



資訊安全驗證篇》

資料還權於民的消費者賦權時代

資安驗證標準再升級 金融業者與TSP共創雙贏

我國金融業開放銀行已發展到第二階段—「消費者資訊查詢」，金融業者在消費者同意的前提下，可開放給金融業者的資訊合作夥伴—第三方服務業者（Third-Party Service Providers, 下稱 TSP 業者），共同提供金融多元服務予消費者。然而，對金融業而言，Open API（開放應用程式介面）雖然帶來許多跨業合作機會，卻也面臨監理科技愈趨複雜、法令遵循成本提高等挑戰。

撰文／鄭以文 攝影／陳鴻文 圖片提供／毛敬豪、Depositphotos





受惠於開放銀行上路，過去 3 年來，英國金融科技的投資金額成長率超過 500%，遠高於美國的 170%、歐洲的 133%。

近年來，金融科技成為全球關注的議題，數位浪潮席捲全球，金融監督管理委員會（下稱金管會）2020 年 8 月發布「金融科技發展路徑圖」，希望以金融科技建構全新的金融生態系，開放銀行也列為重點發展項目。然而，這對我國傳統金融業者來說，無疑是險峻的挑戰，因為競爭對手不再只有金融同業，還涵蓋跨界的金融科技公司、大型電商業者等，加上新冠肺炎疫情蔓延，加速使用者的消費行為模式改變，以及樂天國際銀行、LINE Bank 兩家純網銀相繼開業，勢必對既有金融圈生態產生洗牌效應。

採 Open API 的開放銀行將成世界主流

「金融創新教父」布瑞特·金（Brett King）曾說：「銀行已經不再是一個場所，而是一種行為。」開放銀行的概念充分體現了這句話。所謂的「開放銀行」是在消費者同意之下，金融業者將資料透過 Open API 開放給

TSP 業者，雙方交流、共享數據，使得金融服務在銀行之外的通路上也能取得使用。

為了跳脫既有營運模式，傳統金融業者須提升本身的競爭力，並活用資源以開發新客戶，加入「開放銀行」便成為重要拓展方向。根據巴塞爾銀行監理委員會（BCBS）的報告，開放銀行監理措施分為「規範型（prescriptive）」及「促進型（facilitative）」兩大類。前者是主管機關明定銀行與 TSP 業者分享客戶同意的數據，實施此措施最成功的國家是英國；後者則是發布指導性或原則性的標準，鼓勵銀行採用，多半是讓銀行與 TSP 業者選擇共用的 API 技術，香港就屬於此類。

經政府多方研究與評估分析，決定採用不強制、不修法的促進型模式，較適合我國金融型態，由銀行與 TSP 業者一起加入 Open API，攜手推動開放銀行。金管會將開放銀行的進程分為「公開資料查詢」、「消費者資訊查詢」、「交易面資訊」三階段，並由財金資訊股份有



限公司（下稱財金公司）打造「開放 API 管理平臺」，於 2019 年 10 月正式上線，為第一階段揭開序幕，以非交易面的金融產品（如匯率、信貸與房貸利率）查詢為主，如今已發展到第二階段「消費者資訊查詢」。

這將成為我國金融業發展的轉捩點，銀行業者逐步走向「消費者賦權」，透過讓消費者取得自身資料的可攜權，未來可與 TSP 業者一起推出創新商品、便利的服務，使我國金融業者有機會站上世界舞臺。

根據市場調查公司 Allied Market Research 於 2020 年發表的報告指出，全球開放銀行於 2026 年的市場規模可望達到 431.52 億美元，從 2019 至 2026 年的複合年增率則超過 24%。以最早實施開放銀行的英國來說，截至 2020 年 5 月，進入開放銀行的業者已多達 249 家，開放銀行參與率已涵蓋多達 99% 的金融市

場；受惠於開放銀行上路，過去 3 年來，英國金融科技的投資金額成長率超過 500%，遠高於美國的 170%、歐洲的 133%。

推動開放銀行助力開放金融之躍進

此外，參考金融穩定學院（FSI）2020 年提出的「金融科技樹（Fintech Tree）」概念，可以瞭解傳統銀行、開放銀行、Open API 間的關係，而金管會所提出的「金融科技發展路徑圖」也引用此概念。

金融科技樹將金融科技的發展分成樹冠、樹幹、樹根三大部分，分別代表金融科技活動、賦能技術（將金融創新轉為服務所需之技術）、政策輔佐（政府提出的金融科技相關政策）。以金融科技樹的架構而言，「政策輔佐」是根基所在，政府推出的相關政策，像是建置寬頻網路與數位身分系統、成立金融科技創新中心、

