出國報告（出國類別：實習）

參加美國紐約聯邦準備銀行舉辦之「支付」課程報告

服務機關：中央銀行

姓名職稱：吳姿盈 辦事員

派赴國家：美國

出國期間：114 年 5 月 17 日至 23 日

報告日期：114 年 8 月 1 日

目錄

壹、前言

本次奉派參加由紐約聯邦準備銀行(Federal Reserve Bank of New York, FRBNY)於本(2025)年 5 月 19 日舉辦之支付(Payments)課程，課程共計 3 日，參與的學員約 116 位，除來自全球各國央行及監管組織之成員，國際組織如歐洲央行(European Central Bank, ECB)及國際清算銀行(Bank for International Settlements, BIS)等亦派員參加本次課程。

講師除來自美國聯邦準備體系(Federal Reserve System, Fed)之內部職員，包含聯邦準備理事會(Board of Governors of the Federal Reserve System)、紐約及波士頓等分行，亦邀請 BIS 職員擔任講師。課程內容涵蓋美國傳統的支付系統介紹，包含 Fedwire 證券服務系統(Fedwire Securities Service)、Fedwire 資金服務系統(Fedwire Funds Service)及全國清算服務(National Settlement Service, NSS)等，以及近年上線的即時支付服務系統 FedNow、BIS 支付暨市場基礎設施委員會(Committee on Payments and Market Infrastructures, CPMI)對跨境即時支付互聯機制之設計架構，並就全球因應支付創新所延伸之詐欺風險治理對策等議題進行分享。

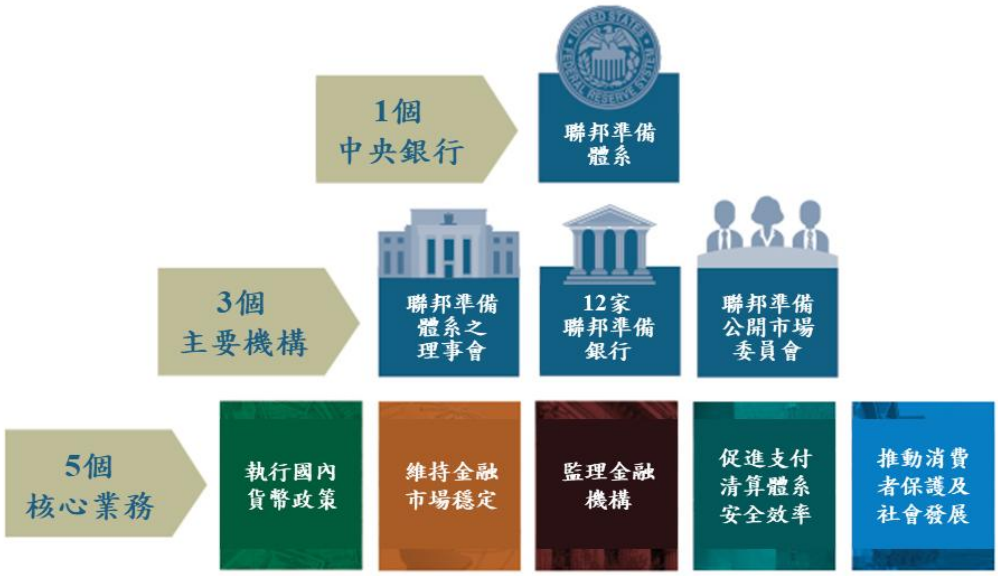
本報告共分 5 章，除第壹章為前言外，第貳章簡介美國聯邦準備體系，第參章介紹美國支付系統及其近期營運概況，第肆章說明主要國家因應支付創新所採取之詐欺防制機制，第伍章為心得及建議。

貳、 美國聯邦準備體系

一、 Fed 之組成架構與職能

Fed 於 1913 年依《聯邦準備法》(Federal Reserve Act)設立，為美國中央銀行體系，由聯邦準備理事會[1](Board of Governors of the Federal Reserve System，下稱理事會)、12 家聯邦準備銀行(Federal Reserve Bank)及聯邦準備公開市場委員會[2](Federal Open Market Committee, FOMC，下稱委員會)組成。Fed 法定上肩負雙重職責(dual mandate)：包括**充分就業**與**穩定物價**。Fed 之**五大核心業務**包括：執行國內貨幣政策、維持金融市場穩定、監理金融機構、**促進支付清算體系安全及效率**及推動消費者保護及社會發展(圖 1)。

圖 1、聯邦準備體系架構圖



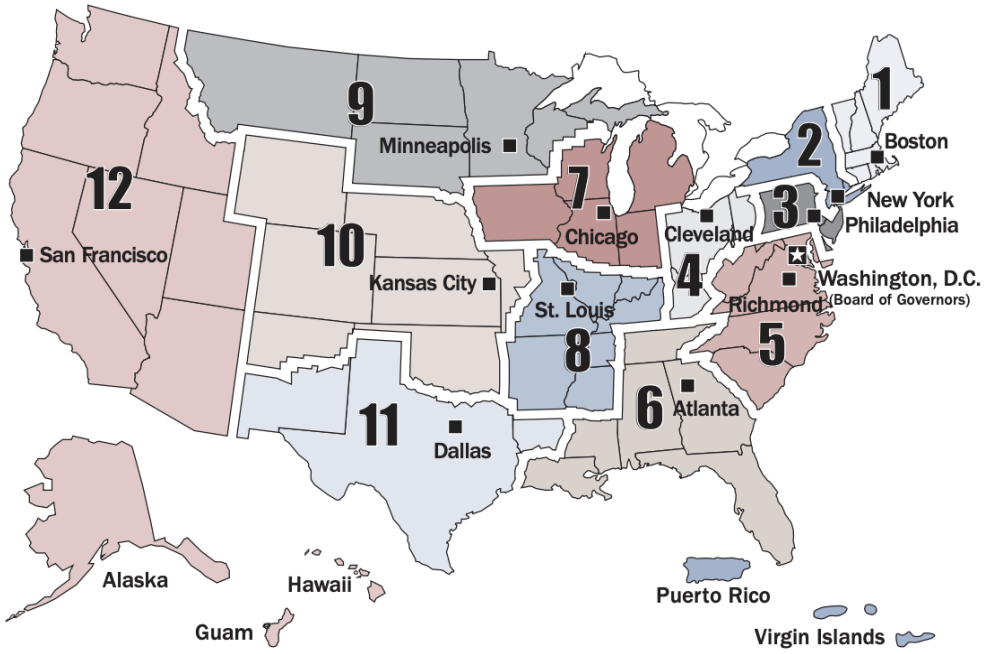
資料來源：本次課程投影片(2025)。

[1] 設於華盛頓特區，理事會由 7 名理事組成，負責管理及監督全體聯邦準備體系之運作，以及制訂政策與法規。

[2] 委員會由 12 位委員組成，包括理事會的 7 位理事、紐約聯邦準備銀行總裁，以及 4 位由其餘 11 家地區聯邦準備銀行總裁輪流擔任的一年期委員，為美國貨幣政策之決策機構，負責設定政策利率與公開市場操作方向。

