金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

111 年度主要檢查缺失

-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

辦理使用者風險評估作業有欠妥適。

缺失情節

- 辦理使用者風險等級評估，所訂風險評估項目之設計欠妥，有未納入特定高風險因子項目(如：使用者或其實質受益人為現任國內外政府之重要政治性職務人士，或其國籍為「未採取有效防制洗錢或打擊資恐之高風險地區或國家」)，致高風險客戶評為中低風險等級。

改善作法

- 應訂定妥適風險評估方法，審慎考量各風險因子及其配分設計，確實反映客戶風險，以利進行定期或不定期之監控、查核與風險控管。

業務項目：防制洗錢、打擊資恐及反武擴作業

缺失態樣

辦理使用者帳戶或交易之持續監控作業有欠妥適。

缺失情節

- 辦理使用者帳戶或交易監控作業，未訂定相關監控政策及程序。
- 雖有以資訊系統輔助篩選異常交易，惟監控範圍欠完整或檢核條件欠妥適，致無法有效篩選出疑似不法或顯屬異常交易。

改善作法

- 應參照「電子支付機構防制洗錢及打擊資恐注意事項範本」第 9 條第 1 項第 4 款「電子支付機構之帳戶或交易監控政策及程序，至少應包括完整之監控型態、參數設定、金額門檻、預警案件與監控作業之執行程序與監控案件之檢視程序及申報標準，並將其書面化」規定辦理。
- 應參照「電子支付機構防制洗錢及打擊資恐注意事項範本」第 9 條第 1 項第 5 款附錄所列疑似洗錢或資恐態樣，確認各項業務之異常交易態樣均已納入監控範圍，並定期檢視資訊系統所訂檢核條件能有效辨識異常交易並產出警示報表。

業務項目：法令遵循

缺失態樣

法令遵循制度之運作有欠妥適。

缺失情節

- 法令遵循單位未對各單位法令遵循作業之成效加以考核，並將考核結果作為單位考評之依據。
- 法令遵循單位未對各單位人員辦理相關法規訓練。

改善作法

- 應參照「專營電子支付機構內部控制及稽核制度實施辦法」第 33 條第 1 項第 4 款「...對各單位法令遵循自行評估作業成效加以考核，經簽報總經理後，作為單位考評之參考依據」規定辦理。
- 應參照上開辦法第 33 條第 1 項第 5 款「對各單位人員施以適當合宜之法令規章訓練。」規定辦理。

業務項目：業務操作管理

缺失態樣

辦理委外作業有欠妥適。

缺失情節

- 作業委託他人處理，未依規報經本會核准或備查。
- 委外作業未訂定相關內部作業制度及程序。

改善作法

- 應參照「電子支付機構業務管理規則」第 45 條第 2 項「前項規定之委外事項範圍，除第 5 款、第 8 款及第 16 款之作業委外，應先報經主管機關核准外，其餘委外事項範圍，應於首次辦理後 5 個營業日內，報主管機關備查」規定辦理。
- 應參照「電子支付機構業務管理規則」第 45 條第 4 項第 1 款「就委託事項範圍、使用者權益保障、風險管理及內部控制原則，訂定內部作業制度及程序，並經董事會通過；修正時，亦同」規定辦理。

業務項目：個資保護

缺失態樣

對個人資料檔案之安全維護作業有欠妥適。

缺失情節

- 辦理個資盤點作業，部分部門及存有個資檔案之伺服器未納入清查，清查範圍欠完整。
- 員工可透過內部管理系統進行客戶資料查詢，惟未建立資料外洩防護機制。
- 辦理個資外洩演練作業，未就外部網路入侵及非法或異常使用行為所致個資外洩進行模擬，並就個資外洩後如何防止損害擴大及通知客戶等重要作業程序，納入定期演練及檢討改善。

改善作法

- 應參照「電子支付機構資訊系統標準及安全控管作業基準」第 13 條第 4 款「應針對電子支付作業環境，包含資料庫、資料檔案、報表、文件、傳檔伺服器及個人電腦等進行清查盤點是否含有個人資料並編製個人資料清冊，並進行風險評估與控管」規定辦理。
- 應參照「電子支付機構資訊系統標準及安全控管作業基準」第 13 條第 6 款「應建立資料外洩防護機制，管制個人資料檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁或網路檔案、或列印等方式傳輸，並應留存相關紀錄、軌跡與數位證據」規定辦理。
- 應加強研擬個資外洩模擬情境，並定期演練及檢討。

業務項目：資訊安全

缺失態樣

對主機系統帳號管理及清查作業欠妥。

缺失情節

- 特權帳號之使用管理欠妥，如：未建立最高權限帳號事前申請及事後覆核機制或未保留最高權限帳號使用紀錄。
- 未落實帳號權限清查作業，如：未列出帳號所擁有之權限並經使用者逐項確認、未刪除或停用已無使用需求之帳號。

改善作法

- 應落實特權帳號使用控管，並確實覆核及留存使用紀錄。
- 應落實辦理帳號權限定期清查作業，並刪除或停用已無使用需求之帳號，以維主機系統安全。

業務項目：資訊安全

缺失態樣

辦理防火牆規則檢視作業欠確實，且有防火牆規則設定欠妥情事，影響網路安全。

缺失情節

- 未規範防火牆檢視作業之重點原則項目，包括：6 個月內流量為零、高風險性網路通訊服務(如：檔案傳輸(FTP)、遠端登入(TELNET、RDP、SSH)、未加密連線(HTTP)等規則)。
- 防火牆規則設定過於寬鬆或控管欠嚴謹，如：來源端、目的端或服務埠設定為 ANY，未評估其安全性及必要性；及存有無業務需求之防火牆規則。

改善作法

- 應建立防火牆規則檢視作業之重點原則項目，依最小授權原則落實辦理防火牆規則設定作業，並刪除非必要連線服務，以確保網路安全。