# 網路詐欺產生的非法金流

**2023 年 11 月**

FATF (防制洗錢金融行動工作組織) 是一個獨立的政府間組織，旨在發展與推廣政策，以保護全球金融系統，防制洗錢、資恐以及資武擴。FATF 建議已成為全球防制洗錢 (AML) 與打擊資恐 (CFT) 的公認標準。如欲進一步瞭解 FATF，請參見：**www.fatf-gafi.org**。本文件及/或本文所含的任何地圖，概不影響任何領土之狀態或主權、國境與國界之界定以及任何領土、城市或地區之名稱。

艾格蒙聯盟金融情報中心 (Egmont Group) 旨在提供全球性論壇，以利各地金融情報中心 (FIU) 加強合作，打擊洗錢及資恐活動，促進於各地境內實施相關領域計畫。如欲進一步瞭解艾格蒙聯盟，請參閱網站：www.egmontgroup.org。

國際刑警組織 (INTERPOL) 的職責是促使 195 個會員國的警方協力打擊跨國犯罪，促進世界安全。組織設有全球資料庫，收錄各類罪犯及刑案相關警政資訊，並提供實務及鑑識方面的支援、分析服務和訓練。警務實施範圍遍及各國，支援下列四項全球計畫：金融犯罪和貪污、反恐、網路犯罪，以及組織和新興犯罪。

引用文獻：

> FATF – 國際刑警組織 - 艾格蒙聯盟 (2023)《*網路詐欺產生的非法金流*》，FATF (法國巴黎)，www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/iIllicit-financial -flows -cyber- enabled-fraud.html

# 目錄

# *縮寫對照表*

| | |
|---|---|
| AML/CFT | 防制洗錢/打擊資恐 (Anti-money laundering/Countering the financing of terrorism) |
| ATM | 自動提款機 (Automated Teller Machine) |
| BEC | 商業電子郵件攻擊 (Business email compromise) |
| CDD | 客戶盡職調查 (Customer due diligence) |
| CEF | 網路詐欺 (Cyber-enabled fraud) |
| DNFBP | 指定之非金融事業或人員 (Designated non-financial businesses and professions) |
| FI | 金融機構 (Financial Institution) |
| FIU | 金融情報中心 (Financial intelligence unit) |
| IBAN | 國際銀行帳號 (International Bank Account Number) |
| IP | 網際網路協定 (Internet protocol) |
| LEA | 執法機關 (Law enforcement agency) |
| ML | 洗錢 (Money Laundering) |
| MLA | 司法互助 (Mutual legal assistance) |
| PSP | 支付服務業者 (Payment service provider) |
| PPP | 公/私合作夥伴關係 (Public-private partnership) |
| STR | 可疑交易報告 (Suspicious Transaction report) |
| TF | 資恐 (Terrorist financing) |
| TBML | 貿易型洗錢 (Trade-based money laundering) |
| VA | 虛擬資產 (Virtual asset) |
| VASP | 虛擬資產服務提供商 (Virtual Asset Service Provider) |
| vIBAN | 虛擬國際銀行帳號 (Virtual International Bank Account Number) |
| VPN | 虛擬私人網路 (Virtual private network) |
| VoIP | 網際網路協定語音傳輸 (Voice over Internet Protocol，簡稱網路電話) |

# 執行摘要

網路詐欺（CEF）是一種日漸猖獗的跨國組織犯罪。網路詐欺犯罪集團通常結構嚴密，依特定犯罪專業領域（包括洗錢）再劃分不同任務的次集團。這類次集團亦可能組織鬆散，以去中心化（de-centralised）型態分布於不同司法管轄區，致使偵辦網路詐欺活動更加困難。網路詐欺集團亦涉及其他類型犯罪活動，尤其是網路詐欺機房的人口販運和強迫勞動，以及有關朝鮮民主主義人民共和國（北韓）非法網路活動的資武擴。

洗錢犯罪團體和專業助力者共同參與網路詐欺洗錢流程，洗錢帳戶網絡通常涉及錢騾，但也可能包括空殼公司或合法企業。洗錢網絡的特徵是其牽涉不同類型的金融機構（FI），包括銀行、支付和匯款服務業者，以及虛擬資產服務提供商（VASP）。罪犯綜合運用多種洗錢技術，例如使用現金、貿易型洗錢（TBML）和未經許可的地下服務，進一步隱藏非法所得金流。

藉助數位化技術，網路詐欺罪犯得以發展並擴大其非法活動的規模、範圍和速度，此等罪犯透過各種工具和技術欺騙被害人，利用其心理狀態和情感弱點，盡可能榨取更多資金。網路詐欺犯罪集團利用科技進步成果，可更容易、迅速清洗犯罪所得。透過遠端線上開戶等虛擬服務，罪犯亦可輕易設立外國帳戶，以近乎即時速度執行金融交易，藉此在境外漂白犯罪所得。社群媒體和訊息傳遞平台蓬勃發展，亦給罪犯可趁之機，大舉招募跨國錢騾，並迅速利用新型數位金融機構、產品及非傳統領域（如電子商務、社群媒體和串流平台）出現的漏洞從事不法。

有鑑於此，司法管轄區需採取更有效的因應對策，其中包括：

- 採取措施提高被害人報案率，並強化可疑交易報告機制；
- 有效分析大量流入的資訊，以應對網路詐欺犯罪；以及
- 考量網路詐欺的跨領域性質，建立強大的國內協調機制，全面打擊並預防網路詐欺及相關洗錢活動。

網路詐欺的前置犯罪和洗錢過程一般不會在相同地點進行。犯罪所得可以透過通常跨越多個司法管轄區和金融機構之帳戶網絡迅速漂白。各司法管轄區必須進行多邊合作，才可有效、迅速攔截跨國洗錢的網路詐欺犯罪所得。為此，各司法管轄區應善用並支持現有（及未來）多邊機制（例如國際刑警組織的 I-GRIP 和艾格蒙聯盟的 BEC 計畫），以利各國迅速合作並交流情資，更有效打擊網路詐欺。

最後，本報告附有一系列風險指標及實用的反詐欺要求和控管措施，有助於公私部門實體偵查和預防網路詐欺及相關洗錢活動。

# 1. 簡介

1. 網路詐欺詐欺是最大宗的網路犯罪型態。若不加以遏制，隨著更多組織犯罪集團參與這類非法活動，並利用生成式 AI 等新技術的可趁之機，手法勢必更加縝密，構成更大的威脅和風險。[1]

2. 在新加坡擔任輪值主席國期間，FATF 啟動一項新措施，重點打擊網路詐欺產生的非法資金流動。本報告是艾格蒙聯盟、FATF 和國際刑警組織聯合計畫的執行成果，亦為三個組織首度合作的專案，反映共同打擊跨國組織犯罪及其網絡的決心。

## 1.1. 重點與範圍

3. 本報告著重探討詐欺犯罪所衍生的非法金融活動，而該等詐欺是藉助或透過網路環境進行，其特徵為：(i) 涉及跨國犯罪，例如跨國行為人和資金流動，以及 (ii) 涉及欺騙性的社交工程手法 (即操縱被害人以取得其機密或個人資料)。有鑑於此類詐欺種類繁多，本報告重點關注下列犯罪活動類型 (統稱為*網路詐欺*(CEF))：

   - **商業電子郵件攻擊 (BEC) 詐欺：**被害人會收到聲稱是其客戶或供應商的電子郵件指示，要求將資金轉移到新的支付帳戶。
   - **網路釣魚詐欺：**被害人遭欺騙而洩露敏感資訊，例如個人資料、銀行明細或帳戶登入憑證。罪犯繼而利用這些資訊，從被害人的支付帳戶榨取資金、開設新的支付帳戶或進行詐欺交易。
   - **社群媒體和電信冒名頂替詐欺：**此情況包括罪犯冒充政府人員、親戚朋友，透過行動或社群媒體應用程式聯絡被害人，並利用被害人情感弱點，誘騙其付款、移交支付帳戶控制權或進行金融活動，例如申請貸款或開戶以收取犯罪所得。
   - **網路交易/交易平台詐欺：**被害人遭虛假廣告或線上顧問欺騙，前往虛設或假冒 (詐欺) 平台，進行法幣資產和虛擬資產相關的交易或投資。
   - **網路愛情詐欺：**被害人受騙並誤信處於戀愛關係後，匯款給罪犯。
   - **就業詐欺：**詐欺者在社群媒體平台刊登虛假工作機會，以各種藉口誘騙被害人向其付款，包括預先購買商品以衝高交易平台營業額，或是要求繳交到職保證金。

[1] 另請參閱國際貨幣基金組織 (2023 年 8 月)《*金融科技工作報告：金融領域中的生成式人工智慧：風險注意事項*》。

4. 涉及勒索軟體和其他惡意軟體犯罪的非法融資不屬於本報告範圍。讀者應參閱 FATF 關於*打擊資助勒索軟體*的報告 (2023 年 3 月) 進一步瞭解勒索軟體、透過虛擬資產 (VA) 和虛擬資產服務提供商 (VASP) 洗錢的手法，以及風險緩解措施的挑戰和優良實務。這些資訊皆與本主題密切相關，因為罪犯有時會利用虛擬資產和虛擬資產服務提供商來漂白網路詐欺的犯罪所得。

## 1.2. 目標與結構

5. 本報告旨在協助權責機關加強瞭解網路詐欺威脅的風險。本報告係基於 FATF 及其他國際機構 (包括艾格蒙聯盟、歐洲刑警組織和國際刑警組織) 的現有工作成果，並試圖確認與加強風險瞭解相關的重大和新興發展。

- 本報告**第 2 章和第 3 章**探討目前有關網路詐欺的運作風險環境，並深入解析網路詐欺及相關洗錢 (ML) 之風險、技術和趨勢，包括數位化和新技術的影響及漏洞。
- 本報告**第 4 章和第 5 章**列舉各司法管轄區所採用的優良實務和運作解決方案，包括國際合作和資產返還機制，藉以克服各種挑戰，加強應對並遏止網路詐欺及相關洗錢活動。

## 1.3. 方法

6. 本計畫係由新加坡 (代表 FATF)、中國香港金融情報中心 (代表艾格蒙聯盟) 及國際刑警組織的專家共同主持，此外，下列司法管轄區及實體亦以計畫團隊成員身分做出貢獻：亞塞拜然、巴西、比利時、加拿大、中國、歐洲理事會、歐盟執行委員會、歐洲刑警組織、德國、西非政府間防制洗錢行動小組 (GIABA)、印度、義大利、以色列、日本、馬來西亞、墨西哥、防制洗錢措施和資恐問題評估專家委員會 (MONEYVAL)、巴基斯坦、葡萄牙、沙烏地阿拉伯、多哥、英國及美國。

7. 本報告結果係以下列資訊為依據：

- 對此主題的相關現有文獻和公開資料的回顧。其中包括艾格蒙聯盟和國際刑警組織所編纂的資料及研究成果。
- FATF 全球網絡及艾格蒙聯盟 (分別由 200 個司法管轄區和 170 個金融情報中心組成) 應要求所提供的風險、執行架構和策略、國內和國際合作及協調機制相關資訊。計畫小組共收到 80 多個代表團的意見。

- 在 FATF 聯合專家會議 (2023 年 4 月) 及私部門諮詢論壇 (2023 年 5 月) 交流的討論及見解，包括與私部門進行目標性議合。

# 2. 風險環境：網路詐欺

## 2.1. Rising money laundering (ML) threat

8. 國際間的網路詐欺活動顯著增加。網路詐欺的全球數量和規模雖無完整估計數據，但依許多司法管轄區報告，近年呈現持續成長之勢。網路詐欺的犯罪所得經常轉移到外國的司法管轄區。然後，這些犯罪所得可能透過其他第三方司法管轄區的金融系統進一步漂白。

9. 根據國際刑警組織 2022 年《全球犯罪趨勢報告》[2]，網路詐欺是最常視為對全球構成「高度」或「極高」威脅的網路犯罪趨勢之一。大多數向本計畫提供資訊的司法管轄區，其國家風險評估皆明確指出網路詐欺衍生的洗錢風險。儘管網路詐欺具有跨國性質，罪犯可不受國界限制輕易鎖定被害人，然而在無現金和數位化技術盛行的區域 (例如可透過網路提供大多數金融中介服務的地區)，預計更容易面臨此類犯罪相關的洗錢風險。下方說明欄彙整各方資訊來源[3]，概述各區域的網路詐欺威脅態勢。

### 說明欄 1. 洗錢威脅與日俱增：區域網路詐欺趨勢

**非洲：**在非洲，快速數位化的金融部門，為罪犯提供大量實行網路詐欺的機會，導致網路銀行詐欺案量激增，包括網路釣魚、身分竊盜和虛擬資產詐欺。此類犯罪造成的經濟損失不斷增加，洗錢威脅也隨之攀升。例如在西非地區，網路詐欺據報導已成為主要的犯罪所得來源。

**美洲：**網路詐欺已確定為一種日漸猖獗或新興型態的風險。某一司法管轄區指出網路詐欺報案數量逐年成長，且相關洗錢風險也隨之升高。另一司法管轄區則報告，罪犯利用虛擬資產的炒作和熱潮，使 2021 年至 2022 年間的虛擬資產投資詐欺增加超過 180%。

**亞太地區：**各個司法管轄區已將網路詐欺列為高度或重大洗錢風險。例如某一司法管轄區指出，在大多數詐欺報案中，均涉及一定型態的網路詐欺，且觀察到網路詐欺相關的洗錢活動有所增加。另一司法管轄區則強調跨國行為人的角色，這類罪犯會透過多種非法投資應用程式欺騙被害人。COVID-19 疫情加速推動當地一般民眾、政府及企業服務和行為的數位化轉型。在此趨勢下，網路詐欺和相關洗錢活動隨之激增，且預計將繼續加劇。

**加勒比海地區：**當地是網路詐欺和相關洗錢犯罪好發地區，過去五年涉及網路詐欺的詐欺案總數有所增加。加勒比海盆地虛擬資產部門 (包括虛擬資產提供商) 日益興盛，亦產生各種洗錢漏洞，包括濫用混幣器 (mixer)，將非法資金洗回給網路詐欺團體等組織犯罪集團。

**歐洲：**一般而言，網路詐欺通常被評估構成洗錢風險。眾多司法管轄區均指出此類活動大幅增加，並認定網路詐欺構成高度威脅。常見利用虛

2 請參閱國際刑警組織 (2022)《*全球犯罪趨勢報告*》

3 包括司法管轄區提供的資訊和資料，以及國際刑警組織和歐洲刑警組織的報告。

擬資產漂白網路詐欺犯罪所得（尤其是涉及虛擬資產的線上交易詐欺，例如詐欺性的首次代幣發行）。

**中東和北非（MENA）**：與全球各地趨勢一致，MENA 地區的政府、企業及民眾，也在疫情期間將大量活動轉移至網路進行，從而加速數位化的進展。網路金融詐騙，包括網路釣魚、冒名頂替詐欺和網路詐欺，均列為高度威脅。MENA 區域亦為洗錢好發地區，尤其海灣國家合作理事會（GCC）成員國均為全球貿易和金融活動的重要樞紐。

10. 數位化和新技術的發展是助長網路詐欺的關鍵驅動因素。數位服務已成為日常生活和公共職能不可或缺的一環，因此有更多民眾（包括亦受影響的群體）參與網路活動。同時，數位化意味著各司法管轄區之間聯繫日益密切，加速了資訊和資金的跨境流動。這兩項因素徹底改變犯罪格局，形成利於犯案的環境，進而提高網路詐欺威脅。

11. COVID-19 疫情加快了轉型速度，原本面對面的實體金融活動，轉變為線上開戶、支付和借貸的互動模式。電話和電子郵件詐欺等詐欺活動；透過網際網路和利用智慧型手機、電子郵件和社群媒體實行的銀行、老年人及醫療照護詐欺（例如涉及個人防護裝備和其他醫護產品相關的案件）以及投資詐欺顯著增加。持續變化的金融行為也對洗錢領域造成影響，包括增加使用數位化的銀行服務、支付平台及遠端交易（另請參閱第 24 頁「數位化和新技術的影響」一節）。[4]

12. 智慧型手機、技術（伴隨持續演進的新工具與應用程式）以及遠端金融交易日益普及，卻也導致使用者的受害風險大幅增加。結合運用虛擬私人網路（VPN）和「洋蔥路由器」[5] 等匿名強化技術，罪犯從事非法活動可隱匿行蹤，更難追查其身分，藉此科技之便，罪犯還可擴大犯罪活動規模、範圍和速度。甚至有罪犯採用「犯罪即服務」（Crime-as-a-Service）模式[6]，其亦可顯著降低網路詐欺集團的進入門檻，其特徵為提升網路詐欺各方面的專業程度，並分派不同次團體執行（見下文第 2.2 節）。[7]

