APG 年度態樣報告 2023

Asia/Pacific Group on Money Laundering

洗錢與資恐之手法與趨勢

亞太防制洗錢組織

2023 年 12 月

APG 秘書處
Locked Bag A3000
Sydney South
New South Wales 1232
AUSTRALIA

電話:+61 2 5126 9100
電郵: mail@apgml.org
網址: www.apgml.org

免責聲明:

依據 2012 年 APG 職權條款第 1 條，APG 為一非政治性、技術性組織，其會員皆致力於有效執行並落實由防制洗錢金融行動工作組織（FATF）制定之國際公認防制洗錢、打擊資恐、及資武擴之標準。本文件及其所載任何陳述，或其中所附任何地圖，均不影響對任何領土之地位或主權、國際邊界之劃分與界線，以及任何領土、城市或區域之名稱。

目錄

前言

亞太防制洗錢組織（APG）是亞太地區的類 FATF[1] 區域性組織。APG 其中一項任務是發布區域性洗錢（Money Laundering, ML）及資助恐怖主義（Terrorism Financing、TF）態樣報告，以協助各國政府與利害關係人更深入瞭解現有及新興之洗錢與資恐威脅的本質，並制定有效因應策略。當一連串洗錢或資恐行為以類似方式或相同手法執行時，通常被歸類為「態樣」（typology）。態樣研究有助於 APG 成員國制定有效調查、並起訴洗錢與資恐的策略，同時設計與落實預防性措施。

APG 會員及觀察員每年均會提供案例研究、趨勢觀察、研究報告、監理執法行動資訊及國際合作範例。本報告所載案例，僅為亞太地區及其他區域執法與情報機關偵查並打擊洗錢與資恐行動之部分成果。許多案件或評估結果，因涉及敏感性或正處於調查／司法程序之中，無法對外公開。

APG 2023 年度態樣報告依據會員之意見回饋調整格式，主要變動如下：

- 新增索引，以便將每則案例依多重主題進行交互檢索。
- 新增資產返還專章，透過案例分析重點說明有效追回犯罪所得、犯罪工具、或等值利益（包括國內外）所面臨的成功經驗與挑戰。
- 擴充 APG 觀察員機構所進行態樣相關工作的內容。

為保護案例隱私，本報告已針對案件中的涉案人與犯罪者之姓名、公司名稱及涉及其他轄區的相關資訊，進行去識別化編輯處理，匿名化案例內容。若 APG 會員提及其轄區及當地主管機關，則予以保留。個人多以「某」稱呼並以字母標識，例如「A某」。於同一案例內，「A某」指同一人；但不同案例中的「A某」則代表不同人。司法管轄區亦復如是。一個案例中的「X司法管轄區」與另一案例的「X司法管轄區」未必是同一個司法管轄區。貨幣除另有標註為美元（USD）外，均以提供案例的 APG 會員國當地貨幣顯示，第 7 節附有貨幣轉換表供參考。

APG 運作委員會（Operations Committee）負責督導態樣研究計畫；2022 至 2024 年由薩摩亞及印度共同擔任主席。

APG 感謝澳洲交易報告與分析中心（AUSTRAC）於關鍵時刻協助 APG 秘書處編輯與彙整 2023 年度態樣報告。

[1] 防制洗錢金融行動工作組織

1 重點領域 - 虛擬資產與虛擬資產服務提供商

1.1 概述

2018 年 10 月，防制洗錢金融行動工作組織（下稱「FATF」）修訂其建議，以明確涵蓋涉及虛擬資產（Virtual Assets，VA）之金融活動，並就虛擬資產服務提供商（Virtual Asset Service Providers，VASPs）之管理與監理制定標準。相關規定載於建議第 15 項（R.15）。自 2018 年起， FATF 與其全球網路一直致力於強化該規定之落實成效。

將虛擬資產納入 FATF 標準，是對該新興技術之潛力及其潛在風險的認可。虛擬資產及其相關服務固然有促進金融創新與提升效率的潛力，但其特殊性質亦為洗錢犯、資恐分子及其他犯罪者開啟新的機會，使其得以藉由洗錢方式處理其犯罪所得、或資助非法活動。透過虛擬資產快速進行跨境交易，通常位於受規範金融體系之外；犯罪者不僅能夠數位化取得、轉移及儲存價值，還能模糊資金的來源或去向，造成申報機構難以及時辨識可疑活動。[2]

FATF 已辨識出多項與虛擬資產及虛擬資產服務提供商有關的新興趨勢，本報告的案例與研究結果也佐證了這些趨勢。近期研究尤其關注北韓透過竊取並洗錢數億美元價值的虛擬資產，以資助武器擴散（PF，下稱「資武擴」）方式金援大規模毀滅性武器。勒索軟體事件近年亦大幅增加，且贖金幾乎全數以虛擬資產支付。洗錢趨勢亦顯示虛擬資產被日益廣泛運用於多種洗錢手法之中。恐怖組織（包括伊斯蘭國、蓋達組織及其關聯團體，以及極右派恐怖組織）也日益使用虛擬資產，在全球範圍內募集與移動資金。

本章將簡要介紹 FATF 針對虛擬資產制定的防制洗錢與打擊資恐（AML/CFT）管控框架、追蹤 APG 會員對該等規範的落實狀況，並討論來自虛擬資產與虛擬資產服務提供商的威脅與趨勢。

FATF 方法論詞彙表

虛擬資產（*VA）是一種可以數位化交易或移轉，且可用於支付或投資目的、數位形式的價值。虛擬資產不包括已在 FATF 其他建議事項中涵蓋的法定貨幣、證券及其他金融資產的數位形式。*

虛擬資產服務提供商（VASP）*是指未於本建議其他部分規範之自然人或法人，以營業方式為其他自然人或法人、或代表其他自然人或法人，從事下列一項或多項活動或業務者：*

i. 虛擬資產與法定貨幣之兌換；
ii. 一種或多種形式的虛擬資產間之兌換；
iii. 虛擬資產之移轉；
iv. 虛擬資產或可控制虛擬資產工具之保管及／或管理；
v. 參與並提供與發行人之虛擬資產發行或銷售相關的金融服務。

[2] FATF 2020 年, *洗錢與資恐的虛擬資產紅旗指標, 前言* https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf

1.2 威脅與趨勢

隨著虛擬資產產業持續發展，犯罪分子獲取犯罪利益運用的手法也隨趨勢日新月異。 APG 特別關注區塊鏈分析公司所提供的研究報告，特別是*Chainalysis發表的《2023 年加密犯罪報告》*（*Crypto Crime Report 2023*）及*TRM Labs提供的《2023年非法加密生態系統報告》*（*Illicit Crypto Ecosystem Report 2023*）。

根據 Chainalysis 的《*2023 年加密犯罪報告*》，2022 年非法加密貨幣交易量創歷史新高，總交易金額約為 206 億美元。[3] 然而值得注意的是，該數額僅占所有加密貨幣交易總額的 0.24%。與虛擬資產相關的常見犯罪類型為洗錢與前置犯罪（predicate offences），但透過虛擬資產進行資恐及資武擴的案例也持續增加（詳見下文 1.3 及 1.4 節）。

根據 APG 成員國與區塊鏈分析公司的報告，詐欺、竊盜、駭客入侵、勒索與勒索軟體攻擊為最常透過虛擬資產進行的非法活動。這些活動所涉及的前置犯罪通常與網路賭博、電腦犯罪、詐欺、逃漏稅、非法或管制物質（例如毒品及槍械）之銷售、兒童剝削（child exploitation）及人口販運等有關。此外，利用虛擬資產規避聯合國及其他國際制裁，也是重點關切領域之一。

Chainalysis《 2023 年加密犯罪報告》： 2022 年洗錢活動摘要

Chainalysis 指出，透過虛擬資產進行洗錢通常涉及以下兩種類型的實體與服務：

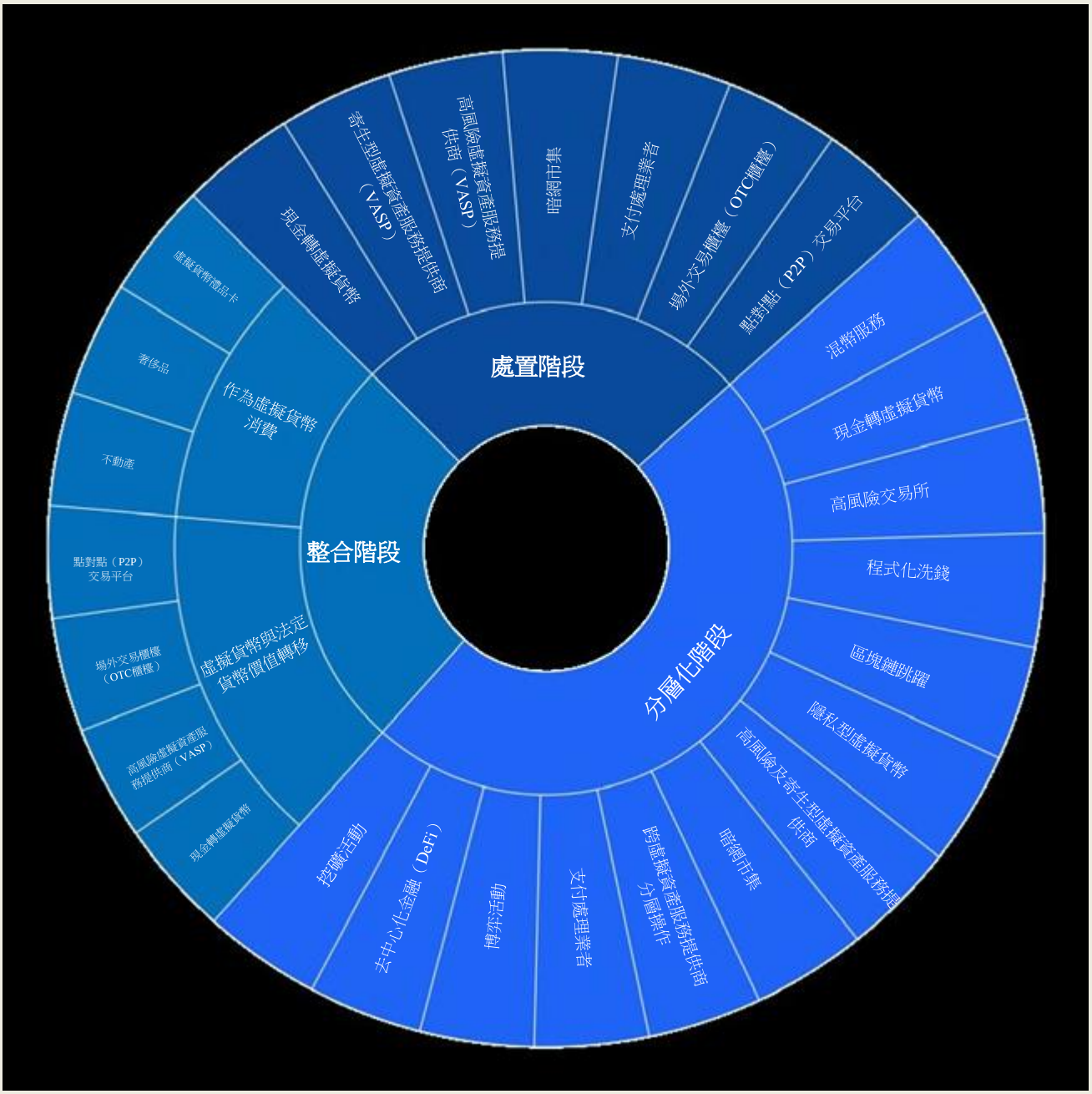
- 中介服務與錢包:包含非託管型錢包（unhosted wallets）、混幣器（mixers）、暗網市場（darknet markets）及其他服務。犯罪分子利用此類服務暫存資金、隱匿資金流向或進行資產間的轉換。
- 法幣出金兌換（fiat off-ramps）：此為允許虛擬資產兌換為法定法幣出金兌換貨幣的服務。一旦完成兌換，資金即無法透過區塊鏈追蹤，只有服務提供者（例如 VASP）可以追蹤資金流向。

在洗錢機制方面，中心化交易所（centralised exchanges）是非法加密貨幣的主要接收方，近半數來自非法地址的資金直接流入中心化交易所。此點值得注意，特別是考量虛擬資產服務提供商負有防制洗錢及打擊資恐的義務。

至於其他機制，有越來越多非法資金流向去中心化金融協議（DeFi protocols）[4]。此為駭客竊取虛擬資產時慣用的管道。暗網市場業者與管理者將非法資金主要送往其他非法服務（例如其他暗網市場）或高風險交易所。勒索軟體攻擊者與詐欺犯罪分子則將大部分資金送往加密貨幣混幣器。

*TRM Labs在《2023 年非法加密生態系統報告》*中，囊括了以下頁圖表說明虛擬資產在洗錢三階段（處置、分層化、整合）中的使用情形。此圖表為評估虛擬資產及其服務提供商洗錢風險、威脅與趨勢的有效工具。

[3] Chainalysis《 2023 年加密犯罪報告》，TRM Labs《 2023 年非法加密生態系統報告》
[4] 去中心化金融協議（DeFi Protocal）由管理去中心化金融應用的標準、程式碼及程序所組成。



示意圖：TRM Labs《2023 年非法加密生態系統報告》

APG 成員國回報多項與虛擬資產及虛擬資產服務提供商相關的趨勢，最明顯可見的是，透過虛擬資產進行洗錢的情況持續增加。

中國澳門

在 2018 至 2022 年間，澳門執法單位對涉及虛擬資產及虛擬資產服務提供商活動進行約 100 起的調查案件。並觀察到此類案件的增加趨勢。在上述調查案件中，98% 的案件與詐欺、或投資詐騙有關；其中部分詐騙案件涉及虛假網站及應用程式，實際上並無任何真實虛擬資產交易。僅少數案件涉及實際使用虛擬資產（尤其是虛擬貨幣），但當地虛擬資產服務提供商的平台並未涉案。

菲律賓

自 2022 年 2 月起，菲律賓監理機關擴大交易報告要求，要求所有受規範對象（Covered Persons）在提交受規範交易報告（covered transaction report，CTR）及可疑交易報告（suspicious transaction report, STR）時，使用針對虛擬資產的專用交易代碼。在此之前，向菲律賓中央銀行註冊的虛擬資產服務提供商提交報告時所使用的交易代碼，是一般性的匯款、存款或外匯貨幣兌換交易代碼。

截至 2022 年 10 月中旬，在針對虛擬資產的大額交易報告中，大部分交易屬於平台內的虛擬資產轉移（占 58%），其次為向外部平台的虛擬資產轉移（占 17%），法定貨幣兌換為虛擬資產（占 15%），以及虛擬資產兌換為法定貨幣（占 10%）。至於交易金額，透過線上銀行轉帳將法定貨幣兌換為虛擬資產的交易占比最高（占 43%），其次為向外部平台的虛擬資產轉移（占 39%），平台內的虛擬資產轉移則占 13%。

被提交的可疑交易報告（STR）絕大多數與將虛擬資產轉移至外部平台有關（占總金額的 93%、及總筆數的 75%）。未經註冊的投資招攬所涉及的詐欺行為及其他違規情形，成為主要可疑原因（占總交易金額的 68%），其次為缺乏實質目的或經濟正當性的交易（占 14%），以及與財務狀況或支付能力明顯不符的交易（占 11%）。其他已辨識的前置犯罪則包括詐欺（5%）、兒童剝削（0.15%）與涉及影像或影片之偷窺行為（0.03%）。上述情形與歷史趨勢一致：菲律賓防制洗錢委員會（AMLC，隸屬菲律賓金融情報中心FIU）在 2020 年 3 月發表的一項研究顯示，投資詐欺相關原因（例如參與詐騙與非法投資計畫），是促使虛擬資產服務提供商向防制洗錢委員會提交可疑交易報告最常見的主因。同時被注意到的是，某些可疑交易的涉案對象亦將法定貨幣的匯款轉給位於境外轄區的虛擬資產服務提供商。此外，一些關係人（POI）亦被發現與其他獨立案件有財務關聯，這些案件涉及詐欺、毒品走私、未經授權的投資招攬、與駭客行為。他們除了相互進行交易外，也被發現以虛擬資產（尤其是加密貨幣）為理由，解釋其異常巨額的資金或交易流動。部分人士利用虛擬資產作為業務掩護，而另一些則聲稱其資金是存入、或來自位於境外的知名虛擬資產服務提供商所獲取的收益。

報告顯示某些關係人大量使用境外的虛擬資產服務提供商，加上國內虛擬資產服務提供商採用虛擬資產交易專用代碼的比例較低，此處所引用的統計數據僅代表透過菲律賓金融系統之虛擬資產相關交易的一小部分。儘管如此，數據顯示有大量虛擬資產被轉移至外部平台（特別是在發現有可疑之處的交易中），此亦證實有理由懷疑犯罪分子可能透過不同監理框架下的虛擬資產服務提供商轉移資金，藉此阻礙主管機關偵察其活動及追蹤資金流向的能力。

中國香港

隨著虛擬資產的日益普及，與虛擬資產相關的非法犯罪活動亦愈發頻繁。虛擬資產被誤用於洗錢程序中「分層化」階段的情形也呈現上升趨勢。2021 年與虛擬資產相關的犯罪案件數量達 1,397 件，較 2020 年增加 182.8%。 2021 年造成的財務損失達 8.241 億港幣，較 2020 年增長四倍。

日本

在日本，虛擬資產交易被評估為洗錢風險相對高於其他產品與服務的特定業務營運者，例如接受存款之金融機構與資金移轉服務提供商。當局認為目前所對網路安全等各類風險等建立的內部控制系統，未能跟上新進入加密資產服務提供領域業者的速度。
2021 年，因網路犯罪被逮捕的人數達 12,209 人，為歷史新高。勒索軟體案件的損害範圍擴大、透過未經授權的存取而洩露資訊、以及由具有國家背景的團體進行的網路攻擊也日益增加。

儘管使用區塊鏈分析工具取得交易歷史被視為降低風險的措施之一，但 FATF 指引亦指出其在技術限制上的相關挑戰。在日本虛擬資產交易服務提供者使用的加密資產當中，有一種資產並不公開轉移紀錄，使其難以追蹤交易，因此較易被用於洗錢及資恐活動。另一種資產則被指出在維護和更新轉移紀錄方面表現較差。若交易所使用的錢包由位於無義務辨識實質受益人的國家或地區內的個人、或虛擬資產交易服務提供商所持有或控制，則更難辨識交易中的加密資產所有人。由於幾乎所有透過加密資產交易服務提供商進行的交易都不是面對面，而是透過網路進行，因此具有高度匿名性。

在辨識與評估虛擬資產相關風險時，必須考量快速變化的環境。加密資產自動櫃員機（ATM）改變了虛擬資產的現金化或購買方式。例如，在日本以外地區已有案例顯示，毒品走私犯透過偽造身分文件，利用加密資產 ATM 將毒品販售所得之犯罪收益轉換為比特幣。公開資訊顯示，已有信用卡支付服務可直接使用虛擬資產（包括所謂的「穩定幣（stablecoins）」）。另外也有報導指出，一些機構投資人已公開表示將開始把虛擬資產納入其投資組合中。

由於全球範圍內存在可供個人使用、且無中央控管之去中心化金融（DeFi）服務，且部分司法管轄區仍未對虛擬資產服務提供商實施有效監管；因此可合理預期，虛擬資產相較其他金融服務，在洗錢及資恐方面之既有風險將持續增加。

1.3 透過虛擬資產進行資武擴

近年來，利用虛擬資產資助大規模毀滅性武器擴散提供資金的情況顯著增加，其中尤以北韓（DPRK）最為突出。

根據聯合國北韓問題專家小組（依據聯合國安全理事會決議第 1874 號成立，UNSCR 1847）2023 年 9 月的報告（見第 4.1 節），北韓國家支持的行為者於 2022 年竊取了將近 17 億美元的虛擬資產，此金額為 2021 年的三倍以上。[5] 此外，該報告亦引用區塊鏈分析公司 Chainalysis 的研究指出，為資助其核武計畫，北韓正將加密貨幣駭客攻擊列為優先行動。[6]

[5] 2023 年 9 月聯合國北韓問題專家小組（依據聯合國安理會第 1874 號決議成立）報告
[6] 圖 XXVII，2023 年 9 月聯合國北韓問題專家小組（依據聯合國安理會第 1874 號決議成立）報告，資料來源：Chainalysis。

2016 至 2022 年北韓網路威脅行動者每年竊取之虛擬貨幣總額

（單位：百萬美元）

資料來源：Chainalysis.

