金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

112 年度主要檢查缺失

-專營電子支付機構

目　　次

金管會檢查局

業務項目：防制洗錢、打擊資恐及反武擴作業

缺失態樣

辦理檢警調單位函調或聯防機制通報作業有欠妥適。

缺失情節

- 受理檢警調單位函調或銀行聯防機制通報，尚未訂定後續處理措施，不利防制詐騙。
- 未於接獲前一受款機構傳真聯防機制通報單時，立即查詢受款電支帳戶交易，並將移轉資料傳真通報下一受款機構之通報窗口，不利後續通報之時效性。

改善作法

- 應請建立受理檢警調單位函調或聯防機制通報作業之後續處理機制。
- 應參照「電子支付機構辦理警示電子支付帳戶聯防機制及衍生管制作業程序」第 2 點第 1 項第 2 款規定，電支機構通報窗口在接獲前一受款機構傳真之通報單，應立即查詢受款電支帳戶之交易，如款項已遭移轉，則接續填寫前一受款機構傳真之通報單，將移轉資料傳真通報下一受款機構之通報窗口。

業務項目：業務操作管理

缺失態樣

辦理特約機構徵審及風險評估作業，有欠妥適。

缺失情節

- 對經審核通過之特約機構，系統未建置覆核功能，致未留存完整之徵審作業軌跡。
- 對屬相同產業之特約機構，風險等級有不一致情形，未檢視評分模型與參數之合理性，不利落實風險控管措施。
- 對於特約機構提供商品較特殊者或允許消費者退貨天數較長者，尚未就結算天數建立一致標準，以降低交易風險。

改善作法

- 應參照「電子支付機構業務管理規則」第 6 條第 1 項規定，建立特約機構之徵信審核機制及流程。
- 應請確實檢視評分模型與參數之合理性，相同產業之風險等級應採一致性之風險控管措施。
- 應參照「電子支付機構業務管理規則」第 4 條規定，電子支付機構應依特約機構類型、交易金額、交易模式、遞延性商品或服務及銷售商品之風險性，建立特約機構徵信審核、風險控管……相關管理機制。

業務項目：個人資料保護

缺失態樣

辦理個人資料保護作業，有欠妥適。

缺失情節

- 測試資料庫有存放客戶機敏資料，尚未進行資料遮罩或相關管制保護作業。
- 外寄電子郵件控管程序欠妥，如：對夾帶含有個資附件之電子郵件僅將附件加密後即予外寄，未建立事前阻擋機制；對外寄圖形檔及加密檔等特殊型態檔案，未建立偵測攔阻機制。

改善作法

- 應確認測試用之機敏資料已進行遮罩或去識別化。
- 應強化外寄電子郵件控管程序，以確保個資安全。

業務項目：資訊安全

缺失態樣

辦理行動裝置應用程式(APP)變更管理作業，有欠妥適。

缺失情節

- 變更作業未依規辦理，如：
  - 具小額匯兌功能之行動裝置應用程式，於上版前未依據 OWASP Mobile Top 10 項目辦理檢測。
  - 未於發布前檢視應用程式所需權限是否與其提供之服務相當。
  - 上架發布作業未由 2 人以上或採 2 項以上技術辦理。
- 行動裝置應用程式引用第三方函式庫，相關作業有欠妥者，如：
  - 未建立函式庫清單及辦理風險評估逕予引用。
  - 有使用存在有風險漏洞之程式套件。

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」研訂行動裝置應用程式變更上架前相關資安檢測、權限檢視及發布作業程序，並落實辦理。
- 應對所引用第三方函式庫建立清單及訂定相關風險評估與檢測程序，以維資訊安全。

業務項目：資訊安全

缺失態樣

辦理對外服務網站相關管理作業，有欠妥適。

缺失情節

- 未建立對外服務網站網頁防竄改機制或納管範圍欠完整，致未於偵測網頁與程式異動時，進行記錄與通知措施。
- 對使用者採用固定密碼進行身分確認者，尚未建立端點對端點加密機制。
- 網站設計未採用安全標頭，如：Content-Security-Policy、Referrer-Policy、Strict-Transport-Security、X-Frame-Options、X-Content-Type-Options。

改善作法

- 應建立對外服務網站相關安全控管機制，檢視對外服務網站設計之妥適性，以確保網頁安全及降低駭客攻擊風險。