金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

114 年度上半年主要檢查缺失

-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

辦理大額通貨申報作業欠妥。

缺失情節

- 辦理一定金額以上之通貨交易，有未於交易完成後5個營業日內向法務部調查局申報。

改善作法

- 應確實依「金融機構防制洗錢辦法」第13條之規定，對達一定金額以上之通貨交易，於交易完成後5個營業日內，向法務部調查局申報。

業務項目：業務操作管理

缺失態樣

辦理電子支付之業務操作有欠妥適。

缺失情節

- 辦理第二類電子支付帳戶儲值餘額有超逾限額 5 萬元之情事。
- 對與超過 3 家以上電子支付機構簽約之特約機構，尚未訂定無實益或風險特約機構之審核管控措施。

改善作法

- 應確實依「電子支付機構身分確認機制及交易限額管理辦法」第 20 條第 1 項規定，落實執行電子支付帳戶之儲值餘額控管作業。
- 應落實「電子支付機構業務自律規範」第 22 條規定，對於申請超過 3 家以上電子支付機構或特約機構負責人申請自然人特約機構，應審慎審核，以避免簽訂無實益或風險特約機構之情事。

業務項目：資訊安全

缺失態樣

行動裝置應用程式(APP)安全控管欠妥。

缺失情節

- APP 未送合格實驗室依「行動應用 APP 基本資安檢測基準」辦理檢測。
- 啟動 APP 時，有未偵測行動裝置疑似遭破解(開啟 USB debugging 及 Root)，並對使用者進行資安風險提示及限制辦理國內外小額匯兌服務。
- APP 有未設計限制同一帳號在同一時間內僅能登入一個連線(session)控制之系統安全設計。

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 8 條及第 11 條規定，檢討行動應用程式 APP 安全控管及檢測作業之妥適性，以維交易安全與客戶權益。

業務項目：資訊安全

缺失態樣

辦理防火牆管理作業有欠妥適。

缺失情節

- 辦公室防火牆及網頁應用程式防火牆(WAF)之特權帳號由個人所持有，尚未納入特權帳號管理系統或封存密碼控管。
- 未建立 WAF 版本更新管控機制，對原廠公布應辦理更新之版本未予查明列管，並評估辦理更新之必要性。
- 辦理防火牆規則定期檢視作業欠確實，未對遠端登入(RDP、SSH 及 TELNET)、未加密連線(HTTP)、網路芳鄰(SMB)、未加密檔案傳輸(FTP)、資料庫存取(MS SQL)等高風險連線服務項目辦理檢視作業。

改善作法

- 應強化防火牆及 WAF 特權帳號之管控，並落實防火牆規則定期檢視作業，以確保網路安全。