4 請參閱 FATF（2020 年 5 月）《*COVID-19 相關洗錢和資恐風險及政策回應*》與（2020 年 12 月）《*更新：COVID-19 相關洗錢和資恐風險*》。

5 又稱為 TOR，是一種允許使用者匿名上網的開源軟體。

6 此即犯罪集團的分工方式，這類組織持續開發並向成員傳授各類專精的犯罪能力、技能和專業知識。

7 請參閱歐洲刑警組織（2023 年 7 月）《*網路組織犯罪威脅評估》(IOCTA) 2023：*以及國際刑警組織（2022）《*國際刑警組織最新報告：金融和網路犯罪成全球警方首要關切*》

13. 組織犯罪集團經常利用現有技術漂白其他非法所得資金，擴大或調整活動範圍，將網路詐欺納入其中。

### 說明欄 2. 網路詐欺及其他罪行常用的犯罪洗錢網絡

某洗錢網絡組織在 A 國經濟特區 (SEZ) 的建物內設立公司，經營線上博弈和網路詐欺事業。該複合建築容納大約 10 家公司，各自經營線上博弈和網路詐欺事業，或將空間出租予他人從事相同勾當。此網絡成員包括鄰國 B 邊境地區聲稱合法的企業，且由 B 國人擔任首腦，利用 B 國貨幣的銀行帳戶，將資金從經濟特區轉移至公司主要投資人所在的 C 國。來自該經濟特區的美元，首先在 B 國的換匯所清洗，轉換為 B 國貨幣後運至 C 國，越過邊界抵達至 C 國領土後，再轉移給公司投資人。

資料來源：《東南亞跨國組織犯罪、賭場與洗錢：威脅分析》(UNODC，2022 年)

## 2.2. 網路詐欺的犯罪特徵

### *網路詐欺的要素*

14. 依據各司法管轄區經驗，網路詐欺罪犯可能利用下列各項要素，成功誘騙被害人轉出資金。網路詐欺可能以不同方式結合這些要素，衍生出各種型態的犯案手法。

- 資訊擷取 (例如透過網路釣魚)；
- 社交欺騙或社交工程、利用情感弱點 (例如冒充另一人或實體，藉此產生急迫感、引發恐懼或博取信任；或謊稱輕鬆賺錢機會)；以及

- 線上媒介或平台 (可用於進行通訊，或是在線上交易詐欺案件中，供被害人進行交易)。

15. 被害人可能不只陷入單一類型網路詐欺；罪犯最終目的是誘使對方轉帳，會動用各種手段達成目標。罪犯詭計多端，倘若最初的騙局未能得逞，即可能動用或轉換為其他類型的網路詐欺手段。例如，罪犯先透過網路釣魚或社群媒體冒充身分博取「信任」，再說服並誘導被害人進入投資騙局。

**說明欄 3. 對同一被害人多次犯案**

「殺豬盤」(Pig butchering) 是愛情詐欺加上投資詐欺的綜合手法，罪犯藉此與被害人建立信任關係，再說服對方將積蓄投資於詐欺性的加密貨幣交易平台。這類詐欺會持續一段時間，最終導致被害人損失大筆金錢。

在被害人察覺受騙後，犯罪者經常冒充律師或執法人員聯絡被害人，聲稱可協助追回資金，但需收取一筆費用。

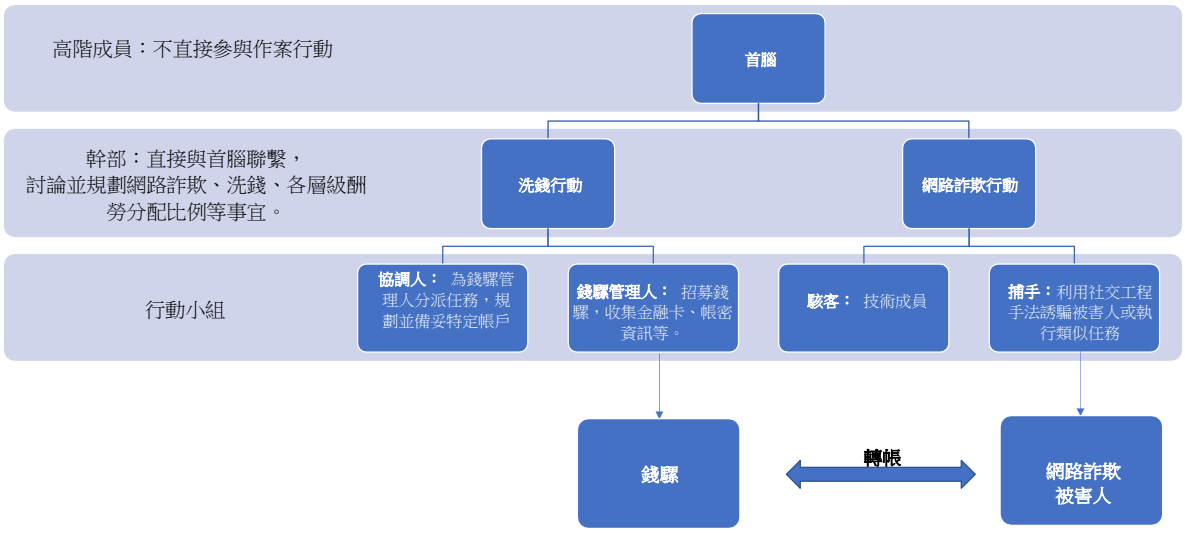
資料來源：歐洲刑警組織 (2023)《網路組織犯罪威脅評估》(IOCTA) 2023

## *組織犯罪結構*

16. 網路詐欺和相關的洗錢活動，通常是由跨國組織犯罪團體或集團執行。網路詐欺集團的結構雖各有不同，但通常是以階層分明的組織型態運作 (請參閱圖 1 範例)；亦可能採鬆散架構，視需要加入或調離成員，以保持靈活機動性。這類集團也可能依犯罪專業進行分工，設立不同專門任務的下屬次團體，例如依上述網路詐欺要素分門別類，包括資訊擷取、社交欺騙；或架設線上平台、洗錢等其他技術專業。大量案例顯示，這類網路詐欺集團具有去中心化特徵，且絕不當面溝通交流，一律透過線上加密通道等媒介互動，使權責機關難以循線調查。

17. 此外，網路詐欺集團通常由高學歷且精通技術的專業人士組成，使得網路詐欺和洗白非法獲利的手段日益縝密複雜。有司法管轄區指出，網路詐欺集團刻意招募專業部門 (包括金融機構) 從業人員，利用其所提供資料及資訊，遂行網路詐欺和洗錢目的。有關網路詐欺集團組織結構和洗錢作案方式，請詳見下文第 2.3 節。

## 圖 1.網路詐欺犯罪結構範例




資料來源：FATF

### *與其他犯罪行為的關聯*

18. 除了洗錢以外，網路詐欺集團也可能涉及其他形式的犯罪行為，常見者包括實施網路詐欺所需的相關活動，諸如駭客竊取個人資料、開發和販售犯罪軟體等網路犯罪活動，以及偽造文件等。網路詐欺集團可能將部分犯罪所得用於購買新設備，以及開發更先進的技術工具，同時藉此洗白該部分犯罪所得。

### 說明欄 4. 獵鷹行動

2020 年，在國際刑警組織、Group-IB 與奈及利亞警方偵辦網路犯罪的聯合行動中，三名嫌犯於奈及利亞拉哥斯遭到逮捕。這三名奈及利亞籍嫌犯據信隸屬於規模更龐大的組織犯罪集團，專門從事散布惡意軟體、網路釣魚，大規模商業電子郵件攻擊等不法行為。嫌犯遭控開發網路釣魚用的連結、網域，並冒充組織代表身分，發起大規模郵件攻擊，從中散布 26 種惡意軟體程式、間諜軟體和遠端存取工具。

嫌犯利用程式滲透和監控被害人的組織及個人系統，然後發動騙局和吸取資金。據 Group-IB 調查統計，此慣犯團體自 2017 年起已入侵 150 多國的政府機關和民間企業。Group-IB 亦證實該團體分為不同小組，且多名成員仍然在逃。

與此同步進行的洗錢調查顯示，嫌犯也使用英國、美國和泰國等海外銀行和虛擬資產帳戶收取被害人的付款。此三名嫌犯已因詐欺和洗錢等非法活動罪名而被起訴。嫌犯的一部豪華車輛已被查扣，其帳戶亦遭凍結，其犯罪所得亦於法庭上宣告沒收。

資料來源：奈及利亞

19. 網路詐欺與人口販運之間的關聯也日益密切，罪犯發布虛假招聘廣告，誘騙被害人至網路機房工作，強迫從事大規模的網路詐欺。由於遭到販運的被害人通曉特定語言及文化，網路詐欺集團遂能利用此一優勢，針對更多不同地區的被害人實施網路詐欺。罪犯也會販運資訊技術從業人員或「數位銷售主管」等高度專業人士，藉此提升網路詐欺機房的先進程度。[8] 這類機房有時刻意在目標被害人所在時區營運，並使用租賃的物業臨時作案，能夠快速遷移和變更 IP 位址，躲避執法單位偵查。[9]

8 請參閱國際刑警組織 (2023 年 6 月)《*國際刑警組織發出全球警告：人口販運助長詐欺*犯罪》

9 請參閱國際刑警組織 (2023 年 7 月)《*東南亞網路詐欺與人口販運實務分析》/更新 2 – 從區域威脅到全球威脅*》(僅供國家執法機關閱覽)。

### 說明欄 5. 風暴製造者行動

在「風暴製造者行動」中，主管機關對組織犯罪集團展開執法，這些集團涉嫌跨境販運亞裔男性、女性和兒童，從中進行剝削及/或牟利。此行動在 25 國逮捕 121 人，並發起 193 項新的調查。

馬來西亞和柬埔寨警方在「風暴製造者」行動密切合作，聯手偵辦一起涉及 15 名男性及 1 名女性的案件，他們聽信豐厚薪酬的承諾，被誘騙到柬埔寨的機房任職，然而抵達後隨即遭到囚禁，被迫每天從事 14 小時的詐騙工作。

註：更多詳細資訊請參閱國際刑警組織 (2022 年 5 月)《*在打擊移民走私和人口販運的行動中逮捕 121 人*》

資料來源：國際刑警組織

20. 在大多數司法管轄區，目前尚無實質證據顯示資恐活動與網路詐欺有所關聯。但在部分恐怖活動和資恐犯罪的運作環節中，亦觀察到網路詐欺行為人的涉入跡象。例如某一司法管轄區的可疑交易報告 (STR) 顯示，在部分案例中，網路詐欺犯罪所得會被轉移到特定衝突地區/司法管轄區，而這類地點均以恐怖活動著稱。

21. 此外，網路詐欺也與武擴融資有所關聯，例如報導指出，網路犯罪是朝鮮民主主義人民共和國 (北韓) 主要的非法收入來源。相關非法網路活動包括販售蒐集得來的個人資料，或提供駭客和網路釣魚的工具及服務，且可能由其他罪犯用於實施網路詐欺。[10]

10 另請參閱聯合國安全理事會 (2023 年 3 月)《*依第 1874 (2009) 號決議所設專家小組 2023 年 3 月 3 日致安全理事會主席函》(文號 S/2023/171)*

### 說明欄 6. 使用北韓網路釣魚工具進行網路詐欺以資助武器計畫

聯合國專家小組提供的資訊顯示，多名與北韓軍需工業部有關聯的北韓資訊科技 (IT) 從業人員，藉由販售語音網路釣魚駭客應用程式、營運多個海外伺服器和 IP 位址等方式賺取外匯。

2020 年 7 月，中國主管機關逮捕四名南韓籍人士，並將其引渡返回南韓。其中一人證稱，犯罪集團向北韓 IT 從業人員購買南韓民眾個人資料以及語音網路釣魚駭客應用程式。

犯罪集團欺騙被害人下載這些非法開發的工具，藉此竊取他們的更多資訊。隨後，他們再冒充金融機構員工誘騙被害人匯款。

註：詳細資訊請參閱聯合國安理會 (2022 年 9 月)《*依第 1874(2009) 號決議所設專家小組 2022 年 9 月 2 日致安全理事會主席函*》(文號 S/2022/668)

資料來源：聯合國專家小組及南韓

## 2.3. 洗錢技術和類型

### *洗錢網絡的結構*

22. 罪犯從各種網路詐欺獲取的犯罪所得，需透過快速、高效率的洗錢管道加以漂白。有司法管轄區發現，這類活動多由專業洗錢團體及第三方專業助力者共同參與，其中不乏律師、會計師、稅務顧問、公司秘書以及銀行從業人士。專業洗錢團體可能隸屬於網路詐欺犯罪集團，也可能是以「犯罪即服務」模式提供洗錢服務的去中心化獨立組織 (專業洗錢網絡)。

### 說明欄 7. QQAAZZ 網絡

在俄語體系的網路犯罪論壇上，QQAAZZ 將其服務宣傳為「全球同謀銀行空殼帳戶服務」，而網路罪犯會聚集在這類論壇中，提供或尋求各種網路犯罪活動所需的專業技能或服務。QQAAZZ 網絡在全球以空殼公司和人頭名義，在全球金融機構開立並維持數百個銀行帳戶，用於接收網路詐欺網路罪犯獲取的資金。然後，再將資金轉移至 QQAAZZ 控制的其他銀行帳戶，或者使用「滾幣」(tumbling) 服務轉換為加密貨幣，藉此隱匿原始資金來源。QQAAZZ 會抽取高達 50% 的佣金，再將剩餘贓款返還給罪犯客戶。

2020 年 11 月，一場 16 國合作的國際執法行動逮捕了 20 人，其涉嫌參與 QQAAZZ 犯罪網絡，企圖為全球犯行最重大的網路罪犯清洗數千萬歐元非法所得。此行動在拉脫維亞、保加利亞、英國、西班牙和義大利展開約 40 起入房搜查行動，並於美國、葡萄牙、英國和西班牙對被捕嫌犯提起刑事訴訟。

資料來源：葡萄牙和歐洲刑警組織

23. 通常，網路詐欺的犯罪所得會透過帳戶網絡迅速洗白。案例研究顯示，這類網絡可能橫跨多個國家和金融機構，形成錯綜複雜的結構，但此特性也因犯罪集團的老練程度而異。[11]

24. 與網路詐欺相關的洗錢帳戶網絡通常涉及個人和法律實體。

- 罪犯常以各種手段招募**個體錢騾**，包括發布職缺和廣告宣傳，以及透過網路社群媒體的互動。錢騾招募者又稱為錢騾的「管理人」。錢騾可能在知情狀況下成為洗錢共犯，抑或在無意間 (因受騙) 或因疏忽而參與犯罪；也可能因處理非法資金而獲得獎勵或酬金。錢騾的控制者 (即錢騾管理人) 會同時招募知情與不知情的共犯，因此難以追查其身分或詐欺資金的來源。部分司法管轄區指出，罪犯會招募與當地無明顯關聯的外國人，指示其親自臨櫃或以網銀方式開立錢騾帳戶。

11 有關專業洗錢者及網絡利用錢騾的手法，請詳見 FATF (2018 年 7 月)《*專業洗錢*》報告

### 說明欄 8. 錢騾招募手法：提供工作機會

RS 女士是一家雜貨店店主，在某位 O 先生的招募下，接受了她以為是合法的工作機會。O 先生是奈及利亞籍人士，曾於 2019 年因涉嫌價值數百萬美元的網路愛情詐欺案被捕，該案造成超過 800 萬菲律賓披索 (約 129,000 歐元) 的損失。

O 先生承諾 RS 女士經手每筆銀行交易，皆可從中抽成。RS 女士在六個月內共處理 83 筆交易，金額達到 360 萬菲律賓披索 (約 58,000 歐元)，且所有交易皆以現金進行 (即現金存款、ATM 和臨櫃提款)。最終在 RS 女士的配合下，執法機關成功誘捕了 O 先生。

資料來源：菲律賓

- **空殼公司**通常是由網路詐欺罪犯透過「稻草人」或代名董事控制的實體。受雇的個體錢騾也可能受派擔任這類稻草人，開立公司帳戶以進一步掩蓋罪犯的實質所有權。部分司法管轄區指出，空殼公司會利用虛擬營業地址[12]，進一步混淆犯罪活動。線上交易詐欺案例顯示，罪犯也會利用這類空殼公司，在商戶服務公司開設虛擬銷售點帳戶，用於處理被害人的付款和轉帳。

12 虛擬營業地址 (virtual business address) 是由特定服務業者提供的實體地址，以供企業接收郵件和包裹。

### 說明欄 9. 空殼公司線上交易平台詐欺

土耳其金融情報機中心接獲多筆可疑交易報告，均涉及同一起線上交易平台騙局，手法為透過電話或社群媒體誆騙被害人進行外匯投資。此騙局的基本運作方式，是透過 209 間公司所組成的網絡相互清洗犯罪所得，這些公司聘有共同會計師，且大多在同一天成立，並於短期內完成清算程序。