其中，聯邦準備銀行將全美劃分為 12 個聯邦準備區(圖 2)，於各自轄區內執行金融機構監理、支付清算與金融服務，以及經濟研究等職責，為 Fed 五大核心業務之主要執行單位。

圖 2、地方聯邦準備銀行轄區分佈圖



資料來源：本次課程投影片(2025)。

二、 Fed 在支付體系中的角色

為確保系統的可及性、安全性與效率，Fed 在美國支付體系中扮演中央銀行與支付系統營運者 2 種角色，分別負責政策監理與系統營運，並透過(1)提供存款機構(depository institutions)及聯邦政府支付服務、(2)監理特定支付系統與金融市場基礎設施、(3)提供參加單位日間流動性，以及(4)監控支付系統運作，並持續優化系統運作效率等方式維繫全國現金、支票與電子支付工具之穩定運作。

然而，為避免身兼支付系統之營運者與監理機關可能產生

之角色衝突，Fed 對其職能區分採取審慎態度，由理事會負責支付政策與監理職能，包含核准重大系統變更、審查定價政策、監控營運風險等；12 家地區聯邦準備銀行則執行實際營運職責。Fed 透過持續監測、內部稽核及制度性審查，確保支付體系之安全、公平與效率。

參、 Fed 營運之支付系統

一、 支付系統概述[3]

Fed 營運之支付系統可分為大額支付系統(Large Value Payment System, LVPS)與零售支付系統(Retail Payment System, RPS)。大額支付系統包含 Fedwire 資金服務系統(Fedwire Funds Service)及全國清算服務系統(National Settlement Service, NSS)[4]，用以處理高金額、低筆數交易，常用於金融機構間交易或金融市場活動相關，強調即時處理與最終清算，需具高穩定性與不可撤銷性。

零售支付系統則包含支票交換結算系統(Check Services)、自動支付結算系統(FedACH)及 FedNow 即時支付系統，主要處理低金額、高筆數之交易，依其系統設計及業務需求，可採批次或即時清算，應用範圍涵蓋個人間(P2P)、個人與商家間(P2B)及商家間(B2B)付款需求，包含支票交換結算、ACH 代收代付及即時小額支付等。

---

3 鄭暐霖(2024)。

4 NSS 係一項多邊淨額清算平台，由清算代理機構(settlement agent)依與存款機構間之協議，批次提送結算淨額至 Fed。系統以參加單位於 Fed 開立之主帳戶完成清算，交易具備最終性與不可撤銷性。NSS 主要用於處理證券、ACH、支票與國庫現金管理系統(TCMS)等私部門清算安排之最終清算，其中以證券交易佔比最高，達 49%。

除上述支付系統外，Fed 亦營運 Fedwire 證券服務系統(Fedwire Securities Service)，係美國主要之證券清算系統(Securities Settlement System, SSS)之一，負責政府與機構債券之電子化託管、交割及利息支付等作業，為維繫金融市場流動性與穩定運作之關鍵基礎設施。

二、 主要核心系統

Fed 營運多項支付與清算系統，其中以 Fedwire 資金服務系統、Fedwire 證券服務系統，以及 FedNow 即時支付系統三項核心基礎設施具高度系統重要性，分別支援大額即時資金清算、政府與機構債券之交割清算，以及全天候即時零售支付。以下就各系統之主要架構與功能進行說明。

(一) Fedwire 資金服務系統

1. 系統概述

Fedwire 資金服務系統採即時總額清算(Real-Time Gross Settlement, RTGS)機制，交易以參加單位[5]在 Fed 開立之主帳戶(master account)[6]進行清算，主要業務包含：銀行間交易、

[5] 參加單位分為直接及間接參加單位：直接參加單位包含美國存款機構、外國銀行在美國的分行、美國財政部(U.S. Treasury)、外國央行及其他國際組織等；間接參加單位係指未具備直接介接 Fedwire 資金服務系統資格之機構，需透過代理行(correspondent bank)或其他具直接參加資格之金融機構轉送交易指令，常見於小型金融機構或參與跨境支付之境外機構。

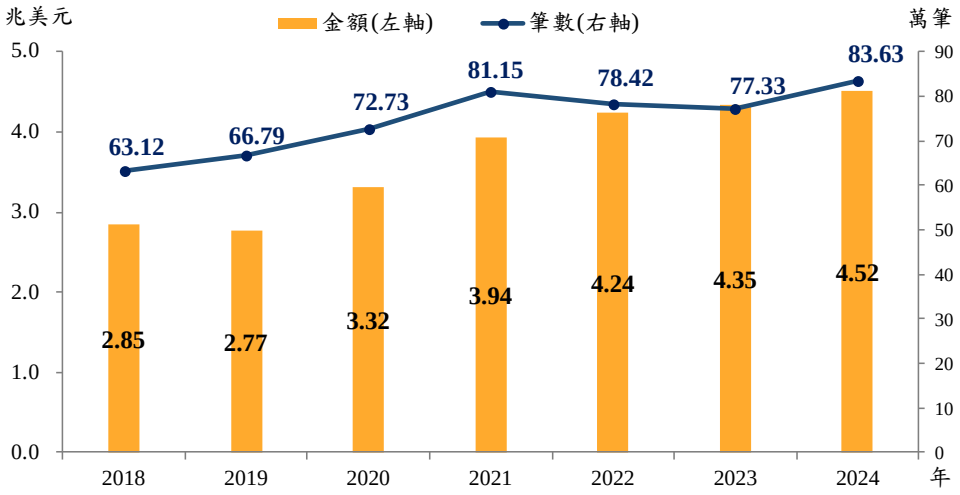
[6] 主帳戶係由 Fed 透過其會計服務(Accounting Services)管理，具備即時入帳與資金最終性清算特性。此帳戶為金融機構參與 Fed 各項支付與清算系統(如 Fedwire 資金服務系統、Fedwire 證券服務系統、NSS 及 FedNow)之基礎，帳戶餘額會依據各系統所接收之付款指令，即時調整增減，以完成資金或證券交易之清算。依據聯邦準備法，具申請開立主帳戶資格的機構包括(1)加入任一家聯邦準備銀行之成員銀行(包括國家銀行、州立銀行、銀行或信託公司)、(2)存款機構(包括商業銀行、互助儲蓄銀行、聯邦儲蓄銀行、儲蓄貸款協會、信用合作社)、(3)外國