FATF 在 2023 年對虛擬資產標準執行情況的專項更新報告（Targeted Update）中指出，北韓透過非法虛擬資產活動來資助大規模毀滅性武器擴散的程度已成為顯著威脅，並呼籲各司法管轄區採取緊急行動落實 FATF 建議第 15 項（R.15），以降低透過虛擬資產進行資武擴的風險。[7]

虛擬資產被用於資武擴的非法活動類型日益增加，且手法日趨複雜，這些活動包括：

- 勒索軟體攻擊。（Ransomware attacks）
- 網路駭客行動。（Hacking）
- 魚叉式網路釣魚攻擊。（Spear-fishing）
- 惡意軟體。（Malware）
- 非同質化代幣（NFT）竊盜。
- 資訊科技人員派遣。（Placement of IT workers）

1.4 透過虛擬資產進行資恐

儘管目前透過虛擬資產進行的非法交易中，用於資恐的比例仍然相對較小，但使用虛擬資產進行資恐的情況正持續增加。

2023 年 2 月聯合國安全理事會決議第 1267 號（UNSCR 1267）專家小組報告指出，雖然伊斯蘭國（ISIL）目前仍主要依靠傳統方式（如哈瓦拉匯款系統 [hawala] 及行動支付服務）移轉資金，但其使用虛擬資產的比例正逐漸增加。[8] 此外，有證據顯示，恐怖主義組織使用虛擬資產的手法正日趨複雜。

[7] FATF（2023），《針對虛擬資產／虛擬資產服務提供商執行 FATF 標準之專項更新報告》，防止洗錢金融行動工作組織（FATF），法國巴黎。https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update- virtual-assets-vasps-2023.html

[8] 2023 年 2 月聯合國安理會決議第 1267 號（UNSCR 1267）專家小組報告—第 82 頁

根據 TRM Labs《2023 年非法加密生態系統報告》顯示，已辨識出數起伊斯蘭國（ISIS）接受虛擬資產捐款的募資活動，這些募資活動的規模達數萬美元。[9]

在 2023 年 FATF 的專項更新報告中， FATF 辨識出一種特定態樣，即虛擬資產被用於資助極右派恐怖主義活動，且通常透過群眾募資平台進行。[10]

1.5 虛擬資產與虛擬資產服務提供商的風險評估

在技術快速發展且不斷變遷的環境中，很明顯地，各司法管轄區對虛擬資產與虛擬資產服務提供商的風險評估是至關重要的第一步。

FATF標準要求各司法管轄區辨識並評估，源自虛擬資產活動與虛擬資產服務提供商活動或業務的洗錢及資恐風險；並根據所辨識出的風險，採取相應的風險導向方法進行風險緩解。虛擬資產服務提供商亦須採取適當措施以辨識、評估、管理並減緩企業本身與產品層面的洗錢及資恐風險。

多個技術援助提供機構已備妥相關資料，以協助進行風險評估。例如，世界銀行（World Bank）發布了名為《*虛擬資產與虛擬資產服務提供商之洗錢／資恐風險評估工具*》（Virtual Asset and Virtual Asset Service Providers ML/TF Risk Assessment Tool），此工具主要提供給各國權責機關使用。[11] 英國皇家聯合三軍國防研究所（Royal United Services Institute，RUSI）發布《*機構虛擬資產服務提供商及虛擬資產風險評估指引*》（Institutional Virtual Asset Service Providers and Virtual Assets Risk Assessment Guide），[12] 用以協助虛擬資產服務提供商辨識與評估企業層面的洗錢與資恐風險。上述工具均可協助各司法管轄區與個別虛擬資產服務提供商，履行其風險評估義務。

許多 APG 成員國已進行風險評估，以辨識與虛擬資產活動和虛擬資產服務提供商業務相關的洗錢／資恐風險，以下是部分成員國回報的案例：

中國香港

香港警務處（Hong Kong Police Force）的財富情報及調查科（Financial Intelligence and Investigation Bureau, FIIB）正進行一個與虛擬資產服務提供商相關洗錢趨勢的專題分析。透過全面檢視特定的可疑交易報告、金融情報中心（FIU）之間交換的情報，以及各種來源取得的犯罪趨勢資訊，並參考香港整體洗錢及資恐的威脅與弱點而成。該專題分析預計於 2023 年內發布調查結果。

[9] 2023 年 6 月TRM Labs《2023 年非法加密生態系統報告》
[10] 2023 年FATF專項更新報告
[11] https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use
[12] https://static.rusi.org/Institutional-VASP-VARAG-web-final.pdf

日本

日本於 2022 年 12 月 1 日發布《*2022 年國家風險評估追蹤報告》（National Risk Assessment Follow-up Report 2022*），其中包含對虛擬資產及虛擬資產服務提供商的風險評估。[13]

此外，日本金融廳（Japan's Financial Services Authority, JFSA）於 2023 年 6 月發布《*JFSA 多邊聯合研究：去中心化金融之信任鏈研究報告*》（Research Report of JFSA Multilateral Joint Research on the Chain of Trust of Decentralized Finance）。[14] 該研究針對具代表性的去中心化金融（DeFi）專案進行案例分析，研究基礎為假設當前主要的 DeFi 專案存在若干可信任節點及中心化要素，而這些要素可能成為監管之標的。研究結果指出：(i) 大多數去中心化金融專案都存在多種不同程度的信任節點及集中式特質；(ii) 必須針對個別去中心化金融專案進行深入分析，以辨識應受監管的對象，因為各專案對「去中心化自治組織（DAO）」[15] 或「治理代幣（Governance token）」的具體內容與定義有極大差異。

中國澳門

澳門已採取一系列行動評估虛擬資產及虛擬資產服務提供商的風險。由 15 個政府機構組成的跨部門「防制洗錢及打擊資恐工作小組」（AML/CFT Working Group）於 2020 年 7 月對虛擬資產及虛擬資產服務提供商進行了檢視。金融情報辦公室（Financial Intelligence Office，GIF）作為該工作小組的協調單位暨金融機構之監理單位，與澳門金融管理局（Monetary Authority of Macao，AMCM）共同合作，為工作小組成員設計並分析了一份關於虛擬資產與虛擬資產服務提供商的調查問卷。

該調查問卷從以下幾個面向評估風險：

- 澳門境內虛擬資產與虛擬資產服務提供商之相關業務概況（列出 18 種業務類型）；
- 現行法律框架下各主管機關對於虛擬資產與虛擬資產服務提供商的法律地位；
- 已辨識出的涉及虛擬資產與虛擬資產服務提供商的民事與刑事案件；以及
- 澳門境內涉及虛擬資產與虛擬資產服務提供商的業務的企業概況

整體而言，澳門的虛擬資產與虛擬資產服務提供商之風險評估結果屬於低風險。目前並未發現正在營運的交易平台，而涉及虛擬資產與虛擬資產服務提供商的刑事案件多數與詐欺及詐騙有關。大部分關於虛擬資產與虛擬資產服務提供商的可疑交易報告與個人投資相關；僅少數案例涉及疑似利用個人帳戶移轉資金至海外虛擬資產平台。在這些可疑交易報告中並未發現實際的虛擬資產交易。

儘管風險評估結果屬於低風險，澳門仍持續採取一系列措施以降低虛擬資產與虛擬資產服務提供商的風險，包括：

- 要求澳門境內所有銀行與支付服務機構不得直接、或間接參與或提供任何涉及虛擬資產的金融服務；
- 要求保險公司不得接受或使用虛擬資產作為保費或理賠款項支付方式，並應評估現行、或規劃中的業務與營運是否符合相關法規；
- 主管機關將辨識任何在澳門成立或營運的虛擬資產服務提供商，並採取必要的後續行動；
- 主管機關將持續對與新興科技相關之潛在風險保持警覺。

[13] https://www.npa.go.jp/sosikihanzai/jafic/en/nenzihokoku_e/nenzihokoku_e.htm
[14] https://www.fsa.go.jp/policy/bgin/ResearchPaper_qunie_en.pdf
[15] 去中心化自治組織（Decentralised autonomous organisation）

- 透過公私部門合作會議向銀行分享並警示與虛擬資產活動及虛擬資產服務商相關的風險。當局亦將定期與銀行分享由不同來源蒐集而來的虛擬資產服務商平台名單，以供銀行內部進行風險分析，並採取相應預防措施。
- 法律禁止在賭場內使用虛擬資產作為合法的支付方式。澳門博彩監察協調局（Gaming Inspection and Coordination Bureau, DICJ）已進行持續監控，防止賭場採用虛擬資產進行交易或與虛擬資產服務提供商從事業務往來。

泰國

泰國防制洗錢辦公室（AMLO）發布了 2022 年國家風險評估（NRA），涵蓋虛擬資產與虛擬資產服務提供商。[16] 此外，防制洗錢辦公室亦針對各虛擬資產服務提供商進行個別的風險評估。該報告屬機密文件，不對外公開。

菲律賓

菲律賓中央銀行（Bangko Sentral ng Pilipinas, BSP）於 2021 年 3 月發布的第三次銀行及其他受 BSP 監理金融機構（*Banks and other BSP-Supervised Financial Institutions, BSFIs*）的部門風險評估中，亦納入針對虛擬資產服務提供商的風險評估。

該部門風險評估指出，虛擬資產服務提供商整體的弱點（Vulnerability）被評估為中等。原因是虛擬資產本身具備一些特性，例如跨境交易、快速結算能力、潛在的高匿名性等，虛擬資產（VA）本身具有固有的弱點，容易被用於洗錢、資恐及資武擴。此外，虛擬資產服務提供商一般的防制洗錢及打擊資恐控制措施品質亦被評為中等。菲律賓虛擬資產服務提供商的防制洗錢及打擊資恐法律、監管及制度框架基本已就緒，且整體符合國際防制洗錢及打擊資恐的標準。

除了進行上述部門風險評估之外，菲律賓中央銀行亦透過各項監理活動，進一步強化對此領域風險的理解。這些活動包括進行檢查與專題審查，以評估風險水準及風險管理架構的品質，同時透過監測活動來辨識並追蹤相關趨勢與態樣。

1.6 APG 會員國落實 FATF 虛擬資產要求的狀況

截至 2023 年 10 月，共有 6 個同時為 FATF 及 APG 成員的國家，以及 14 個僅為 APG 成員的國家，透過相互評鑑或追蹤報告（Mutual evaluation or follow-up report）接受針對建議第 15 項（Recommendation 15）修訂要求的評估；其中來自太平洋次區域的國家僅有 1 個。

此 6 個同時為 FATF 及 APG 成員的國家中，全部皆獲得「大部分遵循」（Largely Compliant）的評等（即達到通過標準）。然而，在 14 個僅為 APG 成員的國家中，僅有 2 個國家（蒙古及泰國）獲得「大部分遵循」，4 個國家評為「未遵循」（Non-Compliant），5 個國家評為「部分遵循」（Partially Compliant）。此意味接受評估的、僅屬 APG 會員的國家中，有 86% 的國家尚未建立監管虛擬資產及虛擬資產服務提供商的適當基本框架。

[16] https://www.amlo.go.th/amlo-intranet/media/k2/attachments/NRAYThailandYforYPublicationYEnglish_6112.pd

此等僅屬 APG 成員的國家中，未能符合建議第 15 項要求的常見缺失包括：

- 選擇禁止框架（prohibition framework），但未具備有效的法律禁止措施。
- 對虛擬資產的涵蓋範圍存有缺口，未充分符合 FATF 定義中的五大要素。
- 缺乏風險評估。
- 未對虛擬資產服務提供商進行有效監理。
- 未能辨識非法運作的情形，亦未施以制裁。
- 有關虛擬資產或虛擬資產服務提供商之國際合作的能力有限。

對多數 APG 成員國而言，進行虛擬資產及虛擬資產服務提供商的風險評估，以及建立管理與監督虛擬資產服務提供商的法律與制度框架，依舊是個重大挑戰。

APG 捐助及技術提供工作組（DAP Group）正致力於強化對 APG 會員國在此優先議題上的支持。在 2022 及 2023 年的 APG 技術援助論壇（Technical Assistance Forums）中，協助落實虛擬資產相關要求的技術援助，是受援助國家最普遍的要求。

選擇禁止框架但未具備有效的法律禁止措施

儘管許多 APG 成員國表示偏好對虛擬資產服務提供商採取禁止措施，但要有效建立、並落實相關的禁止框架仍具相當挑戰性。在僅屬 APG 成員國中，選擇對虛擬資產及虛擬資產服務提供商進行禁止措施的，沒有任何一個國家在 R.15 評估中取得「大部分遵循」（即「通過標準」）的評級。事實上，截至 2023 年 10 月，全球僅有一個採取禁止框架的國家取得 R.15「大部分遵循」的評級。[17]

根據 FATF 於 2023 年 6 月發表的虛擬資產及虛擬資產服務提供商標準執行專項更新報告（FATF 2023 Targeted Update），調查顯示全球選擇對虛擬資產服務提供商採取禁止框架的司法管轄區比例約為 11%。[18] 在依據已修訂標準接受評估的 APG 成員國中，有 7 個國家選擇禁止框架，3 個國家選擇監理框架（regulation regime），另有 1 個國家尚未決定框架。此相當於 64% 的 APG 司法管轄區選擇對虛擬資產服務提供商採取禁止措施，比例遠高於全球平均。

實施禁止框架方面的主要缺失之一，是司法管轄區選擇該框架時，未具備可執行的基礎法律禁止措施。例如，有些司法管轄區僅對大眾發布建議（advice），勸告民眾不要進行加密貨幣交易、或建議指出加密貨幣不被當地承認，但這些建議並無法律基礎。

另一個與禁止框架有關的常見缺失，是誤認為選擇禁止虛擬資產/虛擬資產服務提供商後，即可完全免除該司法管轄區在 R.15 項下的所有義務。

事實上，選擇禁止框架的司法管轄區仍須：

(i) 持續對虛擬資產及虛擬資產服務提供商構成的風險進行評估，並採用風險導向方法，確保防制或降低洗錢／資恐風險的措施，與辨識出的風險程度相稱；
(ii) 採取行動辨識從事虛擬資產服務提供商業務的自然人或法人，以及
(iii) 採取適當制裁措施，並儘可能提供最廣泛的國際合作範圍

[17] FATF（2020），反洗錢與打擊資恐措施——中華人民共和國*第一次強化追蹤報告與技術遵循度重新評級*，FATF，法國巴黎 http://www.fatf- gafi.org/publications/mutualevaluations/documents/fur-china-2020.htm
[18] 2023 年 FATF 專項更新報告

與虛擬資產相關之洗錢、資恐及其前置犯罪的合作。

加密資產有效政策要素：國際貨幣基金組織（IMF）

國際貨幣基金組織近日發布《加密資產之有效政策要素》（Paper on Elements of Effective Policies for Crypto Assets）文件，旨在回應會員國對如何因應加密資產的興起、及其相關風險所提出的問題。該文件對虛擬資產禁止措施提出以下觀察要點：

- 將所有虛擬資產活動視為非法的全面禁止框架，可能會抑制創新，並促使非法活動轉入地下。
- 由於虛擬資產本質上具無國界性，禁止措施的執行成本可能極高；且會增加規避的誘因，導致潛在的金融健全性（financial integrity）風險升高而效率降低。
- 若合法市場中缺乏可替代資產，使用者可能更傾向轉向非法市場，且因獲取此類資產的動機增強，甚至願意支付更高的價格。
- 未受禁止措施規範的虛擬資產可能產生額外的負面外部效應（例如更多虛擬資產活動可能與暗網有所關聯），
- 為管理特定風險，採取針對性限制措施可能具有正當性。
- 限制、或禁止措施不應取代健全的總體經濟政策及可信賴的制度框架，後者才是防範虛擬資產帶來的總體經濟與金融風險的第一道防線。

www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092

1.7 紅旗指標

根據 2017 年至 2020 年間各司法管轄區提供逾百餘案例研究， FATF 於 2020 年 9 月發布《*虛擬資產洗錢及資恐紅旗指標*》報告（*Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*）[19]。該報告旨在協助虛擬資產服務提供商、金融機構（FI）及指定之非金融事業或專業人員辨識、並通報涉及虛擬資產的潛在洗錢與資恐活動。報告中所列的紅旗指標包括交易類型、交易模式、匿名性、發送方或接收方、資金或財富來源，以及地域風險。

[19] FATF *2020 年《虛擬資產洗錢及資恐紅旗指標》*報告，前言 https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf，第六段。

與虛擬資產及虛擬資產服務提供商交易有關的重要紅旗指標包括：

- 不完整的「認識你的客戶」（KYC）資訊，包括客戶可能不願提供 KYC 資訊。
- 將虛擬資產交易拆分成小額、或略低於申報門檻之金額。
- 交易活動與客戶個人資料、或帳戶預期使用方式不符。
- 將虛擬資產轉移至另一司法管轄區的虛擬資產服務提供商，但雙方並不存在任何關係。
- 存入虛擬資產後立即進行提領、或轉換。
- 涉及多種虛擬資產的使用，但缺乏合理商業邏輯之交易。
- 進行虛擬資產與法定貨幣兌換，且交易可能導致虧損，缺乏合理商業邏輯。
- 交易目的似乎為隱匿資金流向，例如透過混幣（mixing）及攪幣（tumbling）服務。
- 使用與犯罪活動相關聯之IP位址。
- 大量看似無關的虛擬資產錢包使用相同的IP位址。
- 經常與防制洗錢控管較弱之司法管轄區的虛擬資產服務提供商進行交易。

來源：FATF《虛擬資產洗錢及資恐紅旗指標》報告，2020年

1.8 國際合作的重要性

FATF 標準的重要面向之一，是要求各司法管轄區具備國際合作的法律基礎，並提供適當的資訊、金融情報及證據，以協助對犯罪分子及其資產採取執法行動。至於虛擬資產方面，建議第 15 項要求各司法管轄區迅速提供最廣泛的國際合作，以應對與虛擬資產及虛擬資產服務提供商有關的洗錢、前置犯罪及資恐活動。特別是，無論其主管機關之性質或地位，亦無論對虛擬資產服務提供商名稱或地位是否存在差異，虛擬資產服務提供商的主管機關應具備與外國對等單位交換資訊的法律基礎。

區塊鏈本質上無國界，且虛擬資產價值轉移快速而便捷，各司法管轄區須透過國際合作，方能有效監管虛擬資產服務提供商，從而成功調查並起訴涉及虛擬資產之犯罪行為。聯合國北韓專家小組（依據聯合國安全理事會決議第 1874 號成立） 2023 年 3 月報告亦強調國際合作的重要性。針對透過虛擬資產及其他網路活動進行非法收入之產生，專家小組建議各司法管轄區「強化合作、促進對話，並提升資訊共享」。[20]

1.9 結語

本章所列資訊強調全球各司法管轄區必須落實建議第 15 項中所規定對虛擬資產及虛擬資產服務提供商之要求。隨著相關產業及犯罪活動持續演變， APG 各成員應確保其監管框架及執法能力仍足以應對日益增加的風險與挑戰。

[20] 聯合國北韓專家小組報告 2023 年 3 月，第 77 頁

2 洗錢與資恐案例研究

APG 成員國提供的案例研究，依據司法管轄區來源的字母順序排列。在每個案例研究的標題下方，均列出與前置犯罪、支付方法或其他相關背景之公認術語。這些術語亦在報告第 8 節索引中亦有提及。

2.1 澳洲

案例研究 #1 - 高價鑽石疑似為毒品犯罪所得

毒品相關犯罪；貴金屬及寶石交易

澳洲邊境執法局（ABF）收到業界通報，指出一顆價值 2,400 萬澳幣，重達 15 克拉的鑽石以「退貨」名義重新進口澳洲，令人起疑。

情報調查顯示，進口商（A某）擁有長期犯罪紀錄，並曾因違反 1985 年《毒品濫用與販運法》（Drug Misuse and Trafficking Act）第 24(1) 條「製造違禁毒品」罪名而認罪服刑。

進一步分析發現該鑽石於 12 個月前出口，即 A 某首次遭指控時。隨後對該鑽石進行實體檢驗，確認其價值，並扣押該批貨物。

該資訊後來轉交合作機構，執法機關取得扣押令後，該鑽石被扣押作為「犯罪所得」。調查確定，A 某利用毒品犯罪所得購買鑽石進行洗錢，並試圖以尋求專業估價作為掩護，將鑽石轉移至另一司法管轄區，規避沒收行動。

來源 - 澳洲

案例研究 #2 - 多筆現金領

稅務犯罪

2021 年 1 月，澳洲數個執法與政府機構接獲情報後，展開聯合行動。調查發現，車手透過銀行分行提領現金，並將款項交至現金交付點。該犯罪活動涉及營造業的數家公司，涉嫌逃漏稅。有 4 人因涉嫌處理疑似犯罪所得及／或犯罪工具之財產遭逮捕。共計扣押現金與資產價值達 400 萬澳幣。

來源 - 澳洲

案例研究 #3 - 國際洗錢集團 — 查扣行動

獨立洗錢犯罪；使用虛擬資產；購置房地產；濫用法人與法律協議；電匯；金融機構；專業協助者（professional facilitators）；跨國有組織犯罪集團；可疑交易通報；國際合作

2023 年，9 名嫌疑人因涉嫌涉及高達 100 億澳幣的洗錢組織（MLO）被捕。該調查起因於先前逮捕攜帶大量現金之嫌疑人，並對犯罪所得進行大規模追蹤。9 名嫌疑人涉嫌處理犯罪所得，利用國內外空殼公司洗錢，並提交偽造的銀行貸款申請。該洗錢組織涉及大量可疑的國際匯入款項，並涉嫌利用會計師及銀行職員等專業協助者（professional facilitators），向國內銀行申請貸款；並利用犯罪所得資金購置不動產，及支付房屋抵押貸款。

本案涉及澳洲國內重要合作，包括刑事資產沒收專案小組（CACT）、澳洲聯邦警察（AFP）洗錢專案小組AVARUS、澳洲交易報告與分析中心（AUSTRAC）、澳洲稅務局（ATO）、澳洲證券與投資委員會（ASIC）及澳洲內政部（Department of Home Affairs）。此外，澳洲聯邦警察亦透過國際警務網路與外國執法機構開展國際合作。

澳洲聯邦警察已查封價值超過 2 億澳幣的財產，包括價值 3,000 萬澳幣的加密貨幣、18 隻名牌手錶、17 個名牌手提包、至少 46 件奢侈珠寶、20 處不動產、66 個銀行帳戶及 5 輛豪華車輛。

有 9 名人士已被控違反 1995 年《刑法典》（*Criminal Code*）及 2006 年《防制錢與打擊資恐法》（*Anti-Money Laundering and Counter-Terrorism Financing Act*）之洗錢罪名。依據 2002 年*《犯罪所得法》*（聯邦）的沒收程序仍在進行中。