土耳其金融情報中心分析顯示，這些空殼公司也依據資金轉移及相關第三方個別共犯的活動，明確分為三種次團體。本案經查總共詐取並洗白約 100 億土耳其里拉 (約 3.367 億歐元)。

- 在這些空殼公司中，有 135 家透過支付業者收取 96 億土耳其里拉 (約 3.232 億歐元) 的詐欺犯罪所得。這些公司設立虛擬銷售點帳戶，以利接收被害人的交易款項，其中以現金提領 1 億土耳其里拉 (約 340 萬歐元)，並將約 60 億土耳其里拉 (約 2.02 億歐元) 轉移至一家黃金公司。
- 另有 59 家公司收取 7 億土耳其里拉 (約 2,360 萬歐元) 的詐欺犯罪所得，其中 2 億土耳其里拉 (約 670 萬歐元) 以現金提領，餘款則透過第三方個別共犯的帳戶洗錢，然後轉移至虛擬資產服務提供商。
- 其餘 23 家公司收取 8.75 億土耳其里拉 (約 2,950 萬歐元) 詐欺犯罪所得。其中 2.2 億土耳其里拉 (約 740 萬歐元) 以現金提領，餘款則透過第三方個別共犯的帳戶洗錢，然後轉移至虛擬資產服務提供商。

資料來源：土耳其

- **合法公司**亦可能面臨個體錢騾的類似處境，遭誘騙接收網路詐欺犯罪所得 (例如謊稱為投資或商業機會)，並受要求將資金轉移或返還至其他由犯罪集團控制的帳戶。觀察發現，合法公司會在特定情況下接受這類「商業機會」，尤其在經濟困難時期。合法公司的參與可營造額外假象，進一步掩蓋非法活動，使偵查更加困難。

25. 在洗錢網絡中，網路詐欺錢騾的培植方式，與別種犯罪的錢騾有所相似；但有司法管轄區觀察到若干差異之處，可能更符合網路詐欺錢騾的特徵。

- **招募方式：**罪犯較可能在線上招募網路詐欺錢騾，方法包括發布虛設公司的招聘廣告或垃圾郵件；亦可能利用經濟條件的弱點，將招募活動偽裝成「輕鬆賺錢」的工作機會誘騙對方。網路詐欺被害人 (例如在愛情詐欺案中) 經常遭誘騙淪為錢騾。在部分案例中，人口販運被害人 (例如非法移民或勞工) 也遭利用開設此類帳戶。

- **帳戶用途：**在網路詐欺中，罪犯會利用錢騾的金融機構帳戶，透過電子支付方法收發詐欺贓款，因為相較於實體轉帳或現金提存更快速，也可能由於罪犯即是以此方式騙取被害人的資金（即透過線上轉帳）。有鑑於數位銀行服務能夠便捷轉移資金，因此與網路詐欺相關的錢騾人選，通常都具備電腦和技術方面的基本知識及技能。

### 說明欄 10. 愛情詐欺被害人淪為錢騾

2022 年 4 月至 5 月期間，一名年長女性原本為領取退休金而開立的銀行帳戶收到兩筆異常高額款項。其中一筆匯款來自國內銀行帳戶，第二筆來自國外的報案被害人。

斯洛伐克主管機關隨後調查發現，該婦女透過社群媒體與某人通訊，並落入愛情騙局。這位年長婦女向詐欺犯提供網路銀行帳密資料，罪犯即利用其帳戶漂白其他犯罪所得。所接收的部分資金，則透過境外虛擬資產服務提供商平台兌換成加密貨幣。

資料來源：斯洛伐克

## *洗錢類型和技術*

26. 網路詐欺發生地（即被害人所在地）通常與相關犯罪所得洗錢地點不同，而且錢騾網絡可能橫跨多個司法管轄區。網路詐欺集團意識到，金融機構或權責機關可能會預先辨識出用於詐欺活動之帳戶，並搶在洗錢之前攔截犯罪所得，使其無法轉移至罪犯帳戶。為提高成功率，罪犯可能透過小額交易進行「測試」，一旦失敗隨即變換資金目的地。

27. 罪犯通常依據網路詐欺手法不同，來決定接收犯罪所得的第一層帳戶類型，以維持合法的假象。但也有觀察發現，第一層帳戶的類型已逐漸改變。例如在商業電子郵件攻擊詐欺案中，網路詐欺集團已從個人帳戶轉向使用企業帳戶，藉此降低偵查的風險。

## 表 1.網路詐欺類型與第一層帳戶類型的關係

| 網路詐欺類型 | 第一層帳戶類型 |
|---|---|
| 商業電子郵件攻擊詐欺 | 公司 (例如空殼公司或新註冊公司) |
| 網路釣魚詐欺 | 個體錢騾 |
| 社群媒體和電信冒名頂替詐欺 | 個體錢騾 |
| 網路交易/交易平台詐欺 | 公司 (例如空殼公司或新註冊公司) |
| 網路戀愛詐欺 | 個體錢騾 |
| 就業詐欺 | 個體錢騾 |

註：本表依各司法管轄區的經驗歸納整體趨勢，概述各類網路詐欺的第一層帳戶類型，但未必適用於所有情況。

28. 網路詐欺集團建立帳戶後，會迅速將詐欺贓款轉入洗錢網絡，隨後透過一系列「轉手」交易，藉由錢騾/稻草人名下或網路詐欺集團操控的國內外帳戶，迅速將資金分層清洗。在後一種情況下，錢騾會交出銀行憑證、銀行卡和代幣，或向網路詐欺集團提供授權書，允許其直接控制帳戶。此過程亦有專業助力者參與其中，例如代為擬定授權書，偽造合法交易的假象，以利掩飾犯罪事實。

29. 為了進一步躲避偵查和隱匿身分，網路詐欺集團會採用各種技術和機制，例如「化整為零」(smurfing)，即在不同金融、匯款或支付服務業者帳戶之間持續跳轉；以及轉換為其他類型金融資產 (例如電子貨幣[13]、預付卡、虛擬資產)。這可能導致金融情報中心和執法單位耗費更多時間，在不同國家、部門和機構取得必要的金融資料，才能夠追蹤、保護並追回非法犯罪所得。部分錢騾的帳戶可能僅允許在特定且有限的時間內使用。短促的時限加上合法的開戶程序，使相關機構更難偵查異常活動。

13 電子貨幣是數位形式的法幣，用途是以電子方式轉移法幣面額的價值。電子貨幣是法幣的數位轉移機制，即以電子方式轉移具法償地位的價值；FATF (2014 年 6 月)《*虛擬貨幣關鍵定義與潛在的防制洗錢/打擊資恐風險*》

### 說明欄 11. 空殼公司、銀行帳戶和虛擬資產

印度警方接獲多起投訴，稱一款行動應用程式假借加密貨幣挖礦投資平台的名義詐騙民眾，該應用程式承諾投資人可享獲利分紅，而相關公司設局引誘被害人投入更多資金後，隨即停止提款/支付功能。使用者無法存取網站和應用程式，且應用程式的系統業者也不再回應投資人。多個地方執法機構對印度各地相關客訴展開調查，要求印度金融情報中心提供案件資訊。印度金融情報中心分析發現，有兩家公司在 Google Play 商店營運該應用程式 (事發後即從 Google Play 商店下架)，另又發現 34 家公司與此兩家公司有所關聯，而在此 36 家公司當中，有 28 家是由外國人擔任董事。

印度執法局 (ED) 也同步展開洗錢防制調查，進而破獲一宗大規模共謀犯罪，及多家空殼公司參與經營類似的詐騙應用程式/網站，訛詐輕信易欺的民眾，從中榨取犯罪所得。經現場核實，相關公司均不在其登記營業地址。追蹤金流後發現，該等公司也參與經營非法博弈和貸款應用程式，並假借應用程式名義詐騙民眾。從被害人騙得的非法資金轉移至多家空殼公司帳戶，其中部分犯罪所得最終也轉換為虛擬資產。在各家空殼公司的銀行帳戶中，共查獲並凍結高達 8.65 億印度盧比 (990 萬歐元) 的犯罪所得餘額。

資料來源：印度

30. 亦有司法管轄區報告其他類型洗錢技術的使用，其旨在混淆不同網路詐欺和洗錢犯罪團體間的聯繫。

- **現金**：本報告的多起案例研究皆顯示錢騾和網路詐欺集團提取現金的行為特徵。在金融機構外部的現金流向可能難以追蹤。現金經過洗錢網絡漂白後，罪犯即可透過 ATM 提領，避免與金融機構當面接觸。這些資金可能交由現金運送者移出境外，再存入銀行進一步洗白。犯罪所得也可用於購買貴重物品和工具 (如預付卡或貴金屬)，然後轉售變現。

### 說明欄 12. 提領現金購買黃金及加油卡

2023 年 3 月，一家中國公司的會計師遭遇冒名詐欺。對方佯稱必須公司帳戶需進行年度查核，以此為由將他加入通訊應用程式的群組中。

隨後，通訊群組中的罪犯冒充公司法定代表人和股東，要求被害人將 780 萬元人民幣 (約 99.6 萬歐元) 轉入該犯罪集團控制的兩個指定公司帳戶。警方調查顯示，這些資金轉移到 26 個二級銀行帳戶，然後臨櫃或從 ATM 擷取現金、轉移至第三方支付平台，以及用於購買黃金和加油卡。

資料來源：中國

- **貿易/服務型洗錢：**罪犯可能利用各種貿易/服務型洗錢技術來跨境轉移犯罪所得。[14] 部分司法管轄區發現罪犯使用貿易型洗錢 (TBML) 技術漂白網路詐欺犯罪所得，例如開立偽造或虛假的發票，以及使用非法犯罪所得購買高價值或易銷商品 (例如車輛零件、票證、家居用品等)。例如，部分司法管轄區報告指出，罪犯會進行詐欺性質的電匯，向知名奢侈品牌、電子品牌及地方小型企業等合法公司購買商品，而這些商品可以運送出境，然後轉換回現金，進一步分層和整合。未落實洗錢防制/打擊資恐制度的商業組織，可能缺乏足夠的警覺或知識，無法有效執行身分驗證或交易監控措施，並於不知情狀況下遭罪犯利用。為 IT 或顧問服務開立超額或虛假發票，也可能是罪犯會採用的洗錢手法。

14 另請參閱 FATF – 艾格蒙聯盟 (2020 年 12 月)《*貿易型洗錢：趨勢和發展*》；以及 FATF (2018 年 7 月)《*專業洗錢*》報告

### 說明欄 13. 網路詐欺、錢騾和貿易型洗錢

愛爾蘭當局逮捕一位名為 MS 的關鍵人士，該人涉嫌透過貿易型洗錢手法，將愛情詐欺和商業電子郵件攻擊網路詐欺的犯罪所得從愛爾蘭轉移至奈及利亞清洗，本案仍在調查當中。截至目前，主管機關研判洗錢計畫至少涉及 60 人和 64 個銀行帳戶。

在此騙局中，詐欺犯罪所得先轉入愛爾蘭錢騾的銀行帳戶，然後以現金提領並轉入與 MS 直接相關或其所持有的愛爾蘭帳戶。許多與 MS 相關的帳戶經查明是以虛假身分開設。

一家奈及利亞公司（由一名據信位於美國的奈及利亞人控制）向合法的歐洲或中國公司訂購商品。這些合法公司營銷各種可供購買、運輸並轉售的貨品，包括酒類、服裝、電子產品和藥品。罪犯使用 MS 的愛爾蘭帳戶支付相關發票，最終將貨品運往奈及利亞的共謀公司。

例如，一家德國製藥公司收到 170 萬多歐元的資金，用於支付這家奈及利亞公司購買的貨品。而這些資金可直接追溯到歐洲和美國的商業電子郵件攻擊網路詐欺和愛情詐欺的犯罪所得，來源為 MS 關聯或持有的各種帳戶，或是直接從被害人的帳戶轉出。這些貨物最終被運往奈及利亞。

資料來源：愛爾蘭

- **未經許可或未註冊的匯款業者和虛擬資產服務提供商：**犯罪所得可能會透過地下匯款或哈瓦拉（Hawala）服務轉移至司法管轄區境外，而這類管道經常缺乏足夠的洗錢防制/打擊資恐控管措施。在涉及虛擬資產的情況下，犯罪集團可能會選擇洗錢防制/打擊資恐控管不足的司法管轄區，利用當地的虛擬資產服務提供商洗錢。
- **虛擬資產匿名強化技術：**[15] 要將虛擬資產相關的網路詐欺犯罪所得快速洗出司法管轄區，首選方法包括使用非託管錢包、點對點交易、剝離鏈和高風險交易所，這些都是罪犯經常結合運用的手段。此外，罪犯也會使用比特幣 ATM 來轉移資金、掩飾資金控制者身分，包括以偽冒或變造的身分證件（例如篡改識別碼、電話號碼或出生日期）來存入或提領資金。其亦採取混淆手法，包括使用混幣器或滾幣器服務、匿名強化型虛擬資產（又稱隱私幣，例如門羅幣）以及去中心化金融（DeFi）服務。

15 FATF (2023 年 3 月)《*打擊資助勒索軟體*》詳盡介紹了這些手法。

### 說明欄 14. 橫跨多部門的複雜洗錢案例

某個境外愛情詐欺集團鎖定大約 70 名日本被害人為下手目標。本案共計 300 萬美元資金轉入日本的多個錢騾銀行帳戶。一名日本男子擔任當地錢騾管理人，將資金洗到詐欺集團的總部所在地迦納。最終在迦納的合作下，國際刑警組織逮捕了該名日本男子。

隨後，錢騾帳戶上的資金被轉入日本錢騾管理人的帳戶。可疑交易報告分析發現，日本錢騾管理人透過三個管道洗錢：

- 將贓款電匯至日本錢騾管理人在迦納持有的銀行帳戶。然後，在迦納以現金提領贓款，交給仍在逃的犯罪集團首腦。進行電匯時，該日本男子向其在日本開戶的銀行出示虛假發票，謊稱用於合法商業活動 (購買可可豆)。
- 部分資金經由日本的虛擬資產服務提供商兌換成虛擬資產。
- 亦有資金透過一間與日本迦納社群有關的地下銀行轉移到迦納。

資料來源：日本

## *數位化和新技術對洗錢的影響*

31. 新技術為消費者帶來嶄新的效益和機會。金融服務業正經歷深刻的數位化轉型，而 COVID-19 疫情更加速了這波進程。現金使用量的減少和線上活動的增加，催生各種創新的工具和流程。金融支付鏈也益趨動態和分散化，支付和交易服務業者的多樣性不斷增加 (另見下文第 3.1 節)。

32. 然而，技術發展也可能成為犯罪集團的優勢，他們可藉此機會大幅改進洗錢技術。此外，由於消費者都期望順暢便捷的體驗，促使更多金融交易能以近乎即時的速度完成。再加上前述的 VPN 等數位匿名技術，罪犯得以快速、連續進行洗錢交易，使監管機關難以追查幕後首謀。

33. 數位化技術讓罪犯更輕易迅速設立洗錢帳戶，並擴大網路詐欺集團跨境作案的勢力範圍。部分司法管轄區指出，民眾愈來愈常在線上辦理兩種手續，其分別為銀行開戶和成立公司。這類遠端虛擬流程無需當事人親自前往實體場所，進而給予罪犯洗錢的可趁之機。

### 說明欄 15. 透過數位化擴大規模

金融情報中心分析發現一個龐大網絡組織，由 147 名個人和分布於 8 家銀行的 276 個銀行帳戶組成。該等人將其國民數位身分 (原本用途是供政府及其他線上平台識別使用者身分) 交給犯罪集團。然後，相關集團使用這些數位身分，以遠端方式開設並直接操控錢騾銀行帳戶，用於清洗網路詐欺犯罪所得。金融情報中心比對發現該等帳戶的共通之處，例如共同銀行交易、資料點 (境外聯絡資訊和裝置 ID) 以及聯絡詳細資料 (郵寄地址、電子郵件、電話)，從而偵獲此犯罪網絡。

此情報提交給新加坡警察部隊轄下專責打擊網路詐欺及相關洗錢活動的的反詐騙指揮處 (ASCom)。ASCom 偵辦此案後，最終逮捕 6 名涉案者，並因他們在詐欺案中的角色起訴其中 3 人。

資料來源：新加坡

34. 憑藉數位工具，犯罪者可以招募境外錢騾，迅速擴大錢騾網絡規模，通常橫跨不同國家。社群媒體和網路電話 (VoIP) 應用程式，也已成為招募錢騾的首選媒介。傳統上，透過錢騾網絡洗錢較為耗時，因為錢騾需等待接收並遵行其他犯罪集團下達的指示。如今網路詐欺集團使用即時通訊平台，已大幅縮短這種時間差。