其他金融基礎設施交易、具時效性商業支付[7]及跨境支付等款項清算。

Fedwire 資金服務系統營運時間為營業日前 1 日 21 時至當日 19 時(共 22 小時)，並提供 2 種主要的直接使用管道，分別為 FedLine Direct 及 FedLine Advantage，多數大型金融機構(如跨國或區域型銀行)透過 FedLine Direct 進行電腦系統直連，提供高度安全之自動化處理管道，佔整體交易筆數約 97%；FedLine Advantage 則為中小型機構(如社區型銀行)的主要連線方式，係透過 VPN 連線至網頁操作介面進行逐筆登錄的人工交易或檔案上傳，亦可作為使用 FedLine Direct 之大型機構的備援連線機制，約佔整體交易筆數 3%。

2024 年 Fedwire 資金服務系統日均交易筆數約 83.6 萬筆，日均交易金額約 4.52 兆元(圖 3)。

圖 3、Fedwire 資金服務系統營運量



資料來源：本次課程投影片(2025)。

銀行在美分行或代理機構、(4)依艾奇法(Edge Act)設立的企業(例如經營國際金融業務的美國當地銀行)、(5)美國財政部、政府機構、政府資助企業等其他依法有權開立的機構。

[7] 具時效性之商業支付(time-critical commercial payments)係指企業或法人機構於營運或契約條件下，須於特定時限內完成之款項支付，例如不動產交易、票據償還、企業間大額交易等，此類交易通常需確保資金即時入帳與最終清算，故常透過具即時性與不可撤銷特性之 Fedwire 資金服務系統進行處理。

2. 近期優化措施

(1) 備援機制

為協助參加單位因應其系統異常情境，Fed 於 2025 年 2 月 18 日推出「FedPayments Manager – Funds Contingency Service」。當參加單位因內部系統[8]異常，無法正常將付款指令傳送至 Fedwire 資金服務系統時，可改由 FedLine Advantage 提供之 FedPayments Manager–Funds 網頁操作介面，匯入檔案進行批次支付，作為付款指令傳送異常時的替代機制，以確保在主要連線方式發生故障時，仍能持續處理重要支付作業，降低交易中斷風險，並提升整體系統之韌性。

(2) ISO20022 格式導入作業

為強化支付系統資料標準化與跨境互通性，Fed 自 2025 年 7 月 14 日起，將 Fedwire 資金服務系統訊息格式由原本的 Fedwire Application Interface Manual(FAIM)專屬格式轉換為 ISO 20022 訊息格式，以促進境內與跨境支付的互通性、承載更豐富的支付資料，並有助於支付流程的追蹤與直通式(STP)處理。

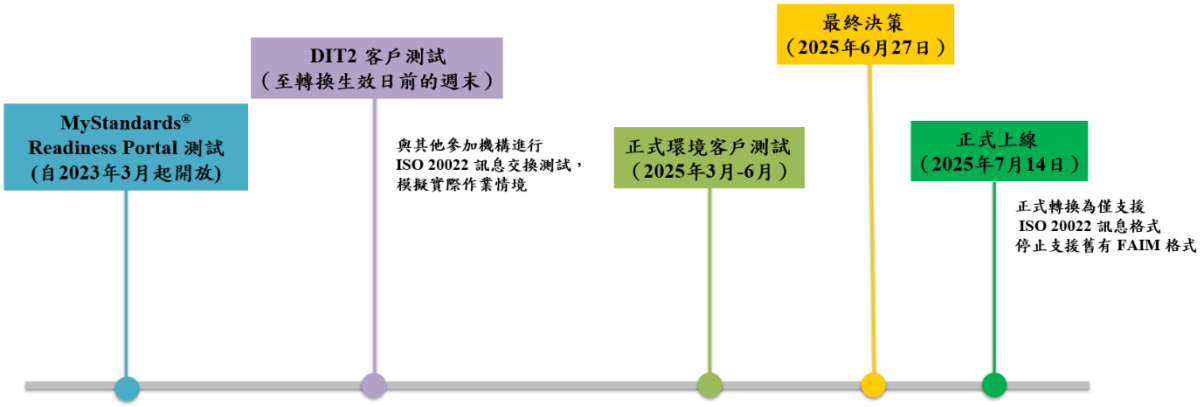
Fed 與金融機構、技術服務供應商、支付系統營運商及其他金融基礎設施機構密切合作，並規劃多項輔導措

[8] 該備援機制僅適用於參加單位內部系統故障之情境，並不適用於 Fed 系統異常、Fedwire 平台故障或 FedLine 連線中斷等情境，由於 FedPayments Manager–Funds 係透過 FedLine Advantage 平台運作，若連線中斷，則此備援機制亦將無法啟動；配合此措施實施，Fed 於 2025 年 2 月 14 日宣布終止原先以電話提供之離線服務。

施以協助系統順利遷移(圖 4)，包括：

- 測試與演練：提供週末點對點測試、封閉用戶群測試與測試環境，供參加單位模擬 ISO 20022 訊息實際作業情境，並於轉換前舉行聯合預演(dress rehearsal)，模擬實際切換流程以強化營運應變能力。
- 教育與訓練：辦理 FedLine Advantage 操作培訓、一對一單位輔導、線上說明會與線上教材，協助不同參加單位熟悉新格式操作介面。
- 驗證與回報：要求 FedLine Direct 服務供應商及主要用戶進行系統驗證測試，並於 2025 年 4 月底前提交上線前準備聲明(attestation)與準備情況調查表，以評估產業整體準備程度。
- 備援規劃：對未按進度完成轉換準備的機構，要求提送應變計畫，確保轉換當日可順利運作。

圖 4、轉換 ISO 20022 訊息格式時程



資料來源：Fed 官網(2025)。

此外，Fed 亦設立「ISO 20022 實施中心」（Implementation Center）網站，彙整技術規格、訊息範例、測試工具及最新公告等資訊，協助機構瞭解轉換流程與重點作業；Fed 已於 2025 年 6 月 27 日完成「Go/No-Go」最終評估，確認按原排程執行轉換。FAIM 格式已於轉換營業日前 1 日(7 月 11 日)19 時停止使用，並自 7 月 14 日起正式全面啟用 ISO 20022 格式。Fed 亦於 7 月 15 日發布聲明，確認 Fedwire 資金服務系統已成功完成遷移。

(二) Fedwire 證券服務系統

Fedwire 證券服務系統係由 Fed 營運之證券清算與登錄平台，具證券集中保管機構(Central Securities Depository, CSD)及證券清算系統雙重角色，提供即時、最終且不可撤銷之證券交割服務。主要業務包括支援美國財政部及其他機構所發行之電子化證券之發行、付息、到期償還、買回、拆分重組等作業。

