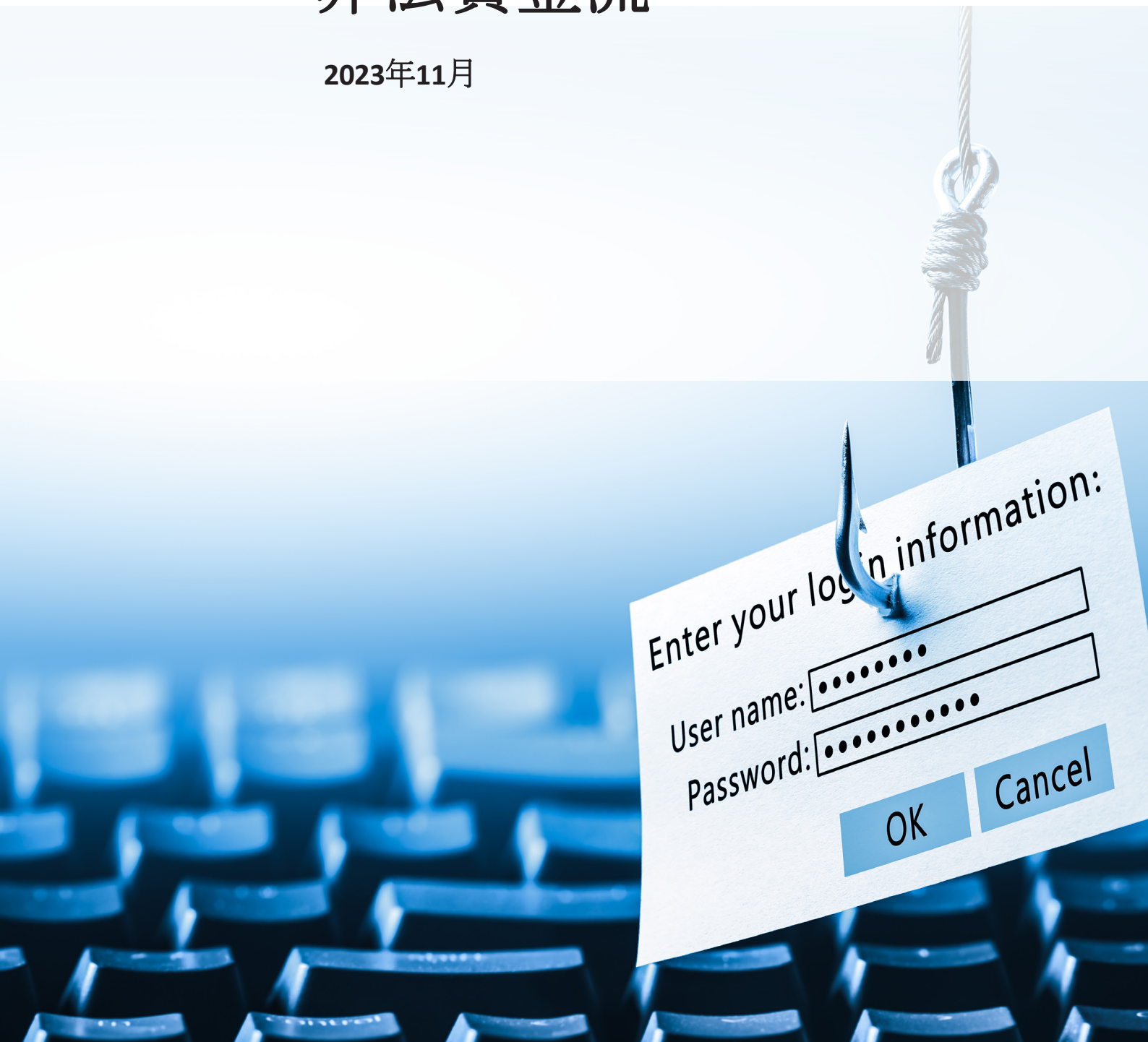
網絡詐騙衍生的非法資金流

2023年11月



財務行動特別組織（特別組織）是獨立跨政府組織，負責制訂和推廣政策，保障全球金融體系免受洗錢、恐怖分子資金籌集及大規模毀滅武器擴散資金籌集的影響，其建議公認為國際標準，用以打擊洗錢及恐怖分子資金籌集活動。有關特別組織的資料，請瀏覽www.fatf-gafi.org。本文件及／或所載地圖並不影響任何領土的地位或主權、國際邊界和疆界的劃分，以及任何領土、城市或地區的名稱。

埃格蒙特金融情報組織（埃格蒙特組織）旨在提供交流渠道，讓各國財富情報單位加強合作，打擊洗錢及恐怖分子資金籌集活動，並推動各地落實相關方案。有關埃格蒙特組織的資料，請瀏覽以下網站：www.egmontgroup.org。

國際刑警組織的職責是讓195個成員國的警隊合力打擊跨國罪行，促進世界安全。組織具備國際警政能力，既設有全球資料庫，內存有關罪犯和罪案的警方資料，亦向各國提供行動和法證支援、分析服務及培訓，支援四個全球方案，分別涵蓋金融罪行和貪污；反恐活動；電腦網絡罪行；以及有組織和新興罪行。

引用參考資料：

FATF – Interpol - Egmont Group (2023), *Illicit Financial Flows from Cyber-Enabled Fraud*, FATF, Paris, France, www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/iIllicit-financial-flows-cyber-enabled-fraud.html

內容

簡稱一覽表

AML/CFT	Anti-money laundering/Countering the financing of terrorism	打擊洗錢及恐怖分子資金籌集
ATM	Automated teller machine	自動櫃員機
BEC	Business email compromise	商業電郵詐騙
CDD	Customer due diligence	客戶盡職審查
CEF	Cyber-enabled fraud	網絡詐騙
DNFBP	Designated non-financial businesses and professions	指定非金融企業及行業
FI	Financial Institution	金融機構
FIU	Financial Intelligence Unit	財富情報單位
IBAN	International Bank Account Number	國際銀行帳戶號碼
IP	Internet protocol	網際網路協定 (IP)
LEA	Law enforcement agency	執法機關
ML	Money Laundering	清洗黑錢／洗錢
MLA	Mutual legal assistance	相互法律協助
PSP	Payment service provider	支付服務提供者
PPP	Public-private partnership	公私營合作
STR	Suspicious Transaction report	可疑交易報告
TF	Terrorist financing	恐怖分子資金籌集
TBML	Trade-based money laundering	貿易洗錢
VA	Virtual asset	虛擬資產
VASP	Virtual Asset Service Provider	虛擬資產服務提供者
vIBAN	Virtual International Bank Account Number	虛擬國際銀行帳戶號碼
VPN	Virtual private network	虛擬私有網絡
VoIP	Voice over Internet Protocol	網絡電話

報告摘要

網絡詐騙日趨嚴重，屬跨國有組織罪行。此類犯罪集團通常極有系統，分成多個分部，每組就其犯罪專長各司其職，包括洗錢。由於該等分部亦可能組織分散，遍佈多個司法管轄區，進一步增加調查難度。這些犯罪集團亦與其他類型的罪行有關，當中包括販運人口、在集團下的電話中心強迫勞役，以及與朝鮮民主主義人民共和國非法網絡活動有關的大規模毀滅武器擴散資金籌集。

網絡詐騙洗錢的過程涉及洗錢集團及相關專業人員，而洗錢帳戶網絡除了借助錢騾，亦會利用空殼公司或合法業務，並牽涉各類金融機構，包括銀行、支付及匯款服務提供者，以及虛擬資產服務提供者。不法之徒亦會利用多種洗錢手法掩飾贓款的線索，包括使用現金、貿易洗錢及無牌服務。

數碼化促進科技發展，令網絡詐騙罪犯得以發展和擴大其非法活動的規模、範圍及速度。罪犯利用多種工具及手法，並利用受害人的心理狀況和感情，盡可能騙取受害人的資金。犯罪集團乘着科技發展，清洗犯罪得益更容易快捷。透過網上遙距開戶等虛擬服務，亦令罪犯可輕易設立海外帳戶及清洗犯罪得益，並可近乎即時進行金融交易。罪犯亦利用社交媒體及通訊程式，在境外大規模招攬錢騾，並迅速利用新數碼金融機構及產品以及非傳統界別（例如電子商貿、社交媒體及串流平台）的漏洞犯案。

為更有效應對，各司法管轄區應：

- 推行措施，鼓勵受害人報案，並加強舉報可疑交易；
- 有效分析大數據，打擊網絡詐騙；以及
- 因應網絡詐騙的跨境特性，建立有效的本地協調機制，以全面打擊及預防網絡詐騙及相關洗錢罪行。

不法分子一般不會在進行網絡詐騙上游罪行的地點清洗黑錢，他們透過橫跨多個司法管轄區及金融機構的帳戶網絡，可快速清洗犯罪得益。各司法管轄區須加強多邊合作，以便有效及迅速地攔截跨境清洗的網絡詐騙得益。為此，各司法管轄區應善用及支持現行（以及未來設立）的多邊機制（例如國際刑警組織的 I-GRIP 及埃格蒙特組織的 BEC 計劃），促進國際合作及情報交流，以更有效打擊網絡詐騙。

最後，本報告亦載有一系列風險指標以及有效的防詐騙要求和管制，以助公營及私營機構偵測和預防網絡詐騙及相關洗錢罪行。

1. 引言

1. 網上騙案為網絡詐騙的主要形式。若不加以制止，將有更多有組織犯罪集團參與此類非法活動，利用新科技如生成式人工智能[1]等帶來的機會，令有關犯案手法愈趨精密，構成更大的威脅和風險。

2. 在新加坡擔任財務行動特別組織（特別組織）主席國期間，特別組織訂立了一項新措施，重點打擊與網絡詐騙有關的非法資金流動。本報告為埃格蒙特組織、特別組織及國際刑警組織的合作成果，亦是三個組織首次聯手推行的項目，反映三方打擊跨境有組織罪犯及其團夥的決心。

1.1. 焦點與範圍

3. 本報告重點探討網絡詐騙所引致的非法融資，而該等網絡詐騙案是透過網絡環境進行，並(i)涉及跨國罪案（如跨國犯罪及資金流）；以及(ii)涉及社交工程攻擊（即操縱受害人以獲取機密或個人資料）。由於網絡詐騙案件的種類繁多，本報告將針對以下六類的網絡詐騙活動：

- **商業電郵詐騙**：受害人收到聲稱為其客戶或供應商發出的電郵指示，要求受害人將資金轉入新帳戶。
- **釣魚式騙案**：騙徒騙取受害人的個人資料、銀行資料或帳戶登入認證等敏感資料後，再利用相關資料從受害人的支付帳戶榨取金錢、開設新帳戶或進行詐騙交易。
- **社交媒體及電話騙案**：騙徒利用手提電話或社交媒體應用程式聯絡受害人，並假扮成政府人員、親戚或朋友，利用受害人的感情，誘使其匯款、交出支付帳戶控制權，或進行金融活動，例如申請貸款或開立帳戶接收犯罪得益。
- **網上拍賣／交易平台騙案**：受害人透過網上的虛假廣告或顧問，登入不存在或虛假的平台，進行與法定資產和虛擬資產有關的交易及投資。
- **網上情緣騙案**：騙徒令受害人相信兩人已建立情侶或親密關係，隨後要求受害人向其匯款。
- **求職騙案**：騙徒在社交媒體平台刊登虛假的招聘廣告，以不同藉口騙取受害人金錢，例如須預先購買產品以提高交易平台營業額，或須提交職位保證金等。

4. 本報告並不涵蓋與勒索軟件及其他惡意軟件相關的非法融資活動。關於勒索軟件、利用虛擬資產及虛擬資產服務提供者的洗錢類型、挑戰及風險緩解的良好做法的資訊，請參閱特別組織於2023年3月發布的《Countering Ransomware Financing》報告。該等資訊與本報告相關，因為虛擬資產及虛擬資產服務提供者有時會被用作清洗網絡詐騙得益。

[1] 請參閱國際貨幣基金組織（2023 年 8 月）《*Fintech Note: Generative Artificial Intelligence in Finance: Risk Considerations*》。

1.2. 目的及結構

5. 本報告旨在加強各主管機構對網絡詐騙所構成的風險的認識。本報告以特別組織及其他國際組織（包括埃格蒙特組織、歐洲刑警及國際刑警組織）的現行工作為基礎，識別有助加強風險理解的最新重大發展。

- 本報告的**第2及第3章**探討現時與網絡詐騙有關的業務操作風險環境，了解網絡詐騙及相關洗錢的風險、技術及趨勢，包括數碼化及新科技的影響及弱點。
- 本報告的**第4及第5章**識別各司法管轄區為打擊及阻遏網絡詐騙及相關洗錢所採用的良好方法及解決方案，包括國際合作及追討資產的機制。

1.3. 方法

6. 項目由來自新加坡（特別組織代表）、中國香港聯合財富情報組（埃格蒙特組織代表）及國際刑警組織的專家牽頭，下列司法管轄區和機構則為項目團隊成員：阿塞拜疆、巴西、比利時、加拿大、中國、歐洲理事會、歐洲聯盟、歐洲刑警、德國、西非政府間反洗錢行動小組、印度、意大利、以色列、日本、馬來西亞、墨西哥、評估反清洗黑錢措施及恐怖分子資金籌集專家委員會、巴基斯坦、葡萄牙、沙特阿拉伯、多哥、英國及美國。

7. 本報告的研究結果根據：

- 目前與主題有關的文獻和開放資料的評論，包括埃格蒙特組織及國際刑警組織的數據及研究。
- 就風險、執法框架和策略，以及本地和國際合作及協調機制，分別向特別組織環球網絡及埃格蒙特組織內超過200個司法管轄區及170個財富情報單位所要求的資料。項目團隊共接獲80多個代表團體的回覆。
- 特別組織的聯合專家會議（2023年4月）及私營機構諮詢會（2023年5月）的討論和交流，包括與特定私營機構交流。

2. 風險環境：網絡詐騙

2.1. 日趨嚴重的洗錢威脅

8. 網絡詐騙在世界各地大幅增加。雖然目前無法完全估算相關騙案在全球的影響範圍及規模，不少司法管轄區近年都錄得持續升幅。與網絡詐騙有關的非法得益，往往會轉移到其他司法管轄區，並透過海外第三方的金融系統進一步清洗。

9. 根據國際刑警組織於2022年發布的《全球罪案趨勢報告》[2]，網上騙案為全球最常被視為具「高」或「極高」威脅的網上罪行趨勢。大部分為項目提供數據的司法管轄區，均在其國家風險評估中肯定網絡詐騙所帶來的洗錢風險。雖然網絡詐騙的犯案不受國際地域所限，但高度無現金化或數碼化的地區（例如可在網上提供大部分的金融中介服務的地區）預期面對更大的相關洗錢風險。以下專題集合各方資訊[3]，概述各地區面對的網絡詐騙威脅。

專題1. 有所增加的洗錢威脅：網絡詐騙地區趨勢

非洲：非洲的金融業急速數碼化，為罪犯提供大量進行網絡詐騙的機會，當中釣魚騙案、身分盜竊及虛擬資產騙案等網上銀行騙案急劇增加。由此引起的經濟損失增加，構成更大的洗錢威脅。例如，西非主要的犯罪得益源自網絡詐騙。

美洲：網絡詐騙被視為日益嚴重或新出現的風險。有司法管轄區指出，網絡詐騙按年增加，而相關的洗錢風險亦相應提高。另一司法管轄區表示，罪犯利用有關虛擬資產的宣傳炒作，令相關投資騙案於2021至2022年間增加超過180%。

亞太區：各司法管轄區均視網絡詐騙為高或主要洗錢風險。例如，有司法管轄區指出，大部分詐騙個案都含有某程度上的網絡詐騙元素，並注意到相關洗錢活動有所增加。另一司法管轄區強調，跨國罪犯利用大量非法投資應用程式瞞騙受害人。2019冠狀病毒病疫情加速該地數碼化進程，市民、政府及企業更趨向使用網上服務。因此，網絡詐騙及相關洗錢風險有所提高，並預期數字將繼續增加。

