pacific's clients could do to minimise the impact	63
Enquired about PCPD's follow-up actions	17

Complaints

Nature of complaints	**Number of complaints (a single complaint may be of multiple nature)**
Dissatisfied with Cathay Pacific's leakage of personal data	101
Asked for compensation from Cathay Pacific	36
Dissatisfied with the fact that Cathay Pacific did not disclose the case until seven months after discovering the leakage of clients' data	34
Wanted to know the places to which and the persons to whom their personal data was leaked	8
Dissatisfied with the prolonged retention of clients' personal data by Cathay Pacific	5
Queried when and under what circumstances Cathay Pacific collected their HKID card numbers	7
Suspected receiving phishing emails as a result of the leakage of personal data	1
Asked for compensation from Cathay Pacific according to the European Union's General Data Protection Regulation	1

5. Among the 131 enquiries mentioned above, 93 were made via telephone hotline while the 38 were written enquiries. The PCPD had replied to all the enquiries. Regarding the 101 complaints, the PCPD has informed the complainants that they had commenced the compliance check/investigation. To those who wish to seek compensation from Cathay Pacific, the PCPD has explained the details of application for and approval of legal assistance, and provided them with relevant reference

material.

Progress of Investigation of Data Leakage

6. The Hong Kong Police Force ("HKPF") received a report on 25 October 2018 from Cathay Pacific, stating that some of the passengers' data from its computer systems was accessed to without authorisation. The case is being handled by the Cyber Security and Technology Crime Bureau (CSTCB) of the HKPF and is still under investigation.

7. CSTCB, on the day of receipt of the above report, met with the representatives from Cathay Pacific and took statements. CSTCB met representatives of Cathay Pacific again on 29 October 2018 at Cathay City of the Hong Kong International Airport to better understand the incident. As of 8 November 2018, Cathay Pacific has provided HKPF with part of the data from the affected computer systems for investigation and digital forensic examination. HKPF will continue to maintain close liaison with Cathay Pacific to obtain more relevant information, and gather intelligence from different channels for following up with the investigation.

8. In general cases involving theft of personal data, victims' personal data could be stolen through phishing websites, phishing emails, fraudulent calls, malware infections or hacker intrusions, etc. HKPF will continue to closely monitor all reports involving suspected theft of personal data and investigate if any of such reported cases are related to this leakage of passengers' personal data.

Cyber Security

9. The Office of the Government Chief Information Officer ("OGCIO") has been adopting a multi-pronged strategy on cyber security matters. This includes establishing the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") to disseminate information on cyber security incidents and security advice, protecting government information systems, nurturing professionals in cyber security, as well as strengthening public education and raising the awareness of public and private organisations through various media and

activities.

10. On prevention of cyber security incidents, public and private organisations should take effective security measures to protect the personal data of their clients, prevent and detect unauthorised access and prevent data leakage, and provide information security training for their employees with sharing on relevant case. In order to provide appropriate advice on cyber threats and security incidents in a more effective manner, the OGCIO launched the Cyber Security Information Sharing and Collaborative Platform ("the Platform") in September 2018 to facilitate the exchange of views among cyber security experts, covering analysis of cyber threats and impact of security incidents, as well as sharing of follow-up strategies, etc. The HKCERT also disseminates security advice to the general public through the Platform. Since its establishment over a month ago, almost 100 public and private organisations have already participated in the Platform. We will continue to invite more organisations from different sectors to participate, with a view to sharing cyber security information more effectively and enhancing the defence capability of different sectors against cyber attacks.

11. In respect of this incident, the HKCERT has immediately issued relevant security advice to public and private organisations and the general public. The OGCIO and the HKCERT will continue to closely monitor development of the incident and issue updated information and advice as appropriate.

Way Forward

12. The SAR Government is highly concerned about this incident. The PCPD will complete the compliance investigation and make a report as soon as possible to decide on the next steps. The Police will spare no effort in investigating the incident and pay special attention to cases that may be related to the leakage of passengers' data by Cathay Pacific and where actual losses are involved.

13. There are views in the society that this incident reflects that there is room for amendment and improvement to the PDPO. The SAR Government, in collaboration with the PCPD, has started a review on the relevant stipulations and penalties under the PDPO, and will seriously

consider how to enhance the regulation of data protection and notification arrangements, etc.

Constitutional and Mainland Affairs Bureau
Security Bureau
Innovation and Technology Bureau
November 2018