來源 - 澳洲

2.2 孟加拉

案例研究 #4 - 利用網際網路駭入銀行帳戶

盜竊；詐欺；使用網際網路

A 某涉嫌透過網際網路駭入受害者的銀行帳戶及行動金融服務帳戶，意圖竊取受害者帳戶內資金。A 某透過向受害者手機號碼傳送含有「一次性密碼」的訊息，以取得其帳戶憑證資訊，並控制受害者帳戶。A 某還使用與受害者銀行類似的偽造 IP 位址，濫用網路銀行服務。

進一步調查發現，A 某以「自由工作者」身分，未提供任何證明文件，開立多個銀行帳戶及行動金融服務（MFS）帳戶。這些帳戶的交易性質相似，均涉及小額的點對點轉帳（peer-to-peer transfer）。多名受害者於數家金融機構的帳戶共遭竊取 359 萬孟加拉塔卡（約 32,404 美元），相關資金隨後由 A 某的帳戶提領為現金。

金融情報中心（FIU）已就此案製作情報報告，並轉交相關執法機關（LEA）。目前該案件仍在調查中。

來源 - 孟加拉

案例研究 #5 - 利用電子商務平台盜取客戶資金

盜竊；詐欺；偽造；使用網際網路；濫用法人與法律協議

一家電子商務公司以提供「雙倍塔卡」與夏季優惠券活動吸引客戶，宣稱可提供電視、機車、冷凍櫃及手機等產品 50% 至 60% 的折扣，但未能交付客戶訂購的商品。相反地，公司所收資金轉入電子商務公司老闆的個人帳戶，用於購買固定資產。

電子商務公司、其關係企業的帳戶共計募集了 116.6679 億孟加拉塔卡（約 1.0531 億美元）。大量資金透過不同的關聯公司及有關個人帳戶被轉移。

金融情報中心（FIU）根據分析結果，向相關執法機關提交情資報告以進一步行動。目前此案仍在調查中。

來源 - 孟加拉

案例研究 #6 - 透過虛報進口軟體與購買線上遊戲幣進行洗錢

走私；詐欺；濫用法人與法律協議；遊戲產業

一家孟加拉公司（A 公司）涉嫌虛報向境外公司（B 公司）進口軟體，藉以非法轉移資金。經金融分析發現，相關資金已被轉入一家遊戲公司，用以購買線上遊戲幣。B 公司的實質受益人為孟加拉籍人士，在六個月內以出口軟體至孟加拉名義，收取約 59 萬美元。

進一步調查顯示，客戶將小額資金存入 A 公司的行動銀行帳戶，以購買線上遊戲幣。這些資金再透過該公司及其關聯者的其他多個帳戶層層轉移。這些公司總共擁有 23 個行動金融服務帳戶，透過 1,320 萬筆交易共存入 21,950 億孟加拉塔卡（約 1.9828 億美元），每筆交易平均存入金額為 167 孟加拉塔卡（約 1.50 美元）。

情資報告已轉交相關執法機關展開調查，目前此案仍在調查中。

來源 - 孟加拉

2.3 中國

案例研究 #7 - 網路詐騙所產生的洗錢犯罪所得

詐騙；利用網際網路；濫用法人身分

2023 年 2 月 12 日，L 省當地警方逮捕了包括 A 某在內的 11 名嫌疑人。自 2022 年 9 月起，A 某等人透過親友介紹，以「高利潤」為噱頭招募下線。他們利用這些從屬人員的身分註冊了超過 40 家空殼公司，並開設多個企業帳戶，為來自境外網路詐欺集團的犯罪所得進行洗錢。

調查發現，A 某及其犯罪同夥涉及國內外超過 3,000 起網路詐欺案件，涉案金額約 10 億人民幣（約 1.37 億美元）。

來源 - 中國

案例研究 #8 - 跨國追回貪污與賄賂所得的犯罪資產

貪污與賄賂；地下銀行；國際商業公司

A 某涉嫌貪污與受賄，並於 2014 年 5 月潛逃出國。2016 年 4 月，國際刑警組織（INTERPOL）發布紅色通緝令（Red Notice）。中國當局與外國執法機構合作，根據國內法律及國際公約，在海外司法管轄區扣押並凍結非法資產。該貪污及賄賂的犯罪所得透過地下匯兌服務、與提供房地產投資服務的國際商業公司，被轉移至境外司法管轄區。目前，該案件於海外司法管轄區的調查仍在進行中。

來源 - 中國

2.4 庫克群島

案例研究 #9 - 破獲國際大麻與洗錢集團

毒品相關犯罪；現金；結構化交易；可疑交易報告；國際合作

此為庫克群島警方（代號「Kotaa行動」）與金融情報中心（代號「Falcon行動」）根據社區與執法夥伴提供的情報，針對一個庫克群島境內運作的毒品集團，所展開的聯合毒品與金融調查。該聯合行動獲得紐西蘭警方、紐西蘭海關與紐西蘭跨國犯罪單位的協助。

情報顯示兩名主要人物（A 某及 B 某）與其同夥經營毒品集團，透過海運從 B 司法管轄區進口大麻至庫克群島。

大麻銷售所得由多名人士存入兩個獨立銀行帳戶，隨後使用庫克群島金融卡於 B 司法管轄區的 ATM 提領現金，估計轉移資金總額約達 40 萬紐西蘭元。

A 某為庫克群島居民，經營一家小型草坪修剪業務。B 某有庫克群島血統，但居住於 B 司法管轄區；擁有多家小型企業，並與一個有組織犯罪集團有關聯。B 某經常前往庫克群島，因此被當地執法機關透過社區蒐集之情資注意。社區成員曾觀察 B 某在當地酒吧出手闊綽，並金援贊助一支當地的橄欖球隊。

A 某與 B 某共同於庫克群島註冊了一間小型公司作為掩護，以合法化其犯罪行為。經調查發現，該公司自登記日起即無實際營運。A 某負責協調向庫克群島多名毒品交易商出售與分銷毒品，並將相關資金存入 B 某位於庫克群島的多個帳戶之中。B 某則透過 B 司法管轄區的自動櫃員機存取該等帳戶，並被確認為庫克群島大麻之主要供應者。

2019 年，一筆可疑活動通報指出 B 某帳戶存入大額現金。經金融調查發現，A 某協調一項「結構化」操作，涉及多名第三方人士存入現金，每筆存款金額介於 300 至 9,000 紐西蘭元間（均低於 10,000 紐西蘭元的通報門檻）。簡訊通訊內容亦顯示 A 某、B 某與多名毒品集團成員間有所聯繫；其中包括兩名有毒品犯罪前科的共犯。兩名共犯經確認為 A 某在庫克群島的主要毒品經銷者或毒品交易者。

本案涉及毒品與金融犯罪的聯合調查，B 司法管轄區當局聚焦位於該司法管轄區的 B 某展開調查，而庫克群島當局則集中調查 A 某。A 某於 2022 年 9 月遭起訴，並因共謀販售／分銷 C 級毒品（大麻）及藐視法庭罪名，被判處 7 年有期徒刑。法庭審理過程中曾提出洗錢相關證據，但檢方並未就洗錢罪名起訴。兩名共犯出庭作證指控 A 某，分別遭判處 4 年徒刑。

來源 – 庫克群島

案例研究 #10 - 再生能源投資詐騙案

詐欺；使用網際網路；可疑交易報告；濫用法人與法律協議；國際合作

一個釣魚網站鎖定外國 A 司法管轄區的投資者，謊稱庫克群島政府推出再生能源投資計畫。

A 銀行（通報機構）提出可疑活動報告。原因是海外 B 銀行要求 A 銀行凍結一筆從 B 銀行客戶向 A 銀行帳戶匯入之 10 萬紐西蘭元交易。該交易用途為投資於虛假的再生能源計畫，並偽稱由 B 銀行所提供。A 銀行依據 B 銀行的要求凍結該筆交易。

目前尚待確認 A 銀行帳戶是否屬於此投資詐騙案的主謀。A 銀行帳戶之所有人為一家國際信託公司；該公司提供數位自動化服務及顧問服務，業務範圍遍及多個司法管轄區的企業。此公司帳戶的創辦人/最終受益人為兩名男性個人。

B 銀行迅速採取行動，通知相關的網際網路服務供應商停止提供該詐騙投資網站的服務，並同時通報金融監理機關與網路安全主管機關。B 銀行亦確保其自身網站已發布警示。此外，庫克群島政府也發布媒體聲明，提醒公眾注意此詐騙事件。4 名曾表達對該投資計畫有興趣的潛在投資者，之後皆被告知該計畫屬於詐欺。

隨後，投資詐騙主謀改變策略，濫用 A 銀行名義，虛假宣稱推廣其投資詐騙計畫。A 銀行對帳戶所有人進行風險評估後，終止雙方業務關係。

在執法機關與 B 銀行的協助下，確認了第三名可能涉及該投資詐騙案的個人，但目前尚未建立該人與前述兩名男性、或該詐騙案本身之明確關聯。目前並未發生或通報其他相關事件，亦未採取進一步行動。

來源 – 庫克群島

2.5 中國香港

案例研究 #11 - 跨國洗錢集團利用無證照匯款業者及其家族成員洗錢

有組織犯罪；洗錢；跨國有組織犯罪集團；地下匯兌

香港警方收到來自 X 司法管轄區的情報，指出跨國有組織犯罪集團（其成員已在 X 司法管轄區被捕）透過非法管道洗錢所得的 3,200 萬港幣犯罪資金，轉入 A 某在中國香港的銀行帳戶。調查發現，A 某透過未經主管機關許可貨幣服務業者收受此等非法資金，隨後再將資金轉入其妻子、女兒及其他同夥銀行帳戶中。A 某的妻子及一名同夥已於 2022 年因洗錢罪被捕，當局並扣押總計 1,300 萬港幣資金。目前此案件的調查仍在持續進行中。目前此案仍在調查中。

來源 – 中國香港

案例研究 #12 - 利用儲值帳戶洗錢性剝削之犯罪所得；

性剝削；新型支付工具；第三方洗錢

2022 年，香港當局對本地一個安排女性提供非法性交易服務的犯罪集團進行調查後發現，該集團以現金收取嫖客支付的服務費用後，將總額約 35,000 美元的現金資金存入由集團旗下人頭持有的儲值帳戶內，之後再轉入犯罪集團控制之帳戶。2022 年年底，執法機關逮捕該集團兩名成員，指控其涉及性交易犯罪。目前此案仍在調查中。

來源 – 中國香港

案例研究 #13 - 利用虛擬銀行帳戶藉由洗錢方式處理非法賭博所得

賭博；使用網際網路；第三方洗錢；可疑交易報告

根據香港聯合財富情報組（JFIU）分析，發現 11 個虛擬銀行帳戶涉嫌用於接收、並藉由洗錢方式處理約 3,800 萬港幣非法網路博弈活動所得資金。隨後該等非法資金被轉入由賭博犯罪集團控制的多個銀行帳戶中。 2022 年，執法機關突擊檢查犯罪集團之營運中心，逮捕包括主謀在內的 5 人，指控其涉犯賭博及洗錢罪行。目前案件仍在調查中。

來源 – 中國香港

案例研究 #14 - 利用期貨公司洗錢

詐欺；使用資本市場；購置高價或文化資產；第三方洗錢；可疑交易報告

香港聯合財富情報組透過主動分析加上涉及誘騙受害者投資的電話詐騙案件，發現一個犯罪集團於 2020 年至 2021 年間涉嫌以錢方式處理 3.45 億港幣（約 4,400 萬美元）的犯罪所得。該集團控制本地一家合法期貨公司（A 公司）進行資金洗錢，手法是透過招募 10 名洗錢人頭，在銀行及 A 期貨公司開立銀行帳戶與證券帳戶。非法資金存入人頭銀行帳戶後，資金再轉入人頭在 A 公司的證券帳戶中、A 之後於期貨市場頻繁且大量交易，導致投資完全虧損，但卻支付高額交易手續費給 A 公司。2022 年，香港警方逮捕其中 7 名洗錢人頭，並在集團主謀居所查獲現金 330 萬港幣及價值約 80 萬港幣（約 10.2 萬美元）之名貴手錶。另扣押犯罪集團使用之 26 個帳戶，總計 1,700 萬港幣（約 220 萬美元）。目前此案仍在調查中。

來源 – 中國香港

案例研究 #15 - 利用賭場帳戶以洗錢方式處理倫敦金（Loco-London'gold）詐騙犯罪所得

詐欺；賭場；資金移轉服務

2016 年 5 月至 2018 年 7 月間，一個詐欺集團透過兩家虛假的倫敦金交易公司進行投資詐騙，誘騙全球受害者，詐騙所得達 6.28 億港幣（約 8,000 萬美元）。收到受害人款項後，該等詐騙所得資金被轉至香港及 B 司法管轄區的多個帳戶。一家經許可資金匯款服務公司的經營者亦涉案，將其中 1.92 億港幣資金轉移至 C 司法管轄區的賭場帳戶內。該倫敦金詐騙案經通報執法機關後，包括資金匯款公司經營者在內共 4 名涉案人員已被捕。 2023 年，上述四人均被檢方依共謀詐欺及洗錢罪名起訴。自犯罪集團持有之數個銀行帳戶內扣押共計 1.6 億港幣（約 2,040 萬美元），另成功防止 13 萬港幣資金遭移轉。本案調查結果乃透過B司法管轄區協助追查犯罪所得而達成。目前此案仍在調查中。

來源 – 中國香港

案例研究 #16 - 新冠（COVID-19）政府貸款詐欺案

詐欺；金融機構；新冠（COVID-19）；第三方洗錢

為紓解中小企業在新冠（COVID-19）疫情期間之財務壓力，中國香港政府推出「百分百特惠貸款保證計畫（Special 100% Loan Guarantee Scheme，PLGS）」，符合資格的企業可借款最高港幣 600 萬元。2022 年，香港警方瓦解兩個詐欺犯罪集團，該集團透過招募洗錢人頭，以虛假的僱傭資料與帳戶文件申請貸款共 2.95 億港幣。貸款核准後，資金隨即存入人頭之銀行帳戶，再迅速轉入犯罪集團主謀控制之帳戶內。兩個犯罪集團共計 38 人遭逮捕，並被控詐欺共謀罪。警方已扣押約 700 萬港幣犯罪所得。目前此案仍在調查中。

來源 – 中國香港

案例研究 #17 - 加密貨幣侵佔案

竊盜；虛擬資產使用；購置不動產；購置高價或文化資產

A 某為金融科技公司財務主管，負責管理公司之加密貨幣帳戶。A 某利用職務之便，將公司約 330 萬美元（約 2,560 萬港幣或元 330 萬美元）之虛擬資產，轉入其本人及親屬之個人加密貨幣錢包。被竊取之加密貨幣隨後在不同加密貨幣間進行多次兌換，並在 A 某與其同夥之間頻繁轉移。

最終，約價值 1,800 萬港幣之加密貨幣被轉換為法定貨幣並存入 A 某之個人銀行帳戶，其餘加密貨幣則轉入另一個加密錢包。A 某及其同夥隨後購買 2 處住宅物業及 1 輛全新車輛。2022 年中，金融科技公司內部稽核發現 A 某之侵佔行為。A 某及其兩名共犯遭香港警方逮捕，並以竊盜罪名被起訴。A 某銀行帳戶內 200 萬港幣，及價值 600 萬港幣之虛擬資產被扣押。目前案件調查仍持續進行中。

來源：中國香港

案例研究 #18 - 以加密貨幣交易掩飾洗錢活動

詐欺；使用虛擬資產；第三方洗錢

香港警方調查發現，一個詐欺犯罪集團利用 136 個自身、或人頭名下的銀行帳戶，以洗錢方式處理多種詐欺犯罪所得、共達 2,700 萬港幣犯罪資金。此等不法資金在帳戶內混合、或進行加密貨幣交易，最終透過自動櫃員機提領為現金。2022 年中，警方逮捕包括主謀在內共 16 名涉案人員，並凍結 550 萬港幣以防止其遭移轉。目前案件調查仍持續進行中。

來源：中國香港

2.6 印尼

案例研究 #19 - 偽裝為捐款及合法商業收入之資恐活動

資助恐怖主義；金融機構；濫用法人；非法武器販運

1998 年至 2006 年間，A 某參與 Negara Islam 組織活動。2005 年，經一名宗教教師介紹，A 某接觸伊斯蘭祈禱團（Jamaah Islamiyah, JI）。2007 年，A 某在該教師邀請下於 Rangkasbitung 宣誓效忠，並正式加入伊斯蘭祈禱團。

隨後被任命為該組織基層結構 Ribabah（僅兩名成員）的領袖（amir）。A 某原為創業家，在 Pandeglang 擁有汽車修理廠，並於其他城市設有數個分店，因此被任命為伊斯蘭祈禱團經濟與商業部門（Tajhiz部門下之 Iqtishod 次部門）成員。

A 某任職期間，與其他 JI 成員（由 B 某，即 B 公司之負責人領導）策劃恐怖主義攻擊，攻擊對象為萬丹省（Banten）華人。該等人員並計劃透過恐怖活動（amaliyah）推翻印尼政府，實施伊斯蘭教法。

A 某及其他 JI 成員計劃資助購買槍枝以執行攻擊。A 某分六次支付共計 7,600 萬印尼盾（約 4,860 美元）。其中四次透過銀行匯款，每次 500 萬印尼盾（約 319 美元），另兩次則以現金支付，分別為 600 萬印尼盾（約 383 美元）與 5,000 萬印尼盾（約 3,197 美元）。這些資金以捐贈名義與 B 公司之商業收入混合，共計 2.86 億印尼盾（約 18,291 美元）。

B 公司員工 C 某（B 公司負責人之弟）收集資金後，C 某將資金交付給 JI 東爪哇地區成員 D 某，用於購置非法槍械。D 某購得 1 把左輪手槍、2 把經改造之軟彈槍左輪手槍、2 把 FN 手槍（附彈匣）、1 把 SS1 步槍（附 2 個彈匣）、3 盒 9 毫米口徑子彈、2 盒 22 口徑子彈，以及數百發 5.56 毫米口徑 SS1 步槍子彈，後遭到逮捕。

2021 年，A 某被判處有期徒刑 4 年，併科罰金 5 千萬印尼盾（約 3,197 美元），相關槍枝彈藥等證物均已依法沒收。

來源 - 印尼

案例研究 #20 - 利用慈善募捐箱的資恐活動

資助恐怖主義；濫用非營利組織；現金

A 某與其他兩人共同成立 X 基金會，以支持伊斯蘭祈禱團（JI）在西蘇門答臘地區的活動。A 某擔任 X 基金會創辦人兼顧問，全面負責該基金會之營運。

為了舉辦活動，X 基金會之集資來源包括

- 將 40 個募捐箱/撲滿分發至捐贈者家中。
- 在 Payakumbuh 城市區域放置 25 個玻璃慈善募捐箱。
- 專門帳戶以資助其「活動計畫」。

X 基金會舉辦的活動包括：
2017 年：「齋戒月人道關懷活動」（與合法非營利組織 Z 基金會合作），該活動募得捐款共 2.6 億印尼盾（約 16,628 美元），資金已轉入 Z 基金會之銀行帳戶。

2018 年:「羅興亞關懷健行活動」（募得捐款共 2,000 萬印尼盾，約 1,279 美元）。所募資金隨後轉入 Z 基金會。

X 基金會同意支持 Z 基金會，但前提是由 A 某以志工身分前往外國 司法管轄區交付募得資金。

A 某明知且蓄意將資金交付予已被指認定為恐怖組織之伊斯蘭祈禱團。2022 年 6 月 8 日，A 某遭東雅加達法院判處有期徒刑 6 年，並罰款 5,000 萬印尼盾（約 3,197 美元）

來源 - 印尼

案例研究 #21 - 合法慈善基金會遭濫用進行資助恐怖主義

資助恐怖主義；濫用非營利組織；新型支付工具

A 某於 2006 年加入伊斯蘭祈禱團（JI），並活躍於北蘇門答臘地區。2014 年底，A 某成為印尼政府認可之合法慈善機構「X 慈善基金會」主席。

A 某就任後推行數項計畫，包括「每日一千盾施捨運動」（Gerakan Sedekah Seribu Sehari）、天課（Zakat），以及包含提供給貧困人士之食物及慈善募款箱的社會捐贈活動。直至 2020 年，共發放 1,800 個慈善募款箱。2014 年至 2020 年間，X 慈善基金會募得資金共總計 12 億印尼盾（約 77,297 美元）。2016 年，A 某開始接觸數位募款方式。

X 慈善基金會所募集之資金，被用於對外活動，包括宣教（da'wah）、教育、社會捐贈、全球伊斯蘭團結活動、促進社會經濟發展、災難應變；以及對內活動，例如向遭逮捕之伊斯蘭祈禱團（JI）成員及其家屬提供法律／訴訟協助等。X 慈善基金會亦會向伊斯蘭祈禱團直接轉帳匯款。

每年，X 慈善基金會竄改資料，向國家天課與慈善捐贈局（Baznas）以及宗教事務部提交虛假報告，以掩飾其為伊斯蘭祈禱團附屬組織之事實。

A 某擔任北蘇門答臘 X 慈善基金會主席期間，參與該基金會之全國會議大會以及董事會，討論各地區執行之計畫報告、未來區域執行計畫，與未來宣導計畫。同時，A 某亦接受伊斯蘭祈禱團指示，包括如何從 X 慈善基金會地區分會轉移資金給予伊斯蘭祈禱團。