加勒比海：該地區特別容易受網絡詐騙及相關洗錢影響。過去五年，整體相關詐騙案件數字錄得增長。加勒比海盆地虛擬資產業的迅速發展亦製造了漏洞，例如不法分子可利用「混幣器」等虛擬資產服務提供者清洗非法資金（包括網絡詐騙得益），再轉移到有組織犯罪集團。

歐洲：該地區普遍把網絡詐騙評估為會構成洗錢風險。大部分司法管轄區發現相關活動大幅增加，認為會構成高度威脅。虛擬資產亦常用於清洗

[2] 請參閱國際刑警組織（2022年）《*全球罪案趨勢報告（Global Crime Trend Summary Report）*》。

[3] 包括各司法管轄區提供的資料和數據，以及國際刑警組織及歐洲刑警的報告。

網絡詐騙得益，特別是與虛擬資產有關的網上交易騙案，例如虛假代幣首次發行騙案。

中東和北非：在疫情期間，政府、企業和市民紛紛轉到網上活動，中東和北非地區與世界各地同樣面臨急速數碼化趨勢。網上金融詐騙列入高度威脅，包括釣魚騙案、假冒騙案和網上騙案。中東和北非亦面對洗錢威脅，尤其海灣阿拉伯國家合作委員會的成員國是環球貿易及金融活動的轉運樞紐。

10. 數碼化和新科技發展是促成網絡詐騙增加的關鍵。現今數碼服務已融入日常生活和公共職能，成為不可或缺的部分。因此，愈來愈多市民（包括易受影響的社群）投身網上活動。同時，數碼化代表各司法管轄區之間的聯繫更趨緊密，資訊和資金可迅速跨境流動。這兩個因素從根本改變罪案環境，創造有利條件增加網絡詐騙的威脅。

11. 2019冠狀病毒病疫情令人們從面對面的金融活動轉到網上開戶、支付及借貸，加快了其過渡進程。透過互聯網利用智能電話、電郵及社交媒體進行的欺詐活動顯著增加，例如電話及電郵騙案；銀行、老人及醫療騙案（例如與個人防護裝備及其他醫療產品相關）；以及虛假投資騙案。不斷變化的金融行為亦影響了洗錢發展，包括更多使用數碼銀行、支付平台及遙距交易（另見第2.3.3節）[4]。

12. 隨着智能電話、科技產品（日新月異的工具和應用程式）及遙距金融交易愈趨普及，用戶的脆弱程度大大增加。配合虛擬私人網路（VPN）和「洋蔥路由器」（TOR）[5]等匿名技術，罪犯進行非法活動可更易隱藏身份。他們亦可利用科技增加犯罪活動的規模、範圍及速度。據觀察所得，不法分子現採用「犯罪服務」模式[6]，不同分部負責網絡詐騙各個專業範疇，令犯罪集團可更容易參與其中（見下文第2.2節）[7]。

13. 在很多情況下，有組織犯罪集團已擴大或調整其犯罪活動參與網絡詐騙及利用現有技術清洗其他非法獲取資金。

[4] 請參閱特別組織（2020 年 5 月）《*COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*》及（2020 年 12 月）《*Update: COVID-19-Related Money Laundering and Terrorist Financing Risks*》。

[5] 又稱為 TOR，是一套讓用戶匿名上網的開放源碼軟件。

[6] 這是進行分工的地方。犯罪集團日漸發展並向他人提供合適的能力、技術和專業知識。

[7] 請參閱歐洲刑警（2023 年 7 月）《*Internet Organised Crime Threat Assessment (IOCTA) 2023*》；及國際刑警組織（2022 年）《*Financial and cybercrimes top global police concerns, say new INTERPOL report*》。

專題2. 用作網絡詐騙及其他罪行的常見洗錢犯罪網絡

一個洗錢網絡在其公司位於國家 A 經濟特區的大廈經營網上賭博和網絡詐騙業務。該建築物內有約十間公司，這些公司自行經營網上賭博和網絡詐騙業務，或把地方租予他人經營相同業務。該網絡包括一些位於鄰近國家 B 邊境地區的一些聲稱合法企業。該網絡由國家 B 的公民管理，他們利用國家 B 貨幣的銀行帳戶，把資金從經濟特區轉移到公司主要投資者所在的國家 C。透過國家 B 的找換店清洗來自經濟特區的美元，再兌換成國家 B 的貨幣，然後運到國家 C，最後在國家 C 的邊境轉移到公司投資者手上。

來源：東南亞的跨國有組織罪行、賭場及洗錢：威脅分析（聯合國毒品和犯罪問題辦公室，2022年）

2.2. 網絡詐騙的罪行特徵

網絡詐騙的元素

14. 根據各司法管轄區的經驗，要成功誘騙受害人轉帳，網絡詐騙罪犯會依賴以下一個或多個元素。不同種類的網絡詐騙會以不同方式結合上述元素。

- 資料擷取（例如透過釣魚）；
- 社交欺詐或工程，並利用他人的脆弱情感（例如冒充他人或機構，製造迫切性、恐懼或信任；或提供虛假聲明以便賺取金錢）；以及
- 網上媒介或平台（在網上買賣騙案中，可用作溝通或供受害人進行交易）。

15. 受害人可能墜入不止一種網絡詐騙。騙徒的最終目的是誘使受害人轉帳，為此會採用各式各樣的技倆。若然最初的詐騙方法失敗，他們會發揮創意，參與或轉移到其他種類的網絡詐騙。例如，騙徒會利用早已建立的「信任」，說服釣魚或社交媒體假冒騙案的受害人，引導受害人進行虛假投資。

專題3. 單一受害人，連環受騙

「殺豬盤」結合網上情緣騙案和投資騙案。罪犯先與受害人建立互信關係，再說服受害人把積蓄投資到虛假的加密貨幣交易平台。受害人長期深陷其中，導致大量金錢損失。

行騙成功後，罪犯通常會假冒律師或執法機關聯絡受害人，聲稱幫助他們討回資金並要求收取費用。

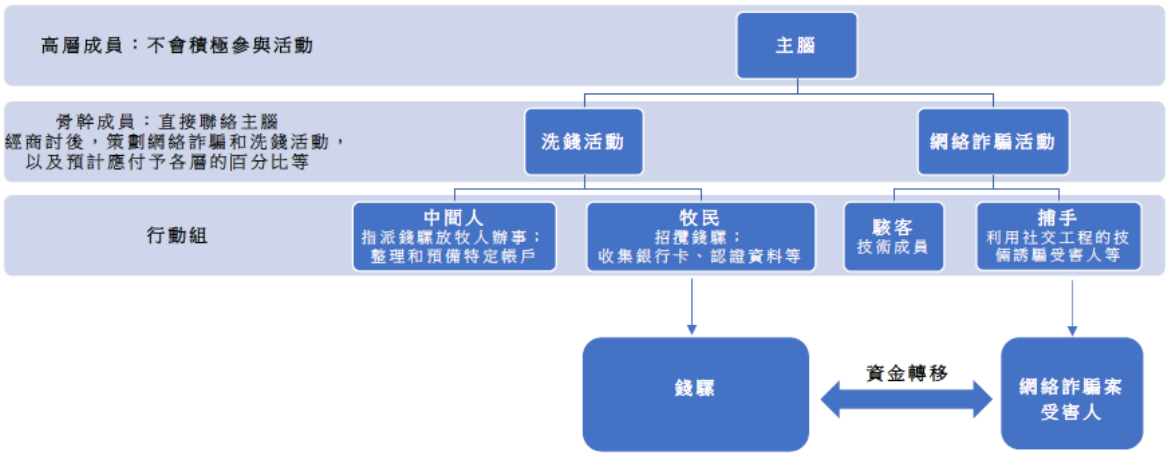
來源：歐洲刑警（2023年），互聯網有組織罪案威脅評估2023

有組織罪行的結構

16. 網絡詐騙或相關洗錢通常涉及跨國有組織犯罪集團。雖然這些集團的結構各異，但一般以等級分層的形式運作（見圖1範例）；亦可能組織鬆散，以保持彈性，因應需要加入或解散成員；甚或由多個具備不同範疇專業技術的分部組成（例如符合上述網絡詐騙元素（資料擷取、社交欺詐；或其他專業技術，例如創建網上平台或洗錢））。在很多情況下，這些犯罪集團組織大多不受任何中央實體管控，從不親身會面（例如透過網上加密渠道），因此有關當局難以就此進行調查。

17. 此外，網絡詐騙犯罪集團通常由高學歷的專業技術人員組成，因此進行網絡詐騙及清洗非法利潤的手法亦愈趨成熟。多個司法管轄區關注相關犯罪集團或意圖招聘專業界別（例如金融機構）人士，藉此取得數據和資訊進行網絡詐騙，以便清洗黑錢。就相關犯罪集團的架構和洗錢操作模式，請參閱下文第2.3節。

圖1. 網絡詐騙犯罪集團的架構範例



來源：特別組織

與其他犯罪活動的關聯

18. 除洗錢外，網絡詐騙犯罪集團亦與其他形式的犯罪活動相關。常見的罪案包括與網絡詐騙相關或進行網絡詐騙所需的犯罪活動，例如入侵系統盜取個人資料、研發及售賣犯罪軟件、偽造證件等。犯罪集團可能會利用部分犯罪得益以購買新裝備及研發更先進的科技工具之用。

專題 4.「禿鷹」行動

2020年，經國際刑警組織 Group-IB 及尼日利亞警方展開聯合電腦網絡罪行調查後，三名疑犯於尼日利亞拉各斯被捕。該等尼日利亞籍人士相信為一個龐大的有組織犯罪集團成員，負責散播惡意軟件；執行釣魚騙案和大規模商業電郵詐騙。疑犯涉嫌假冒不同組織的代表發送釣魚網站的超連結、域名及群發郵件，藉此散播26個惡意軟件程式、間諜軟件及遙距存取工具。

犯罪集團先利用這些軟件程式滲透和監控受害組織和受害人的系統，再進行詐騙並榨取資金。根據 Group-IB，自2017年起，相信該集團已入侵超過150個國家的政府機構及私營公司。Group-IB 亦證實該集團分為多個分部，其中部分人仍然在逃。

經同步洗錢調查後發現，疑犯亦利用在英國、美國及泰國的海外銀行及虛擬資產帳戶接收受害人的匯款。三名疑犯因參與違法活動被控詐騙及洗錢罪。疑犯的一輛豪華房車遭沒收，戶口亦被凍結。法庭正進行充公程序。

來源：尼日利亞

19. 網絡詐騙與人口販賣的關係亦漸趨緊密。透過虛假招聘廣告，罪犯誘騙受害人到網上電話中心工作，強迫受害人從事大規模網絡詐騙。相關犯罪集團可利用受害人的語言及文化知識，增加網絡詐騙目標受害人的地域多樣性。集團亦可販賣資訊科技人員及數碼銷售主管等專業人才[8]，提升詐騙中心的能力。這些電話中心有時會刻意在目標受害人的時區運作，並利用出租物業進行臨時犯罪活動，以便快速遷移及更換網際網路協定(IP)地址，逃避執法機關的追查[9]。

[8] 請參閱國際刑警組織（2023 年 6 月）《*INTERPOL issues global warning on human trafficking-fueled fraud*》。

[9] 請參閱國際刑警組織（2023 年 7 月）《*Operational Analysis Online Scams and Human Trafficking in South East Asia / Update 2 – From Regional to Global Threat*》；只提供予國家執法機關。

專題5.「造風者」行動

在「造風者」行動中，有關當局針對有組織犯罪集團展開執法行動。據報相關集團販運多名亞裔男子、女子及兒童，以進行剝削及／或賺取報酬。這次行動在25個國家拘捕了121人，並開展了193項調查。

經過「造風者」行動，馬來西亞和柬埔寨警方緊密合作，偵破一宗涉及15名男子及1名女子的案件。他們被誘騙到柬埔寨的電話中心工作，對方答應給予豐厚酬勞。然而，他們抵達後隨即被關起來，被迫充當騙子，每天工作14小時。

註：詳見國際刑警組織（2022年5月）《*121 arrests in operation against migrant smuggling and human trafficking*》
來源：國際刑警組織

20. 大部分司法管轄區均沒有充分的證據證實網絡詐騙與恐怖分子資金籌集活動有關。然而，有發現反映部分恐怖分子活動及資金籌集的元素與網絡詐騙犯罪分子有關。例如，一個司法管轄區的可疑交易報告指出，在某些情況下，網絡詐騙得益會被轉移到以恐怖主義相關活動聞名的特定衝突地區／司法管轄區。

21. 網絡詐騙亦與大規模毀滅武器擴散資金籌集有關，而電腦網絡罪行據報為朝鮮民主主義人民共和國主要的非法收入來源。非法網上活動包括出售收集到的個人資料，或提供入侵及釣魚工具和服務，這些服務或會被其他不法分子利用進行網絡詐騙[10]。

專題 6. 利用朝鮮民主主義人民共和國的釣魚工具進行網絡詐騙以資助武器計劃

根據聯合國專家小組提供的資料，與軍需工業部有關的朝鮮民主主義人民共和國資訊科技人員透過出售語音釣魚入侵應用程式以及經營多個海外伺服器和 IP 地址賺取外匯。

2020年7月，四名大韓民國公民被中國當局拘捕並引渡回南韓。其中一人作供指，犯罪集團從一名朝鮮民主主義人民共和國的資訊科技人員處購入韓國公民的個人資料及釣魚入侵應用程式。

犯罪集團誘騙受害人下載這些工具以盜取更多資料，隨後又假冒金融機構員工誘騙受害人匯款。

註：詳見聯合國安全理事會（2022年9月）*第1874（2009）號決議所設專家委員會於2022年9月2日致安全理事會主席的信函（S/2022/668）*
來源：聯合國專家小組及南韓

[10] 另見聯合國安全理事會（2023 年 3 月）*第 1874 (2009)號決議所設專家委員會於 2023 年 3 月 3 日致安全理事會主席的信函（S/2023/171）*

2.3. 洗錢方法及類型學

洗錢網絡架構

22. 不法分子需要快捷有效地清洗各種網絡詐騙得益。各司法管轄區發現，當中涉及專業的洗錢團隊以及第三方專業輔助人員，包括律師、會計師、稅務顧問、公司秘書及銀行家。這些專業的洗錢團隊可能是網絡詐騙犯罪集團的一分子，或是為專業洗錢網絡提供洗錢服務的分散獨立組織。

專題 7. QQAAZZ 網絡

QQAAZZ 在俄語網上論壇上宣傳，聲稱提供「全球銀行同謀洗錢服務」。電腦網絡犯罪分子都聚集在這些論壇上，提供或尋求參與電腦網絡罪行所需的專門技術或服務。QQAAZZ 網絡在全球開設數百間空殼公司，並在金融機構開立個人銀行帳戶，以接收電腦網絡詐騙的犯罪得益。資金隨後會轉移到其他由 QQAAZZ 持有的銀行帳戶，有時則會利用「轉幣」服務兌換成虛擬貨幣，藉此隱藏資金來源。在收取50%費用後，QQAAZZ 會將餘下的贓款轉移到客戶。

2020年11月，涉及16個國家的國際執法行動展開，20人被捕。該等被捕人士涉嫌為 QQAAZZ 犯罪網絡成員，並企圖為世上惡名昭彰的電腦網絡罪犯清洗數千萬歐元。執法機關在拉脫維亞、保加利亞、英國、西班牙及意大利進行約40次搜查。美國、葡萄牙、英國及西班牙亦對被捕人士展開刑事法律程序。

來源：葡萄牙及歐洲刑警

23. 一般而言，網絡詐騙得益會透過帳戶網絡快速清洗。案例研究顯示，這些網絡錯綜複雜，橫跨多個國家及金融機構，但會因應各個犯罪集團的精細程度而有所不同[11]。

24. 與網絡詐騙相關的洗錢帳戶網絡通常涉及個人及法人團體。

- **錢騾**通常由罪犯以各種方式招聘，例如提供工作機會或透過招聘廣告以及網上社交媒體互動。錢騾招聘者又稱為錢騾「放牧人」。錢騾可以是在知情、不知情（即是被誘騙）、因疏忽或為了金錢回報而參與洗錢。由於操縱錢騾的人會同時招聘知情和不知情的錢騾，執法機關往往難以識別他們的身份及詐騙資金的來源。有些司法管轄區表示，罪犯會招聘與該司法管轄區沒有明顯關聯的外地人作錢騾，並指示他們親身到訪當地或以虛擬方式開設錢騾帳戶。

