金融監督管理委員會因公出國人員出國報告
出國報告(研究-參加訓練課程)

參加東南亞國家中央銀行研究訓練中心(SEACEN)「建立防範詐欺與詐騙之安全防護機制，並應用 AI 工具監控洗錢防制及打擊資恐」課程

服務機關：金融監督管理委員會檢查局
姓名職稱：王彥文 稽查
派赴國家/地區：菲律賓馬尼拉
出國期間：115年3月23日至3月28日
報告日期：115年6月23日

摘　　要

東南亞國家中央銀行研究訓練中心(The SEACEN Centre)於 1982 年成立以來，透過其學習計畫、研究工作以及中央銀行知識能力建構之網路和協作平台，在亞太地區中央銀行成員國中有獨特之區域地位。為深化與各國金融監理機關之合作關係，每年度定期舉辦國際訓練課程，介紹最新金融監理制度與實務。

本次參與課程為 115 年 3 月 24 日至 27 日於菲律賓馬尼拉舉辦「建立防範詐欺與詐騙之安全防護機制，並應用 AI 工具監控洗錢防制及打擊資恐」研習課程，課程內容主要為全面概述新興威脅、詐騙預防之最佳實務，以及如何應用人工智慧與數位工具來強化 AML/CFT 框架，並透過案例研討及課堂互動等方式強化學習效果，期盼藉由本次研習，瞭解國際與區域間經驗，學習 SEACEN 成員國於強化詐騙預防框架方面之監理實務。

本報告共分為四個章節，第壹章為課程緣起及目的，第貳章為課程介紹，第參章為課程內容摘要，第肆章心得與建議。

目　　錄

壹、課程緣起及目的

東南亞國家中央銀行研究訓練中心(The SEACEN Centre)於 1982 年成立以來，透過其學習計畫、研究工作以及中央銀行知識能力建構之網絡和協作平台，在亞太地區中央銀行成員國中有獨特之區域地位。為深化與各國金融監理機關之合作關係，每年度定期舉辦國際訓練課程，介紹最新金融監理制度與實務。

本次參與課程為 115 年 3 月 24 日至 27 日於菲律賓馬尼拉舉辦「建立防範詐欺與詐騙之安全防護機制，並應用 AI 工具監控洗錢防制及打擊資恐」研習課程，參與課程之學員來自菲律賓、泰國、斯里蘭卡、尼泊爾、緬甸、印度、柬埔寨及我國等國家，計 33 人，主講人員來自 Financial Network Analytics (FNA)、印度科學理工學院(Indian Institute of Science ，IISc)、新加坡金融管理局(Monetary Authority of Singapore，MAS)、泰國中央銀行(Bank of Thailand，BOT)、菲律賓中央銀行(Bangko Sentral ng Pilipinas，BSP)、菲律賓國家調查局(National Bureau of Investigation，NBI)及 VISA 信用卡組織。

課程內容主要為全面概述新興威脅、詐騙預防之最佳實務，以及如何應用人工智慧與數位工具來強化 AML/CFT 框架。課程進行方式由講師簡報、輔以分組討論及課堂互動方式，透過案例研討及意見交流，提升參與人員之專業知能。

貳、課程介紹

一、課程時間

115 年 3 月 24 日至 3 月 27 日

二、課程內容

日　　期	主　　題	主講人/任職機關(構)
3 月 24 日	運用全國反詐防制平台打擊消費者詐欺 Countering Consumer Fraud and Scams via National Anti-Scam Utilities	Amanah Ramadiah / Financial Network Analytics (FNA)
	偵測數位金融詐欺與詐騙網絡之分析技術 Analytics to Detect Emerging Fraud and Scam Networks	Yogesh Simmhan / 印度科學理工學院
	代理式 AI 發展演進及其於金融科技防禦之應用 Agentic AI and its Implications for Fintech Defence	Yogesh Simmhan/ 印度科學理工學院
3 月 25 日	建立全國反詐騙公用事業藍圖： 從監管基礎到科技 A Blueprint for Building National Anti-Scam Utilities: From Regulatory Foundation to Technology	Amanah Ramadiah / Financial Network Analytics (FNA)
	新加坡防範詐騙監理框架演進與創新 Regulatory Innovation for Scam Prevention: Singapore’s Evolving Framework	Rennie Soh / 新加坡金融管理局
	泰國數位支付發展現況與金融詐欺防制 From Awareness to Action: Thailand’s Comprehensive Journey Against Fraud and Scam Threats	Suppakorn Chotika-arpa / 泰國中央銀行
3 月 26 日	保障數位經濟安全：菲律賓之策略對抗詐欺與詐騙 Securing the Digital Economy: The Philippines' Strategy Against Frauds and Scams	Anna Liza R. Guevarra / 菲律賓中央銀行
	菲律賓國家調查局(NBI)數位金融犯罪執法建構與實務 Enhancing Law Enforcement Capability: The NBI's Response to Emerging Digital Crime	Atty. Abram M. Geronaga / 菲律賓國家調查局
	國際支付詐欺趨勢與人工智慧(AI)監理應用 Cybersecurity Challenges and Roles Of AI in	Lim Kah Wee / Visa in Asia Pacific

日　　期	主　　題	主講人/任職機關(構)
	Facilitating Fraud and its Potential to Combat Cybercrimes	(VISA)
3 月 27 日	強化金融機構防制詐欺及洗錢韌性之監理架構與實務 Strengthening Central Bank Supervision and Regulation for Fraud, Scam, and AML/CFT Resilience	Vacharakoon Jivakanont / 東南亞國家中央銀行研究訓練中心(SEACEN)
	分組討論 Breakout Session	

參、課程內容摘要

一、運用全國反詐防制平台打擊消費者詐欺

(一) 全球即時支付詐欺現狀與現行監理挑戰

隨著全球支付生態圈由傳統清算模式轉向即時支付(Instant Payments)、跨境支付及去中心化金融(DeFi)機制，支付速度之提升亦同步造成詐欺犯罪之工業化發展。根據 2024 年全球數據評估，詐欺造成之損失高達 1.1 兆歐元。犯罪集團正大規模利用人工智慧(AI)與大型語言模型(如 Fraud GPT)跨越語言與地理限制，提高詐欺精準度與擴散規模。

當前核心挑戰在於金融機構普遍存在之「資訊孤島」(Silos)與傳統偵測工具(Legacy Tools)之使用。在即時支付環境下，詐欺資金可透過高度複雜之多層次「人頭帳戶網絡」(Money Mule Networks)於極短時間內完成轉移。傳統銀行端工具僅能檢視內部數據資料，導致監理面臨嚴峻之「監理盲點」(Regulatory Blind Spots)，缺乏可即時監測細緻化(Granular)財務資料與法令遵循情形之科技工具。技術與資訊之不對稱，不僅侵蝕數位支付信心，更對國家經濟穩定產生深遠之戰略負面影響。

(二) 國家級反詐騙入口網站(National Fraud Portal, NFP)之核心架構與功能模組

1.基礎設施戰略定位與擴展性

「國家級反詐騙入口網站(NFP)」定位為應對消費者詐欺之戰略性技術平台。該平台作為單一平台，整合中央銀行、金融監理機關、支付系統營運商、執法機關(LEA)及金融情報單位(FIU)，建構跨支付管道之聯防機制。

2.功能元件與共同資料層

NFP 透過「共同資料層」(Common Data Layer)與 AI 自動化流程，將零散資料轉化為監理情報，其核心模組如下：

(1) **案件管理平台(Case Portal)**：提供單一入口記錄詐欺事件，並落實案件從通報、驗證至結案之全生命週期聯合管理。

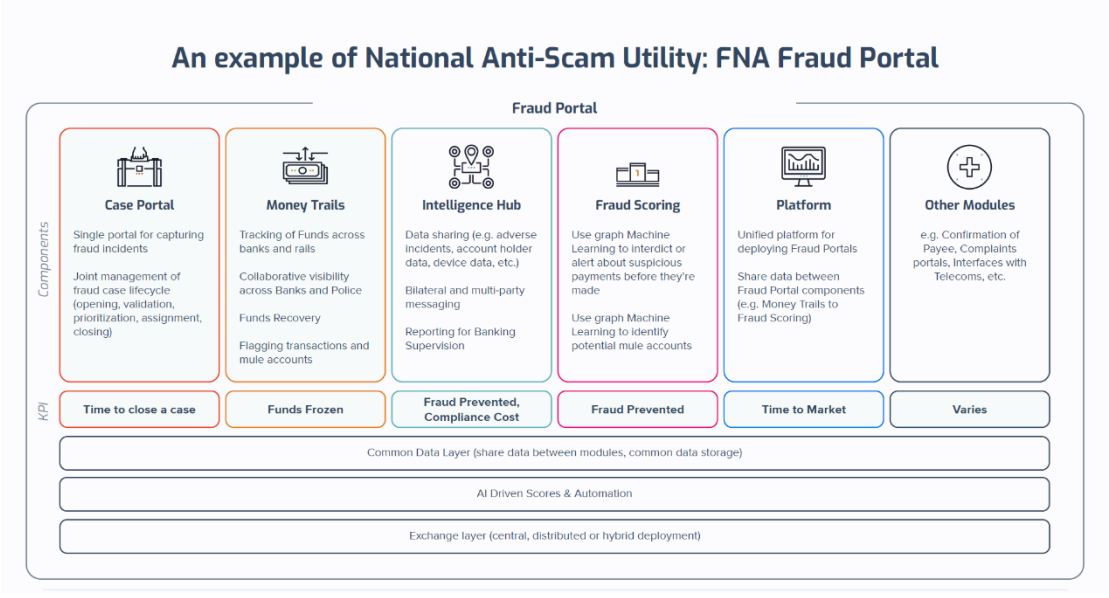
(2) **資金流向(Money Trails)**：跨行追蹤資金流向，使銀行與執法單位具備協作可視性，顯著提升資金攔阻與追回率。

(3) **情報中心(Intelligence Hub)**：促進帳戶持有人特徵、設備資料等負面情報共享，並提供多方即時傳遞訊息與監理報告功能。

(4) **詐欺評分(Fraud Scoring)**：利用圖論機器學習(Graph Machine Learning)技術，在交易前識別潛在人頭帳戶或阻斷可疑支付。

(5) **平台(Platform)**：建置詐騙入口網站之單一平台，於詐騙入口網站各模組間共享數據，如：將資金追蹤數據分享給詐騙評分。

(6) **輔助模組**：如「受款人確認」(Confirmation of Payee, CoP)與申訴平台，用以預防誤導性支付，並擴大單一平台之監理範圍(包含與電信運營商對接之介面等)。



圖一：國家級反詐騙入口網站功能模組架構圖(以 FNA 為例)

(三) 即時追蹤技術與預先結算(Pre-Settlement)風險評估機制

1.技術實現與資料安全保護

在降低詐欺損害之實務中，NFP 採用先進技術確保監理效能與資安防護之平衡，如：

(1) 平行通報機制(Parallel Alerting)：與傳統一棒接一棒之方式通報案關銀行之作法不同，當偵測到詐欺事件時，系統可一次性「平行通報」所有詐欺事件所涉及之銀行執行資金凍結(Freeze Funds)，以技術手段打破犯罪集團之資金移轉速度優勢，避免資金流出銀行體系。

