國泰航空有限公司

二零一八年十一月十四日(星期三)

政制事務委員會、資訊科技及廣播事務委員會、及保安事務委員會聯席會議

香港特別行政區立法會（“立法會”）要求國泰航空有限公司（“國泰”）出席在二零一八年十一月十四日(星期三)舉行的政制事務委員會、資訊科技及廣播事務委員會及保安事務委員會的聯席會議。立法會並要求國泰在二零一八年十一月十二日正午前向聯席會議提交一份書面文件。書面文件的內容如下：

國泰航空公司於二零一八年十月二十四日向香港私隱專員公署及香港證券交易所通告本公司有部分資訊系統遭未獲授權者入侵及部份客戶資料被取覽，我們同時亦就此事向香港警務處報案。隨後本公司亦馬上向其他有關監管機構通告這事，亦同時通知受影響的香港及世界各地乘客。

在詳細闡述事件的經過及交代已經採取的行動之前，國泰希望就是次事件向公眾表達深切的遺憾，及向受影響的乘客誠懇致歉。國泰重視與香港市民的關係，並致力自我改善，希望繼續獲得乘客的信心和信任。

在調查是次事件的過程中，我們首要考慮的重點是為受影響顧客提供準確及完整的整套相關資訊，並為我們受影響的乘客提供協助。國泰深明及尊重所有個人資料都需要受到保護，我們亦了解個人資料對每位客人都十分重要。國泰亦會嚴肅處理乘客因此次事件而產生的憂慮。在調查中的每一刻，我們都希望能够更盡早提供有關此次事件的資訊，但是由於調查工作艱巨複雜，較預期需時，故未能早日完成，就此鄭重向公眾致歉。

事件發生的情況說明

精密的網絡罪犯入侵國泰的系統使國泰及受影響的乘客都成為受害者。在發現可疑活動後，國泰即時聘請一家有國際領導地位的專家協助展開全面調查，以確定事件發生的情況及受影響資料的範疇。在調查的最初期，國泰已確認其航班運作及安全系統並沒有受到影響，飛行安全亦從未受到影響。國泰就此次事件的調查是專注於以下三個目標: (i) 調查、控制及補救; (ii) 確認那些資料曾被取覽及是否可以被黑客閱讀; 以及(iii) 確定每一位受影響乘客的個人資料類別及通知。調查結果達到這三個調查目標後，我們便馬上通知受影響的乘客及有關當局。

受影響的乘客及被取覽的資料

這次受到影響的乘客包括馬可孛羅會及亞洲萬里通會員，亦包括曾經乘坐國泰或國泰港龍航班的非會員乘客。根據我們的調查，全球大約有九百四十萬乘客受到是次事件的影響。

受到取覽的個人資料包括乘客姓名、國籍、出生日期、電話號碼、電郵地址、通信地址、旅行證件/護照號碼、身份証號碼、飛行常客計劃的會員號碼、顧客服務備註及過往的飛行記錄資料。每位受影響的乘客被不當取覽的資料都有所不同。據我們的分析顯示，大部份受影響的乘客他們被取覽的資料僅限於乘客姓名及電話號碼，或乘客姓名及電郵地址。

我們的調查亦顯示，我們處理付款資料的系統是具有適當的遮蓋功能，信用卡資料是受到保護的。是次事件中，並沒有一套完整的信用卡資料曾被取覽。但是有一小部分的信用卡號碼因為被錯誤輸入於並非儲存信用卡資料的欄位曾被取覽，這類信用卡絕大部分是已過期的。

在調查中我們確認並沒有任何一位乘客及常客的資料被整套取覽，亦沒有任何乘客密碼外洩。

在調查的過程中，國泰聘請了一家網絡安全專家機構搜尋暗網及其他網站。根據至今的搜尋，我們沒有證據顯示任何被竊取的資料曾在這些網站上出現。我們亦會繼續進行這類搜尋。

給予乘客的協助

國泰深明全面及準確地了解每位受影響乘客被取覽的個人資料範圍及具體細節至為重要。 這樣才能確保在通知他們的時候，我們所提供的資料是整套、完備及具意義的。

國泰就事件在通知全球乘客上亦制定了一套全面的全球通知計劃，我們透過電郵及郵寄發送個人通知信件給每一位受影響的乘客，並在信件中清楚列明每位乘客所被取覽的資料類別。而就無法個別通知的乘客，我們亦於專屬網站 infosecurity.cathaypacific.com 上發佈了一份概括的通知。

除了個人化的通知，國泰亦設立了不同客戶服務渠道協助受是次事件影響的乘客，包括建立免費專屬顧客查詢熱線及專屬電郵地址 (infosecurity@cathaypacific.com)，讓乘客可查詢有關事件的的事宜。