[11] 就不法分子如何利用錢騾洗錢，請參閱特別組織（2018 年 7 月）《*Professional Money Laundering*》。

專題8. 招聘錢騾：提供工作機會

RS 女士是一間日用品店的店主，自稱獲 O 先生合法聘用。O 先生是尼日利亞公民，曾參與網上情緣騙案，騙取超過800萬菲律賓披索（約129,000歐元）損失，於2019年因涉嫌詐騙被捕。

O 先生答應 RS 女士，她處理每宗銀行交易都會獲得部分收益。RS 女士在六個月內合共處理了83宗交易，交易金額達360萬菲律賓披索（約58,000歐元），全部均為現金交易（即透過自動櫃員機及銀行櫃台存取現金）。在 RS 女士的協助下，O 先生最終被捕。

來源：菲律賓

- **空殼公司**通常透過「稻草人」或代名董事，由網絡詐騙罪犯控制。受聘的錢騾亦會被指示充當「稻草人」，開設公司帳戶，以進一步掩飾罪犯的擁持有權。有些司法管轄區注意到，空殼公司利用虛擬業務地址[12]進一步掩飾其犯罪活動。在網上交易騙案中，罪犯亦會利用這些空殼公司與商戶服務營運商開設虛擬銷售點帳戶，以處理受害人的匯款及轉帳。

專題 9. 涉及網上交易平台騙案的空殼公司

土耳其的財富情報單位收到多份可疑交易報告，涉及一個網上交易平台詐騙計劃。受害人透過電話或社交媒體投資外幣。該計劃以209間公司組成的網絡為基礎，這些公司會互相清洗犯罪得益。他們聘用相同的會計師，大多數於同一日成立，並在短期內破產清盤。

根據這些空殼公司的資金流向及交易對手分析，土耳其的財富情報單位相信這些空殼公司分為三個不同分部，共騙取並清洗約100億土耳其里拉（約3億3,670萬歐元）。

- 當中135間公司透過支付公司接收96億土耳其里拉（約3億2,320萬歐元）詐騙得益。為方便受害人進行交易，該等公司設立了虛擬銷售點。其中1億土耳其里拉（約340萬歐元）其後以現金提取，而約60億土耳其里拉（約2億200萬歐元）則轉移到一間金行。
- 當中59間公司接收7億土耳其里拉（約2,360萬歐元）詐騙得益，其中2億土耳其里拉（約670萬歐元）以現金提取，其餘則經其他同黨帳戶清洗後再轉移到虛擬資產服務提供者。
- 當中23間公司接收8億7,500萬土耳其里拉（約2,950萬歐元）詐騙得益，其中2億2,000萬土耳其里拉（約740萬歐元）以現金提取，其餘則經經其他同黨帳戶清洗後再轉移到虛擬資產服務提供者。

來源：土耳其

[12] 虛擬業務地址是由一些服務提供者提供的實體地址，讓企業接收郵件和包裹。

- **合法公司**與錢騾相似，同樣可能被誘騙接收網絡詐騙得益（例如作為投資或商業機會），其後罪犯可能會要求公司將資金轉移或退回罪犯操控帳戶。在某些情況下，特別是在經濟困難時，合法公司會接受此類「商業機會」。合法公司的參與成為這些非法活動的幌子，令執法機關難以偵測相關非法活動。

25. 為網絡詐騙建立的洗錢網絡中的錢騾與其他罪行的錢騾都有相同之處。然而，各司法管轄區發現到一些較適用於網絡詐騙的錢騾的相異之處。

- **招聘方法：**網絡詐騙的錢騾多數於網上招聘，包括透過虛假公司的招聘廣告或濫發電郵。罪犯亦會利用經濟環境，將之掩飾為合法「賺快錢」的工作機會。網絡詐騙（例如網上情緣騙案）的受害人亦常被誘騙充當錢騾。在某些情況下，人口販賣受害人（例如非法入境者或非法勞工）亦會被利用開設此類帳戶。
- **帳戶的使用：**有別使用於實體轉帳或提取現金，罪犯透過電子支付方式使用網絡詐騙錢騾的帳戶快速收發騙款。這通常與受害人的被騙方式有關（即透過轉帳）。鑑於數碼銀行服務令資金流動更方便，與網絡詐騙相關的錢騾對電腦科技都有一定的基本認識或水平。

專題 10. 網上情緣詐騙案受害人變成錢騾

2022年4月至5月，一名老婦原為收取退休金而開設的銀行帳戶接收到兩筆金額比過往活動為高的匯款，其中一筆匯款來自一個本地銀行帳戶，而另一筆則來自境外一名已報案的受害人。

斯洛伐克當局在隨後的調查中發現，該名婦人透過社交媒體結識了一名人士，並墜入網上情緣騙案。她向騙徒提供自己的網上銀行認證資料後，騙徒利用她的銀行帳戶清洗其他犯罪得益，部分接收到的款項透過海外虛擬資產服務提供者兌換成加密貨幣。

來源：斯洛伐克

洗錢類型學及方法

26. 網絡詐騙發生的地點（即受害人所在之處）通常與清洗相關得益的地點不同，而錢騾的網絡可能橫跨多個司法管轄區。網絡詐騙犯罪集團發現金融機構或主管當局可能在洗錢前已經識別了進行詐騙活動的帳戶，導致犯罪得益在轉移到罪犯的帳戶前已被攔截。為提高成功率，罪犯或會進行「測試」，即進行小額交易，若測試失敗便會改變轉賬的目的地。

27. 一般來說，用作接收借網絡詐騙得益的第一層帳戶類型取決於相關詐騙的類型，以維持表面的合法性。第一層帳戶的類型亦會隨時間而改變。以商業電郵詐騙為例，犯罪集團為減低被發現的風險從以往使用個人帳戶轉為企業帳戶。

表 1. 網絡詐騙的類型與第一層帳戶的關係

網絡詐騙的類型	第一層帳戶類型
商業電郵詐騙	企業（例如空殼公司或新註冊公司）
釣魚騙案	個人
社交媒體及電話假冒騙案	個人
網上拍賣／交易平台騙案	企業（例如空殼公司或新註冊公司）
網上情緣騙案	個人
求職騙案	個人

註：此表格根據各司法管轄區的經驗整理出各種網絡詐騙類型所使用的第一層帳戶類型的整體趨勢，並不適用於所有案件。

28. 一旦網絡詐騙犯罪集團建立了帳戶，詐騙獲得的得益便會快速流入洗錢網絡。此後，資金會透過一系列「轉手」交易，經由錢騾／稻草人或犯罪集團控制的本地或海外帳戶迅速分層。在後者的情況下，錢騾會交出銀行資料、銀行卡及代幣，或授權犯罪集團直接使用其帳戶。由於部分過程涉及專業人員（例如訂立授權書），因此增加了過程的合法性，有助掩飾罪行。

29. 為了進一步逃避偵查及保持匿名，網絡詐騙犯罪集團使用多種技術及機制，例如「化整為零」；在不同的金融、匯款或支付服務提供者帳戶之間不停轉換；以及轉化成其他種類的財務資產（例如電子貨幣[13]、預付卡、虛擬資產）。這樣使財富情報單位及執法機關需要花費更多時間，才得以從不同國家、業界及機構取得必需的財務數據，以便追查並討回非法得益。部分錢騾可能只容許犯罪集團在特定時限內使用其帳戶。這樣短時限使用，加上合法的開戶程序，令相關機構難以偵測到異常活動。

[13] 電子貨幣是一種數碼形式的法定貨幣，用於透過電子方式轉移以法定貨幣計值的價值。電子貨幣是法定貨幣的數碼轉移機制，即以電子方式轉移具有法定貨幣地位的價值；特別組織（2014 年 6 月）《*Virtual Currencies key Definitions and Potential AML/CFT Risks*》。

專題 11. 空殼公司、銀行帳戶及虛擬資產

印度警方接獲多宗投訴，有人利用流動應用程式經營虛擬資產挖掘平台詐騙。該應用程式承諾用戶可得到該項投資的利潤及利用不同方式誘騙受害人增加投資。一段時間後，平台停止提款／匯款服務、用戶無法登入網站及應用程式，而應用程式營運商亦不再回覆投資者。執法機關在接獲全國各地的客戶投訴後，要求印度財富情報單位就案件提供資訊。經分析後，印度財富情報單位識別兩間在 Google Play Store 上營運該應用程式的公司，兩者隨後被 Google Play Store 移除。另發現34間公司與該兩間公司相關；而36間公司之中，28間公司的董事為外國公民。

印度執法當局展開的同步洗錢調查亦顯示，該案件為大規模串謀詐騙，涉及多間空殼公司，利用相似的虛假應用程式／網站欺騙受害人，榨取犯罪得益。經實地查核，證實該等公司並沒有在註冊地址經營業務。根據財務線索顯示，其中幾間公司亦涉及經營非法賭博及貸款應用程式，並利用該等應用程式對公眾進行詐騙。案件中受害人的騙款被轉移到多個空殼公司的帳戶，部分得益其後轉換成虛擬資產。當局鎖定及凍結了留在銀行帳戶內的犯罪得益餘額，金額高達 8億6,500萬印度盧比（約990萬歐元）。

來源：印度

30. 各司法管轄區亦報告了其他類型的洗錢手法，罪犯會藉這些手法模糊網絡詐騙集團和洗錢組織的關聯。

- **現金：**本報告中多個案例研究都涉及錢騾和網絡詐騙犯罪集團提取現金的情況。金融機構以外的現金流動難以追查。罪犯經洗錢網絡洗錢後，可透過自動櫃員機提款，避免與親身與金融機構接觸。這些資金可能經現金運送人跨境流出其他司法管轄區，再存入銀行以進一步清洗。犯罪得益亦可用作購買貴重物品和工具（例如預付卡或貴金屬），再轉售成現金。

專題12. 提取現金購買黃金及油卡

2023年3月，一間中國公司的會計師陷入一宗假冒銀行騙案。罪犯聲稱由於公司帳戶需進行年度審查，把他加進一個通訊軟件的群組內。

該群組內的罪犯隨後假冒公司的法律代表及股東，要求受害人把780萬人民幣（約996,000歐元）轉移到由犯罪集團控制的兩個指定的公司戶口。警方調查顯示，該筆資金被轉入另外26個銀行帳戶，罪犯其後在銀行櫃台或透過自動櫃員機提取成現金，再轉到第三方支付平台，以及用作購買黃金和油卡。

來源：中國

- **貿易洗錢**：罪犯或利用若干貿易洗錢手法，把犯罪得益轉移到境外[14]。就網絡詐騙得益而言，有些司法管轄區發現罪犯會利用貿易洗錢手法，例如發出虛假或錯誤的發票，以及利用非法得益購買高價值或易於轉售的物品（例如汽車零件、門票及家居用品等）。舉例來說，有些司法管轄區報告指，罪犯把騙款電傳轉帳到合法公司購買貨品，這些合法公司涵蓋知名奢侈品或電器品牌，以至本地小型商店。這些貨品可轉移到境外，再轉換成現金作進一步分層和整合。在反洗錢及恐怖分子資金籌集制度以外的商業機構，或未有足夠的反洗錢意識或知識，以核實客戶身分或監察交易，從而在不知不覺中被罪犯利用。為資訊科技或顧問服務提供高報價或虛假發票亦是罪犯會採用的洗錢手法。

專題13. 網絡詐騙、錢騾及貿易洗錢

愛爾蘭當局拘捕了一個洗錢計劃的關鍵人士 MS。該名人士透過貿易洗錢，在尼日利亞清洗從愛爾蘭進行網上情緣騙案及商業電郵詐騙獲得的得益。調查仍在進行中。當局相信該洗錢計劃至今涉及至少60名人士及64個銀行帳戶。

計劃中，詐騙得益首先轉移到愛爾蘭錢騾的銀行帳戶，然後以現金提取，再轉移到與 MS 直接相關或 MS 持有的愛爾蘭帳戶。很多與 MS 相關的帳戶都以虛假身分開設。

一間尼日利亞公司（由一名相信位於美國的尼日利亞人操控）向歐洲或中國的合法公司訂購貨品。該等合法公司提供可運到外地轉售的貨品，包括酒類、服飾、電器及藥品。該尼日利亞公司會利用 MS 的愛爾蘭帳戶為相關訂單付款，而貨品最終運到位於尼日利亞同黨的公司。

有一次，一間德國藥廠收到超過170萬歐元用以支付一間尼日利亞公司的貨款。這些資金部分從多個與 MS 有關或 MS 持有的帳戶存入，並可直接追溯自歐洲及美國的商業電郵詐騙及網上情緣騙案的犯罪得益，有些更直接來自受害者的帳戶。 這些貨品最終運到尼日利亞。

來源：愛爾蘭

- **無牌經營或未經登記的匯款人及虛擬資產服務提供者**：犯罪得益或透過地下匯款人或哈瓦拉系統移離一些在打擊洗錢及恐怖分子資金籌集方面缺乏或並無管制的司法管轄區。在涉及虛擬資產的情況下，犯罪集團或利用這類的司法管轄區的虛擬資產服務提供者。

[14] 請參閱特別組織—埃格蒙特組織（2020 年 12 月）《*Trade-based Money Laundering: Trends and Developments*》；及特別組織（2018 年 7 月）《*Professional Money Laundering*》。

- **虛擬資產強化匿名技術**[15]：罪犯通常以組合形式利用非託管錢包、點對點交易、剝離鏈和高風險交易所，以快速清洗和轉移與虛擬資產相關的網絡詐騙得益離開司法管轄區。罪犯亦漸趨利用比特幣自動櫃員機轉移資產，掩飾資金操控人的身分，包括在存取資金時提供偽造或經篡改的身分證明文件，例如不同識別碼、電話號碼或生日日期。他們亦會利用混淆手法，包括使用「混幣器」或「轉幣器」服務、具強化匿名功能的虛擬資產（又稱隱私幣，例如門羅幣）及去中心化金融服務。

專題14. 橫跨多個界別的複雜洗錢案件

一個外國網上情緣詐騙犯罪集團成功騙取70名日本人，並把300萬美金騙款轉移到多個日本錢騾的銀行帳戶。一名日籍男子充當本地錢騾放牧人，將資金清洗並轉移到犯罪集團所在地迦納。經國際刑警組織與迦納合作，該名日籍男子最終被捕。

錢騾帳戶的資金隨後轉移到日本錢騾放牧人的帳戶。可疑交易報告分析顯示，錢騾放牧人利用三個渠道清洗資金：

- 資金經電傳轉帳到錢騾放牧人在迦納的銀行帳戶，然後在迦納以現金提取款項，再親身交到仍然在逃的集團首腦手上。在進行電傳轉帳時，該名日籍男子向日本銀行出示虛假發票，並訛稱款項用於合法商業活動（購買可可豆）。
- 部分資金經日本的虛擬資產服務提供者兌換成虛擬資產。
- 透過一間在日本與迦納社群有關的地下銀行把資金轉移到迦納。

來源：日本

數碼化及新科技對洗錢的影響

31. 新科技為用戶帶來新好處及機會。2019 冠狀病毒病疫情期間，金融服務加速轉向數碼化。人們減少使用現金，增加網上活動，產生了創新的工具和流程。金融支付鏈不斷發展及分散，而支付和交易服務提供者的服務亦漸趨多元化（見下文第 3.1 節）。

32. 然而，科技發展亦為犯罪集團帶來好處，讓他們藉此大幅改善洗錢技術。用戶期望暢通無阻的交易體驗，令愈來愈多金融交易在近乎轉瞬間完成。如上文所述，配合虛擬私人網路等數碼匿名技術，罪犯可連續快速地進行洗錢交易，令有關當局難以識別背後的終極罪犯。