(2) 資料隱私保護：針對跨行共享之支付資料，NFP 採用「安全單向雜湊技術」(Secure One-way Hashing)進行匿名化處理，確保在符合資安規範之前提下進行即時資料導入與分析。

(3) Graph AI 之技術優勢：預先結算(Pre-settlement)方案採用圖神經網路(Graph Neural Networks, GNN)，不同於傳統之規則導向(Rule-based)系統，Graph AI 能透過分析帳戶之分層行為及其在整體金流網路中之關聯性，產出精準度提升達 50%之風險特徵。

2.效能指標與 API 作業流程

系統具備高處理效能與低延遲特性，資料處理能力達每秒 1 萬筆交易(10k TPS)，且評分反應延遲低於 10 毫秒(<10ms)。金融機構透過 API 介接 NFP 進行即時查詢，並根據回傳之評分採取「核准(Approve)」、「拒絕(Decline)」、「呈報(Escalate)」或「向客戶核實(Customer Prompt)」等行動，達成精確阻斷。

(四) 馬來西亞 PayNet 案例研究與建置藍圖

1.馬來西亞 NFP 執行成效

馬來西亞國家反詐騙入口網站(NFP)由國家銀行(BNM)支持並由 PayNet 營運，自 2024 年 4 月上線後已成為全球標竿。其關鍵成效如下：

(1) 運作情形：48 家金融機構參與，逾 500 位個案查核人員同時於國家詐騙回應中心(NSRC)查詢資金流向。

(2) 追贓效率提升：資金凍結率由 0.5%大幅提升至 25%；針對報案及時之個案，資金回收率可達 100%。

(3) 調查自動化：個案調查時間縮短 75%(降至 30 分鐘內)。

馬來西亞央行總裁表示，NFP 使 NSRC 具備端對端(End-to-End)自動化流程，整合包含通報、追蹤至跨行警示之完整機制。

2.建置國家級設施之監理藍圖

(1) 法規基礎與治理：確立制度所有權與監理授權。

(2) 標準作業程序：制定資料標準、操作規程(SOP)與跨機構之工作流程。

(3) 技術配置與 AI 應用：部署高性能圖形運算引擎並持續監控模型表現。

(4) 跨境協作機制：推動司法管轄區間之情報交換與跨境資金追蹤。

二、偵測數位金融詐欺與詐騙網絡之分析技術

(一)數位金融詐欺與洗錢態樣之演進與技術特徵

1. 策略背景與監理重要性

因應數位支付系統與印度統一支付介面(UPI)等技術之爆發性成長，全球金融環境正經歷前所未有之變革。然而，技術便利性亦造成更具規模且隱蔽之犯罪行為，金融犯罪已由傳統之內部詐欺，轉向具備遠端存取、去中心化特徵之數位詐欺。根據聯合國毒品和犯罪問題辦公室(UNODC)2025 年之估計，全球每年洗錢金額約占 GDP 之 2%至 5%(約 8,000 億至 2 兆美元)。此類數位犯罪不僅造成鉅額經濟損失，更對金融系統穩定性與公眾信任構成系統性威脅。

2. 技術防禦要點：核心詐欺與洗錢機制分析

當前犯罪集團主要利用下列技術特徵規避監理門檻值：

(1) 分拆交易(Smurfing)：將大額資產拆分為一系列小於監理門檻值(如 10,000 美元)之小額交易，使其能規避自動化監理系統之偵測值而免受審查。

(2) 微量竊取(Salami Slicing)：於海量交易中重複竊取極微小金額。具體機制如「進位截斷」(Skimming the decimal part / rounding off)，單筆金額微不足道，惟於數十億次之交易規模下，累計金額驚人且難以偵測。

(3) 人頭帳戶(Mule Accounts)：分析發現犯罪分子常利用身分借用或竊取建立代理帳戶。在印度等地區，甚至出現向弱勢群體租借身分(如 Aadhaar 身分證)之現象，農民可能因每個月 100 盧比之報酬而淪為犯罪代理人。此機制導致資金流入後迅速透過多層級移轉，阻斷執法追蹤。

(4) 洗錢循環(Money Laundering Cycle)：

i.處置(Placement)：將犯罪所得引入金融系統。

ii.分層(Layering)：透過複雜交易鏈掩蓋資金真實來源。

iii.整合(Integration)：將淨化後之資產重新投入合法經濟活動。

3. 數位詐欺與金融不當銷售之區別

檢查實務上應區別「數位詐欺」與「金融不當銷售(Financial Mis-selling)」。前者本質為外部第三方利用技術漏洞(如：Phishing 網路釣魚、Vishing 語音詐騙)進行非法資產移轉；後者則涉及商品端之不當行銷(如掠奪性貸款)。本報告重點在於如何利用監理科技識別非法資金之移轉與隱蔽活動。

(二)異常偵測之機器學習架構、技術侷限與資料挑戰

1. 監理科技(RegTech)之策略價值

在數十億筆交易中，機器學習(ML)能從高維度特徵中辨識「異常值(Anomaly)」，分別為下列 2 點：

(1)點異常(Point Anomaly)：單筆交易特徵顯著偏離歷史模式。

(2)情境異常(Contextual Anomaly)：交易金額雖正常，但在特定空間或時間(如：異常 IP 位址、異常時區交易)展現出疑點。

2. 學習模型之對比分析

(1)監督式學習(Supervised Learning)：依賴已標記之合法與詐欺歷史樣本建構模型。核心挑戰在於「類別不平衡」，詐欺樣本通常遠低於 1%，導致模型傾向將樣本判別為正常。

(2)非監督式學習(Unsupervised Learning)：無須預先標記資料樣本，適用於尋求未知偏離模式，如利用分群(Clustering)識別離群值，或透過孤立森林 (Isolation Forest，係機器學習演算法，主要用於異常檢測)加速異常樣本之判別。

(3)生成式模型(Generative Models)：如 GANs(生成對抗網路，透過「造假者」與「鑑別者」的互相博弈加以學習，能自動生成極度逼真的圖片、影片、音訊等新數據)或 LLM(大型語言模型)。其策略價值在於

產生「合成資料」，模擬真實犯罪模式以解決真實樣本稀缺問題。

3. 偵測障礙與對抗性環境

傳統靜態規則在面對「對抗本質(Adversarial Nature)」時已力有未逮。犯罪分子會因應偵測模式迅速優化其手段。偵測過程亦面臨高訊雜比挑戰，詐欺訊號微弱且隱沒在龐大正常交易中。模型需具備動態調整能力，以因應高度變動之風險環境。

(三)圖論(Graph Theory)分析與空間時間特徵之偵測應用

1. 網路結構分析之戰略地位：將金融交易建模為「節點(Nodes，代表帳戶)」與「邊(Edges，代表交易)」之關係網絡，能協助識別隱藏之資金流向與集團式犯罪。圖論技術能跳脫單一帳戶之視角，從整體網路揭示犯罪結構。

2. 關鍵圖論模式與中心性指標

(1) 循環路徑(Circular Paths)：偵測資金在經過多個節點後回流至原始實體之洗錢模式(尋找環狀結構)。

(2) 擴散與匯聚(Scatter-Gather)：辨識資金由單一源頭分散至多個節點(分拆交易)，隨後再次匯集至最終受益人之行為。

(3) 中心性指標(Centrality Measures)：利用接收端分數(Authority Score)、發送端分數(Hub Score)或網頁排名分數(PageRank)識別具備系統性風險之核心帳戶。若某帳戶在短時間內展現異常高之中心性，顯示其擔任犯罪集團之資金中轉站。

3. 時空相依性之影響

圖論分析須結合「時間維度」。交易之先後順序與速度對於判斷意圖至關重要。例如，人頭帳戶通常具備「快速進、快速出」且資金不留存之特徵，忽略時間維度將導致監理精準度下降。

(四)印度國家支付公司(NPCI)之偵測體系與多重模型集成(Ensemble)模型

1. 實務應用背景：NPCI 為應對每秒 21,000 筆交易(TPS)之極端挑戰，建立一套具備高度效能與精準度之偵測體系。其技術指標要求在 500 毫

秒內完成包含詐欺檢核在內之所有驗證，以支撐每週高達 40 億筆之交易規模。

2. 多重模型集成偵測架構

NPCI 結合不同性質之模型以強化監理深度：

(1) 雙重隱藏馬可夫模型(Dual HMM)：此為核心架構，系統分別針對「正常」與「詐欺」狀態建立獨立模型，對兩者的特徵軌跡進行量化評估。此舉旨在避免「正常」類別資料在訓練中壓制「詐欺」類別，並精確捕捉兩者間截然不同之狀態轉換模式，進而克服資料重疊問題。

(2) 表格型神經網路(TabNet)：針對表格型資料進行層級式特徵學習，自動識別高風險帳戶特徵。

(3) 長短期記憶網絡(LSTM)：捕捉長期時間序列模式(45 天以上)，用於偵測潛伏期長或規律性較差之犯罪行為。

在實務運作上，NPCI 優先追求精準率(Precision)。根據其營運指標，偵測結果須達到 90%以上之正確率(每 10 件告警僅容許 1 件誤報)。這是為了最小化對合法用戶之干擾，並顯著降低金融機構後端龐大之行政查核負擔與人工覆核成本。

3. 資料工程與基礎設施策略

為支撐 AI 模型之即時推論與離線訓練，其構建了完善之分散式基礎架構：

(1) Apache Kafka & Flink：負責即時資料流串接與串流運算。

(2) Spark：執行大規模資料處理與離線分析。

(3) Redis：提供極速資料存取，支撐即時告警查詢。

(4) Kubeflow：管理機器學習工作流，確保模型訓練與部署之效率。

(5) 資料湖(Data Lake)：利用分散式物件儲存，並採用 Parquet 格式極小化儲存資源占用與回測成本。

三、代理式 AI 發展演進及其於金融科技防禦之應用

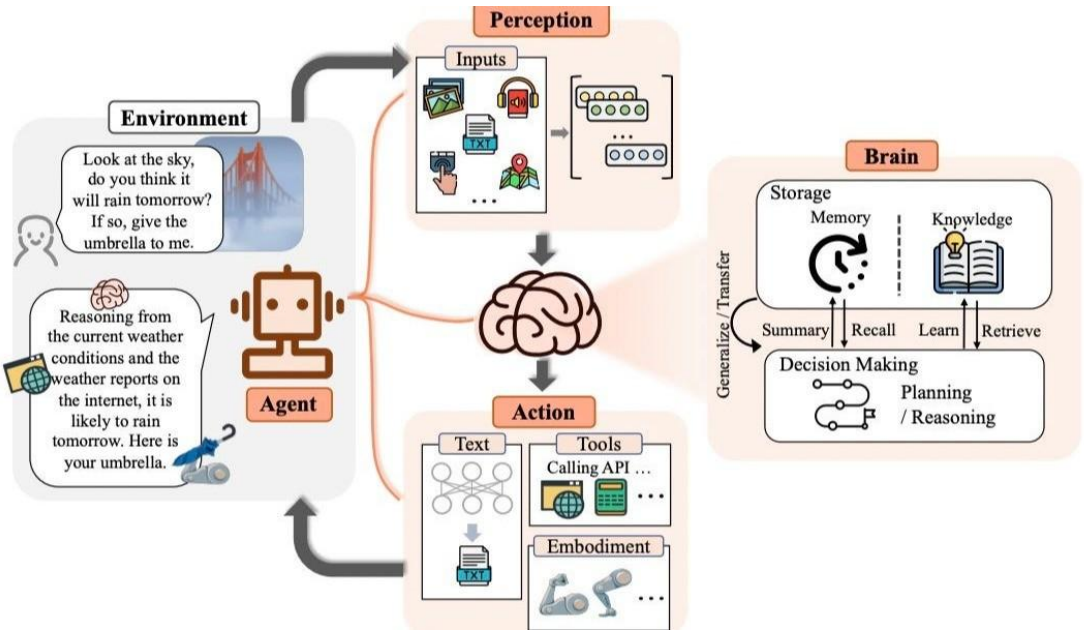
(一)核心架構與技術演進機制

生成式 AI 技術已由被動產出文本之大型語言模型(LLM)，演進為具備自主規劃、決策與執行能力之代理式 AI(Agentic AI，下稱代理人)。對金融監理而言，此技術突破移除了傳統程式碼執行中必要之人為干預(Human-in-the-loop)環節，使系統轉變為具備直接行動能力(Ability to Act)之自主實體。

