缺失態樣

辦理個資外洩應變演練之模擬情境有欠完整或演練作業欠周延。

缺失情節

- 對個資外洩應變演練之模擬情境，未依本會規定納入外部網路入侵、非法或異常使用行為所致之個資外洩事件等情境。
- 辦理個資演練僅為敘述性討論，未研擬具體演練案例；或未將個資外洩後如何防止損害擴大及通知客戶等重要作業程序納入演練，演練作業有欠確實、周延。

改善作法

- 對外部網路入侵及非法或異常使用行為等所致之個資外洩事件，應依規定納入演練情境辦理演練。
- 應訂定個資外洩事件通知當事人等應變演練處理程序，並確實辦理演練。

缺失態樣

對行員使用虛擬私有網路(VPN)，自行外登入銀行內部網路之控管措施欠妥適。

缺失情節

- 行員因業務需要，須由行外遠端連線至銀行內部處理事務，未申請虛擬私有網路帳號，以借用他人帳號作業，致有多人共用使用者帳號之情形。
- 對行員使用虛擬私有網路帳號登入銀行內部網路之行為，未留存使用稽核紀錄；或雖已留存使用稽核紀錄，惟未對該紀錄建立覆核機制。

改善作法

- 對行員使用虛擬私有網路帳號應訂定相關管理規範並建立控管機制。行員依規定提出申請，應依業務需要覈實審核，並嚴禁行員共用帳號，以明權責。
- 對使用虛擬私有網路帳號自遠端登入者，應留存使用之稽核紀錄，建立事後審核措施，並落實執行。

缺失態樣

未落實個人資料之使用及控管作業。

缺失情節

- 辦理資訊系統應用程式變更作業，有運用個人資料進行測試後，未予去識別化或刪除，逕留存於資訊部門檔案卷宗，不利個人資料保護作業。
- 申請將個人資料以電子檔案型式輸出利用，惟未建立個人資料運用後刪除之控管程序，不利於控管個人資料使用情形。

改善作法

應建立客戶資料產製運用及使用後刪除之控管機制。

缺失態樣

對於端點控制及敏感性個人資料遮罩之控管措施欠妥適；對外傳送電子郵件未建立有關個人資料之過濾機制。

缺失情節

- 對負責保單保全、收費及客戶服務話務人員有授予端點控管軟體解密權限，且其使用之個人電腦開放使用 USB，致有資料外流風險。
- 測試作業主機資料庫未對敏感性個人資料欄位予以遮罩；各作業部門對於作業過程中使用之個人資料仍置於本機電腦未予刪除，致他人登錄時仍可讀取之情形。
- 對於經由電子郵件系統對外傳送含有個資或機敏資料，未建立過濾機制及控管措施。

改善作法

- 涉及個資之存取，應嚴格控管該等資料之存取權限，依職務需要覈實授權，並應對資料之存取及傳遞建立申請、保管、使用及刪除等規範，並留存完整稽核軌跡、建立主管覆核及定期清查等管控機制。
- 應避免將客戶真實資料複製至測試環境作業，如確有須將未去識別化個資複製至測試環境之業務需求，應建立申請、刪除、留存完整稽核軌跡等管控程序。
- 應建置電子郵件內文過濾系統，並就對外傳送含有個資或機敏資料之電子郵件建立審核及追蹤控管機制。

缺失態樣

對客戶個人資料未能妥善使用及保管。

缺失情節

- 財富管理部之行銷研發人員負責理專業績統計及保險商品維護及系統管理人員負責系統權限建檔，依職務性質均無查詢客戶財管資料之必要，惟有賦予該等人員設定可查詢全行財管客戶個人資料之權限。
- 公用資料夾存有多筆客戶個人資料，可供查詢、複製及列印，並未建置存取權限控管。
- 未確實設定關閉 USB 讀取功能，致有未經主管核准授權之個人電腦，也可使用 USB 裝置情事。

改善作法

- 應依據員工工作需求設定查詢權限，另涉及個資檔案之存取，應嚴格控管該等資料夾之存取權限，依權限需要覈實授權，相關存取應留存完整稽核軌跡、建立主管覆核及定期清查等管控機制，並落實執行。
- 對個人電腦之 USB、軟碟機、燒錄機等設備，應降低使用比率，並建置軟體工具管制及建立使用管理機制；對前開儲存媒體及工具攜出檔案之使用紀錄，應產製稽核報表及建立覆核機制，並及時覈實覆核。