35. 罪犯可能會更常使用各種手法和技術工具竊取身分，包括網路釣魚、以購買或誘騙方式使被害人自願交出身分資訊。有時，罪犯可能使用偽造身分和合成身分，這類手法會混用真實和虛假的身分資訊，藉此開設用於詐欺之帳戶，然後利用遭竊或偽冒的身分直接設定和操控帳戶。這導致洗錢活動更難追查，因為帳戶持有人甚至可能不知道自己涉入其中。

36. 某一代表團指出罪犯利用深偽技術 (deepfake) 從事帳戶接管 (account takeover) 詐欺的風險。藉助深度學習演算法，詐欺犯可使用深偽技術仿造某人的語音或影像，在電話或生物辨識驗證系統中冒充該人。深偽技術亦可與社交工程手法結合使用，誘騙被害人交出其帳戶的帳密憑證。深偽技術仍屬於新興階段，目前用於帳戶接管詐騙的風險尚稱有限。但若此技術持續發展並益趨普及，日後恐將形成重大風險。

### 說明欄 16. 遠端盜竊並直接操控身分

在一系列網路釣魚相關詐欺中，罪犯誘騙被害人在電腦上安裝遠端存取工具。在許多案例中，罪犯以被害人名義向虛擬資產服務提供商開立帳戶，而被害人毫不知情。罪犯利用了遠端存取工具所竊取的資料，因此得以成功開戶。罪犯也涉嫌使用遠端存取工具隱藏實際的操作介面，引導被害人完成線上開戶的驗證流程。

被害人最終受騙，將資金轉入虛擬資產服務提供商的帳戶。然後，犯罪者即可直接利用這些虛擬資產服務提供商帳戶進行洗錢。在此一系列案件中，被害人據估計總共損失超過 60 萬歐元。

資料來源：奧地利

# 3. 其他新興洗錢漏洞

37. FATF 標準 (第 9 至 23 項建議 ) 訂有基本要求，規定金融機構、指定之非金融事業或人員 (DNFBP) 及虛擬資產服務提供商採取預防措施，防止網路詐欺犯罪所得流入金融和其他部門。本節重點介紹網路詐欺集團可能利用的新興洗錢漏洞。

## 3.1. 數位金融機構產生的風險[16]

38. 隨著金融支付的進展，新型數位金融機構應運而生，例如支付服務業者 (PSP)、電子貨幣發行機構等。相較於這類新興數位金融機構，傳統金融機構可能擁有更多資源，控管機制也相對穩健。有鑑於此，罪犯可能會轉移目標，試圖利用上述非傳統金融業者的漏洞洗錢。

39. 支付網絡也可能呈現分散型態，這類機構彼此形成各種嵌套式的金融關係，例如不同支付機構間相互交易，或向規模較小的業者提供帳戶，而這些小型業者又進一步提供其他類型的金融服務 (另請參閱下方說明欄 17)。在分散化的趨勢下，要追蹤「支付鏈」中各類機構的交易更加困難，也較不易立即查明支付鏈各環節轉帳活動，以掌握有關匯款人及受款人的基本資訊[17]。

40. 依 FATF 標準，各司法管轄區應嚴格監管新興金融機構，包括實施適當的許可或註冊制度，並防止罪犯及同夥操控這些實體。監管機關應確保所有交易機構充分監督各自業務領域，所有機構均有責任對匯款人及收款人節點執行或確保適當的客戶盡職調查 (CDD) 和交易監控。

16 本報告亦指出虛擬資產及虛擬資產服務提供商產生的洗錢風險。有關虛擬資產服務提供商相關的法規風險和挑戰，請詳見 FATF (2023 年 3 月)*《打擊資助勒索軟體》*及 (2023 年 6 月)《*虛擬資產： 虛擬資產與虛擬資產服務提供商實施 FATF 國際標準之現況*》。

17 FATF 目前亦考慮修訂第 16 項建議 (電匯相關主題)，以因應支付系統架構中近期演進和即將問世的發展。

### 說明欄 17. 支付服務業者遭濫用

法國監管機關在 2021 年上半年的分析發現，若干主要的支付服務業者遭利用接收詐欺電匯款項。這些主要支付服務業者通常提供「銀行即服務」解決方案，其中部分機構在法國設有分行，唯一目的為提供法國的國際銀行帳戶碼 (IBAN)，實體場址規模極小。

分析發現，這些主要支付服務業者風險大約為其他機構的 200 倍，其身分驗證和交易監控措施大多十分薄弱。罪犯利用竊得的身分開設帳戶，先嘗試小額交易，迅速確認支付服務業者是否識破詐欺帳戶，並於必要時變更資金目的地。然後，他們再將詐欺所得資金快速轉移到一或多個帳戶。透過將資金拆分至多個帳戶，罪犯得以規避支付服務業者實施的服務管制措施，例如現金提領限額，或要求保持在內部制定的營運監控限值以內。

資料來源：法國

## 3.2. 虛擬國際銀行帳戶碼的濫用[18]

41. 利用金融創新成果進行網路詐欺的另一案例，即是濫用虛擬國際銀行帳戶碼 (vIBAN)。諸如銀行和支付服務業者等多種機構，均會向客戶核發虛擬國際銀行帳戶碼。虛擬國際銀行帳戶碼雖有多種合法用途，例如促進及分類多方支付流程，但部分司法管轄區已發現，罪犯會濫用虛擬國際銀行帳戶碼，進行網路詐欺的相關洗錢。

18 有關虛擬國際銀行帳戶碼的相關風險和挑戰，請詳見：(2023 年 6 月)《*歐洲刑警組織金融情報公私合作夥伴關係 (EFIPPP) 關於虛擬國際銀行帳戶碼的威脅情報資訊》(僅適用於 EFIPPP 會員)*。

## 說明欄 18. 什麼是虛擬國際銀行帳戶碼？

虛擬國際銀行帳戶碼在功能上與傳統國際銀行帳戶碼相同，皆可在全球收發付款。此數碼甚至沿襲傳統格式，同樣由最多 34 個字母與數字的字元組成。因此在功能和外觀上，其與常規國際銀行帳戶碼並無區別。

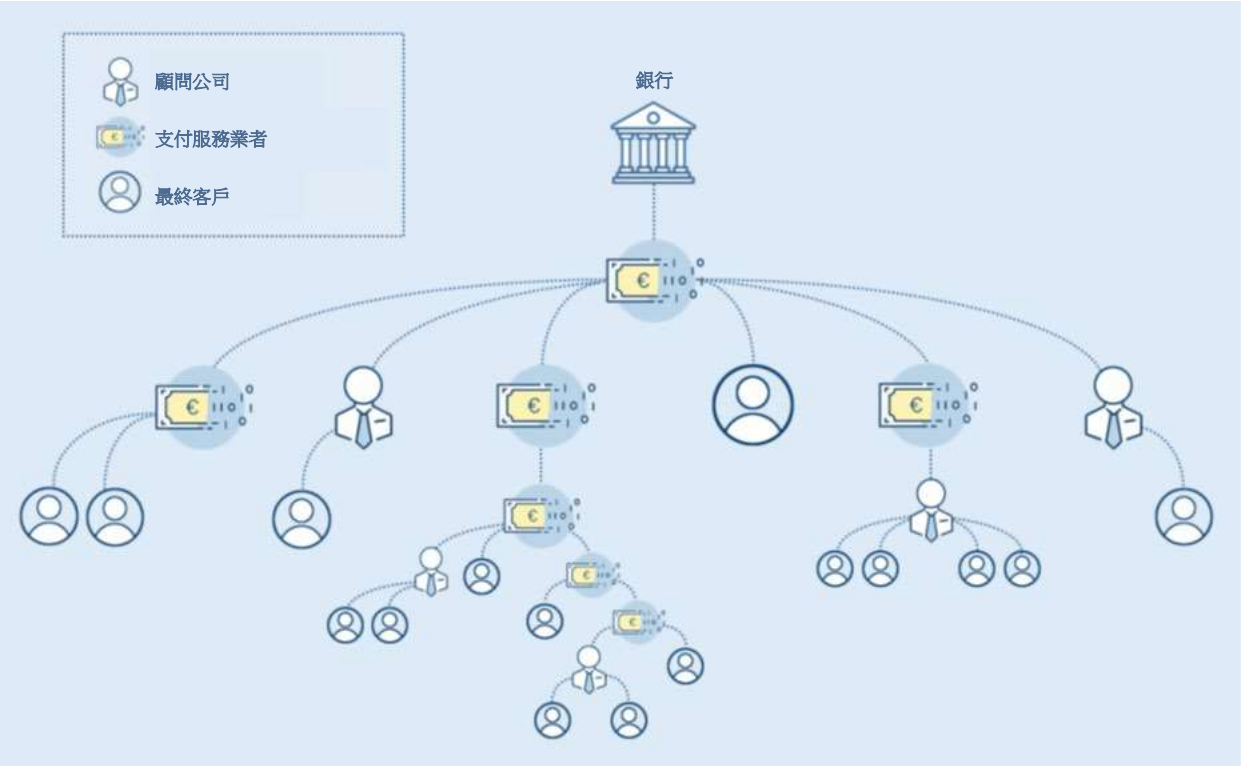
常規與虛擬國際銀行帳戶碼之間的主要區別在於帳戶配對方式。常規國際銀行帳戶碼與銀行帳戶之間為一對一的匹配關係，亦即每個國際銀行帳戶碼僅關聯至單一實體銀行帳戶。因此，若有人使用國際銀行帳戶碼付款，資金會自動存入與該碼關聯的銀行帳戶。

相對之下，虛擬國際銀行帳戶碼屬於虛擬號碼，並無對應的實體銀行帳戶。其為銀行核發的參考編號，可將入帳款項轉移至實體國際銀行帳戶碼，而後者本身則連結某一實體銀行帳戶。這些虛擬號碼並不持有任何資金，其餘額一律為零。持有人亦可持有多組不重複的虛擬國際銀行帳戶碼，將所有款項集中轉移至單一實體銀行帳戶，如圖 3 所示。


資料來源：歐洲刑警組織金融情報公私合作夥伴關係

42. 由於常規與虛擬國際銀行帳戶碼外觀相同，罪犯利用這一點欺騙被害人，例如使其誤信匯款至銀行帳戶，事實上卻是轉入虛擬國際銀行帳戶碼，用來為某個電子錢包儲值。更棘手的是，金融機構可向客戶重發虛擬國際銀行帳戶碼，尤其是對另一家同為金融機構的客戶。如此將更難查明虛擬國際銀行帳戶碼的來源國以及主帳戶。

## 圖 2.金融機構核發和重發虛擬國際銀行帳戶碼的傳遞網絡




資料來源：歐洲刑警組織金融情報公私合作夥伴關係

43. 簡言之，罪犯可能會濫用虛擬國際銀行帳戶碼隱匿最終實質受益權資訊，並掩蓋非法資金流向，導致難以確認真正的主帳戶及發碼金融機構，且不易落實適當的交易監控措施。最終，權責機關將難以查獲實體帳戶並凍結資金 (因為虛擬國際銀行帳戶碼僅為銀行核發的參考號，而非存有實體餘額的實際帳戶)。為此，部分司法管轄區已採取良好做法，與核發虛擬國際銀行帳戶碼的銀行合作，力求在發現網路詐欺當下，迅速查明與主帳戶關聯的支付機構。

### 說明欄 19. 虛擬國際銀行帳戶碼遭濫用於網路詐欺

2023 年 2 月至 3 月期間，盧森堡金融情報中心接獲多起「嗨！媽媽」(Hi Mum) 詐騙報案，歹徒冒充被害人子女，使用陌生本地電話號碼向被害人發送 WhatsApp 訊息，被害人收到以盧森堡手機號碼傳來的盧森堡語簡訊，其中附有一組盧森堡國際銀行帳戶碼。

偵辦本案期間，盧森堡金融情報中心發現詐欺犯提供的是虛擬國際銀行帳戶碼，均由盧森堡銀行機構核發給國內的支付服務業者，而後者則向歐洲客戶提供預付信用卡。使用者轉帳至虛擬國際銀行帳戶碼，即可為這類預付信用卡儲值，而罪犯則圖謀利用虛擬國際銀行帳戶碼，進一步清洗贓款。

本案查獲 6 組用於詐欺的虛擬國際銀行帳戶碼，詐取資金共計 55,000 歐元，盧森堡金融情報中心成功凍結或追回其中 40,000 歐元。盧森堡金融情報中心的行動成果，應歸功於其與核發虛擬國際銀行帳戶碼的銀行相互合作，方可快速識別最終客戶相關帳戶所在的支付機構。

Source: Luxembourg
資料來源：盧森堡

## 3.3. 非傳統部門

44. 許多司法管轄區強調與非傳統部門合作的重要性，包括社群媒體平台、電子商務、電信和網際網路服務業者，必須共同打擊網路詐欺相關的洗錢犯罪。這類非傳統部門雖不屬於防制洗錢/打擊資恐監管範圍，但具備各種實用資訊，有利於偵辦洗錢案件，特別是其遭利用進行網路詐欺和招募錢騾的情況。社群媒體平台以及電信和網路服務業者可以提供重要的數位鑑識資訊，包括 IP 位址、電話號碼、電子郵件地址等，有助於追查最終的犯罪首謀。若罪犯透過詐欺性的網站或廣告進行網路詐欺，這些部門亦持有與罪犯相關的金融交易和支付資訊 (例如託管網站、廣告費用之付款明細等)。

45. 各司法管轄區的經驗和案例研究也顯示，罪犯如何濫用電子商務或社群媒體、串流媒體或遊戲平台，作為清洗網路詐欺犯罪所得的管道。社群媒體、串流媒體或遊戲平台日益普及，使用者可以接收來自觀眾和公眾的捐贈、禮物、代幣或積分。但這類平台通常未被要求遵守洗錢防制/打擊資恐規定，可能遭罪犯用於清洗犯罪所得。

### 說明欄 20. 透過社群媒體和串流平台清洗網路釣魚犯罪所得

調查發現，罪犯對特定銀行的客戶發動網路釣魚攻擊，造成 19 個銀行帳戶蒙受損失。德國金融情報中心分析顯示，這些銀行帳戶交易是透過兩名使用者持有的支付帳戶進行，相關資金隨後傳送至社群媒體和串流媒體平台，為使用者在串流媒體平台上的帳戶儲值，轉換為串流媒體平台上的「代幣」(平台使用者彼此交易用的原生貨幣)，用於購買虛擬禮物。這些禮物可傳送給內容創作者，而後者又可將此代幣進行兌換為普通貨幣，並提領相等幣值的現金。

相關調查正著手進行中。記錄資料顯示，詐欺交易均是透過相同登入 IP 位址進行。金融情報中心分析顯示，同一名罪犯透過社群媒體和串流平台清洗大部分的網路釣魚犯罪所得，以便隨即兌換為現金。

資料來源：德國

# 4. 國家行動因應措施和策略

46. 本章首先討論司法管轄區偵查網路詐欺所依據的關鍵資訊來源，隨後探討境內的協調和合作架構，以及司法管轄區如何藉此架構調查和防止網路詐欺和相關洗錢行為。

## 4.1. 主要偵查情報來源

47. 根據各司法管轄區的經驗和案例研究，偵查網路詐欺相關洗錢有兩個主要資訊來源：被害人報案和可疑交易報告 (STR)。

48. 司法管轄區也採取各種措施提升報案率，以期充分利用所有可得資訊，進而提升執法成效。權責機關憑藉這些資訊和資料，採用數位策略和工具分析和識別犯罪集群，以利採取更有效、更具目標性的執法行動。[19]

### *被害人報案*

49. 被害人報案是偵查網路詐欺相關犯罪所得的重要情資來源。在商業電子郵件詐欺和網路釣魚等特定詐欺案件中，被害人通常較快自覺受騙 (例如合法的交易對手開始要求繳交欠款)。在投資詐欺、愛情詐欺或網路釣魚等其他類型的網路詐欺案中，被害人可能經過一段時間後才驚覺上當。

50. 被害人及時報案，對於權責機關迅速採取行動追查犯罪所得非常重要，且可提高執法行動的成功率。被害人可向執法機關舉報疑似犯罪行為，包括負責受理詐欺報案的專門單位。若發現帳戶疑似出現詐欺交易，被害人亦可通報金融機構、支付服務業者和虛擬資產服務提供商。其他司法管轄區指出，除執法機關以外，被害人也可以聯絡金融消費者保護機構。

