調查報告

根據香港法例第 486 章《個人資料(私隱)條例》
第 48(2) 條發表

快圖美（遠東）有限公司

數據庫遭勒索軟件攻擊

報告編號：R22 - 18947

發表日期：2022 年 11 月 14 日

PCPD.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

調查報告：快圖美（遠東）有限公司
數據庫遭勒索軟件攻擊

香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）第48(2)條訂明，「[個人資料私隱]*專員在完成一項調查後，如認為如此行事是符合公眾利益的，可－*

(a) *發表列明以下事項的報告－*

(i) *該項調查的結果；*

(ii) *由該項調查引致的、專員認為是適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守本條例條文（尤其是各保障資料原則）的任何建議；及*

(iii) *由該項調查引致的、專員認為適合作出的任何其他評論；及*

(b) *以他認為合適的方式發表該報告。*」

現根據《私隱條例》第 48(2)條履行所賦予的權力，發表本調查報告。

鍾麗玲
個人資料私隱專員
2022 年 11 月 14 日

目錄

調查報告

根據《個人資料（私隱）條例》第 48(2) 條發表

快圖美（遠東）有限公司
數據庫遭勒索軟件攻擊

摘要

背景

1. 2021 年 11 月 1 日，快圖美（遠東）有限公司（快圖美）向個人資料私隱專員公署（私隱專員公署）作出資料外洩事故通報（該資料外洩事故通報），表示其網上商店的數據庫（該數據庫）遭勒索軟件攻擊及惡意加密，一名黑客要求快圖美支付贖金，為已被加密的檔案解鎖（該事件）。

2. 在接獲該資料外洩事故通報後，私隱專員公署隨即對快圖美展開循規審查，以取得更多有關該事件的資料。在收到快圖美所提供的進一步資料後，個人資料私隱專員（專員）相信快圖美在該事件中的作為或行為可能涉及違反香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）的規定，遂於 2021 年 12 月根據《私隱條例》第 38(b)條就該事件對快圖美展開調查。

調查

3. 專員在進行調查過程中，審視及考慮了快圖美提供與該事件有關的資料，包括就快圖美對該數據庫所採取的保安措施進行了七次的查

訊，並審視了快圖美委任的兩間獨立資訊科技顧問公司提供的調查報告。專員亦考慮了快圖美在該事件發生後的跟進及補救工作。

4. 快圖美指該事件合共影響 544,862 名會員及 73,957 名曾在 2020 年 11 月 16 日至 2021 年 10 月 26 日期間於其網上商店訂購產品及／或服務的訪客。

該事件及相關的保安漏洞

5. 快圖美於 2018 年 3 月向一間服務供應商（該服務供應商）購買一台防火牆（該防火牆），並於 4 月安裝及啟用，以加強網絡安全。快圖美隨後於 2019 年 3 月啟用保密插口層虛擬私有網絡（Secure Sockets Layer Virtual Private Network, SSL VPN），以供資訊科技部門有需要時遙距登入其系統。

6. 2019 年 5 月，該防火牆生產商在其網站發出保安建議（該建議），表示留意到有黑客披露其作業系統的漏洞（相關漏洞）。攻擊者可以通過相關漏洞繞過保安限制直接取得 SSL VPN 帳戶名稱及密碼，並可於目標系統執行任何程式。根據該建議，該防火牆生產商呼籲用家立即停用 SSL VPN 功能，直至更新作業系統及重設所有帳戶密碼，同時建議啟用多重認證。

7. 政府電腦保安事故協調中心於 2019 年 8 月就相關漏洞發出高危保安警報，建議機構應立即為受影響的系統安裝修補程式。假如無法立即修補，應先停用 SSL VPN 直到已為受影響的系統進行修補。香港電腦保安事故協調中心隨後於 2020 年 12 月亦呼籲相關的本地網絡供應商及機構就相關漏洞盡快採取適當的補救措施。

8. 2021 年 10 月 26 日早上，快圖美的資訊科技部門職員發現網上商店及該數據庫無法正常存取，其後發現除了該數據庫外，部份位於辦公室的伺服器和電腦同樣遭勒索軟件加密。

資訊科技顧問公司的調查結果

9. 快圖美於該事件後委任了兩間資訊科技顧問公司檢視其資訊系統安全。綜合兩間資訊科技顧問公司的報告，資訊科技顧問公司認為(i)快圖美未有為受影響的系統安裝修補程式，導致黑客利用相關漏洞首先取得 SSL VPN 帳戶名稱及密碼，並在入侵系統取得系統管理員權限後執行勒索軟件，最終成功加密該數據庫，及(ii) 快圖美未有為 SSL VPN 啟用多重認證。

快圖美對該事件的解釋

10. 快圖美向私隱專員公署承認早於 2019 年 9 月已經知悉相關漏洞，並指稱曾與該服務供應商透過電話討論有關事宜。

11. 快圖美解釋，由於已經設置一系列的資訊保安措施包括防毒軟件、防勒索軟件程式以及防火牆，經諮詢該服務供應商及內部評估後，認為毋須即時安裝修補程式修補相關漏洞。

12. 快圖美亦承認由於當時 SSL VPN 僅供資訊科技部門在有需要時遙距登入系統，故未有就相關漏洞進行詳細評估。即使後來因應本地 2019 冠狀病毒病疫情推行在家工作安排，讓員工在家工作期間可使用 SSL VPN 遙距存取其系統，快圖美亦未有重新評估相關漏洞，致使相關漏洞直至該事件發生時仍未修補。

調查結果及違例事項

快圖美屬該事件的資料使用者

13. 快圖美在香港營運，並收集及管理該數據庫內的個人資料。因此，快圖美屬《私隱條例》第 2(1)條釋義下的資料使用者，須遵從《私隱條例》的規定行事，包括《私隱條例》附表一所列明的六項保障資料原則。

公署對該事件肇因的理解

14. 專員在審視兩間資訊科技顧問公司的調查報告、快圖美對該事件的解釋，以及私隱專員公署在調查中獲得的所有資料後，同意調查報告的內容，認為事件源於快圖美未有為受影響的系統安裝修補程式，導致黑客利用相關漏洞首先取得 SSL VPN 帳戶名稱及密碼，在入侵系統取得系統管理員權限並執行勒索軟件後，成功加密該數據庫；同時，快圖美亦未有為 SSL VPN 啟用多重認證，以加強相關系統保安。

