



金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

115 年度上半年主要檢查缺失

-專營電子支付機構

目 次

防制洗錢、打擊資恐及反武擴作業	1
個人資料保護	2
業務操作管理	3
資訊安全	4

☑ 業務項目：防制洗錢、打擊資恐及反武擴作業



缺
態

失
樣

辦理警示電子支付帳戶之通報作業欠妥適。

缺
失
情
節

- 受理警察機關通報警示電子支付帳戶，未於接獲通報時立即將資料通知財團法人金融聯合徵信中心。

改
善
作
法

- 應依「電子支付機構業務管理規則」第 35 條第 1 款第 2 目規定，對經法院、檢察署或司法警察機關通報之警示電子支付帳戶，立即通知財團法人金融聯合徵信中心，以利其他金融機構即時掌握警示帳戶資訊及對後續產生之衍生管制帳戶採取處理措施。

☑ 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

- 辦理個資外洩演練作業之模擬情境均相同，且未將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，並就個資外洩後之因應措施納入定期演練及檢討改善。

改善
作法

- 應依「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第 10 條第 3 項規定，加強研擬個資外洩模擬情境，並定期演練及檢討改善。

☀ 業務項目：業務操作管理



缺
失
情
態

辦理特約機構之交易限額控管作業欠妥適。

缺
失
情
節

- 對開立多個電子支付帳戶之特約機構未歸戶控管，致合計每月交易收款限額有逾該特約機構最高帳戶類別之金額。

改
善
作
法

- 應依「電子支付機構身分確認機制及交易限額管理辦法」第 21 條及第 22 條規定，對同一使用者於同一電子支付機構開立一個以上之電子支付帳戶，各帳戶收款及付款金額不得超過該帳戶類別之限額，歸戶後總限額不得超過該帳戶中最高類別之限額。



✓業務項目：資訊安全

缺
態
樣

防火牆規則檢視作業及設定欠妥適。

缺
失
情
節

- 防火牆規則檢視作業欠妥善，如：對採用高風險連線服務之防火牆規則未評估敘明保留之必要性、對 6 個月以上無流量之防火牆規則未檢視，或有已下線主機未及時調整防火牆規則。
- 防火牆規則或安全設定欠妥，如：未限縮來源端、目的端主機及可使用之網路服務，允許所有 IP 以任意服務連線至所有 Server(來源及目的地均設定為 any/all)。

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 4 款及第 5 款規定，落實辦理防火牆規則檢視作業及審視防火牆參數設定作業之妥適性，以確保網路安全。



✓業務項目：資訊安全

缺
態
失
樣

行動應用程式(APP)管理作業欠妥適。

缺
失
情
節

- 辦理行動應用程式 APP 基本資安檢測欠完整，如：僅針對 Android 版辦理 OWASP Mobile Application Security Checklist L2，未檢測 iOS 版。
- APP 程式交付未建立來源辨識性(如 ZIP)及完整性(如 MD5)驗證機制。
- 行動應用程式 APP 之參數設定允許資料以明文於網路通訊。

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 11 條第 4 款第 7 目規定，督導受託廠商落實辦理 APP 檢測，建立程式交付確認機制，並檢討行動應用程式相關參數設定，以維護行動應用程式安全。