51. 然而，並非所有網路詐欺被害人都會報案，尤其是僅蒙受輕微損失的情況，加上感到難堪或恐懼等情緒因素，被害人可能會決定默不作聲。

52. 部分司法管轄區採取良好實務來提升被害人報案率，設置專門的平台 (包括線上入口網站) 供被害人舉報網路詐欺。這些平台可提供結構化的報告格式，實現標準化的資料記錄流程，促進被害人報案的集群分析，且有助於識別犯罪趨勢和模式。這些平台亦可提供實用資源，以利防範網路詐欺和援助被害人。

19 有關金融情報中心和執法機構如何利用數位轉型，以實現有效的防制洗錢/打擊資恐分析和調查能力，請詳見艾格蒙聯盟 - FATF (2021 年 10 月) 的機密報告《防制洗錢/打擊資恐執行機關之數位轉型：*可疑活動偵測與金融情報分析 (第一階段)*》及 FATF (2022 年 5 月)《*執法機關及資訊交換 (第二階段)*》。

### 說明欄 21. 英國 Action Fraud 反詐騙機構

Action Fraud 是英國全國性的詐騙和網路犯罪通報中心，提供集中聯絡窗口，專門受理詐欺和基於謀財動機的網路犯罪，由倫敦市警察局和國家詐騙情報局 (NFIB) 共同管理。Action Fraud 網站提供各種公眾宣導資源，指在預防犯罪，以及保護和援助被害人。

Action Fraud 也營運全年無休的 24 小時線上入口網站，專供被害人報案使用。Action Fraud 接獲報案後，會傳交給國家詐騙情報局，由後者對全英國各地進行評估和分析，追查最終的犯案首謀。然後，相關報告會發送給英國境內的相關地方警隊進行偵辦。國家詐騙情報局也會利用這些報告記錄詐欺犯使用的銀行帳戶、網站和電話號碼。

資料來源：英國

## *可疑交易報告*

53. 有鑑於被害人可能未如實報案，可疑交易報告即成為偵查網路詐欺相關金流的重要獨立情資來源。

54. 根據金融情報中心蒐集的資料，大多數與網路詐欺相關的 可疑交易報告均是由銀行業提交。然而，隨著網路詐欺集團作案手法不斷進化，銀行應繼續加強偵查網路詐欺和相關洗錢的能力。資料也顯示，金錢價值移轉服務 (MVTS) 和虛擬資產服務提供商提交的可疑交易報告較少，後者的可能原因在於，部分司法管轄區未充分依循 FATF 標準，據以監管虛擬資產服務提供商產業。[20]

55. 由於網路詐欺犯罪所得可能散逸流失，因此必須確保及時分析與網路詐欺相關的可疑交易報告。部分金融情報中心系統設有優先性排序系統，用於篩選大量可疑交易報告並專注於風險較高者，其中即包括網路詐欺相關可疑交易報告。其他機構則對金融情報中心人員進行網路詐欺相關洗錢風險的培訓，使其能夠篩選並分類所收到的網路詐欺可疑交易報告。上述措施皆有利於金融情報中心及時分析，使執法機關得以迅速追查網路詐欺案件。

20 另請參閱 FATF (2023 年 6 月)《*虛擬資產：虛擬資產與虛擬資產服務提供商實施 FATF 國際標準之現況*》。

### 說明欄 22. 網路詐欺相關可疑交易報告的優先性排序和集群分析

2021 年至 2022 年，智利金融情報中心收到 1,500 多份涉及線上交易平台騙局的可疑交易報告。為處理如此大量的資料，智利金融情報中心採用集群技術進行分析，在可疑交易報告中發現特定模式。

金融情報中心採用文字探勘工具，根據偵測到的關鍵字和已知短句進行分析。隨後依分析結果識別出地理集群，將目標明確且經多方彙整的案件資料呈交檢察署偵辦。透過集群分析，使調查得以發現，這些資金後來透過 ATM 提領，再轉手給組織犯罪集團的高階成員。

資料來源：智利

56. 除了偵查之外，司法管轄區也致力宣導正確觀念，以及進一步改善通報機制。許多司法管轄區發布特定形式的網路詐欺相關準則，或針對銀行及其他部門人員舉辦教育研討會，提高整個產業對最新網路詐欺趨勢和洗錢類型的認識。另請參閱附錄 A 風險指標彙編，該資訊可能有助於改善網路詐欺偵查成效。其他司法管轄區的金融情報中心則編製了有關網路詐欺的策略分析文件。這些措施旨在加強銀行第一線員工的能力，以期更有效偵防詐欺及洗錢活動。

### 說明欄 23. 關於網路詐欺錢騾的策略分析

西班牙金融情報中心進行一項策略分析，著重於瞭解一項已知的錢騾特徵：同一人於 20 日內，在三家以上金融機構開設銀行帳戶。該研究根據 2020 年 12 月至 2022 年 2 月銀行帳戶登記處 (BAR) 資訊發現近 40,000 個其他銀行帳戶與大約 10,000 人有所關聯。在已識別的銀行帳戶中，有 15% 在西班牙金融情報中心資料庫中查到相符資料。這些帳戶歸類為高風險等級，並協同四家金融機構展開先導研究計畫，以加強瞭解這些帳戶的風險概況。

此先導計畫旨在防止網路詐欺和其他可能的詐欺行為，並增進與私部門的合作成效，亦盼能加強金融機構發現系統缺失的能力，深入瞭解網路詐欺活動現況，以利偵防更多潛在犯罪行為。最終，此先導計畫成功實施交叉檢查系統，運用銀行帳戶登記處資料，主動偵測網路詐欺相關的洗錢網絡。

資料來源：西班牙

## 4.2. 境內的協調與協作

### *權責機關之間的協調*

57. 鑑於網路詐欺（CEF）的跨領域性質，各國境內各機構之間顯然需要強而有力的協調。部分司法管轄區採用全政府策略方法進行協調，引導當地落實防制網路詐欺的相關政策。此方法需設立統籌式的跨部門機構，由司法、執法、監管及資訊通訊領域的關鍵部會組成。協調一致的方法可讓司法管轄區識別重大漏洞，並制訂跨關鍵部門的全方位政策因應措施。

58. 國內各部門在行動上的協調，亦可動員技術機構參與其中，以期強化偵蒐及調查能力，包括：

- 建立金融情報中心、警察和檢察官之間的溝通管道，以確保實施集中化通報機制、簡化情資和證據交換，以及執行凍結和扣押資產的指令。亦可能包括使用自動化的資料分類技術，協助判定可能須注意的相關事項，並迅速識別適當的執法機關，指派其偵辦任務。由於網路詐欺罪犯可能在司法管轄區內各處鎖定被害人下手，因此這類協調亦可減少執法工作的重複性（請見下文「適當劃分權責」一節）。
- 延請科技網路犯罪專家提供支援，尤其是涉及網路入侵、其他技術基礎設施犯罪以及隱私保護機構的情況。這反映了網路詐欺的多面性，以及數位鑑識證據（如 IP 位址、網際網路網域相關識別碼等）對於識別網路詐欺犯罪集團及推動洗錢調查進展的重要性。

#### 說明欄 24. 聯合警務網路犯罪協調中心

聯合警務網路犯罪協調中心（JPC3）是由澳洲聯邦警察（AFP）領導的機構。JPC3 的成員包括聯邦和各州執法機關、澳洲交易報告與分析中心(AUSTRAC)等政府分析機構，以及澳洲各銀行的分析師等產業合作夥伴。JPC3：

- 協調澳洲警方應對高度危害、數量龐大的網路犯罪，以最大力度整肅犯罪環境；
- 加強聯邦、各州和領地警方及產業的情報交流和目標擬定；
- 協調警方與產業合作夥伴組成聯合任務小組，以應對首要的網路犯罪威脅；
- 協調全國各部門共同提升能力，方法包括交叉技能訓練、聯合培訓，以及開發協作工具；以及
- 向全國產業和公眾傳達一致的防詐教育、觀念宣導和媒體活動。

JPC3 能與產業和公領域合作推行防詐政策，共同打擊網路犯罪。為有效支援 JPC3，AUSTRAC 也設有一支金融網路犯罪團隊，透過專門提供有關網路實施型（cyber-enabled）和網路依賴型（cyber- dependent）金

融犯罪（包括網路詐欺洗錢）的金融情報。

2020 年 1 月，AFP 成立 DOLOS 行動組，此為 AFP 領導的多機構特別任務小組 [1]，旨在打擊實施或協助商業電子郵件攻擊的跨國網路罪犯。DOLOS 行動組與商業電子郵件攻擊受害者（包括澳洲公民和中小企業）合作，阻止犯罪所得流入或流出商業電子郵件攻擊集團。自 DOLOS 行動展開以來，任務小組開發各種新技術，減輕了澳洲公民和企業蒙受的損害。2022 年 7 月 1 日至 2023 年 6 月 30 日期間，DOLOS 行動破壞罪犯的金融運作模式，成功保護澳洲及國際被害人免於 3,060 多萬澳幣的損失。

資料來源：澳洲

1 該任務小組成員包括各州和領地警察、情報和網路安全機構、金融情報中心以及金融部門。

### *與私部門的行動夥伴關係*

59. 司法管轄區也尋求透過公私合作夥伴關係（PPP）與私部門合作。這些公私合作夥伴關係有助於改善偵查工作負荷，交換戰術情資以識別隱藏的洗錢網絡，並強化資產返還的應對行動能力。

#### 說明欄 25. 計畫：快速防詐行動

斯里蘭卡金融情報中心啟動一項名為「快速防詐行動」(RAPS) 計畫，一旦被害人通報潛在的網路詐欺，計畫就會立即採取行動。其目標是集結金融情報中心和金融機構的法遵主管，快速偵查罪犯及其同夥使用的非法帳戶活動，進而遏阻斯里蘭卡金融體系中的詐欺行為，其中即包括網路詐欺。

此機制包括根據公眾投訴的資訊，查出詐欺犯的帳密憑證，並將相關資料提供給金融機構的法遵主管。金融機構依此資訊監控潛在詐欺犯的帳戶活動，並採取適當行動阻止其使用金融系統，藉此防範詐欺行為。此外，本計畫也會將詐欺犯的資訊交給斯里蘭卡警方，以便對相關嫌犯進行調查。

資料來源：斯里蘭卡

60. 鑑於網路詐欺及相關洗錢風險顯著提高，眾多司法管轄區在執法機關或監管機構中設立集中化應變中心，以加強對網路詐欺展開反制行動，並提高公眾意識（有關反網路詐欺專責單位，另請參閱下文章節）。良好的實務做法之一，是讓金融機構和虛擬資產服務提供商的代表共同駐點於這類集中式應變中心，能以近乎即時的速度存取金融資料，並橫跨各金融實體和部門進行追蹤，進而加快權責機關攔截和凍結資金的能力。

### 說明欄 26. 各家銀行專員共同駐點

沙烏地阿拉伯為各家銀行設立一間聯合行動室（JOR）。JOR 的任務是追蹤和監控銀行客戶可能遭遇的金融詐欺案件。JOR 在單一統籌架構下，集結所有銀行和相關金融機構資源，致力解決已確認的金融詐欺案件。

JOR 由沙烏地阿拉伯各家銀行共同主持，旨在促進協力合作，維護銀行業穩定發展。JOR 全年無休 24 小時營運，致力在沙烏地阿拉伯所有銀行之間實現快速有效的合作和整合，以遏制詐欺案件發生，迅速回應詐欺投訴案件，盡可能即刻採取措施防範詐欺行為。

資料來源：沙烏地阿拉伯

61. 這些夥伴關係也提供實用平台，可交流最佳實務和常見態樣，共同擬定打擊非法活動的建議措施。

### 說明欄 27. 歐洲刑警組織金融情報公私合作夥伴關係

歐洲刑警組織金融情報公私合作夥伴關係（EFIPPP）是第一個以洗錢防制/打擊資恐宗旨而設立的跨國資訊交流公私合作機制。EFIPPP 匯集歐盟和非歐盟國家的執法機構、金融情報中心和私人實體。

EFIPPP 內的威脅和態樣任務小組專門負責網路詐欺相關的各種主題及不同犯案手法，包括商業電子郵件攻擊、投資詐欺、錢騾帳戶、虛擬國際銀行帳戶碼及加密資產。雖然 EFIPPP 目標是提出策略性態樣報告，但亦可作為交流平台，探討如何促進成員之間的合作。

資料來源：歐洲刑警組織

62. 公私合作夥伴關係的組成方式不一。許多司法管轄區仍關注傳統利害關係人（尤其是銀行和其他金融機構），但指定之非金融事業或人員、虛擬資產服務提供商及其他非傳統部門（例如電信業務系統業者和網路服務業者）的涉入程度日益增加。具體組成取決於公私合作夥伴關係的宗旨和目標。

### 說明欄 28. 與電信部門的合作

近年來，中國持續推動加強打擊和防治電信網路詐欺，並於 2022 年 12 月 1 日正式實施《中華人民共和國反電信網絡詐騙法》，旨在提供強而有力的法制保障，打擊並阻止電信網路詐欺犯罪活動，並已有效遏止相關犯罪行為。

此法匯集公部門主管機關（包括執法、金融、電信和網際網路資訊機構）以及金融機構（銀行及非銀行支付服務業者）、電信業務營運商及網際網路服務業者，共同建立預警和勸阻系統。此系統可發出預警識別潛在被害人，以利及時採取適當的勸阻措施。

金融機構亦可使用此系統開立銀行帳戶、支付帳戶，提供支付結算服務。此系統可用於加強客戶盡職調查流程，允許金融機構採取風險緩解措施，以防止銀行帳戶和支付帳戶等資產遭竊用於詐騙活動。

資料來源：中國

## 4.3. 實用的國內執法策略

63. 本節探討各司法管轄區已採取的良好實務做法及實用的執法策略。一般而言，此等策略皆採用上文第 4.1 節所述資訊來源，更有效地識別、調查和預防網路詐欺及相關洗錢犯罪。

64. 這些實用執法策略通常涉及多個機構和私部門實體，因此要落實策略，則需國內各部門強效穩健的協調與合作（如上文第 4.2 節所述）。

### *適當劃分權責*

65. 許多司法管轄區報告顯示，過去數年的損失金額和網路詐欺案件數量皆有所增加。雖然特定個案可能損失較小，但此類詐欺數量可觀，表示各個犯罪集團累積的犯罪所得總額甚鉅。

66. 部分司法管轄區指出，鑑於網路詐欺報案數量龐大，有必要明確劃分調查責任。已有司法管轄區採取良好實務做法，除原本設立的各種反詐欺或反網路犯罪機構以外，也致力指派專責主管機關處理相關案件。其他司法管轄區則頒行法令，規定涉及同一犯罪集團且多人受害的複雜案件應合併調查，全案偵辦均由單一權責機關負責監督。此措施可避免不同權責機關重複工作、防止案件成為「漏網之魚」，並有效因應犯罪的跨國性質。

### 說明欄 29. 運用科技劃分調查權責

香港警務處 (HKPF) 於 2022 年 9 月成立電子罪案處理及分析中心 (e-Hub)，旨在提升處理科技犯罪及詐騙相關報案的效率。e-Hub 使用強化電腦系統，對常見類型的網路詐欺案件進行關聯性分析，並歸納出案件群集。

2022 年，詐騙案件數量增加 45.1% 至 27,923 起，幾乎佔犯罪總數的 40%，其中近 80% 的詐騙案件皆與網路詐欺有關。愈來愈多民眾透過網路通報網路詐欺，而且大多數網路報案均彼此相關，例如源自同一犯罪集團。相關聯的案件會分派給單一調查小組集中偵辦，以利更妥善協調資源。

e-HUB 採用集群演算法，可識別資料中不易立即察覺的模式和相似性，進而深入瞭解案件的範圍和性質，其中包括常見類型的犯罪數位工具及罪犯使用的錢騾帳戶，以及網路詐欺的策畫、執行和隱匿方式。

資料來源：中國香港

## *防制網路詐欺及相關洗錢的專責單位*

67. 在不斷變化的犯罪態勢下，為加強洗錢防制/打擊資恐的能力，許多司法管轄區設立特別單位或任務小組，專責偵辦網路詐欺和相關洗錢活動。這些司法管轄區分配額外資源，用於加強金融調查、情報偵蒐、地方執法機關培訓，以及培養私部門的能力。這些集中化單位整合了全體執法機關的反網路詐欺專業資源，能夠更妥善遏阻網路詐欺運作、追查清洗後的資金，並返還相關犯罪所得。

68. 各司法管轄區一致認為，設立這類機構可實現多重效益。由單一執法單位統整所有網路詐欺案件，可更妥善分析案情、運用資料分析工具，分析犯罪網絡關聯性，進而查出犯罪集團。其可進一步成為私部門利害關係人及國外對等單位的單一聯絡窗口，有助於發展長期的策略關係。如此可強化執法機關的介入措施，例如切斷電話線路、移除可疑的線上帳號和廣告，並改善資產返還成果。