快圖美違反保障資料第 4(1)原則

15. 根據保障資料第 4(1)原則，資料使用者須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。

16. 經考慮與該事件有關的事實及在調查過程中所獲得的證據，專員認為快圖美在風險意識及個人資料保安措施方面存在以下嚴重不足，導致該數據庫在可避免的情況下被黑客利用保安漏洞入侵系統並存取個人資料：—

(1) 錯誤評估保安漏洞的風險：雖然快圖美早於 2019 年 9 月已經知悉該防火牆存在保安漏洞，但快圖美表示經內部評估後認為當時的資訊保安措施已經足夠應對相關漏洞帶來的威脅，因此未有採取任何行動。專員認為快圖美對已知風險抱有過份樂觀甚或僥倖心理，明顯地錯誤評估相關漏洞對其載有個人資料的資訊系統造成的風險，以及一旦遭黑客入侵可能引致的後果，令人遺憾。假如快圖美認真注視該防火牆生產商、政府電腦保安事故協調中心及香港電腦保安事故協調中心再三的提醒，採取謹慎的態度重新檢視以往的決定，應能發現相關漏洞對系統構成嚴重的潛在風險，並可盡早修補相關漏洞，從而避免該事件發生。

(2) 資訊系統管理有欠妥善：快圖美未有制訂嚴謹的修補程式管理程序，以致未有及時修補該防火牆的保安漏洞，讓黑客成功透過相關漏洞入侵系統，並加密該數據庫。此外，快圖美沒有強制執行密碼政策，導致系統內超過 30 個帳戶的密碼強度不足，令有關帳戶容易被黑客攻擊入侵；而快圖美亦在其他資訊保安方面有所缺失。專員認為以上都反映了快圖美的個人資料保安管理有欠妥善，欠缺嚴謹措施規範員工行為及適時檢視系統設定，令載有個人資料的資訊系統的保安無法有效應對風險和威脅。

(3) 拖延啟用多重認證功能：早於 2019 年 5 月，該防火牆生產商曾呼籲用家立即停用 SSL VPN，以防攻擊者透過相關漏洞繞過保安限制直接取得 SSL VPN 帳戶名稱及密碼，直至更新作業系統及重設所有帳戶密碼，同時建議啟用多重認證功能。然而，快圖美直至該事件發生時仍未有為 SSL VPN 實施多重認證功能，防止黑客利用外洩的密碼攻擊系統。

17. 在考慮本個案所有證據後，專員認為快圖美：—

(1) **錯誤評估保安漏洞的風險，沒有為系統保安採取任何行動，讓數據庫內的個人資料曝露於黑客攻擊的風險之中；**
(2) **沒有妥善管理載有個人資料的資訊系統，包括未有制訂嚴謹的修補程式管理程序，導致沒有及時修補保安漏洞，讓黑客成功透過相關漏洞入侵系統，並加密該數據庫；及**
(3) **沒有跟從防火牆生產商的建議，在機構內廣泛推行在家工作安排前為保密插口層虛擬私有網絡（SSL VPN）實施多重認證功能，防止黑客利用已獲取的密碼攻擊系統。**

18. **在本個案中，專員發現快圖美在個人資料風險意識及個人資料保安措施方面存在嚴重不足，導致公司的數據庫遭勒索軟件攻擊。專員認為快圖美對已知風險抱有過份樂觀甚或僥倖心理，明顯地錯誤評估相關漏洞對其載有個人資料的資訊系統造成的風險，以及一旦遭黑客入侵可能引致的後果，令人遺憾。專員認為快圖美沒有採取所有切實可行的步驟以確保涉事的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，因而違反了保障資料第 4(1)原則有關個人資料保安的規定。**

19. 雖然快圖美在該事件中有需要改善之處，但專員樂見快圖美及時作出資料外洩通報，配合私隱專員公署的調查，並致力從該事件中汲取教訓。該事件發生後，快圖美通過採取多種機構性和技術性的改善措施，已經修補保安漏洞，提升整體系統保安以保障個人資料私隱。

執法行動

20. 專員已依據《私隱條例》第 50(1)條所賦予的權力，向快圖美送達執行通知，指示快圖美採取以下步驟以糾正違規情況，以及防止違規事件再發生：—

(1) 徹底檢視快圖美載有個人資料的系統保安，確保該些系統沒有已知的惡意軟件及保安漏洞；

(2) 聘請獨立的資料保安專家對快圖美的系統保安（包括快圖美網上商店的數據庫）進行定期檢視及審核；

(3) 修訂系統保安政策，明確訂定快圖美對其網絡設備（包括防火牆及／或伺服器）定期進行漏洞掃描；

(4) 修訂系統保安政策，明確訂定修補程式的管理政策及要求，並採取措施確保有關員工及提供系統保養服務的服務提供者依循相關政策及要求；及

(5) 由執行通知的日期起計三個月內向專員提供文件，證明已完成上述第 (1)至 (4)項指示。

建議

21. 專員希望通過本報告提醒處理顧客個人資料的機構須特別注意以下範疇：—

(1) **提高警覺，防止黑客攻擊**：面對着不同的保安漏洞，機構應時刻提高警覺，定時進行風險評估，以檢視黑客攻擊對系統可能帶來的影響，並加以維護載有個人資料的系統例如電子郵件伺服器、顧客資料庫等。

(2) **設立個人資料私隱管理系統**：機構應備有健全的個人資料私隱管理系統，循規使用及保留個人資料，有效管理由收集至銷毀個人資料的整個生命週期，令機構可迅速應對任何資料外洩事故，以及贏得客戶及其他持份者的信任。

(3)**委任專責人員作為保障資料主任**：機構應明確制訂保障資料主任的角色及職責，包括監察遵從《私隱條例》的情況並向高級管理層匯報，以及把員工提出的保障資料事宜和涉及客戶個人資料外洩事故的經驗及教訓納入機構的培訓材料中。