全球開放銀行於 2026 年的市場規模可望達到 431.52 億美元。





（左）金融科技樹將金融科技的發展分成樹冠、樹幹、樹根三大部分，分別代表金融科技活動、賦能技術、政策輔佐。

（右）我國推動開放銀行由銀行公會訂立自律規範來約束參與的銀行，同時列出 TSP 業者應當遵循的事項，比其他模式更有機會維持與原金融機構體系標準的一致性。

設置監理沙盒（Regulatory Sandboxes）、推動新創公司的加速器與孵化器、讓開放銀行上路等，對金融科技的成敗皆扮演著舉足輕重的角色。

在金融科技樹的藍圖上，開放銀行屬於金融科技的「政策輔佐」樹根部分，API 則屬於「賦能技術」的樹幹，再搭配生物辨識、雲端運算等技術，才能長出包含「數位銀行」等服務在內的健全樹冠。當一棵樹的根基穩固，樹冠與樹幹方能良好生長，金融科技的政策亦同，必須方向正確與徹底執行，API、AI 人工智慧、生物識別等「賦能技術」才能蓬勃發展，而存款與借貸、保險、募資、資產管理、金融交易、支付、加密資產等「金融科技業務」方可順利上線。

「採取 Open API，風險相對容易控管。」國際性第三方驗證機構、國內 TSP 合規推動的主要參與者之一——環奧國際驗證公司（TCIC）全球營運總經理梁日誠表示，我國推動開放銀行採取香港模式，並由銀行公會訂立自律規範來約束參與的銀行，同時列出 TSP 業

者應當遵循的事項，比其他模式更有機會維持與原金融機構體系標準的一致性。

而參與金管會開放銀行進程第二階段的 TSP 業者，除了第一階段已參與，並有亮眼成績的麻布記帳外，還有遠傳電信旗下「friDay 理財+」、CW Money、錢管家推出的「保險小存摺」App，以及好好投資推出的 FundSwap 基金互換平臺，這些業者正積極與合作的金融業者洽談。「我國開放銀行的推動，還算是順利。」梁日誠觀察指出，加入開放銀行的金融業者，希望能夠透過 TSP 業者獲取有助於推動相關商品或服務的資訊，甚而在平臺或手機 App 上整合其他金融業的資料，邁開大步朝「開放金融」的方向前進。

善用 Open API 滿足消費需求 落實普惠金融

梁日誠指出，以我國而言，金管會推動的「金融資安行動方案」有詳盡規範，鼓勵金融機構導入國際資安管理標準、國際營運持續管理標準，並取得相關驗證，其後再透過第三方



獨立機構檢視管理及營運的有效性，目前資通訊安全的國際標準則包含 ISMS/ISO 27001 與 PIMS/ISO 27701。

Open API 在「技術標準：Open API 技術規格文件」與「資安標準：業務安全控管作業規範」皆已具備標準性規範，不論主管機關或銀行業者，對 Open API 具有充分的信任感，這也有助於帶動消費者信任以 Open API 為基礎的服務。而在開放銀行上路後，不僅能滿足一般消費大眾的需求，更有機會將服務觸角伸向無信用紀錄族群，打造業者與用戶的雙贏局面，有助於實現普惠金融。

梁日誠也認為，TSP 業者透過 Open API 方式，串接不同銀行的商品或服務，提供給消費者更多元的選擇，有利消費者了解自身財務性格與風險所在，進而達到提醒自己審慎理財的效果，或可於 App 中，透過大數據與 AI 的輔助、自動化分析客戶的消費概況，必要時還

可給予警示、提醒，或直接提供財務管理、資金控管的意見。上述的應用，都能透過兩階段 Open API 來實現。

個資隱私權保障、 監理科技皆加重法遵成本

機會的背後往往伴隨著挑戰。首先，我國開放銀行採促進型模式，優點是彈性空間較大，缺點則是因業者自行合作開發，難免會影響推行的進度。梁日誠表示，特別是大型銀行，其客戶數夠多，既有的產品與服務也比同業豐富，多半有能力自行建立生態系，不一定要透過加入 Open API 吸引客戶，若是中大型業者沒有積極投入，帶動開放銀行的速度勢必不如預期。

再者，隨著數位科技在金融場景中愈來愈普及，為了因應創新科技，大量使用客戶個人資料在所難免，隱私權的議題、監理科技

TSP 業者透過 Open API 方式，利用大數據與 AI 的輔助、自動化分析客戶的消費概況。





不論推動何種金融科技的創新服務，資訊安全永遠是首要考量。

（RegTech）的規範均備受重視，金融業者的法令遵循成本勢必加重。在這樣的挑戰下，銀行若將消費者資料交由 TSP 處理、保存，勢必需要強化資訊安全保護措施與降低客戶個資外洩風險。

然則，不論推動何種金融科技的創新服務，資訊安全永遠是首要考量。在開放銀行第二階段中，資料會不斷轉移，守護資訊安全與客戶個資的能力便格外重要。「這也是為什麼像美國 CrowdStrike 這樣的資安服務公司能走紅。」資策會資安科技研究所資安鑄造廠總經理毛敬豪指出，TSP 業者當務之急，便是確認 ISO 相關規範、銀行的個資安全標準，才能與銀行的 Open API 串接起來。

