缺失態樣

辦理電話行銷業務之個人資料保護作業欠妥適。

缺失情節

- 與人壽保險公司合作辦理電話行銷作業，所傳遞之電子檔案有提供客戶之其他非必要個人資料。

改善作法

- 提供客戶個人資料應檢視內容之妥適性，避免提供不必要之資訊；個人資料檔案對外傳輸時，應適當遮蔽，俾利落實個人資料之保護作業。

缺失態樣

辦理個人資料安全維護作業有欠確實。

缺失情節

- 辦理年度個資盤點作業，未將含有客戶個人資料之實體紙本文件及數位檔案資料納入清查範圍，或個人資料管理單位未定期提出自我評估報告。
- 員工個人電腦(含筆電)未建置隨身碟(USB)使用控管措施，或對員工使用內部電子郵件信箱，及利用個人電腦連結外部私人電子郵件信箱傳遞涉及個人資料，未建置控管措施。
- 辦理個人資料保護評估及盤點作業，對個人資料流程識別清單所列業務或範圍有欠完整，致個資盤點有缺漏情形。

改善作法

- 應依「本會指定非公務機關個人資料檔案安全維護辦法」第 4 條及第 15 條規定，定期查核確認所保有之個人資料現況，界定其納入本計畫及處理方法之範圍，並定期提出相關自我評估報告，經董事會決議或經其授權之經理部門核定。
- 應建置員工個人電腦(含筆電)使用 USB 及電子郵件信箱傳遞涉及個人資料之控管措施，以維護個人資料之安全。

缺失態樣

辦理個人資料安全性保護作業有欠周延。

缺失情節

- 對外郵寄電子郵件個資過濾原則，未將出生年月日、銀行帳號、證券帳號等敏感性個人資料納入過濾條件。
- 寄送董事會、審計委員會、薪資報酬委員會涉機敏性會議資料及函復外部機關調閱之客戶資料，未予加密。
- 將含有客戶個人資料之文件直接放置於開放空間或棄置於資源回收桶。
- 客戶個人開戶及交易資料等文件內容涉及客戶個人資料，有留存於公用資料夾，未予以加密或於使用後刪除。

改善作法

- 應依「本會指定非公務機關個人資料檔案安全維護辦法」第 9 條規定，為維護所保有個人資料之安全，應採取防範資料洩漏之適當措施，對外郵寄電子郵件應將敏感性個人資料納入過濾或篩選條件。
- 應加強員工教育訓練，強化個人資料保護之觀念及文化，以維護個人資料之安全。

缺失態樣

資料外洩防護機制及留存紀錄欠完善。

缺失情節

- 資料外洩防護(DLP)過濾規則設定欠妥，且實測發現 DLP 未阻擋電子郵件傳送多筆個資並留存紀錄；另對特定副檔名檔案(如：jpg 圖檔)尚未建立過濾阻擋機制，不利客戶個資保護。
- 尚未建立資料外洩防護偵測機制，且對寫出檔案至 USB 者未予記錄；另尚未建立於網頁(如：雲端硬碟及留言板等)上傳個資相關偵測機制並予以記錄之機制。

改善作法

- 應建立資料外洩防護偵測機制，並適時檢討過濾規則之妥適性，以確保客戶個資安全。
- 應依「電子支付機構資訊系統標準及安全控管作業基準」規定，建置留存個人資料使用稽核軌跡，以利追蹤客戶個人資料使用狀況。

缺失態樣

辦理子公司間共同行銷客戶資料之運用作業，對資料儲存、保管、使用之控管措施有欠妥適。

缺失情節

- 子公司定期透過加密電子郵件將同意共同行銷之客戶資料傳送予金控母公司，惟未建立定期清查與刪除客戶資料之控管機制，致有客戶資料留存於經辦個人電子郵件信箱之情事。

改善作法

- 應依「金融控股公司子公司間共同行銷管理辦法」第 11 條第 2 項規定，對客戶資料建立妥善之儲存及保管措施，以確保客戶資料安全。

缺失態樣

個人資料維護管理作業欠妥。

缺失情節

- 未定期辦理個資外洩演練作業，亦未研擬個資外洩情境、防止個資外洩損害擴大及通知客戶等作業程序之演練計畫。
- 未建立個資阻擋、例外免偵測(白名單)等過濾規則之定期檢視機制。

改善作法

- 應依「本會指定非公務機關個人資料檔案安全維護辦法」規定，對防止外部網路入侵對策，定期演練及檢討改善。
- 應建立過濾規則定期檢視機制，以維個資安全。

缺失態樣

對客戶個人資料之保護與控管機制有欠妥適。

缺失情節

- 未建立因應個人資料遭竊取、竄改、毀損、滅失或洩漏等安全事故之應變、通報及預防機制。

改善作法

- 應依「本會指定非公務機關個人資料檔案安全維護辦法」第 6 條規定，訂定個人資料之竊取、竄改等安全事故之應變、通報及預防機制。