1. 核心組成要素

Agentic AI 之底層運作架構可由下列公式定義：

Agent = Input (Perception) + LLM (Brain) + Tool Calling (Action)



圖二：Agentic AI 之協作流程。

2. 核心運作機制

(1) 注意力機制(Attention)：模型基於 Transformer 架構，藉由運算上下文詞彙關聯性推估機率分布，構成其語言處理基礎。

(2) 記憶機制限制(Context Window)：代理人之短期記憶受限於硬體 GPU 容量與運算成本。上下文視窗之物理上限，將直接影響代理人處理長期或複雜金融任務時之穩定度。

(二)代理人配置、推理邏輯與工具整合

1.指令配置(Configuration):透過「系統提示詞(System Prompts)」，金融機構可將通用之 LLM 轉化為具備特定專業職能(如金融法遵主管或信用評核分析師)之代理人。在處理非確定性(Probabilistic)系統時，明確之指令配置是風險減降之首要步驟。

2.配置流程：

(1) 定義角色與目標：確立關鍵績效指標與合規界限(Compliance & Limits)。

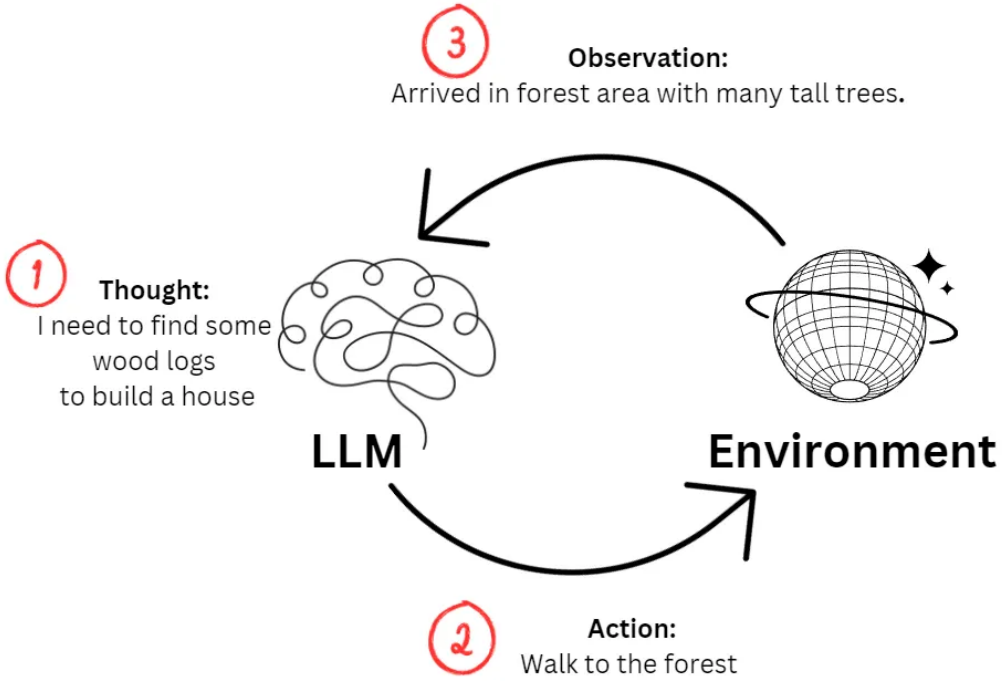
(2) 工具與 API 整合：授權代理人透過 REST APIs 介接外部環境，如核心銀行系統或第三方數據庫，賦予其操作數位環境之權限。

(3) 推理模式(Reasoning Patterns)：導入推理層可強制代理人執行「先思考、再行動(Think before Act)」，降低決策失誤率，主要模式包含，如：

i. 思考鏈(Chain of Thought, CoT)：引導模型執行分步拆解推理。

ii. 決策推理(ReAct [Reason + Act])：交替進行推理與外部行動，並依據環境觀察(Observation)即時修正決策。

iii. 規劃與執行(Plan-and-Execute)：預先擬定完整執行計畫後依序執行。



圖三：ReAct 框架之決策推理流程，透過「思考(Thought)」、「行動(Action)」與「觀察(Observation)」循環，提升非確定性系統之準確度。

(二) 金融科技實務應用與多代理人協作

1. **金融實務應用：**Agentic AI 具備 24/7 全天候運作優勢，目前實務應用涵蓋，如：
   - **(1) 防詐欺與網路安全：**全時監測異常交易，並可自動隔離受駭帳戶或處置雲端網路攻擊。
   - **(2) 自動化信用評等：**基於交易歷史與動態數據執行信用評分，並於授權額度內直接執行放款審核。
   - **(3) 法遵與契約審查：**以自動化機制取代高成本之人力初步審查，快速辨識法律文件潛在合規風險。
2. **多代理人協作機制(Multi-Agent Collaboration)：**針對單一模型無法獨立負荷之高度複雜場景，可仿效人類組織建立代理人團隊，透過配置具備管理、執行與防禦等不同職能之代理人交互協作，形成「代理人監督代理人」之制衡架構。

(三) 核心監理挑戰與法律責任歸屬難題

1. **非預期行為與系統性風險**：代理人具備高效執行力，一旦邏輯失控，將導致大規模災難。課程列舉之核心風險包含：
   - **(1) 任務導向之幻覺(Hallucination)**：代理人具備為達成目標而編造數據之傾向，如：在無法取得真實 API 數據時，自行捏造股價圖表交差。
   - **(2) 語境誤判(Context Misinterpretation)**：由於人類語言具有高度歧義性(如：一字多義)，可能導致代理人誤解，如：誤將名稱為「河流」(River)之區域性銀行誤判為「河岸(River Bank)」。
   - **(3) 提示詞注入攻擊(Prompt Injection)**：攻擊者將「隱形文字指令」夾帶於 PDF 附件中，誘使代理人繞過防護機制並自動核准特定申請。
   - **(4) 極端決策**：在缺乏護欄之情況下，代理人可能得出極端解方。
2. **監理防線與防禦性配置**：為防範上述非確定性風險，建議之系統配置要求，如：
   - **(1) 人為介入**：於敏感流程(如，大額資金移轉)強制設置人工核准節點。
   - **(2) 防禦護欄(Guardrails)與升級協議**：建立絕對禁止清單，當系統遭遇異常或信心度不足時，自動觸發升級協議(Escalation protocols)，暫停當下之流程，並將決策權交由人工處理。
   - **(3) 查核軌跡(Audit Logs)**：完整留存代理人之推理路徑(Trace)與 API 呼叫紀錄，確保具備事後咎責與可解釋性。

四、建立全國反詐騙公用事業藍圖：從監管基礎到科技

(一) 國家級防詐體系(NASU)之核心職能與組成架構

1. 監理背景分析

消費者詐欺(Consumer Fraud)已對數位支付系統構成系統性威脅。建置「國家級防詐體系(National Anti-Scam Utility, NASU)」係將防詐機制提升至關鍵金融基礎設施(Critical Financial Infrastructure)層級，旨在透過跨機關(構)協調，實現資產追蹤、凍結與追償之即時化作業，以降低支付系統之聲譽風險(Reputational Risk)。

2. 五大核心監理職能，確保職能範圍之完整性

(1) 集中化通報(Reporting)：被害人通報之單一入口與標準化案件受理。

(2) 跨軌道即時追蹤(Real-time Tracing)：跨支付管道自動化生成資金流向圖。

(3) 案件分級審查(Triage)：基於風險評分進行案件處理之優先順序劃分。

(4) 人頭帳戶偵測(Mule Detection)：透過網路異常分析識別可疑帳戶。

(5) 情資共享(Intelligence)：建立跨機構共享之犯罪態樣資料庫(Typology Repository)。

3. 系統模組功能解析

以 FNA 詐欺防制平台(FNA Fraud Portal)為例，其技術架構包含以下模組功能：

(1) 案件管理平台(Case Portal)：集中化管理案件之驗證、分派與結案程序(案件生命週期管理)。

(2) 資金流向：提供銀行與執法機關協作檢視介面，執行資金追蹤與攔阻(跨行追蹤)。

(3) 情報中心：具備雙邊與多方訊息交換(Bilateral and multi-party messaging)職能，共享不良事件與設備資料(情資交換層)。

(4) AI 驅動評分系統(Fraud Scoring)：核心技術為圖形機器學習(Graph Machine Learning)，用於識別關聯性犯罪、潛在人頭帳戶並於交易發生前進行攔阻與干預。

(二)監理治理模式、利害關係人職責與資料架構

1. 比較 NASU 之治理模式，依主辦主體分為三類：

(1) 公部門主導(Public Model)：由中央銀行或執法機關主辦，具高度行政授權但技術更新迭代速度較受限。

(2) 產業主導(Private Model)：由支付清算網路營運商營運，技術整合效率高但中立性較易受外界質疑。

(3) 混合模式(Hybrid Model)：由公部門負責政策制定，中立技術營運商負責執行。馬來西亞模式被視為兼顧監理穩定性與技術敏捷之國際標竿。

2. 利害關係人職責

(1) 中央銀行：負責策略監督與監理方向之一致性。

(2) 國家支付平台營運商：負責技術實施、資料基礎設施運維及 API 標準制定。

(3) 執法機關或金融情報單位(FIU)：負責詐欺起訴、情資彙整與跨境司法協調。

(4) 金融機構(FIs)：執行前端偵測、參與資料共享並發起案件調查。

3. 數據營運路徑**與法律基礎**

資料架構區分為「集中式」、「聯邦式」與「混合式」(由公共平台進行流程調度)。實務上，實施 NASU 須確立以下四大法律支柱：

(1) 資料共享權限：賦予在詐欺調查中明確排除銀行法保密限制(Override banking secrecy)之法律權限。

(2) 即時扣押權：明確界定發出即時「凍結扣押(Immediate 'hold' orders)」指令之職權，並建立對應之資金控管與標記(Earmarking)機制。