2021 年 12 月，A 某經法院審理後，以恐怖主義及資助恐怖主義罪，判處有期徒刑 5 年，及併科罰金 1 億印尼盾（約 6,395 美元）。

來源 - 印尼

案例研究 #22 - 跨司法管轄區非營利組織遭濫用以資助恐怖主義

資助恐怖主義；濫用非營利組織

2020 年 4 月至 5 月間，印尼金融交易報告和分析中心（PPATK）與其他國外金融情報中心（FIU B）進行資訊交換，共同分析多個非營利組織（NPO）透過募集與分配捐款進行疑似資助恐怖主義之情形行為。這些非營利組織有全球性業務活動，並分別位於印尼及 B 金融情報中心（B 司法管轄區）。其中一個非營利組織為之一即為已註冊於 B 司法管轄區之 B 慈善基金會。於 2019 年 5 月 6 日至 2021 年 7 月 23 日期間，B 慈善基金會經查曾國際電匯總金額約 375,915 澳幣（約 240,873 美元）至其他相關司法管轄區。

印尼境內有三人被查接收來自 B 慈善基金會之資金，分別為 A 某（合計 133,213,091 印尼盾）、B 某（合計 71,665,605 印尼盾）與 C 某（合計 76,743,325 印尼盾）。此外，B 慈善基金會，一名管理人 D 某，亦透過電匯向 C 司法管轄區內執法機關關注之特定人士匯出資金。

2020 年 5 月，另查出 D 某將 13,710,540 印尼盾資金轉帳予另一名人士。

2021 年 7月 27 日，印尼金融交易報告與分析中心（PPATK）與印尼國家警察反恐特遣隊（Densus 88 AT）協調，確認 A 某涉嫌資助印尼東部穆賈希丁組織（MUJAHIDIN INDONESIA TIMUR，與伊斯蘭國（ISIS）相關聯）之恐怖主義活動，且該資金疑似來自 B 司法管轄區內的非營利組織與個人（A 某即為接收 B 慈善基金會匯款之人士之一）。

此外，印尼金融交易報告與分析中心（PPATK）亦根據其與 B 金融情報中心（FIU B）共同分析的結果，提供相關情報資訊。2021 年 7 月 29 日，A 某因資助恐怖主義罪名遭到逮捕，地點為南蘇拉威西省望加錫。調查顯示，A 某係受 N 某指示，資助印尼東部穆賈希丁組織（Mujahidin Group）活動。2022 年 3 月，印尼檢察總署表示將對 A 某提起公訴。

PPATK 針對印尼境內接收來自 B 慈善基金會與 D 某之電匯資金的相關人士進行金融分析，並監控印尼境內相關人士之社群媒體活動，另發現多名其他可疑人員，分析結果皆提交給反恐特遣隊（Densus 88 AT）。

PPATK 亦與金融情報中心 B 及 C 司法管轄區之 C 金融情報中心共同展開三方金融分析合作（C司法管轄區在先前分析中已確定接收來自 B 慈善基金會與 N 某之資金）。三個金融情報中心亦共同向 D 司法管轄區之金融情報中心提出請求，以取得當地捐款人及可能涉及恐怖組織之相關資訊。

此外，PPATK 亦與印尼海關總署（DGCE）合作進行情報交換。2022 年 2 月 11 日，DGCE 提交旅客風險管理資料，確認 D 某曾兩度入境印尼。調查發現，D 某入境目的係與 A 某會面，並於印尼境內分配資金。因此，當局已對D某啟動入境旅客通報警示。

來源 - 印尼

案例研究 #23 - 透過貨幣兌換商取得美元，用以資助前往加入恐怖組織的旅程

資助恐怖主義；金融機構；貨幣兌換

A 某於 2019 年遭逮捕，其後經法院認定觸犯恐怖主義罪，判處有期徒刑六年。

A 某與數名同夥慣常地制定國際旅行計畫，企圖加入境外恐怖組織。行動前，他預先自銀行提領現金 5,000 萬印尼盾（約 3,197 美元），在亞齊省的兌換店兌換成美元。除此之外，A 某的銀行帳戶已收到 1 億印尼盾，兌換為 6,950 美元。

該美元資金及銀行轉帳款項係用於支付前往衝突地區之機票。部分銀行轉帳係透過 A 某同事之配偶帳戶辦理。

來源 - 印尼

案例研究 #24 - 以合法企業資金進行資助單一獨立恐怖主義

資助恐怖主義；現金

A 某擁有一家麵包工廠，其雖非伊斯蘭祈禱團（JI）成員，但與該恐怖組織某些資深成員熟識，並為 JI 關聯的伊斯蘭寄宿學校提供財務資助，包括提供米與 3.5 億印尼盾（約 22,384 美元）。印尼當局調查資金流向後發現，資金是透過中間人轉交學校，而該中間人是 JI 的財務主管。2021 年，A 某被法院以資助恐怖主義罪判處有期徒刑 4 年 6 個月，併科罰金 1 億印尼盾（約 6,395 美元）。

來源 - 印尼

案例研究 #25 - 利用第三方洗錢處理毒品犯罪所得

毒品相關犯罪；第三方洗錢

A 某代表印尼境內三處高風險毒品矯正機構（Narcotics Correctional Institution）之受刑人，擔任境外毒品網路資金接收者。A 某註冊成立 12 家公司，包括進出口、旅遊業、資訊科技與電子商務服務及貨幣兌換公司，藉此以洗錢方式處理毒品交易 所得；犯罪所得金額估計達 3,902 億印尼盾（約 2,500 萬美元）。

A 某被判處有期徒刑 6 年，併科刑事罰金 50 億印尼盾（約 319,780 美元）。依法沒收之資產包括 3 棟房屋、1 輛汽車及相關銀行帳戶。

來源 - 印尼

案例研究 #26 - 保險業自我洗錢

詐欺；市場操縱；獨立洗錢

A 某與另外六人共同控制保險 A 公司之投資業務。A 某於 2012 年至 2014 年期間擔任 A 公司之投資與財務總監。

2012 年至 2019 年間，A 某與其他人持有其他公司股份，透過市場操縱手法提高股價後，再透過其在 A 公司的職位將股份出售予 A 公司。

此類股票與投資工具之購買具有高度風險，因未執行實質基本面與技術面之分析，僅為符合購買股份之行政程序要求。

A 某將出售股份予 A 公司之犯罪所得用於購買土地及建物，意圖藉此掩飾資產之來源、出處、所在地、權利歸屬或實際所有人為其本人及家人之事實。

J 先生被判處有期徒刑 15 年，併科刑事罰金 7.5 億印尼盾（約 48,000 美元）。法院亦命令 J 先生向國庫支付 314,868,567,350 印尼盾（約 2,000 萬美元），此金額係其非法活動所得利益。此外，法院亦依法沒收其資產，包括 1 輛汽車及 7 間公寓。

來源 - 印尼

案例研究 #27 - 利用法人進行獨立洗錢

獨立洗錢；濫用法人

2017 年中，B 某聯繫 A 某（被告），要求其為 X 公司開設公司帳戶。隨後，A 某聯繫 C 某與 D 某，以準備接收來自海外資金之帳戶。

2018 年 1 月 5 日，Y 公司帳戶收到來自海外資金匯入，共計 43,953,170,300 印尼盾（約 4,938 美元）。被告積極參與將 Y 公司帳戶內的資金拆分後轉移至 X 公司帳戶，並假藉購置土地名義，掩飾該資金來自 B 某之事實。

法院判處 A 某有期徒刑 3 年，並科處罰金 10 億印尼盾（約 66,938 美元）。

依法沒收之資產包括：

- 款項 20,009,571,418 印尼盾（約 130 萬美元）
- 款項存於 M 銀行、Y 公司名下帳戶內的 19,896,963,138 印尼盾（約 130 萬美元）
- 款項 100,444,759 印尼盾（約 6,720 美元）及現金 61,410,913 印尼盾（約 4,150 美元）。

來源 - 印尼

案例研究 #28 - 以非法網路賭博所得購置不動產與財物

賭博活動；購置不動產及財物

線上及線下賭博在印尼皆屬違法行為。2021 年 3 月，警方於蘇門答臘占碑逮捕 13 人，該處所涉嫌用於非法網路博弈。

調查顯示，A 某為非法彩券博弈業務之所有人與經營者。A 某經由銀行帳戶轉移非法博弈賭博活動所得，用於購置不動產與機車。

來源 - 印尼

2.7 日本

案例研究 #29 - 使用虛假姓名以洗錢方式處理網路販毒所得

毒品相關犯罪；使用網際網路；金融機構

A 某因非法販賣走私危險藥品並隱匿犯罪所得，涉嫌違反《確保藥品及醫療器材品質、效能與安全法》（*Act on securing Quality, Efficacy and Safety of Products including Pharmaceuticals and Medical Devices*）及《組織犯罪處罰法》（*Act on Punishment of Organised Crimes*）而被逮捕。

A 某透過從 B 司法管轄區進口原料，並與其他毒品前驅原料混合後，製成非法毒品於網路上銷售以牟利。A 某母親透過自動提款機進行 54 筆匯款交易，將網路販毒所得存入其銀行帳戶。 A 某母親並未涉及犯罪活動，對該資金為犯罪所得並不知情。存入其母親帳戶總金額達 15,709,000 日圓（約 104,000 美元）。此外，A 某亦以虛假姓名透過 15 筆交易將另外 8,755,000 日圓（約 58,000 美元）匯入其個人銀行帳戶。

來源 - 日本

案例研究 #30 - 有組織犯罪集團之毒品販運所得

有組織犯罪；毒品相關犯罪；金融機構

A 某為日本有組織犯罪集團成員，透過將毒品販運所得現金存入 3 個以第三者名義開立之銀行帳戶的方式，進行洗錢。2020 年 8 月至 2021 年 6 月期間，A 某在這些帳戶內共進行 56 筆現金交易，總金額達 278 萬日圓（約 18,000 美元）。

此案件依據違反《反毒品特別規定法》（Anti-Drug Special Provisions Law）之犯罪所得取得後掩飾事實罪，進行司法程序。

來源 - 日本

案例研究 #31 - 證券公司員工透過虛設帳戶欺詐客戶

竊盜；詐欺；使用網際網路；金融機構

A 某受僱於一家證券公司，負責開發並維護該公司之網路證券交易系統。2017 年 6 月至 2019 年 11 月間，A 某以公司客戶名義開設銀行帳戶，並自該等客戶證券帳戶轉出總額達 1.6 億日圓（約106 萬美元）至虛設帳戶中。A 某被起訴並被判決觸犯電腦詐欺罪及違反《組織犯罪處罰法》，處以有期徒刑 4 年 6 個月。

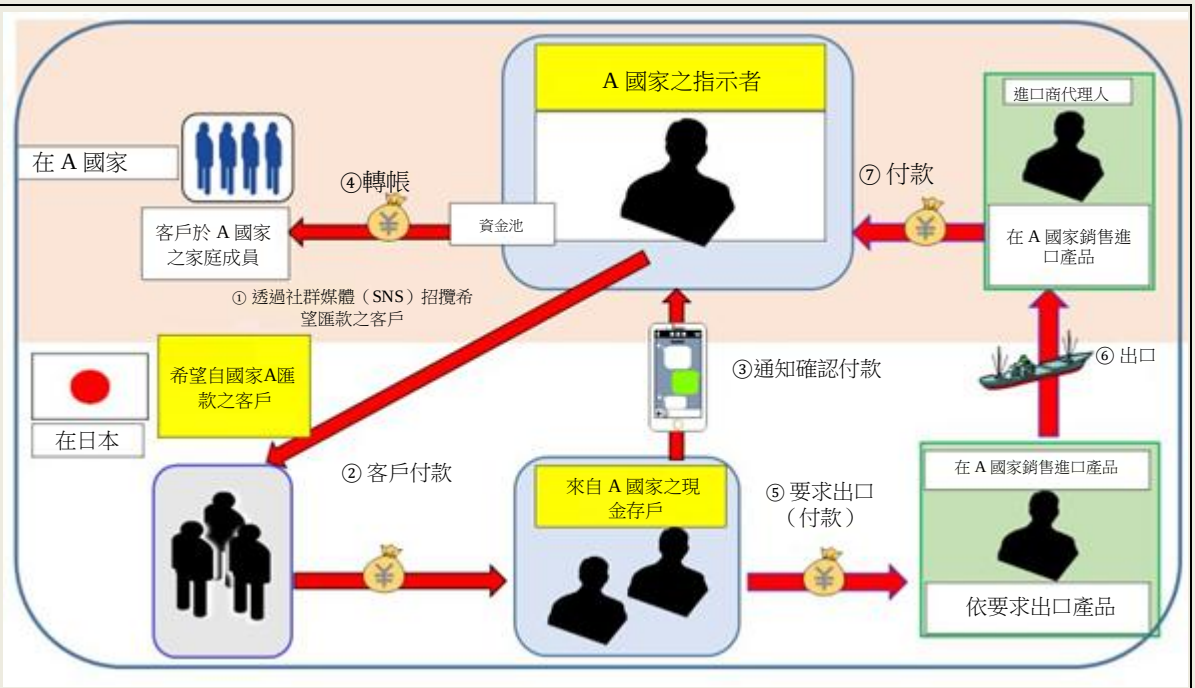
來源 - 日本

案例研究 #32 - 地下匯兌與進出口業務交集

地下匯兌

A 司法管轄區的指示者透過社群媒體（SNS）尋找欲從日本匯出資金的客戶，隨後指示日本境內的現金存款人決定交易匯率並指定銀行帳戶。收到指示後，現金存款人確認匯款人已付款，隨即要求出口代理商以合法貿易名義為掩護出口商品。透過此方式，日本境內的現金被兌換成 A 司法管轄區之貨幣，並存入 A 司法管轄區的銀行帳戶。此類交易的佣金相對較低，但嫌疑人可能從客戶支付的佣金中獲利。

來源 - 日本



案例研究 #33 - 透過交友網站鎖定投資人的加密貨幣詐欺案

詐欺；使用虛擬資產

A 某與其同夥開發出毫無價值的加密資產，作為募資投資虛構海外業務之代幣。該犯罪集團假冒女性投資人身分，透過交友網站誘騙受害人投資加密資產。受害人共計使用 42 枚比特幣（Bitcoin）及 140 萬枚瑞波幣（Ripple）購買此虛假加密資產。

隨後，該犯罪集團將透過詐欺取得之虛擬資產轉移至另外兩個虛擬錢包及一家加密貨幣經紀商，最終將虛擬貨幣轉換為現金。

來源 - 日本

案例研究 #34 - 透過轉移虛擬資產隱匿電腦詐欺之犯罪所得

詐欺；使用虛擬資產；第三方洗錢

B某從事電腦詐欺，並將比特幣轉移至受其控制之C某。 C 某再將比特幣轉移予 A 某，以換取現金共計 2.09 億日圓（約 140 萬美元）。2021 年 3 月，A某為隱匿犯罪所得，將 41.28 枚比特幣存放於以 D 某名義開設、但實際由 A 某掌控之虛擬錢包。

A 某隨後遭到逮捕並依違反《組織犯罪處罰法》「隱匿犯罪所得」罪名被起訴。

來源 - 日本

2.8 韓國

案例研究 #35 -「Omnis Gold」網際網路詐欺案

詐欺；電話詐欺；使用網際網路；使用虛擬資產

此為一宗詐欺案件，犯罪者向 141 名受害者詐騙約 359 億韓圜（約 2,646 萬美元）。該詐欺案涉及誘騙受害者透過智慧型手機應用程式儲值點數，購買「Omnis Gold」虛擬貨幣，並承諾 4% 的投資回報率。金融情報中心（FIU）亦提供金融交易報告，協助警方進行調查。檢察官與警方透過迅速且強制性的調查行動，確認犯罪者的犯罪事實並將其全部逮捕歸案。檢察官及相關主管機關查明犯罪者所獲得的經濟利益，法院亦於起訴前核准對犯罪者名下非犯罪相關之一般財產進行沒收保全措施，從而協助受害者追回資金。

來源 - 韓國

2.9 中國澳門

案例研究 #36 - 獨立洗錢方式處理外國 犯罪所得

獨立洗錢；金融機構；電匯

2021 年 12 月至 2022 年 3 月期間，澳門地區的 4 名人士收到來自 A 司法管轄區之 3 名人士共計 125 筆匯款，總額達 280 萬美元。這些資金匯入 4 人帳戶後，隨即被以現金提領。金融機構在進行客戶盡職調查（CDD）程序時，要求該 4 人提供現金用途說明，4 人表示是用於購買貨物，但無法提供充足的證明文件。同時，澳門金融情報中心收到境外當局提供情報，指 A 司法管轄區之 3 名人士曾利用其銀行帳戶接收詐騙所得資金。此 4 名澳門人士因涉嫌跨境轉移資金，以洗錢方式方式處理非法所得，金融情報中心將該可疑交易報告轉交澳門檢察院。

來源–中國澳門

案例研究 #37 - 九名當地男子和女子經營洗錢集團，使用金融卡購買黃金

跨國有組織犯罪集團；詐欺；貴金屬與寶石交易商；第三方洗錢；使用金融卡

2022 年 3 月，司法警察局（Judiciary Police）接獲金飾店負責人舉報，有數位海外顧客使用金融卡進行大量交易。由於交易款項涉嫌來自犯罪所得，相關金融機構暫停支付。

調查顯示，跨境犯罪集團利用海外銀行帳戶接收境外詐騙所得，隨後派遣持卡人前往中國澳門，以金融卡購買黃金。金融卡及購得之黃金隨後交由犯罪集團成員，經由多名集團成員進行多次洗錢交易，最終將該批黃金送至酒商變現。

某日，4 名境外持卡人前往兩家金飾店共計 5 次，使用 5 張不同的金融卡購買價值 74 萬美元的黃金。

其中約 37 萬美元為一宗涉及 55 名受害人的電信「刷單詐騙」之犯罪所得。

2022 年 10 月 19 日，9 名嫌犯於不同地點遭到逮捕。扣押物品包括黃金顆粒 1 顆，以及折合超過12.5 萬美元的各種貨幣現金；以及 4 輛汽車。部分涉案人士坦承受犯罪集團指示，以使用金融卡購買黃金之方式協助轉移、並洗錢犯罪所得；每次成功交易可獲約 430 美元報酬。本案仍在調查中。

來源–中國澳門

案例研究 #38 - 透過賭場、及貴金屬與寶石交易洗錢

有組織犯罪；賄賂；勒索；獨立洗錢；境外前置犯罪；賭場；現金；貴金屬與寶石交易；可疑交易報告；使用金融卡

2021 年，澳門檢察院針對金融情報中心通報的可疑活動展開調查。案件中，A 某於 X 司法管轄區組織黑幫犯罪集團，指使成員進行包括暴力行賄、控制與侵占國有資產、媒介性交易、勒索與恐嚇等犯罪行為。上述犯罪活動所得總額約達 2.9 億美元。A 某於 2020 年在 X 司法管轄區被判處無期徒刑。

調查發現，X 司法管轄區的犯罪所得被隱匿後帶往澳門，由 A 某在多家賭場以博弈方式進行洗錢。2012 年至 2017 年間，A 某多次赴澳門賭博，並使用信用卡與金融卡提領現金。此外，A 某將約 290 萬美元存入其賭博帳戶，並購買價值約 58.3 萬美元的金條。

2022 年，澳門檢察院以洗錢罪起訴 A 某。

來源–中國澳門

案例研究 #39 - 偵破跨境毒品販運及相關洗錢案件

獨立洗錢；使用金融卡；現金

2020 年 5 月，澳門司法警察局與 Y 司法管轄區警方共同執行反毒聯合行動，偵破一起跨境毒品販運案。隨後，Y 司法管轄區警方查獲 4 張屬於澳門人士的金融卡，據說，這些與金融卡連結的銀行帳戶中存有販毒所得。經調查，該等銀行帳戶屬於兩名澳門人士，這兩個帳戶於 2020 年 1 月至 2020 年 5 月期間用於洗錢，約 19.8 萬美元。涉案嫌疑人供稱曾於海外使用自動提款機提領犯罪所得現金。

2022 年 1 月，共 29 名嫌疑人接受調查，其中 9 人承認曾購買毒品並將毒資存入上述兩個銀行帳戶。進一步調查發現，帳戶持有人提供金融卡及密碼予他人使用，以掩飾犯罪所得資金。兩名嫌疑人被控加重洗錢罪，並移送相關檢察機關依法偵辦。

來源–中國澳門

案例研究 #40 - 利用電信網路詐欺之犯罪所得購買虛擬貨幣

跨國有組織犯罪集團；詐欺；第三方洗錢；使用虛擬資產；使用金融卡；境外前置犯罪；國際合作

2022 年 3 月底，澳門司法警察局接獲境外司法管轄區執法機關通知，有犯罪集團涉及跨境虛擬貨幣洗錢活動。經深入調查後發現，該集團將部分電信網路詐欺之犯罪所得用於購買虛擬貨幣，並透過當地一家電信商店進行洗錢。

根據調查，該犯罪集團自 2020 年 10 月開始運作，指示旗下成員於 A 司法管轄區開設約 180 個銀行帳戶，專門接收並處理當地及多個其他司法管轄區之電信詐欺非法所得，同時接收來源不明的大量存款。自 2021 年 7 月起，該集團指示若干成員前往澳門，使用 A 司法管轄區所發行的銀行卡於自動提款機提取現金，之後再透過一家電信商店購買虛擬貨幣，隨後於海外虛擬資產服務提供商之交易平台售出。販售虛擬資產所得的金錢，再以現金形式在中國澳門提領，達成洗錢目的。該犯罪集團於不同司法管轄區的銀行帳戶共處理可疑 資金約 1.41 億美元，其中 A 司法管轄區及中國澳門的集團成員共計提領現金約 4,600 萬美元。

澳門司法警察局與 A 司法管轄區執法機關展開聯合行動，澳門司警於旅館拘捕兩名來自 A 司法管轄區的嫌疑人，並分別於公寓與電信商店拘捕兩名澳門本地人、及其他來自 B 司法管轄區的嫌疑人。

