金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

112 年度下半年主要檢查缺失

-金控公司

目　　次

業務項目：子公司管理

缺失態樣

子公司對客戶使用行動裝置相關異常檢核機制有欠完善。

缺失情節

- 證券子公司對於不同客戶以同一手機號碼進行APP下單憑證設定作業之OTP簡訊驗證，未檢核合理性。
- 銀行及證券子公司未管控同一行動裝置綁定客戶人數之上限，亦未於綁定前檢核客戶間是否有合理綁定關係，且對不同客戶以同一行動裝置登入或交易尚未建立異常監控機制。

改善作法

- 應督導子公司建立不同客戶以同一行動裝置綁定、登入或交易，及以同一手機號碼進行OTP簡訊驗證之異常檢核機制，以加強客戶交易安全與資安控管。

業務項目：風險管理

缺失態樣

提報董事會之風險管理報告未完整涵蓋金控集團整體風險。

缺失情節

- 提報董事會之風險管理報告，關於市場風險、產業集中度、預期信用損失等數值，僅含第一層子公司個體暴險數據，未納入第二層子公司及以下各層子公司。

改善作法

- 應強化提報董事會風險管理報告之完整性，以確保有效控管相關風險並採行妥適之因應措施。

業務項目：內部管理

缺失態樣

辦理資料共享之控管機制有欠妥適。

缺失情節

- 金控公司及子公司向資訊部門提出產製客戶資料之需求表單，未敘明資料需求目的及產製檔案內容，不利審核申請之必要性及勾稽比對所交付資料之正確性。
- 未要求需求單位回報客戶資料使用及銷毀/刪除紀錄，致無法追蹤各需求單位對客戶資料利用之妥適性。

改善作法

- 應強化金控公司及子公司對客戶資料共享之申請、交付及追蹤控管機制，並督導子公司落實客戶資料保護，以維客戶資料安全。

業務項目：資訊安全

缺失態樣

辦理客戶個資及公司機敏業務資料保護作業有欠妥適。

缺失情節

- 雖已建置資料外洩防護機制(Data Loss Prevention，簡稱 DLP)，將電子郵件寄送、上傳檔案至外部網頁等納入監控範圍，惟未訂定檢視 DLP 有效性之內部規範，對符合 DLP 所偵測之行為，亦未建立妥適之審核及控管機制。
- 對 USB 可攜式儲存媒體白名單人員之管控，未建置 DLP 機制並留存 USB 攜出檔案之完整內容。
- 對銀行子公司員工查詢非所屬客戶個資之行為未建立妥適之管控機制。

改善作法

- 應檢討金控公司及子公司員工寄送電子郵件、使用 USB 等之 DLP 機制，並建立對員工查詢非所屬客戶個資之控管機制，以強化客戶個資保護及資訊安全。