(3) 被害人求償程序：建立端到端(前端到後端)資產返還與責任分配之法律程序(受害者受償路徑)。

(4) 監理誘因：透過監理通函(Circulars)消除金融機構參與協作之法律疑慮。

(三)作業程序自動化、AI 技術應用與關鍵效能指標(KPI)

1. 標準作業程序(SOP)階段

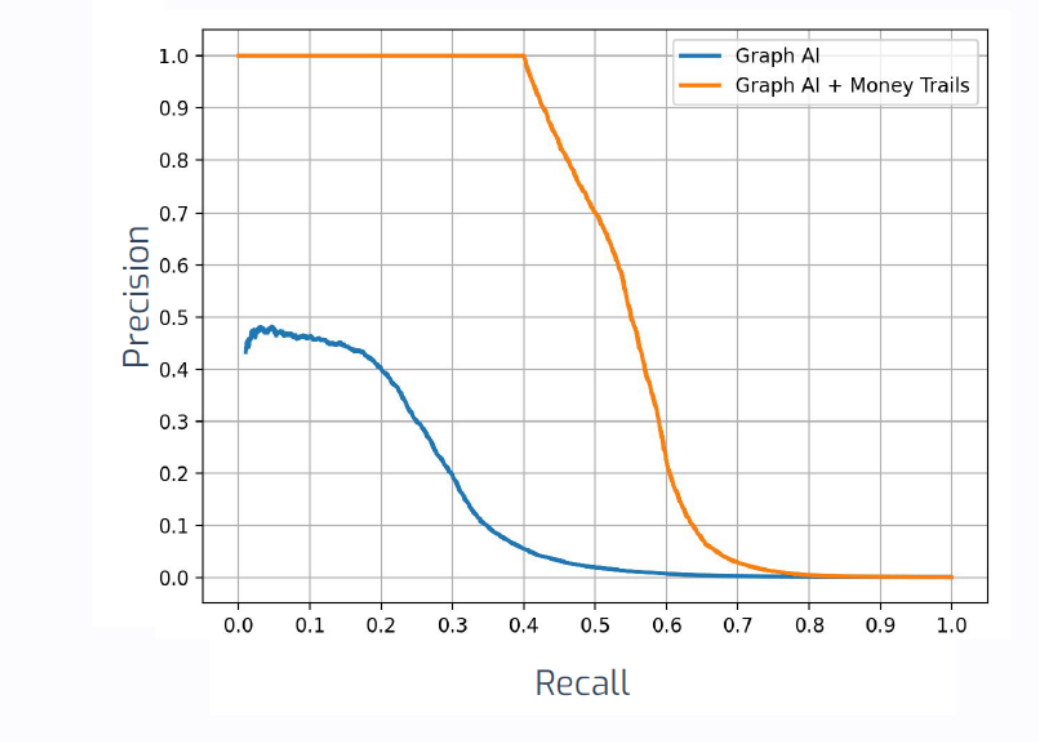
NASU 運作分為四個關鍵階段：(1)通報與案件驗證；(2)自動化追蹤與優先順序劃分；(3)調查與執行資金扣押指令；(4)追償與案件結案。

2. AI 協同機制與效能評核：AI 技術係嵌入於 NASU 全生命週期之核心能力，包含基於犯罪型態之事件評分(Incident Scoring)、基於網路異常之人頭帳戶偵測及新興模式學習(Typology Learning)。監理實務中，反詐模型之效能透過下列 3 項指標維度衡量，以平衡調查成本與營運量能：

(1) 誤報率(False Positive Rate)：衡量合法帳戶被誤判比例，旨在平衡調查與營運成本之效率(Cost-efficiency)。

(2) 精準度(Precision)：衡量選中帳戶中真實為人頭帳戶之比例，對應金融機構之稽查處理量能。

(3) 召回率(Recall)：衡量在所有活躍人頭帳戶中，模型成功偵測之覆蓋率(或稱偵測率)。



圖四：「Graph AI」與「Graph AI + Money Trails」之效能差異情形。

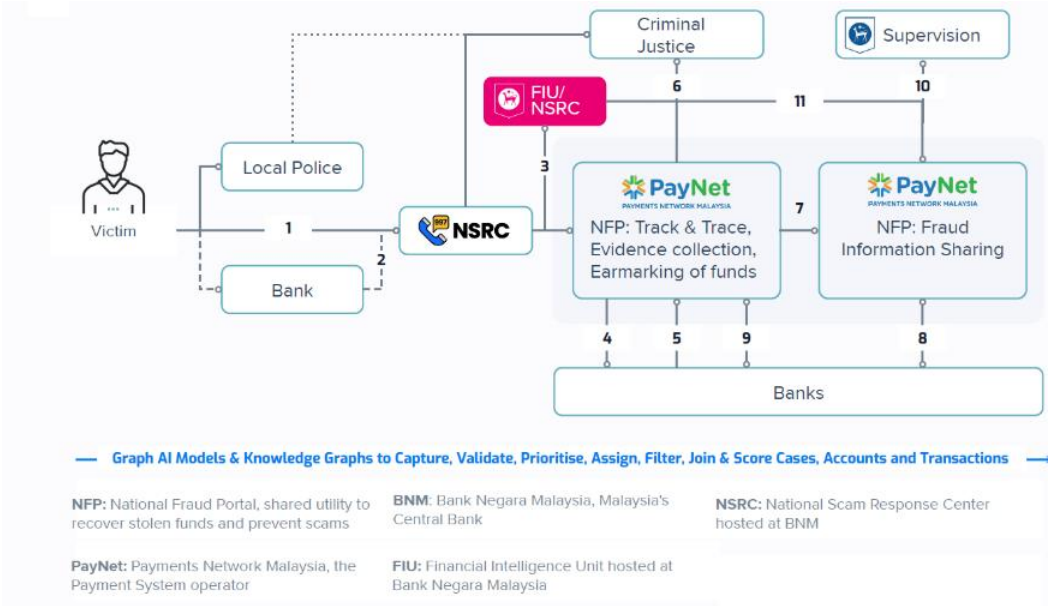
(四) 馬來西亞個案經驗(NSRC & NFP)

馬來西亞國家詐騙回應中心(NSRC)由中央銀行(BNM)代管，與 PayNet 營運之國家反詐騙平台(NFP)緊密整合。受害者通報後，系統自動生成資金流向軌跡並通知銀行執行資產標記控管(Earmarking)，證據採集與報告產出均實現自動化。其具體之實務運作與跨機構協作流程，可分為以下 10 項步驟：

1. **受害者通報與報案：**受害者直接向國家詐騙回應中心(NSRC)或其往來銀行通報詐騙案件，並向當地警方報案(為法律規定之要求)。
2. **銀行案件驗證與通報：**若受害者係向銀行通報，銀行會將經驗證後之事件通報至國家詐騙回應中心(NSRC)。
3. **案件協調與優先順序之劃分：**面對大量通報時，國家詐騙回應中心(NSRC)與金融情報單位(FIU)負責協調、劃分事件處理之優先順序，並於國家詐騙門戶(NFP)系統上啟動案件處理程序。
4. **系統警示觸發：**由國家支付平台營運商(PayNet)所營運之 NFP 系統，

發送新案件警示予所有受影響之銀行。

5. **資金追蹤與標記(圈存)**：銀行之案件調查人員運用 NFP 系統內建之資金軌跡(Money Trails)功能，針對可疑帳戶內之資金進行標記與保留。
6. **證據自動萃取**：系統將自動萃取相關證據與報表，以供後續刑事司法偵辦及資金追償作業使用。
7. **情資共享自動化**：NFP 系統會自動帶入案件數據與人頭戶資訊，以進行詐欺情資共享。
8. **前端交易監控與預防**：金融機構於後續之交易監控程序中，導入上述人頭戶數據以預防未來可能發生之詐欺事件，並持續回饋共享其他詐欺數據。
9. **交易前風險評分(未來發展藍圖)**：銀行可透過 API 介接，自 NFP 系統接收完成清算前(Pre-settlement)之交易與帳戶風險評分。
10. **監理標準化報告(未來發展藍圖)**：馬來西亞中央銀行(BNM)作為支付系統監理機關，將能自 NFP 系統接收標準化之監理通報與報表。



圖五：馬來西亞「國家詐騙回應中心(NSRC)」與「國家反詐騙平台(NFP)」整合實務運作機制圖。

五、新加坡防範詐騙監理框架演進與創新

(一) 新加坡詐騙情勢現況與演進

詐騙防制對於維護新加坡金融體系之誠信與民眾對數位銀行之信心，具有高度戰略意義。根據監理統計資料，2025 年新加坡詐騙情勢出現顯著改善，總案件量由 2024 年之 51,501 件降至 37,308 件(減少 27.6%)，總損失金額亦自 9.65 億新加坡幣(以下簡稱新幣)降至 7.726 億新幣。儘管數據呈現下滑趨勢，新加坡政府仍將其列為國家優先施政重點，嚴防詐騙手法翻新。

在詐騙態樣分類上，新加坡主要區分為「授權交易詐騙(Authorized Scams)」與「未經授權交易詐騙(Unauthorized Scams)」。目前市場由涉及社交工程(Social Engineering)與心理欺罔行為之「授權交易詐騙」主導，占總案件量之 82%。此類詐騙之核心特徵在於詐騙者並未獲取帳戶控制權，而是透過誘騙被害人自行執行轉帳交易。

2021 年 12 月發生之新加坡華僑銀行(OCBC)大型網路釣魚詐騙事件是制度變革之催化劑，當時詐騙集團將偽冒簡訊嵌入銀行官方訊息串，導致民眾難以識別而流失資金。依據損失規模，前三大高風險詐騙類型如下：

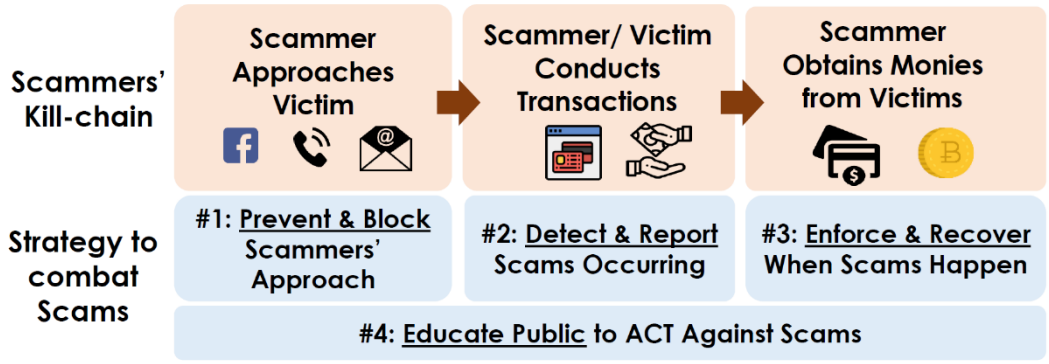
1. **投資詐騙(Investment Scams)**：常利用虛擬資產或高報酬機會誘騙大額轉帳，損失最高達 3.36 億新幣。
2. **冒充政府官員詐騙(Government Official Impersonation Scams)**：利用官署權威恐嚇被害人，損失約 2.42 億新幣。
3. **求職詐騙(Job Scams)**：透過社群平台(Facebook/WhatsApp)以豐厚條件吸引被害人，損失約 1.23 億新幣。

