因應與變革篇》

金融科技監理與資安
從純網銀的身分認證談起

純網銀即將開張，未來消費者不需要走進分行填表單，利用手機螢幕即可完成所有手續，真正全年無休的讓人隨時隨地可以進行金融活動，讓金融科技監理與資安技術比起以往更顯其重要性，如何找出事半功倍的方法，值得業者與相關單位多加謹慎規劃。

撰文：廖世偉

面對《台灣銀行家》雜誌邀稿寫純網銀之金融科技及生態，筆者完稿後發現，在當下純網銀新聞過熱時，必須重寫新題以避免讀者無限上綱（編按：作者為純網銀審查委員），所以本文將講科技而不談當今生態，從監理與資安出發，在不談當下商業生態及各方利害時，科技的結晶將沒有被穿鑿附會之可能。

本期先談監理科技，來日再說自動科技監理。沒有監理科技，合規金融科技也無法健全發展。首先，不同於傳統銀行的用戶有實體分行可去，純網銀用戶主要是從手機來認識這個新銀行。不需走進分行填表單，使用介面是手機螢幕，而非表單。24小時都可從手機或桌機操作，用戶體驗依賴好用、感動人心、激勵人心的App。一套銀行系統可從分行表單思維去設計，也可從手機用戶體驗去展開，兩種將差異很大，不易兼顧，可說一種是鯰魚，一種像沙丁魚，若一套系統兩種個性（personality）往往會造成精神分裂，弄巧成拙。

純網銀後台系統必須符合現有資安規範，如ISO 27001（資訊安全管理系統認證），但強度是24小時線上等級。而前台變化尤大，不只是量變，而是質變：用戶不再是到分行在表單上簽名蓋章，而是數位簽章，體驗與資安態樣完全不同。法規「銀行受理客戶以網路方式開立數位存款帳戶作業範本」的第三條定義了銀行如何受理開立數位帳戶。但我國自然人憑證普及率不高，手機開戶者往往隨身沒有自然人憑證，內政部規劃的晶片身分證將於2020年10月開始導入，到時用戶可以手機NFC（近距離無線通訊）讀取身分證晶片裡的憑證，並可數位簽章，但這對純網銀緩不濟急。難道要各家網銀去開模，打造一個手機 USB dongle（轉接器）以在過渡期間時，用戶可插入自然人憑證接上手機？我們只能說，克難式讀卡機之手機版，並不是最好解法。

起手式：身分認證的監理與資安

上述實為痛點中的痛點：在應用五花八門的AI及區塊鏈金融科技前，純網銀第一要「獲客」。在短時間內，人數要達到各家宣示的百萬級，又不想用戶碰到如日本 7pay 近日之用戶盜用問題，純網銀的挑戰不小。純網銀的起手式是身分認證，如何成功獲客是其馬上面對的痛點。深入起手式前，要先幫讀者打底一個重要概念：安全元件（Secure Element, SE）或硬體安全元件。SE的應用之一可為eID，如上述的中華民國晶片身分證，在硬體保護下，安全存放用戶自己的憑證，以供數位簽章。mID（mobile ID）即為上述之手機版。當今悠遊卡或健保卡上的晶片皆沒有憑證，若要等明年開始導入的晶片身分證又太久，可多方嘗試如下方式：