除交割作業外，該系統亦提供多項輔助功能，包括：支援聯邦貼現窗口所設之限制用途帳戶、特定擔保存款用途之專用帳戶，以及債券附買回期間涉及債券票息及本金支付之自動調整處理作業。

由於 Fedwire 證券服務系統負責處理大量且多樣化的證券交割作業，係維持金融市場運作穩定與交割秩序之重要基礎。雖該系統目前未被正式指定為金融市場基礎設施，惟考量其在金融市場中具不可替代性與高度集中度，Fed 仍要求其遵循嚴

格的監理標準，以確保系統安全與營運韌性。

2024 年 Fedwire 證券服務系統日均交割筆數約 13.2 萬筆，日均交割金額約 6 兆元(表 4)。

表 1、2024 年 Fedwire 證券服務系統營運資料

項目	交易數據
營運時間	前 1 營業日 19 時 50 分至當日 19 時 (合計 23 小時 10 分)
參加單位	約 2,000 家
登錄證券總面額	約 115 兆美元
日均交割筆數	約 13.2 萬筆
日均交割金額	約 6 兆美元
2024 年發行總面額	41 兆美元 (其中約 29 兆為美國財政部發行的公債)

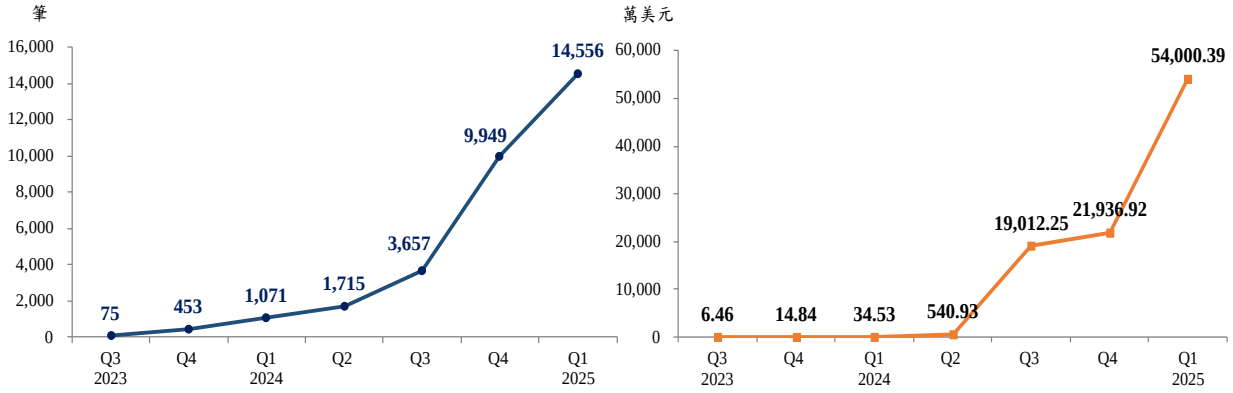
資料來源：本次課程投影片。

(三) FedNow 即時支付系統

1. 系統概述

FedNow 係 Fed 於 2023 年 7 月起提供之 24 小時營運、全年無休之快捷零售支付系統，採 RTGS 機制，2024 年全年交易筆數超過 1.5 億筆，目前已有超過 1,300 家金融機構參與，應用情境涵蓋即時薪資發放、商業付款及小額貸款等多元交易場景。2025 年第 1 季 FedNow 日均交易筆數約 1.46 萬筆，日均交易金額約 5.4 億元(圖 5)。

圖 5、FedNow 營運量



資料來源：Fed 官網(2025)。

2. 近期發展重點

(1) 強化請求付款(Request for Payment, RfP)功能

請求付款(Request for Payment, RfP)係由收款方參加單位代表其用戶主動發出付款請求，經付款方審核後，透過即時支付完成資金撥付之功能。

FedNow 現階段提供的 RfP 功能仍屬初階版本，僅開放予具備「可發送客戶付款指令及接收來自他行付款」(Customer Credit Transfer Send and Receive)資格的參加單位使用，且該功能預設為停用，須由參加單位主動向 Fed 申請啟用。

Fed 預計擴大 RfP 功能之應用範圍，涵蓋數位錢包儲值、定期或一次性帳單繳付(如水電費、醫療費用)、應收帳款管理、商家間(B2B)交易收款流程之自動化、公用事業費繳納與公益捐款等情境。藉由 RfP 機制可提升付款流程效率，強化交易資訊結構化與自動化處理能力，進一步拓展即時支付之應用場景。

(2) 導入進階風險管理機制

為強化風險控管，FedNow 系統設計納入多項風險管理機制，包含轉帳金額或筆數限制、累積金額上限、付款對象黑名單、帳戶狀態(如警示帳戶)與偵測可疑交易之處理規則等，並提供參加單位依據自身風險承受能力彈性設定與調整，以協助建立交易審查與詐欺識別防線。FedNow 未來亦將透過功能更新，持續強化即時風險控管能力，預計導入異常交易偵測條件、集中式可疑帳戶管理，以及跨機構詐欺資料共享等進階機制，以建立健全可靠之即時支付生態系；惟 Fed 表示相關措施目前仍在研議階段，尚未訂定具體上線時程。

然而，實務上詐欺風險常透過跨平台、跨通路方式進行，單一機構難以全面掌握並即時阻斷詐騙行為。FedNow 目前以提供安全、穩健之支付基礎設施為核心，其風控功能雖可協助識別可疑交易，但對於交易完成後的資金追回仍需仰賴參加機構自行處理。

(3) 退款與錯誤處理機制

FedNow 提供退回請求(Return Request)功能，允許參加單位於識別可疑或錯誤交易後，向對方參加單位提出退款請求。此功能係依據 ISO 20022 標準格式傳送，並標示為「接受但暫不入帳(Accept without Posting)」，可延後資金入帳以利合規或審查。此外，FedNow 建有詐欺通報機制，要求參加單位即時回報可疑交易資訊，以利整

體系統快速辨識與因應潛在威脅。

惟目前退款處理仍須由雙方金融機構協議辦理，尚未建立統一的自動退款或用戶救濟機制，實際追回率與速度受限於參加單位意願與內部流程，對於用戶保障仍有限。

肆、 主要國家因應支付創新之詐欺防制機制

隨著即時支付系統快速發展，數位錢包與各類支付應用程式日益普及，亦衍生出多元且複雜的詐欺手法與風險挑戰，支付詐欺問題因而受到各國央行與監理機關重視。

近年常見的詐欺事件多為誘導用戶主動發起轉帳的授權支付詐欺(authorized push payment fraud)，即用戶在遭詐騙者誘導下主動發起付款之詐騙行為，與傳統盜刷或未經授權的轉帳不同。其手法包括假冒商業機構、政府部門或親友等冒名詐騙(Imposter scams)、透過社交工程誘導用戶下載惡意應用程式或洩露帳戶憑證，或引導參與假投資、異常開戶等。