33. 數碼化讓開設帳戶洗錢變得更方便快捷，擴大了網絡詐騙犯罪集團的境外版圖。有司法管轄區留意到遙距開戶和建立公司的數目有所增加，這些遙距虛擬流程無須用戶親自處理，罪犯可利用這些機會洗錢。

[15] 有關相關技術的詳情，請參閱特別組織（2023年3月）《*Countering Ransomware Financing*》。

專題15. 透過數碼化擴展的罪案

財富情報單位分析發現一個由147名人士以及來自8間銀行共276個銀行帳戶組成的龐大網絡。該等人士把自己的國民數碼身份（在政府及其他網上平台作識別身分之用）交給犯罪集團。集團隨後利用這些數碼身分遙距開設銀行帳戶，並直接控制這些錢騾戶口，藉以清洗網絡詐騙得益。財富情報單位憑著識別帳戶的共通之處，例如共同的銀行交易、數據點（海外聯絡資料及設備識別碼）以及聯絡方法（郵寄地址、電郵、電話），偵測到這個網絡。

這些情報轉交到「反詐騙指揮處」(Anti-Scam Command)。該處為新加坡警察部隊轄下的專責部門，負責打擊網絡詐騙及相關洗錢。反詐騙指揮處最終拘捕6人，3人因參與犯罪計劃被檢控。

來源：新加坡

34. 罪犯可以利用數碼工具擴大跨境招聘錢騾的範圍，從而迅速拓展錢騾網絡的規模。在招聘錢騾的過程中，罪犯常以社交媒體和網絡電話應用程式為媒介。傳統上，透過錢騾網絡洗錢會有一定的延滯，因錢騾需要時間接收和遵從其他犯罪集團的指示。但透過即時通訊平台，網絡詐騙集團現在可以大大縮短延滯時間。

35. 罪犯愈來愈趨向使用各種手法及技術工具盜取身分，包括釣魚、購買或誘騙他人自願交出個人身分資料。他們有時會利用偽造身分或合成身分（即是把真實和虛假的身分資料結合）。罪犯會直接使用這些身分開設和控制帳戶。帳戶持有人未必知道自己牽涉其中，這增加了追查相關洗錢活動的難度。

36. 一個司法管轄區指出深度偽造被用作接管帳戶詐騙的風險。騙徒可借助機器學習算法，偽造他人的聲音或影片，在電話或生物認證系統假冒該人。深度偽造還可結合社交工程技術，誘騙受害人交出帳戶資料。深度偽造技術仍然相對較新，目前相關的詐騙風險有限。然而，若該技術繼續發展，並更為廣泛應用，則未來有可能構成重大風險。

專題16. 直接控制遙距盜取的身分

在一系列與釣魚相關的詐騙中，罪犯誘騙受害人在電腦上安裝遙距存取工具。有很多案件中，罪犯透過遙距存取工具盜取受害人的資料，並在受害人不知情的情況下，以其名義在虛擬資產服務提供者處開設帳戶。罪犯亦涉嫌利用遙距存取工具隱藏真實界面，引導受害人完成網上核實開戶流程。

受害人最終被騙轉移資金到這些虛擬資產服務提供者帳戶。罪犯可以直接利用這些帳戶洗錢。這一系列詐騙案件中，受害人估計共損失超過600,000歐元。

來源：奧地利

3. 其他新出現的洗錢漏洞

37. 根據特別組織標準（建議 9 至 23），金融機構、指定非金融業人士以及虛擬資產服務提供者須採取預防措施，定下基礎防止網絡詐騙得益流入金融及其他行業。本節將聚焦可能被犯罪集團利用的新洗錢漏洞。

3.1. 數碼金融機構構成的風險[16]

38. 隨著金融支付的發展，新興數碼金融機構冒起，例如支付服務提供者、電子貨幣發行人等。由於傳統金融機構的資源相對更豐富，因此相比這些新興數碼金融機構有更穩健的管控措施，或導致罪犯利用這些新興金融提供者的漏洞洗錢。

39. 支付網絡亦可能是分散的，機構之間可能存在多種套式金融關係，例如多個支付機構互相進行交易；或向較小型的提供者提供帳戶服務，繼而該小型提供者亦向客戶提供其他金融服務（另見下文專題17）。這種分散特性亦令執法機關難以追踪「支付鏈」中各類機構之間的交易，以及即時取得支付鏈[17]交易中匯款人及受益人的基本資料。

40. 根據特別組織標準，司法管轄區對較新的金融機構應實施穩健的監管，包括訂立適當的發牌或註冊制度，以及防止罪犯操控該等機構。監管當局應確保所有交易機構都對各自的業務範圍作出充分監管——所有機構都有責任對匯款人及受益人進行或確保已進行客戶盡職審查和交易監察。

專題17. 濫用支付服務提供者

法國監管當局於2021年上半年進行的分析識別了用作接收詐騙電傳轉帳的主要支付服務提供者。這些支付服務提供者通常提供「銀行服務」，部分於法國設有分行，專門提供法國國際銀行帳戶號碼，只有少數實體存在。

根據分析，這些主要支付服務提供者的風險約為其他機構的200倍。這類服務提供者大部分在核實身分和監察交易方面的表現欠佳。罪犯利用盜取的身分開設帳戶，可以透過進行小額交易迅速測試開立的帳戶是否已被支付服務提供者識別為欺詐帳戶，有需要時可更改資金去向。他們隨後把詐騙得益快速轉入一個或多個帳戶。把款項分散在多個帳戶可確保罪犯能避過支付服務提供者施加的服務限制，例如現金提取限額，或保持在支付服務提供者內部制訂的業務監察範圍內。

來源：法國

[16] 本報告亦知悉虛擬資產及虛擬資產服務提供者引致的洗錢風險。有關虛擬資產服務提供者的監管風險及挑戰，請參閱特別組織（2023 年 3 月）《*Countering Ransomware Financing*》以及（2023 年 6 月）《*Virtual Assets: Targeted Update on the Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*》。

[17] 特別組織亦正考慮修訂建議 16（有關電傳轉帳），以應對支付系統結構最近的改變及未來的發展。

3.2. 濫用虛擬國際銀行帳戶號碼[18]

41. 罪犯濫用虛擬國際銀行帳戶號碼，就是利用金融創新進行網絡詐騙的另一例子。多個機構都有向客戶提供虛擬國際銀行帳戶號碼，包括銀行和支付服務提供者。雖然虛擬國際銀行帳戶號碼有多種合法用途，例如方便進行多方支付或分類支付，但多個司法管轄區均指出，虛擬國際銀行帳戶號碼有機會被濫用作網絡詐騙相關洗錢活動的工具。

專題 18. 什麼是虛擬國際銀行帳戶號碼？

虛擬國際銀行帳戶號碼的功能與傳統國際銀行帳戶號碼相同，同樣可在全球匯款及收款，並且同樣以最多34個字母數字字符組成。因此，在功能或外觀上，兩者之間並無區別。

傳統和虛擬國際銀行帳戶號碼的主要分別在於帳戶配對。傳統國際銀行帳戶號碼與銀行帳戶的配對比例為1:1，即每個獨立的號碼只會對應一個實體銀行帳戶。因此，若有人以國際銀行帳戶號碼付款，該資金將自動存入與之相連的銀行帳戶。

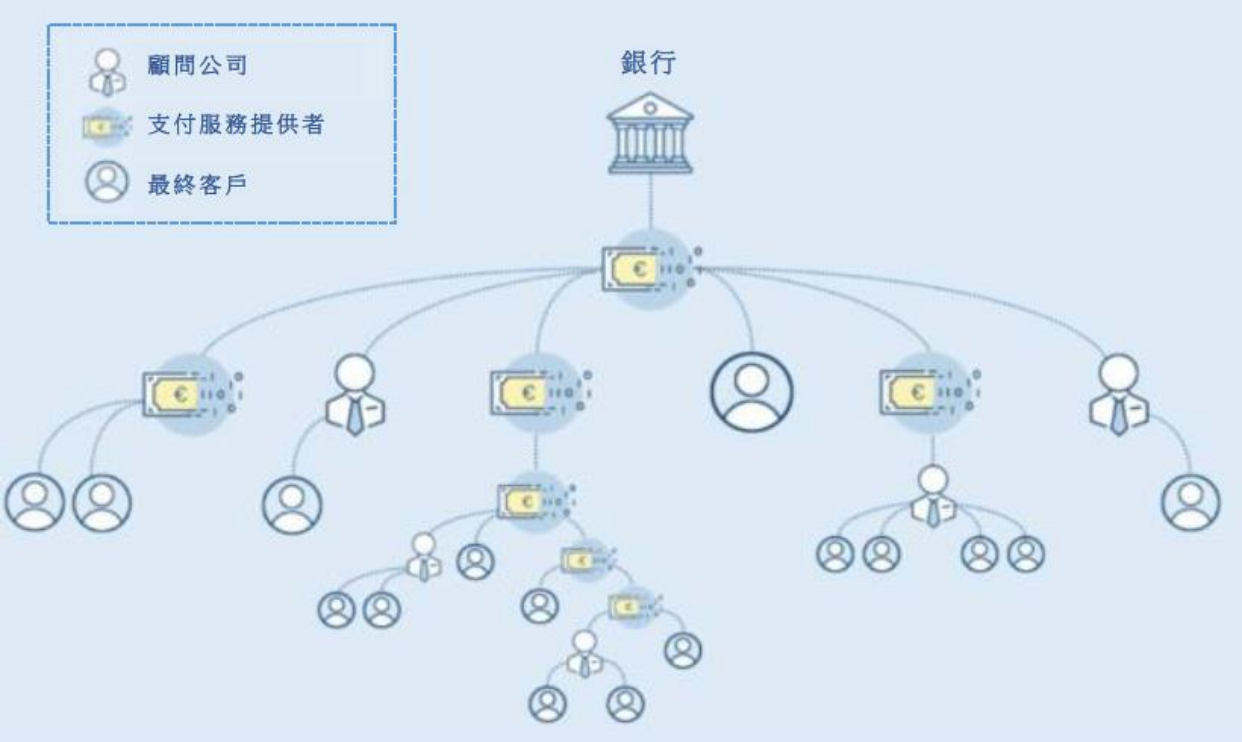
相反，虛擬國際銀行帳戶號碼是一個虛擬號碼，並沒有相對應的實體銀行帳戶。該號碼是由銀行發出的參考編號，可以把收款轉到一個與實體銀行帳戶相連的實體國際銀行帳戶號碼。虛擬國際銀行帳戶號碼無法保存任何資金，餘額為零。如圖3所示，持有人亦可持有多個獨一無二的虛擬國際銀行帳戶號碼，把所有款項集中轉到同一個實體銀行帳戶。

來源 ：歐洲刑警財富情報公私營協作

[18] 就與虛擬國際銀行帳戶號碼相關的風險及挑戰，請參閱（2023年6月）《*Europol Financial Intelligence Public Private Partnership (EFIPPP) Threat Intelligence Information on Virtual IBANs (available only to EFIPPP members)*》。

42. 由於國際銀行帳戶號碼和虛擬國際銀行帳戶號碼外觀一致，罪犯藉此誘騙受害人，令他們以為資金會轉移到一個銀行帳戶，但實際上資金可能被存到一個虛擬國際銀行帳戶號碼，為一個電子錢包充值。更複雜的是，金融機構的客戶可重新獲發虛擬國際銀行帳戶號碼，特別是如果該客戶為另一間金融機構。這令執法機關難以識別虛擬國際銀行帳戶號碼的來源地以及主帳戶的所在地。

圖2. 虛擬國際銀行帳戶號碼提供者發出及重發虛擬國際銀行帳戶號碼的傳播網絡



來源 ：歐洲刑警財富情報公私營協作計劃

43. 總的來說，罪犯可利用虛擬國際銀行帳戶號碼隱藏最終實益擁有權的資訊，並掩飾非法資金的流動，令當局難以識別簽發金融機構及真正的主帳戶的所在地，亦難以確保適當的交易監察。由於虛擬國際銀行帳戶號碼只是銀行發出的參考號碼，並非持有實際餘額的真實帳戶，最終導致主管當局在追踪實體帳戶位置及凍結資金方面困難重重。有見及此，部分司法管轄區與簽發虛擬國際銀行帳戶號碼的銀行合作，以便在發現網絡詐騙個案時，能夠快速識別與主帳戶有關連的支付機構。

專題 19. 濫用虛擬國際銀行帳戶號碼作網絡詐騙

2023年2月至3月期間，盧森堡的財富情報單位接獲多個「Hi Mum」騙案報告。騙徒會假冒受害人的孩子，以陌生的本地電話號碼向受害人發出WhatsApp 短訊。受害人透過盧森堡電話號碼接收到以盧森堡語書寫的短訊，並付上一個盧森堡國際銀行帳戶號碼。

調查此案期間，盧森堡的財富情報單位發現騙徒提供的國際銀行帳戶號碼為虛擬國際銀行帳戶號碼。該號碼由盧森堡的一間銀行機構向一個盧森堡支付服務提供者發出，該公司向歐洲客戶提供預付卡。客戶可透過轉款到虛擬國際銀行帳戶號碼為預付卡充值，而罪犯打算以此進一步洗錢。

在涉案的六個已識別的虛擬國際銀行帳戶號碼中，受害人共損失55,000歐元，盧森堡財富情報單位成功封鎖或收回其中的40,000歐元。有賴當地財富情報單位及發行該虛擬國際銀行帳戶號碼的銀行互相合作，才能快速識別持有終端客戶相關帳戶的支付機構。

來源：盧森堡

3.3. 非傳統界別

44. 很多司法管轄區都非常重視與非傳統界別的合作，包括社交媒體平台、電子商貿、電訊服務及網絡供應商，以共同打擊網絡詐騙相關洗錢活動。雖然非傳統界別不受打擊洗錢及恐怖分子資金籌集規例監管，但該界別掌握的資訊有助洗錢調查，特別是當他們被利用執行網絡詐騙及招聘錢騾的時候。社交媒體平台和電訊服務及網絡供應商可以提供重要的數碼法理資料，包括IP 地址、電話號碼、電郵地址等，有助識別最終犯案者。若不法分子利用虛假網站或廣告進行網絡詐騙，非傳統界別亦能掌握與罪犯相關的金融交易及付款資料（例如支援網站及廣告的付款資料）。

45. 各司法管轄區的經驗及案例研究亦顯示，罪犯如何利用電子商貿或社交媒體、串流或線上遊戲平台作為清洗網絡詐騙得益的渠道。社交媒體、串流或線上遊戲平台備受廣泛應用，用戶可在平台上接收觀眾及大眾的捐贈、禮物、代幣或點數。這些平台並無打擊洗錢及恐怖分子資金籌集規定，罪犯或利用這些平台清洗犯罪得益。

專題**20. 透過社交媒體及串流平台清洗釣魚得益**

執法機關發現19個銀行帳戶因釣魚攻擊而蒙受損失。德國的財富情報單位分析顯示，該等銀行帳戶交易均透過兩名用戶持有的支付帳戶進行。這些資金隨後轉移到一個社交媒體及串流平台，用作購買「金幣」（平台用戶之間使用的一種原生貨幣）為用戶的串流平台帳戶充值。該等「金幣」亦可用作購買虛擬禮物，這些禮物可轉移到內容創作者的帳戶，而內容創作者又可把這些金幣兌換並提取成等同幣值的一般貨幣。

調查仍在進行中。IP 地址數據顯示，該等詐騙交易都是透過同一個 IP 地址登入。財富情報單位分析指，一個罪犯透過社交媒體及串流平台清洗大部分釣魚得益，以便隨後兌換成現金。

來源：德國

4. 國家應變行動及策略

46. 本章會首先討論各司法管轄區偵測和調查網絡詐騙的主要資訊來源，其後會探討各地的協調及合作架構，以及各司法管轄區如何利用這些結構調查和預防網絡詐騙及相關洗錢。