缺失態樣

將含有大量客戶個資檔案置於安全防禦較弱之環境，且透過網際網路對外傳遞，亦未建置完善之加密通訊保護機制。

缺失情節

- 將存有大量客戶個資檔案之傳檔伺服器(FPT SEVER)放置於網路安全防禦較弱之非軍事區（DMZ），且未建立攻擊及管制連線等相關安全防範措施。
- 以 FTP 傳檔方式對外傳遞含客戶個資之檔案，惟未將檔案加密處理或僅使用安全性低之資料壓縮程式加密，傳輸過程未能確保資料隱密性及安全。

改善作法

- 應避免將存有個人資料檔案之傳檔伺服器或資料庫置於非軍事區（DMZ），如因特定作業需要，除應加強資料檔案之保密性外，並應建立相關存取控管機制或其他強化保護措施。
- 對傳送個資檔案至外部單位作業，應建立完善之加密通訊保護機制，強化檔案傳輸之安全性。

缺失態樣

對傳檔伺服器之使用者帳號密碼管理及存取權限設定欠妥適。

缺失情節

傳檔伺服器之使用者帳號及權限管理，有下列情事：

- 供傳檔連線認證之使用者帳號密碼，以明碼方式儲存，且未嚴格控管存取權限，允許全行使用者（Users）均得讀取。
- 部分供系統自動傳輸檔案之使用者帳號，有另供人工作業使用，權責不清。
- 傳檔伺服器內存放明碼個資檔案，未依業務需要授予存取權限，允許全行使用者（Users）均得讀取該伺服器內之檔案。

改善作法

- 應建立傳檔伺服器之使用者帳號及檔案存取權限管理機制，並落實執行，且應定期清查使用情形是否妥適，強化傳檔伺服器管理。
- 傳檔認證之使用者帳號密碼應亂碼化處理，或建立密碼保護措施，確保其隱密性，並嚴禁使用者共用帳號，以明權責。
- 對傳檔伺服器使用者之作業權限，應依業務需要設定檔案存取權限，對含有個資之檔案資料應建立保密措施，避免不當存取，俾確保個資檔案之安全。

缺失態樣

對個資之儲存、傳遞及使用之控管機制欠嚴謹。

缺失情節

- 部分應用系統未設計留存個資查詢或列印之稽核軌跡，或留存之軌跡欠完整。
- 對使用外部信箱、Line、社群網站及員工透過網際網路使用 webmail 或員工個人行動裝置透過 Push mail，收取公司電子郵件，尚未建立過濾控管機制。
- 員工寄送含有個資之電子郵件，未建立郵件阻擋、審核與追蹤機制；或已建立過濾機制，惟過濾原則有欠完整。
- 對寫出至 USB 之檔案未建立稽核軌跡，或雖產製稽核軌跡，惟未建立覆核機制。

改善作法

- 對使用應用系統查詢或列印個資等行為，應留存相關作業完整之稽核軌跡。
- 對員工使用外部信箱、社群網站，及透過 Push mail 收取電子郵件，應建立資料傳輸過濾機制或相關控管措施。
- 對電子郵件應建立完整之個資過濾原則，並對加密或無法辨識之電子郵件附檔建立管控機制。
- 對寫出至 USB 之檔案應建立稽核軌跡及覆核機制，並對檔案複製至 USB 後之資料流向建立管控措施。

缺失態樣

調閱或運用客戶個人資料，於使用單位運用結案後，無後續資料銷毀之管控機制。

缺失情節

- 客服部門申請提供業務員歸屬客戶名單，於運用結案後，無後續資料銷毀之紀錄及管控機制。
- 資訊單位辦理系統變更作業，有申請單位提供個人資料予資訊單位修訂參考，資訊單位完成相關變更作業後，未將該等個人資料刪除或去識別。
- 資訊單位辦理異地備援演練測試結果，其底稿留存個人資料，未去識別化。

改善作法

應依「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第 14 條：「非公務機關依本法第 11 條第 3 項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：一、刪除、停止處理或利用之方法、時間。…軌跡資料、相關證據及紀錄，應至少留存五年」之規定辦理，並建立客戶個資運用後之銷毀管控機制。