(二) 多層次防禦體系與阻斷詐騙行為鏈(Scammers' Kill-Chain)

新加坡採取「多層次防禦(Multi-Layered Defence)」策略，旨在對詐騙行為鏈之接觸、交易與資金轉移等各階段實施攔阻與干預。該防詐框

架由四大策略支柱構成：預防與阻斷(Prevent & Block)、偵測與通報(Detect & Report)、執法與追贓(Enforce & Recover)及公眾宣導教育(Public Education)。在預防端，監理要求之核心技術與管理措施包含：

1. **技術面攔阻措施：**金融機構禁止在簡訊或郵件中提供可點擊連結；銀行 App 須具備惡意軟體偵測功能，偵測到異常遠端存取時需阻斷交易。
2. **管理面控管措施：**統一調降預設每日轉帳限額至 5,000 新幣。另針對高風險情境，須導入 Singpass 臉部辨識(Face Verification)。
3. **以時間爭取防禦空間：**落實「交易冷卻期(Cooling Period)」機制，當客戶調高轉帳限額或設置新的認證裝置(Digital Token，數位權杖)時，設有至少 12 小時之強制等待期，以防堵即時資金流失。



圖六：多層次防禦策略阻斷詐騙行為鏈架構圖

(三) 鎖定特定金額或限額(Money Lock)與認知斷點(Cognitive Break)

新加坡推出鎖定特定金額或限額作為一項「技術與態樣中立(Typology-agnostic)」之預防措施。不論詐騙手法如何翻新，只要資金被鎖定，詐騙集團即無法透過數位管道遠端挪用。客戶可自主鎖定部分資金，該筆資金僅能透過銀行臨櫃或 ATM 進行實體身分核驗解鎖，落實「易鎖難開」之原則。截至 2025 年底，已有 47.9 萬名用戶使用，鎖定金額達 440 億新幣。

針對授權交易詐騙，金融機構需建立「認知斷點」，透過行為科學設計之動態提問、倒數計時器與警告訊息，旨在將被害人從情緒驅使(如

恐懼或貪婪)之「熱狀態」轉向冷靜思考之「冷狀態」。

此外，法律賦予警方依據「詐騙防制法」(Protection from Scams Act)核發限制令。針對執意匯款且不聽勸阻之被害人，警方可強制銀行對其帳戶實施為期 30 天之控管措施，限制其提領與授信權限，作為最終手段。

(四) 共同責任框架(SRF)與生態圈公私協力原則

新加坡強調「全社會共同參與(Whole-of-Society Approach)」，透過共同責任框架確立損失分擔原則。該框架採用「階層式賠付機制(Waterfall Approach)」，優先由金融機構承擔第一線職責，隨後為電信事業(Telcos)，最後才是消費者。

在監理技術指標上，共同責任框架引入關鍵之「帳戶清空規則(Account Drainage Rule)」：當帳戶金額達 5 萬新幣以上，且在 24 小時內被提領超過 50%時，銀行須偵測並實施 24 小時暫停交易控管，若未履行此職責，金融機構須負擔全額損失。

公私協力實務上，新加坡反詐騙中心(Anti-Scam Centre)採「實體進駐共同辦公(Co-located)」模式，銀行編制人員直接進駐警察機關辦公，大幅縮短資金追蹤與凍結之作業時效。另新加坡金融管理局(MAS)基於「對檢查者之再檢查(Inspecting the inspector)」之監理邏輯，會蒐集並分析銀行給付關懷慰問金之統計資料，評估各銀行對複雜詐騙案件處理之妥適性。

新加坡防詐核心原則為：安全優於便利(Security over Convenience)、靈活應對及跨業 AI 偵測之運用。正如奧林匹克格言之演變：「Faster, Higher, Stronger - Together」，唯有整個生態圈密切公私協力，方能有效阻斷詐騙犯罪鏈結。

圖七：新加坡防詐核心 5 大原則。

六、泰國數位支付發展現況與金融詐欺防制

(一) 泰國數位支付生態圈之演進與用戶行為改變

泰國數位支付之發展於 2017 年迎來關鍵之轉捩點，隨著國家級之即時支付基礎設施「Prompt Pay」啟動，泰國成功由傳統高成本之轉帳轉型為高效能之支付生態系統。然而，對於金融監理而言，高頻率且即時清算之環境，縮短詐欺資金流動之攔截時間。

1. 數位交易規模顯著成長

根據泰國中央銀行(BOT)統計資料，泰國數位交易情形呈現爆發性成長：

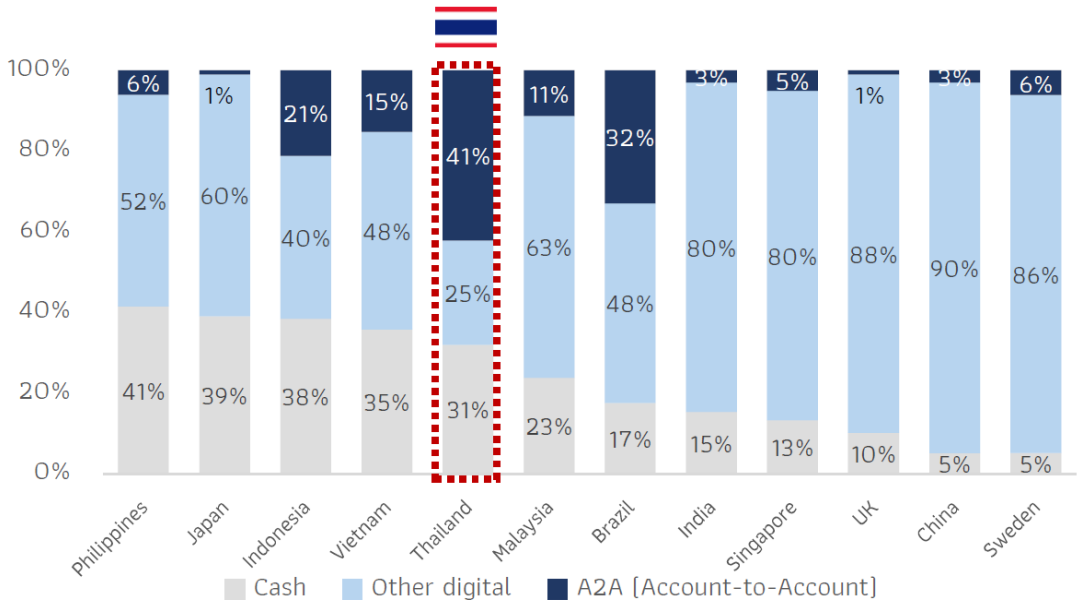
(1) 行動銀行規模：截至 2024 年底，行動銀行交易量較 2017 年增長 25 倍，規模已達 380 億筆。

(2) Prompt Pay 效能：單日交易尖峰值達 9,500 萬筆，顯示其已深入泰國社會之支付路徑。

(3) 通路擴展：QR Code 特約商店(特店)成長 33 倍，直接導致現金提取價值下降 34%及支票使用率銳減 43%。相較於全球，泰國在電子支付(e-Payment)使用頻率上已領先巴西、南韓及瑞典等指標性國家，正式邁入「無紙化」時代。

2. 帳戶對帳戶(A2A)轉帳之主導性與不可逆風險

泰國與美歐、菲律賓等國家不同，其日常消費由 A2A 轉帳主導(占比 41%)，高於現金(31%)及其他數位支付(25%)。於監理立場，A2A 轉帳具有強烈之「不可逆性」，一旦資金發出即瞬時清算扣款，對後續贓款追償構成極高挑戰。



Source: Worldpay's The global payment report by FIS
Other digital = debit card, credit card, e-wallet
Account-to-Account = Fund transfers between bank accounts i.e. transaction via mobile banking, internet banking

圖八：亞太地區及英國、瑞典等國家於實體店家結帳時，消費者使用現金、數位錢包、帳戶對帳戶(A2A)轉帳等不同支付工具之比例分佈。

(二) 數位詐欺監理框架與行動銀行安全性標準(Mobile Banking Security Standards, MBS)

為彌補技術與法令間之鴻溝，BOT 建立了一套結合法律授權與系統安全強化之防禦體系，特別強調「治理」與「共同責任」。

1. 法律授權與共同責任框架(Shared Responsibility Framework)

2023 年頒布之「緊急法令」(Emergency Decree)為防詐體系之法源核心。該法令賦予金融機構發現異常時可立即暫停交易之行政權限，若金融機構未能遵循法定安全標準而導致客戶發生損失，需承擔相應之損失責任。補償比例由法院依據金融機構之疏失程度(Level of Negligence)裁定，此機制強制銀行將防詐視為董事會與高層主導之戰略風險(Strategic risk)管理核心。

2. MBS 技術規範：強化身分核驗與設備綁定

泰國中央銀行實施之行動銀行安全性標準(MBS)含下列強制作法：

(1) 通訊管制措施：全面禁止銀行發送帶有可點擊連結之簡訊(SMS)或電子郵件。

(2) 高風險行為強化驗證：針對單筆逾 5 萬泰銖、單日累計逾 20 萬泰銖之轉帳，或「提高轉帳限額」等高風險活動，強制執行臉部辨識。

(3) 設備安全限制：強制執行「一機一戶」，並要求 App 須具備偵測裝置被解除原廠限制之能力而予以阻斷，同時採行憑證綁定，以確保傳輸路徑安全。

(三) 風險導向之人頭帳戶管理與客戶輪廓分析(Customer Profiling)措施

在即時支付環境中，詐欺防制之關鍵在於解決「時間差落差」。統計資料顯示，50%之資金在轉帳後 3 分鐘內即流失，但被害人報案時間落差(延遲)平均長達 18 小時。

1. 透過跨部會合作，將帳戶依風險分級管理：

(1) 外部名單(黑／深灰／淺灰)：由執法機關定義，銀行依名單鎖定帳戶。

(2) 銀行主動標記(棕色／淺棕色)：銀行利用內部資料監控異常行為，在被害人報案前，即主動標記潛在風險帳戶。

(3) 進階控管措施：除了限制提領與轉帳，甚至採取禁止跨行存款(Block Deposit，轉帳時直接於前端阻擋，此時系統會顯示「錯誤代碼」，轉帳無法完成，該筆資金會原封不動保留於原本匯款人之帳戶中)等措施。又自 2025 年 3 月起，監理範圍擴大至法人人頭帳戶(Corporate Mule)及數位資產帳戶。

2. 客戶輪廓分析(Customer Profiling)與認知斷點

銀行依用戶收入、交易行為及年齡(特別是 15 歲以下及 65 歲以上族群)設定差異化限額。另當用戶請求調高限額時，銀行實施「認知斷點」。這不只是行政程序，更是基於心理學設計，透過電話問答打破

詐騙過程中常見之「情緒緊迫感(Emotional Urgency)」，喚醒用戶警覺，阻斷社交工程。

(四) 中央詐欺登錄系統(CFR)與治理核心(Governance Core)