4.1. 偵查的主要來源

47. 根據各司法管轄區的經驗及案例研究，偵測和調查與網絡詐騙相關洗錢的主要資料來源有兩個：受害人舉報和可疑交易報告。

48. 各司法管轄區亦推行多種措施用以加強舉報工作，務求獲取最多資訊，從而有效地執法。憑着這些資料和數據，主管當局可利用數碼策略及工具，分析並識別犯罪團夥，以更有效及針對性執法[19]。

受害人舉報

49. 受害人舉報是偵測和調查網絡詐騙相關非法得益的重要資訊來源。在商業電郵詐騙和釣魚等詐騙案中，受害人通常相對較快發現自己受騙（例如合法的交易對手會提醒受害人繳付欠款）。在其他種類的網絡詐騙案中，例如投資騙案、網上情緣騙案或其他釣魚騙案等，受害人則可能在一段時間後才發現受騙。

50. 受害人及時作出舉報非常重要。這可助主管當局快速追查非法得益流向，增加成功執法的機會。受害人可向執法機關舉報涉及違法的行為，包括向負責處理詐騙報告的專責單位舉報。另外，受害人亦可就其帳戶內的懷疑詐騙交易通知其金融機構、支付服務提供者及虛擬資產服務提供者。個別司法管轄區指出，除了執法機關外，受害人亦可聯絡金融服務消費者保護組織。

51. 然而，獲舉報的網絡詐騙數字往往較實際個案數目少，特別是當受害人的損失微不足道，加上尷尬或恐懼等情感因素，受害人或因而選擇不作舉報。

52. 為鼓勵受害人作出舉報，有些司法管轄區為舉報網絡詐騙建立了專門的平台，包括舉報網站。這些平台可提供有系統的報告格式，統一數據搜集方式，以便分析受害人舉報，有助識別犯罪趨勢及模式。這些平台亦可提供實用的預防網絡詐騙資訊，為受害人提供支援。

[19] 就財富情報單位及執法機關如何利用數碼轉型有效進行打擊洗錢及恐怖分子資金籌集分析及提升調查能力，請參閱機密報告《Digital Transformation of AML/CFT for Operational Authorities: Egmont Group-FATF》（2021 年 10 月）《*Detection of Suspicious Activities and Analysis of Financial Intelligence (Phase 1)*》；及特別組織（2022 年 5 月）《*Law Enforcement Authorities and Information Exchange (Phase 2)*》。

專題 21. 英國反詐騙行動機構(Action Fraud)

反詐騙行動機構是英國的詐騙及網絡罪行報案中心，由倫敦市警察局及國家詐騙情報局管理，集中處理詐騙和以榨取金錢為目標的網絡罪案。反詐騙行動機構的網站提供多種公眾宣傳資源，以預防罪案以及保護和支援受害人。

反詐騙行動機構亦提供全天候24小時網上舉報網站。機構會把舉報轉介國家詐騙情報局，在英國各地進行評估及分析，以識別幕後主腦。國家詐騙情報局隨後再把報告送到國內的相關警署進行調查。國家詐騙情報局亦會根據這些舉報移除騙徒的銀行帳戶、網站及電話號碼。

來源 ：英國

可疑交易報告

53. 由於受害人未必全都會作出舉報 ，可疑交易報告是偵測網絡詐騙相關資金流動的重要獨立情報來源。

54. 根據財富情報單位蒐集的數據，大部分與網絡詐騙相關的可疑交易報告均由銀行業提交。然而，由於網絡詐騙集團的犯罪手法不斷演變，銀行仍需繼續加強偵測網絡詐騙及相關洗錢的能力。數據亦顯示金錢或價值轉移服務及虛擬資產服務提供者提交的可疑交易報告較少，後者或因部分司法管轄區並未完全按照特別組織標準[20]監管虛擬資產服務提供者所致。

55. 罪犯可能會轉移網絡詐騙得益，因此必須確保及時分析與網絡詐騙有關的可疑交易報告。有些財富情報單位會編定先後次序，從大量可疑交易報告中篩查出風險較高的報告，其中包括與網絡詐騙有關的可疑交易報告；亦有些財富情報單位會就網絡詐騙相關洗錢風險向人員提供培訓，讓他們有能力篩選及分類接獲的相關可疑交易報告。這些措施都有助財富情報單位及時進行分析，讓執法機關迅速跟進網絡詐騙案件。

[20] 請參閱特別組織（2023 年 6 月）《*Virtual Assets: Targeted Update on the Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*》。

專題 22. 為與網絡詐騙相關的可疑交易報告編定次序及分群

自2021至2022年，智利的財富情報單位接獲超過1 500份與一個網上交易平台詐騙計劃有關的可疑交易報告。為應付大量可疑交易報告，有關當局採取分群方法進行分析，並從中發現特定模式。

該財富情報單位利用偵測到的關鍵詞及已知短句，透過一個文字勘探工具，識別到詐騙計劃的地區聯網，從而針對相關案件一併轉介到檢察機關。透過分群方法，當局調查發現罪犯經自動櫃員機提取騙款，並將資金轉移到有組織犯罪集團的更高層人員。

來源：智利

56. 除了偵查外，各司法管轄區亦致力提高防騙意識及改善進一步報告的情況。很多司法管轄區發出網絡詐騙相關指引，或為銀行及其他界別的員工舉辦教育講座，提高業界對最新的網絡詐騙趨勢及洗錢手法的意識。有關加強偵測網絡詐騙的風險指標，請參閱附件甲。其他司法管轄區的財富情報單位亦就網絡詐騙制訂策略分析文件。這些措施均旨在加強銀行前線員工在偵測及預防網絡詐騙及洗錢活動方面的能力。

專題 23. 就與網絡詐騙相關的錢騾進行策略分析

西班牙的財富情報單位發表一份策略分析聚焦一個錢騾的背景資料：可疑錢騾定義為在20天內於三間或以上的金融機構開設銀行帳戶。根據當地銀行帳戶註冊處的資料，於2020年12月至2022年2月期間，有接近40 000個銀行帳戶與約10 000人符合篩選條件。在這些銀行帳戶中，其中15%曾被紀錄於西班牙財富情報單位的數據庫。這些帳戶被列為高風險帳戶，財富情報單位以這些帳戶為依據，與四間金融機構合作展開試驗研究，加強了解風險狀況。

該試驗旨在預防網絡詐騙及其他可能的欺詐行為，並加強與私營機構的合作。此外，試驗亦旨在提高金融機構偵測系統漏洞的能力，獲取更多有關網絡詐騙的資料，以偵測及預防其他犯罪活動，並最終促成利用銀行帳戶註冊處資料的覆查系統，主動偵測與網絡詐騙有關的洗錢網絡。

來源：西班牙

4.2. 本地協調及合作

主管當局之間互相協調

57. 因應網絡詐騙的跨境特性，本地各機構之間顯然需要建立強而有力的協調機制。有些司法管轄區透過「全政府」策略達致協調，以制定該司法管轄區的網絡詐騙相關政策。這涉及由司法、執法、監管及資訊通信界別的幹部所組成的跨功能組織。這種協調方法有助司法管轄區識別重要界別的主要漏洞，訂定全面的對應政策。

58. 本地協調行動亦可與技術性機構合作，以加強偵測及調查，包括：

- 拓展金融機構、警方及檢控機關之間的溝通渠道，確立中央申報制度、簡化資訊及證據交流，以及凍結及沒收資產的指示。這亦包括使用自動數據分流，以助識別可能相關的事項，並快速確定合適的執法機關進行調查。由於網絡詐騙罪犯可以在同一司法管轄區內多處尋找受害對象，因此協調亦可避免執法機關之間的工作重疊（見下文第4.3節）。
- 利用網絡犯罪技術專家，特別是與網絡入侵及其他技術基建罪行相關的專家，以及私隱保護機構。這反映了網絡詐騙的多向性，以及數碼法證證據（例如IP地址、互聯網域連絡識別碼等）在識別網絡詐騙集團及進一步展開洗錢調查的功用。

專題 24.聯合警務網絡罪行協調中心 (Joint Policing Cybercrime Coordination Centre, JPC3)

JPC3由澳洲聯邦警察主導，成員包括各聯邦和州份的執法機關；政府分析機構，包括澳洲交易報告及分析中心；以及業界伙伴，例如澳洲銀行的分析人員。聯合警務網絡罪行協調中心的工作如下：

- 協調澳洲警方應對大量嚴重網絡罪行，以加強對犯罪環境造成的影響；
- 加強各聯邦、州份及地方的警察和業界之間的情報交流及提高目標；
- 協調聯合專責小組及警方和業界伙伴，打擊重點網絡罪行威脅；
- 透過提供交叉技術訓練和聯合培訓，以及研發協作工具，提升國內協作能力；以及
- 在全國統一推行媒體宣傳活動，加強業界及公眾的防罪意識。

JPC3旨在防止罪案，與業界及公眾合作打擊網絡罪行。為有效支援JPC3，澳洲交易報告及分析中心亦設有金融網絡罪行小組，專責就借助網絡進行的金融罪行（包括網絡詐騙相關洗錢）提供金融情報。

2020年1月，澳洲聯邦警察展開「DOLOS 行動」。該行動由澳洲聯邦警察主導的多機構專責小組負責，旨在打擊進行或協助進行商業電郵詐騙的跨國網絡罪犯。行動針對商業電郵詐騙的對象（包括個別澳洲公民和中小企業），阻截商業電郵詐騙集團的犯罪得益運轉。自展開以來，專責小組研發多種新技術，減低相關罪行對澳洲公民及企業帶來的損害。於2022年7月1日至2023年6月30日，該行動透過干擾罪犯的金融營運模式，成功阻止澳洲及世界各地受害人超過3,060萬澳元的經濟損失。

來源：澳洲

[1] 專責小組包括多個州份及地方警隊、情報及網絡安全機構、財富情報單位以及金融業界。

與私營企業建立合作伙伴關係

59. 各司法管轄區亦透過公私營合作模式，尋求與私營機構合作。公私營合作有助提升偵查工作效率；透過交換戰略性情報識別隱藏的洗錢網絡；以及加強追討資產的能力。

專題 25. 項目：快速防騙行動（Rapid Actions to Prevent Scams）

斯里蘭卡的財富情報單位推行名為「快速防騙行動」的項目，在接獲受害者舉報潛在網絡詐騙後，立即採取行動。該項目旨在透過聯合財富情報單位及金融機構的合規人員，快速偵測罪犯及同伙的非法帳戶活動，以制止斯里蘭卡金融系統內的詐騙活動，包括網絡詐騙。

該機制包括根據接獲的公眾投訴識別騙徒的個人資料，並與金融機構的合規人員分享有關資料。金融機構會根據這些資料，監察潛在騙徒的帳戶活動，並採取適當行動制止騙徒濫用金融系統，預防詐騙活動。此外，騙徒的資料亦會傳送到斯里蘭卡警方，以進行相關調查。

來源：斯里蘭卡

60. 鑑於網絡詐騙以及相關洗錢風險顯著增加，很多司法管轄區已在執法機關或監管機構設立中央應對中心，以加強打擊網絡詐騙，並提高公眾的防騙意識（有關打擊網絡詐騙的專責單位，另見下文第4.3節）。理想的做法是金融機構及虛擬資產服務提供者的代表可在此類中央應對中心共同合作，以接近即時的速度獲取金融數據，並追查各金融機構及界別的資料庫，加快主管當局攔截及凍結資金。

專題 26. 匯集各銀行的人員共同辦事

沙特阿拉伯為銀行設立聯合行動工作室，負責跟進和識別銀行客戶可能面對的金融詐騙。工作室匯集所有銀行及相關金融機構，共同處理金融詐騙個案。

聯合行動工作室由沙特阿拉伯的銀行管理，致力推動各銀行聯手維持業界的穩定。工作室全天候運作，旨在促進並加強所有當地銀行之間的合作和融合，阻止詐騙個案發生，迅速應對詐騙投訴，並在可行的情況下採取即時行動，避免欺詐行為。

來源：沙特阿拉伯

61. 這些合作亦提供了一個有用的平台，互相交流理想做法和常見犯案手法，並共同制訂建議措施，以制止非法活動。

專題 27. 歐洲刑警財富情報公私營合作計劃 (Europol Financial Intelligence Public Private Partnership)

歐洲刑警財富情報公私營合作計劃為首個針對打擊洗錢及恐怖分子資金籌集的跨國公私營資訊共享機制。計劃聚集了多個歐盟及非歐盟國家的執法機關、財富情報單位及私營企業。

該計劃內的威脅及手法工作小組專責研究網絡詐騙及／或相關騙案以及各種犯案手法，包括商業電郵詐騙、投資騙案、錢騾戶口、虛擬國際銀行帳戶號碼及加密資產。雖然計劃旨在編製類型學策略報告，但亦提供平台討論如何促進成員國之間的合作。

來源：歐洲刑警

62. 每個公私營合作計劃的成員結構都不盡相同。很多司法管轄區仍然著重傳統持份者（特別是銀行及其他金融機構），但指定的非金融企業及行業、虛擬資產服務提供者及其他非傳統行業（例如電訊服務營辦商及互聯網服務供應商）的參與亦日益增加。每個計劃的具體成員都會因應其宗旨和目標而有所不同。

專題 28. 與電訊業合作

近年，中國繼續推廣加強打擊及管理電信網絡詐騙，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》，為打擊及遏止電信網絡詐騙提供有力的法治保障，有效遏止相關犯罪行為。

該法例匯聚各公營部門（包括執法機關；財富、電信及互聯網資料機構）、金融機構（銀行及非銀行支付服務提供者）、電訊服務營辦商及互聯網服務供應商，建立預警及勸止系統，透過發出預警識別潛在受害人，以便採取適時的勸阻措施。

金融機構在開設銀行帳戶和支付帳戶，以及提供支付結算服務亦可利用該預警勸阻系統。該系統用於加強客戶盡職審查程序，讓金融機構採取風險緩減措施，防止銀行及支付帳戶等被用作詐騙行為。

來源：中國

4.3. 有用的本地執法策略

63. 本部分探討各司法管轄區採取的良好做法及有用的執法策略。一般而言，這些策略利用上文第4.1節提及的資料來源，更有效識別、調查及預防網絡詐騙及相關洗錢活動。

64. 由於這些有用的執法策略一般涉及多個機構及私營企業，這代表通常需要有效的本地協作才能實施該等策略（如上文第4.2節所述）。

適當分工

65. 過去幾年，不少司法管轄區均報告指網絡詐騙個案的數量及金錢損失都有所增加。雖然部分個別案件的損失不大，但此類騙案的數量龐大，每個犯罪集團累積的犯罪得益總額可能為數不少。

66. 多個司法管轄區表示因應龐大的網絡詐騙報告的數量，他們有需要就調查工作進行分工。司法管轄區提供的理想做法包括設立專職機構調查詐騙或網絡罪行其他司法管轄區則立法規定，若同一犯罪集團的案件涉及多名受害人，相關案件須合併處理，由同一個主管當局監督整個調查。這些措施可避免各主管當局的工作重疊、防止遺漏任何案件及可應對此類案件的跨國性質。

專題 29. 利用科技劃分調查工作

香港警務處於2022年9月成立電子報案處理及分析中心（e-Hub），旨在提升警隊處理科技罪案及詐騙案的效能。中心透過優化的電腦系統對常見的網絡詐騙個案類型進行關聯性分析，歸納案件群組。

在2022年，香港的詐騙案上升45.1%至27,923宗，佔整體罪案近四成，其中接近80%的詐騙案與網絡詐騙有關。愈來愈多人在網上舉報網絡詐騙，而大部分透過電子舉報的案件都有關連，例如來自同一犯罪集團。互有關聯的案件會分派至同一調查小組進行合併調查，以更妥善分配資源。

透過分群演算法，e-Hub 可從數據庫中找出無法即時辨認出的同類型案件，以更深入了解案件的範圍和性質。這包括常見的數碼犯罪工具、錢騾帳戶類型，以及罪犯如何策劃、執行及隱藏網絡詐騙。

