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

-本國銀行

目　　次

防制洗錢、打擊資恐及反武擴作業……1
法令遵循……3
消費者保護……4
個人資料保護……7
轉投資事業管理……8
授信業務……9
數位金融……12
內部管理……13
資訊安全……14

業務項目：防制洗錢、打擊資恐及反武擴作業

缺失態樣

未確實辦理網路借貸平台業者(P2P)之客戶審查作業。

缺失情節

- 對存款客戶為網路借貸平台業者(P2P)，未依風險基礎方法(RBA)規劃辨識審查、風險控管及持續監控機制，藉以評估 P2P 業者之洗錢及資恐風險。

改善作法

- 辦理網路借貸平台業者(P2P)之辨識審查、風險控管及持續監控機制，確實考量客戶背景、職業及社會經濟活動特性，以評估其洗錢風險；對客戶業務關係中之交易，詳細審視各項交易與客戶業務及風險是否相符；並建立風險管控措施，定期辦理審查及對異常交易之檢核與調查。

業務項目：防制洗錢、打擊資恐及反武擴作業

缺失態樣

未落實對異常交易之監控與查證作業。

缺失情節

- 雖有以資訊系統輔助清查存款帳戶之異常交易，惟未設定異常交易情境以為檢核，或檢核參數設計有欠妥適，致未能有效及時發現疑似不法或顯屬異常交易。
- 對持續觸及異常交易態樣預警指標之存款帳戶，未加強檢視客戶身分背景與帳戶交易模式是否相稱，並通報總行進行後續交易監控或管制，致事後遭通報為警示帳戶或衍生管制帳戶。

改善作法

- 應檢視異常交易態樣之檢核條件與參數設定之妥適性，落實異常交易查證及申報作業，以防杜詐騙集團利用人頭帳戶進行洗錢交易。

業務項目：法令遵循

缺失態樣

法令遵循作業有欠妥適。

缺失情節

- 未配合金融法規增修，確實檢視相關作業規範符合法令要求。
- 未落實督導國外營業單位確實遵循當地金融法規，致該營業單位未能確認內部管理規章是否與當地國更新之法規相符。

改善作法

- 應依「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 34 條第 1 項規定，確認各項作業及管理規章均配合相關法規適時更新，使各項營運活動符合法令規定。
- 應依上開辦法第 34 條第 3 項規定，督導國外營業單位強化法令遵循功能，以確保遵守其所在地國家之法令。

業務項目：消費者保護

缺失態樣

對高齡客戶權益保障作業有待強化。

缺失情節

- 對高齡客戶銷售投資型保險商品，未研議將常見保險招攬爭議類型(如：未告知不保本、非存款商品或體況加費因素於投資虧損時導致保單帳戶價值產生較大變化等)納入錄音問卷問項。

改善作法

- 應落實遵循本會 107 年 11 月 19 日金管保壽字第 10704548390 號及 108 年 11 月 8 日金管保壽字第 10804358671 號函之規定，自行檢視內部常見爭議類型納入錄音問卷問項，以減少事後爭議。

業務項目：消費者保護

缺失態樣

辦理金融消費者對保險商品適合度確認作業有欠妥適。

缺失情節

- 對保險公司照會業務員(理財專員)招攬疑義之案件，僅由與自身利害關係之業務員一人簽章回覆，未有主管審核確認機制，不利確認金融消費者對保險商品之適合度及瞭解業務員是否據實填寫招攬報告書。

改善作法

- 應就保險公司照會案件建立照會審核確認機制，落實遵循「保險代理人管理規則」第 49 條第 24 款及第 29 款規定，確認金融消費者對保險商品之適合度，並據實填寫招攬報告書。

業務項目：消費者保護

缺失態樣

辦理預售屋不動產開發信託及價金信託作業有欠妥適。

缺失情節

- 未留存賣方交付信託價金明細之日期資料及核對紀錄，不利確認賣方是否依信託契約約定期限將買方所繳價金交付信託。
- 對於賣方未將買方所繳價金於收訖之次一營業日交付信託，未以書面限期催告賣方將不足金額補足。

