金融機構提供 QR Code 掃描支付應用安全控管規範摘要說明

壹、 本規範用詞定義如下：

一、 QR Code：係二維條碼的一種，為矩陣式黑白相間的點狀或條狀圖形，除能表示文字、圖形及聲音等資訊，尚有容量大、可靠性高及資料完整性等特性。

二、 QR Code 受理終端：指參與 QR Code 條碼解析與生成之終端裝置，包含但不限於行動、POS 及自動化服務設備等裝置，並依照 QR Code 資訊以進行相關交易作業。

三、 消費商店：指提供商品販售或服務等場所，採 QR Code 支付技術向客戶收取商品或服務費用，簡稱商店。

四、 QR Code 處理平臺：QR Code 之管理平臺，提供 QR Code 條碼解析與生成、重要資料之加解密、加解密系統金鑰管理及交易訊息處理等功能。

五、 主掃模式：金融機構、商店、收款機構或收款客戶生成交易之 QR Code，付款客戶持行動裝置應用程式掃描以確認交易，傳輸至 QR Code 處理平臺或其他支付系統，完成支付交易。

六、 被掃模式：付款客戶持行動裝置應用程式生成 QR Code，提供商店或收款客戶掃描後，傳輸至 QR Code 處理平臺或其他支付系統，完成支付交易。

七、 交易資訊類：係指該 QR Code 用於取代人工輸入之行為，該 QR Code 被掃描後，掃描之處理端應用程式顯示相關資訊，經使用者檢視 QR Code 內容後，由客戶另啟動交易指示者。

八、 交易指示類:係指該 QR Code 被 QR Code 受理終端掃描解析後，應用程式依所含指示內容進行交易，涉及資金轉移或直接影響客戶及商店權益者。

貳、 QR Code 掃描支付過程中，所存取之資訊應遵循該業務所需最小化原則。

參、 採用交易資訊類 QR Code 者，應用程式應以彈出式視窗或其他方式提供接收方檢視 QR Code 之資料內容，再由接收方處理後續事宜。

肆、 被掃模式採用交易指示類 QR Code 者，因係屬使用者產生授權資訊同意扣款性質，應設定 QR Code 合理使用時效，且在時效內以使用一次為限。

伍、 QR Code 受理終端所提交之 QR Code 訊息請求應進行檢查。

陸、 QR Code 受理終端相關應用程式，應能針對所解析之 QR Code 進行檢查。

柒、 QR Code 受理終端相關應用程式，應能針對所解析之交易指示類 QR Code 進行檢查，對於未驗證通過之 QR Code 應予明確提示並拒絕執行交易。

捌、 QR Code 受理終端相關應用程式，對所解析之 QR Code 產生網站連結，應進行檢查。

玖、 主掃模式及被掃模式等各類應用情境，所生成之交易指示類 QR Code 收付不得共用。