(4)**提升資訊系統管理**：機構應制訂有效的修補程式管理程序，盡早修補保安漏洞，並因應系統載有的個人資料數量及敏感度採取相應的技術保安措施，例如連接虛擬私有網絡時使用多重身份認證，為系統及帳戶帶來額外安全保障。

(5)**妥善記錄內部通訊**：機構當面對網絡設備生產商的建議與資訊系統服務提供者的意見有所不同時，盡職和審慎的做法是以書面諮詢有關生產商，以尋求進一步意見或釐清合適的跟進辦法，並將諮詢期間所有往來文件妥為保存，以便日後檢討時參考。

其他評論

22. 專員理解很多機構都會推出會員計劃，部份會員計劃更容許將消費金額累積，以便日後交易時換算為現金折扣，令會員帳戶具有一定價值。然而，消費者未必會定期管理名下的帳戶，這些長期閒置的非活躍帳戶除了會增加機構保障個人資料的成本，亦會增加資料外洩的風險。而且資料保留的時間越長，資料因過時而變得不準確的機會亦越大。

23. 根據快圖美向私隱專員公署提供的資料，在受影響的 544,862 名會員中，約 65%的會員（約 35 萬名會員）由創建帳戶至該事件發生前不曾有任何登入活動。雖然快圖美指出會員可主動要求刪除其會籍及個人資料，但**專員認為機構單憑未接獲刪除帳戶要求，便長期保留非活躍用戶的個人資料，未必符合顧客對個人資料私隱的合理期望。**快圖美其後向專員表示，將刪除過去三年沒有進行消費的非活躍用戶的個人資料。

24. **此外，專員留意到快圖美的網上商店網站已在 2020 年 11 月 16 日更新後停止收集會員的出生日子。專員認為機構須小心考慮收集個人資料的目的，並應在不損害使用資料的目的的情況下，謹慎制訂合適的個人資料保留期限，而非只為運作上的便利而保留個人資料。專員藉此提醒快圖美重新審視其個人資料庫，盡快刪除不必要的個人資料（包括審視繼續保存已收集得的會員的出生日子是否必要）。**

25. 隨着資料數碼化趨勢加速、資訊及通訊科技的互聯互通，以及資料本身的價值不斷上升，個人資料保安的風險亦隨之而增加。近年在香港和其他司法管轄區所發生的資料保安事故之上升趨勢亦證明了這一點。不論資料使用者是中小企業還是跨國企業，資料保安事故都可在聲譽及財務兩方面為其帶來嚴重後果。

26. 專員藉此指出，穩健的資料保安系統是構成良好資料管治的一個重要元素。專員理解資料使用者所需採取的保護個人資料措施會因情況而異，資料使用者除了應諮詢專業資料保安專家和法律顧問，以確保遵從《私隱條例》的相關規定，亦可參考私隱專員公署最近出版的《資訊及通訊科技的保安措施指引》[1]，了解與資訊及通訊科技相關的資料保安措施建議及加強資料保安系統的良好行事方式。

[1] www.pcpd.org.hk//tc_chi/resources_centre/publications/files/guidance_datasecurity_c.pdf

I. 背景

1. 2021 年 10 月 29 日，快圖美（遠東）有限公司（快圖美）的母公司中港照相器材集團有限公司發布一則公告[2]，表示快圖美系統內的沖印及影像解決方案數據庫於同年 10 月 26 日遭未經授權取覽，受影響的數據庫載有快圖美顧客的個人資料。

2. 2021 年 11 月 1 日，快圖美向個人資料私隱專員公署（私隱專員公署）作出資料外洩事故通報（該資料外洩事故通報），表示其網上商店的數據庫（即上述的沖印及影像解決方案數據庫）（該數據庫）遭勒索軟件攻擊及惡意加密，一名黑客要求快圖美支付贖金，為已被加密的檔案解鎖（該事件）。

3. 在接獲該資料外洩事故通報後，私隱專員公署隨即對快圖美展開循規審查，以取得更多有關該事件的資料。在收到快圖美所提供的進一步資料後，個人資料私隱專員（專員）相信快圖美在該事件中的作為或行為可能涉及違反香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）的規定，遂於 2021 年 12 月根據《私隱條例》第 38(b)條就該事件對快圖美展開調查。

[2] www1.hkexnews.hk/listedco/listconews/sehk/2021/1029/2021102900964_c.pdf

II. 法定權力及相關法律規定

<u>法定權力</u>

4. 《私隱條例》第 38 條授權專員在下述情況下可進行調查：

(i) 當專員收到由受影響的資料當事人或其代表作出的投訴，除《私隱條例》第 39 條另有規定外，專員須根據第 38(a)條就有關的資料使用者進行調查，以確定在有關的投訴中指明的作為或行為是否屬違反《私隱條例》下的規定；或

(ii) 當專員有合理理由相信有資料使用者已經或正在作出或從事關乎個人資料的作為或行為，而有關作為或行為可能屬違反《私隱條例》下的規定，專員可根據第 38(b)條就有關的資料使用者進行調查，以確定有關行為或作為是否屬違反《私隱條例》下的規定。

5. 專員在展開調查後，可根據《私隱條例》第 43(1)(a)條，為調查的目的而自她認為合適的人處獲提供她認為合適的資訊、文件或物品，以及作出她認為合適的查訊。

6. 《私隱條例》第 48(2)(a)條訂明，專員在完成一項調查後，如認為如此行事是符合公眾利益的，可發表報告列明該項調查的結果及由該項調查引致的、專員認為適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守《私隱條例》的任何建議及其他評論。

7. 根據《私隱條例》第 50(1)條，如專員在完成一項調查後，認為有關的資料使用者正在或已經違反《私隱條例》下的規定，專員可向該資料使用者送達書面通知，指示該資料使用者糾正該項違反，以及（如適當的話）防止該項違反再發生。

8. 根據《私隱條例》第 50A 條，資料使用者違反執行通知，即屬犯罪，一經首次定罪，最高可被判處第五級罰款（即港幣 50,000 元）及監禁兩年。

相關法律規定

資料使用者

9. 《私隱條例》，包括附表一的保障資料原則，旨在規管資料使用者的行為及作為。根據《私隱條例》第 2(1)條，就個人資料而言，資料使用者指「*獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或使用的人*」。

