缺失態樣

推動及督導個人資料保護安全維護之作業有待加強。

缺失情節

- 金控公司尚未依「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」訂定個人資料保護相關規範，以為各單位及子公司遵循，且亦未對各單位作業進行個人資料盤點，致難以掌握公司內重要個人資料檔案及書面文件是否採取適當安全防護措施。
- 金控公司稽核單位查核子公司發現個資保護機制有欠完善，如：未建立專責單位、相關政策(管理辦法)、或未進行個資盤點，雖已提列建議事項，惟未要求提報改善計畫及時程並定期追蹤其辦理情形，子公司亦未改善。

改善作法

- 金融控股業者保有大量且重要之個人資料檔案，其所負之安全維護責任較一般行業為重，爰應儘速訂定執行個人資料檔案安全維護計畫及業務終止後個人資料處理方法，並落實執行。
- 金控公司稽核單位查核發現子公司個資保護機制有欠完善者，應採取持續追蹤覆查等積極作為，以加強管理、確保個人資料之安全維護。

缺失態樣

未確實要求子公司改善客戶機敏性資料之控管流程。

缺失情節

- 金控子公司曾因使用印有客戶資料之回收紙張，致客戶資料外洩並遭本會裁處，惟未落實改善，仍再度發生類似缺失。
- 金控公司稽核單位查核發現其他子公司將客戶機敏性資料置放或廢棄於任何人皆可取得之處，均僅以建議事項處理，未追蹤改善辦理情形，不利個資保護作業之進行。

改善作法

- 印有客戶機敏性資料之紙張，應予妥善保存，對於無須使用者應確實銷燬，不得回收再利用，以免易滋客戶資料外洩之虞。
- 對於子公司未能妥善控管機敏性資料，應督促落實改善辦理情形，以免日後發生損及消費者權益之情事。

缺失態樣

對個人電腦網路位址、最高權限及各類儲存裝置未建立控管機制或管理欠妥。

缺失情節

- 個人電腦網路位址採用浮動配發（DHCP）之方式，未建立辨識是否為內部電腦設備之機制。
- 行員可使用本機最高權限使用者帳號登入其個人電腦，致可任意安裝或移除其個人電腦之相關軟體。
- 對已報廢之硬碟，未儘速執行低階格式化或實體破壞。
- 可攜式儲存裝置（USB）使用之稽核報表內容欠完整。

改善作法

- 建立辨識內部電腦設備之機制，加強控管內部網路連線。
- 回收個人電腦最高權限使用者帳號密碼，建立資訊資產清查管理機制。
- 檢討回收個人電腦作業流程，對報廢之硬碟，建立後續追蹤管控機制，並落實執行。
- 使用可攜式儲存裝置（USB）之稽核報表內容宜包含檔案大小、名稱、內容及執行作業使用者代號與時間等資訊，並落實稽核報表覆核作業。

缺失態樣

對客戶集保密碼以明碼方式儲存於客戶基本檔內，未建立控管程序；另對員工存取客戶個人資料作業，未做成稽核紀錄。

缺失情節

- 未留存公司代理客戶向集保公司申辦集保密碼之證明文件，且將集保密碼設定為客戶帳號後 4 碼，並以明碼儲存於客戶基本檔內，倘客戶未變更密碼，公司內部人員均可以此密碼查詢客戶庫存部位。
- 對於員工存取客戶個人資料 (如：查詢、列印、下載等)，尚未做成稽核紀錄，核與「建立證券商資通安全檢查機制」第 8 點第 5 款及「個人資料保護法施行細則」第 12 條之規定不符。

改善作法

- 應建立代理客戶申辦集保密碼之控管程序，以確保客戶個人資料安全。
- 應依照「建立證券商資通安全檢查機制」規定，建立個人資料之使用紀錄、軌跡資料及資料安全等之稽核機制。

對客戶個人資料檔案之刪除、保管及使用未建立相關控管機制，或委外作業對於客戶資料之控管有欠妥適。

缺失情節

- 以電子郵件方式傳遞至分行有關基金及台外幣綜合電子對帳單寄送失敗名單，收件者包括非業務經辦人員。
- 測試主機留有未去識別化之個資檔案、業務經辦人員長期保存大量未加密客戶個資檔案、理財人員私自保管客戶個資及交易文件，以及客服人員具查詢及列印客戶個資及多項業務交易資料權限。
- 委外單位將所傳遞予受託機構之客戶資料儲存於專屬公用電腦久未刪除，且該電腦尚留有 USB 存取槽可供存取檔案資料，或雖有將客戶資料檔案刪除，惟未留存檔案刪除之稽核軌跡。

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。
- 對電腦之儲存媒體及工具，應降低使用比率，建置使用及管控機制，並對使用紀錄產製稽核報表及建立覆核機制。

缺失態樣

對存放含有客戶個資之公用檔案伺服器及個人電腦資料檔案之權限管理有不利個資安全防護情事。

缺失情節

- 存放含有客戶個資明碼資料之公用檔案伺服器及個人電腦檔案夾相關存取權限及檔案分享功能有授予非職務所需之人員。
- 對存放含有客戶個資檔案之伺服器及個人電腦，有開啟「網路芳鄰分享資料夾」功能，且未建立定期檢視分享資料夾權限及留存存取紀錄等管理機制，不利個資安全維護。

改善作法

涉及個資檔案之存取，應嚴格控管該等資料夾之存取權限，依職務需要覈實授權，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。

缺失態樣

對外傳送電子郵件未建立控管機制。

缺失情節

經由電子郵件系統或連接外部網頁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

- 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。
- 建置資料外洩防護(DLP)系統，以監控、管理並預防個資或機敏資料外洩。

缺失態樣

未留存稽核軌跡或稽核軌跡留存欠完整，或對稽核軌跡未建立覆核機制。

缺失情節

- 未留存稽核軌跡或稽核軌跡留存欠完整：
  - 電子商務服務系統未留存執行查詢及變更密碼交易之稽核紀錄。
  - 伺服器僅留存開啟傳檔連線之紀錄，未啟用檔案傳輸稽核功能，留存檔案存取之稽核紀錄。
  - 僅對資料庫特殊權限帳號管理作業啟用稽核功能，其他使用帳號則未予以稽核，且對資料選取（select）、更新（update）及刪除（delete）等存取作業，亦未留存稽核軌跡。
- 資料庫帳號管理、系統參數設定及執行查詢、變更等作業，雖已留存稽核紀錄，惟未建立覆核機制。

改善作法

- 清查應用系統是否已設計留存查詢個人資料之稽核紀錄、傳檔系統是否已建立檔案傳輸稽核軌跡，確實留存完整之稽核軌跡。
- 檢討資料庫稽核軌跡之完整性，除調整資料庫系統之稽核功能或建置資料庫稽核系統外，並留存完整之資料存取稽核軌跡。
- 建立稽核軌跡覆核作業機制，並落實執行。

缺失態樣

對業務員疑似個資外洩事故之通報及後續改善措施欠完善。

缺失情節

- 對業務員疑似個資外洩事件，未納入個資事故通報範圍，且未明定事故通報相關部門主管及核定層級。
- 對疑似個資事故通報案件之改善措施，僅對業務員加強宣導保護個資，未對業務員個人行動裝置所儲存之客戶個資研議加強保護措施。

改善作法

- 對個資外洩事件建立妥適之通報及善後處理標準作業程序，以利個資外洩事件作業風險控管及處置。
- 對業務員個人行動裝置應訂定使用規範，並對所儲存之客戶個資建立適當保護措施，俾防範個資外洩。