### 說明欄 30. 國家詐騙應對中心

馬來西亞國家詐騙應對中心 (NSRC) 是全方位的應變機構，匯集國家反金融犯罪中心、馬來西亞皇家警察 (RMP)、中央銀行和其他公私部門實體的各種資源和專業知識。

國家詐騙應對中心發揮樞紐作用，受理各種來源收到的詐欺資訊，並運用網路分析查出錢騾和洗錢網絡。私部門實體 (包括金融機構) 逐層追蹤資金流向，一經查獲隨即扣押錢騾帳戶。馬來西亞皇家警察將進一步偵辦案件，並採取執法行動，例如對帳戶發出凍結令。

資料來源：馬來西亞

### *改善金融情蒐效率*

69. 由於網路詐欺案件數量龐大，且會立即造成影響，因此及時取得金融和銀行資訊對於加快偵辦和追查網路詐欺犯罪所得至關重要。部分司法管轄區經常與私部門合作，運用特定技術掌握網路詐欺迅速轉移的犯罪所得流向。其他司法管轄區則藉助中央登記系統或開發資料庫，來簡化資訊檢索流程。這些優良實務通常需要設立單一集中化平台，匯集多方利害關係人資源，加快情資交換速度。

- **運用科技檢索資訊：**在同一司法管轄區內，由各權責機關議定一致的資料欄目格式，將有利於金融機構迅速向執法機關提供相關資訊。若權責機關向相關金融機構提出多種請求，而每項請求又各有不同的回覆格式，私部門可能需耗費大量時間處理。部分司法管轄區採取良好做法，由執法機關擬定標準化範本，列出預先議定的資料欄目，以供金融機構填入所需資訊。然後，權責機關可彙整相關請求，以機器可讀格式分批傳送給金融機構。金融機構亦可透過數位方式回覆執法機關的合法請求，進而提高資料分析的效率。

### 說明欄 31. 運用機器人流程自動化技術，加速取得金融機構持有的財務記錄

及時取得銀行和金融資訊，對於有效攔截和資產返還至關重要。新加坡運用機器人流程自動化技術 (RPA) 取得銀行資訊，大幅縮短以往所需的時間。現在，執法機關會採用標準化範本，透過電子方式向銀行發出指令。銀行會自動執行金融資訊檢索流程，然後以電子方式回覆執法機關，而執法機關可立即使用這些電子資料進行分析。

此流程將處理時間縮短多達 97%，進而提高偵辦效率。現在，相關資訊皆以數位格式提供，可以立即進行分析。對於銀行而言，此措施免去人工作業流程，大幅節省了成本。同樣，其亦透過自動化流程支援銀行進行資料探勘，進一步偵查隱藏的洗錢網絡。

資料來源：新加坡

- **促進跨金融機構的資產追蹤：**罪犯的轉手交易和帳戶跳轉範圍橫跨多個金融機構，這會增加執法追查的工作負擔，因為需要耗時從相關金融機構蒐集資訊，逐層調查各筆交易，才能識別資金的來源和最終目的地。若再考慮到交易速度，此任務可謂十分艱鉅。良好的實務做法包括開發協作平台，以利不同金融機構快速追蹤和交換資訊，進而攔截非法犯罪所得。

### 說明欄 32. 公民金融網路詐欺通報和管理系統 (CFCFRMS)

CFCFRMS 是由印度網路犯罪協調中心開發的線上系統，用途是快速通報金融網路詐欺，並阻止詐欺犯罪所得在整個金融部門流竄。此系統集結印度全國的執法機關和金融實體 (即銀行、錢包、聚合支付業者、支付閘道、電子商務平台等) 協力合作，針對透過 CFCFRMS 通報的投訴立即採取行動。目前，所有州和聯邦直轄區的執法機關以及 243 家金融實體已加入此模組系統。

一旦被害人向執法機關舉報詐欺行為，相關機構隨即記錄詐欺交易受款人詳細資訊，並以任務工單形式提交給 CFCFRMS 系統。此任務工單會轉呈至相關金融實體 (銀行、支付錢包等)，並顯示於實體的系統儀表板。實體會確認詐欺贓款是否仍在帳戶中，並將其凍結。倘若資金已轉移到另一實體，則工單會轉呈至下一實體層。此流程會持續重複直到截獲資金。若資金已遭提出，金融機構會填寫提領詳系資訊，供執法機關採取進一步行動。

記錄顯示，此系統可有效防止詐騙交易資金落入詐欺者手中。自 2021 年 4 月啟動以來，此系統攔截的金額已超過 60.2 億印度盧比 (約 6,610 萬歐元)。

資料來源：印度

- **運用中央登記系統：**透過中央銀行登記系統，執法機關可快速存取基本銀行資訊，並有助於加快網路詐欺的偵辦速度。執法機構可依此資訊核實嫌犯設有帳戶的銀行，或帳戶持有人的身分。這有助於執法機構及早確定偵辦範圍，並鎖定於嫌犯開設帳戶的金融機構，進而簡化資訊檢索流程。

### 說明欄 33. 識別隱藏的錢騾帳戶

馬爾他有一份可疑交易報告指出，一名錢騾疑犯向不同受款人進行一系列可疑交易。這些資金被轉移到多家當地和國際銀行，而這些實體均涉及一件疑似愛情詐欺的案件。

在全國中央銀行帳戶登記系統進行搜尋後，金融情報中心立即查獲嫌犯在另一家銀行持有的活躍帳戶。藉此，金融情報中心得以快速釐清案情全貌，並確定需進行額外金融分析的範圍。最終，金融情報中心迅速發現若干共通點，顯示資金進一步清洗並轉移至其他境外人士。

資料來源：馬爾他

- **開發私部門實體間資訊交流資料庫：**在專業洗錢網絡案件中，會有大量錢騾帳戶已知或疑似涉入先前的詐欺（例如愛情、彩券和就業詐欺）或身分竊盜活動。用於識別詐欺和錢騾網絡的資料和流程，也具有類似的重疊狀況。部分司法管轄區採取良好實務做法，試圖集中整合反詐欺和洗錢防制資料庫中的跨領域資料，識別各金融機構之間更深層的洗錢網絡，以利防止詐欺並促進資產返還。

### 說明欄 34. 集中化私部門實體間資料庫

巴西近期通過一項決議，強制要求所有金融和支付機構設立單一資料庫，集中統整所有詐欺 (包括未遂案件) 相關資訊。此資料庫由巴西中央銀行 (BCB) 執行，訂於 2023 年 11 月開始運作。

此決議強制要求機構必須共享詐欺 (包括未遂案件) 相關資訊，並規定必須共享的最低限度資訊。其中包括識別參與詐欺的人員 (包括錢騾)、涉及的金融機構以及所使用的帳戶。此系統旨在促進私部門之間資訊交流，以預防和打擊詐欺，並追回非法詐欺的犯罪所得。

資料來源：巴西

### *嚇阻錢騾*

70. 如前所述，錢騾在網路詐欺洗錢網絡中發揮重要作用。罪犯會以多種手法招募錢騾。錢騾對所涉網路詐欺計畫的瞭解和參與程度不盡相同，這取決於實際的招募方式，及其是否不自知受騙或遭剝削 (請參閱上文第 2.3 節)。

71. 因此，權責機關要以洗錢罪名起訴錢騾可能並非易事，很難找出充足證據來證明錢騾的洗錢犯罪意識 (即對自己參與洗錢的知情程度)。為因應此問題，部分司法管轄區藉由增修法令，降低洗錢犯罪的*犯罪意識*構成要件標準，例如從「知情」降低到「懷疑」。

### 說明欄 35. 歐洲理事會華沙公約第 9(3) 條

要有效起訴洗錢犯罪，根本問題之一在於證明*犯罪意識*，即洗錢者自知其經手的收益屬於犯罪所得。在涉及專業洗錢者的複雜洗錢案件中，被告通常會否認自己明確知悉所處理的資金為犯罪所得。因此要證明洗錢罪名成立，最具挑戰的任務之一即是證明被告的「心理構成要件」已達相關門檻。

有鑑於證明*犯罪意識*的困難，《華沙公約》的起草人在第 9 條增訂有關洗錢罪的新規定。除《維也納公約》和《巴勒莫公約》既定的構成要件外，《華沙公約》第 9 條第 3 款進一步規定，即使犯罪者僅懷疑或理應假設相關收益屬犯罪所得，亦已構成洗錢罪。

資料來源：防制洗錢措施和資恐問題評估專家委員會

72. 其他司法管轄區通常透過推行公眾教育，並主動向潛在錢騾進行宣導，藉此因應錢騾問題帶來的挑戰。在社群媒體上的全球宣傳活動，例如歐洲刑警組織支持的 *#DontbeaMule* 和國際刑警組織的 #YourAccountYourCrime，均可作為實用宣導平台，有助於協調國際社會資源，提高各界對錢騾活動的警覺，尤其關注錢騾可輕易跨境洗錢的事實。與私部門的合作可充分發揮此類宣傳工作的效用和成果。權責機關亦可運用既有偵查機制 (可疑交易報告和被害人報案)，來識別可能曾經手網路詐欺犯罪所得的潛在錢騾。此外，另可發布目標性的宣傳和警告，勸阻這類潛在的錢騾切勿再犯。倘若再犯，過去發布的宣傳或警告記錄，均可用作判定洗錢犯意的確鑿證據。

## 4.4. 預防和遏阻

73. 鑑於資金流失速度極快，許多司法管轄區致力開發防範網路詐欺和相關洗錢發生的措施。此方法可削弱網路詐欺集團的整體獲利能力，並大幅節省偵辦到被害人管理等後續階段需投入的資源。

### *公眾教育與宣傳*

74. 主管機關可採取預防方法，教育公眾提高警覺免於受騙上當，包括實施全民觀念宣傳活動，倡導網路素養的重要性。為實現此目標，部分司法管轄區運用科技推行資訊宣傳活動，協助公民發現詐欺行為、提高對可疑跡象的警覺，並鼓勵被害人報案。

### 說明欄 36. 運用科技推行網路詐欺的公眾宣導

香港警務處（「HKPF」）於 2022 年 9 月推出一站式詐騙及陷阱搜尋引擎「防騙視伏器 」(Scameter)。此應用程式旨在協助公眾識別詐騙和線上陷阱。

若民眾發現可疑電話和網路賣家、不請自來的交友邀請、隨機發出的招聘訊息、疑似詐欺投資網站等情況，可至「防騙視伏器 」輸入疑似詐欺犯的相關帳戶名稱或號碼、支付帳號、電話號碼、電子郵件地址、網址等資訊，即可評估詐騙和網路安全風險。

「防騙視伏器」的資料和評級來自各種可靠來源，包括向警方提交的公開報告、組織提供的資訊、可疑電話號碼資料庫以及資安公司的資料庫和即時分析。

資料來源：中國香港

## *防制洗錢/打擊資恐之反詐欺安全及控管措施成果*

75. 公私部門的經驗逐漸顯示，反詐欺與洗錢防制流程互有相輔相成的作用。其中包括運用科技協助使用者自動拒接詐欺訊息；與私部門合作進行前瞻性評估以主動緩解新興詐欺趨勢；開發帳戶安全功能、控管機制和規則，以及透過防毒軟體發出潛在網路釣魚網站的警告訊息 (請參閱附錄 B 的優良實務範例彙編，瞭解金融監管機關如何同步實施防制洗錢/打擊資恐控制與反詐欺相關規定)。

76. 另一項良好做法是鼓勵金融機構採用即時交易監控程序，在第一時間識別和防止詐欺或非法活動。藉由即時監控異常帳戶持有人的資訊 (例如實體、IP 和電子郵件位址、手機號碼等) 和交易，金融機構可以快速識別、調查和通報任何異常或可疑活動。

77. 即時交易監控程序涉及使用精密軟體和演算法來監控金融交易，據信可有效偵查和預防網路詐欺活動。由於數位化趨勢導致資訊氾濫，單憑人工處理恐怕難以發現網路詐欺。藉助即時交易監控程序，縱使多個帳戶或交易沒有直接關聯，金融機構仍可識別並調查其中可疑的活動模式，達到預防犯罪的效果。[21]

## *消除犯罪工具*

78. 鑑於網路詐欺亦可透過非傳統部門實施 (請參閱上文第 3.3 節)，部分司法管轄區已就此類非傳統部門加強反詐欺防控措施。重點包括網路詐欺工具，例如關閉罪犯使用的行動線路和詐欺網頁、篩選網路釣魚訊息和惡意網頁連結等。

21 有關如何運用科技防制洗錢/打擊資恐，另請詳閱 FATF (2021 年 7 月)《新科技為*防制洗錢/打擊資恐帶來的機會與挑戰*》

### 說明欄 37. 移除可疑網站和網路釣魚活動

在沙烏地阿拉伯，執法和監管機關與電信業者合作，大幅增強有效預測、預防、偵查和應對詐騙事件的能力。為打擊犯罪工具，沙烏地阿拉伯國家網路安全局實施嚴格的品牌保護規定，重點反制社群平台上的複製網站和網路釣魚訊息。此外，沙烏地阿拉伯中央銀行 (SAMA) 分別制定強力的網路安全和反詐欺架構，規定受監管實體必須採取的強制性基準控管措施。此架構旨在主動防範新興詐欺威脅，保障該國金融部門的穩定和安全。

這些國家監管法規的關鍵之處，在於要求組織主動監控犯罪工具。為此，組織必須採用精密技術和品牌保護措施，持續監視潛在詐欺活動，例如可疑網站和網路釣魚攻擊。一旦發現可疑活動，則立即通報相關權責機關。及時通報可確保迅速採取行動，調查並遏阻犯罪活動，防止進一步損害，並減輕詐欺事件的影響。

資料來源：沙烏地阿拉伯

## *防止資產流失*

79. 許多司法管轄區發現，偵辦網路詐欺最重大的挑戰之一，即是網路詐欺犯罪所得的洗錢速度極快。各界一致認為，權責機關必須迅速介入，及早追回資金，以免網路詐欺犯罪所得從多個銀行帳戶流失無蹤。各司法管轄區已採取各種措施，更有效地追回網路詐欺相關資產 (見下文第 5.1 節)。

80. 另一項理想的做法，則是與主要私部門金融機構的代表議合，協助並鼓勵其在接獲受害客戶通報詐騙後，即應主動攔截非法資金，而非等到權責機關聯絡後才展開行動，相關措施亦包括國內外金融機構或虛擬資產服務提供商之間的情資交換 (另見下文說明欄 41)。

### 說明欄 38. 艾格蒙聯盟的商業電子郵件攻擊詐欺公告

2019 年 7 月，艾格蒙聯盟發佈一份公告，詳列商業電子郵件攻擊相關的主要情境和風險指標，提醒成員金融情報中心及其司法管轄區注意商業電子郵件攻擊詐欺日益嚴重的威脅。公告進一步闡明金融機構 (FI) 的重要角色，包括促進內部洗錢防制、業務、詐欺預防和網路安全部門之間加強溝通和協作，進而識別、預防和通報商業電子郵件攻擊詐欺。

為協助偵辦商業電子郵件攻擊案件並追回被害人資金，此公告建議，若受款金融機構接獲情資 (例如 SWIFT 撤回訊息) 稱某一客戶的帳戶執行詐欺交易，則切勿執行任何可能導致資金損失的交易，並立即聯絡執法機關或金融情報中心，以評估所收交易款項的有效性。

資料來源：艾格蒙聯盟

## 5. 國際合作與資產返還

81. 如前所述，網路詐欺發生的司法管轄區（即被害人通常所在的司法管轄區）往往與清洗犯罪所得的司法管轄區不同。這可能帶來各種挑戰，包括阻礙跨境偵辦、難以有效進行國際合作以成功取得資訊和證據，進而瓦解網路詐欺集團並追回非法犯罪所得。例如，清洗網路詐欺犯罪所得的司法管轄區，可能難以識別每位與洗錢帳戶相關聯的被害人，因為他們可能散布在多個司法管轄區。

82. 網路詐欺的去中心化性質進一步增加這方面的複雜性。就國際合作而言，司法管轄區重視的優先事項可能各有不同，例如司法管轄區 A 的被害人將資金轉移到司法管轄區 B，但司法管轄區 B 的被害人位於司法管轄區 C（亦即 A 可能優先考慮與 B 合作，但 B 可能優先考慮與 C 合作）。由於需要國外公私部門多方利害關係人和合作夥伴共同參與，亦使識別和追蹤非法資金殊為不易。

- 網路詐欺集團會利用各種金融服務和資產類別犯案。不同業者和部門之間的交易，皆可近乎即時跨境進行，導致資金轉移流向難以追蹤和溯源。
- 相關的數位鑑識證據，也可能分散於不同的司法管轄區，因此難以掌握犯罪集團如何運作和清洗犯罪所得的全貌。數位鑑識證據具有易變特徵，若無法迅速保存，則容易消失無蹤，使情況更加棘手。