由於此類詐騙付款交易係由用戶主動授權啟動，難以歸責於金融機構，且因即時支付具備資金即刻撥付且不可撤銷等特性，使防詐策略更需於交易前即透過預警機制及風險控管即時阻斷可疑交易。

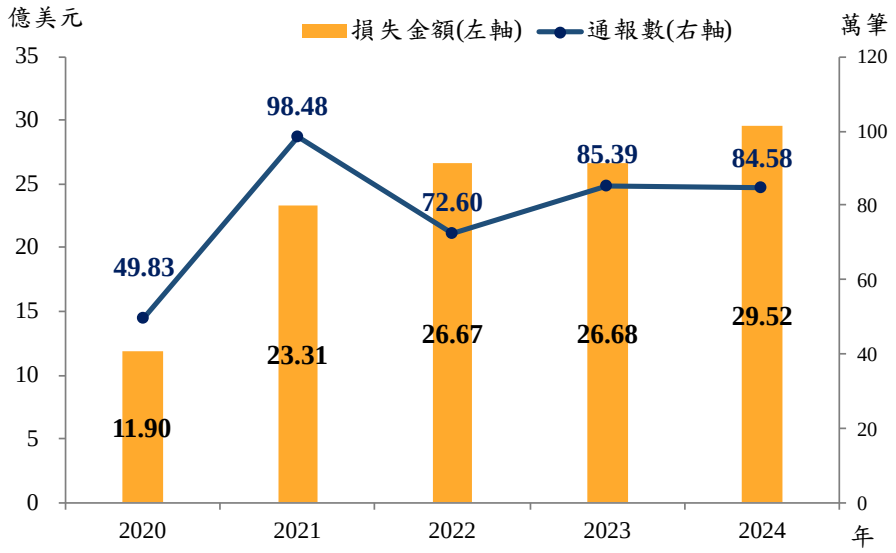
本章節整理美國、泰國、印度與巴西等國面對即時支付與創新金融服務所衍生之詐欺風險，所採取之防制機制與治理作法。

一、美國

(一) 現行 P2P 平台詐欺風險與補償機制不足

近年美國因 Zelle、Venmo 等 P2P 支付平台[9]的普及，導致授權支付詐欺案件顯著上升。根據聯邦貿易委員會(Federal Trade Commission, FTC)統計，2024 年冒名詐騙通報案件達 84.58 萬件，損失金額高達 29.52 億元，分別較 2020 年增加約 70%與 148%(圖 6)。

圖 6、近年冒名詐騙案件數及損失金額統計



資料來源：Federal Trade Commission 官網(2025)。

美國現行支付詐欺防制機制主要建立在既有金融法規與市場自律體系。然而，現行《電子資金轉帳法》(Electronic Fund Transfer Act)僅適用於未經授權的轉帳，對於用戶在詐騙誘導

[9] Zelle 與 Venmo 為美國主流的 P2P 支付平台，提供用戶透過手機號碼或電子郵件轉帳至他人銀行帳戶或錢包。Zelle 由多家大型銀行聯合推出，資金於銀行帳戶間直接清算，具備即時到帳、無需儲值等特性；Venmo 則為 PayPal 旗下產品，偏重社交功能與應用程式內互動，雖可即時顯示轉帳結果，但實際資金提領至銀行帳戶仍需時間。由於兩者交易快速、操作便利且多為不可撤銷付款，亦經常遭詐騙集團利用作為詐騙工具。

下主動授權的交易則多不適用。儘管部分平台如 Zelle 自 2023 年起，已針對特定詐欺情境(例如用戶誤信冒名為銀行或政府機構人員而匯款)提供有限度之賠償方案，惟整體補償機制仍屬平台自律性質，補償範圍與認定標準不具一致性，金融機構亦通常無退款義務，缺乏統一的補償機制及處理原則。對於受害用戶而言，跨機構協調與申訴程序仍面臨高度困難，退款結果往往取決於個別機構的政策與配合意願。

(二) 民間倡議團體對 Fed 提出之政策建議

針對即時支付詐欺風險與現行補償機制之不足，全國消費者法律中心(National Consumer Law Center, NCLC)協同其他倡議團體曾於 2021 年提出政策建議[10]，呼籲監理機關將因詐騙而產生之授權支付交易納入法律保障範圍，並由主管機關主導建立統一的補償標準與跨機構爭議處理機制，以彌補平台自律制度的落差，縮短受害者救濟流程，進而提升用戶信任與支付市場之整體韌性。

當時，NCLC 亦針對 FedNow 制度設計方面提出五大訴求：包括：1.建立付款可逆與更正流程；2.導入付款前對收款帳戶之確認機制(Confirmation of Payee)；3.將詐欺交易納入《電子資金轉帳法》適用範圍；4.建立跨機構詐欺資訊共享平台，以及 5.設計由付款銀行先行承擔補償責任、再行追償的制度架構，並強調，隨著即時支付普及，若未同步建置對應的保護機制，將使得用戶暴露於詐騙損失風險。

[10] NCLC(2021)

美國即時支付創新快速，現行制度對於用戶防詐保障機制仍存在結構性缺口，包括法規適用範圍限縮、補償責任未明、平台技術與處理機制落差大等問題，未來相關法規修訂、跨機構協作與資訊整合技術發展將是提升支付體系安全之重要關鍵。

二、 泰國

(一) P2P 詐欺風險與制度挑戰

隨著泰國即時支付系統 PromptPay 與數位金融工具快速普及，P2P 轉帳、網購付款與社群平台交易已成為主要支付模式，亦帶動詐騙風險大幅上升。泰國央行(Bank of Thailand, BOT)指出，近年授權支付詐欺案件通報數與損失金額持續攀升，已成為該國主要的數位詐欺類型。

