金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

113 年度下半年主要檢查缺失

-專營電子支付機構

目　　次

業務項目：防制洗錢、打擊資恐及反武擴作業

缺失態樣

對電子支付帳戶之加強身分驗證措施欠妥適。

缺失情節

- 對帳戶或交易之監控態樣，未就高風險客戶訂定較低交易金額或交易筆數等較嚴格之參數，以強化持續監督措施。
- 對高風險客戶之確認身分措施，未以加強方式執行客戶身分驗證。

改善作法

- 應依「電子支付機構防制洗錢及打擊資恐注意事項範本」規定，對評估辨識為高風險或具特定高風險因子之客戶，以加強方式執行驗證，並加強對於業務往來關係採取強化之持續監督。

業務項目：個人資料保護

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。

業務項目：業務操作管理

缺失態樣

辦理作業委託他人處理作業欠妥。

缺失情節

- 對作業委託他人處理之資格審核、管理及查核作業等事項，有未確實依內規辦理。
- 辦理第一類非個人之特約機構契約簽訂作業，對受委託機構推廣收單業務所簽訂之特約機構，未以實地審查方式確認其身分。

改善作法

- 應確實辦理受委託機構之資格審核及監督查核，並依規定落實辦理受委託機構推廣特約機構之身分確認作業。

業務項目：資訊安全

缺失態樣

辦理主機特權帳號管理欠妥。

缺失情節

- 部分主機高權限帳號未納入特權帳號管理系統，並建立事前申請及事後覆核機制。
- 系統人員辦理日常維運所持有之網域(AD)帳號，皆為 Domain Admins 群組之成員，無須申請即取得同一網域所有 Windows 伺服器之最高權限。
- 虛擬主機管理系統(VMware vSphere)維運人員所持有之帳號具有系統管理員權限，並以該等帳號進行日常維運。
- 對特權帳號登入後相關操作所留存紀錄，未建立覆核機制，不利及時發現有無異常使用。

改善作法

- 應檢討各主機特權帳號使用控管與覆核程序，以確保資訊安全。

業務項目：資訊安全

缺失態樣

辦理行動裝置應用程式(APP)管理及發布作業欠妥。

缺失情節

- 未於首次發布前辦理程式碼掃碼或黑箱測試及依據 OWASP 公布之 Mobile Top 10 項目辦理並通過檢測，即逕行上線。
- 未於發布前檢視應用程式所需權限應與提供服務相當，並於首次發布或權限變動經資安、法遵及風控等主管同意。
- 內部人員持有 APP 發布權限，僅 1 人即可完成 APP 發布作業，未建立應用程式發布程序，由兩人以上或採用兩項(含)以上技術管控。
- 未建立商店帳號權限定期盤點機制，且所列帳號清冊未將具管理權限帳號納入。

改善作法

- 應全面檢討行動應用程式安全控管之妥適性，以維交易安全與客戶權益。