金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

114 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

對客戶洗錢風險評估作業欠妥適。

缺失情節

- 辦理客戶洗錢風險評估作業，未將組織型態、股權複雜度及註冊管道等項目，納入風險評估項目，如：基金會、股份有限公司等不同組織型態之特約機構及採 APP 線上申請之客戶。

改善作法

- 應確實依「電子支付機構評估洗錢及資恐風險及訂定相關防制計畫指引」第 3 點規定，辨識客戶洗錢及資恐風險，參照客戶之註冊管道、組織型態及股權複雜度等因素，採取合宜措施以識別、評估其洗錢及資恐風險。

業務項目：防制洗錢、打擊資恐及反武擴作業

缺失態樣

辦理客戶身分之持續審查及定期審查作業未臻落實。

缺失情節

- 對高風險客戶有逾 1 年未辦理定期審查情形。
- 對高風險客戶之持續審查作業，未採取強化審查措施。
- 未明確訂定中、低風險客戶之定期審查頻率，致部分客戶逾多年未辦理定期審查。
- 公司或行號已登記解散，其所開立之電子支付帳戶仍持續辦理交易。

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」第 6 條第 1 項第 1 款規定，對高風險客戶辦理定期審查作業及強化審查措施。
- 應依「金融機構防制洗錢辦法」第 5 條規定，確實考量前次執行審查之時點及所獲得資料之適足性等因素，辦理客戶身分持續審查。
- 應依「電子支付機構防制洗錢及打擊資恐注意事項範本」第 5 條第 3 款規定，客戶之交易或帳戶之運作方式出現與該客戶業務特性不符之重大變動時，應依第 4 條規定對客戶身分再次確認。

業務項目：個人資料保護

缺失態樣

個人資料保護作業欠妥適。

缺失情節

- 對遠端登入正式環境資料庫行為，尚未留存完整稽核軌跡，不利客戶資料安全。
- 個資防護管理作業欠妥，如：未定期檢討個資外洩過濾規則；外寄電子郵件過濾條件未納入姓名、行動電話；對已達所訂個資閾值之電子郵件及網頁傳輸行為，未能有效阻擋。

改善作法

- 應依「電子支付機構資訊系統標準及安全控管作業基準」第 16 條第 5 款規定，建置留存個人資料使用稽核軌跡或辨識機制。
- 應定期檢討個資過濾條件之妥適性，強化個資外洩防護機制，以維個資安全。

業務項目：業務操作管理

缺失態樣

辦理特約機構徵信審核及風險控管作業欠妥適。

缺失情節

- 未將特約機構類型、交易模式列為審核標準，均將每月收款額度核予第二類特約機構最高上限額度。
- 辦理特約機構之徵信審核，未考慮交易金額，即核予每月收款額度。
- 對特約機構銷售遞延性商品或服務者，未確認其是否已依規辦理履約保證或交付信託。

改善作法

- 應依「電子支付機構業務管理規則」第 4 條規定，依特約機構類型、交易金額、交易模式、遞延性商品或服務及銷售商品之風險性，建立相關控管機制。

業務項目：資訊安全

缺失態樣

遠端連線安全控管機制欠妥適。

缺失情節

- 對可遠端連線至正式環境伺服器之設備，尚未建立設備識別及安全性檢測機制，並建立允許連線設備清冊，不利主機系統安全。
- 允許遠端連線正式營運環境，惟未限制複製(copy)及貼上(paste)功能，且未留存資料輸出作業軌跡，不利客戶資料安全。

改善作法

- 應依「電子支付機構資訊系統標準及安全控管作業基準」第 21 條第 8 款規定，強化遠端連線資安控管機制及資料存取與輸出入管理機制，以維系統及客戶資料安全。

業務項目：資訊安全

缺失態樣

特權帳號管理機制欠妥適。

缺失情節

- 由個人持有最高權限使用者帳號，並辦理日常維運管理，且對特殊權限使用者未建立覆核機制。
- 已建立特權帳號管理系統控管主機最高權限帳號之使用，惟有領用密碼進行登入，未於使用結束後儘速變更密碼。

改善作法

- 應依「電子支付機構資訊系統標準及安全控管作業基準」第 15 條第 3 款第 3 目規定，檢討特權帳號管控機制之妥適性，依最小權限原則授予權限，強化覆核機制，並於使用後立即回收變更密碼，以維系統安全。