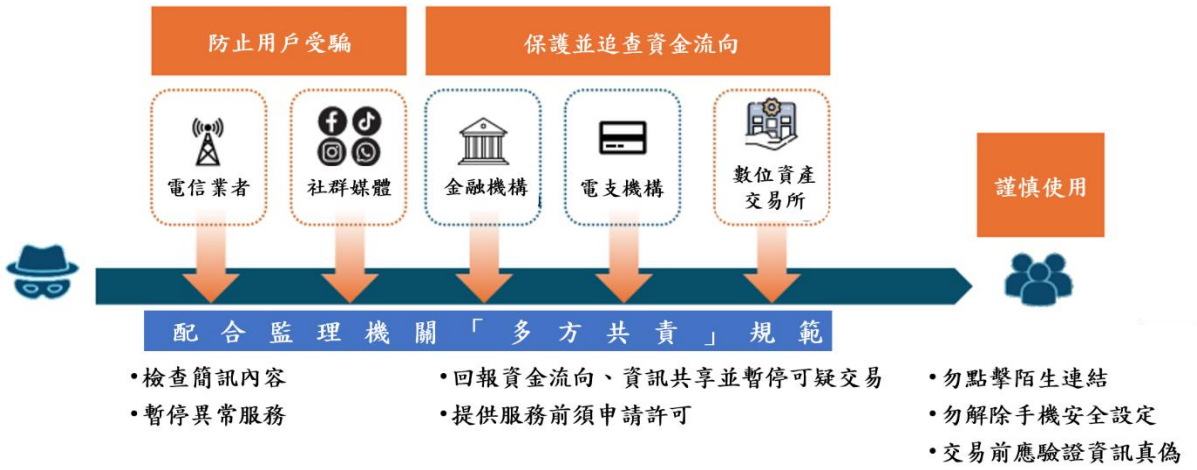
此類詐騙多源自社交工程誘導、帳戶資訊外洩與即時支付不可逆特性，加上用戶防詐意識薄弱、跨平台交易頻繁且缺乏統一監理標準，使詐騙者得以快速完成多筆轉帳並分散資金，增加追查與攔阻難度。雖然泰國銀行公會與商業銀行近年已強化交易限額與驗證流程，惟在缺乏統一申訴機制與跨機構資料整合下，受害者遭詐後之補償與救濟程序仍具高度不確定性。

(二) 監理機關主導下之防詐制度設計與協作機制

面對支付詐欺風險，BOT 自 2023 年起推動多項防詐政策，強調跨部門協作與分工治理，並建立「多方共責」制度架構。金融機構、電信業者與數位平台皆需依其職責落實用戶識別、

交易風險管控與資訊封鎖等防詐機制(圖 7)。

圖 7、泰國多方共責阻詐架構



資料來源：本次課程投影片。

2023 年，BOT 公布「防制詐欺五大強化措施[11]」，要求所有金融機構落實以下規範：

1.禁用連結訊息：不得透過簡訊與電子郵件傳送附有連結的訊息；

2.單一裝置登入：限制每一帳戶僅能綁定並登入一部行動裝置；

3.高額交易驗證：對高額交易或新增受款人強制啟用生物辨識驗證(如臉部辨識)；

4.提供用戶 24 小時客服：建立全天候通報管道，供用戶即時通報及凍結帳戶；

5.即時異常通報：發現異常帳戶時須即時通報 BOT 與銀行資安協調中心(Thai Bank Sector CERT, TB-CERT)，以

[11] Bank of Thailand(2023)

利資訊共享與聯防應變。

2024 年，BOT 再發布《數位詐欺風險管理指引》草案[12]，強調金融機構應建立涵蓋詐欺預防、偵測、通報、補償與用戶協助等完整管理機制，並鼓勵導入人工智慧行為分析與跨行警示系統，以提升防詐應變能力與資料共享效率。此外，草案亦提出，金融機構應建立具明確時限之補償處理流程，並強化黑名單帳戶資料庫與標準化申訴機制，以提升詐騙受害者之救濟可行性與處理效率。

為強化制度執行力，BOT 與反洗錢辦公室、國家網路安全局及金融機構建立跨部門協調機制，推動跨機關「聯合打詐專案小組」與資訊整合平台，提升詐欺事件的通報、分析與應變效率。BOT 並促使金融業者建置「防詐資訊共享平臺(Fraud Portal)」，整合用戶風險資訊與詐欺資料查詢服務，強化資料交叉比對與即時風險識別能力。

截至 2024 年底，泰國在 BOT 主導下已停用逾 175 萬個人頭帳戶，顯示其跨機構聯防機制具備明確成效。在防制支付詐欺方面，泰國展現高度整合力與執行效率，透過制度設計、跨機構合作與資料共享，已建立出一套相對完整且具實效的即時支付詐欺防制體系。

[12] Tilleke & Gibbins (2025)

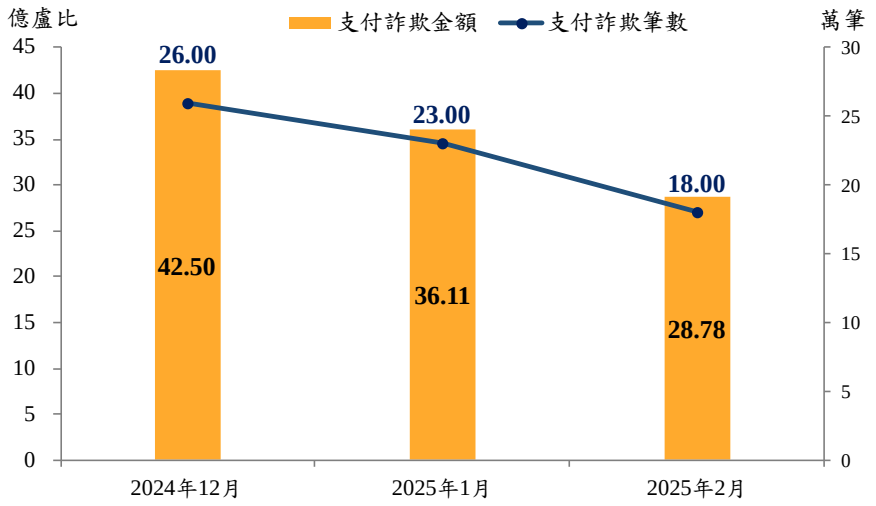
三、印度

(一) 詐欺樣態與數位支付環境特性

印度近年數位金融基礎建設快速發展，2024 年每日平均處理數位支付交易量高達 4.56 億筆，涵蓋即時轉帳、行動支付及 QR Code 付款等多元場景，整體數位交易年增率持續攀升。其中，以印度國家支付公司（National Payments Corporation of India, NPCI）營運之即時支付系統「統一支付介面」（Unified Payments Interface, UPI）最為普及，占整體交易量逾七成，已成為印度行動支付之主要工具。

隨著數位支付規模擴大，詐欺案件亦同步上升。2024 年每月平均通報之國內數位支付詐騙案件約為 24.5 萬件，較 2023 年之 22.1 萬件成長約 11%，每月平均損失金額亦自 32 億盧比增至 44.1 億盧比，損失金額成長幅度達 38%，雖 2025 年略為改善，惟整體詐欺數量仍高(圖 8)，顯示詐欺風險已成為印度金融安全之重要挑戰。

