缺失態樣

客戶不同意揭露、轉介或交互運用其個人資料，仍提供子公司辦理電話行銷。

缺失情節

- 提供子公司辦理電話行銷之客戶資料，除基本資料以外，尚包含未經客戶同意提供之帳戶資料。
- 客戶不同意其帳戶及保險資料交互運用者，仍依其他子公司所定篩選條件進行分析後，將達一定條件者之基本資料提供子公司辦理電話行銷。

改善作法

- 金控公司及子公司對於客戶個人基本資料、往來交易資料及其他相關資料之管制作業，應注意下列事項：
  - ◎ 應訂定讓客戶選擇是否同意提供前述資料作為共同行銷運用之欄位及簽名處，並應列明運用資料之子公司名稱，供客戶勾選。
  - ◎ 應切實依客戶勾選結果正確建檔，並對建檔結果予以覆核。
  - ◎ 客戶已表明不同意交互運用基本資料以外之資料者，亦不得逕自設定篩選條件分析使用。

缺失態樣

對外寄送含有客戶個資之電子郵件，未建立控管措施。

缺失情節

對員工寄送含有客戶個資之電子郵件，未建立事先偵測、阻擋控管機制，且事後亦未留存完整稽核軌跡，致員工即使透過電子郵件夾帶附檔，將客戶個資檔案不法寄出行外，亦無從得知且不利追查。

改善作法

對電子郵件應制定管理規範，包括對寄送含有客戶個資檔案之郵件應建立過濾、篩選、阻擋、留存稽核軌跡等監控管理機制，以確認資料傳送之合法性，並應定期檢討控管機制執行之有效性。

缺失態樣

測試環境作業管制欠妥，未落實個資安全防護。

缺失情節

- 因應特殊業務需求，將正式主機個資傳遞至測試主機作業，未建立妥適控制程序，且對資料檔案權限設定亦欠嚴謹，致客戶個資有外洩風險。
- 辦理應用系統測試，未能落實個資去識別化作業，致測試主機存有正式客戶檔案或資料庫，不利個資安全維護。

改善作法

- 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作業之業務需求，除應建立申請、刪除、留存完整稽核軌跡等管控程序外，並應嚴格管理該等資料檔案之存取權限。
- 應重新檢視複製正式主機檔案及資料庫至測試主機去識別化作業程序之妥適性，並落實執行。

缺失態樣

對使用隨身碟等可攜式儲存媒體未建立控管機制或管理欠妥。

缺失情節

- 對個人電腦之 USB、軟碟機、燒錄機等設備之使用，尚未建立控管機制，易致客戶個資及業務機敏性資料外洩。
- 對個人電腦之 USB、軟碟機、燒錄機等設備之使用，雖採防護軟體控管，惟對上開設備之使用軌跡紀錄，尚未產製稽核報表及建立覆核機制、或未及時覆核，管控措施尚欠周全，不利個資檔案安全維護及事後追蹤控管。

改善作法

- 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，落實執行。
- 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

共用資料夾檔案存取管制欠妥，不利個資安全防護。

缺失情節

因應業務需求，有以開啟共用資料夾分享方式，授權同一單位人員均可存取該等資料夾內個資檔案，惟未依職務需要適當授權，且對該等資料夾檔案存取未留存稽核軌跡，控管措施有欠妥適，不利個資安全維護及事後追蹤。

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

對電腦主機下載含客戶個資檔案至外接儲存裝置，未建立妥適控管措施；且發現員工以外接儲存裝置下載大量客戶個資，未列為重大資安事件依程序通報。

缺失情節

銀行員工於離職前，將電腦主機公用資料夾（內含上萬筆客戶個資）檔案下載至私人外接儲存裝置(USB)，銀行對外接儲存裝置之使用情形未予即時監控，致行員離職後始發現此重大資安事件，且發現後未陳報該行高階管理階層，以積極改善資安弱點，亦未向本會通報重大偶發事件。

改善作法

- 銀行電腦主機公用資料夾，應避免存放大量客戶個資。
- 對授權存取機敏資料之員工，應建立即時監控機制。
- 對發生客戶個資遺失、遭竊取或外洩等重大資安事件，應即時通報高階管理階層及主管機關，以利追蹤及管控。

缺失態樣

申請調閱客戶交易資料，有未依規定辦理之情事。

缺失情節

客戶申請調閱交易資料，有未填寫申請表且未依規定以流水編號製作之情事，核與「證券商受僱人員查詢客戶資料管理作業要點」第 8 點規定不符；或員工申請調閱客戶交易資料，有未載明所調閱之資料期間、交易內容者，不利事後追蹤管理。

改善作法

- 證券商應詳實紀錄所調閱或複製之客戶資料內容。
- 應落實客戶調閱交易資料作業，切實依 100.6.24 證交所所訂「證券商受僱人員查詢客戶資料管理作業要點」之規範，確實填寫申請表敘明調閱資料內容，並依序編號列管。