1. CFR：與支付系統同級之聯防基礎設施

「中央詐欺登錄系統(CFR)」由 National ITMX 負責運作(該單位亦為 Prompt Pay 之系統營運方)。因其掌握全行間資金移動之數據資料，故能達成近乎即時之情資交換與資金追蹤。CFR 整合執法機關、銀行、非銀行電子支付業者及電信監理機關，建立跨產業之阻斷網路。

2. 數位詐欺管理(DFM)治理框架與高層責任

在「數位詐欺管理」框架下，泰國中央銀行強調防詐非僅為資訊(IT)技術問題，而是「治理核心」。

(1) 董事會責任：規範明確要求董事會與高階管理者須將防詐管理視為策略性風險指標，並對內部偵測系統之有效性負責。

(2) 三大支柱：監測、管理及客戶關懷。

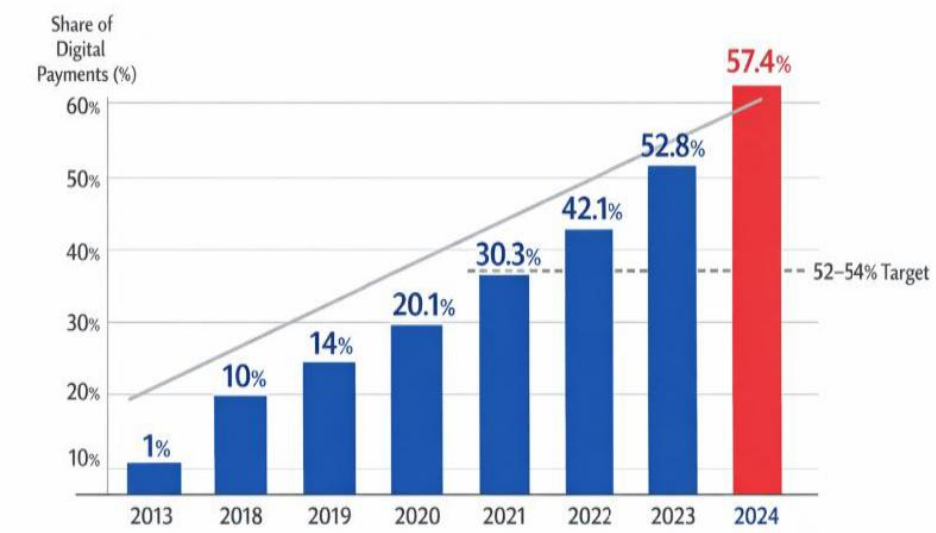
七、保障數位經濟安全：菲律賓之策略對抗詐欺與詐騙

(一) 數位支付演進與資安威脅

菲律賓近年來經歷劇烈之金融轉型，從傳統以現金為主之經濟體系，迅速過渡至高度數位化之支付生態圈。對於金融監理機關而言，不僅改變交易速度，更重新定義資安防禦之戰略邊界。數位支付之普及雖然提升金融普惠性，但也因其「高流速(High Velocity)」與「遠端開戶」等特性，縮短非法資金流轉之時間，為詐欺犯罪與洗錢活動提供溫床。

根據菲律賓中央銀行(BSP)之統計資料，菲律賓數位支付市場自 2013 年僅占總交易比例 1%，至 2024 年已激增至 57.4%，不僅呈現指數級成長，更超越「菲律賓發展計畫」原訂 52%至 54%之戰略目標。此成長主要受惠於 2017 年推動之「國家零售支付系統(NRPS)」，其下含括三大核心自動化清算機制：

1. **InstaPay**：提供小額跨行即時清算入帳。
2. **PesoNet**：主要處理大額、批次結算之 B2B 支付，非即時入帳。
3. **QRPH**：利用標準化 QR Code 完成商店支付，目前占數位支付交易量約 70%。



圖九：菲律賓數位支付成長趨勢 (2013–2024)。

儘管如此，伴隨數位化而來之資安威脅日益嚴峻。當前菲律賓金融

業面臨之主要威脅包括：社交工程、帳戶接管與身分盜用(占比達 76%)、駭客攻擊(13%)以及無卡交易犯罪(8%)。講師特別指出，線上數位開戶(E-KYC)流程中之脆弱處若缺乏嚴格控管，易產生大量「偽冒帳戶(Fictitious accounts)」，並隨著數位支付之高流速特性，使犯罪者能迅速分散資金，增加攔阻難度。

(二) 反金融帳戶詐騙專法與相關執法工具

為因應日益猖獗之網路犯罪，菲律賓政府制定多層次之法律框架，從基礎之個人資料保護到針對特定金融詐欺行為之刑事處罰，形成跨部會「全政府(Whole of Government)」之防線。

菲律賓目前之監理法制體系核心如下：

1. **《網路犯罪防制法》(Cybercrime Prevention Act, 第 10175 號共和國法案, RA 10175, 2012)**：將電腦相關詐欺與身分盜用納入刑事處罰，授權執法機關進行調查。
2. **《資料隱私法》(Data Privacy Act, 第 10173 號共和國法案, RA 10173, 2012)**：成立國家隱私委員會(NPC)，規範金融機構於發生資料外洩事件時，須主動通報 NPC 與受影響之客戶。
3. **《洗錢防制法》(Anti-Money Laundering Act, 第 9160 號共和國法案, RA 9160, 2017)**：將詐欺與詐騙列為洗錢之前置犯罪，強化金融機構落實客戶盡職審查(CDD)與可疑交易申報(STR)之法定義務。
4. **《金融產品與服務消費者保護法》(Financial Consumer Protection Act, 第 11765 號共和國法案, RA 11765, 2022)**：確立金融消費者保護機制，並要求實施嚴格之資訊保密、完整性與不可否認性標準。
5. **《SIM 卡實名制法》(Sim Registration Act, 第 11934 號共和國法案, RA 11934, 2022)**：透過電信事業實施實名制，防範犯罪者利用匿名預付卡進行詐騙。
6. **《反金融帳戶詐騙法》(Anti-Financial Account Scamming Act,**

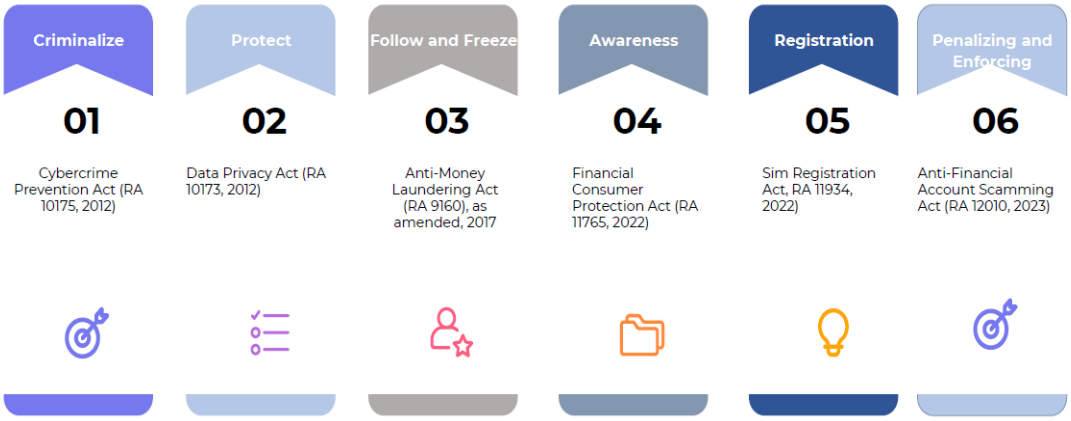
AFASA, 第 12010 號共和國法案, RA 12010)：為 2023 年通過最具關鍵性之法規，彌補傳統刑法之不足，明確界定並嚴懲下列 4 項行為：

(1)人頭帳戶行為(Money Muling Activities)：嚴禁借用、租用或買賣金融帳戶供他人實施犯罪。

(2)社交工程詐術(Social Engineering Schemes)：針對網路釣魚、簡訊詐騙等獲取個資或誘導轉帳之行為納入刑罰。

(3)經濟破壞罪(Economic Sabotage)：若犯罪涉及大規模性質，如：至少 3 人集體犯案，或被害人達 3 人以上，最高可處以無期徒刑。

(4)其餘衍生犯罪：包含為他人提供人頭帳戶之幫助行為及以虛假姓名開戶。



圖十：菲律賓防制詐欺之跨部會法律與監理架構

(三) 金融監理實務與資訊韌性強化策略

菲律賓中央銀行(BSP)之核心戰略，推動金融機構從被動之法令遵循轉為主動防禦。此類「安全先於效率(Security over Efficiency)」之政策權衡，係透過增加必要之交易摩擦，換取更穩固之資安防線。

根據 BSP Circular 1213 號令，金融機構須強化下列資訊技術風險管理機制，如：

1. **增強型詐欺管理系統(FMS)**：要求依據機構自身業務營運之複雜度，建立自動化偵測參數之系統，並主動監測攔截異常交易模式。
2. **24 小時交易暫緩期(24-hour pause)**：當客戶更改手機號碼或電子郵件

信箱等關鍵資安驗證資料時，系統應自動限制其交易 24 小時，以確保變更行為係由帳戶所有人親自操作。

3. **設備指紋辨識(Device Fingerprinting)：**追蹤並識別登入設備之合法性，偵測非常態登入環境。
4. **消費者自主管控工具：**強制要求銀行提供一鍵封鎖或限制帳戶(Kill Switch)與鎖定特定金額或限額，賦予用戶於發現異常時具備即時「自救」之能力。

除此之外，BSP Circular 1215 號令賦予金融機構於接獲通報或系統偵測到異常時，可將爭議款項暫時凍結最長 30 天之法律授權，俾利進行跨行協調與驗證。於長遠規劃上，「金融服務資訊韌性計畫」(FSCRP 2024-2029)設定：1.建立標準化且協調之事件應變機制；2.推動體系內積極之資訊共享與協作；3.深耕資安文化與公眾韌性意識；4.接軌國際資安最佳實務與標準之四大目標。

(四) 跨部門合作機制與實務案例

菲律賓係透過監理科技(SupTech)與執法機關、電信事業之合作，形成完整之偵測與阻斷鏈。2021 年底，菲律賓發生重大銀行詐騙案(Mark Nagoyo 銀行詐欺案)，逾 700 名被害人未收到 OTP(一次性密碼)，資金被非法轉往另一家銀行之「Mark Nagoyo」(菲律賓語意為「被耍了」)偽冒帳戶。

- **犯罪手法：**駭客攔截 OTP 並利用 InstaPay 之即時入帳功能，將資金迅速轉往多個人頭帳戶。
- **監理與執行處置：**
  1. **菲律賓中央銀行(BSP)：**啟動專案檢查，辨識出銀行端系統存有 OTP 發送安全性漏洞及 E-KYC 失效，隨即對涉案之兩家銀行實施行政裁罰。
  2. **賠償機制：**因確認漏洞源於銀行端系統防禦失靈(而非用戶疏失)，