圖 8、近月印度詐欺案件統計



資料來源：本次課程投影片(2025)。

(二) 監理機關之防詐規範與機制

為防制支付詐欺風險，印度央行自 2020 年起逐步推動多項制度與技術強化措施，涵蓋交易驗證、安全控管、異常偵測及用戶宣導教育等層面，主要措施包括：

1.多重驗證與身份識別措施：要求金融機構於交易過程中導入手機裝置綁定、生物特徵辨識與雙因子認證，並針對高額交易設定額外驗證門檻。

2.即時監控與異常攔阻機制：建立風險評分模型與異常行為偵測系統，並可預先凍結疑似詐欺資金，提升防堵成效。

3.用戶教育與警示機制：鼓勵業者強化用戶識詐教育，於交易頁面提供即時警語，提醒高風險交易風險情形。

4.跨部門合作與通報體系：監理機關協調相關業者參與跨部門資訊共享與通報流程，包含建立報案熱線、假帳戶查詢與可疑資訊通報。

此外，印度央行亦規劃推動進一步強化之防詐措施，包括建立「可疑帳戶監控」與「統一退賠制度」，要求支付業者定期查核用戶是否具詐騙風險標記，並設計付款與收款金融機構間作業流程之標準化退款流程及配套之跨機構協作規則，以提升受害者救濟效率與處理一致性。

整體而言，印度已建構涵蓋身分驗證、異常偵測、用戶教育與跨部門協作等多元防詐機制，惟在制度執行力與中小型金

融機構資源配置方面仍存在落差，例如在視訊開戶及身分驗證等特定環節，部分中小型金融機構落實程度仍不一致，形成潛在防線缺口。未來若能持續強化退費制度、資訊共享與中小型機構之技術支援，將有助於提升整體支付體系之安全韌性與使用者信任。

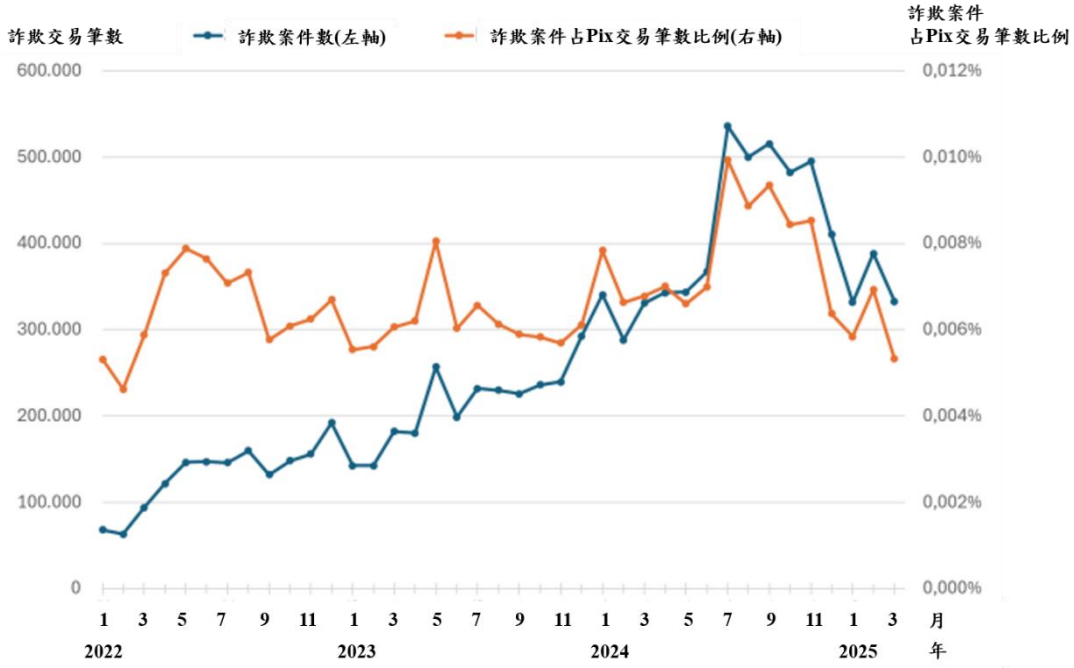
四、 巴西

(一) Pix 系統發展與詐欺樣態

Pix 係巴西央行自 2020 年 11 月起提供之即時零售支付系統，具全年無休、即時清算與免手續費等特性，推行後迅速普及。截至 2024 年底，用戶數達 1.81 億人，約占全國人口 76%，全年交易筆數達 63.7 億筆，較 2023 年成長 52%，已成為民眾日常交易之主要工具。

然而，依據巴西央行統計，2024 年 Pix 詐欺發生率為每 10 萬筆交易中約 7.8 件，2025 年略降為 6 件，惟整體詐欺數量仍高居不下(圖 9)。其中，授權支付詐欺占 Pix 詐欺案件之 97%，且多數受害者為經濟弱勢族群，顯示詐欺問題具明顯社會結構性特徵。

圖 9、巴西 Pix 詐欺案件趨勢



資料來源：本次課程投影片。

(二) 防詐治理架構與關鍵措施

為應日益嚴峻之詐欺風險，巴西央行以 Pix 系統為核心，建構「安全治理架構(Governance for Security)」，結合系統設計、資訊共享、業者責任與用戶保護等措施，建立多層次防詐治理架構，並要求所有 Pix 參加單位推動下列關鍵機制：

1.特殊退款機制(Mecanismo Especial de Devolução, MED)：允許付款人於遭詐後向其所屬支付服務提供者(Payment Service Provider, PSP)申請啟動退款程序。若雙方 PSP 根據用戶通報、交易行為異常與內部風控機制判斷該筆交易具詐欺特徵，並協議進入退款流程，則收款方 PSP 須配合凍結並返還資金。2024 年 MED 申請件數約 495 萬件，其中約 31%獲得全額或部分退款，至 2025 年比例升至 40%，顯示其執行成效逐步提升。

2.集中式詐欺資料庫：由巴西央行建置並營運，彙整參加單位回報之詐欺資料，並供各金融機構用於內部交易授權與攔阻決策，實現跨機構風險資訊共享與交叉比對，以提升交易監控與異常偵測能力。

3.交易限額與裝置控管：為提升交易風險管理彈性，Pix 系統允許金融機構依據不同情境(如夜間時段、異常行為模式或新設備登入)設定個別用戶之交易上限，作為識別高風險交易並即時控管金額風險之手段；另自 2024 年起，單筆超過 200 巴西幣(BRL)之交易，若透過新裝置或未完成登錄之裝置操作，須先完成裝置綁定程序，作為防範帳戶遭非法使用之額外驗證機制，有效攔阻詐騙者透過陌生設備進行中小額詐騙轉帳。

4.帳戶資訊揭露與雙向確認：交易授權前，系統將提示受款方姓名與稅號，提升用戶對轉帳對象之辨識能力；此外，系統允許付款方金融機構於交易發起後保留一定緩衝時間(30-60 分鐘)，以執行異常行為偵測與詐欺風險評估，俾利於必要時攔阻或延後可疑交易。