個人資料

10. 《私隱條例》涵蓋的資料使用者在處理「個人資料」時須遵守保障資料原則，而根據《私隱條例》第 2(1)條，「個人資料」是「*指符合以下說明的任何資料—*

(a) 直接或間接與一名在世的個人有關的；
(b) 從該資料直接或間接地確定有關的個人的身分是切實可行的；及
(c) 該資料的存在形式令予以查閱及處理均是切實可行的。」

資料保安

11. 保障資料第 4(1)原則就個人資料的保安訂明以下原則：—

「 *須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料（包括採用不能切實可行地予以查閱或處理的形式的資*

料）受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，尤其須考慮—

(a) 該資料的種類及如該等事情發生便能做成的損害；

(b) 儲存該資料的地點；

(c) 儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；

(d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及

(e) 為確保在保安良好的情況下傳送該資料而採取的措施。」

12. 根據《私隱條例》第 2(1)條，「切實可行」指「*合理地切實可行*」。

13. 保障資料第 4(1)(a)原則所述的「損害」測試，需考慮資料使用者就其持有的個人資料而採取的保安措施是否與資料的敏感程度及資料被未獲准許或意外查閱所導致的損害相稱。

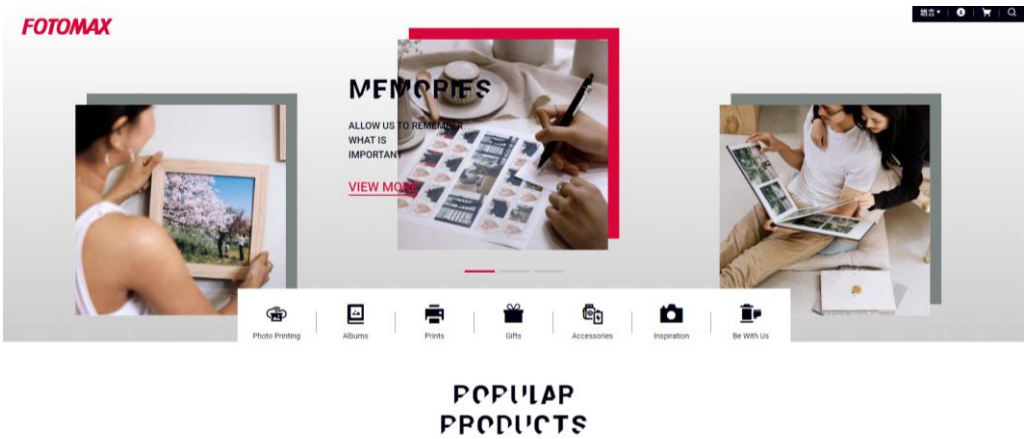
III. 調查所取得的資料及證據

14. 專員在進行調查過程中，審視及考慮了快圖美提供與該事件有關的資料，包括就快圖美對該數據庫所採取的保安措施進行了七次的查訊，並審視了快圖美委任的兩間獨立資訊科技顧問公司提供的調查報告。專員亦考慮了快圖美在該事件發生後的跟進及補救工作。

公司背景及會員計劃

15. 快圖美於 1982 年成立，由 2001 年起成為中港照相器材集團有限公司的全資附屬公司，提供菲林處理、相片沖印、拍攝證件相以及周邊商品零售服務，在香港擁有 55 間實體店及網上商店。

16. 快圖美自 2000 年 10 月起設有會員計劃，顧客只需填妥網上表格[3]，提交個人資料後便可成為會員。會員計劃收集的個人資料包括姓名、性別、出生月份及日子[4]、電郵地址及電話號碼。除非會員主動聯絡快圖美要求刪除會籍，否則其會籍將被視作永久有效，而快圖美會永久保留其會籍資料。



快圖美網站截圖（2022 年 8 月）

[3] www.fotomax.com/zh-hk/account/register
[4] 出生日子已於 2020 年 11 月 16 日網上商店網站更新後停止收集。

該事件及相關的保安漏洞

17. 2021 年 10 月 26 日早上，快圖美的資訊科技部門職員發現網上商店及該數據庫無法正常存取，其後發現除了該數據庫外，部份位於辦公室的伺服器和電腦同樣遭勒索軟件加密。

18. 快圖美隨即檢視防火牆的活動日誌，發現一名黑客於 10 月 25 日晚上利用其中一名職員的帳戶，透過保密插口層虛擬私有網絡（Secure Sockets Layer Virtual Private Network, SSL VPN）[5]登入快圖美的系統，然後透過暴力攻擊[6]登入其他電腦及伺服器，包括系統管理員帳戶，並安裝勒索軟件以索取贖金。

快圖美提供涉事的勒索訊息

19. 根據快圖美提供的資料，受該事件影響的伺服器中只有其中一台伺服器載有該數據庫及個人資料。

---

[5] SSL VPN 讓用戶使用互聯網瀏覽器便可以加密通訊連接虛擬私有網絡裝置。（www.infosec.gov.hk/tc/best-practices/business/vpn-security）

[6] 暴力攻擊是指通過試誤法以破解憑證，反覆試驗所有可能的組合，直至猜到正確密碼。（www.infosec.gov.hk/tc/knowledge-centre/bruteforce）

20. 快圖美表示它於 2018 年 3 月向一間服務供應商（該服務供應商）購買一台防火牆（該防火牆），並於 4 月安裝及啟用，以加強網絡安全。快圖美隨後於 2019 年 3 月啟用 SSL VPN，以供資訊科技部門有需要時遙距登入其系統。

21. 2019 年 5 月，該防火牆生產商在其網站發出保安建議（該建議）[7]，表示留意到有黑客披露其作業系統[8]的漏洞[9]。攻擊者可以通過相關漏洞繞過保安限制直接取得 SSL VPN 帳戶名稱及密碼，並可於目標系統執行任何程式。根據該建議，該防火牆生產商呼籲用家立即停用 SSL VPN 功能，直至更新作業系統及重設所有帳戶密碼，同時建議啟用多重認證。