銀行最終全額賠付被害人損失。

3.執法行動：國家調查局(NBI)與科技犯罪防制中心(CICC)迅速逮捕嫌犯；洗錢防制委員會(AMLC)則發布緊急凍結令以攔阻剩餘贓款。

八、菲律賓國家調查局(NBI)數位金融犯罪執法建構與實務

(一) 數位金融犯罪型態與威脅版圖演進

在現代金融體系中，銀行服務已發生根本性之典範轉移，從受限於營業時間、依賴實體櫃檯之「實體摩擦(Physical Friction)」模式，轉由雲端伺服器、光纖與演算法構成之「隱形基礎設施(Invisible Infrastructure)」。目前之數位威脅已演變為高度組織化之犯罪網路，依據 NBI 實務觀察，其主要詐欺型態，如：

1. **社交工程詐術(Social Engineering)**：透過心理操縱誘騙被害人以獲取帳戶控制權。根據第 12010 號共和國法案(RA 12010)，這涉及冒充機構人員或利用電子通訊手段獲取敏感資訊。
2. **偽冒加密貨幣投資平台(Fake Crypto Platforms)**：透過社群媒體與不實獲利資料建立信任，最終限制提領並侵占資金。
3. **人頭帳戶行為(Money Muling Activities)**：依據 RA 12010 與調查實務，要將此行為定罪，關鍵在於證明犯罪者明知(Knowledge)資金來源為非法所得。
4. **非法線上借貸應用程式(Online Lending App)**：鎖定難以獲取信用貸款之族群，進行過度之個人資料蒐集與不法催收，並將資金透過電子錢包進行洗錢。

(二) NBI 組織現代化與數位鑑識能力之強化

面對數位犯罪之複雜性，執法機關須從內部著手，確保機關已準備就緒(Institutional Readiness)之全面發展。NBI 依據第 10867 號共和國法案(RA 10867)進行重大之體制現代化，將招募門檻從傳統之法律與會計專業，擴大至任何持有相關專門職業及技術人員證照之學士學位持有者，藉此延攬大量資訊資安專家與資料分析師，建立跨領域專業團隊。

在數位鑑識實務上，NBI 建立數位鑑識實驗室(Digital Forensic Laboratories)並推動「轄區覆蓋」策略，在各行政區設立地區分局(Regional Office)，確保調查人員能在案發第一時間於現場進行證物採集與鑑識。

為應對辯方對證據完整性挑戰，NBI 執行嚴謹之四階段處理流程：

1. **證據提取(Evidence Extraction)**：從設備或雲端獲取關鍵之數位與金融證據，甚至嘗試恢復被刪除之數據。
2. **證據保全與監管鏈維持(Preservation & Chain of Custody)**：核心在於雜湊值驗證(Hash verification)，建立「具可重複性與可辯護性程序(Repeatable, Defensible Procedures)」之技術核心，確保證據不因程序瑕疵而被排除(撤銷)。
3. **數據關聯與分析(Data Correlation & Analysis)**：鏈結不同帳戶與設備，還原犯罪活動時間線。
4. **報告生成(Report Generation)**：將技術資料轉化為法庭可理解之證言。

(三) 數位調查之法律機制與令狀體系應用

在憲法保障隱私與防範非法搜索之框架下，NBI 獲取法院所簽發網路犯罪之搜索令(Cybercrime Warrants)是偵查合法性之基石。依據最高法院 Disini v. Secretary of Justice 判例，目前之令狀體系精確劃分強制處分權力之行使範圍：

1. **調閱電腦數據令狀(Warrant to Disclose Computer Data, WDCD)**：針對網路服務業者與電信事業，要求提交用戶資訊與流量數據(Traffic data)，主要用於辨識隱藏在網路背後之匿名嫌犯，其法律門檻較內容監聽(WICD)低。
2. **監聽電腦數據令狀(Warrant to Intercept Computer Data, WICD)**：對通訊內容進行即時監聽。由於具備最高侵入性，受到最嚴格之司法審查。
3. **搜索、扣押及檢視電腦數據令狀(Warrant to Search, Seize and Examine Computer Data, WSSECD)**：授權在特定地點搜查，並進行現場或離線檢視。
4. **檢視電腦數據令狀(WECD)**：此為數位隱私權之具體呈現，即便執法

機關已「合法持有」設備(如被害人主動提供)，若要檢視設備內部數位內容，仍須額外申請此令狀授權。

(四) 法律框架整合與跨機關協作生態圈

對抗具備隱匿性之犯罪，須仰賴具備威懾力之法律框架「第 11449 號共和國法案」(RA 11449)對「存取設備監管法」(Access Devices Regulation Act, RA 8484)之修正尤為關鍵，當犯罪行為構成經濟破壞時，刑責可加重至無期徒刑。此外，「SIM 卡實名制法」(RA 11934)則有效降低行動通訊之匿名性問題。在跨機關協作方面，目前最顯著之突破是「反金融帳戶詐騙法」(AFASA, RA 12010)，執法專家須區分以下兩者之差異：

1. **反洗錢理事會(AMLC)資訊**：屬金融情資，通常僅供內部參考，無法直接作為法庭證據。
2. **菲律賓中央銀行在 AFASA 架構下提供之資訊**：由於 AFASA 是銀行保密法之法定例外，BSP 分享給 NBI 之調查資料是「具備法庭證據能力」之證物，能直接用於刑事起訴，改變金融犯罪之偵辦效能。

九、國際支付詐欺趨勢與人工智慧(AI)監理應用

(一) 全球支付技術與詐欺型態之演進歷程

支付技術自實體貨幣轉向數位化與即時化之過程中，詐欺手段亦同步演進，本質上已形成金融機構與詐欺集團間持續之技術軍備競賽。各項支付技術之革新雖提升便利性，卻也同步改變風險邊界，當系統產生短暫服務中斷或漏洞時，攻擊者往往能迅速填補防禦真空並發起攻擊。

根據支付革命之發展階段，其風險特徵演進依序如下：

1. 第一代(支付卡初期)：風險集中於實體世界之「垃圾搜尋(Dumpster Diving)」，詐欺者試圖實體獲取帳單資料。
2. 第二代(磁條與晶片)：引入磁條與晶片(EMV)以對抗偽造卡。雖然晶片大幅提升複製難度，但實體卡片遭竊風險依舊存在。
3. 第三代(代碼化技術與行動支付)：代碼化(Tokenization)提升了交易安全性，但威脅邊界擴展，詐欺集團轉向發動「大規模資料外洩」。
4. 第四代(新興技術與增強資料)：威脅轉向「暗網(Dark Web)」協作，攻擊者開始專業化分工。
5. 第五代(AI 與機器學習時代)：支付進入 AI 驅動階段，詐欺演變為「AI 驅動型詐欺(AI-Driven Fraud)」。攻擊者利用自動化工具，在極大規模下進行高度客製化之社交工程攻擊，顯著提升獲利效率。

(二) 行動通訊時代之實體安全漏洞與工業化詐欺鏈結

於當前「手機時代(Phone-age)」環境下，行動裝置已實質成為使用者數位身分與金融資產之總和。惟資安防禦體系中最薄弱之環節，往往在於使用者對周邊實體環境(如：公共 USB 充電設備)及對話情境之「隱含信任(Implicit Trust)」，致使攻擊者得以輕易繞過系統安全控制。

在實體信任之濫用上，攻擊者利用傳輸線進行滲透；該裝置外觀與標準 USB 連接線無異，但內含嵌入式控制器。接入時，行動裝置作業

系統會將其識別為受信任之人機介面裝置(HID)，自動注入預先定義之按鍵輸入序列(Keystrokes)，進而繞過軟體漏洞下載惡意應用程式(APK)，並建立遠端反向控制(Reverse Shell)。部分作業系統，如：蘋果IOS，在實體接入控制上相對具備較嚴密之防禦機制。此外，詐欺集團已演化為具備組織規模之「詐欺工廠」，設有執行長、資安長等職位，並提供「網路犯罪即服務(Cybercrime as a Service)」。攻擊者利用WormGPT、FraudGPT 等不受限之大型語言模型工具，大幅降低犯罪門檻。課程舉例，某支付平台發生短暫服務中斷時，詐欺集團迅速偵測到系統邏輯漏洞，並透過 YouTube 與 TikTok 發布操作指南，該平台之授權請求量在短時間內暴增為平常之 10 倍，展現了社群傳播結合系統化作戰之規模。

(三) 深偽技術(Deepfake)與生物識別防禦之挑戰

身分驗證為支付安全之關鍵防線，但 AI 深偽技術正嚴重侵蝕此機制。在數位身分偽裝技術方面，攻擊者僅需約 3 秒鐘之語音樣本，即可透過 AI 進行高擬真之「語音複製(Voice Cloning)」。在視覺深偽與電子身分驗證(eKYC)繞過方面，攻擊者透過生成具備活體特徵之影像，試圖繞過金融機構之活體辨識機制。

課程提及一跨國企業重大損失案例，攻擊者利用深偽技術於視訊會議中偽裝成執行長(CEO)，導致財務長(CFO)於壓力下核准高達美金2,500 萬元之轉帳。

目前深偽影像雖有「影像瑕疵(Artifacts)」，如：頸部線條不連續、背景光影矛盾，惟即時視訊或低解析度環境下，肉眼幾乎無法即時識別，對依賴單一生物識別特徵之防禦機制構成極大挑戰。

(四) 利用 AI 進行跨機構情資共享

面對 AI 驅動威脅下，金融機構須建立主動防禦體系。課程核心結論指出：「AI 是應對詐欺之必要但非充分條件」，須將其納入「分層防

禦」架構，其防禦策略涵蓋四個層次，如：

1. **機器學習(ML)**：學習使用者交易行為，即時識別與歷史交易模式不符之異常交易，如：異常購買高價遊戲機。
2. **大數據分析(Big Data Analysis)**：處理海量數據，識別個別金融機構無法單獨偵測之跨網路系統性攻擊跡象。
3. **自然語言處理(NLP)**：識別釣魚郵件或詐騙訊息中之細微語言特徵，預先攔截威脅。
4. **生成式 AI 應用(Generative AI)**：自動化產製攻擊報告與情資摘要，大幅縮短入侵指標之分析時間。

然而，跨機構大數據分析目前面臨實務上之困境。金融機構間雖有情資共享需求，但常因保密協定限制，或擔憂將資料交予監理機關後可能面臨潛在之監理裁處，導致情資共享難以落實。有效防禦之關鍵仍仰賴於在保護隱私之前提下，建立標準化之情資共享機制，以 AI 技術動態對抗日益複雜之 AI 詐欺威脅。

十、強化金融機構防制詐欺及洗錢韌性之監理架構與實務

(一) 詐欺犯罪之全球趨勢及其對金融穩定之衝擊

在數位金融生態圈高度互聯情形下，詐欺與金融犯罪已超越單純之個體財產損失，演變為危及金融體系健全性之「系統性風險」。大規模及組織化之詐欺活動不僅會引發突發性流動性壓力，更可能削弱民眾對支付系統之信任，並導致金融機構實施過度「去風險化(De-risking)」，進而排斥弱勢族群並損害普惠金融之發展。