1. 手機 SIM卡換發有SE的SIM卡：是電信商的最愛方式，尤其今日 SIM 卡大多尚未含SE。

2. Embedded SE（eSE）：是手機商的最愛方式，手機裡嵌入硬體SE。

3. Thin SIM（薄膜卡）：在日本稱為 Sub-SIM，在中國叫做貼膜卡。這是在 SIM卡上貼上一層薄膜，不用換SIM，也不用換手機，就提供了SE。

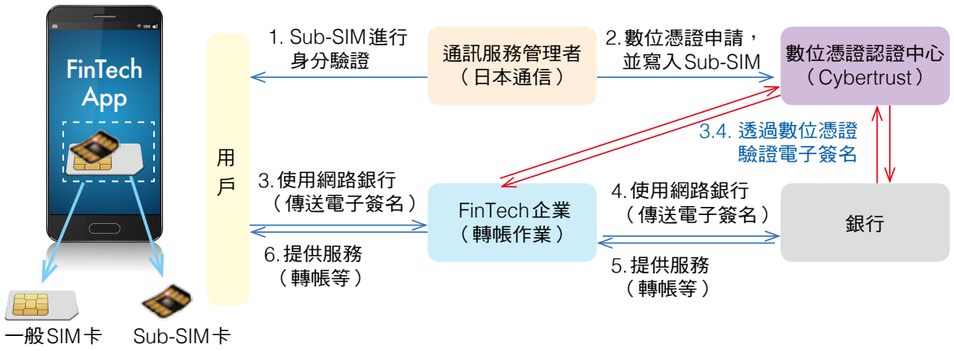
根據法規「金融機構辦理電子銀行業務安全控管作業基準」及上述作業範本，金融作業的中心思想是實名制，跟網際網路不同，而欲符合安控基準高風險場景，關乎資安之私鑰管理更是重中之重，不能放在App或網頁瀏覽器，必須有「第三方認證」確保金鑰儲存安全。以上3種形式俱有第三方認證，如具有 NIST安全認證的Thin SIM。

日本金融廳（FSA）今年對Sub-SIM的實驗結果報告指出，FSA認證除對中間人攻擊、瀏覽器惡意程式攻擊防護度高外，在身分認證上也沒有問題。相對OTP（One-Time Password，一次性密碼）之低安全性，FSA認證之FPoS（FinTech Platform over Sub-SIM，薄膜卡金融科技平台）值得台灣借鏡。過去25年來，網際網路已然發生，食衣住行娛樂乃至廣告紛紛數位化，而如本文所言，下一階段的ID數位化勢在必行，但進度遲緩，監理與資安比網際網路複雜。網際網路是On-to-Offline，食衣住行是多多益善，但數位ID卻是Off-to-Online：關乎權益時，再小的投票都需實名制，金融的本質導致Off-to-On必然性。Off-to-On是一小群一小群先鏈起來，需要時間。這也是筆者與Don Tapscott寫的《區塊鏈革命》的觀點相左之處。

純網銀資安及生態中立性

監理思維之核心是中立性（neutrality）：生態中立性以遍地開花。筆者在Google工作時，這些OTT（Over-the-Top，指服務提供者透過網路向使用者提供內容、服務或應用）公司，如Facebook、Google最關心網路中立（Net Neutrality）：如果底層的電信商（Telco）沒有Net Neutrality，則OTT 無法健康發展，而我們今天用的就不是Google、Facebook提供的服務，而是電信商的內容了，非用戶所樂見。當然，互聯網已經起來，OTT層穩固了，這時即使川普總統取消Net Neutrality，影響不大。但當純網銀及數位 ID 正在興起路上，筆者認為數位金融層必須依賴底層的中立性。筆者拙見電信中立（Telco-Neutrality）及手機中立（Handset-Neutrality）是必須提供的選項。這是日本金融廳驗證 FPoS 的主因〔見圖1〕，不應獨厚某一家電信商及手機商，金融服務不要偏愛某一家電信商。台灣的支付業碎片化，孤島林立，支付普及率不足，互聯互通不夠，未來金融科技繼續發展，我們希望監理上，能夠強調電信及手機中立，打破孤島，讓最好的FinTech服務就拿到對應市占，孤島自然不敢故步自封，互聯互通成幾個太陽才是台灣用戶之福。

圖1 2018年日本金融廳實證試驗了FPoS在下述企業：日本通信、群馬銀行、千葉銀行、德島銀行、Money Forward、Cybertrust。



資料來源：日本金融廳，2019/1/24

以上是必須存在Thin Sim選項的主因。在台灣過渡到晶片身分證期間，FPoS 也能讓各網銀發卡，此卡即含薄膜卡，用戶不需換 SIM 卡或換手機，純網銀就能獲客，以達成電信及手機中立。

獲客（或可指稱身分認證作業）是純網銀馬上面對的痛點。本文從純網銀起手式的監理與資安談起，監理目標是達成純網銀資安及生態中立性。但監理往往是事後監理，對消費者傷害已經造成，事前自律及自動科技監理才是事半功倍的方法。普惠金融是純網銀的重點，年輕族群是必爭之地，以下是年輕人關心之兩大局勢，挑戰了普惠金融監理，自律及自動監理刻不容緩。

