



金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

113 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	3
業務操作管理	4
資訊安全	5



✓ 業務項目：防制洗錢、打擊資恐及反武擴作業

缺失
態樣

對電子支付帳戶使用者未落實身分驗證程序及所留存紀錄欠妥適。

缺失
情節

- 對尚未依規於調整期內完成身分驗證程序之電子支付帳戶使用者，仍有進行代理收付實質交易之情事。
- 受理外籍客戶電子支付帳戶註冊時，雖有徵提居留證正反面照片影像檔，惟經查有留存影像檔非屬可供辨識之有效證件。

改善
作法

- 應就未完成身分確認之使用者，限制不得建立業務關係或進行臨時性交易，以符合「電子支付機構身分確認機制及交易限額管理辦法」及「金融機構防制洗錢辦法」規定。
- 應落實電子支付帳戶使用者註冊之身分確認作業，並依規定保存身分證明文件影本、影像檔或相關紀錄。



業務項目：防制洗錢、打擊資恐及反武擴作業

缺失
態樣

受理檢警調單位函調或聯防機制通報作業欠妥適，及對疑似不法顯屬異常電子支付帳戶控管作業欠確實。

缺失
情節

- 於接獲前一受款機構傳真聯防機制通報單時，未儘速查證並將該受款電子支付帳戶金額圈存。
- 經司法警察機關通報之警示電子支付帳戶，有未經原機關再行通報即逕予解除。
- 設定疑似不法顯屬異常交易情境檢核條件不足，不利辨識異常交易帳戶並採取後續處理措施。

改善
作法

- 應確實依「金融機構辦理警示帳戶聯防機制作業程序」規定，於接獲聯防機制通報單時，應儘速查證並辦理圈存。
- 警示電子支付帳戶應依原通報機關之通報，或警示期限屆滿，方得解除電子支付帳戶之限制。
- 應檢視疑似不法顯屬異常電子支付帳戶之交易監控情境條件之完整性，以確保異常交易監控機制之有效性。



✶業務項目：個人資料保護

缺
失
態
樣

資料外洩防護機制及留存紀錄欠完善。

缺
失
情
節

- 資料外洩防護(DLP)過濾規則設定欠妥，且實測發現 DLP 未阻擋電子郵件傳送多筆個資並留存紀錄；另對特定副檔名檔案(如：jpg 圖檔)尚未建立過濾阻擋機制，不利客戶個資保護。
- 尚未建立資料外洩防護偵測機制，且對寫出檔案至 USB 者未予記錄；另尚未建立於網頁(如：雲端硬碟及留言板等)上傳個資相關偵測機制並予以記錄之機制。

改
善
作
法

- 應建立資料外洩防護偵測機制，並適時檢討過濾規則之妥適性，以確保客戶個資安全。
- 應依「電子支付機構資訊系統標準及安全控管作業基準」規定，建置留存個人資料使用稽核軌跡，以利追蹤客戶個人資料使用狀況。

☑ 業務項目：業務操作管理



缺
態
樣

未經本會許可逕行辦理電子支付附隨及衍生業務項目。

缺
失
情
節

- 辦理電子支付附隨及衍生業務，尚未依規定於開辦前向本會申請許可即逕行辦理。

改
善
作
法

- 應於首次開辦「電子支付機構管理條例」第4條第2項第5款及第6款規定之業務前，檢具營業計畫書向本會申請許可。

業務項目：資訊安全



缺
失
態
樣

使用者帳號權限盤點作業及特權帳號管理機制欠妥適。

缺
失
情
節

- 尚未建立定期盤點及審查各主機、應用系統、資料庫等使用者帳號及權限機制，以確保帳號使用之合法性與符合最小權限原則。
- 對特權帳號之使用，未建立使用結束立即變更密碼並覆核相關作業軌跡之機制，不利主機系統安全。
- 對經由網際網路連接至內部伺服器，以特權帳號進行遠距系統管理工作，雖有側錄留存操作紀錄，惟未定期覆核作業軌跡。

改
善
作
法

- 應建立定期盤點帳號權限機制，以符合最小權限原則。
- 應請重新檢討特權帳號申請及控管措施，落實帳號權限控管作業並建立作業軌跡覆核機制，以維系統安全。