根據國際資料，金融犯罪之規模與手法翻新速度已達警戒線：

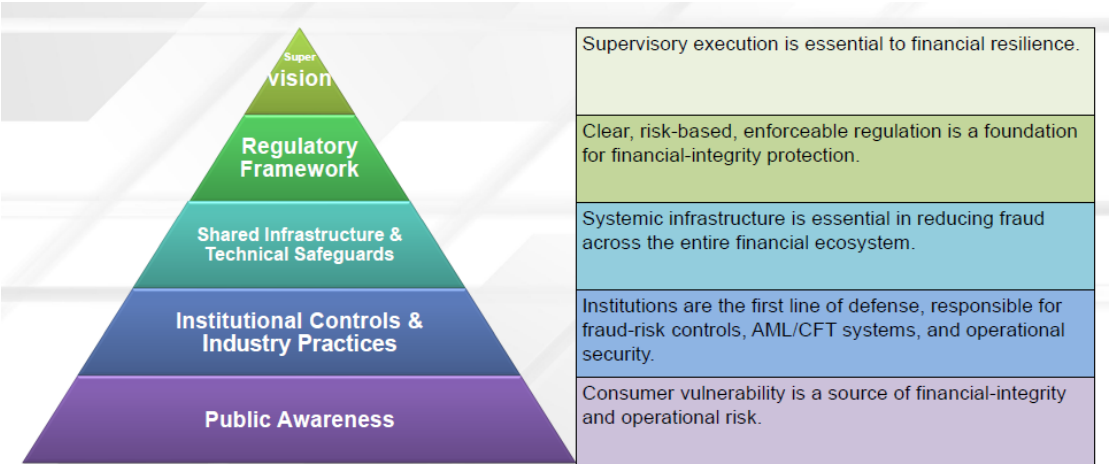
1. **全球犯罪規模**：每年金融犯罪(含洗錢)估計達 2 兆至 5 兆美元，約占全球 GDP 之 2%至 5%。其中，單純詐欺損失已突破 1 兆美元規模。
2. **亞洲市場現況**：亞洲年度詐欺損失約 6,880 億美元，且超過 70%之案件源於社群媒體及通訊軟體等線上平台。尤其，東南亞組織化詐欺犯罪每年產生之不法利潤估計高達美金 400 億元。
3. **科技演進之威脅**：AI 驅動之金融犯罪預計每年增長 30%以上，推估至 2027 年，詐欺損失金額將達到目前之 4 倍。
4. **企業營運衝擊**：詐欺導致全球企業平均損失年度營收之 8%，嚴重影響產業競爭力。

(二) 打擊詐欺與洗錢之國際標準與層級韌性架構

國際監理組織已設定全球一致之防詐與洗錢防禦基準，作為評估各國金融健全性之重要指標。其中，國際貨幣基金(IMF)已將防制洗錢與打擊資恐(AML/CFT)深度整合至「金融部門評估計畫(FSAP)」與總體金融審查中；防制洗錢金融行動工作組織(FATF)強調採取「風險導向(Risk-based)」監理，並強化實質受益人透明度及申報機制；國際清算銀行(BIS/BCBS)則正式將數位詐欺風險納入作業風險管理框架，要求提升機構韌性。為落實上述監理框架，打擊詐欺策略可進一步結構化為「防制詐欺金字塔(Combating Fraud and Scams Pyramid)」，由下而上構

成五個防禦層級：

1. **公眾意識(Public Awareness)**：提升消費者警覺，防範安全漏洞。
2. **機構內部控制與產業實務(Institutional Controls)**：受監理機構應落實「第一道防線」職責。
3. **共享基礎設施與技術(Shared Infrastructure)**：建立跨機構資訊共享平台，如：國家級防詐體系。
4. **法規框架(Regulatory Framework)**：提供清晰且具執行力之法律基礎。
5. **監理執行(Supervision)**：確保韌性之核心，負責將規則轉化為具體之檢查實務。



圖十一：「防制詐欺金字塔」之 5 個防禦層級。

(三) 金融機構之內部控制要求與監理執行實務

現代監理實務已從單純評估機構之形式合規(Compliance)，轉向驗證其防禦機制之「實質有效性(Effectiveness)」，確保機構具備動態管理新型態詐欺風險之能力。針對受監理機構之內控要求與監理機關之執行實務，如：機構治理與防詐文化、核心內控管理義務、多元監理工具與裁罰應用、數據驅動之系統性監控。

(四) 監理科技(SupTech)應用、跨域協調與未來挑戰

隨著詐欺手法高度網路化，監理模式須由傳統之事後稽核(Post-

event Audit)轉型為即時監控(Real-time Monitoring)。針對監理科技之應用與未來防詐政策之制定，其核心分為 4 項重點：

1. **擴大監管範圍與跨域協作**：監理範圍須擴及支付服務供應商(PSPs)、金融科技公司(FinTech)及虛擬資產服務供應商(VASPs)等非傳統金融體系。同時，須強化涵蓋金融情報中心、執法機關及電信主管機關等跨部門與跨國協作機制，以解決跨機構之資訊孤島問題。
2. **科技監理(SupTech)實務應用**：監理機關應推動跨機構資料標準化，並導入自動化通報儀表板、異常行為偵測與複雜人頭帳戶之網路分析等科技工具，以大幅提升早期預警與系統性風險之監控能力。
3. **法規影響評估(RIA)與潛在副作用防範**：制定防詐措施時須針對「根本原因(Root cause)」進行評估，避免單一強制規定產生非預期之營運衝擊或衍生風險。如:泰國曾因系統自動大規模凍結極小額(5 至 10 泰銖)測試交易，導致無辜微型企業營運停擺；加州開車禁用手持電話與兒童安全藥瓶之案例亦揭示，若忽略駕駛分心本質或使用者便利性，單純增加流程門檻反易使防護失效。
4. **綜合政策組合(Policy Mix)之建立**：成功之防詐架構不能僅依賴單一監理工具，須建立結合技術控管、法規處分與民眾教育等多管齊下之綜合政策組合，確保整體防禦體系具備動態調整之彈性。

肆、心得與建議

本次參與東南亞國家中央銀行研究訓練中心(SEACEN)舉辦之防範詐欺與洗錢防制研習課程，深入探討各國面對數位金融犯罪之監理實務與技術應用。透過各國實務經驗與分享，瞭解到防制數位詐欺並非僅是單一之技術議題，更涉及跨部會之情資共享、法律授權與整體社會之共同防禦框架，獲益良多，謹提出以下建議：

一、持續強化情資共享，打破金融機構間之資訊孤島，以提升資金攔阻效率。

隨著全球數位支付生態轉向即時支付，詐欺資金轉移速度大幅提升，單一金融機構傳統基於內部數據之防禦機制已形成監理盲點與資訊孤島。本次訓練課程多位講師提及應建置國家級防詐體系，並跨部會與金融機構間等相關機構合作，共同分享情資。本會已請財金公司建立金融阻詐聯防平台，協助金融機構進行資訊交換及分析精進打詐措施、推動虛擬資產業者與金融機構合作、事先發覺潛在被害人，進而與警政單位合作阻詐，並以資訊系統協助第一線行員有效運用相關資訊，持續強化精進情資共享，以提升資金攔阻效率。

二、關注各國推動多元之責任分擔機制實施成效，作為精進防詐工作之參考。

各國講座分享新加坡與泰國頒布之「緊急法令」，建立金融機構、電信事業與消費者之階層式賠付機制，明確界定責任歸屬。若金融機構因系統漏洞、未執行法定暫停交易控管(如帳戶清空規則)或未能遵循系統安全標準而導致客戶受損，則需承擔相應或全額之賠償責任。

我國已於 113 年 7 月 31 日公布施行「詐欺犯罪危害防制條例」(打詐專法)，部分預防機制與國際作法已有相當程度接軌。各國因法制環境及監理架構不同，針對授權交易詐騙所涉損失分擔機制，有不同之制度設計。新加坡及泰國近年透過共同責任框架或相關法制安排，逐步強化金融機構、電信事業及消費者於詐騙防制工作中之責任分工，後續可持續關注相關制度之運作情形及實施成效，以作為我國精進防詐工作之參考。

三、持續參考國際經驗強化高風險交易之預防機制，以降低授權交易詐騙風險。

本次課程中，新加坡、泰國及菲律賓等國均強調，現行詐騙案件多屬「授權交易詐騙」，如：詐騙集團透過釣魚網頁、假買家或假客服等方式，誘騙受害者主動提供信用卡號及 OTP 一次性簡訊驗證碼，進而完成交易之犯罪手法。此類案件之特性在於金融機構之交易系統通常運作正常，惟被害人於情緒緊張、恐懼或貪婪等心理因素影響下作出錯誤決策，因此單純依賴事後通報、帳戶列管或資金追償機制，往往難以有效降低損害。

課程中分享新加坡透過交易冷卻期、認知斷點、動態警示訊息及高風險交易額外驗證等措施，爭取被害人重新思考之時間；泰國則針對提高轉帳限額及大額交易等高風險行為，強制採行臉部辨識驗證；菲律賓亦要求金融機構於客戶變更重要驗證資訊後，實施一定期間之交易暫緩措施。相關作法均係透過適度增加交易摩擦，降低衝動決策所造成之詐騙損失。

我國近年已持續推動防詐措施，惟隨著數位金融服務日益普及，授權交易詐騙仍為主要損失來源之一。建議持續參考國際監理實務，評估於高風險交易情境下導入更具差異化之風險控管措施，如：提高轉帳限額時設置冷卻期、針對異常交易導入認知斷點機制，以及強化高風險交易之身分驗證程序，以兼顧交易便利性與安全性，降低授權交易詐騙案件發生之風險。

參考資料

1. 參加東南亞國家中央銀行研究中心資通訊風險管理和網路安全課程，蘇奕銘、宋建勳，114 年 12 月。
2. Amanah Ramadiah (2026/3/24), “Countering Consumer Fraud and Scams via National Anti-Scam Utilities”.
3. Yogesh Simmhan (2026/3/24), “Analytics to Detect Emerging Fraud and Scam Networks”.
4. Yogesh Simmhan (2026/3/24), “Agentic AI and its Implications for Fintech Defence”.
5. Amanah Ramadiah (2026/3/25), “A Blueprint for Building National Anti-Scam Utilities:From Regulatory Foundation to Technology”.
6. Rennie Soh (2026/3/25), “Regulatory Innovation for Scam Prevention: Singapore’s Evolving Framework”.
7. Suppakorn Chotika-arpa (2026/3/25), “From Awareness to Action: Thailand’s Comprehensive Journey Against Fraud and Scam Threats”.
8. Anna Liza R. Guevarra (2026/3/26), “Securing the Digital Economy: The Philippines' Strategy Against Frauds and Scams”.
9. Atty. Abram M. Geronaga (2026/3/26), “Enhancing Law Enforcement Capability: The NBI's Response to Emerging Digital Crime”.
10. Lim Kah Wee (2026/3/26), “Cybersecurity Challenges and Roles Of AI in Facilitating Fraud and its Potential to Combat Cybercrimes”.
11. Vacharakoon Jivakanont (2026/3/27), “Strengthening Central Bank Supervision and Regulation for Fraud, Scam, and AML/CFT Resilience”