本會106年7月27日第12屆第9次理監事聯席會議討論通過
金管會106 年8月30日金管銀國字第10600201710號函洽悉

金融機構提供QR Code掃描支付應用安全控管規範

第一條　中華民國銀行商業同業公會全國聯合會（以下簡稱本會）為確保金融機構提供QR Code（Quick Response Code）掃描支付應用具有一致性之安全控管作業，俾於國內建立方便及安全之QR Code支付環境，特訂定本規範。

第二條　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。

第三條　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。

第四條　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。

第五條　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。

第六條　QR Code 受理終端所提交之 QR Code 訊息請求應確保傳輸過程中的資訊完整性及隱密性，並確保在傳輸過程中不被篡改及洩露。

第七條　QR Code 受理終端相關應用程式，應能針對所解析之 QR Code 進行格式檢查，確保資料格式合理性，預防程式碼注入。

第八條　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 進行來源辨識性及完整性檢查，對於未驗證通過之 QR Code 應予明確提示並拒絕執行交易。

第九條　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，應採包括但不限於白名單或伺服器認證等機制進行網站合法性檢查，以預防連結惡意網站或執行惡意程式風險。

第十條　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，以確保專碼專用。

第十一條　本規範經本會理事會通過並函報金融監督管理委員會核備後實施，修正時亦同。