金融科技便捷了大規模群募

今天所謂的Big Tech，如Google、Facebook、Amazon，這些也是台灣國民常用的外國服務，因此資料也都在Big Tech手上。當數位金融及區塊鏈興起之際，據稱是台灣最大的區塊鏈新創，光是創辦人公開揭露的募資成果加總即達5千萬美金的柯賓漢公司，卻在今年5月停業。超過120位員工被資遣外，其Cobinhood交易所無法出入金，許多投資者也沒有拿到所發行的Dexon虛擬通貨，大家聽過的台灣唯一在做區塊公鏈技術的公司重演了18年前台灣互聯網最大公司的停業之路，對台灣在區塊鏈興起之際影響深遠。事實上不只重演，相比20年前，今日金融科技影響一般人更大、更迅速，且今日金融科技更容易割韭菜（消費者），例如學生寫遊戲App還沒開幹，其遊戲裝備及寶物幣都已經賣完了，區塊鏈的高效價值傳遞網路，量變成質變，雖說變的不一定是詐欺，惡質發幣卻比比皆是，幣價沒有支撐點，如何保護消費者？政府在6月提出Security Token（ST，證券型代幣）監理方案後，不在該STO（Security Token Offering，證券型代幣發行）規範監理之下的各種Utility Token（UT，功能型代幣）才是當今主流，加上鑽縫的人跑得比監理機構快，我們只能依靠自律組織（Self-Regulatory Organization）。自律在美國早有成功案例，例如Journalism（《紐約時報》等）的行業自律（Code of Conduct），卓然有成，蓋行業才知道眉角，也不願劣幣驅逐良幣。參考他們，筆者列出自律4大重點如下：

1.自我揭露：舉例亞太區塊鏈發展協會2年前在規劃自律公約前，即上網自律聲明：與任何ICO（Initial Coin Offering，虛擬貨幣首次發行）無合作關係，規劃者不兼職，專任學者自然有針砭ICO（包含UT及ST）及興利防弊的底氣。我們也建平台，讓金融科技業者自我揭露，惜成效不彰。

2. 防止利益衝突：例如亞太區塊鏈發展協會儘量開源，服膺前台大校長傅斯年的「貢獻於宇宙」精神，非一己之私，自然降低利益衝突。

3. 多方求證與平衡報導（Multi-stakeholder and balance）：這在台灣也有進步空間，筆者在Corporate America工作多年，Google的管理準則之一即為「背後是非之言者，即為是非之人」，到處八卦者，管理者應自律不聽其言。

4.保密義務：以往審查過程常有人八卦出去，導致許多委員不敢得罪人，審查過程如何正氣凜然？幸好近年已有改善，審查者簽保密協定已是常規。

以上提到的交易所事件並非區塊鏈技術問題，而是監理問題。如果有上述自律，加上自律公約（SRG）裡的信託機制，今年數個交易所事件就不會讓用戶損失慘重。在事件頻傳之際，大家更認知到2018年明確版自律公約的重要。美國證管會（Securities and Exchange Commission, SEC）是採取開放積極的監理。除了對金融科技犯罪者毫不鮑鳥，更積極管理利益衝突，當Telegram申請STO時，SEC即要求Telegram退幣之前從ICO（UT）募得之17億美元，而且這要求退幣已是慣例。

科技金融的開放金融時代到來

筆者觀察四周年輕人往往是使用科技金融的服務，而不是坐等金融科技的產品。從國外coinlend.org的存放款服務利率來觀察，很多學生使用這所謂「開放金融」，而不是網銀來滿足他們的金融需求。DeFi（Decentralized Finance，去中心化金融）用戶與純網銀的客群重疊。任何純網銀不應走到國外網銀的老路：「高利吸存款、低利放款以及亂投資搶回報。」

DeFi雖號稱Decentralized（去中心化），但往往比CeFi（Centralized Finance）還中心化（Centralized）。最後領錢常不在智能合約上，手動式風險大。政府對此的態度為何？筆者相信DeFi在洗錢防制、反資恐的國際趨勢中，還是需要適度監理才走得久遠。

金融科技監理與資安有眾多挑戰。本文從起手式談起，力求身分認證痛點之合理解決，兼顧資安及生態中立，最後以兩個年輕人高度關心的局勢收尾：第一，政府對金融科技監理是否像美國一樣開放積極；第二，我們如何面對DeFi中存借放款的金融服務？不管以上政府的時程表，事前自律及自動科技監理將事半功倍，也不牴觸政府監理。適度監理才能更健康長遠，而自律及自動科技監理則可作為日後監理的參考。（本文作者為臺大資訊工程系副教授）