立法院第 10 屆第 1 會期

財政委員會第 16 次全體委員會議

「我國推動行動支付的相關規範與面臨可能資訊安全風險的因應機制」專題報告

中央銀行

109 年 5 月 14 日

主席、各位委員、各位女士、先生：

今天承邀前來貴委員會報告，至感榮幸。

以下謹就財金資訊股份有限公司(簡稱財金公司)協同金融機構制定「QR Code 共通支付標準」的緣由、成效、適用的相關規範及可能面臨資訊安全風險的因應機制，提出報告，敬請惠賜指教。

財金公司係依銀行法第 47 條之 3 設立，經營金融機構間資金移轉帳務清算的金融資訊服務事業，旨在促進金融業的資源共享、資訊互通，以及提升金融體系全面自動化服務；其擔任全國金融資訊與跨行交易處理的樞紐角色，處理金融機構間跨行交易訊息轉接業務，提供社會大眾安全、便利的金流服務，包括跨行 ATM 提款轉帳、大眾匯款、全國繳費稅及企業撥款等各項支付交易，為國內關鍵金融基礎設施之一。

壹、制定 QR Code 共通支付標準的緣由

一、國內電子支付工具多元

我國電子支付工具發展多元，包括信用卡、金融卡

及悠遊卡、一卡通等電子票證(表 1)，這些支付工具經由完善的金融基礎設施，提供大眾便利的電子支付服務，例如繳費、繳稅、轉帳及購物消費等。2019 年全年使用電子支付工具消費的金額合計 4.27 兆元，較上(2018)年 3.81 兆元增加 12%。

表 1、我國電子支付工具流通概況

項目	流通卡數	每人平均持有卡數
金融卡	10,701 萬	約 4.53 張金融卡
信用卡	4,803 萬	約 2.03 張信用卡
電子票證	12,902 萬	約 5.47 張電子票證

資料來源：金管會、內政部(統計至 2020 年 2 月資料)

二、推動行動支付為國家重要政策

近年，因應數位科技及行動商務的發展，透過行動載具結合各類電子支付工具的行動支付隨之興起，行政院爰於 2017 年將行動支付發展列為重要政策之一，並推動 2025 年行動支付普及率達 90%目標。

惟因國內行動支付 QR Code 規格互異、無法互通，個別商家與個別支付業者介接不便，衍生商店管理成本高、民眾難以識別及使用等問題。此外，因支付業者眾

多，大多數業者如中小型銀行或基層金融機構，礙於服務規模或資源配置，無法參與行動支付服務，不利於整體市場健全發展。

為建構更完善的行動支付環境，財金公司在財政部的協助下，協同銀行於 2017 年 9 月共同制定「QR Code 共通支付標準」，希望透過既有跨行金融資訊系統及該共通標準建立互聯互通的共用平台(簡稱 QR Code 共用平台)，打造我國行動支付數位金流的高速公路，讓各銀行、基層金融機構、社會大眾及大小商家等，共享行動支付的便利，實踐普惠金融。

貳、使用 QR Code 共通支付標準的交易量

QR Code 共用平台自 2017 年 10 月上線至今，處理的交易金額逐年成長。截至 2019 年底，計有 32 家金融機構、逾 10 萬家特約商店導入，累計的交易筆數及金額分別為 1,482 萬筆及 669 億元。其中 2019 年交易金額 498 億元，較 2018 年成長 2 倍(表 2)。

表 2、QR Code 共通支付標準的交易量

期間	筆數	金額
2017 年 10~12 月	32 萬筆	8 億元
2018 年	356 萬筆	163 億元
2019 年	1,094 萬筆	498 億元
合計	1,482 萬筆	669 億元

資料來源：財金公司

參、適用的規範及資訊安全風險的因應機制

「QR Code 共通支付標準」的參與機構有財金公司、銀行業及基層金融機構等。為確保整體金融支付體系的安全與順暢運作，主管機關金管會針對參與機構各自擔任的角色、屬性及業務服務範圍，訂定相關法令；另銀行公會亦分別就不同性質的業務，制定產業自律規範。謹針對財金公司辦理跨機構作業適用的規範及資訊安全風險的因應機制，分述如下：

一、適用的相關規範

(一) 業務開辦的法令依據

銀行法 47 條之 3 授權訂定的金融機構間資金移轉

帳務清算之金融資訊服務事業許可及管理辦法。

(二) 資通安全管理的法令依據

主要為資通安全管理法及其相關子法，包括資通安全管理法施行細則、資通安全責任等級分級辦法、資通安全事件通報及應變辦法、特定非公務機關資通安全維護計畫實施情形稽核辦法、資通安全情資分享辦法。