根據銀行公會擬定的自律規範，規定銀行必須與 TSP 業者簽訂合約，並要求符合資安標準，以及符合 ISO 27001 或相關認證。梁日誠表示，銀行與 TSP 業者的互信機制建立在三個基礎上，第一，通過公正第三方 ISO 27001 驗證；第二，由公正第三方檢視相關服務與功能，

提出資訊系統及安全控管作業評估報告；第三，在規定申請許可時，以及之後每年 4 月底前，由公正第三方驗證單位進行檢視，並提出相關評估報告。

萬一出現資料外洩爭議時，必須由銀行端負責，對銀行業者產生不小壓力。「金融業者一定是將隱私權、資安考量放第一，對資訊安全有高度監管機制，但金融科技業者多數是一心想著怎麼開發創新的服務、新的商業模式。」毛敬豪表示，如果雙方考量太過迥異，則很難順利合作。究其原因，金融新創業者與金融機構在資本、規模上都有顯著差異。毛敬豪舉例指出，一個提供轉帳服務的 App 若要通過銀行公會的相關作業規範，購買一套檢測平臺，可能花費百萬元；在資安實驗室檢測一個版本，直到確定可以上線，整體費用約莫數十萬元。對銀行業者也許不算是高昂的費用，但對新創業者而言，卻是很沉重的負擔。

這也形成市場上所見到的現象：金融業者與 TSP 業者一開始討論時，通常先側重於業務面，



接著才進展到資訊面，最後才會討論到法令遵循需要注意之處，但 TSP 業者的構想很容易卡在無法合法合規的瓶頸，導致延誤雙方作業時間，甚至造成合作破局。

為避免這種問題，多數銀行的作法是先與風險相對較低的大型 TSP 業者合作，小型 TSP 則排在最後，但這又造成小型 TSP 業者努力投入資源以符合規範後，依舊很難通過申請，或者根本未受注意。此外，不少 TSP 業者使用與合作銀行協議的「策略夥伴 API (Partner API)」，將 Open API 放在後面的順位，連帶影響 Open API 的普及率，加上若與策略夥伴 API 的安全要求標準不一致，將使合作出現潛在性問題，如介面不能相容、資安風險更不易控管等。

客戶體驗為金融產業未來發展重點

毛敬豪建議，無論是開放銀行或其他數位金融服務，終究會結合 5G、IoT 等科技。既然如此，我國政府若能為 TSP 業者建立分級認證的合規機制，就像目前大部份的半導體、IC 設計大廠都會遵照 BSIM 的標準模型，在同一套基準下，金融業者將能更精準選擇合規且合適的合作夥伴。

Open API 上路後，已有一些值得參考的範本，財金公司與 TSP 業者推創新金融科技的成功案例，備受業界稱許。其中最知名成功的案例為通過國內開放銀行第一階段的指標業者—麻布記帳 (MoneyBook)，藉由 ISO 27001 與 Open API 資安標準建立合規資格，與金融業者或金管會監理沙盒合作，目前已串接 20 間



//PROFILE

梁日誠

現職：環奧國際驗證公司 (TCIC)

全球營運總經理

學歷：國立中山大學電機工程學系



//PROFILE

毛敬豪

現職：資策會資安科技研究所資安
鑄造廠總經理

學歷：國立臺灣科技大學資訊工程
學系博士

銀行之商品資訊及繳費服務 API，加上依照金管會核備 Open API 安控作業規範，提前完成各項測試與演練等，比照金融機構的資安水準，竭力提昇自我能力，因此吸引許多銀行業者合作。

此外，新創科技業者「好好投資」推出的「基金互換案」也是一例。此案的模式是透過區塊鏈技術，在基金免贖回的情況下與他人互換基金，讓投資人省下手續費支出。而在網路安全上，「好好投資」通過 ISO 27001 國際資訊安全管理驗證；資金運用方面，所有基金交易的款項收付都與投信業者相同，管理措施採用將資金交付給保管銀行之信託專戶，此舉吸引遠東商銀 Bankee 搶先合作，並於 2019 年取得金管會核准函，進入監理沙盒實驗，在經過

18 個月驗證後，「好好投資」成功取得特許金融執照，並改制為「好好證券」，成為我國首例金融科技创新實驗落地案件。

整體而言，「開放 API」改變「交換數據 DATA」的傳統模式，金融業者、TSP 業者能藉由「交換數據 數據交換」創造資料價值，共同開拓創新的商業模式，同時消費者也擁有個人資料的主導權，不但是金融業者與 TSP 業者的雙贏，更創造金融業、TSP 業者及消費者的三贏局面。

在銀行與 TSP 業者競相加入 Open API 的趨勢下，客戶體驗絕對是金融服務業者保持競爭力的最重要項目，如何整合各種新技術、強化數位金融產品與服務，提供客戶更具價值、個人化的體驗，將是未來發展重點之所在。