改善作法

- 應依「中華民國信託業商業同業公會會員辦理預售屋『不動產開發信託』與『價金信託』業務應行注意事項」第 6 條第 1 項規定，落實執行與賣方就買方所繳價金交付信託之約定事項。
- 應落實上開應行注意事項第 8 條第 2 項及第 3 項規定，於發現應交付信託款項有金額、日期不符或未依約提供、遲延交付等情形，應即書面限期催告賣方提出說明或將不足金額補足或要求改善，以保護消費者權益。

業務項目：個人資料保護

缺失態樣

辦理電話行銷業務之個人資料保護作業欠妥適。

缺失情節

- 與人壽保險公司合作辦理電話行銷作業，所傳遞之電子檔案有提供客戶之其他非必要個人資料。

改善作法

- 提供客戶個人資料應檢視內容之妥適性，避免提供不必要之資訊；個人資料檔案對外傳輸時，應適當遮蔽，俾利落實個人資料之保護作業。

業務項目：轉投資事業管理

缺失態樣

對轉投資事業之管理作業待加強。

缺失情節

- 對子公司向關係人取得不動產使用權資產，母公司未依規定辦理公告。
- 對派任子公司之董監事，未訂定績效考核辦法，以評估派任人員之經營績效及適格性，且簽報派任名單亦未評估說明現任董監事參與董事會及監督業務等情形，對轉投資事業之管理欠積極。
- 融資性租賃子公司承作融資性租賃業務比重過低，雖已陳報改善計畫，擬逐年提高融資性租賃業務比重，惟未能如期完成改善。

改善作法

- 應依「公開發行公司取得或處分資產處理準則」第 31 條第 1 項及第 34 條第 1 項規定，公開發行公司向關係人取得或處分不動產或其使用權資產，應於事實發生之即日起算二日內將相關資訊於本會指定網站辦理公告申報；公開發行公司之子公司非屬國內公開發行公司，取得或處分資產有前開應公告申報情事者，由公開發行公司為之。
- 對派任轉投資事業之董事及監察人，應訂定績效考核辦法，並落實執行；另對子公司擬具之改善計畫，應切實督導子公司辦理相關改善作業及追蹤執行進度，以確保如期完成改善計畫。

業務項目：授信業務

缺失態樣

辦理利害關係人授信案件有欠妥適。

缺失情節

- 對屬金控母公司利害關係人之變更授信條件案件，未報經董事會三分之二以上董事之出席及出席董事四分之三以上同意。

改善作法

- 應落實金融控股公司法第 44 條及銀行法第 33 條第 1 項後段之規定，檢討利害關係人授信條件變更案件之審核機制。

業務項目：授信業務

缺失態樣

防杜人頭帳戶申辦貸款之措施有欠周延。

缺失情節

- 辦理線上個人信用貸款之徵信審查作業，對不同客戶利用相同 IP 位址申請貸款者，未審慎分析其合理性，不利防杜人頭帳戶申辦貸款。

改善作法

- 應建立不同客戶使用同一 IP 申辦貸款之檢核機制，以防杜人頭帳戶申辦貸款。

業務項目：授信業務

缺失態樣

未審慎辦理銀行法第 72 條之 2 住宅建築及企業建築放款之限額控管。

缺失情節

- 辦理銀行法第 72 條之 2 住宅建築及企業建築放款之限額控管，有未納入統計者：
  - 對實際資金用途為購置擬辦理都市更新或危險及老舊建物加速重建之不動產，有因故未取得縣(市)主管機關核准者，而未納入銀行法第 72 條之 2 統計範圍。
  - 對借戶購置不動產興建住宅建築或企業建築之放款，有以所徵持分土地尚待整合為由，即排除列入銀行法第 72 條之 2 限額控管。
  - 核予鉅額營運週轉金，未確認最終資金用途，即全數排除列入銀行法第 72 條之 2 限額控管。

改善作法

- 應確實依本會 110 年 12 月 1 日金管銀法字第 1100272811 號函規定，加強借款用途調查及貸後資金流向追蹤，俾利控管銀行法第 72 條之 2 之限額。