以下的統計數據列出受影響乘客使用上述客戶服務渠道的情況：

客戶服務渠道	截至二零一八年十一月十二日凌晨
網站	181,700 次網頁瀏覽
通過顧客查詢熱線的查詢	收到 5,031 個電話查詢
通過網站的查詢	收到 19,005 則查詢
infosecurity@cathaypacific.com 收到的電郵	收到 5,622 封電郵

國泰亦繼續向受影響乘客提供一個免費的身份監察服務 - IdentityWorks。此項服務由一家名為 Experian 的公司在不同地區(包括香港)提供。截至二零一八年十一月十二日凌晨，共有 50,271 位乘客登記使用該服務。

Experian 與許多世界各地行業領先公司、金融機構及政府機關都有合作。而我們的研究亦顯示他們在網絡(包括暗網)上搜索被未獲授權使用的個人資料方面的能力對受影響的乘客尤其寶貴。乘客可自由選擇是否使用該服務，而每位乘客在這項服務上可選擇他們希望受監察的個人資料類別。Experian 於二零一五年曾發生網絡安全事件，但 Experian 的個人信貸資料庫並沒有被取覽。該公司為持續努力改善安全，已實施全球網絡安全計劃, 透過實施識別、保護、及偵測規格，進一步增強其安全性並提高應對網絡安全威脅的標準。Experian 持續達到全球保障資料及私隱的準測。

國泰資訊技術安全

國泰了解資訊技術安全至關重要。過去三年，我們投放了超過十億港元於資訊基建及資訊網絡安全上。國泰的資訊技術安全的任務是由一隊專家團隊負責，該團隊並沒有受到二零一七年的架構重組影響。他們負責監管及保障資訊技術安全的工作，並有行業領先的專家輔助及提供專業知識 。 我們深明隨著黑客手段愈趨精密和複雜，我們應對網絡安全威脅的反應亦需因時制宜，資訊技術保安的規劃上亦要不斷改良演變，包括強化壯大我們的資訊技術安全團隊以應付急速變化環境所帶來的挑戰。

為何調查時間這麼冗長？

我們對事件的調查及應對是分為三個階段 ，這三個階段是順序進行的，執行時間上亦時有重疊。這三個階段是 - (i) 調查、控制及補救; (ii) 確認那些資料曾被取覽及是否可以被黑客閱讀; 以及(iii) 確定每一位受影響乘客的個人資料類別及通知。

第一階段於二零一八年三月展開。當時國泰首次在系統中發現可疑活動跡象，我們馬上採取行動了解事件並堵截該等活動，並聘請了一家在行業上有領導地位的國際知名全球網路安全公司協助，調查事件情況及阻止事件繼續深化。在這調查階段，我們的系統仍然不斷地受到更多攻擊，其中三月、四月及五月尤為強烈。持續不斷的攻擊驅使我們把內部及外部的資訊技術安全資源集中放在控制及防範上。即使我們往後被成功攻擊的次數有所下降，但我們仍顧慮到系統會有可能受到新的攻擊，不敢鬆懈。

此後，持續的攻擊的範疇亦不斷擴大，使到我們在了解可能被取覽的資料範圍上，添加了不少挑戰，亦令到在第二階段的工作更冗長及複雜。

在第二階段，我們面對的兩大問題為：那些乘客資料被取覽或洩漏；以及，由於受影響的資料庫只是被局部取覽，該等資料是否可在國泰的資訊系統外被重建為可閱讀的格式，從而被黑客使用。要在這些問題上得出答案實在是十分困難及耗時，最終我們只可以在八月中旬才能找到答案。

在第三階段期間，我們工作的重點轉移至確認每一位受影響乘客被取覽資料的類別。我們希望給予每一位受影響乘客一個單一、準確及具意義的通知，而不是提供一個流於空泛且不具體的告示。直到十月二十四日，國泰才能完成確認每位受影響乘客所被取覽的個人資料。與此同時，國泰亦為在回應乘客的查詢上作出了有效的安排 (詳見以上「給予我們乘客的協助」) 。二零一八年十月二十四日，我們開始了向有關部門通佈的工作，我們亦在二零一八年十月二十五日開始通知受影響的乘客。

總括而言，國泰是次受到的攻擊既精密而且先進，受到影響的範疇涉及數個複雜的系統，調查涉及大量高度技術性的工作，在分析上耗時。而將被竊取的資料在進行確認、處理、及將該等資料連繫至個別乘客上的過程複雜，因此由首次發現事件到向公眾公佈事件之間的時間上因而延長。

.....

最後，國泰重申我們非常重視我們在保護乘客個人資料上的責任，亦從此次事件中吸取了許多教訓。我們藉此再次就是次事件及因其而引起的任何憂慮向我們的乘客深表歉意。

國泰航空有限公司
二零一八年十一月