22. 政府電腦保安事故協調中心於 2019 年 8 月就相關漏洞發出高危保安警報，建議機構應立即為受影響的系統安裝修補程式。假如無法立即修補，應先停用 SSL VPN 直到已為受影響的系統進行修補[10]。

23. 2020 年 11 月，一名黑客在網上分享一份列表（該列表），列出超過 49,000 台尚未修補相關漏洞的設備的 IP 地址[11]。該防火牆生產商隨即於同月再度發文提醒用戶盡快安裝修補程式[12]。

24. 香港電腦保安事故協調中心隨後於 2020 年 12 月亦提醒各界該列表中有約 1,000 個 IP 地址來自香港，並呼籲相關的本地網絡供應商及機構就相關漏洞盡快採取適當的補救措施[13]。

---

[7] www.fortiguard.com/psirt/FG-IR-18-384

[8] 受影響的作業系統包括 FortiOS 5.4.6 至 5.4.12、FortiOS 5.6.3 至 5.6.7 及 FortiOS 6.0.0 至 6.0.4。

[9] 根據香港電腦保安事故協調中心的保安公告（www.hkcert.org/tc/security-bulletin/fortinet-fortos-multiple-vulnerabilities），相關漏洞的識別碼為 CVE-2018-13379。

[10] www.govcert.gov.hk/tc/alerts_detail.php?id=414

[11] 即互聯網規約地址

[12] www.fortinet.com/blog/psirt-blogs/update-regarding-cve-2018-13379

[13] www.hkcert.org/tc/blog/patch-fortios-ssl-vpn-vulnerability-cve-2018-13379-immediately

快圖美的資訊保安政策

25. 在調查過程中，快圖美向私隱專員公署提交了以下與保障個人資料相關的政策：—

26. 快圖美在該事件發生前訂有一份「資訊安全政策」（"*Information Security Policy*"）（該資訊安全政策），就其擁有的資料釐定了整體的保安管理框架，包括互聯網及電郵使用政策、檔案存取權限規定及實體保安政策。

27. 快圖美在 2018 年 4 月及 2019 年 10 月分別發出了「密碼政策」（"*Password Policy*"）（該密碼政策）及「自攜裝置政策」（"*BYOD Policy*"），前者訂明了不同類型帳戶的密碼有效期限、密碼最低長度及所需的複雜程度；後者則要求員工在辦公範圍使用自攜裝置前須先向資訊科技部門註冊有關裝置及確認已經安裝有效的防毒軟件。

28. 快圖美表示在該事件發生前已透過內聯網提供以上三份政策給員工閱讀。另外，自 2016 年 11 月 1 日後入職的員工須簽署確認已閱讀及同意遵從該資訊安全政策的規定。

受影響的個人資料

29. 快圖美指該事件合共影響 544,862 名會員及 73,957 名曾在 2020 年 11 月 16 日至 2021 年 10 月 26 日期間於其網上商店訂購產品及／或服務的訪客。

30. 快圖美表示，受影響會員及訪客所涉及的個人資料分別如下：—

受影響的會員	受影響的訪客
(i) 姓名 (ii) 性別 (iii) 出生月份及日子 (iv) 電話號碼 (v) 電郵地址 (vi) 聯絡地址 (vii) 送貨地址	(i) 姓名 (ii) 電話號碼 (iii) 電郵地址 (iv) 送貨地址

31. 快圖美向私隱專員公署提供了受該事件影響的每項個人資料種類的相關數字：—

	受影響的會員	受影響的訪客
姓名	544,862 (100%)	73,957 (100%)
性別	358,012 (65.7%)	
出生月份	330,378 (60.6%)	
出生日子	202,514 (37.2%)	
電話號碼	486,050 (89.2%)	73,414 (99.3%)
電郵地址	544,862 (100%)	73,957 (100%)
聯絡地址	3,293 (0.6%)	
送貨地址	1,030 (0.2%)	1,190 (1.6%)

（括號為該項個人資料數目佔該類資料當事人總數百分比）

32. 至於網上商店交易所需的信用卡資料（包括姓名、信用卡號碼及到期日）則由第三方網上繳費系統直接處理，快圖美表示並無儲存有關資料。

33. 快圖美表示會員註冊時只須提供姓名、電話號碼及電郵地址，其他資料均為選填項目；而一般訪客只須提供姓名、電話號碼及電郵地址作網上購物登記。會員可於註冊後填寫聯絡地址作為預設送貨地址。假如會員及訪客選擇送貨服務而非前往實體店自取，則須另填寫送貨地址。

資訊科技顧問公司的調查結果

34. 快圖美於該事件後委任了兩間資訊科技顧問公司檢視其資訊系統安全，並在調查過程中提交報告予私隱專員公署檢視。綜合兩間資訊科技顧問公司的報告：—

(i) 快圖美未有為受影響的系統安裝修補程式，導致黑客利用相關漏洞首先取得 SSL VPN 帳戶名稱及密碼，並在入侵系統取得系統管理員權限後執行勒索軟件，最終成功加密該數據庫。系統紀錄顯示可疑的登入活動最早可追溯至 2021 年 10 月 1 日，這意味著黑客在該事件發生前已潛伏在快圖美的電腦系統內一段時間；

(ii) 快圖美未有為 SSL VPN 啟用多重認證；

(iii) 系統內超過 30 個帳戶的密碼強度不足，部份密碼僅由數字組成、與帳戶名稱相似或是預設密碼。然而有關報告未有足夠證據證明密碼強度不足是導致黑客成功入侵系統的肇因之一；及

(iv) 資訊保安檢視識辨出一系列的缺失[14]，儘管沒有跡象顯示這些缺失直接引發該事件。

[14] 為保障相關資訊系統安全的敏感資料，有關詳情被略去。

快圖美對該事件的解釋

35. 快圖美向私隱專員公署承認早於 2019 年 9 月已經知悉相關漏洞，並指稱曾與該服務供應商透過電話討論有關事宜。

36. 快圖美解釋，由於已經設置一系列的資訊保安措施包括防毒軟件、防勒索軟件程式以及防火牆，經諮詢該服務供應商及內部評估後，認為毋須即時安裝修補程式修補相關漏洞。然而，由於快圖美與該服務供應商的討論並沒有附帶任何書面紀錄，專員無法得悉有關的討論內容及其他細節。