來源：中國香港

反網絡詐騙及相關洗錢的專責小組

67. 由於罪案的形式層出不窮，為加強打擊洗錢及恐怖分子資金籌集活動的能力，很多司法管轄區設立特定單位或專責小組調查網絡詐騙及相關洗錢。這些單位或專責小組獲調撥額外資源，用以增強機構財富調查及情報蒐集方面的能力、為其他執法機關提供培訓和鞏固私營機構的相關能力。這些中央單位整合各執法機關的反網絡詐騙專業知識，提高他們阻截網絡詐騙、追查洗錢資金及追討相關得益的能力。

68. 各司法管轄區都認為中央單位的好處甚多。由單一執法機關集中處理所有網絡詐騙案件，可更有效運用數據和網絡進行分析，以識別犯罪集團。中央單位更可成為私營機構持份者和海外業界的唯一聯絡點，這有助發展雙方長遠戰略關係，以便執法機關在不同情景下介入，例如中斷犯罪集團使用的電話線及移除可疑的網上帳號及廣告，從而提高追討的資產總值。

專題 30. 國家反詐騙反應中心（National Scam Response Centre, NSRC）

馬來西亞 NSRC 是個多元應對中心，匯聚來自全國反金融罪案中心、馬來西亞皇家警察、中央銀行及其他公私營機構的資源及專業知識。

NSRC 作為負責接收各個渠道的詐騙資訊的樞紐，利用網絡分析識別錢騾及洗錢網絡；私營機構（包括金融機構）會逐層追查資金流向，隨後扣押錢騾的帳戶；馬來西亞皇家警察則會進一步調查案件，並展開執法行動，例如向帳戶發出凍結令。

來源：馬來西亞

加快獲取財務資料

69. 網絡詐騙案的數量龐大，並且可造成即時影響，因此必須及時取得財務資料，加快調查及追蹤相關得益。部分司法管轄區與私營機構合作，利用科技鎖定網絡詐騙得益的資金流向。其他司法管轄區則設立中央名冊或研發數據庫，以簡化資訊檢索程序。這些做法通常需要一個中央平台，聚集多個持份者以快速交換資訊。

- **利用科技進行資料檢索：**為使各金融機構能夠迅速向執法機關提交相關資料，司法管轄區內的各主管當局應就與調查相關的資料請求欄目達成共識。若金融機構需要就各主管當局不同的請求作出特製回覆，他們需耗費大量時間處理。有些司法管轄區的執法機關制訂了一套標準資料請求範本，其中包括與金融機構預先協定的所需資料欄目。相關請求經整合後，執法機關可以利用機讀格式分批發送至各金融機構。金融機構其後亦可以數碼方式回覆執法機關，從而更有效分析數據。

專題 31. 利用機械人流程自動化加快獲取金融機構的財務記錄

有見及時取得銀行和財務資料對有效阻截及追討資產的重要性，新加坡正利用機械人流程自動化技術更快及更有效率地獲取銀行資料。現在銀行可透過標準範本格式處理執法機關的要求。自動化技術使銀行可自動完成財務資料檢索程序，並以電子方式發送至執法機關，讓執法機關能即時利用相關資料進行分析。

整個流程所需的時間減少了97%，大大提高調查效率。數據資料現以數碼格式提供，執法機關可隨時進行分析。這項措施減省了人手處理工序，為銀行大幅節省成本。同樣地，銀行可透過自動化流程進行數據勘探以進一步偵測隱藏的洗錢網絡。

來源：新加坡

- **促進金融機構之間的資產追查**：執法機關追查交易流向往往涉及多個金融機構之間的帳戶流轉。這需耗費大量時間從各個金融機構間蒐集資料；及抽絲剝繭地分析各層交易，以確定資金來源及最終目的地。快速的交易速度進一步增加了調查難度。司法管轄區的理想的做法包括建立平台，促進不同金融機構之間的資產追查及資訊交流。

專題 32. 人民金融網絡詐騙報告及管理系統 (Citizen Financial Cyber Fraud Reporting and Management System)

人民金融網絡詐騙報告及管理系統是印度網絡罪行協調中心研發的網上系統，用作快速舉報網絡金融詐騙，以及防止詐騙得益流入金融業界。該系統聯合全國的執法機關及金融機構（即銀行、錢包、支付收集商、支付網關、電子商貿平台等），就系統接獲的投訴採取即時行動。現時印度所有邦和聯邦的執法機關以及243間金融機構均已加入系統。

執法機關一旦接獲詐騙受害人的舉報，便會記錄該詐騙交易受益人的資料，並會以票據形式呈交予人民金融網絡詐騙報告及管理系統。該票據會上報相關金融機構（銀行、支付錢包等），並會顯示在系統的報告板上。該機構會檢查被騙資金是否仍在帳戶內，並暫緩處理該資金。如資金已被轉移到另一機構，票據會上報到下一個機構，整個過程會不斷重複直至成功阻截資金。如資金被提取，金融機構會記錄提取詳情，以便執法機關採取進一步行動。

該系統在預防詐騙交易方面非常有效。自2021年4月成立以來，該系統已成功攔截超過60.2億印度盧比（約6,610萬歐元）。

來源：印度

- **利用中央登記冊**：中央銀行登記冊讓執法機關快速獲取基本的銀行資料，加快進行網絡詐騙調查。執法機關可利用相關資料核實疑犯持有帳戶的銀行，或帳戶持有人的身分。這樣有助簡化資料檢索程序，讓執法機關盡早確定調查範圍，集中向疑犯持有帳戶的金融機構檢索資料。

專題 33. 識別隱藏的錢騾帳戶

在馬耳他，有關當局接獲一宗相關可疑交易報告指一名錢騾與不同受益人進行一連串可疑交易，該交易的資金其後被轉移到多個與網上情緣詐騙有關的本地及國際銀行戶口。

經檢索國家中央銀行帳戶登記冊後，財富情報單位發現該名錢騾於另一間銀行持有仍活躍的帳戶，情報單位迅速掌握情況及進行所需的額外財務分析，情報單位最終成功識別到額外帳戶內可疑交易的共通之處，發現該錢騾進一步向其他外國人洗錢。

來源：馬耳他

- **為私營機構之間的相互資訊交流開發數據庫：**在專業洗錢網絡內，很多錢騾帳戶可能因為先前參與詐騙（例如網上情緣詐騙、獎券騙案及求職騙案）或盜取身分活動而曝光或受到懷疑，因此用於識別詐騙及用於識別錢騾網絡的資料和程序亦有相似的重疊部分，作為理想的做法，有些司法管轄區把反詐騙和反洗錢的數據庫集中起來，以識別橫跨各金融機構間更深層次的洗錢網絡，藉此預防詐騙以及追討資產。

專題 34. 私營機構之間的中央數據庫

巴西最近通過一項決議案，強制所有金融及支付機構建立一個數據庫，集中處理詐騙（包括企圖詐騙）有關資料。該數據庫由巴西中央銀行負責執行，預計將於2023年11月開始運作。

該決議案規定，各機構必須互通詐騙（包括企圖詐騙）資訊，並訂定必須提供的最低限度資料，包括涉及詐騙的人員身分（包括錢騾）、涉及的金融機構及使用的帳戶。該系統旨在促進私營機構之間互通資訊，以預防及打擊詐騙，以及追討非法詐騙得益。

來源：巴西

阻嚇錢騾的招攬

70. 如上文所述，錢騾在網絡詐騙相關洗錢網絡中擔當重要的角色。騙徒會用各種方法招攬錢騾，而根據錢騾被招攬的方式，以及因應他們是否在不知情的情況下受騙或被利用，他們對網絡詐騙計劃的認知及參與程度都會有所不同（見上文第2.3節）。

71. 因此，主管當局在提出洗錢罪的檢控時或會遇到困難。有關當局難以找到充分證據證明錢騾的洗錢犯罪意圖（即他們對參與洗錢過程的認知程度）。為解決這個問題，有些司法管轄區立法降低洗錢案件中犯罪意圖的標準，例如從「知悉」降至「懷疑」。

專題 35. 歐洲理事會《華沙公約》第9(3)條

提出有效洗錢罪檢控必須證明犯罪意圖，即洗錢者知悉他／她處理的得益為犯罪得益。在涉及專業洗錢者的複雜洗錢案中，被告通常否認自己清楚知悉他／她所處理的資金為犯罪得益。因此，證明被告的「意念元素」達到洗錢罪的門檻非常困難。

考慮到證明犯罪意圖的難度，《華沙公約》草擬人員於第9條載列的洗錢罪引入新元素。除了現行《維也納公約》和《巴勒莫公約》所載的元素外，《華沙公約》第9條第3段進一步規定，即使犯罪者只要懷疑或應曾假設該資金為犯罪得益，亦構成洗錢罪。

來源：Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)

72. 其他司法管轄區一般透過公眾教育及宣傳向潛在錢騾宣傳切勿借/賣戶口。社交媒體上的全球運動，如歐洲刑警的「#DontbeaMule」及國際刑警組織的「#YourAccountYourCrime」活動，都是統籌國際間合作打擊錢騾活動的有用平台，特別是由於錢騾便利跨境洗錢，與私營機構合作更可加強宣傳活動的成效。有關當局亦可利用現行的偵測機制（可疑交易報告及受害人舉報），識別可能曾處理網絡詐騙得益的潛在錢騾。當局可針對這些潛在錢騾進行宣傳及作出警告，勸戒其今後不要重犯。而宣傳及警告記錄可作為有用的證據，在這些錢騾重犯時確立定其犯罪意圖。

4.4. 預防及制止

73. 鑑於資金能夠快速轉移，很多司法管轄區投放資源推行預防網絡詐騙及相關洗錢措施。這種做法幫助減少網絡詐騙集團的整體得益，從而協助當局大幅減少其後投放到洗錢調查以及受害人管理的資源。

公眾教育及宣傳

74. 為了預防騙徒利用大眾市民進行網絡詐騙及相關洗錢，當局採取預防方法教育大眾及提高市民警惕，當中包括舉辦全國宣傳計劃及提高大眾的網絡知識。為此，有些司法管轄區利用科技為市民舉辦宣傳活動，協助他們偵測欺詐行為，提高對相關行為的警覺性，並鼓勵受害人報案。

專題 36. 利用科技推行網絡詐騙公眾教育

香港警務處於2022年9月推出一站式詐騙陷阱搜尋器「防騙視伏器」，協助公眾辨識詐騙及網絡陷阱。

當市民遇到不明來電、可疑網上賣家、自來交友請求、招聘短訊和疑似詐騙投資網站時，可在「防騙視伏器」輸入懷疑騙徒的帳戶名稱或號碼、收款號碼、電話號碼、電郵地址及網址等，評估詐騙及網絡安全風險。

「防騙視伏器」的資料或評級來自各種可靠來源，包括市民向警方報案的資料、機構提供的資料、可疑電話號碼舉報資料庫，以及資訊安全公司的資料庫及實時分析的評分。

來源：中國香港

反詐騙保安管制以打擊洗錢及恐怖分子資金籌集

75. 公私營機構的經驗開始顯示反詐騙及反洗錢過程是相輔相成的，包括利用科技協助用戶自動拒絕接收詐騙信息；與私營機構合作進行前瞻性偵測，主動緩和新興詐騙趨勢；建立帳戶保安功能、管制措施及規則；以及在防毒軟件加入潛在釣魚網站的警告信息（附件乙載列了金融監管機構如何在推行打擊洗錢及恐怖分子資金籌集措施的同時採取反詐騙規定的良好做法）。

76. 另一個良好做法是鼓勵金融機構實時監察交易，以即時識別及預防詐騙或非法活動。透過監察異常帳戶持有人的資料（例如實體地址、IP 地址、電郵地址、手提號碼等）及實時交易，金融機構可快速識別、調查及報告任何異常或可疑活動。

77. 實時交易監察利用先進的軟件和演算法監察金融交易，有助偵測及預防網絡詐騙。鑑於數碼化導致資訊泛濫，利用人手處理難以偵測網絡詐騙。實時交易監察可以協助金融機構偵測及調查多個帳戶或交易的可疑活動模式（即使該等帳戶或交易並沒有直接關聯），以預防相關犯罪活動[21]。

移除犯罪工具

78. 由於罪犯可透過非傳統界別進行網絡詐騙（見上文第3.3節），部分司法管轄區就這些非傳統界別加強預防及管制詐騙，包括針對網絡詐騙工具，例如關閉罪犯使用的手機號碼及詐騙網頁；過濾釣魚信息及惡意網站連結等。

專題 37. 移除可疑網站及釣魚活動

沙特阿拉伯的執法機關及監管機構與電訊服務供應商合作，有效地大幅提高了預測、預防、偵測及應對詐騙活動的能力。為打擊犯罪工具，沙特阿拉伯國家網絡安全局實施嚴格的品牌保護規定，重點打擊虛假網站及社交平台上的釣魚信息。此外，沙特中央銀行分別建立了強力的網絡安全及反詐騙框架，概述對受規管機構的強制性基準規定。該框架旨在防範新興詐騙的威脅，以確保及維護國內金融業穩定。

這些國家監管規定必須依靠各組織主動監察犯罪工具，包括透過先進科技及各組織推行的品牌保護措施，持續監察潛在詐騙活動，例如可疑網站及釣魚活動。一旦偵測到詐騙活動，將即時向有關當局報告，確保迅速採取行動，調查並停止犯罪行動，防止造成進一步損害，並減低詐騙事件的影響。

來源：沙特阿拉伯

防止資產轉移

79. 很多司法管轄區發現，由於網絡詐騙得益能夠迅速被清洗，令網絡詐騙調查非常困難。司法管轄區一致認為主管當局必須在網絡詐騙得益轉移到其他銀行帳戶前及早介入。為有效追討與網絡詐騙相關的資產，各司法管轄區推行了各種措施。（見下文第5.1節）。

80. 一旦接獲詐騙受害人通知，司法管轄區鼓勵私營金融業界代表在主管當局聯絡前主動攔截非法資金。此舉相信可更具效益攔截詐騙得益。這包括本地及海外金融機構或虛擬資產服務提供者之間的資訊交換（另見下文專題41）。

[21] 就利用科技打擊洗錢及恐怖分子資金籌集，請參閱特別組織（2021 年 7 月）《*Opportunities and Challenges of New Technologies for AML/CFT*》。

專題 38. 埃格蒙特組織的商業電郵詐騙報告

2019年7月，埃格蒙特組織發表報告提醒各財富情報單位成員及其司法管轄區日益嚴重的商業電郵詐騙威脅和分享商業電郵詐騙的情況及風險指標。報告透過鼓勵金融機構與內部負責打擊洗錢、商業、防騙及網絡保安的單位加強溝通和協作，進一步確立其在識別、預防及報告商業電郵詐騙方面的角色。

為協助調查商業電郵詐騙事件及為受害人追討資金，若有金融機構接獲資訊（例如 SWIFT 撤回信息），指其客戶的帳戶用於接收詐騙轉帳，報告建議該機構不要進行任何會導致資金損失的交易，並聯絡執法機關或財富情報單位，以評估該交易是否有效。

來源：埃格蒙特組織

5. 國際合作及追討資產

81. 如上文所述，發生網絡詐騙的司法管轄區（即一般受害人的所在地）往往並非清洗得益的地方，以致調查涉及跨境原素和國際間的合作。有關當局在獲取資訊和證據、瓦解網絡詐騙集團及追討非法得益方面面對不少挑戰。舉例來說，罪犯在一個司法管轄區清洗網絡詐騙相關得益，但該司法管轄區或難以辨識所有與洗錢帳戶有關的受害人，因受害人可能分散在多個不同的司法管轄區。

82. 網絡詐騙的去中心化性質亦令情況更加複雜。各司法管轄區之間的國際合作重點可能並不相符。例如，司法管轄區甲的受害人將資金轉移到司法管轄區乙，而司法管轄區乙的受害人卻身處司法管轄區丙（即司法管轄區甲可能優先考慮與司法管轄區乙合作，但司法管轄區乙卻可能優先考慮與司法管轄區丙合作）。由於個案涉及多個地區的公私營持份者及合作伙伴，這亦增加了識別及追查非法資金的難度。