83. 正式合作程序（包括司法互助）通常需較長時間。數位犯罪和相關洗錢活動速度極快（證據若無法保存則可能迅速消失），單憑正式合作程序的效果恐大幅減弱。為保持靈活敏捷，及時提供跨境援助，以成功遏制網路詐欺犯罪活動，權責機關日益仰賴非正式合作機制，直接與國外對等單位交流資訊。此合作可透過各種管道在執法或金融情報中心層級進行，包括艾格蒙安全網絡、國際刑警組織的 I-24/7 以及其他非正式網絡，例如卡莫登資產返還機構間網絡（CARIN）和區域資產返還機構間網絡（ARIN）。

### 說明欄 39. 透過非正式多邊網絡攔截網路詐欺犯罪所得

為打擊日趨猖獗的網路詐欺，法國檢調機關積極運用非正式網絡 (其中包括卡莫登資產返還機構間網絡 (CARIN) 的歐洲資產返還辦公室 (ARO) 子網絡)，以利有效執行國際合作和相關資產返還。法國 ARO 與此二網絡成員密切合作，支援多個司法管轄區中負責追查、扣押及沒收犯罪資產的對等執法機關和金融情報中心迅速交換資訊，尤其在緊急情況下，可於 8 小時內回覆請求。此合作機制可迅速攔截資金，使其保存於最初查獲的目的地帳戶，以及其他所有後續各層帳戶中。

例如在 2022 年，法國 ARO 聯絡斯洛伐克 ARO，通報一筆 1,875,000 歐元的詐欺性銀行轉帳，表明此交易已損害一家法國受害公司的利益，並要求將資金凍結在斯洛伐克的受款人銀行帳戶中。在兩國 ARO 辦公室交換情資的合作下，不僅成功凍結資金，斯洛伐克主管機關也取得所有必要資訊，據以起草和執行司法凍結請求。最終成功凍結 1 874,907 英鎊並返還給受害公司。

資料來源：法國

84. 為充分提高偵辦網路詐欺洗錢和追回犯罪所得的成效，合作機制應著重於多邊而非雙邊互助。本節著眼於下列兩項行動結果，探討國際合作的挑戰和優良實務：(i) 資產返還以及 (ii) 強制執行和起訴。

## 5.1. 資產返還

85. 網路詐欺資產返還的關鍵挑戰在於洗錢速度極快。為克服這項挑戰，各個機構制定多邊「快速應變」計畫來追蹤並追回網路詐欺犯罪所得，包括國際刑警組織的「全球支付快速介入機制」(I-GRIP)、艾格蒙聯盟的「BEC 計畫」和美國的「金融詐欺摧毀鏈」(Financial Fraud Kill Chain)。上述機構的經驗普遍顯示，在詐欺交易發生後 24 至 72 小時內進行介入最為有效。這類優良實務降低資金散逸至後續多層帳戶的流失風險，大幅縮小洗錢防制偵辦範圍，有利於非法犯罪所得的返還。

### 說明欄 40. 金融詐欺摧毀鏈與資產返還團隊

金融詐欺摧毀鏈 (FFKC) 由 FBI 和金融犯罪執法網絡 (US FIU) 於 2016 年建立，旨在反制日益嚴重的商業電子郵件攻擊詐欺。FFKC 試圖藉助 FinCEN 與金融情報中心艾格蒙聯盟的合作關係，以利追回依詐欺計畫轉出的跨國電匯款項。此流程僅適用於符合下列條件的詐騙電匯：(1) 電匯金額 5 萬美元以上；(2) 電匯為跨國性質；(3) 已發出 SWIFT 撤回通知；(4) 電匯發生未超過 72 小時。

2018 年，FBI 網路犯罪投訴中心 (IC3) 成立資產返還小組 (RAT)，以解決國內電匯體系中的漏洞。RAT 簡化了與金融機構的溝通程序，並協助 FBI 各地分局凍結以詐欺理由執行的國內轉帳資金。RAT 成效卓著，在 IC3 受理報案的詐欺資金中，迄今已成功凍結其中的 73% (5.9062 億美元中的 4.333 億美元)。美國一項案例顯示，此計畫在特定情況下可迅速查獲第二層帳戶並凍結資金，進而追回全數詐欺贓款。

資料來源：美國

86. 這類多邊計畫主要旨在達成兩項目標：蒐集執法行動所需最低限度資訊，並將該資訊傳遞給「正確對象」。為確保有效落實跨境應變措施，多邊網絡的所有節點亦就治理規則和程序達成協議。雖然此多邊網絡通常為全球性質，但基於既有區域協作架構，進一步發展區域倡議，亦有助於克服相關挑戰。

### 說明欄 41. 多司法管轄區反詐騙計畫

鑑於詐欺的跨境性質，金融情報顧問小組 (FICG)1 內部制訂了一項名為「多司法管轄區反詐欺計畫」的區域倡議。此倡議由馬來西亞、印尼和新加坡的金融情報中心共同領導，旨在偵查、追蹤和追回被害人的資金。

現已建立一項涉及 FICG 成員國之間跨境交易的應變機制。此計畫協助 FICG 成員快速、輕易交流金融情報訊息，支援主管機關迅速採取行動，打擊詐欺並追回遭竊資金。

資料來源：馬來西亞

1 FICG 是由東南亞、紐西蘭和澳洲金融情報中心組成的區域性機構。

## *跨境資訊蒐集與交換：「蒐集最低限度資訊」*

87. 依 FATF 第 3 項建議，若國內法律規定網路詐欺屬於重罪，則網路詐欺應視為洗錢前置犯罪。此外，網路詐欺有別於傳統詐欺形式，此類案件多由熟人所為，難與潛在的債務-債權人民事糾紛作區別；但網路詐欺通常發生於陌生人之間，較容易初步證明構成犯罪，因此不同於其他類型犯罪 (未經普遍認定為前置犯罪者)，網路詐欺案件較無需透過冗長的司法互助程序來闡明和界定犯罪關聯。

88. 各項快速應變計畫均採用範本加速蒐集和交換資訊，這是一項良好的實務做法。使用範本可快速蒐集定罪所需的最低限度資訊，亦有助於現場應變單位專注搜查刑事控告初期階段所需的重大證據和資訊。此類範本亦可避免交換情資品質不彰的問題，並改善跨境執法的應變能力。

89. 除了概述網路詐欺犯罪案情重點，範本通常亦需提供追查資金所需的基本資料。標準化的請求格式，有利於司法管轄區快速處理任何收到的請求，進而加快執法單位攔截流入其管轄範圍的非法資金。

90. 範本中的資料欄目可以包括匯款人和受款人的帳戶資訊及交易明細 (日期、時間、轉帳金額)。為進一步提高成效，若資金已從受款人帳戶轉出，範本亦可註明資金下一目的地的相關資訊。另一項可能有用的做法，則是盡量降低資訊揭露限制，以利司法管轄區接獲通報時，可充分向國內權責機關散布資訊，俾使各相關單位交換情報。

### 說明欄 42. 國際刑警組織 I-GRIP

國際刑警組織建立了「國際刑警組織全球快速支付介入」(I-GRIP) 全球止付機制，支援成員國提交和處理追蹤、攔截或暫時凍結網路詐欺犯罪所得的請求。此機制簡稱 I-GRIP，最初於 2022 年作為防制洗錢快速應變協定 (ARRP) 的先導計畫，並在此先導階段多次止付成功，遂於 2022 年 11 月正式啟動。

I-GRIP 有助於國際刑警組織國家中央局 (NCB) 之間快速溝通，以防止可疑非法資產在成員國之間轉移。透過 I-GRIP 提交的請求，應載明充分詳細資訊，以利接收請求的國家中央局採取行動，例如交易日期、貨幣和金額、受款人和匯款人帳戶的帳號和金融機構名稱。

資料來源：國際刑警組織

91. 此外，標準化的範本資料欄目可讓國際組織集中彙整資料，簡化分析工作，充分提高案件偵辦和資產返還的成效。例如，國際刑警組織透過其管道交換取得情資，據以建立「金融犯罪分析檔案」(FINCAF) 內部資料庫，促進關於各種金融犯罪的跨國情報分析，並識別跨境案件、偵辦工作、威脅、犯罪趨勢及犯罪網絡之間的關聯 (另見下文說明欄 45)。

92. 為進一步加快資產返還行動，部分司法管轄區允許外國被害人直接向其國內執法機關提交網路詐欺投訴，包括透過線上通報平台直接填寫執法行動所需的資料欄目 (請參閱上文「被害人報案」一節)。如此可免去額外層級的溝通，使權責機關能夠迅速採取任何可行措施，處理司法管轄區內受款人帳戶的可疑交易。

## *有力行動的關鍵：情報需交給「正確對象」*

93. 有鑑於速度至關重要，因此任何蒐集到的資訊，皆應直接交給具備適當權限和專業的主管機關，以利有效追蹤和返還資產。如此可確保相關單位收到請求後，立即採取臨時措施，防止資產遭進一步遭清洗或流失。此舉也為執法部門提供關鍵時間，得以持續偵辦、擴大線索和蒐集證據，並於後續提出正式司法互助請求。

### 說明欄 43. 義務實體提出延付請求

義大利金融情報中心收到一間義務實體發出的延付請求，涉及四筆金額為 49 萬歐元的可疑電匯。這些交易款項是由一家義大利服裝批發貿易商匯出，受款方則是某東亞國家的多家公司。

義務實體認為這四筆交易甚為可疑，因資金皆源自轉入款項，而匯款行已對其發出撤回通知，理由為該等資金係因一家西歐受害公司的「執行長詐欺」而匯出。義大利金融情報中心也收到該西歐國家金融情報中心自發性交換的跨國情資。而金融情報中心另接獲報案指出，該義大利公司可能透過另一東歐國家涉入上述亞洲國家的增值稅詐欺案，進一步顯示網路詐欺與其他類型組織犯罪的關聯。

這些交易均已成功延付。因此，外國主管機關可以發布境外扣押令，以追回義大利境內的資金。

資料來源：義大利

94. 然而，由於不同司法管轄區的立法和執行架構差異，這類直接合作可能會面臨挑戰。解決挑戰的良好做法包括建立國內協調機制，以便將請求傳送給正確主管機關，並善加發揮公私協作管道和金融機構的能力，以利在收到權責機關的可疑交易通知後，立即自發性採取臨時措施。

### *治理與規則：《集體協議》*

95. 多邊架構的治理和規則提供了保證和承諾，要求各方互相承認犯罪活動，並在接獲情資後迅速採取行動。由於各方已預先議定加入架構和互助的條件，因此有助於克服國際機構之間優先事項不一致的問題。作為良好實務，這類規則和標準應盡量清晰明瞭。

96. 上述原則同時適用於非正式和正式國際合作機制。明顯的範例為歐洲議會和理事會 (EU) 2018/1805 條例允許相互承認境外凍結及沒收命令，此直接執行機制允許快速採取跨境介入措施。

97. 在加速資訊交流同時，不應犧牲資料保護和資料保密。為確保資訊傳輸安全，多邊架構通常運用國際刑警組織、歐洲刑警組織、艾格蒙聯盟等公信力機構既有的安全通訊管道。現有的安全通訊管道亦有利於上述多邊架構輕易擴展，因為無需再行發展雙邊通訊管道。

### 說明欄 44. 艾格蒙 BEC 計畫小組

為因應商業電子郵件攻擊對金融機構及其客戶日益嚴重的威脅，11 間金融情報中心成立「艾格蒙 BEC 計畫小組」，重點分析商業電子郵件攻擊趨勢、指標和方法，並與各金融情報中心交流主要發現。常見的商業電子郵件攻擊金融類型和案例研究顯示，迅速反應以阻止和追查電匯流向，是解決此類犯罪最有效的方法。

為此，計畫小組 [1] 訂定相關協定，規定執法機關與金融情報中心合作，並要求各國金融情報中心彼此互助，協力追查和凍結商業電子郵件攻擊的犯罪所得。

- 在收到涉嫌跨境商業電子郵件攻擊金流的相關可疑交易報告後，匯款人所在地的金融情報中心即向目的地金融情報中心提出「快速應變」請求。
- 該請求應載明事先議定的基本資料，以及採取執法行動需交換的基本情資。
- 目的地金融情報中心需盡可能採取立即行動，攔截並追回非法犯罪所得，以犯罪發生後 72 小時內為宜。

BEC 計畫透過艾格蒙聯盟的安全平台溝通，並交換「快速應變」請求的相關情資。

資料來源：艾格蒙聯盟

1 目前計畫小組成員包括：AUSTRAC (澳洲)、BFIU (孟加拉)、CTIF-CFI (比利時)、TRACFIN (法國)、GHFIU (加納)、HFIU (匈牙利)、IMPA (以色列)、SIC (黎巴嫩)、FIU 盧森堡、UPWBNM (馬來西亞)、FinCEN (美國) 和歐洲刑警組織。

## 5.2. 執法和起訴

98. 除了資產返還之外，網路詐欺的跨國性質也導致整個執法過程困難重重，從情蒐、偵辦到蒐集起訴證據皆然。科技發展提升了交易速度，使跨國分散作案更加容易，也迫使執法機關耗費更多時間和精力追查罪犯。

### *數位證據的蒐集*

99. 雖然數位鑑識證據不僅與洗錢相關，但可提供關鍵線索，引導執法部門深入偵辦洗錢案件。VPN (虛擬私人網路) 等身分隱藏服務的普及和易用性質，導致追查網路詐欺最終首謀變得更加棘手。

100. 可惜的是，目前尚無全球統一的管理制度，可據以規範數位資料的保留期限（包括與技術服務業者相關的資料）。若干司法管轄區強調數位證據流失的重大風險，而正式合作機制的延誤，也將對及時保護數位證據構成挑戰。

101. 下列幾項優良實務有助於減輕上述問題。

- **善用非正式管道**在初步階段蒐集和取得情報。然後透過正式合作管道取得必要的證據和陳述，以準備執行司法程序。
- 《網路犯罪公約》（又稱《布達佩斯公約》）等**公約和調查工具**，可讓相關單位快速保存電子資料並自發傳遞資訊，有助於加快查出網路詐欺的最終首謀。《布達佩斯公約》亦設立一個全年無休 24 小時運作的網絡，確保立即支援調查，包括提供技術建議、蒐集證據、保存資料等。
- 與外國服務業者**直接合作**，無需經過司法互助流程即可取得服務訂閱者資訊等必要的鑑識證據。某一司法管轄區指出，與自願的外國服務業者直接合作，是蒐集相關數位證據的最有效機制。[22]

[22] 另請參閱歐洲理事會（2020 年 7 月）*《布達佩斯網路犯罪公約：實務效益*及影響》瞭解與外國服務業者自願合作的更多資訊。

### 說明欄 45. 布達佩斯公約

《布達佩斯公約》規定下列各方面的程序權：加速儲存資料保存、流量資料加速保存和部分揭露、提供資料令、電腦資料的搜尋與扣押、流量資料即時擷取以及內容資料攔截。該公約亦規定快速有效的國際合作制度。

《網路犯罪公約》關於加強合作與揭露電子證據的第二附加議定書亦為下列事項提供法源依據：揭露網域名稱註冊資訊、與服務業者直接合作取得訂閱者資訊、取得訂閱者資訊及流量資料的有效方式；緊急狀況的即時合作、互助工具以及個人資料保護措施。

資料來源：歐洲理事會

## *聯合執法行動*

102. 跨國聯合調查團隊 (JIT) 需由兩個以上司法管轄區的權責機關就執行刑事調查而簽訂法律協議，以利共享資訊和跨境追查金流。相關單位通常透過各種架構和協議 (例如歐洲司法組織，以及歐洲刑警組織支持的聯合網路犯罪行動小組) 交流資訊。

103. JIT 採取跨國和去中心化的行動模式，亦提供重要的協調點，支援多邊執法行動打擊網路詐欺。隨著犯罪活動門檻降低，網路詐欺集團可以輕易從遠端遷移和建立新的數位行動中心。因此必須採取協調行動，同時根除各個下屬次團體(可以跨多個司法管轄區展開行動)。

### 說明欄 46. 聯合行動打擊大規模投資詐欺 [1]

塞爾維亞聯合奧地利、保加利亞及德國，再加上歐洲司法組織的支援，成功打擊兩個涉嫌大規模網路交易投資詐欺的組織犯罪集團。塞爾維亞主管機關逮捕五名嫌犯，搜查九處地點，並繳獲五棟公寓、三輛汽車、大量現金和 IT 設備；亦將 30 多個塞爾維亞銀行的帳戶納入監控。此外，此行動在保加利亞逮捕四名嫌犯，並攔截德國一家涉入詐欺案公司的資金，凍結其銀行帳戶內 250 萬歐元。