37. 快圖美亦承認由於當時 SSL VPN 僅供資訊科技部門在有需要時遙距登入系統，故未有就相關漏洞進行詳細評估。即使後來因應本地 2019 冠狀病毒病疫情推行在家工作安排，讓員工在家工作期間可使用 SSL VPN 遙距存取其系統，快圖美亦未有重新評估相關漏洞，致使相關漏洞直至該事件發生時仍未修補。

跟進工作及補救措施

38. 快圖美表示在該事件後，即時停用受影響的系統包括 SSL VPN，並派員檢查其他系統及更新防護軟件。

39. 快圖美隨後亦已更新該防火牆的作業系統以修補相關漏洞，並更改所有系統管理員的帳戶密碼及重新設定所有 SSL VPN 帳戶的密碼以加強密碼強度。

40. 因應資訊科技顧問公司在調查報告中所述的其他建議，快圖美採取了以下補救措施防止同類型事件再發生：—

(i) 為 SSL VPN 增設雙重認證功能；

(ii) 為電腦及伺服器安裝程式偵測可疑的網絡傳輸，提升防範網絡攻擊的能力；

(iii) 定期進行漏洞掃瞄及檢查可供安裝的修補程式，並保留有關評估紀錄；及

(iv) 對其資訊保安系統進行了一系列的提升[15]，加強保障系統安全。

[15] 為保障相關資訊系統安全的敏感資料，有關詳情被略去。

IV. 調查結果及違例事項

41. 根據保障資料第 4(1)原則，資料使用者須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。在本個案中，專員考慮的因素包括：(i) 該事件是否屬資料外洩事故；(ii) 誰是需要為該資料外洩事故負責的資料使用者；及(iii) 涉事的資料使用者是否已按保障資料第 4(1)原則的規定採取所有切實可行的步驟保障其持有的個人資料。以下是專員的調查結果：—

該事件的性質

42. 資料外洩事故一般指資料使用者持有的個人資料懷疑外洩，令此資料有被未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險。資料外洩事故可構成違反《私隱條例》下的保障資料第 4(1)原則。

43. 在調查過程中，快圖美向私隱專員公署表示沒有足夠證據證實該事件導致個人資料外洩。然而，專員認為該名黑客利用相關漏洞存取載有個人資料的該數據庫，表面已經構成未獲准許的查閱及／或處理個人資料的情況。

快圖美屬該事件的資料使用者

44. 快圖美在香港營運，並收集及管理該數據庫內的個人資料。因此，快圖美屬《私隱條例》第 2(1)條釋義下的資料使用者，須遵從《私隱條例》的規定行事，包括《私隱條例》附表一所列明的六項保障資料原則。

公署對該事件肇因的理解

45. 專員在審視兩間資訊科技顧問公司的調查報告、快圖美對該事件的解釋，以及私隱專員公署在調查中獲得的所有資料後，同意調查報告的內容，認為事件源於快圖美未有為受影響的系統安裝修補程式，導致黑客利用相關漏洞首先取得 SSL VPN 帳戶名稱及密碼，在入侵系統取得系統管理員權限並執行勒索軟件後，成功加密該數據庫；同時，快圖美亦未有為 SSL VPN 啟用多重認證，以加強相關系統保安。

資料保安的嚴重不足

46. 保障資料第 4(1)原則訂明，資料使用者須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，尤其須考慮 —

(a) 該資料的種類及如該等事情發生便能做成的損害；
(b) 儲存該資料的地點；
(c) 儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；
(d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及
(e) 為確保在保安良好的情況下傳送該資料而採取的措施。

47. 在此個案中，為了考慮快圖美是否符合保障資料第 4(1)原則的規定，專員會考慮快圖美在關鍵時間（即該事件發生時）對該數據庫所採取的保安措施及快圖美如何處理已知資料保安風險。

48. 經考慮與該事件有關的事實及在調查過程中所獲得的證據，專員認為快圖美在風險意識及個人資料保安措施方面存在嚴重不足，導致該數據庫在可避免的情況下被黑客利用相關漏洞入侵系統並存取個人資料。

(1) *<u>錯誤評估保安漏洞的風險</u>*

49. 雖然快圖美早於 2019 年 9 月已經知悉該防火牆存在相關漏洞，但快圖美表示經內部評估後認為當時的資訊保安措施已經足夠應對相關漏洞帶來的威脅，因此未有採取任何行動。

50. 由於快圖美未能提供任何文件證明曾經與該服務供應商就相關漏洞進行討論，亦未能提供任何相關的內部評估紀錄，專員未能基於客觀證據信納快圖美的上述解釋。從調查所得的證據及資料顯示，快圖美未曾就相關漏洞進行正式或有紀錄的風險評估，而相關漏洞直至該事件發生時仍未修補。

51. 專員認為防火牆屬保護系統的重要屏障，而黑客利用防火牆的相關漏洞取得帳戶名稱及密碼，性質形同密碼外洩，安全風險實在不容忽視。在本個案中，專員認為快圖美對已知風險抱有過份樂觀甚或僥倖心理，明顯地錯誤評估相關漏洞對其載有個人資料的資訊系統造成的風險，以及一旦遭黑客入侵可能引致的後果，令人遺憾。

52. 快圖美由 2019 年 9 月決定不就相關漏洞採取任何行動，直至 2021 年 10 月該事件發生前，該防火牆生產商、政府電腦保安事故協調中心及香港電腦保安事故協調中心曾經再三提醒用戶修補相關漏洞。專員認為假如快圖美認真注視這些提醒，採取謹慎的態度重新檢視以往的決定，應能發現相關漏洞對系統構成嚴重的潛在風險，並可盡早修補相關漏洞，從而避免該事件發生。

(2) *資訊系統管理有欠妥善*

53. 專員認為快圖美未有制訂嚴謹的修補程式管理程序，以致快圖美在知悉該防火牆存有保安漏洞的情況下，未有及時修補相關漏洞，讓黑客成功透過相關漏洞入侵系統，並加密該數據庫。專員認為快圖美明顯未有承擔作為資料使用者的責任，未有採取所有切實可行的步驟保障該數據庫內的個人資料。

