

# 金融機構辦理多功能視訊櫃檯(Video Teller Machine) 作業自律規範

本會 112 年 6 月 29 日第 14 屆第 8 次理監事聯席會議通過  
金管會 113 年 1 月 29 日金管銀國字第 1120224870 號函修正後備查

## 第一條（訂定目的及原則）

- 一、中華民國銀行商業同業公會全國聯合會（以下簡稱本會）為協助金融機構辦理多功能視訊櫃檯（Video Teller Machine；以下簡稱 VTM）業務及確保 VTM 相關安全控管具有一致性之作業標準，特訂定本自律規範。
- 二、金融機構設置 VTM 並透過 VTM 提供金融服務，除應遵循相關法令外，悉依本自律規範辦理。

## 第二條（名詞定義）

本自律規範所稱 VTM 係指由一般具有視訊、掃描及證件之辨識模組、具有後台人員進行真人、本人認證，並可觀察客戶簽章及周邊之環境監控模組、24 小時保全及直接連結金融機構內部網路之設備。

## 第三條（可辦理業務項目）

客戶利用 VTM 可辦理之業務項目，區分為帳務交易類、申請指示類及查詢類。

一、帳務交易類：現金存提款、轉帳、匯款、繳費、付款指示、投資相關等。

二、申請指示類：

（一）存款業務：開立新臺幣、外幣活期、定期存款帳戶暨新臺幣支票存款帳戶、申請銷戶、非約定轉帳、約定轉入帳號、申請各類證明書、晶片金融卡及網路/行動銀行相關申請等。

（二）授信業務：申請個人貸款、增貸原抵押權擔保範圍內之

房貸及車貸、申請授信條件變更、同意授權查詢財團法人金融聯合徵信中心個人信用資料等。

(三) 財富管理業務：認識客戶作業(KYC)、客戶風險承受度測驗、同意結構型商品業務之推介或終止推介等。

(四) 其他：同意及停止共同行銷、申請變更個人資料。

三、涉及帳務類之查詢項目。

#### 第四條 (辦理業務應遵循之要求)

透過 VTM 辦理之業務項目應遵循下列要求，如有提供自動櫃員機業務項目應遵循自動櫃員機相關規範辦理：

- 一、依本自律規範第三條所涉業務項目之臨櫃相關業務作業規定辦理。
- 二、限具本國國籍成年自然人親自辦理。
- 三、開立活期、定期及支票存款帳戶之帳號，應有相關區別機制，且開戶初期需有別於一般臨櫃開戶帳戶之管控方式（如交易功能、金額）。
- 四、應由金融機構與客戶確認其身分與交易或指示內容，並即時檢核客戶是否為高風險客戶，俾引導至臨櫃辦理。
- 五、相關業務書件應由客戶簽名或蓋原留印鑑，客戶簽署之文件如委外運送應依「金融機構作業委託他人處理內部作業制度及程序辦法」第三條第一項第十八款辦理。
- 六、過程應進行錄音及錄影，並至少留存六個月，其他交易文件保存期限則依各業務相關規範辦理。
- 七、提供蒐集、處理及利用個人資料告知事項內容，供客戶審閱及確認等功能，並具備檢核機制。
- 八、帳戶交易持續加強各項疑似洗錢或資恐交易表徵之監控。

#### 第五條 (設置地點及機台環境面之安全需求)

VTM 設置地點及機台環境面之安全需求，應遵循下列要求：

一、設置地點：

- (一) 如於營業場所內設置 VTM，須由法令遵循主管出具法令遵循聲明書，確認該項營運活動符合法令及內部規範後辦理。
- (二) 如於營業場所外設置 VTM，除依前款程序辦理外，應於事前將擬設置 VTM 之相關資料，包括設置地址、啟用日期、台數等函報金融監督管理委員會；設置後如有遷移或裁撤等異動情形亦同。

二、建立安全防護策略：

- (一) 若提供現金提存功能者，其安全防護應依「金融機構自動櫃員機安全防護準則」第參點第五項暨「中華民國銀行公會會員安全維護作業規範範本」第拾點第二項第三款及第四款辦理。
- (二) 機台環境面之安全需求，應依「金融機構自動櫃員機安全防護準則」第參點及「中華民國銀行公會會員安全維護作業規範範本」第拾點第二項第三款辦理。

三、提高系統可靠性之措施：警示通報系統及監視系統應分別依「金融機構安全維護管理辦法」第六條第三款及「中華民國銀行公會會員安全維護作業規範範本」第拾點第二項第三款辦理。

第六條（端末設備面之安全設計）

VTM 端末設備面之安全設計，應遵循下列要求：

- 一、金庫（如提供現金提存功能者）、鍵盤、讀卡機及處理卡片交易時，應比照「金融機構辦理電子銀行業務安全控管作業基準」自動櫃員機之安全設計及「金融機構提供自動櫃員機系統安全作業規範」。
- 二、應具備確認客戶本人申辦業務之舉證能力及方法（如照片、影像或聲音），並留存驗證紀錄與交易軌跡，遇有爭議時則

可調閱相關紀錄。

- 三、應具備國民身分證辨識要項之模組，其中國民身分證辨識模組應能檢視防偽特徵，惟排除手觸（壓凸觸摸圖形）及翻轉（折光變色油墨）兩項防偽設計，並可參考其他輔助項目檢核。
- 四、應能檢視環境，並提供即時檢視現場影像及收音，輔助後台人員觀察有無異常舉止或遭脅迫。
- 五、應直接連結金融機構內部網路並建置必要防護措施（如防火牆、防毒偵測、入侵偵測等），並關閉不必要服務。
- 六、如產製或存取晶片金融卡或簽帳金融卡，應符合卡片發卡、個人化或金鑰管理，其金鑰應儲存於經第三方認證（如 FIPS 140-2 Level 3 以上）之硬體安全模組，並應具備卡片沒收裝置；如放置於無人看管處應增加保全 24 小時監控。

#### 第七條（核定程序）

本自律規範經本會理事會通過並報經金融監督管理委員會備查後施行；修正時，亦同。