- 網絡詐騙集團利用多種金融服務及資產類別。不同供應商及界別之間的跨境交易幾乎可以瞬間進行，難以追查及歸納轉移資金。
- 相關的數碼法理證據亦可能分布在不同司法管轄區，使有關當局難以全面掌握犯罪集團如何運作及清洗得益。數碼法理證據多變難測，不盡快保存便可能會消失，令情況變得更加複雜。

83. 正式合作（包括相互法律協助）一般需時較長。由於數碼罪行及相關洗錢活動過程快速，證據如不加以保存將很快消失，依靠正式合作效果或未如理想。為了繼續靈活地提供跨境協助，以阻遏網絡詐騙活動，主管當局趨向依靠非正式合作機制直接與外國的合作伙伴分享資訊。這可以透過各種渠道在執法機關或財富情報單位層面進行。這些渠道包括埃格蒙特組織的保安網絡、國際刑警組織的 I-24/7，以及其他非正式網絡，例如卡姆登資產追回跨機構網絡（CARIN）及地區性資產追回跨機構網絡（ARINs）。

專題 39. 透過非正式多邊網絡阻截網絡詐騙得益

為了打擊日益嚴重的網絡詐騙，法國調查當局主動利用非正式網絡，其中包括 CARIN 下的歐洲資產追回辦公室（ARO）分網絡，以促進有效的國際合作及相關資產追討。法國的資產追回辦公室與這兩個網絡的成員緊密合作，使其他司法管轄區專責追查、檢取及沒收犯罪資產的執法機關以及財富情報單位能夠迅速與法國交換情報。在緊急情況下，法國當局可最快在8小時內回覆請求。此類合作讓資金可以快速保存在最初識別的目的地帳戶及所有其他後續分層帳戶中。

例如，在2022年，一間法國受害公司被騙存入1,875,000歐元到一個斯洛伐克受益銀行帳戶內，法國資產追回辦公室聯絡斯洛伐克的資產追回辦公室要求凍結相關戶口。經兩地的辦公室互相交流，該筆資金成功被攔截，而斯洛伐克當局亦獲得所需資料向法庭申請凍結令。最終，共1,874,907歐元被凍結，並隨後歸還受害公司。

來源：法國

84. 為有效提高調查網絡詐騙相關洗錢及追討得益的效率，司法管轄區應採取多邊合作而非雙邊合作。本節透過兩個可行成果探討國際合作的挑戰和做法：(i)追討資產以及(ii)執法及檢控。

5.1. 追討資產

85. 快速的洗錢活動為追討網絡詐騙得益帶來莫大挑戰。為此，多個機構創立了多邊「快速應對」計劃，以追討網絡詐騙得益，其中包括國際刑警組織的I-GRIP、埃格蒙特組織的商業電郵詐騙計劃及美國的金融詐騙攻擊鏈。根據這些機構及司法管轄區的經驗，一般最有效的介入時間為詐騙交易進行後的24至72小時。這有效減低資金其後被轉移到多個分層帳戶的風險，從而大幅縮窄洗錢調查的範圍，有利追回非法得益。

專題 40. 金融詐騙攻擊鏈（Financial Fraud Kill Chain）及追討資產小組

美國聯邦調查局及金融罪行執法網絡（美國財富情報單位）於2016年成立金融詐騙攻擊鏈，以應付日益嚴重的商業電郵詐騙。攻擊鏈利用金融罪行執法網絡與埃格蒙特組織財富情報單位的聯繫，試圖協助追討詐騙案件有關的國際電傳轉帳。然而，電傳轉帳必須符合以下條件方可執行有關程序：(1)該電傳轉帳金額達50,000美元或以上；(2)該電傳轉帳為國際電匯；(3)已就該電傳轉帳發出 SWIFT 撤回通知；以及(4)該電傳轉帳在72小時內匯出。

2018年，美國聯邦調查局的網絡犯罪投訴中心(IC3)成立追討資產小組，以應對本地電傳轉帳的漏洞。小組簡化了與各金融機構的溝通程序，並協助各聯邦調查局地區辦事處凍結與詐騙有關的本地轉帳資金。小組的工作獲得顯著成效，至今已凍結73%被呈報至 IC3的詐騙案資金（即5億9,062萬美元中的4億3,330萬美元）。根據美國的一宗案例，這個計劃在某些情況下可以快速識別第二層帳戶並凍結資金，因而有可能追討全數騙款。

來源：美國

86. 這些多邊計劃的主要目的有兩個：為採取執法行動收集最低限度的所需資料，並把資料交到「對的人」。為確保有效跨境應對問題，多邊網絡內的所有成員已就網絡的管治規則及程序達成共識。雖然這些多邊網絡通常屬全球性質，但在已建立的區域性合作項目中提出倡議項目亦有助減輕有關挑戰。

專題 41. 跨司法管轄區的反詐騙計劃

因應詐騙的跨國特性，金融情報諮詢小組(Financial Intelligence Consultative Group)[1]推出一項由馬來西亞、印尼及新加坡的財富情報單位領導，名為跨司法管轄區反詐騙計劃的地區倡議，旨在為受害人偵測、追查及追討資金。

金融情報諮詢小組成員國之間建立了一個涉及跨境交易的應變機制，讓成員可更快捷方便地分享金融情報及資訊，協助有關當局迅速採取行動，以打擊詐騙及追討贓款。

來源：馬來西亞

[1] 金融情報諮詢小組是一個由東南亞國家、新西蘭及澳洲的財富情報單位組成的地區組織。

跨境蒐集及交流資訊：「收集最低限度的資料」

87. 在特別組織建議 3 的規定下， 如果根據當地法例網絡詐騙屬嚴重罪行，司法管轄區必須將網絡詐騙定為洗錢上游罪行。此外，傳統形式的詐騙案多涉及熟人，與涉及債務人和債權人之間的潛在民事爭議相似，難以作出區別；而網絡詐騙的涉案人士多數並不相識，因此相對較容易提出表面證據，無須像其他類型的罪案（沒有被普遍承認為上游罪行的罪案）般費時闡述和界定案件的犯罪關聯。

88. 作為良好的做法，各個快速應對計劃都應使用範本，以加快收集和交流資訊。範本有助快速收集定罪所需的最低限度資料，讓應對單位可集中處理刑事投訴最初階段所需的關鍵證據或資料；亦可確保交流所得的資訊質素，加強跨境執法的應對。

89. 除了網絡詐騙的案情摘要外，範本一般亦要求提供追查資金所需的基本資料。統一請求標準能讓接獲請求的司法管轄區快速處理收到的請求，加快執法機關攔截已流入該區的非法資金。

90. 範本上的資料欄目可包括匯款人及受益人的帳戶資料及交易資料（日期、時間、轉帳金額）。為進一步提升成效，如資金已被匯出受益人的帳戶，範本亦有可包括下一層帳戶的資料。此外，各司法管轄區亦可以減少對其他司法管轄區的在資訊披露限制，以便接收資訊方可與當地各主管當局披露接獲的資訊。

專題 42. 國際刑警組織環球快速支付干預機制（I-GRIP）

國際刑警組織建立了一個全球性止付機制 I-GRIP，讓組織成員呈交及處理與跟進、阻截或臨時凍結網絡詐騙得益有關的請求。I-GRIP 最初於2022年作為反洗錢快速應對機制試行，全賴試行階段期間多宗成功止付案例，機制於2022年11月正式推行。

I-GRIP 促進國際刑警組織中成員之間的交流，以預防可疑非法資產在成員國之間轉移。透過 I-GRIP 提交的請求須包含充足的資料，以便接獲請求的成員採取行動，例如交易日期、貨幣和金額、受益人和匯款人帳戶的帳戶號碼及金融機構名稱。

來源：國際刑警組織

91. 此外，標準範本上的資料欄目可便利國際機構集中分析數據，提高調查及追討資產的效率。例如，國際刑警組織利用其渠道交換獲得的資料建立內部數據庫（即金融犯罪分析檔案），以便分析各種金融罪行形式的跨國情報，以及識別跨境案件與調查、威脅、犯罪趨勢及犯罪網絡之間的關係（另見下文專題45）。

92. 為進一步加快追討資產，部分司法管轄區讓外國受害人直接向其執法機關提交網絡詐騙投訴，包括透過網上報案平台直接獲取執法行動所需的資料（見上文第4.1 節）。這樣可免除額外的溝通，讓主管當局快速採取可行的措施，打擊在其司法管轄區內向受益帳戶進行的可疑交易。

採取行動所需的力量：「對的人」

93. 由於速度是關鍵，因此較理想的做法是把收集到的資料直接交到已具備適當權力及追討資產專業知識的有關當局，以便其在接獲請求後立即採取臨時措施，防止資產進一步被清洗或轉移，亦為執法機關提供重要的時間繼續調查、拓展及蒐集證據，以及跟進正式的相互法律協助請求。

專題 43. 實體提出延期請求

意大利的財富情報單位接獲一宗暫緩交易請求，涉及四筆總值490,000歐元的可疑電傳轉帳。該交易由一間意大利服裝批發貿易公司向數間位於亞洲國家的公司發出。該電傳轉帳的資金相信源自一宗涉及一間西歐受害公司的商業電郵詐騙案。

意大利財富情報單位接獲上述西歐國家的財富情報單位提供的資料；並收到有關該意大利公司的舉報，指該公司涉嫌透過另一東歐國家參與上述亞洲國家的稅務詐騙。這亦證明網絡詐騙及其他類型的有組織罪行有關聯。該等交易最終獲得暫緩，令外國當局能夠發出外國扣押令，在意大利追討資金。

來源：意大利

94. 然而，由於各司法管轄區的立法和執法框架不同，此類直接交流或會遇到挑戰。最理想的應對方法包括建立本地協調機制，以便把請求轉到合適當局處理，並善用公私營合作渠道及金融機構的能力，讓它們在接獲主管當局發出的可疑交易通知後自發採取臨時措施。

管治及規定：「集體協議」

95. 多邊框架的管治及規定確定了司法管轄區之間相互承認的犯罪活動性質，亦為在接獲資訊後迅速採取行動制訂了承諾。由於司法管轄區之間已事先商定加入並提供協助的條件，有助解決國際機構間優次考慮不相符的情況。在理想的狀況下，這些規則及準則應清晰易明。

96. 上述原則適用於正式及非正式的國際合作機制。舉例來說，歐洲議會和理事會第 2018/1805 號條例接納互認外國凍結令和沒收令。這個直接執法機制讓有關當局可迅速作出跨境干預。

97. 加快資訊共享並不應以犧牲數據的安全保密為代價。為確保資料安全傳送，多邊框架通常利用現有的安全通訊通道，例如由國際刑警組織、歐洲刑警及埃格蒙特組織提供的渠道。這些現有通道免卻了發展雙邊交流渠道的必要，令多邊框架更易於擴張。

專題 44. 埃格蒙特組織商業電郵詐騙項目小組

商業電郵詐騙對金融機構及其客戶構成的威脅日益嚴重，11個財富情報單位因而推行「埃格蒙特組織商業電郵詐騙項目小組」，專責分析商業電郵詐騙趨勢、指標及方法，並與其他財富情報單位分享主要結果。常見的商業電郵詐騙手法及案例顯示，迅速採取行動攔截和追蹤電傳轉帳是打擊這類罪行的最有效方法。

因此，項目小組[1]在執法機關與財富情報單位及國際財富情報單位之間訂立協議，以跟進及凍結商業電郵詐騙得益。

- 在接獲與可疑的跨境商業電郵詐騙有關的可疑交易報告後，接獲報告的財富情報單位會向目的地財富情報單位發出「快速應對」請求。
- 請求應包含協定的基本資料以及採取執法行動所需的交換資料。
- 在情況許可下，目的地財富情報單位會被要求即時採取行動阻截及追討非法得益，最理想的做法是在罪案發生後的72小時內行動。

商業電郵詐騙項目利用埃格蒙特組織的保安平台作溝通，以交換「快速應對」請求。

來源：埃格蒙特組織

[1] 目前計劃成員包括來自澳洲、孟加拉、比利時、法國、加納、匈牙利、以色列、黎巴嫩、盧森堡、馬來亞西和美國的金融情報單位及歐洲刑警。

5.2. 執法及檢控

98. 除了追討資產外，網絡詐騙的跨國特性亦導致執法過程困難重重，從蒐集情報及展開調查到收集證據以提出檢控都絕不容易。科技發展提高了交易速度，令分散的跨境行動更方便，使執法機關需要更多時間和精力去追查和識別騙徒。

蒐集數碼證據

99. 雖然數碼法理證據與洗錢並非完全相關，但數碼法理證據可為執法機關提供重要線索，以進一步展開洗錢調查。隨着身分隱藏服務（如虛擬私人網路）日漸普及又易於使用，要找出網絡詐騙的最終犯案人變得更加困難。

100. 可惜現時並無一個全球制度管理數碼數據的保留限期，包括與技術服務提供者相關的數據。多個司法管轄區強調數碼證據的消失會帶來重大風險，而正式合作機制的需時亦會導致無法快速獲取數碼證據。

101. 以下幾個做法有助減少挑戰：

- **利用非正式渠道**先蒐集及獲取情報，再透過正式合作渠道取得所需證據及陳述，預備展開司法程序。
- **公約及調查工具**（包括《電腦網絡罪行公約》，又稱《布達佩斯公約》）等可快速保存電子數據並傳送自動提供的資料，有助加快找出最終的網絡詐騙犯案人。《布達佩斯公約》亦建立了一個全天候網絡，確保即時就技術諮詢、證據蒐集、數據保存等方面提供調查協助。
- 與海外服務提供者**直接合作**，在無須經過相互法律協助程序下取得用戶資料等所需法理證據。有司法管轄區表示，海外服務提供者自願直接合作是蒐集相關數碼證據的最有效機制[22]。

專題 45.《布達佩斯公約》

《布達佩斯公約》列明以下程序權力：加快保存儲存資料、加快保存和披露部分流量數據、交出令、搜尋和檢取電腦數據、實時收集流量數據，以及截取內容數據。公約亦提供了一個快捷有效的國際合作制度。

《電腦網絡罪行公約》的第二附加議定書關乎加強合作及電子證據的披露，並就以下事項提供法律依據：披露域名註冊資料；與服務提供者直接合作以取得用戶資料；獲取用戶資料及流量數據的有效手段；緊急情況下的即時協作；相互協助工具；以及個人資料保護措施。

來源：歐洲議會

[22] 就自願與海外服務提供者合作事宜，請參閱歐洲議會（2020 年 7 月）《*The Budapest Convention on Cybercrime: benefits and impact in practice*》。

聯合執法行動

102. 跨境聯合調查小組涉及兩個或以上的司法管轄區的主管當局為展開刑事調查而簽訂的法律協議，以便分享資訊及跨境追查。有關當局一般會透過各種框架及協議（例如歐洲司法合作組織、歐洲刑警轄下聯合網絡犯罪行動特別工作組）來分享資訊。

103. 聯合調查小組的跨境及去中心化運作模式，為打擊網絡詐騙的多邊執法行動提供了一個重要的協調點。隨着犯罪活動的門檻降低，網絡詐騙集團可輕易轉移和建立遙距運作的數碼中心。因此，各主管當局必須互相協調以同時將在多個司法管轄區運作的犯罪分部連根拔起。

專題 46. 就大規模投資詐騙採取聯合行動[1]

在歐洲司法合作組織的支持下，塞爾維亞、奧地利、保加利亞及德國針對兩個涉嫌參與大規模網絡交易投資詐騙的有組織犯罪集團展開行動。塞爾維亞當局拘捕了五名疑犯，經搜查九個地點後，檢獲五個公寓、三輪汽車、大量現金及資訊科技設備，另有三十多個塞爾維亞銀行帳戶受到監察。此外，四名疑犯於保加利亞被捕及250萬歐元來自一間參與詐騙計劃的公司銀行帳戶於德國被凍結。

根據行動期間蒐集得來的資料，有關當局於兩日後迅速對一間位於貝爾格萊德的公司展開另一次行動，並拘捕一名疑犯以及檢獲多個伺服器、其他資訊科技設備及文件。

在這案件中，塞爾維亞當局引用《布達佩斯公約》第26條與其他合作伙伴分享資訊。歐洲司法合作組織進一步協助調查，資助一個聯合調查小組，並在其位於海牙的大樓舉辦一個合作會議及一個視像會議。

