金融監督管理委員會檢查局
Financial Examination Bureau, Financial Supervisory Commission, ROC

108 年度主要檢查缺失

-專營電子支付機構

目　　次

防制洗錢及打擊資恐作業……1

資訊安全管理……2

個人資料保護……4

業務操作管理……5

業務項目：防制洗錢及打擊資恐作業

缺失態樣

對疑似洗錢、資恐及其他可疑交易之檢核及查證作業有欠確實。

缺失情節

- 僅對儲值限額、電子支付帳戶轉帳及提領進行監控，對帳戶常有頻繁不正常退款等異常交易活動之態樣則未納入監控範圍。
- 雖以資訊系統輔助電子支付帳戶或交易之監控作業，惟對疑似洗錢、資恐及其他可疑交易態樣參數設定欠妥適，致未能有效發揮監控功能，且對由系統產出符合疑似洗錢或資恐交易態樣之報表，未妥適審核。

改善作法

- 應參酌「電子支付機構防制洗錢及打擊資恐注意事項範本」附錄所列疑似洗錢或資恐交易態樣，切實檢視確認各項業務之異常交易態樣及表徵均已納入監控範圍，如有疏漏，應檢討修改篩選條件，以確保檢核機制之有效性。
- 應加強員工教育訓練及主管覆核作業，對監控報表所列之警示交易，詳實填寫研判紀錄並留存適足之佐證資料，如認定非疑似洗錢或資恐交易者，應記錄分析排除理由，如研判有疑似洗錢或資恐之交易，應依規定向法務部調查局申報。

業務項目：資訊安全管理

缺失態樣

行動裝置應用程式(APP)之維護管理作業有欠妥適，不利資訊安全。

缺失情節

- 未於 APP 發布前檢視應用程式所需權限是否與提供服務相當，如：要求存取位置、電話、聯絡人、儲存空間及相機等權限，未檢視所需各項權限之必要性及合理性，並經法遵及風控部門同意。
- 尚未對 APP 發布平台建立蒐尋檢視機制，不利預先辨識偽冒之 APP 及採行適當處理措施。

改善作法

- 應確實遵循「金融機構提供行動裝置應用程式作業規範」之規定，如：
  - 於 APP 首次上架或權限變動時，應逐項檢視 APP 所需各項權限之必要性及合理性，並經法遵及風控等部門同意，以綜合評估是否符合「個人資料保護法」之告知義務。
  - 應建立偽冒 APP 之偵測機制，於發現有偽冒 APP 之情事應即時處理，以維護客戶權益。

業務項目：資訊安全管理

缺失態樣

辦理程式及資料庫資料變更作業，分工有欠牽制；或未留存完整紀錄，不利控管程式變更之正確性。

缺失情節

- 辦理程式變更作業，未訂定相關作業規範，致有應用程式原始碼由程式開發部門自行管理，及應用程式上版由程式開發人員執行等欠牽制情事。
- 辦理程式變更及資料修改，相關異動未留存測試紀錄及變更前後比對表供主管覆核，不利確認變更之正確性及完整性。

改善作法

- 應訂定應用系統開發及維護作業規範並落實執行，如：
  - 正式營運環境之程式及資料變更作業（如執行、覆核）應由二人以上進行，以相互牽制，並留存相關紀錄。
  - 程式不應由開發人員自行換版或產製比對報表，並應建立程式原始碼管理機制，以符合職務分工與牽制原則。
- 應訂定資料變更相關管理規範，並確實依分工牽制原則辦理資料變更作業及留存相關紀錄。

業務項目：個人資料保護

缺失態樣

對含有客戶個人資料檔案之個人電腦或筆記型電腦，未建立妥適控管機制，不利防範個資外洩風險。

缺失情節

- 允許個人電腦可寫出資料至可攜式儲存媒體(如USB隨身碟、隨身硬碟、光碟機等)，惟對寫出資料含有個資檔案者，未建立過濾機制，亦未留存軌跡紀錄及建立審核放行等控管機制。
- 允許員工透過網際網路連線至內部讀取郵件(Web Mail)，並將客戶資料下載儲存於員工之個人電腦或手機等設備裝置，惟尚未建立偵測管控機制。

改善作法

- 對電子支付作業環境之個人資料保護應建立資料外洩防護機制，管制個人資料檔案傳輸至個人電腦或筆記型電腦，並應留存相關紀錄、軌跡與數位證據，如：
  - 對 USB 儲存媒體寫入內含個資檔案或加密檔案應建立妥適控管措施，並強化主管覆核機制。
  - 對客戶資料下載儲存至員工之個人電腦或手機等設備應建立偵測管控機制。

業務項目：業務操作管理

缺失態樣

接受使用者申請註冊及開立電子支付帳戶，對使用者身分確認作業欠完善，不利防範偽冒開戶之風險。

缺失情節

- 使用者身分資料確認機制欠完善，致有使用假名成功註冊及開立電子支付帳戶之情形。
- 對不同使用者申請註冊，有身分證字號或行動電話號碼相同等異常情形，未進一步驗證合理性。

改善作法

- 應強化使用者身分確認機制，並落實遵循「電子支付機構使用者身分確認機制及交易限額管理辦法」規定，如：
  - 於使用者有疑似使用假名者，應拒絕其註冊之申請。
  - 對於已提供用於身分確認之同一行動電話號碼，遭不同使用者重複提供用於身分確認，且無法提出合理說明，得拒絕其註冊之申請。

業務項目：業務操作管理

缺失態樣

辦理未成年人註冊電子支付帳戶作業有欠妥適，不利保護未成年人使用者之權益。

缺失情節

- 受理未滿 20 歲未成年人開立電子支付帳戶，對未提供法定代理人同意書者，有未拒絕開戶之情形。
- 雖拒絕未滿 20 歲未成年人申請開立電子支付帳戶，並由系統檢核須年滿 20 歲始得開戶，惟程式檢核邏輯有誤，致有個人會員註冊時未滿 20 歲，而未拒絕其註冊申請之情形。

改善作法

- 應確實依本會 106 年 6 月 30 日金管銀票字第 10600143600 號函示，就受理未成年人註冊及開立電子支付帳戶作業，應遵循民法相關規定辦理，並明定業務規範(處理手冊)，適時檢討修訂。
- 應強化資訊系統程式邏輯正確性之驗證測試，及建立妥適之覆核機制，並落實執行。

業務項目：業務操作管理

缺失態樣

辦理風險管理作業有欠妥適，不利落實風險管控。

缺失情節

- 未對電子支付業務建立風險管理政策及程序，不利作業遵循。
- 雖有建立收款使用者風險評等機制，惟對新申請註冊之使用者，未依其風險等級核定交易額度；另對已開戶之使用者亦未定期辦理使用者風險評估。

改善作法

- 應依「電子支付機構內部控制及稽核制度實施辦法」第 33 條規定，訂定適當之風險管理政策及程序，建立獨立有效之風險管理機制，以評估及監督整體風險承擔能力、決定風險因應策略及風險管理程序遵循情形。
- 應依收款使用者之風險等級及實際需要核予交易額度，對風險等級較高之收款使用者，應採取限制交易金額、加強交易監測、實地訪視等措施，以降低交易風險。
- 應根據不同之風險等級，訂定收款使用者適當之調查、評估或實地訪視頻率，據以辦理使用者風險評估並留存相關紀錄。