司法警察調查發現，來自 A 司法管轄區的兩名嫌疑人自 2021 年 12 月起，在中國澳門透過自動提款機提領現金約 1,000 次，提領總額約 360 萬美元。此二名嫌疑人的銀行帳戶亦接收來自 12 宗詐騙案件的款項，共計 24.2 萬美元。

其等同時坦承使用自己與親友之銀行卡提錢，並協助 A 司法管轄區之犯罪分子透過海外虛擬資產平台進行虛擬貨幣交易。其中一名澳門本地嫌疑人及其他來自 B 司法管轄區的嫌疑人，皆為上述電信商店員工。

澳門司法警察以觸犯組織犯罪及洗錢罪名將前述嫌疑人移送檢察院依法偵辦，並持續追緝其他涉案人士。

來源：中國澳門

2.10 馬來西亞

案例研究 #41 - 交通罰單折扣詐欺集團

賄賂與貪污；可疑交易報告

馬來西亞金融情報中心接獲多家金融機構提交的可疑交易報告，涉及疑似收受並處理金額超過收入水平的執法人員。經分析，該些執法人員收取的款項介於 30 馬來西亞幣（約 7 美元）至 20,000 馬來西亞幣（約 4,270 美元）之間，付款方備註涉及罰單繳付與車輛牌照號碼。金融情報中心查明收款方為執法人員，且隨後均以現金方式提領該等款項。之後將涉案嫌疑人移送馬來西亞 反貪污委員會（MACC）調查。

馬來西亞反貪污委員會調查顯示，有兩個獨立的犯罪集團採用相似的犯罪手法，執法人員於是透過社群媒體尋找希望以低於罰單金額繳納交通罰款的個人。犯罪集團成員收到款項後，隨即

以現金方式提領，其中部分現金透過執法人員可操作的罰單支付系統，以折扣金額支付罰單，剩餘現金則由集團成員瓜分。

反貪污委員會的調查導致 60 個帳戶遭凍結，11 名涉嫌參與犯罪集團的嫌疑人遭拘捕，該集團自 2016 年以來涉及交易金額超過 500 萬馬來西亞幣（約 106 萬美元）。

來源 - 馬來西亞

2.11 蒙古

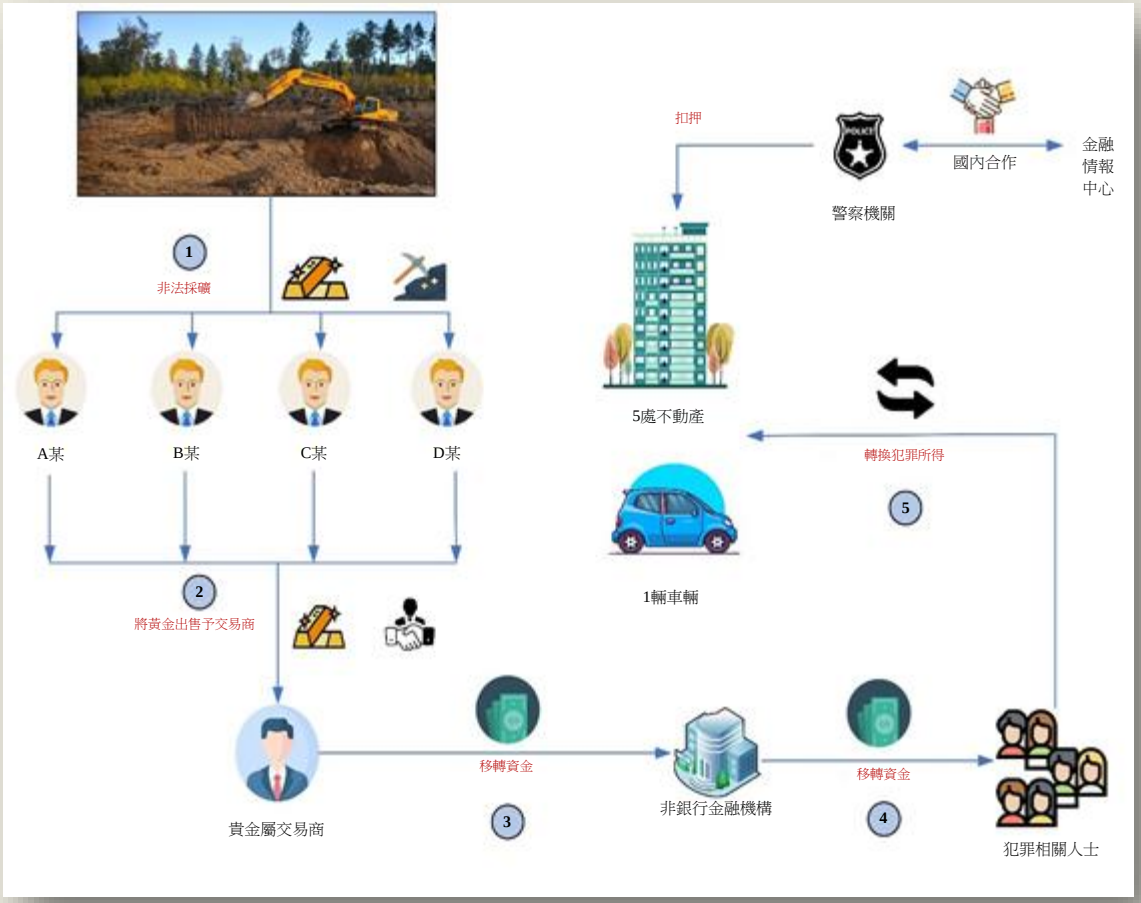
案例研究 #42 - 以洗錢方式處理非法採礦之犯罪所得

環境犯罪；使用不動產；貴金屬與寶石交易商

A、B、C 及 D 四名人士利用土地修復許可非法開採黃金，並將黃金出售給貴金屬交易商。犯罪者透過非銀行金融機構將資金匯入其同夥名下的銀行帳戶以隱匿犯罪所得，並購置大量不動產及車輛。蒙古金融情報中心應執法機關要求，提供犯罪者相關之金融情報資訊，對本案的偵破有重大貢獻。此外，執法機關亦沒收 5 間公寓及 1 輛車輛。整體而言，本案調查所沒收之犯罪所得總額達 6.57 億蒙古幣（MNT）（約 190,629 美元）。

本案於 2022 年 5 月展開調查，並於 2023 年 1 月進入司法程序。

來源 - 蒙古



案例研究 #43 - 透過賭博帳戶洗錢毒品販運犯罪所得

毒品相關犯罪；博弈活動；國際合作

A 某經營一個涉及毒品販運的犯罪組織。A 某透過國際郵件自兩個國家取得毒品，並寄送至其同夥之地址。A 某透過旗下毒品交易商銷售毒品，交易商將犯罪所得存入國際賭博帳戶，A 某再透過該帳戶提領資金。A 某利用該犯罪所得購買動產及不動產，包括汽車及房地產。

本案調查自 2022 年 5 月起持續進行。執法機關已扣押價值約 16 億蒙古幣（約 464,000 美元）的車輛與不動產。

蒙古毒品管制部門與國內外多個執法機構合作，包括海關、外國警方、國際刑警組織（INTERPOL）等。

來源 - 蒙古

案例研究 #44 - 社群媒體詐欺–遺產詐騙案

包含身分詐欺的詐欺行為；使用網際網路；現金；金融卡；國際合作

A 某為外國 B 司法管轄區之國民，透過臉書及 Instagram 等社群媒體，與蒙古國民建立關係。A 某捏造遺產詐騙情事，聲稱蒙古國民透過支付交易手續費即可繼承大筆美元遺產。受害人被指示將手續費轉入網銀資訊遭盜用之民眾帳戶 。A 某另要求其中一名受害人申辦一張國際金融卡，並透過國際郵件寄送給 A 某。隨後，A 某於 B 司法管轄區之自動提款機提領資金。

蒙古持續與經濟犯罪部門及詐欺調查部門合作，而本案亦自 2022 年 1 月起持續調查。透過艾格蒙聯盟（Egmont Group）與國際刑警組織（INTERPOL）的資訊交換對本案調查至關重要。本案涉案金額估計約為 1.58 億蒙古幣（約 45,843 美元）。

來源 - 蒙古

案例研究 #45 - 竊取個人物品並兌換現金

搶劫或竊盜；第三方洗錢；貨幣兌換

2022 年 8 月，A 某與 B 某闖入一間公寓，竊取 12 萬美元現金、1 個中型碧玉鼻煙壺、1 副馬鞍、1 塊金條、1 支腕錶、1 枚鑲鑽戒指及其他珠寶。A 某之妻子及岳母透過非銀行金融機構兌換部分美元，並購買 1 輛汽車。

調查期間已扣押 89,000 美元現金及 1 輛汽車。本案預定於 2023 年 3 月進行審判。

來源 - 蒙古

案例研究 #46 - 利用惡意程式自他人錢包轉移虛擬資產

使用網際網路；第三方洗錢；使用虛擬資產；洗錢

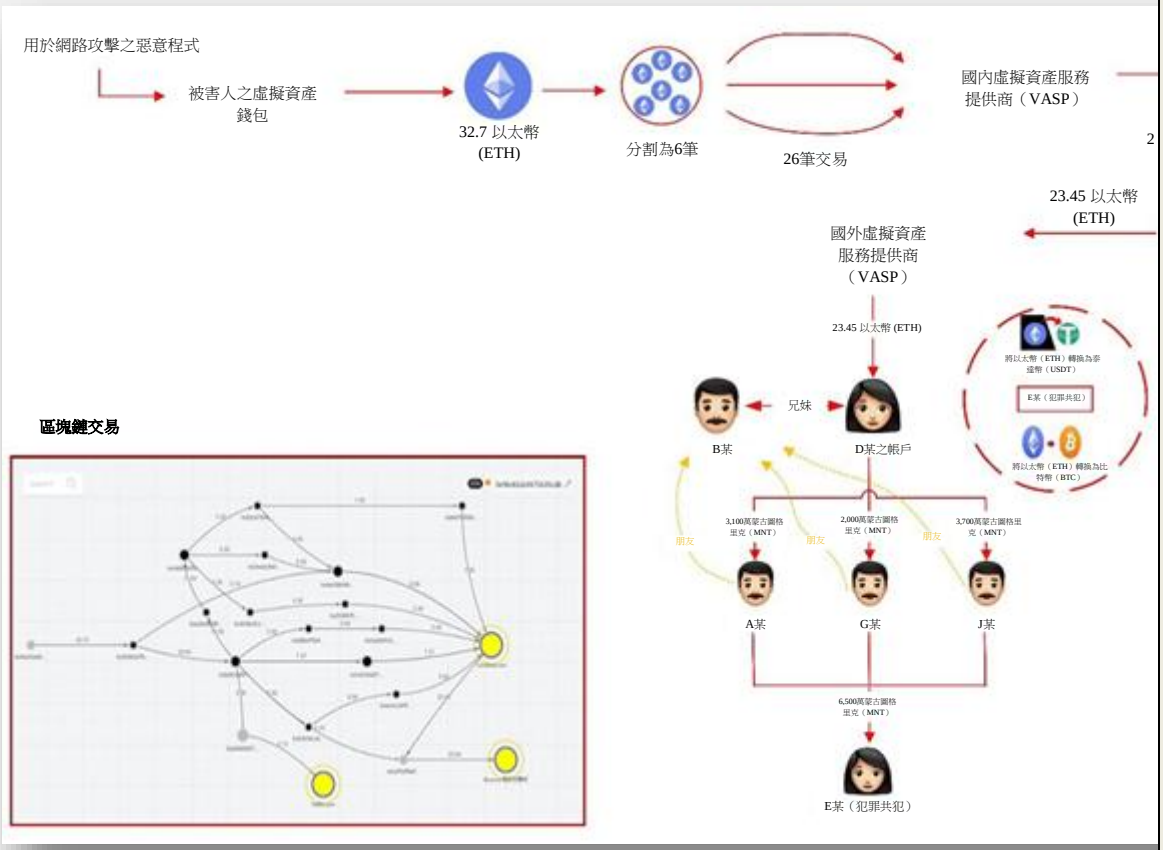
2021 年 7 月，B 某透過惡意程式入侵受害人的個人電腦，竊取其虛擬資產錢包內 32.7 枚以太幣（Ethereum）。該 32.7 枚以太幣隨後被分成 6 筆、共 26 次區塊鏈交易，移轉給一家國內虛擬資產服務提供商。其中 23.45 枚以太幣被再次轉入區塊鏈錢包，並轉移至 D 某於境外虛擬資產服務提供商的帳戶。

D 某為網路攻擊者 B 某之妹妹，B 某透過其妹之帳戶將盜取之以太幣轉換為比特幣及其他加密貨幣，以掩飾非法來源。隨後，B 某將虛擬貨幣轉移予其友人 M、友人 N 及友人 O。接著，將 6,500 萬蒙古幣轉移給共犯 E某。

調查期間，調查人員於 D 某在境外虛擬資產服務提供商帳戶內查獲剩餘的 0.5 枚比特幣，該比特幣為盜取以太幣轉換後之餘額，調查人員隨即凍結 D 某之帳戶。

B 某於法院審理階段已全額賠償損失。2022 年 10 月，B 某依據蒙古刑法中「非法入侵電子資訊」、「製作及販賣非法入侵電子資訊網路程式與設備」及「洗錢」罪名，被判處有期徒刑 2 年 6 個月。

2023 年 1 月，刑事上訴法院對 B 某維持原判。



來源 - 蒙古

2.12 紐西蘭

案例研究 #47 - 比特幣交易商協助詐欺案件

詐欺；使用虛擬資產

一名透過 localbitcoins.com 網站進行點對點（P2P）交易的比特幣交易商，協助境外國際詐欺集團將詐騙所得的法幣兌換成比特幣。境外詐欺集團以浪漫交友及「預付款詐騙」等欺騙手法，聯絡紐西蘭境內被害人並誘導其交付金錢。詐騙集團指示被害人與當地的「同夥」（即上述比特幣交易商）會面並交付現金，並告知被害人具體的會面時間與地點。

同時，詐騙集團亦聯繫比特幣交易商，聲稱希望以紐西蘭元購買比特幣，指示交易商在指定的時間與地點與其「同夥」（實際上即被害人）會面並收取現金。詐騙集團向交易商提供其比特幣錢包地址，要求交易商將等值於從被害人取得的現金之比特幣轉入該錢包。該比特幣交易商在進行上述交易時未履行任何客戶盡職調查（CDD）程序，即無條件接受被害人的現金，並將等值比特幣轉入詐欺集團提供之錢包地址。

來源 - 紐西蘭

2.13 巴基斯坦

案例研究 #48 - 以透過境外虛設公司/實體方式進行洗錢

貿易洗錢；地下匯兌；走私；稅務犯罪；可疑交易報告

巴基斯坦金融情報中心，金融監控單位，收到數家外幣兌換公司及 1 家銀行通報，有關在某省會城市營運之 A 公司負責人 A 某之多筆可疑交易報告。

A 公司向位於境外司法管轄區之 B 公司出口不同種類貨物，但 A 公司多次變更貨物出口分類代碼，引發銀行警示。此外，多家外幣兌換公司通報指出，A 某涉及購買價值約 200 萬美元的高額外幣。該通報銀行後續調查發現，所謂境外司法管轄區的 B 公司為不存在之虛設公司，並無實際出口貨物作為支付予巴基斯坦之款項依據。

A 公司將跨境交易所得美元款項共 78 萬美元，用於支付聲稱為出口貨物的 4 筆預付款項。該批美元是透過多家外幣兌換公司，以化整為零方式取得。此外，A 某透過不同銀行帳戶與無關交易相對人進行轉帳，共計轉移約 15 億巴基斯坦盧比。

A 某過去的稅務紀錄顯示僅在 2018 年支付了 36.5 萬巴基斯坦盧比（約 130 萬美元）的微薄稅款。A 某涉嫌從事貿易洗錢、逃漏稅及地下匯兌（Hawala/Hundi）。FMU將相關金融情報通報相關執法機關與監管機構，根據 FMU 提供的金融情報，A 公司營業場所因此被搜索，發現該申報營業地點並無實際業務活動，後續調查進一步確認存在貿易洗錢（TBML）情事。

目前已有數人遭逮捕，檢察官並已對相關人士提出訴訟，目前案件正在法院審理中。

來源 - 巴基斯坦

個案研究 #49 - 小型企業資助恐怖主義

資助恐怖活動；地下匯兌與哈瓦拉（hawala）；可疑交易報告

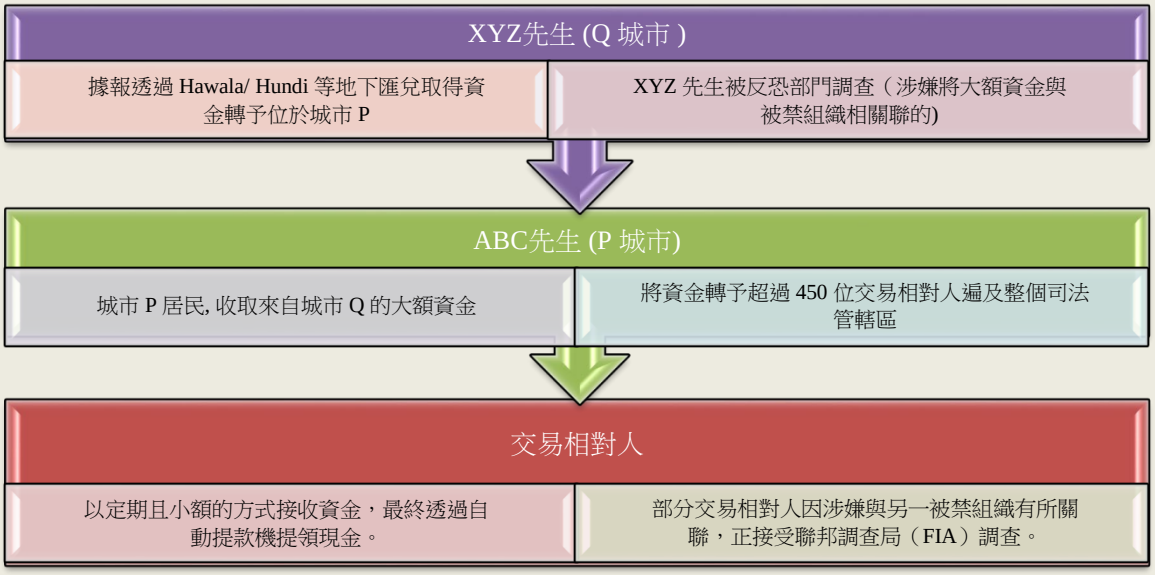
因財務活動異常且與個人申報的財務狀況不符，A 某被舉報疑似洗錢或資恐交易。A 某為 P 城市居民，經營一間小型布料店，但卻收到來自包括 Q 城市等偏遠地區的無關交易相對人（counterparties）資金。調查發現 A 某在三家不同銀行開設七個銀行 帳戶，過去三年累計存入資金達 4.74 億巴基斯坦盧比（約 165 萬美元）。

資金流入分析顯示，A 某大部分款項來自 Q 城市的 B 某。經查詢金融情報中心內部資料庫後發現，FMU已向反恐部門及聯邦調查局通報 B 某涉嫌從事非法地下匯兌（Hawala/Hundi）業務，並可能與國內被禁組織有所聯繫。進一步分析發現，A、B 兩人皆已遭反恐部門調查。

針對 A 某的資金流出分析顯示，其以定期、小額方式將 資金轉移給境內約 450 名交易相對人。進一步對這些交易相對人進行分析發現，多名接收資金 的個人早已遭聯邦調查局調查，涉嫌與國內被禁組織有關。

金融情報中心已將分析結果移交給反恐部門與聯邦調查局，以進行進一步調查。資金流向示意圖如下所示。

來源 - 巴基斯坦



案例研究 #50 – 以資恐方式資助車載簡易爆炸裝置之犯罪活動

資助恐怖活動；資金移轉服務；國際合作

2021 年，巴基斯坦某大城市發生一起車載簡易爆炸裝置（Vehicle-Borne Improvised Explosive Device，VBIED）攻擊事件，造成數人傷亡。初步調查發現，主嫌 A 某為此次攻擊使用之車輛所有人。反恐部門（CTD）已對 A 某及其共犯 B 某、C 某、D 某等人立案調查，並要求FMU提供相關之可疑交易報告／現金交易報告（CTR），以及嫌犯之銀行帳戶／金融交易資訊。

金融監控單位隨即於內部資料庫進行檢索，並將其等之國民電腦身分證號碼（CNIC）發送至各申報機構。申報機構回覆的資訊顯示，A 某之妻子與兒子、A 某帳戶介紹人、A 某與 D 某之資金提供者，以及 C 某之兄弟（被列管人員）等人皆涉案。