根據行動期間蒐得的情資，主管機關於兩日後迅速針對在貝爾格勒的一家公司展開另一場行動，逮捕一名嫌犯並沒收伺服器、其他 IT 設備及文件。

在本案中，塞爾維亞主管機關依據《布達佩斯公約》第 26 條 (自發性資訊) 等規定，與其他合作夥伴分享資訊。歐洲司法組織進一步協助調查，為聯合調查小組 (JIT) 提供經費，舉辦一場位於海牙總部的協調會議，以及一場視訊會議。

資料來源：塞爾維亞、歐洲理事會 (2020 年 7 月)《布達佩斯網路犯罪公約：實務效益及影響》

1 更多資訊另見 Eurojust (2020 年 4 月) 新聞稿，網址為：www.eurojust.europa.eu/news/action-against-large-scale-investment-fraud-several-countries

104. 縱如上述，聯合執法行動仍面臨挑戰。

- 即使在聯合調查小組內部，**法律壁壘**也可能對非正式的資訊交流造成限制。某一司法管轄區認為，目前仍需仰賴司法互助請求，才可充分交換資訊，而這可能會阻礙執法成效和參與度。可共享資訊也可能受到限制，尤其是涉及金融交易資訊所包含的細節數量。
- **能力水準和優先事項不一致**也可能阻礙司法管轄區參與聯合行動。如前所述，即使網路詐欺益趨嚴重，但考量國內優先事項可能與聯合行動不一致，加上資源受限的情況，各司法管轄區可能面臨平衡各方利益的艱難決定。

105. 除 JIT 外，國際刑警組織等多邊組織的聯合行動亦提供重要的協調點，支援多邊執法行動打擊網路詐欺。雖然這類行動不具正式法律協議，相較 JIT 更屬於非正式性質，但仍可提供重要合作平台，支援相關司法管轄區聯合打擊網路詐欺。

### 說明欄 47. 國際刑警組織 HAECHI 行動

自 2020 年起，國際刑警組織展開每年一度的 HAECHI 行動，支援參與行動的司法管轄區彼此交換資訊，共同打擊網路金融犯罪及相關洗錢活動。近期的 HAECHI III (2022 年) 有 30 個司法管轄區參與，逮捕近 1,000 名嫌犯，並凍結 2,800 個銀行帳戶和虛擬資產帳戶，共涉及 1.3 億美元非法犯罪所得。國際刑警組織透過 HAECHI III 協調成員國合作偵辦多起案件，共同打擊網路詐欺。

HAECHI 行動也成為 FINCAF 資料庫平台，蒐集各方資訊，並查明不同成員國現行偵辦任務之間的案情關聯。FINCAF 的結構可收錄任何類型金融犯罪及跨國犯罪相關的資料及其他資訊項目。國際刑警組織運用 FINCAF 資料庫與會員國合作，以期加強整體戰術應變能力，有效反制網路詐欺等國際組織犯罪。FINCAF 是一項重要工具，可更準確洞察跨境犯罪活動、犯罪組織、其集團結構、個人角色和關鍵人物、作案手法及詐欺金融交易。

資料來源：國際刑警組織

## *公私協同合作*

106. 鑑於網路詐欺的跨國影響範圍，公私協同合作可以超越國界，實現更顯著的成果。如同國內的公私合作夥伴關係，這類合作亦可涵蓋態樣或策略交流以及行動協調。這類夥伴關係的組成也取決於具體目標，可能包括與傳統洗錢防制/打擊資恐相關之部門以及非傳統部門。

## 說明欄 48. 歐洲錢騾行動

歐洲錢騾行動是基於公私資訊共享原則的國際行動，旨在打擊複雜的現代化犯罪。

2022 年，在歐洲銀行聯盟的持續協調下，約 1,800 家銀行、金融機構以及線上匯款服務業者、加密貨幣交易所、金融科技和 KYC 公司，以及跨國電腦科技公司，共同支援此行動的執法工作。

此行動由 25 個司法管轄區 [1] 的執法部門組成，並得到歐洲刑警組織、歐洲司法組織和國際刑警組織的進一步支援。行動查獲 8,755 名錢騾及 222 名「錢騾」招募者，共攔截 1,750 萬歐元資金，並逮捕 2,469 名錢騾。

資料來源：歐洲刑警組織

1 澳洲、奧地利、保加利亞、哥倫比亞、塞浦路斯、捷克、愛沙尼亞、希臘、匈牙利、新加坡、香港 (中國)、愛爾蘭、義大利、摩爾多瓦、荷蘭、波蘭、葡萄牙、羅馬尼亞、斯洛伐克共和國、斯洛維尼亞、瑞典、瑞士、西班牙、英國和美國。

# 6. 結論和重點領域

107. 網路詐欺是跨國組織犯罪集團實施的犯罪。隨著全球數位化和虛擬服務日益成長，網路詐欺的規模和程度預計會持續增加。司法管轄區亦應注意各部門（包括數位金融機構和非傳統部門）的額外漏洞，罪犯可能會加以利用，憑藉不斷演進的數位化技術，加強網路詐欺和洗錢手法。

108. 司法管轄區需致力打破孤立，加速並強化國內和國際各部門和實體之間的合作。網路詐欺及相關洗錢活動皆有去中心化性質，關鍵金融資訊和證據往往分散在不同地點，因此更難調查和瓦解網路詐欺集團，以及追蹤和追回網路詐欺犯罪所得。

109. 網路詐欺可能對被害人造成重大且嚴峻的經濟影響。但此影響不僅限於金錢損失；亦可能對社會和經濟帶來災難性的危害。司法管轄區應採取相應行動，更有效解決網路詐欺和相關洗錢防制問題，本報告為此總結三項重點領域：加強國內協調、支持多邊合作、加強偵查及預防。

## 有效防制網路詐欺和相關洗錢的重點領域

加強國內公私部門間之協調

- 司法管轄區應建立協調機制，聯合相關權責機關，全方位因應網路詐欺及相關犯罪所得的洗錢問題。此機制的成員包括科技網路犯罪專家，以及社群媒體平台、電子商務、電信和網路服務業者等非傳統部門。司法管轄區亦應善用公私合作夥伴關係，提升偵蒐調查能力，並加速資產返還行動。
- 良好的做法包括建立集中化的專責單位，允許其運用相關資訊並協調各公私部門採取行動，包括偵辦、資產返還和詐欺預防。

支持多邊國際合作

- 為提高資產返還成效，並避免網路詐欺相關犯罪所得流失，各司法管轄區應共同努力，迅速攔截網路詐欺犯罪所得。行動經驗顯示，網路詐欺事件發生後 24 至 72 小時內的介入通常最為有效。網路詐欺犯罪所得通常會洗入並分散至多個司法管轄區，因此需要採取全球統一的方法，才可有效追蹤和追回資金。
- 為此，各司法管轄區應善用並支持現有 (及未來) 多邊機制 (例如國際刑警組織的 I-GRIP 和艾格蒙聯盟的 BEC 計畫)，以利各國迅速合作並交流情資，以利打擊網路詐欺。這種多邊機制也可讓各司法管轄區合作，並聯手瓦解跨國網路詐欺集團。

加強偵查和預防

- 為加強偵查，司法管轄區應確保被害人易於報案，例如透過簡化通報流程的專門平台。司法管轄區也應與私部門合作，改善可疑交易報告機制。
- 司法管轄區應實施公眾教育，提高人們對網路詐欺的認識和警覺，包括宣導網路詐欺的可疑跡象，並改善民眾的網路素養。預防措施具有關鍵作用，可全面降低網路詐欺集團的牟利能力。司法管轄區亦應與私部門合作，支援落實網路詐欺預防策略，例如推行消費者保護措施，以及消除犯罪工具。

# 附錄 A：網路詐欺風險指標

以下潛在風險指標歸納自 FATF 全球網絡、艾格蒙聯盟及私部門各司法管轄區所提供的經驗和資料。這些指標旨在加強偵查能力，以利識別與網路詐欺相關的可疑交易。此清單進一步從開戶到交易監控等各種觀點，將指標細分為不同類別。這些指標可能與受監管實體相關，包括金融機構、虛擬資產服務提供商、指定之非金融事業或人員及其他金融和支付機構。

單憑一項與客戶或交易相關的指標，並不足以判斷網路詐欺的犯罪嫌疑，且單一指標也未必構成這類活動的明確跡象，但可作為參考線索，供相關單位酌情展開進一步監控和檢查。

## *交易模式*

- 開戶後迅速或立即執行不符合開戶目的的交易，無論金額高低
- 收到轉入的資金後，迅速或立即提領現金或大額轉帳，將帳戶清空
- 頻繁執行大額交易，與帳戶持有人的經濟狀況不符 (例如突然國際轉帳、在國外 ATM 使用支付卡提領現金、大量購買虛擬資產或貨物出口至境外，或付款給未經許可的外國金錢價值移轉服務商)
- 資金轉入高度洗錢風險的司法管轄區，或從該區轉出
- 大額頻繁交易，涉及近期成立的公司，及/或所涉主要活動不符受款人所從事活動，或其用途過於籠統廣泛
- 成功向受款人支付小額款項後，迅速同一受款人支付大額款項
- 頻繁及/或大量購買整數金額的商品，顯示有購買禮品卡的可能

## *客戶交易指示及備註*

- 一筆客戶交易成功付款後，立即要求支付額外款項，且收款帳戶並非客戶原先用於支付其供應商/廠商的帳戶。此行為可能符合罪犯得知詐欺付款成功後，試圖發出未經授權的額外付款指示。
- 在客戶貌似合法的交易指示中，出現有別以往的用語、時間和金額，不同於先前經過核實的交易指示。
- 交易指示中出現標記、聲明或用詞，指定交易請求為「緊急」、「秘密」或「機密」性質

- 客戶出示格式不當的訊息/電子郵件（內有拼字及/或文法錯誤）作為交易正當性的證明文件。
- 交易指示直接付款給已知受款人；但受款人的帳戶資訊與先前使用的不同
- 交易說明中的預期受款人與受款行所知的帳戶持有人姓名不一致
- 由不具財務經驗和專業的自然人（所謂投資人）發出轉帳指示，以投資和購買金融產品為由付款給特定公司（通常設址於高風險司法管轄區）
- 帳戶的商號/公司名稱與交易對手不相稱，可能表明此交易企圖隱匿大額資金的跨國轉移（例如號稱家具公司的實體多次大額轉帳給一間以石油貿易公司為名的實體）
- 使用時區不相符的裝置進行交易

### *帳戶持有人的個人檔案存疑*

- 帳戶持有人不願或無法通過客戶盡職調查
- 帳戶持有人不熟悉透過其帳戶轉移的資金來源，或自稱代其他人執行交易
- 頻繁使用外文詞句或術語變更法律實體/獨資企業名稱
- 客戶不甚瞭解交易或往來關係的性質、對象、金額或目的，或提出不切實際、令人困惑或不一致的說明，足以懷疑該名客戶是在擔任錢騾

### *帳戶使用者身分存疑*

- 使用者企圖使用共享、偽冒、竊盜或變造的身分資訊（地址、電話號碼、電子郵件）隱匿真實身分
- 開戶後頻繁變更聯絡方式、電話號碼、電子郵件地址
- 電子郵件地址似乎與帳戶持有人的姓名不相符，或在多個帳戶使用類似電子郵件地址模式
- 客戶個人檔案資料不符規定，例如與其他帳戶使用相同帳密憑證（例如由兩名以上使用者共用）
- 透過網路行為發現的異常情況，例如輸入資料時猶豫不決、按鍵延遲、有使用自動化程式的跡象、多次登入嘗試失敗等
- 帳戶關聯的實體預計不會在司法管轄區內活動（例如海外留學生畢業後出售的帳戶）

- IP 位址或 GPS 座標位於高度洗錢風險的司法管轄區
- 使用虛擬私人網路 (VPN)、遭入侵裝置 (例如 IOT 設備) 以及託管公司，可能藉此掩飾使用者的 IP 位址
- 多個 IP 位址或電子裝置關聯至同一個線上帳戶
- 單一固定 IP 位址或電子裝置關聯至不同帳戶持有者的多個帳戶
- 透過 TeamViewer 等應用程式所使用的電腦通訊埠，從遠端桌面建立連線來存取帳戶，藉此隱匿真實的裝置和位置
- 帳戶的擊鍵或導覽操作速度過快，表示可能是機器人在控制

### *帳戶持有人的負面資訊*

- 客戶或交易對手有實質相關且可驗證的負面新聞，例如已知或疑似為先前詐欺、錢騾或身分竊盜活動被害人持有的帳戶
- 往來金融機構或其他第三方詐欺資料庫提出的詐欺報告或撤回請求
- 有電匯撤回請求記錄
- 金融情報中心或地方執法機關提供的交易相關人員負面資訊

### *虛擬資產交易*

- 大額或頻繁將小額虛擬資產傳送至或接收自非託管錢包位址，或涉及暗網市場、兒童性侵素材平台、網路漏洞利用市場、勒索軟體團體、混幣/滾幣服務商、高風險司法管轄區、博弈網站及詐欺犯的位址
- 比特幣 ATM 交易量達到每日資金限額
- 沒有文件證明虛擬資產或轉換為加密資產的資金來源
- 將虛擬資產轉移到與暗網非法活動 (例如恐怖主義、兒童色情、毒品等) 相關的錢包
- 涉及多種類型的虛擬資產交易，尤其是匿名性較高者
- 使用點對點平台相關錢包進行的異常虛擬資產交易活動，且缺乏合理的商業理由

### *其他*

- 帳戶持有人的帳號和姓名不符

- 閉路電視（CCTV）畫面顯示使用者以電話交談或有人陪同，在交易過程中接受指示或指導
- 受款人公司管理的網站提供交易/投資服務，通常未獲國內監管機關授權或登記立案

# 附錄 B：利用反詐欺與洗錢防制/打擊資恐控制之間的協同作用

本附錄彙編若干優良實務範例，說明金融主管機關如何同步落實反詐欺規定和洗錢防制/打擊資恐控管措施，其中部分著重於遏止罪犯遠端註冊、存取和控制錢騾帳戶的能力。其中包括客戶驗證和交易監控相關的各項措施。

這些控管措施對金融機構、虛擬資產服務提供商及其他金融和支付機構均可能有所助益。

- 實施嚴格的認識客戶 (KYC) 或認識業務流程、在數位化開戶流程中納入生物識別功能，使用單一行動裝置或安全設備用於驗證網路銀行交易 (封鎖或管制其他設備以加強風險緩解措施)。
- 規定首次註冊網路銀行服務或安全裝置的客戶需等待一段冷靜期 (即開戶後無法立即使用整套銀行服務)，並限制該客戶的金融交易次數或金額。
- 擬定預期交易的定義 (交易數量、金額、交易對手類型、涉及國家) 以利偵測可疑交易、加嚴詐騙偵測規則及觸發條件，以先發制人方式封鎖非法交易。
- 使用「收款人驗證」服務，以供轉帳指示的匯款人/付款人/債務人確認支付訊息提及的受款人/收款人/債權人是否與帳戶持有人的姓名相符。
- 除非傳達一般資訊，否則盡量避免使用電子郵件和社群媒體與客戶溝通，並明確表示不應透過電子郵件與金融/虛擬資產服務提供商交換任何身分資訊或個人資料。
- 在與客戶的溝通中，加入語音識別軟體和人工智慧輔助功能，確保客戶身分的真實性。
- 需採用多因素身分驗證機制來核實客戶身分並執行金融交易，並使用不同管道新增或啟用受款人。
- 在遠端開戶期間驗證使用者身分，並防止罪犯利用錢騾或被害人帳戶資料存取多個帳戶，方法如下：
    - 透過活體測試 (即確保客戶為真實的活人) 來提高客戶識別流程的可靠性，包括在活體測試期間確認客戶是否受到社交工程影響；或者
    - 監控用於連線至網路銀行網站等的 IP 位址，包括偵測遠端存取工具的使用和「瀏覽器中間人」攻擊。

- 擴大申報實體蒐集和分析的客戶資料類型範圍，包括手機號碼、IP 位址、GPS 座標、裝置 ID 等。為預防詐欺，金融機構可採用以風險為本的方法重複此類識別流程 (例如發現異常行為時執行這類檢查)。
- 實施以風險為本的即時交易監控系統，確保能夠迅速發現、調查任何異常活動，並視需要提交可疑交易報告。監控系統的精密程度應與金融機構處理的交易量和性質相稱。

www.egmontgroup.org | www.interpol.int | www.fatf-gafi.org

2023 年 11 月


**網路詐欺產生的非法金流**

本報告分析了網路詐欺所使用的方法、與其他犯罪的關聯，以及罪犯如何利用新技術的漏洞，並舉出重要範例，闡述各種已知有效遏阻網路詐欺的國家行動應變措施和策略。本報告亦介紹各項風險指標和實用的反詐欺要求和控管措施，可能有助於公私部門實體偵防網路詐欺及相關洗錢活動。