來源：塞爾維亞；歐洲議會（2020年7月）《*The Budapest Convention on Cybercrime: benefits and impact in practice*》

[1] 請參閱歐洲司法合作組織（2020年4月）發布的新聞稿：
https://www.eurojust.europa.eu/news/action-against-large-scale-investment-fraud-several-countries

104. 雖然如此，聯合執法行動亦存在挑戰：

- **法律上的障礙**可能對非正式的資訊共享造成限制，即使在聯合調查小組內也不例外。有司法管轄區表示，依靠相互法律協助請求才可交換資訊的做法，可能影響效率及參與意欲，而可以分享的資料亦可能有所限制，特別是有關金融交易資料精細程度的資料。
- **能力不均及優先次序不同**亦可能影響司法管轄區參與聯合行動。如上文所述，各司法管轄區內的優先次序或許未能配合聯合行動，即使面臨日益嚴重的網絡詐騙，但在資源有限的情況下，各司法管轄區在平衡各方利益時亦須作出艱難的決定。

105. 除了聯合調查小組外，國際刑警組織等多邊組織推行的聯合行動，也為打擊網絡詐騙的多邊執法行動提供了一個重要協調點。雖然這些行動沒有如聯合調查小組般擁有正式法律協議，但仍為相關司法管轄區提供了重要的平台共同打擊網絡詐騙。

專題 47. 國際刑警組織 HAECHI 行動

自2020年起，國際刑警組織針對借助電腦網絡的金融罪行及相關洗錢展開一年一度的 HAECHI 行動，以支持參與行動的司法管轄區之間的資訊交流。2022年的 HAECHI III 行動獲得30個司法管轄區參與，接近1 000名疑犯被捕，2 800個銀行及虛擬資產帳戶被凍結，帳戶內的相關非法得益達1億3,000萬美元。國際刑警組織透過 HAECHI III 行動在成員國之間協調了多個案件，共同打擊網絡詐騙。

HAECHI 行動也提供機會讓各成員透過金融犯罪分析檔案(FINCAF)為尚在進行的調查之間的關聯作分析。金融犯罪分析檔案包含與任何種類的金融罪行及跨境罪行有關的數據和其他資料。國際刑警組織透過檔案與各成員國合作，加強對網絡詐騙等國際有組織罪行的整體戰術應對。金融犯罪分析檔案是一個重要工具，讓各成員國更深入了解跨境犯罪活動、犯罪集團、集團的組織架構、其成員的角色及關鍵人物、犯罪手法以及虛假金融交易。

來源：國際刑警組織

公私營合作

106. 由於網絡詐騙不受地域所限，因此可超越國界的公私營合作能夠取得更大成效。一如本地公私營合作，此類協作可涵蓋手法或策略分享以及行動協調。因應行動目的，參與這些合作計劃的成員亦有所不同，可包含相關的傳統打擊洗錢及恐怖分子資金籌集界別及非傳統界別。

專題 48. 歐洲錢騾行動

歐洲錢騾行動是一個以公私營資訊共享為基礎的國際行動，旨在打擊新式的複雜案件。

2022年，在歐洲銀行聯合會的持續協調下，約1 800間銀行及金融機構聯同網上匯款服務供應商、加密貨幣交易平台、金融科技及「認識你的客戶」公司，以及跨國電腦科技公司，為這個行動的執法工作提供支援。這次行動由來自25個司法管轄區[1]的執法機關組成，並得到歐洲刑警、歐洲司法合作組織及國際刑警組織支持。行動中發現8 755名錢騾及222名錢騾招聘者，共攔截了1,750萬歐元資金，並拘捕了2 469名錢騾。

來源：歐洲刑警

[1] 澳洲、奧地利、保加利亞、哥倫比亞、塞浦路斯、捷克共和國、愛沙尼亞、希臘、匈牙利、新加坡、中國香港、愛爾蘭、意大利、摩爾多瓦、荷蘭、波蘭、葡萄牙、羅馬尼亞、斯洛伐克共和國、斯洛文尼亞、瑞典、瑞士、西班牙、英國及美國

6. 總結及主要工作範疇

107. 網絡詐騙涉及跨國有組織犯罪集團。隨着全球數碼化及虛擬服務漸趨普及，預期網絡詐騙的規模及程度會不斷擴大。各司法管轄區不應忽視各行業（包括數碼金融機構及非傳統業界）的新增漏洞，罪犯或藉着數碼化普及來提升網絡詐騙及洗錢技術。

108. 各司法管轄區應打破各自為政的局面，在本地及國際層面上加快和加強各行業與機構之間的合作。由於網絡詐騙及相關洗錢的去中心化性質，重要的金融資料及證據經常分散各地，增加了調查及瓦解犯罪集團以及追討網絡詐騙得益的難度。

109. 網絡詐騙不但會對受害人造成嚴重經濟損失，亦會對社會及經濟環境造成損害。為更有效打擊網絡詐騙及相關洗錢，本報告在總結部分列出各司法管轄區的三個主要工作範疇：加強本地協作；推動多邊合作；以及加強偵測及預防。

有效打擊網絡詐騙及相關洗錢的主要工作範疇

加強本地公私營協作

- 各司法管轄區應建立協調機制，聚集相關的主管當局，全面打擊網絡詐騙及相關洗錢，包括電腦網絡罪行技術專家以及非傳統界別（例如社交媒體平台、電子商貿、電訊及網絡服務供應商）。各司法管轄區亦應善用公私營合作，以加強偵測及調查，並加快追討資產的應對行動。
- 理想的做法是設立一個中央單位，專責處理相關資訊及協調各公私營機構的行動，包括調查、追討資產及預防詐騙。

推動多邊國際合作

- 為提升追討資產的成效以及防止網絡詐騙相關得益被轉移，各司法管轄區應攜手合作，迅速阻截網絡詐騙得益。根據行動經驗，最佳的介入時間一般為網絡詐騙發生後的 24 至 72 小時。要有效追討被清洗及分散到多個司法管轄區的網絡詐騙得益，必須聯合全球的有關當局採取行動。
- 為此，各司法管轄區應善用及支持現行（以及未來設立）的多邊機制（例如國際刑警組織的 I-GRIP 及埃格蒙特組織的 BEC 計劃），促進國際合作及情報交流，以打擊網絡詐騙。該等多邊機制促使各司法管轄區互相合作，共同瓦解跨國網絡詐騙集團。

加強偵測及預防

- 為加強偵測，各司法管轄區應採取便利受害人舉報的措施，例如透過專門平台簡化報案程序，亦應與私營機構合作，改善可疑交易的報告。
- 各司法管轄區應透過公眾教育，提高市民對網絡詐騙的意識及警覺性，包括分享網絡詐騙的危險信號及提高大眾的網絡知識。預防網絡詐騙至為重要，可大幅減少網絡詐騙集團的整體收益。各司法管轄區亦應與私營機構合作，支持預防網絡詐騙的策略，例如實施消費者保障措施及移除犯罪工具。

附件甲：網絡詐騙的風險指標

以下潛在風險指標汲取了來自特別組織全球網絡、埃格蒙特組織及不同司法管轄區的私營機構的經驗及數據，旨在加強偵測與網絡詐騙有關的可疑交易。指標進一步從開立帳戶到監察交易劃分成多個範疇，適用於受規管實體，包括金融機構、虛擬資產服務提供者、指定的非金融企業及行業以及其他金融及支付機構。

有關當局無法僅憑一項指標，便懷疑客戶／交易涉及網絡詐騙，亦不能就此斷定客戶／交易涉及有關活動，但卻可適時就此進行進一步監察和檢查。

交易模式

- 開戶後迅速或立即進行與開戶目的不相符的大額或小額交易
- 在收到資金轉帳後，迅速或立即提款或轉移大額資金，以清空帳戶
- 頻繁進行大額交易，與帳戶持有人的經濟狀況不相符（例如突然進行國際轉帳、利用支付卡在外地的自動櫃員機提款、大量購入虛擬資產或出口到國外的貨品，或付款予無牌經營的海外價值轉移服務）
- 將資金轉入高洗錢風險的司法管轄區，或從該等司法管轄區轉撥出來
- 與新成立的公司及／或其主要活動與受益人進行的活動不相符或具一般用途的公司頻繁進行大額交易
- 成功向受益人支付小額資金後，隨即向同一受益人支付大額資金
- 頻繁及／或大額購買金額為整數的貨品，表示貨品可能為禮品卡

客戶交易說明和備註

- 客戶在成功交易後立即要求追加付款，但該名客戶過往未曾利用此帳戶支付供應商。這種行為與罪犯行騙的方式一致，罪犯得知詐騙付款成功後，會試圖再次在未經授權的情況下追加付款。
- 客戶看似合法的交易指示中，包含與過往已核實的交易指示不同的語言、時間及金額
- 交易指示包含標記、說明或文字指定該交易請求為「急件」、「高度機密」或「機密」
- 客戶以格式不當的信息／電郵（拼寫及／或語法錯誤）作為交易的理據
- 交易指示直接向一名已知受益人付款，但該名受益人的帳戶資料與過往使用的不同
- 交易說明上的預定受益人與受益銀行所知悉的帳戶持有人名字不一致
- 交易指示來自沒有金融經驗或專業知識的自然人（投資者）並以支付與投資及金融產品相關的款項為由向一些公司（多數是設立在高風險司法管轄區的公司）轉帳

- 帳戶的業務／公司名稱與交易對手方不相乎，可能表示該公司在隱藏大額的國際資金轉移（例如報稱為家具公司的公司多次向一間以石油貿易公司為名的公司進行大額轉帳）
- 以時區不相符的裝置進行交易

帳戶持有人背景可疑

- 帳戶持有人不願意或無法通過客戶盡職審查
- 帳戶持有人不熟悉流經其帳戶的資金來源，或聲稱為他人進行交易
- 頻繁使用外國的詞句或術語更改法律實體／獨資業務的名稱
- 客戶對交易或業務關係的性質、對象、金額或目的缺乏了解，或提供不切實際、令人混淆或前言不對後語的解釋，令人懷疑該名客戶在充當錢騾

帳戶用戶身分可疑

- 用戶試圖以共享、偽造、盜取或經修改的身分證明（地址、電話號碼、電郵）隱藏身分
- 開戶後頻繁更改聯絡資料、電話號碼、電郵地址
- 電郵地址與帳戶持有人姓名不相符，或有多個帳戶使用相似的電郵地址
- 客戶個人資料不符合規定，例如與其他帳戶共用資料（例如兩個或更多用戶）
- 發現異常的網絡行為，例如輸入數據時猶豫不決、延遲按鍵、自動化跡象、嘗試多次登入失敗等
- 帳戶與預期在該司法管轄區內不再活躍的實體有關（例如海外學生畢業後出售的帳戶）
- IP 地址或全球地位系統（GPS）源自高洗錢風險的司法管轄區
- 使用虛擬私人網路（VPN）、被入侵的裝置連結而成的網絡（如 IOT 裝置）及網頁寄存公司以隱藏用戶的真實 IP 地址
- 多個 IP 地址或電子儀器與同一個網上帳戶有關聯
- 一個固定 IP 地址或電子儀器與多個帳戶持有人的多個帳戶有關聯
- 透過電腦連接埠(如 TeamViewer 等應用程式)以遠端桌面連接登入帳戶，隱藏真正的裝置及位置
- 帳戶操作中出現過於迅速的按鍵或導航，表示可能由機械人控制

帳戶持有人的負面資訊

- 存在與客戶或交易對手相關並可核實的負面消息，例如已知或懷疑曾為詐騙受害人、錢騾或身分盜竊受害人所持有的帳戶
- 來自往來銀行或其他第三方詐騙數據庫的詐騙報告或交易撤回請求
- 存在電傳轉帳撤回請求
- 存在由財富情報單位或執法機關提供有關交易所涉及的人員的負面資訊

虛擬資產交易

- 發送／接收大額虛擬資產或頻繁地發送／接收小額虛擬資產到非託管錢包地址；或與暗網市場、兒童性虐待物品平台、網絡剝削市場、勒索軟件集團、混幣／轉幣服務、高風險司法管轄區、賭博網站及不法之徒相關的地址
- 用盡比特幣自動櫃員機的每日交易限額
- 無法提供文件證明虛擬資產或兌換成加密資產的資金的來源
- 轉移虛擬資產到與暗網非法活動（例如恐怖主義、兒童色情物品、毒品等）有關的錢包
- 交易涉及多於一種虛擬資產，特別是匿名性較高的虛擬資產
- 在沒有合理商業理由下，利用與點對點平台相關的錢包進行異常的虛擬資產交易活動

其他

- 帳戶號碼與帳戶持有人姓名不相符
- 透過閉路電視可見用戶以電話與他人聯絡或由他人陪同，並在交易過程中接受命令或指示
- 受益公司管理貿易／投資服務網站，而該等網站未經本地監管機構授權或列入名單

附件乙: 借助反詐騙和打擊洗錢及恐怖分子資金籌集管制之間的協調效應

本附件彙集金融監管機構採取的反詐騙以及打擊洗錢及恐怖分子資金籌集管制措施，部分針對不法之徒遙距註冊、登入及控制錢騾帳戶的能力。這些實例包括各種與客戶身分核實及交易監察有關的措施。

這些管制措施對金融機構、虛擬資產服務提供者及其他金融及支付機構非常有用。

- 建立嚴謹的認識你的客戶或認識你的業務程序、在數碼登入過程中應用生物特徵，以及識別手提電話或安全裝置，以核實網上銀行交易（其他裝置則被封鎖或採取較強風險緩減措施）。
- 為首次登記網上銀行服務或安全裝置的客戶設立冷靜期（即開戶時並不能即時享用所有銀行服務），並限制客戶的金融交易數量或金額。
- 制定預期交易的定義（交易數量、金額、交易對手方類型、涉及國家），以助偵測可疑交易；並加強詐騙偵測規則，以先發制人阻截非法交易。
- 使用「核實收款人」服務，讓轉帳指示涉及的匯款人／付款人／債務人檢查付款信息上提及的受益人／收款人／債權人與帳戶持有人的姓名是否一致。
- 減少透過電郵及社交媒體與客戶溝通，如有需要亦只僅限於一般資訊交流，並清楚說明不應透過電郵與金融機構／虛擬資產服務提供者交換任何身分證明或個人資料。
- 在與客戶的溝通中加入語音辨識軟件及人工智能支援，以確認客戶的真正身分。
- 採取多重認證機制，以核實客戶身分及進行金融交易，並透過不同渠道加入或啟動受益人。
- 利用以下方式，在遙距開戶期間核實用戶身分，並防止罪犯利用錢騾或受害人的帳戶資料登入多個帳戶：
    - 透過活體偵測測試（即確保客戶為真正活生生的人類）提升客戶身分認證程序的可靠性，包括在測試期間測試客戶有否利用社交工程；或
    - 監察連接到網上銀行網站的 IP 地址等，包括偵測遙距存取工具及「瀏覽器中間人」攻擊。
- 擴大舉報機構所蒐集及分析的客戶數據類型，包括手提電話號碼、IP 地址、GPS 坐標、裝置識別碼等。為預防詐騙，金融機構可採取以風險為本的方式重複進行身分認證（例如在偵測到異常行為時進行這些檢查）。
- 實施以風險為本的實時交易監察系統，確保能夠迅速偵測及調查異常活動，並在有需要時提交可疑交易報告。監察系統的結果應與金融機構處理的交易數量和性質相應。

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

INTERPOL

FATF

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

2023年11月

網絡詐騙衍生的非法資金流

本報告會先剖析借助電腦網絡詐騙的手法、該行為與其他罪行的關連，以及罪犯如何利用新科技的弱點，再列舉國家應變行動及策略的成功例子，顯示如何打擊借助電腦網絡詐騙活動，然後指出各項風險指標及有效的防騙規定和管控措施，以助公私營機構偵測和預防借助電腦網絡詐騙及相關洗錢罪行。