CATHAY PACIFIC

Response to questions in letter by Dr. Hon. Elizabeth Quat dated 13 November 2018 by Cathay Pacific Airways Limited

The Legislative Council ("**LegCo**") has requested Cathay Pacific Airways Limited ("**Cathay**") to provide a written response to questions prepared by Dr. Hon. Elizabeth Quat. Our written response to those questions is set out below.

As you will appreciate, the security of our IT systems and of our passengers' personal data is of utmost importance to Cathay. As a result, we are unable to provide detailed answers to many of the questions below as to do so would involve divulging sensitive information relating to the security of our IT systems that may put our IT systems and passenger personal data at risk. We thank you in advance for your understanding on this matter and, by way of assurance, we would like to take the opportunity to emphasise that Cathay is fully co-operating with the Hong Kong Privacy Commissioner for Personal Data (HK PCPD) and the Hong Kong Police in their investigation.

1) **Would Cathay Pacific submit a remedial and investigation report to announce the details of the incident and the root cause of the data breach?**

   As part of our full co-operation with the HK PCPD, we have provided detailed responses to the HK PCPD in relation to the data breach, including details of the incident and what we are able to ascertain with respect to the root cause. As we have mentioned above, we are unfortunately unable to share this information in a public forum as it may put our IT security at risk.

2) **Was there a gap analysis done on data storage/retention to understand the current compliance situation and the degree of difference based on different regulations (such as; PCI DSS, EU GDPR, HK Personal Data Privacy Ordinance)?**

   Cathay conducts regular reviews of its policies and procedures to ensure compliance with laws and industry standards relating to data protection. Such reviews have included compliance with the recently introduced EU GDPR, compliance with PCI DSS and, in the past, has included reviews based on changes to the Hong Kong Personal Data Privacy Ordinance.

3) **Would Cathay Pacific submit a current Information Security Risk Assessment Status and Security impact Analysis, including a response to similar incidents in the future?**

   For IT security and data breach incidents, Cathay has an established procedure for dealing with security incidents and data breach events. Following this data breach event and consistent with the assurances Cathay provided to the joint panel session of the Legislative Council on 14 November 2018, we will be reviewing our procedures to ensure we capture the many lessons we have learnt.

4) **How does Cathay conduct its remediation plans and Internal Information Security OLA to handle all potential scenarios?**

   Cathay manages its remediation activities as a programme of work and assigns an overall Programme Manager supported by Project Managers. The Programme Manager

and Project Managers are responsible for the implementation, tracking, monitoring and reporting on the progress of such programme of work.

To supplement the above, Cathay has implemented many remediation activities in response to the data breach. Some of these steps were short term to protect our perimeter and keep the attackers out. Some were longer term and more strategic. We blocked IPs, shut down certain servers, made changes to our protections such as firewalls and set up alerting of certain activity. We launched an advanced threat detection system across the environment. As the investigation progressed, we began implementing more strategic actions such as extending network segmentation and further security improvements. Strategic and long term remediation efforts have also been developed and will be implemented. It should be noted that we did have a robust security program and security defences in place. However, this was a very sophisticated attack and used malware not seen or know before.

5) **Was the system virus identified using a virus identity process and its source?**

As part of our investigation, a variety of malware and utilities used by the attackers were discovered. Some of the signatures of these malware or tools were not previously known, and therefore were not detected by Cathay's up to date anti-virus system. We regret that we are unable to provide the list of actual malware or utilities due to the sensitive nature of this information.

6) **Whether this involves failure of security monitoring systems, improper settings, or failure to mask all sensitive data systems, resulting in a delay in discovery of the virus?**

As part of our full co-operation with the HK PCPD, we have provided detailed responses to the HK PCPD in relation to our security systems. As we have mentioned above, we are unfortunately unable to share this information in a public forum as it may put our IT security at risk. However, we would like to reiterate that Cathay recognizes the critical importance of IT security. Over the past three years, we have spent over HK$1 billion on IT infrastructure and security. Cathay is cognizant that changes in the cybersecurity threat landscape continue to evolve at pace as the sophistication of attackers increase. Our plans, which includes growing our team of IT security specialists, will necessarily evolve in response to this challenging environment.

7) **Which systems did the data breach involve? If it is the inflight sales system, does it involve a 3rd party service provider?**

The incident involved some of our IT systems containing certain passenger data. No employee, flight safety or operations systems were affected and we can confirm in particular that the Inflight Sales system was not affected by this incident.

Cathay Pacific Airways Limited
November 2018