業務項目：數位金融

缺失態樣

未確實遵循「金融機構辦理電子銀行業務安全控管作業基準」規定。

缺失情節

- 對客戶線上申辦信用卡，未建立不得以簽帳金融卡進行身分核驗之機制。
- 對客戶以手機 APP 開啟非約定轉帳功能之安全設計，僅以簡訊一次性密碼(OTP)作為身分驗證，或對客戶透過網路銀行辦理非約定轉帳交易，選擇以簡訊傳送 OTP 之安全設計時，未有加強防護機制。

改善作法

- 應依「金融機構辦理電子銀行業務安全控管作業基準」第 7 條第 9 款規定，驗證他行信用卡有效性時，應透過聯合信用卡處理中心及財金公司之「信用卡輔助持卡人身分驗證平臺」辦理。
- 應依上開作業基準第 8 條第 3 款第 1 目第 3 子目規定，受理已開戶之客戶辦理申請網路銀行或晶片金融卡之非約定轉帳功能應採用第 7 條第 1 款第 1 目、第 2 款至第 5 款任一安全設計進行身分確認，惟排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計；另依第 7 條第 3 款第 2 目第 3 子目規定，採用簡訊傳送一次性密碼並應用於非約定轉入帳戶轉帳交易者，應加強防護機制。

業務項目：內部管理

缺失態樣

對作業系統及公用電腦之使用安全作業有待強化。

缺失情節

- 國外營業單位辦理作業系統使用者權限管理作業，未即時移除調職人員系統權限，或未依據職務工作項目設定相稱操作權限。
- 分行營業廳公用電腦下載區有留存客戶使用後未刪除之個人資料，易遭他人不當存取使用。

改善作法

- 應確實依據職務需求設定系統權限，並落實系統權限及密碼之變更控管作業，以符內控牽制原則及資訊安全。
- 應研議改善客戶使用公用電腦未刪除之個人資料控管機制，落實客戶資料保護。

業務項目：資訊安全

缺失態樣

對外服務網站安全設計機制欠妥。

缺失情節

- 未採用 Referrer-Policy 保護資訊避免洩漏、Permissions-Policy 管控特定應用程式介面(API)或瀏覽器功能、Content-Security-Policy 防禦跨網站指令攻擊、X-Frame-Options 防禦點擊劫持攻擊、X-Content-Type-Options 避免瀏覽器誤判文件格式、Strict-Transport-Security 強化網頁瀏覽機制等安全標頭(Headers)。
- 使用不安全第三方 Javascript 函式庫，未評估更新或採補償性控管措施。
- 接受不安全加密方式，可能導致攻擊者進行中間人攻擊，解密網站伺服器與使用者間的通訊，如：不支援 Forward Secrecy、Secure Renegotiation 保密功能、接受弱式 Diffie-Hellman 公開金鑰值或弱加密方式等。

改善作法

- 應檢討對外服務網站安全設計機制，強化網頁安全標頭設計，以確保網頁安全及降低駭客攻擊風險。

業務項目：資訊安全

缺失態樣

重要網路設備之韌體及作業系統版本具風險漏洞，且參數設定欠妥。

缺失情節

- 對原廠已公告停止提供系統更新(EOS)或現行版本具風險漏洞之防火牆，未妥適評估設備汰換或系統版本更新。
- 未辦理參數定期檢視作業，且有參數設定欠妥，如：未啟用密碼政策、未開啟日誌紀錄、未停用無需使用之通訊埠或服務、採用不安全加密或認證機制等。

改善作法

- 應確實辦理網路設備作業系統更新評估作業，並定期執行安全參數設定檢核作業，以維網路安全。

業務項目：資訊安全

缺失態樣

應用程式介面(API)管理作業欠妥。

缺失情節

- 未建立 API 定期盤點機制，並依據 API 存取資料之重要性、存取行為(如：POST、GET 等)、頻率及資料量等，訂定 API 分類分級與管理規範。
- 未限制可存取來源，且未定義對外服務 API 異常(如:短時間超過流量上限或持續無流量)告警指標、事件通知處理流程及日誌留存與管理方式。
- 認證授權過程中有傳輸含個資或機敏資料欄位，未建立加密等保護機制。
- 未建立金鑰(API Key)管控規範，如：金鑰產製人員、交付控管機制、使用期限及定期更換機制。

改善作法

- 應檢討API盤點及各項管理機制，就對外服務API所傳輸含有個資或交易機敏資料之欄位建立防護措施，以維資料安全。