5.詐欺帳戶凍結與限制措施：規範所有參加單位須主動阻斷與高風險或疑似詐欺帳戶相關之收付款行為，避免可疑帳戶繼續進行資金收受或轉出交易，強化預防性控管機制，並強制刪除其所登記的 Pix 別名[13](alias)，防止詐

[13] 係指以手機號碼、電子郵件地址、稅務識別號碼、字串等識別資訊取代銀行帳戶(如銀行名稱、銀行分行、銀行帳號)資料，進行支付。

欺者重複使用身分。

6.政策制定與業者參與：設立「安全策略小組(GE-SEG)」，作為巴西央行與金融機構定期檢討防詐對策與強化防詐機制實施成效之平台。

整體而言，巴西以中央銀行主導方式建立自上而下的防詐治理模式，Pix 系統在設計階段即納入多項防詐機制，並持續強化各項功能，包含即將於 2026 年上線之「MED 2.0」，將可追溯詐欺資金之後續流向並執行跨帳戶凍結[14]，提升詐欺資金追回率。

惟在實務執行層面，防詐機制仍面臨中小型金融機構風控能力與資源配置不均、用戶防詐意識薄弱，以及詐欺手法不斷演化等挑戰，需仰賴業者強化即時偵測能力並導入 AI 技術應用。未來若能同步推動用戶教育、資訊透明與防詐技術創新，將有助於提升支付體系整體之安全性與公信力。

伍、 心得及建議

一、 心得

(一) 國際間支付系統採行共通訊息格式可提升跨境支付處理效率

ISO 20022 格式具備結構化資料欄位，能承載更完整之付款與交易資訊，有助於提升支付流程之追蹤能力、減少人工介

[14] Pix 系統原有之 MED 機制雖已具備詐欺退款功能，惟其僅能針對第一層收款帳戶執行資金凍結與退還，對於已透過人頭帳戶分散之資金仍難以追討。為強化詐欺交易資金之跨帳戶與跨機構追蹤能力，MED 2.0 將擴大可追溯範圍，允許金融機構於資金流出第一層詐欺帳戶後，持續追蹤其後續流向並執行凍結處理。

入與錯誤，並支援更複雜之業務需求，亦可作為監理機關與金融機構風險辨識與交易監控之工具。

為提升全球跨境支付效率，各國正積極探索即時支付系統之跨境互連模式，因此，CPMI 倡導各國一致採用 ISO 20022 國際標準，以提升資料可讀性與結構化程度，增進系統間之技術整合效率與連結可行性，進而促進全球快捷且安全之跨境支付發展。

Fed 亦規劃自 2025 年 7 月起將 Fedwire 資金服務系統轉換為 ISO 20022 訊息格式，藉以提升資料標準化程度、交易資訊透明度及自動化處理能力。而目前我國同資系統採專屬訊息規格，外幣結算平台則已配合 SWIFT 規劃時程，於 114 年 6 月將電文格式轉換為 ISO 20022 國際標準。

(二) 各國逐步建立支付系統防詐機制與監管作為

隨著即時支付系統快速發展與跨境資金流動日益頻繁，各國面臨之詐欺風險亦日趨嚴峻，跨境支付互連所涉及之詐欺防制成為國際關注重點之一。本次課程中美國、泰國、印度與巴西等央行代表均分享其近期詐欺趨勢與應對策略，顯示即時支付系統之防詐機制已由事後補救導向交易前預防。各國普遍推動在系統設計階段即納入相關控管機制，包括設定交易金額與筆數上限、導入異常帳戶管理與黑名單控管、建立可疑交易即時攔阻規則等，並透過建置資料集中平台及跨機構資訊共享架構，以強化風險辨識與應變能力。此外，部分國家亦逐步建立強制退款或補償處理機制，以提供受害用戶一定程度之救濟，

顯示提升用戶保障與強化支付安全已成為即時支付制度設計之重要趨勢。

二、建議

(一) 持續關注國際間支付系統現代化發展，並強化我國支付基礎設施之營運韌性與標準化程度

隨著全球即時支付系統加速建置，各國央行普遍重視提升支付系統之處理效率、資訊透明度與整體營運韌性。本行應持續關注主要央行與國際組織在資料標準化(如 ISO 20022)、備援設計及安全控管等方面之最新進展，俾利據以評估制度調整或技術引入之可行性。

以 Fed 為例，為協助參加單位因應內部系統異常，Fed 於 2025 年推出「FedPayments Manager – Funds Contingency Service」，提供以檔案匯入方式進行批次支付之替代機制，作為主要連線異常時之備援處理機制，有助於降低重要交易中斷風險，強化系統整體韌性。目前本行已有連線異常應變作業(包括離線媒體轉帳及支票轉帳)，以因應參加單位電腦設備故障或線路中斷之情形。未來我國如規劃導入新支付系統備援機制，亦可參考其處理架構、標準化資料格式及參加者支援機制，逐步強化支付基礎設施之穩定性。

(二) 持續關注國際間即時支付系統防詐機制與監管作為，作為未來我國建構安全有效率之支付服務

各國為因應即時支付系統快速發展所衍生之詐欺風險，已

逐步建立支付系統防詐機制與監管作為，美國、巴西、泰國、印度等國在本次課程中，就異常帳戶管理、跨機構黑名單共享、可疑交易即時攔阻、統一退款流程與補償標準、資料集中與共享平台建置等，分享其各自發展經驗，值得有意建構防詐機制的其他國家借鏡。

目前我國已由財金公司配合政府打詐政策，完成金融阻詐聯防平台之規劃，預計陸續建置同業查詢與照會機制、聯防廣播、前期金流查詢及金流履歷等功能，另由金管會督導金融機構強化支付交易之風險控管，包含推動虛擬帳號查詢平台及建置異常交易預警與灰名單通報機制，以發揮即時攔阻不法金流之效，提升支付詐騙防制成效。相關單位應持續關注國際間發展情形，適時將其納入我國建構安全效率支付服務之參考，俾強化安全控管機制，以提升我國防詐聯防基礎，將有助於建立更為健全且具韌性之支付安全治理架構。

參考資料

1. 本次 Payment 課程投影片(2025)。
2. 鄭暐霖(2024)。〈參加美國紐約聯邦準備銀行舉辦之「支付」課程報告〉。中央銀行。
3. NCLC, National Community Reinvestment Coalition (NCRC), and National Consumers League (NCL) (2021), “Comments on Proposed Rules for the FedNow Service under Regulation J, Docket No. R-1750,” September
4. Bank of Thailand (2023), “The Bank of Thailand issues additional measures to combat financial fraudulent activities,” March
5. Tilleke & Gibbins (2025), “Bank of Thailand Releases Draft Guidelines for Digital Fraud Management,” March