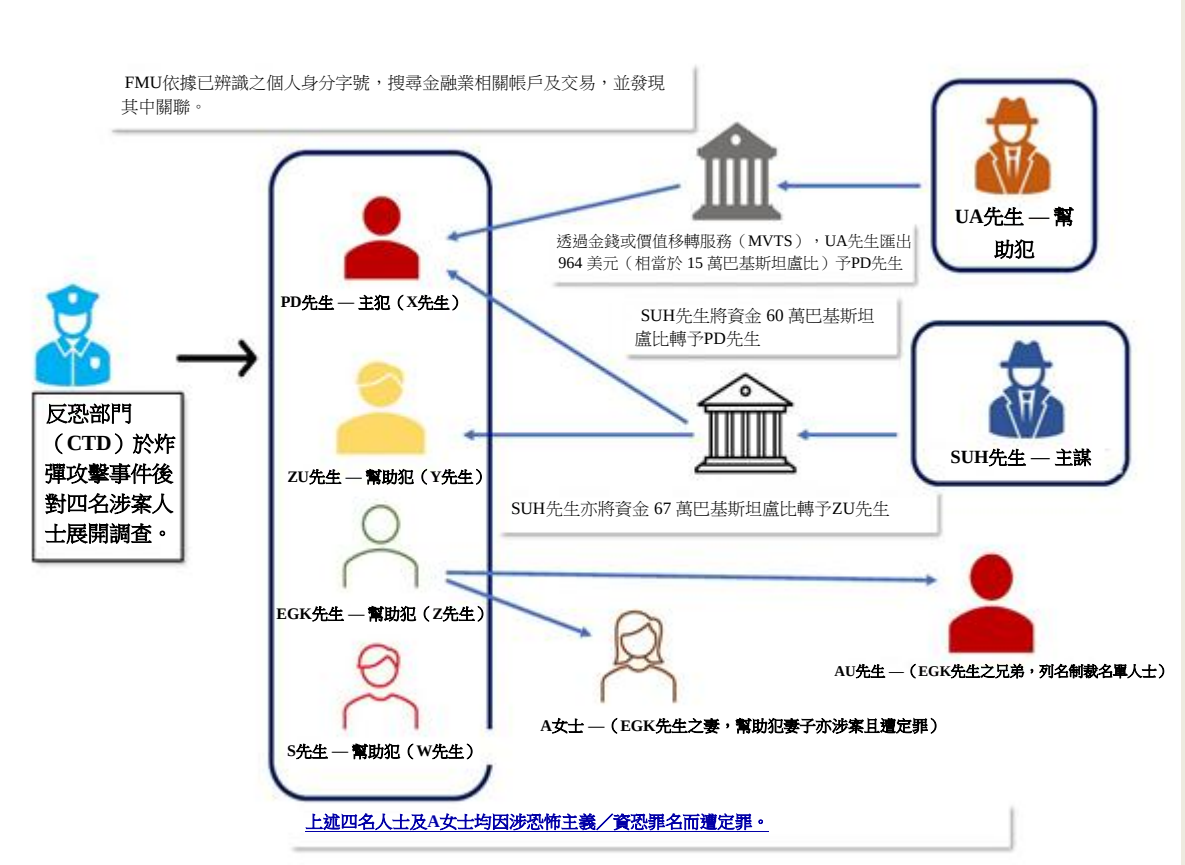
金融監控單位將其金融情報提供給反恐部門，後續提交了一份詳盡分析報告。報告指出，A 某居住於巴基斯坦最大城市，曾前往另一個大城市重新啟動一個靜止帳戶，提領現金後再將帳戶關閉。所提領之資金據指稱是用以購買恐怖攻擊所使用的車輛。C 某為 A 某提供後勤支援，亦為被列管人員之兄弟，後續確認 C 某為該攻擊事件之主嫌。深入分析進一步發現，A 某之資金提供者亦曾與 D 某進行明顯為資恐之交易。反恐部門之後續調查顯示，A 某之資金提供者實為此次恐怖攻擊之主謀。此外，嫌犯亦經常往返國外。

金融監控單位調查發現 A 某曾接收來自國外的匯款。因此金融監控單位亦就境外匯兌資訊尋求國際合作。金融監控單位向外國金融情報中心要求資訊，之後並將資訊轉交反恐部門。

此次恐怖攻擊的主謀/資金提供者、執行者及共犯（包含 A 某）皆已遭逮捕，並依據 1997 年《反恐怖主義法》及其他相關法規定罪。但其中僅有 2 人之資恐罪名成立，分別被判處 5 年及 7 年有期徒刑，併科罰金分別為 50,000 及 100,000 巴基斯坦盧比（約合 174 至 348 美元）。

再者，法院亦裁定沒收／追繳共計 3,144,000 巴基斯坦盧比（約 10,956 美元）之資產，雖然最初扣押／凍結資產之價值為 4,025,000 巴基斯坦盧比。

來源 - 巴基斯坦



案例研究 # 51 - 家族成員逃稅案件

稅務犯罪；可疑交易報告；濫用法人與法律協議

A 公司因涉嫌逃稅而被列可疑交易報告。金融監控單位分析發現，A 公司由同一家族之四名成員在巴基斯坦證券交易委員會（SECP）登記註冊。此外，該批家族成員在證券交易委員會登記共 15 間法人實體，並於多家銀行擁有多個個人與企業帳戶，該等帳戶皆出現大額資金轉入情形。上述法人／實體亦頻繁進行大量外幣交易，透過不同銀行帳戶間之資金移動，使資金流向變得複雜，疑似企圖掩蓋資金來 源。

巴基斯坦聯邦稅務委員會（FBR）資料庫顯示，儘管上述帳戶有龐大資金流量，A 公司與家族成員卻僅繳納極為有限的稅款給政府。公開資料查詢亦顯示，上述個人涉嫌錯報、竊取及逃稅等行為。該案已於 2021 年 2 月移送聯邦稅務委員會內地稅收部門進行進一步調查，目前案件仍在審理中。

來源 - 巴基斯坦

案件研究 # 52 - 豪華汽車詐欺案件

詐欺

A 公司於巴基斯坦證券交易委員會（SECP）正式登記註冊，為知名外國汽車製造商（下稱 B 公司）之授權經銷商，專門銷售高性能跑車、休旅車（SUV）與轎車。

A 公司之負責人 X 某於多家銀行持有數個個人及公司帳戶，帳戶內有頻繁大額資金流入。經查閱帳戶交易紀錄發現，A 公司最後一次向 B 公司寄賣交易款項為 2017 年。另查，B 公司近兩年因法律問題未再向 A 公司交付任何車輛。然而，X 某仍對外謊稱有車輛可供訂購，並持續向一般民眾收取預付款項。進一步分析亦顯示，X 某開立多張退款支票皆遭拒付。

調查發現，X 某以交付豪華汽車為由，向一般民眾詐取資金，惟實際上未曾交付任何車輛，亦未曾退還預收款項。估計 X 某經由此詐欺行為，共非法取得約 8 億巴基斯坦盧比（約合 280 萬美元）。

X 某於犯案後潛逃至國外。金融監控單位已將相關金融情報提供予執法機關，進行深入調查，並已正式對 X 某提起訴訟。

來源 - 巴基斯坦

案例研究 #53 - 龐氏騙局（Ponzi Scheme）,以高獲利投資方案詐欺一般民眾

詐欺犯罪；組織犯罪；濫用法人及法律協議；利用網際網路

A 某自稱為 A 公司之所有人，該公司聲稱從事資訊科技服務、電子商務及網路廣告業務。2019 年，A 某以企業 A 名義於多家銀行開設 5 個帳戶。該等帳戶之交易行為主要為網路轉帳（包含銀行間轉帳 IBFT、網際網路銀行及手機應用程式）及來自巴基斯坦全國各地民眾的大量現金存款。該等帳戶存入交易金額雖小，但交易頻率極高；相對之下，提款交易次數較少，惟單筆提款金額龐大。

同期，A 某另於巴基斯坦證券交易委員會登記設立一家私人有限公司，名稱亦為 A 公司，登記業務為網路購物及電子商務。登記資料顯示，該公司設有 3 名董事，分別為 A 某（持股 51%）、董事 2（持股 25%）及董事 3（持股 24%）。2021 年初，相關人士於巴基斯坦多家銀行開立公司帳戶 ，惟各帳戶僅 A 某一人為該公司各帳戶之被授權簽署人。

該等公司帳戶交易行為亦主要涉及網路轉帳（包括銀行間轉帳 IBFT、網路銀行及手機應用程式）及不同個人之現金投資存款。分析顯示該帳戶遭用以向全國一般民眾募集資金，聲稱可獲取高額利潤，明顯違反該公司原始登記業務範圍。

該同名私人有限公司同時擔任外國外匯交易公司於巴基斯坦之代理商，並利用各社群媒體平台展示如何透過該公司帳戶，將款項匯至國外外匯交易應用程式。惟巴基斯坦中央銀行已宣布此類網路外匯交易平台屬非法，並禁止授權外匯交易商提供相關交易服務。

金融機構、監理單位及執法機關接獲一般民眾針對該公司之詐欺與集體詐騙投訴。經銀行查詢後，包括 A 某在內的相關人士即以現金、及數位轉帳方式迅速將帳戶內資金悉數提領，銀行隨後依據執法機關之指示關閉或凍結相關帳戶 。

相關執法機關取得金融情報後，隨即對 A 公司及其董事展開調查。此外，該情報亦同步提供予監理機關（regulators），以提醒金融機構注意並採取適當之監理措施。

巴基斯坦證券交易委員會（SECP）已將 A 公司列入從事未經授權之租賃／融資業務、多層次傳銷（MLM）、金字塔式／龐氏騙局，以及以求職、投資或交易等名義非法向社會大眾募集資金之公司名單。此外，巴基斯坦聯邦調查局已對 A 公司及其董事（含 A 某）立案調查。

來源 - 巴基斯坦

案例研究 #54 - 利用家族成員個人帳戶進行商業交易

稅務犯罪；哈瓦拉（Hawala）

多家銀行針對四名以分批方式存入現金、疑似規避申報門檻的個人提交可疑交易報告（STR）。

這些人士從事糖品仲介及乾果買賣，與分散於不同地區、互無關聯的交易對象進行資金往來，其交易情形顯示可能涉及哈瓦拉（hawala）式的非正式資金移轉活動。金融監控單位分析前述可疑交易報告資料時發現，上述個人亦曾與多家砂糖廠進行交易。當時媒體報導，有調查委員會正針對轄內多家砂糖廠涉嫌囤積砂糖一案進行調查；由此提供另一調查方向，以釐清上述 4 名個人是否涉入此一活動。

金融監理單位已將分析結果移交相關執法機關，分別就稅務逃漏及哈瓦拉行為展開調查。目前本案已進入起訴階段，並已依法扣押四筆資產。

來源 - 巴基斯坦

個案研究 #55 - 貴金屬及寶石交易商因涉嫌洗錢罪而遭檢察機關起訴

獨立洗錢; 貴金屬與寶石交易

一名從事寶石及礦石標本交易之個人，被查出在同一銀行位於 3 個不同城市之多家分行持有數個帳戶，各帳戶均有大量境外匯入款項。經銀行查詢，該名個人聲稱此為其寶石及礦物出口所得款項，惟無法提供相關證明文件。此外，該人亦出現在巴基斯坦高風險邊境地區的若干現金交易報告（CTR）中。

依據金融監理單位提供之金融情報，相關執法機關已展開調查，並因其帳戶資金往來與申報之進出口資料明顯不符，以洗錢罪嫌移送法辦。

來源 - 巴基斯坦

案例研究 #56 - 透過公司洗錢之銀行詐欺案件

濫用法人及法律協議；國際商業公司；詐欺犯罪；境外前置犯罪；國際合作

FMU 接獲本地一家銀行可疑交易報告，內容涉及巴基斯坦籍國民 A 某。該通報係依據媒體負面報導，指出 A 某及其家族成員涉嫌於國外涉及一起重大銀行詐欺案件。媒體報導 A 某已獲取超過 1 億英鎊（約合 1 億 2,300 萬美元）之 犯罪所得。

2000 年，A 某成立 C 公司，主要業務為向國會議員、職業足球員及企業家提供融資服務。 2004 年，A 某於該外國司法管轄區獲選為「年度青年企業家」。

分析公開資訊發現，C 公司已於 2007 年因巨額債務倒閉；惟 A 某透過偽造帳目，仍成功自外國銀行取得大筆貸款，並將貸款資金轉匯至其家族於巴基斯坦之銀行帳戶。另據媒體報導，A 某已於該外國司法管轄區遭判刑入獄。

FMU經分析可疑交易報告（STR）及現金交易報告（CTR）後發現，A 某及其家族成員於巴基斯坦境內多家銀行持有多個帳戶。可疑交易報告內「認識你的客戶」（KYC）及「客戶盡職調查」（CDD）文件分析指出，A 某曾於巴基斯坦變更國民身分證之姓名。此外，報告分析亦顯示，上述帳戶多以 A 某及其家族成員個人名義開設，實際控制著家族成員帳戶，皆歸 A 某所有。帳戶內資金流動涉及美元、英鎊、歐元與巴基斯坦盧比等多種貨幣，資金流動金額龐大且方式多元，經由 A 某及其家族的帳戶進行流轉。

進一步公開資料分析顯示，A 某之家族成員亦涉嫌房地產詐欺案，並於巴基斯坦當地法院出庭應訊。此外，調查亦顯示 A 某在巴基斯坦境內亦成立房地產公司及時尚品牌企業。

基於上述金融情報及分析結果，金融監理單位已將相關資料移送執法機關。經執法機關調查，確認 A 某涉犯洗錢罪，並刻意隱匿應課稅所得與資產，以達逃漏稅之目的。調查期間，執法機關並透過金融監理單位取得外國金融情報中心之國際合作，協助案件偵辦。

來源 - 巴基斯坦

案例研究 #57 - 利用網路平台進行龐氏騙局

詐欺；使用網際網路；利用虛擬資產；濫用法人與法律協議；國際合作

犯罪所得/ 洗錢來源

執法機關於 2021 年 1 月偵破此一複雜的網路詐欺犯罪案件。

同年初，FMU 亦接獲一份可疑交易報告，並於分析後發布相關分析報告，指出下述 A&B 集團所屬公司及其帳戶之運作模式可能涉及異常情事。

A 某及 B 某為此龐氏騙局案件之主要涉案人，涉嫌於 2019 年 1 月至 2021 年 2 月期間，以該騙局向一般民眾詐取共約 170 億巴基斯坦盧比（約合 9,440 萬美元）。兩人成立 A&B 集團，並在另一名人士協助下架設網站平台，謊稱可以提供每月 7% 至 20% 的高額投資報酬。

這些公司宣稱其業務涵蓋房地產交易、加密貨幣交易所、資訊科技、運輸服務及貿易等項目以招攬投資，惟實際上從未進行上述任何投資活動，而是將新投資人的資金用於支付既有「投資人」之利息，形成龐氏騙局。據調查，新募集資金之 50% 用於支付既有投資人利息及支付介紹新投資人之代理人佣金。上述網路平台資金流動，皆經由 A&B 集團所屬公司進行轉移。

洗錢調查重點

A&B 集團係由 A 某成立之 26 家公司組成，各公司皆登記於 A 某家族成員名下，包括其子、堂表親及兩名配偶。

經向巴基斯坦證券交易委員會（SECP）調查發現，上述公司均未依法取得向社會大眾募集存款之許可，其相關業務皆屬非法活動。

調查期間亦查出涉案人及其親屬、其未依法登記之公司、及經 SECP 登記之公司，自 2019 年起於巴基斯坦境內多家商業銀行開設共 70 個銀行帳戶。執法機關會同銀行專家進行深入分析這些帳戶， 查明該龐氏騙局如何利用上述銀行帳戶洗錢犯罪所得, 並進一步轉入 A 某及其共犯之私人帳戶及投資項目。調查團隊向中央銀行取得相關帳戶資料，分析逾 50,000 筆交易紀錄。

資產調查發現，犯罪所得已用以購置 31 筆不動產及 30 筆動產，資產總值估計達 67 億巴基斯坦盧比（約合 3,720 萬美元）。

跨機關與國際合作

執法機關於 2021 年 9 月成立調查小組，由伊斯蘭馬巴德防制洗錢及打擊資恐局（AML/CFT Directorate，Islamabad）領導，並指派一名資深調查官擔任專案負責人，以及一名主要調查官進行案件偵辦。另聘請電腦鑑識專家協助回復並分析一個複雜資料庫，紀錄透過多層次虛假推薦制度進行之投資交易。該資料庫儲存於雲端，須由專業人士協助方能回復。其內含超過 100 萬筆交易資料，調查團隊已將資料庫內之記錄與 A&B 集團銀行帳戶資金流向進行核對分析。

調查團隊向人口資料庫暨登記主管機關蒐集被告之家族關係及相關資料，並取得其出入境紀錄以輔助調查。此外，金融監控單位及巴基斯坦證券交易委員會提供之資訊與證據，以及經由主管機關（巴基斯坦中央銀行，SBP）自多家商業銀行取得之紀錄，亦對本案調查提供重要協助。

分析被告網站取得之數位資料發現，被告等人亦曾於 B 及 C 司法管轄區從事類似詐欺活動。此外，金融調查亦顯示犯罪所得已被轉移至 D 司法管轄區，執法機關已透過國際合作機制發出調查請求。目前國際合作機制亦持續運作中，以追查 B 及 C 司法管轄區內之資產，並追緝該地區之涉案共犯。

現代調查技術之運用

本次洗錢犯罪調查採取之技術包括法務會計（forensic accounting）、數位鑑識、社群媒體社交工程分析（social engineering）、銀行帳戶紀錄分析、證人及嫌犯訪談，以及向國外司法管轄區尋求司法協助。

查封／扣押

- 依據 1999 年《國家問責條例》（NAO）第 12 條，於 2021 年 5 月至 7 月期間，凍結 41 個銀行帳戶，帳戶內存款約計 30 億巴基斯坦盧比（約合 1,660 萬美元）。
- 查封 17 筆不動產，依據 NAO 第 12 條，於 2021 年 5 月至 7 月期間，凍結估計價值約 25 億巴基斯坦盧比（約合 1,380 萬美元）。
- 於 2022 年 1 月，依據 NAO 第 12 條再凍結 13 筆不動產，價值約 7 億巴基斯坦盧比（約合 350 萬美元）。
- 於 2022 年 3 月，依據 NAO 第 12 條凍結 30 輛車輛，價值約 5 億巴基斯坦盧比（約合 250 萬美元）。
- 上述所有已確認之資產，皆已依法扣押並持續處於凍結狀態。
- 截至目前為止，經法院裁定查封/扣押之資產總額，包括銀行帳戶內存款、31 筆不動產、與 30 筆動產，共達 67 億巴基斯坦盧比（約合 3,720 萬美元）

巴基斯坦證券交易委員會亦已完成對該集團及其主事者之裁處程序，理由為該集團違反《 2017 年公司法》（Companies Act, 2017），涉及非法向一般大眾募集資金及經營金字塔型騙局。該集團包含 18 家依據《2017 年公司法》正式註冊之公司，以及另有 5 家未經正式登記之企業。集團主要負責人為 A 某及其直系家族成員。巴基斯坦證券交易委員會依法完成正當法律程序後，已裁定該集團之主事者五年內不得擔任任何公司之董事，並對每名主事者各裁處 1 億巴基斯坦盧比之罰鍰。同時，依據《2017 年公司法》，該等主事者不得設立新公司。

案件複雜性、涉案多方與組織犯罪網路

如前所述，本案涉案人等以組織化犯罪網路之形式運作，透過建立網路平台並控制資金流入 A&B 集團，以遂行非法龐氏騙局。此多層次虛假推薦制度透過獎勵介紹新客戶之代理人，並利用新投資人所投入之資金支付既有債務，以維持該騙局之運作。

調查過程涉及分析該平台於 2019 年至 2021 年間超過 100 萬筆交易紀錄，確認該平台共計募集約 170 億巴基斯坦盧比（約合 9,440 萬美元），該筆資金係透過 A 某及其共犯所成立之空殼公司進行移轉。由於犯罪集團透過具複雜架構之多家空殼公司、多個銀行帳戶，以大量網路交易，以及網路投資平台等方式掩飾犯罪所得之採集與流向，導致本案調查過程異常複雜，需逐一追查超過 70 個銀行帳戶，並進行法務銀行帳務鑑識。

此外，調查團隊另須資金追蹤及帳戶分析司法管轄區內 26 家人頭公司之銀行帳戶，過程極具挑戰性。確切金額。最終，調查團隊成功破解涉案之電腦系統及網路資料庫，獲取相關交易紀錄，確認犯罪所得之確切金額。

來源 - 巴基斯坦

案例研究 #58 - 重要政治性職務人士涉入之毒品販運案件

毒品相關犯罪；重要政治性職務人士

2022 年，執法機關（LEA）攔截一輛機車後發現 0.5 公斤大麻脂（Hashish），隨即逮捕涉案人 A 某。調查期間，執法機關要求金融機構提供資訊，以追查 A 某之資產與資金往來情形。

依據該項調查結果，金融監控單位收到某儲蓄銀行通報之可疑交易報告，指出 A 某於 2020 年購買價值 30 萬巴基斯坦盧比（約合 1,045 美元）之儲蓄憑證，該憑證已依執法機關之資產調查公文遭到銀行凍結。金融監控單位分析調查期間發現，A 某於 2022 年赴某銀行分行，以 5 筆現金交易將大筆資金存入 B 某之帳戶。進一步調查確認 B 某為重要政治性職務人士（Politically Exposed Person, PEP）。進一步分析 B 某銀行帳戶之交易紀錄後發現，B 某簽發付款委託書，將自 A 某收到之等額款項匯付給第三方，用以購置不動產。金融監控單位已將該金融情報移送主管執法機關。

A 某亦已依《1997 年毒品管制法》（Control of Narcotics Substance Act 1997）正式遭到起訴。

來源 - 巴基斯坦

案例研究 #59 - 比特幣交易商涉入詐欺及毒品犯罪案件

毒品相關犯罪；使用虛擬資產

A 銀行因懷疑 A 某涉嫌未經授權之虛擬資產交易，而針對其帳戶提出可疑交易通報。根據虛擬資產交易平台紀錄，A 某涉及比特幣買賣。依巴基斯坦中央銀行之規定，此類交易於巴基斯坦境內屬非法活動。A 銀行經調查發現，A 某帳戶出現大量異常交易，且多次與無明顯關聯之交易相對人進行資金往來。深入分析交易活動，證實 A 某確實從事虛擬資產交易。