54. 此外，專員從快圖美委任的兩間資訊科技顧問公司的調查報告中，注意到在該事件發生時，快圖美在資訊系統保安措施方面存在以下問題：—

(1) 沒有強制執行該密碼政策，導致系統內超過 30 個帳戶的密碼強度不足，令有關帳戶容易被黑客攻擊入侵；及

(2) 其他資訊保安方面的缺失[16]。

55. 雖然沒有跡象顯示這些缺失直接導致該事件發生，但專員認為以上都反映了快圖美的個人資料保安管理有欠妥善，欠缺嚴謹措施規範員工行為及適時檢視系統設定，令載有個人資料的資訊系統的保安無法有效應對風險和威脅。

(3) *拖延啟用多重認證功能*

56. 該防火牆生產商曾在 2019 年 5 月發出的建議提到，攻擊者可以透過相關漏洞繞過保安限制直接取得保密插口層虛擬私有網絡（Secure Sockets Layer Virtual Private Network, SSL VPN）帳戶名稱及密碼，並可於目標系統執行任何程式。該防火牆生產商因此呼籲用家立即停用 SSL VPN，直至更新作業系統及重設所有帳戶密碼，同時建議

[16] 為保障相關資訊系統安全的敏感資料，有關詳情被略去。

啟用多重認證功能。然而，快圖美直至該事件發生時仍未有為 SSL VPN 實施多重認證功能，防止黑客利用外洩的密碼攻擊系統。

57. 因應本地 2019 冠狀病毒病疫情，快圖美曾於 2020 年至 2021 年 2 月期間三度推行在家工作安排，每次為期約四星期，並容許員工使用自攜裝置或公司手提電腦，透過 SSL VPN 連接公司系統。

58. 對於廣泛推行在家工作安排前未有啟用多重認證功能，快圖美解釋由於每次推行在家工作安排為期不長，經評估後認為當時的保安措施已經足夠防範網絡攻擊。

59. 專員認為快圖美對其資料保安措施抱持過份信心，亦對為期共約三個月的在家工作安排採取輕率的態度，未有進行合適而謹慎的風險評估及採取適當的資料保安措施。專員認為根據該防火牆生產商的建議，以及快圖美讓員工在在家工作期間透過 SSL VPN 遙距連接公司系統的情況下，快圖美應合理地啟用多重認證功能以提升保安措施及保障其載有個人資料的系統安全。在該事件中，快圖美容許載有個人資料的資訊系統曝露在已知風險中，是導致該資料庫在可避免的情況下仍遭勒索軟件攻擊的主要原因。

60. 在衡量何謂足夠的資料保安措施時，專員參考了政府資訊科技總監辦公室提供的網絡保安的良好行事方式[17]，當中包括：—

(1) 在網絡設計時加入保安的考慮：所有保安事項，例如管理政策，技術訓練和外判要求應該早在網絡設計階段開始考慮。

(2) 將伺服器設定至較佳的保安狀態：移除不必要的服務和軟件、及時修補系統的漏洞和取消沒被使用的帳戶。

[17] www.infosec.gov.hk/tc/best-practices/business/securing-company-network

(3) 加強應用程式的保安：安裝保安修補程式、強化應用程式的設定或鎖上應用程式運作的環境。

(4) 建立保安管理的程序：例如保安事件紀錄監測程序，改革管理程序或修補程式管理程序。

(5) 保存有關設定和程序的文件紀錄。

(6) 職員培訓：網絡／資訊保安管理員及支援職員以及一般員工要接受培訓以確保他們可以遵從保安最佳作業守則和保安政策。

61. 專員注意到快圖美在該事件發生時未能符合上述指引建議的大部份保安措施的要求，以保障其載有個人資料的數據庫免受黑客攻擊。

結論：違反保障資料第 4(1)原則

62. 專員注意到資料使用者根據保障資料第 4(1)原則保障其持有的個人資料的所需步驟在每一個案中都不盡相同，需要考慮許多因素，包括資料的數量、類別和敏感性；資料外洩可能導致的損害及傷害；資料管治和機構所採取的措施；以及相類似機構合理預期所應採用的技術政策、運作、控制和其他保安措施的質量和標準。

63. 專員認為快圖美作為管理遍及全港多間影像沖印及零售服務實體及網上商店的資料使用者，持有大量客戶的個人資料，理應就收集、持有、處理及使用這些資料制訂完善的政策、進行適當的風險評估，並按照保障資料第 4(1)原則採取所有切實可行的保安措施，以確保由其持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。

64. 在考慮本個案所有證據後，專員認為快圖美：—

(1) **錯誤評估保安漏洞的風險，沒有為系統保安採取任何行動，讓數據庫內的個人資料曝露於黑客攻擊的風險之中；**

(2) **沒有妥善管理載有個人資料的資訊系統，包括未有制訂嚴謹的修補程式管理程序，導致沒有及時修補保安漏洞，讓黑客成功透過相關漏洞入侵系統，並加密該數據庫；及**

(3) **沒有跟從防火牆生產商的建議，在機構內廣泛推行在家工作安排前為保密插口層虛擬私有網絡（SSL VPN）實施多重認證功能，防止黑客利用已獲取的密碼攻擊系統。**

65. **在本個案中，專員發現快圖美在個人資料風險意識及個人資料保安措施方面存在嚴重不足，導致公司的數據庫遭勒索軟件攻擊。專員認為快圖美對已知風險抱有過份樂觀甚或僥倖心理，明顯地錯誤評估相關漏洞對其載有個人資料的資訊系統造成的風險，以及一旦遭黑客入侵可能引致的後果，令人遺憾。專員認為快圖美沒有採取所有切實可行的步驟以確保涉事的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，因而違反了保障資料第 4(1)原則有關個人資料保安的規定。**

66. 雖然快圖美在該事件中有需要改善之處，但專員樂見快圖美及時作出資料外洩通報，配合私隱專員公署的調查，並致力從該事件中汲取教訓。該事件發生後，快圖美通過採取多種機構性和技術性的改善措施，已經修補保安漏洞，提升整體系統保安以保障個人資料私隱。