(三) 銀行公會相關自律規範

銀行公會針對金融機構辦理行動支付業務及相關訊息傳輸等，制定自律規範，包括金融機構辦理電子銀行業務安全控管作業基準、金融機構辦理行動金融卡安全控管作業規範、信用卡業務機構辦理行動信用卡業務安全控管作業基準、金融機構提供行動裝置應用程式作業規範、金融機構提供 QR Code 掃描支付應用安全控管規範等。

(四) 國際卡安全規範

主要為國際卡組織(如 EMVCo.、VISA、MasterCard)制定的開發、建置、卡片組成、訊息規格、資料傳輸等安全規範。

(五) 國內卡共通標準規範

財金公司協同金融機構制定的金融資訊系統相關卡片組成、訊息規格、資料傳輸、作業安全及「QR Code 共通支付標準」等規範。

(六) 跨行結(清)算作業

使用「QR Code 共通支付標準」進行的交易，其後端涉及金融機構間的跨行資金結(清)算作業，須依中央銀行同業資金電子化調撥清算業務管理要點辦理。

二、資訊安全風險的因應機制

(一) 遵守法令與國內外規範並加強安全防護

為因應資訊安全風險，財金公司除須遵守前述相關法令與規範外，在行動支付交易安全部分，特別加強點對點的安全防護設計，以確保交易無法被偽冒及竄改；對於應用程式、重要參數及資料的防護，則嚴格要求與國際同步，同時運用多樣化技術，避免單一設備暴露或遭破解，引發系統性風險，至於使用者認證機制設計強度，則須確保支付指示，均為合法使用者的意思表示。

此外，對於行動裝置、應用程式、網站等使用者的安全防護，設有監控機制，協助使用者防範駭客攻擊，

以維護行動支付體系的安全。

(二) 持續強化內部資訊安全管理制度與程序

為維護整體資訊安全的強度，財金公司持續強化內部資訊安全管理制度與程序、培養專業技術人力，取得國內外資安專業證照、定期辦理全員資訊安全訓練、提升人員資安意識，並就「交易安全」、「作業安全」、「系統安全」、「網路安全」及「實體安全」等面向建構多層次縱深防禦體系，輔以定期舉辦各項安全防護演練及檢測，並委託外部公正第三方專業機構，定期辦理滲透測試、弱點掃描、防阻斷攻擊及紅隊演練等，以驗證相關機制與程序的有效性及合宜性，並持續改善精進，確保跨行金融資訊系統以及行動支付相關系統運作的安全。

(三) 符合國際標準的資安品質

財金公司就該等資訊安全風險的因應機制與布署管理，除了通過國際「PCI DSS 支付卡產業資料安全標準」審查驗證，確保支付卡片行動應用的安全外，並通過英國標準協會「ISO 27001 資訊安全管理系統」、「BS 10012 個人資料管理系統」、「ISO 22301 業務持

續運作管理系統」及「ISO 9001 品質管理系統」的驗證與定期審查，以確保各項資通訊安全機制、個人資料管理、系統營運不中斷運作及資安作業品質，皆符合國際標準。

肆、財金公司將協同金融機構持續精進相關基礎設施

為促進行動支付的發展，亞洲國家陸續推展 QR Code 共通支付標準(表 3)，以整合國內不一的規格，便利商家及消費者使用。我國推動時程早於新加坡、澳洲、馬來西亞及日本等國，未來財金公司仍會持續協同金融機構共同推廣行動支付，更便利大眾使用。

表 3、亞洲國家 QR Code 共通支付標準推出時程

國家或地區	推出時程	國家或地區	推出時程
1.印度	2016 年 9 月	2.台灣	2017 年 9 月
3.新加坡	2018 年 9 月	4.香港	2018 年 9 月
5.澳洲	2019 年 6 月	6.馬來西亞	2019 年 7 月
7.日本	2019 年 8 月	8.印尼	2019 年 8 月

資料來源：彙整自網路公開資料

伍、 結語

綜上，財金公司長久以來，一直提供跨行服務的中立角色，協同金融機構因應科技、市場發展及民眾需求，精進各項跨行支付的金融基礎設施，取得金融體系的信賴，未來仍會繼續協同金融機構發展創新金融服務，深化普惠金融。

以上報告，敬請各位委員惠賜指教，謝謝。