且多筆大額交易來自涉及疑似從事哈瓦拉（Hawala）、或涉及其他犯罪活動之交易相對人。巴基斯坦金融情報中心資料庫亦確認，A 某之交易相對人之一為 B 某，係 X 公司之負責人。經巴基斯坦反毒品部隊（Anti-Narcotic Force）調查發現，X 公司之資金來源涉及販毒犯罪所得。此外，B 某帳戶內有來自A某帳戶大量轉入之資金，但缺乏明確合理交易目的。

因懷疑 A 某涉及虛擬資產交易，並可能協助他人透過 虛擬資產轉移犯罪所得，該金融情報已移送執法機關及中央銀行。

來源 - 巴基斯坦

2.14 菲律賓

案例研究 #60 - 員工詐欺

疑似洗錢或資恐交易通報；竊盜；電信詐欺

A 公司之帳戶於 2019 年 11 月 4 日至 12 月 12 日期間，共有 174 筆可疑交易報告。期間自該帳戶轉出資金總額約 2.26 億美元，匯至分布於 14 個國家之 69 個收款帳戶，包括 B 司法管轄區之某個人帳戶。A 公司之帳戶為集團內多家關係企業共同使用之帳戶。而上述收款人均非A 公司之供應商，亦無任何業務往來。經調查發現，上述匯款至銀行帳戶係由 A 公司之關鍵員工「員工 1」及「員工 2」所操作。兩人雖獲授權可操作該帳戶，但並未被授權進行上述特定交易。員工 1 聲稱其為一起網路愛情詐騙之受害者，竊取A公司資金以支付詐騙犯。

B 司法管轄區之該名個人於同日收到 A 公司匯入兩筆各 50 萬美元之匯款，分別存入當地兩個銀行帳戶內。B 司法管轄區之金融情報中心提供該個人相關資訊，於 2019 年 12 月 10 日至 16 日成功追回 999,464 美元之款項。

此外，B 司法管轄區之金融情報中心亦與 C 司法管轄區之對口單位協調合作，以確認其他可能之涉案共犯。

來源 - 菲律賓

案例研究 #61 - 販售兒童性剝削素材之犯罪所得

性剝削；資金移轉服務

A 某係一名男性外籍國民，因涉及兒童性犯罪，於是遭到 A 司法管轄區主管機關逮捕。調查發現，A 某透過行動支付工具將資金匯予 B 司法管轄區之涉嫌人士，以供 A 某購買兒童性剝削素材。經調查 A 某使用之電子裝置，發現其於 2022 年 12 月 29 日至 2023 年 1 月 2 日期間，透過行動支付工具進行多筆資金轉移，合計金額為 1,300 菲律賓比索。

目前，B 司法管轄區之金融情報中心亦正就本案進行同步調查。

來源 - 菲律賓

案例研究 #62 - 非洲毒品集團

有組織犯罪；跨國有組織犯罪集團；毒品相關犯罪

158 筆可疑交易報告發現，5 名嫌疑人涉案，交易總金額約 380 萬菲律賓比索（約合 317,000 美元）。該人等被懷疑為非洲毒品集團（ADS）之成員。2017 年 11 月 8 日，執法機關於 X 省逮捕 A 某及 B 某，兩人涉嫌於該區域販賣冰毒（當地俗稱「Shabu」）。

銀行資料顯示，A 某經營一家美容院，與 C 某為情侶關係；後者亦涉及前述可疑交易報告所揭露之活動。A 某之帳戶 因涉嫌參與非法毒品案件，業於 2020 年 10 月 22 日依據法院核發之凍結令予以凍結，惟因該帳戶資產價值不足，最終未被裁定沒收。

B 某與 D 某間存有可疑交易往來。

E 某則與一名外籍人士於 2018 年 3 月 10 日共同遭逮捕。情報顯示，該等人士涉嫌於 X 省及鄰近區域大量販售冰毒（俗稱「Shabu」）。下圖呈現所有涉案人士間之關聯性，該等人士均為非洲毒品集團之成員。

就交易筆數而言，與非洲毒品集團相關之跨境（國際）交易於可疑交易報告中以匯入占比最多，158 筆交易中有 45 筆屬此類型。以金額計算，與非洲毒品集團相關之跨境（國際）匯出交易總額達 140 萬菲律賓比索（約占可疑交易報告全部跨境匯出金額之 38%）。由於 A 某及 D 某之交易活動，2017 年為該集團在交易筆數及金額上最為活躍之年度。隨著 A 某、B 某與 E 某相繼遭逮捕，後續年度交易活動明顯減少。

來源 - 菲律賓

案例研究 #63 - 頻繁存提交易

可疑交易報告；賭場

2014 年，A 某於 ABC 銀行開立一般儲蓄帳戶，初始存款 449,000 菲律賓比索（約 7,913 美元）。其聲稱收入來源係其經營之顧問業務。

2017 年 3 月 27 日至同年 4 月 20 日期間，該帳戶陸續出現數筆大額現金及支票存款，金額介於 35 萬 7 千至 490 萬菲律賓比索（約 86,000 美元），隨後亦有數筆大額提款交易，金額介於 605,600 至 708 萬菲律賓比索之間。

ABC 銀行於進行強化客戶盡職調查（Enhanced Customer Due Diligence，ECDD）後發現，A 某實際擔任車手角色，負責將現金帶至賭場。A 某向分行表示，其友人將資金存入其帳戶內，當該等友人於賭場有現金需求時，再由 A 某將款項交付予該等友人。當分行進一步詢問該等交易之性質後，A 某即停止使用該個人帳戶。

同時，ABC 銀行亦對法人 A（亦即 A 某之顧問公司）提交可疑交易報告。法人 A 之帳戶自 2014 年 6 月 20 日開立至 2017 年 4 月期間，未有明顯交易活動。然而自 2017 年 4 月 3 日至 2018 年 1 月 24 日間，分行記錄該帳戶有 853 筆交易，金額介於 12 萬 6 千 500 元至 1,009 萬菲律賓比索（約 2,200 至 178,000 美元）。另於 2018 年 3 月 23 日至同年 11 月 8 日間，再次記錄 132 筆交易，金額介於 1 萬 7 千至 1,300 萬菲律賓比索。金融機構認定，上述受規範之 A 某及法人 A ，其等之交易活動缺乏法律或商業實質義務、交易目的及經濟合理性。

來源 - 菲律賓

案例研究 #64 - 公民詐欺犯（Citizen frausders）

可疑交易報告；濫用法人及法律協議

ABC 銀行於 2016 年 3 月 31 日，針對 2 名涉案人—1 名菲律賓籍人士及 1 名 X 司法管轄區國民—提交 2 份可疑交易報告，懷疑二人涉及 X 司法管轄區詐欺犯之犯罪手法。根據 ABC 銀行提供之資訊，該詐騙手法涉及 X 司法管轄區一眾詐欺犯利用菲律賓籍女性協助設立短期空殼公司。之後取得菲律賓貿易暨工業部（Department of Trade and Industry, DTI）核發之商業登記證明，並利用此證明作為開戶文件。

金融機構之報告顯示，涉案 X 司法管轄區公民詐欺犯開立之帳戶於開戶時僅存入最低額度之資金。帳戶於開戶後維持一年無任何交易，隨後即有高額且明顯可疑之款項匯入。

來源 - 菲律賓

案例研究 #65 - 愛情詐騙

使用網際網路；詐欺

金融機構發現網路上有多筆受規範對象之貼文，懷疑其擁有之帳戶疑似用於網路愛情詐騙（romance scam）活動。愛情詐騙係指詐騙者透過網路以虛假之愛情意圖誘騙被害人，取得其信任後再行詐財之犯罪行為。

受規範對象報告顯示，社群媒體之貼文明確指出詐欺嫌疑人為 A 某。A 某自稱係海軍陸戰隊成員。隨後再佯裝其上級長官傳訊給被害人，要求支付所謂軍方代理人代訂機票之費用。A 某遂指示被害人將款項匯入 X 銀行他人名下之人頭帳戶。

來源 - 菲律賓

案例研究 #66 - 資金循環交易

利用可疑交易報告；使用網際網路；新型支付方式

2021 年 10 月，金融機構針對受規範對象 PQR 與 A 某提出 74 筆可疑交易報告，原因為二者帳戶於該月份內有多筆電子錢包間轉帳交易，惟交易規模與 A 某作為司機之職業及經濟能力明顯不符。

經交易資料分析，該 A 某帳戶疑似為人頭帳戶。A 某涉案交易模式如下：起始有單一匯款人轉入固定金額 1 萬菲律賓比索（約 176 美元）。隨後再由 A 某將款項轉匯他人帳戶，之後再由他人將相同款項匯回 A 某帳戶。

依據 PQR 提繳之交易資料分析後發現，上述交易模式與 PQR 當時舉行之促銷活動「Send Money Challenge」之交易時間明顯吻合。該促銷活動允許菲律賓境內之 PQR 帳戶持有人透過該機構「Send Money」功能，向經 PQR 驗證之特定用戶轉帳至少 1 萬菲律賓比索以獲取禮券。每名用戶最多可參與 10 次以取得最高獎額。

每個交易日，A 某與至少兩組不同 PQR 帳戶持有人進行此類交易。交易對象涵蓋司法管轄區內各地。

來源 - 菲律賓

案例研究 #67 - 疑似過渡帳戶（pass-through accounts）

可疑交易通報

2018 年 12 月 13 日，X 銀行就 A 某帳戶交易異常頻繁之情形提出 23 筆根據該報告內容 疑似頻繁洗錢或資恐交易報告。報告顯示，A 某之帳戶於短短 35 日內累計進行 97 筆交易， 交易總額達290 萬菲律賓比索（約 51,000 美元）。包括現金存款 17 筆共 110 萬菲律賓比索； 線上轉帳 23 筆共 40 萬菲律賓比索、臨櫃提款 10 筆共 110 萬菲律賓比索，以及自動櫃員機提款 37 筆共 30 萬菲律賓比索。

調查過程中，A 某聲稱帳戶內大部分資金係親屬提供之生活津貼及學費。但未能說明該親屬之姓名及具體背景。此外，A 某坦承其帳戶亦供若干未具名之友人收取款項。上述帳戶資金流動

型態符合過渡賬戶特徵，其中資金流入總額為 150 萬菲律賓比索，流出總額則達 140 萬菲律賓比索。

另有 2 家受規範對象（CP）基於針對 X 司法管轄區學生所進行之防制洗錢（AML）調查，亦因認定 A 某資金匯出情形與其所申報之個人背景不符，而針對 A 某提出可疑交易報告（STR）。且收款對象既無親屬關係，亦無合法商業往來。同時未能提供足資證明交易合理性之文件。

來源 - 菲律賓

案例研究 #68 - 涉入銀行駭客案件

利用網際網路；詐欺

11 名個人及 3 家法人涉入共計 56 筆可疑交易報告（STR），交易總金額約 2,470 萬菲律賓比索（約 435,000 美元），與 2021 年 ABC 銀行駭客入侵事件相關。A 某係菲律賓國家調查局（NBI）逮捕之 5 名嫌疑人之一，涉嫌於 2022 年 1 月未經授權將 ABC 銀行 700 多名客戶帳戶內資金轉移至 XYZ 銀行之帳戶。執法機關線民舉報，有犯罪人士以電子郵件方式向被害人發送提供釣魚網站的連結，B 司法管轄區之人士則提供犯罪集團得以非法提領資金之設備。此外，另有 2 名本地人士擔任網站開發人員，負責搜尋銀行網站之弱點。

媒體報導指出，涉案網路犯罪集團成功入侵 ABC 銀行客戶帳戶；即使客戶被害人未點擊任何可疑連結。仍收到電子郵件及簡訊通知其帳戶資金已遭轉移。犯罪人士並成功規避銀行之 OTP（一次性密碼）安全機制。

菲律賓防制洗錢委員會之金融情報報告指出，XYZ 銀行之 B、C、D 及 E 四名本地人士帳戶收取 ABC 銀行轉出之資金，但實際使用該等帳戶者為非 XYZ 銀行帳戶持有人之 J 某。此部分可疑交易總額達 770 萬菲律賓比索（約 135,711 美元）。

另涉案人 F 某之帳戶通報最多 STRs，總金額達 930 萬菲律賓比索。該帳戶除直接收取 ABC 銀行駭客事件之資金外，亦為 B 某及 D 某二人帳戶後續資金轉移之第一至第三層受益帳戶。F 某聲稱其資金來源係身為醫學生之收入，被要求提出文件以證明交易之合法性。其自述亦涉及加密貨幣交易活動。

ABC 銀行駭客事件之相關交易多發生於 2021 年，其中帳戶間轉帳 41 筆共 2,230 萬菲律賓比索（約 393,000 美元），現金存款則約 150 萬菲律賓比索（約 26,436 美元）。

來源 - 菲律賓

案例研究 #69 - 車手招募

使用網際網路; 詐欺

犯罪集團通常透過面對面招募、網路求職詐騙、社群媒體網路、及網路愛情詐欺等方式招攬車手。部分人士遭誘騙，誤信所涉為合法交易，且被豐厚報酬所吸引。

例如，A 某經營合法便利商店之人員，經 B 某招攬，誤以為其所參與為合法之資金交易。B 某承諾 A 某，每進行一筆銀行交易即能取得相應報酬。B 某係 X 司法管轄區籍人士，2019 年因涉嫌經營涉數百萬菲律賓比索之網路詐騙案件遭到逮捕。調查發現，B 某係持學生簽證入境菲律賓，並利用網路愛情詐騙方式，向多名女性詐騙約 800 萬菲律賓比索（約 141,000 美元）。

A 某於警方調查過程中提供協助。經查，A 某於 2019 年六個月間進行 83 筆交易，涉及金額共計 360 萬菲律賓比索（約 63,500 美元）。該批交易皆以現金方式進行（包括現金存款、自動櫃員機提款及臨櫃提款），以規避資金之真實來源（存款端）與去向（提款端）之查核。

來源 - 菲律賓

案例研究 #70 - 包裹詐騙

詐欺; 新型支付方式

X 司法管轄區籍人士 A 某，係某受規範之電子貨幣機構（Electronic Money Institution, EMI）提供之可疑活動涉案名單中之客戶，因涉及使用行動電話進行可疑交易活動而遭通報。A 某帳戶交易金額歷年來有顯著異常變化。並曾以行動電話進行一筆提款交易（電子現金卡／禮物卡／簽帳金融卡），金額 2,298 菲律賓比索。2018 年，A 某透過 6 筆匯款交易收到 B 某匯入合計 20 萬菲律賓比索；另自 C 某收到 104 筆匯款交易，金額合計 370 萬菲律賓比索（約 65,209 美元）。

調查顯示，C 某所匯出之資金係來自多名可能遭其詐欺之人士，且該等匯款交易之用途多聲稱係商務用途，匯款人與收款人間之聲稱關係則多為客戶或朋友。通報機構指出，C 某進行 104 筆匯出交易，金額合計 370 萬菲律賓比索；並有 78 筆匯入交易，金額合計 270 萬菲律賓比索。

此外，C 某疑似為 D 某之同夥。某當鋪客戶請求該當鋪提供涉及 D 某及 C 某之相關文件，因其懷疑 D 某、C 某 2 人涉及詐欺活動。該客戶曾赴當鋪某分店向 D 某匯出共計 78,000 菲律賓比索，聲稱該筆匯款係用於支付包裹費用，並聲明與收款人 D 某之關係為全球快遞公司（EG）之公司代表。該筆匯款由當鋪之授權代理人當日即予以發放，申報之用途為支付費用，匯款人並聲稱與收款人為朋友關係。當鋪進行客戶盡職調查（CDD）後，發現該客戶表示該筆匯款係用於支付自其女婿寄送之包裹費用。該客戶表示曾接獲自稱 EG 公司代表之電話，通知有包裹已抵達機場，但須支付 78,000 菲律賓比索之手續費，且該手續費需透過代理人 D 某支付。客戶女兒告知其夫婿（客戶之女婿）並未曾寄送任何包裹，受害者始確認遭詐騙。客戶再試圖聯繫該所謂代理人，惟該人已無法取得聯絡。針對上述情事，該當鋪業已調取涉及 D 某及 C 某之監

視器畫面及相關必要文件， 並已向主管警察機關完成 報案登記（blotter）。該當鋪基於包裹詐欺案之被害人提出詐欺控訴，認定 D 某及 C 某之交易活動可疑。

來源 - 菲律賓

案例研究 #71 - 由疑似具親屬關係人士代為收取之境外匯款

新型支付方式

有一群來自 3 個不同司法管轄區之外籍男性遭通報，疑似涉及非法活動。該群人士代替一名身分不明之女性客戶收取境外匯款，並聲稱與該女性具有親屬關係。多數交易於同一日在貨幣服務業者（MSB）A 分行同時領取，其他交易則透過該業者之行動應用程式（MSB A Service App）進行。此外，該群人士於登記資料中留有可疑之電子郵件地址，且基於相似的姓氏、居住地及職業背景，顯示彼此可能具有親屬關係。據通報內容，該群人士可能涉入駭客及勒索犯罪活動。

來源 - 菲律賓

案例研究 #72 - 客戶提領現金致無法追蹤交易

詐欺；利用網際網路

A 某之帳戶因涉及一筆因電子郵件遭駭客入侵而取消之匯款，成為調查對象。該筆匯款來自某家公司，因 A 某先前已提供相關文件（例如公寓預約合約、價格表，以及與經認可之匯款業者簽訂之加盟協議書），因此被允許入帳至 A 某帳戶。A 某自 B 某處共收到 3 筆匯款，合計 1,660 萬菲律賓比索（約 292,000 美元）。隨後 A 某進行數筆現金提款，金額介於 90,000 至 500 萬菲律賓比索，提款總金額約 1,634 萬菲律賓比索。A 某聲稱 B 某係其友人，匯款用途係用於協助設立 MSB 之 B 匯款加盟分店，及購置兩間公寓單位。然而，該帳戶之交易紀錄及相關業務文件，並未顯示與其所聲稱之匯款代理業務或貿易活動相關之交易。基於上述資訊，金融機構認為 A 某之交易活動可疑，主因為遭撤回之匯款係因電子郵件遭駭客入侵所致。同時涉案匯款金額龐大，且均透過臨櫃方式提領現金，致使資金流向無法追蹤。

來源 - 菲律賓

案例研究 #73 - 可疑指標:交易活動與客戶財務能力不相稱（四個案例）

可疑交易通報

某通報機構接獲 C 銀行之報告，指出其客戶 A 某之帳戶涉及已證實之網路釣魚（Phishing）案件，並遭未經授權之資金轉移。存入 A 某帳戶之資金後續即被透過自動櫃員機提領、或被轉帳至其他帳戶。該帳戶歷史交易紀錄顯示多筆現金存款及線上轉帳，單筆金額介於 300 至 10 萬菲律賓比索（約 1,762 美元）之前，且匯款之匯入／匯出方身分不明，超出 A 某原申報之經濟狀況。A 某此前聲稱其資金來自經營網路商店及一間未經登記之雜貨店，每月收入約 5 萬菲律賓比索。

另有某銀行注意到 B 建築公司有 3 筆交易， 該等交易明顯與公司之業務性質及財務能力不符。該交易包括自國外一非政府組織（NGO）匯入 34,276 美元（約 24,914 歐元）之款項。 一張面額 1 億菲律賓比索（約 176 萬美元）的支票存款，該筆款項於次一銀行營業日即遭退回。此外，另有一筆面額 5,000 萬歐元、聲稱係由某外國銀行簽發之偽造銀行匯票亦曾被試圖存入帳戶。調查另揭露，前述 34,276 美元匯入款項涉及一項詐欺投訴案件。申訴人聲稱該筆款項原係作為一國內非政府組織（NGO）之受益款項，但因詐欺而未能到位。經網路查證發現，B 公司及其負責人 X 某已遭控以詐欺（estafa）罪名，X 某與另一名涉案人員因涉嫌侵占原用於尤蘭達颱風（Typhoon Yolanda）救援款項共計 600 萬菲律賓比索（約 105,745 美元），而遭菲律賓國家調查局（National Bureau of Investigation, NBI）逮捕。上述人士涉嫌透過駭入某國內 NGO、及某外國 NGO 之電子郵件，使得相關救援款項無法匯入原訂之國內 NGO 帳戶，反遭轉入該建築公司之帳戶。

A 某任職於 X 行銷公司，擔任團隊領袖及「代碼庫存管理人員」。A 某之帳戶涉及 138 筆現金存款、356 筆網路資金轉帳存入、11 筆國內外匯款存入，以及 143 筆帳單繳費存入交易。A 某之客戶購買所謂之「代碼（codes）」，以供啟用 X 行銷公司之會員帳戶，正式成為該公司會員。依據受規範事業所提交之報告指出，X 行銷公司之經營模式疑似為金字塔型騙局，因該公司實際並無商品可供銷售，而是透過人員招募拓展業務。其收益模式主要有二：第一為輸入驗證碼（captcha encode），（該方式係網站常用以防止駭客及垃圾訊息散布者（spammers）濫用之驗證手段，利用腳本（script）或自動程式機器人（bots）立即執行特定動作。犯罪分子則傾向利用機器人程式（bots）入侵多個帳戶密碼、或於部落格（blogs）中濫發垃圾訊息）；第二為邀請其他人士加入。帳戶交易筆數與規模顯示，X 行銷公司可能使用該帳戶從事金字塔型騙局活動；此等交易規模與 A 某所申報之經濟狀況顯然不符。