V. 執法行動

67. 專員認為快圖美違反了《私隱條例》附表一的保障資料第 4(1) 原則，因此依據《私隱條例》第 50(1)條所賦予的權力向快圖美送達執行通知，指示快圖美採取以下步驟以糾正違規情況，以及防止違規事件再發生：—

(1) 徹底檢視快圖美載有個人資料的系統保安，確保該些系統沒有已知的惡意軟件及保安漏洞；

(2) 聘請獨立的資料保安專家對快圖美的系統保安（包括快圖美網上商店的數據庫）進行定期檢視及審核；

(3) 修訂系統保安政策，明確訂定快圖美對其網絡設備（包括防火牆及／或伺服器）定期進行漏洞掃描；

(4) 修訂系統保安政策，明確訂定修補程式的管理政策及要求，並採取措施確保有關員工及提供系統保養服務的服務提供者依循相關政策及要求；及

(5) 由執行通知的日期起計三個月內向專員提供文件，證明已完成上述第 (1)至 (4)項指示。

68. 根據《私隱條例》第 50A 條，資料使用者違反執行通知，即屬犯罪，一經首次定罪，最高可被判處第五級罰款（即港幣 50,000 元）及監禁兩年。

VI. 建議及其他評論

69. 《私隱條例》第 48(2)(a)條訂明，專員在完成一項調查後，如認為符合公眾利益，可發表報告列明該項調查的結果及由該項調查引致的、專員認為適合作出的任何建議及其他評論。

建議

70. 專員理解網絡世界瞬息萬變，機構面對安全風險時，可能基於當時所得的有限資訊而未能作出適切回應。尤其在經歷 2019 冠狀病毒病疫情後，很多機構的運作模式急劇轉變，在家工作或網上網下混合工作模式已成為疫情下的「新常態」。在本個案中，SSL VPN 最初僅供資訊科技部門在個別情況下使用，惟後來因應疫情在機構內部廣泛推行在家工作安排，過去適用的保安措施亦因此變得不合時宜。因此，專員認為定期監察與個人資料系統安全風險相關的資訊尤其重要。

71. 專員希望通過本報告提醒處理顧客個人資料的機構須特別注意以下範疇：—

(1) **提高警覺，防止黑客攻擊**：面對着不同的保安漏洞，機構應時刻提高警覺，定時進行風險評估，以檢視黑客攻擊對系統可能帶來的影響，並加以維護載有個人資料的系統例如電子郵件伺服器、顧客資料庫等。

(2) **設立個人資料私隱管理系統**：機構應備有健全的個人資料私隱管理系統，循規使用及保留個人資料，有效管理由收集至銷毀個人資料的整個生命週期，令機構可迅速應對任何資料外洩事故，以及贏得客戶及其他持份者的信任。

(3)**委任專責人員作為保障資料主任**：機構應明確制訂保障資料主任的角色及職責，包括監察遵從《私隱條例》的情況並向高級管理層匯報，以及把員工提出的保障資料事宜和涉及客戶個人資料外洩事故的經驗及教訓納入機構的培訓材料中。

(4)**提升資訊系統管理**：機構應制訂有效的修補程式管理程序，盡早修補保安漏洞，並因應系統載有的個人資料數量及敏感度採取相應的技術保安措施，例如連接虛擬私有網絡時使用多重身份認證，為系統及帳戶帶來額外安全保障。

(5)**妥善記錄內部通訊**：機構當面對網絡設備生產商的建議與資訊系統服務提供者的意見有所不同時，盡職和審慎的做法是以書面諮詢有關生產商，以尋求進一步意見或釐清合適的跟進辦法，並將諮詢期間所有往來文件妥為保存，以便日後檢討時參考。

其他評論

72. 專員理解很多機構都會推出會員計劃，部份會員計劃更容許將消費金額累積，以便日後交易時換算為現金折扣，令會員帳戶具有一定價值。然而，消費者未必會定期管理名下的帳戶，這些長期閒置的非活躍帳戶除了會增加機構保障個人資料的成本，亦會增加資料外洩的風險。而且資料保留的時間越長，資料因過時而變得不準確的機會亦越大。

73. 根據快圖美向私隱專員公署提供的資料，在受影響的 544,862 名會員中，約 65%的會員（約 35 萬名會員）由創建帳戶至該事件發生前不曾有任何登入活動。雖然快圖美指出會員可主動要求刪除其會籍及個人資料，但**專員認為機構單憑未接獲刪除帳戶要求，便長期保留非活躍用戶的個人資料，未必符合顧客對個人資料私隱的合理期望。**快圖美其後向專員表示，將刪除過去三年沒有進行消費的非活躍用戶的個人資料。

74. **此外，專員留意到快圖美的網上商店網站已在 2020 年 11 月 16 日更新後停止收集會員的出生日子。專員認為機構須小心考慮收集個人資料的目的，並應在不損害使用資料的目的的情況下，謹慎制訂合適的個人資料保留期限，而非只為運作上的便利而保留個人資料。專員藉此提醒快圖美重新審視其個人資料庫，盡快刪除不必要的個人資料（包括審視繼續保存已收集得的會員的出生日子是否必要）。**

75. 隨着資料數碼化趨勢加速、資訊及通訊科技的互聯互通，以及資料本身的價值不斷上升，個人資料保安的風險亦隨之而增加。近年在香港和其他司法管轄區所發生的資料保安事故之上升趨勢亦證明了這一點。不論資料使用者是中小企業還是跨國企業，資料保安事故都可在聲譽及財務兩方面為其帶來嚴重後果。

76. 專員藉此指出，穩健的資料保安系統是構成良好資料管治的一個重要元素。專員理解資料使用者所需採取的保護個人資料措施會因情況而異，資料使用者除了應諮詢專業資料保安專家和法律顧問，以確保遵從《私隱條例》的相關規定，亦可參考私隱專員公署最近出版的《資訊及通訊科技的保安措施指引》[18]，了解與資訊及通訊科技相關的資料保安措施建議及加強資料保安系統的良好行事方式。

－完－

[18] www.pcpd.org.hk//tc_chi/resources_centre/publications/files/guidance_datasecurity_c.pdf