A 銀行接獲通報，指出其客戶 A 某之帳戶涉及因網路釣魚（phishing）事件取得未經授權之資金，與 B 銀行某客戶之儲蓄帳戶有關。經審查該 B 銀行客戶之帳戶發現，有 13 筆線上轉帳交易，金額自 2,500 至 50,000 菲律賓比索不等，皆轉入 C 某之儲蓄帳戶。調查 C 某帳戶發現，其內存入資金來源包括現金存款、網路付款及轉帳交易，該等資金流動與 C 某所聲稱之個人經濟背景與資金來源不符；帳戶資金流出則多透過臨櫃及 ATM 提款，或轉至其他存款帳戶。經詢問資金來源時，C 某聲稱資金來自其父母，並否認與 D 銀行之客戶有任何聯繫或認識，惟坦承曾向家人及朋友提供其帳戶號碼。

來源 - 菲律賓

案例研究 #74 - 電子貨幣機構（EMI）電子錢包遭帳戶接管（2起案例）

詐欺；新型支付方式

電子貨幣機構 1（EMI 1）於 2019 年因數家銀行提出關於帳戶遭非法接管（account takeover）之投訴案件進行調查後，共通報 8,847 筆相關交易。調查指出，該等銀行之若干帳戶因遭駭客入侵而洩漏帳戶資訊，致使相關資金遭轉移至多個 1A（EMI 1A）電子錢包帳戶內。肇事者透過網路釣魚（phishing）手段進行駭客攻擊涉案帳戶，非法取得進行轉帳所需之帳戶資料。

2021 年，電子貨幣機構 1（EMI 1）通報涉及帳戶遭接管案件之交易共 13,116 筆，受害對象涵蓋多名電子貨幣機構 1A 客戶。該批案件包括客戶透過接聽詐騙電話、收取詐騙簡訊、收取詐騙電子郵件、點擊釣魚連結、或假冒之電子貨幣機構 1A 網頁、透過社群媒體聊天工具之虛假頁面，或電子商務平台應用程式遭受詐騙，以及遺失或手機被盜等情形，導致帳戶遭非法接管。

來源 - 菲律賓

案例研究 #75 - 社群媒體平台使用者帳戶遭駭客入侵

利用網際網路

通報指出，客戶 A 某之帳戶遭用以非法轉移資金。手法為透過駭入一名男性受害人之社群媒體帳戶後，詐騙其妻子透過便利商店匯款 13 萬菲律賓比索（約 2,324 美元）。該案件涉及由兩家受規範事業（covered persons）提出之 6 筆可疑交易報告。

來源 - 菲律賓

案例研究 #76 - 交易活動缺乏法律或商業實質義務、正當目的或經濟合理性（2 起案例）

可疑交易報告

(1) A 某案：通報銀行指出，A 某提交之認證文件顯示其被授權在帕賽市（Pasay City）某處經營業務。但銀行之客戶資訊紀錄卻登記地址位於巴石市（Pasig City）。經分行經理實地查訪 A 某所聲稱之營業地址，惟該處已人去樓空。A 某於 2018 年 10 月至 12 月間，有大量現金存款交易，金額合計 1,056 萬菲律賓比索（約 189,000 美元）。每筆現金交易金額介於 100 萬至 300 萬菲律賓比索之間。銀行曾要求 A 某提供佐證，惟其未能提出任何文件。

(2) 另一案例：B 某於 2015 年 8 月 24 日至 2016 年 11 月 14 日期間，收受多筆匯款，金額合計約 1,499 萬美元（約 7.1451 億菲律賓比索）。通報機構認為該等匯款交易缺乏經濟合理性，且注意到 B 某聲稱該等匯款係來自經授權支付服務業者，惟未提供任何佐證文件。另查 B 某之帳戶簽署人與 C 某相同，後者亦因交易模式與 B 某相似，成為數筆可疑交易報告之通報對象。B 某及 C 某均為服務提供商（Service Providers, SPs）。

來源 - 菲律賓

案例研究 #77 - 客戶交易金額與其業務或財務能力不相稱

可疑交易報告

2018 年，服務供應商（SP）A 某因 2017 年至 2018 年間涉及多筆可疑交易（STR）通報，尤其包括 8 筆支票交換入帳交易（總額 3,074 萬菲律賓比索）、122 筆現金存款交易（總額 4.3106 億菲律賓比索）、58 筆支票存款交易（總額 2.4715 億菲律賓比索）、13 筆帳戶間轉帳交易（總額 1.1975 億菲律賓比索）以及 1 筆通用編碼 STR （約合計 1,470 萬美元）。銀行表示密切監控 A某之交易活動原因為，該客戶經常進行巨額交易，單筆交易金額介於 256,000 至 8,900 萬菲律賓比索。客戶向銀行聲稱該等交易來自多名個人及法人支付之租賃款項。惟客戶無法提供相關佐證文件，以支持其聲稱之交易用途。銀行因此認定上述交易金額與 A 某所聲明之資金來源顯不相稱。

來源 - 菲律賓

案例研究 #78 - 異常頻繁入境

可疑交易報告；現金；賭場

2019 年 12 月至 2020 年 3 月期間，現金攜帶者 J（Individual Carrier J）自境外 A 或 B 司法管轄區入境馬尼拉合計 33 次。除其中 2 趟旅次外，J 均自 A 司法管轄區攜帶大量現金入境（單次金額相當於 132,632 美元至 360 萬美元不等）。另兩次則攜帶美元現鈔，分別為 25 萬美元及 1,180 萬美元。J 於外幣申報表中聲稱從事國際貿易銷售業務。並在部分申報中自述為現金所有人，指定收款者為 A 某。

經調查發現，A 某除接收 J 攜入之外幣現金外，另亦接收來自 C 司法管轄區之現金攜帶者 K 、L，以及 A 司法管轄區之現金攜帶者 M、N 所攜入之外幣。上述 5 名攜帶者於同一期間合計入境 38 次，均聲稱攜入之資金係交付予 A 某，用於賭場博弈用途。短短約 4 個月間，A 某自上述 5 名攜帶者共計收取約 6,090 萬美元。

前述 5 名攜帶者（J、K、L、M、N）中，僅一人與菲律賓金融情報中心資料庫比對符合。菲律賓防制洗錢委員會（AMLC）於 2020 年 7 月 7 日接獲資訊指出，L 某曾遭其原籍 C 司法管轄區之地方警政單位通報，懷疑其涉入有組織犯罪活動。同日一筆可疑交易報告顯示，應菲律賓賭場監理機關之要求，L 某已被列為審查對象，原因即其涉入攜帶大量現金入境菲律賓。

來源 - 菲律賓

案例研究 #79 - 加密貨幣竊盜案

使用虛擬資產；資恐；濫用非營利組織

A 某為某非營利組織專案主管，執法機關懷疑該組織透過資金援助方式，支持位於菲律賓南部某團體之資恐活動。調查發現，A 某於虛擬資產服務提供商 C 開立帳戶，接收來自 300 餘個外部加密貨幣錢包，以及其他虛擬資產服務提供商 C 內帳戶之虛擬資產（主要為比特幣），累計價值約 856,000 菲律賓比索（約 15,309 美元）。上述資金累積於 A 某之帳戶後，旋即轉入未知地址之加密貨幣錢包。

來源 - 菲律賓

案例研究 #80 - 詐騙募捐所得資金轉換為加密貨幣

使用虛擬資產；資恐

H 女士為居住於資恐高風險地區之女性大學生，目前因涉嫌參與恐怖組織相關資恐活動，正接受調查。H 女士透過電子貨幣機構（EMI）X 及貨幣服務業者（MSB）Z，於四個月內接受多筆小額捐贈款項（單筆均未超過 2,000 菲律賓比索），累計約 92,000 菲律賓比索。此外，H 女士亦透過多筆銀行轉帳收取資金，總金額約 263,000 菲律賓比索（約 4,703 美元）。經追查資金流向後發現，前述資金並未用於其所聲稱之慈善目的，而係用於購買手機預付卡及個人現金提領用途；另有部分資金用以購買少量比特幣，之後再轉移至未知地址之加密貨幣錢包。

本案由執法機關轉介至菲律賓防制洗錢委員會（AMLC）秘書處 請求針對 H 女士本人及其名下銀行帳戶展開金融調查。前述帳戶曾於社群媒體平台發布 以接受民眾捐款，聲稱用以援助受颱風影響之災區，但可能被用於資助菲律賓的恐怖活動。案件調查仍在進行中。

來源 - 菲律賓

案例研究 #81 - 詐騙慈善捐款將資金轉換為加密貨幣

使用虛擬資產; 資恐

2022 年，菲律賓防制洗錢委員會收到某虛擬資產服務提供商通報，指出某帳戶持有人透過貨幣服務業者（MSB）匯入資金，並將其轉換成比特幣。這些資金隨後被轉移至一個未標記地址之加密貨幣錢包。進一步利用區塊鏈平台分析顯示，該加密貨幣錢包內之比特幣最終被轉移至另一個錢包地址，而該地址涉及與恐怖主義組織相關聯之轉帳活動。

本案已轉介國內執法機關，以及相關國際防制洗錢合作對口單位。

來源 - 菲律賓

案例研究 #82 - 將組織犯罪所得資金轉換為加密貨幣

有組織犯罪；洗錢；使用虛擬資產

I 某及 O 某偽裝為 X 司法管轄區籍之學生，並在菲律賓地方院校註冊入學。R 某為 29 歲菲律賓籍加密貨幣交易商，其帳戶曾接收來自 X 司法管轄區籍人士之匯款，該等人士涉嫌一起駭客入侵事件。根據 Y 銀行交易模式分析顯示，R 某與 X 司法管轄區籍人士均使用同一家律師事務所處理相關業務。調查顯示，I 某透過其於 Y 銀行開設之帳戶，於虛擬資產服務提供商 C 進行多筆大額現金匯入交易，金額介於 11,000 至 220 萬菲律賓比索之間。O 某亦於虛擬資產服務提供商 C 進行類似之大額現金匯入交易。

同時，R 某在收到 I 某匯入資金到他的帳戶後，透過虛擬資產服務提供商 B 進行總額達 550 萬菲律賓比索之加密貨幣出售交易（即現金化）。此外，R 某亦匯出兩筆匯款至 S 司法管轄區之一名外國重要政治性職務人士，金額合計 180 萬菲律賓比索，該司法管轄區被認定為資恐及駭客活動之高風險區域。菲律賓防制洗錢委員會（AMLC）初步調查顯示，依據 I 某、O 某及其他匿名犯罪成員之策劃與安排，上述駭客入侵事件之犯罪所得，最終有相當部分流向身分不明之加密貨幣錢包。此外，I 某與 O 某另涉嫌在菲律賓境內廣泛招募人員擔任車手。

以上調查資訊已於 2020 年 9 月 29 日移送菲律賓國家調查局（National Bureau of Investigation, NBI）

另案調查發現，R 先生係某毒品相關案件中一名偶發涉案人之關聯方。該資訊於 2021 年4月舉行之「目標情報整合（Target Intelligence Packaging，TIP）」工作坊中，提供予執法機關。

菲律賓防制洗錢委員會近期於《環境掃描：網路犯罪威脅與涉案人研究》（Environmental Scanning:Cybercrime Threats and Perpetrators）（還路掃描研究）中，亦將I某、O 某及 R 某列為 2020 年 6 月駭客入侵案件中 13 名相關涉案人士之一。根據多家銀行、當舖與電子貨幣機構（EMI）之通報，前述 13 名個人及 1 間公司法人涉及共 801 筆可疑交易，金額高達 16.23 億菲律賓比索（約 290 萬美元）。該環境掃描研究報告已於 2022 年 11 月與 12 月間，發布予菲律賓防制洗錢委員會各利害關係人，包含各相關執法機關。

來源 - 菲律賓

2.15 新加坡

案例研究 #83 - 利用網路平台進行資恐案件

資助恐怖活動

2022 年，一名於 A 司法管轄區工作之外籍人士，依據新加坡《2002 年防制資助恐怖主義法》（Terrorism (Suppression of Financing) Act 2002），因提供資金予恐怖主義實體，而遭法院判處有期徒刑2年8個月。該涉案人士因自我激進化，並受伊斯蘭國（ISIS）於敘利亞建立「伊斯蘭哈里發國（Caliphate）」之目標所吸引。調查指出，2020 年 A 某透過網路平台，前後 15 次將共計 891 新加坡元（約 654 美元）轉帳至支持敘利亞組織之募款活動。A 某於匯款時明知其全部或部分之資金，可能用於支援「沙姆解放組織」（Hayat Tahrir Al-Sham）之活動，該組織已遭聯合國依據伊斯蘭國及蓋達組織制裁名單（ISIL (Da'esh) and Al-Qaida Sanctions List）指定為恐怖主義實體。

來源 - 新加坡

案例研究 #84 - 跨國合作偵辦洗錢案件調查

詐欺；境外前置犯罪；第三方洗錢；貨幣兌換；現金；國際合作

2019 年至 2020 年期間，新加坡警察部隊商業事務局（Commercial Affairs Department, CAD）陸續接獲通報指出，有被害人因虛構投資機會遭詐騙，將總額約 54,940 新加坡元（約 40,314 美元）之款項，匯入設於 A 司法管轄區之兩個銀行帳戶其中一帳戶在 A 司法管轄區之法人（A 公司）名下，另一帳戶則在 B 司法管轄區之國民 B 某名下。

前述款項於入帳後四日內，即自 A 公司及 B 某之帳戶，匯轉至另一名 B 司法管轄區之國民 C 某設於新加坡之個人銀行帳戶。進一步調查顯示，從 A 公司帳戶匯出之款項，乃由 C 某於 B 司法管轄區從事非法跨境無照貨幣兌換、及匯款交易而進行；另 B 某之帳戶匯出款項，則聲稱用於向 C 某購買奢侈手錶。

2020 年 8 月，C 某於 A 司法管轄區遭控非法經營匯款業務，並依據《貪污、販毒及其他重大犯罪（利益*沒收*）法》（*Corruption, Drug Trafficking and Other Serious Crimes* (*Confiscation of Benefits*) Act）犯下洗錢罪名。C 某於 A 司法管轄區經法院許可離境後未再返回。法院遂發布拘捕令，並由新加坡商業事務局請求 B 司法管轄區協助追查並遣返 C 某。2022 年 10 月，C 某於 B 司法管轄區試圖離境前往第三地時，遭該國執法機關逮捕。並被送至 A 司法管轄區。C 某隨後已向被害人全額歸還款項，並經法院判處 12 週有期徒刑。B 司法管轄區與 A 司法管轄區執法當局間的成功合作，對於起訴透過 A 司法管轄區銀行帳戶所犯之洗錢犯罪，以及將 C 某遣返回國接受相關罪名之指控與訴追，具有重要價值。

來源 - 新加坡

案例研究 #85 - 因可疑交易報告啟動之投資詐騙調查

詐欺；境外前置犯罪；第三方洗錢；濫用法人及法律協議

2018 年，新加坡金融情中心－可疑交易報告辦公室（Suspicious Transaction Reporting Office, STRO）接獲線報，關於新加坡註冊法人 A 公司在新加坡境內開設之銀行帳戶。該公司涉嫌收受來自 B 司法管轄區之投資詐騙犯罪所得資金。新加坡警察部隊商業事務局（CAD）依據 STRO 提供之金融情報，立即展開洗錢犯罪調查。

調查顯示，A 公司係由 A 某設立。2017 年間，A 某與其友人 B 某達成協議，約定 A 某依據 B 某指示，協助處理 A 公司名下銀行帳戶之交易活動，並依每筆交易金額收取佣金。經調查，A 某為前述用途共開立 3 個公司帳戶。於 2017 年 12 月至 2018 年 11 月間，該等帳戶總計透過 307 筆交易，收取約 1,960,478 美元及 1,606,191 新加坡元（約 118 萬美元），其中已確認至少 331,822 美元及 4,250 新加坡元，為來自 B 司法管轄區與新加坡境內投資詐騙案之犯罪所得。

A 某隨後因違反新加坡《貪污、販毒及其他重大犯罪（利益沒收）法》之洗錢罪名遭起訴與指控。B 某因招募 A 某參與該協議，依據《貪污、販毒及其他重大罪行（沒收利益）法》之洗錢罪名被定罪，判處 26 個月有期徒刑，並科罰金 70,000 新加坡元（約合 51,000 美元）。迅速傳遞之金融情報確保新加坡當局能即時採取果斷行動，有效防止 A 公司及其帳戶持續遭濫用作為犯罪所得之收款管道。

來源 - 新加坡

案例研究 #86 - 涉及非法野生動物販運活動之洗錢案件調查

環境犯罪；有組織犯罪；第三方洗錢；境外前置犯罪；跨國有組織犯罪集團

新加坡警察部隊商業事務局（CAD）與國家公園局（National Parks Board）共同針對涉及犀牛角非法販運活動所衍生之洗錢案件進行聯合調查，該案犯罪所得約達 120 萬新加坡元（約 88 萬美元）。各執法機關密切合作，採取多管齊下之方式，包括針對非法野生動物交易進行執法行動，並追查資金流向，以查明集團成員（例如盜獵者、運輸者、中間人）及幕後資助這些非法活動的境外金主。上述資訊交換工作係透過國際刑警組織（INTERPOL）、金融情報中心（FIU），以及各相關國家執法機關間之直接合作管道共同完成。其中國際刑警組織提供寶貴情資，協助宣導多邊聯絡與合作工作，功不可沒。

鑑於來源國、過境國與目的地國間之國際合作對遏止非法貿易至關重要，前述機關共同參與國際刑警組織行動支援小組（INTERPOL Operational Support Team, OST），一同前往 A 司法管轄區協助當地執法單位調查非法野生動物販運犯罪集團之活動。國際刑警組織行動支援小組之核心任務即在於促進各國執法機關間之情報交換，並深化雙邊合作關係。期能建立一套國際合作模式， 強化情報分享與交換機制，以深入揭露非法野生動物販運犯罪集團之結構。

來自 A 司法管轄區之 A 某因涉嫌非法販運野生動物，遭新加坡法院依據《瀕危物種（進出口）法》（Endangered Species (Import and Export) Act）提起兩項指控，罪名為未取得有效之《瀕危野生動植物種國際貿易公約》（CITES）輸出或再輸出許可，即攜帶 18 件白犀牛角及 2 件黑犀牛角入境新加坡。此外，A 某另遭依據 1992 年《貪污、販毒及其他重大犯罪（利益*沒收*）法》（*Corruption, Drug Trafficking and Other Serious Crimes* (*Confiscation of Benefits*) Act 1992）提起一項指控，原因係其明知 B 某參與非法貿易，仍協助 B 某保有其犯罪所得。

來源 - 新加坡

案例研究 #87 - 涉及增值稅詐欺所得之洗錢案件

稅務犯罪；走私；詐欺；第三方洗錢；境外前置犯罪；現金

2021 年 3 月，新加坡海關與商業事務局（CAD）接獲情報後展開聯合調查，該情報涉及有人前往外國 B 司法管轄區某城市，企圖在該城市機場以詐欺方式申領增值稅（VAT）退稅，但未成功。調查發現，前述旅客所申報之珠寶商品事實上並非購自 B 司法管轄區，相關退稅發票亦偽造。該批旅客於先前已成功詐領增值稅退稅款共計 42,975 歐元（約 45,700 美元）。取得現金後即返回新加坡。

本案調查過程中，各方透過國際刑警組織（INTERPOL）、金融情報中心，以及新加坡與 B 司法管轄區之間直接的機關對機關合作管道，進行極為密切且廣泛的情資交流。兩國刑事司法互助（MLA）權責機關亦積極聯繫並提供調查建議，以迅速取得足以成功起訴洗錢罪所需之證據。

2022 年 12 月，A 某與前述涉案旅客遭依據新加坡《貪污、販毒及其他重大犯罪（利益沒收）法》第 47(1)(c) 條（CDSA 2000年版本），合併適用《刑法典》（Penal Code）第 109 條規定，被控密謀持有詐欺取得之增值稅退稅款項。上述旅客亦另涉違反同法（CDSA）第 48C(2) 條，因其攜帶超過法定額度之現金入境新加坡，但未依法申報。據稱 B 某返回新加坡時，未依《海關法》（Customs Act）之規定申報相關珠寶物品。B 某亦因未依據《海關法》（Customs Act）第 128B(1)(a) 條之規定，申報攜入新加坡之進口物品，而遭到起訴。此外，A 某亦因涉協助旅客違反現金申報義務，以及協助 B 某違反《海關法》之申報規定，而另遭提起控訴。目前案件仍在法院審理程序中。

來源 - 新加坡

案例研究 #88 - 公司董事涉及逃漏稅、洗錢及詐欺案件

稅務犯罪；詐欺；獨立洗錢；金融機構；購買不動產；購買高價或具文化價值資產

A 某係新加坡某商品及服務稅（Goods and Services Tax, GST）登記公司（A 公司）之董事。雖 A 公司已完成 GST 登記，惟 A 某於 2011 年 5 月 1 日至 2017 年 10 月 31 日期間，仍持續透過現金銷售商品予客戶，未於 A 公司之所得稅及 GST 報稅表揭露上述營業收入，導致該期間內少報 GST 稅額達 110,119 新加坡元（約 81,000 美元），另於 2013 至 2017 課稅年度間，漏報企業所得稅共計 69,391 新加坡元（約 51,000 美元）。此外，約於 2013 年間，A 某曾指使公司員工竄改存貨紀錄、並虛增 A 公司盈餘，企圖以不實之財務資 料誘使某金融機構核准 A 公司所申請之貸款。

調查亦發現，A 某將 A 公司之未申報銷售收入，用於支付其個人公寓及車輛之頭期款與房貸，總金額超過 40 萬新加坡元（約 294,000 美元）。

本案由駐派於新加坡警察商業事務局（CAD）衛星辦公室之調查官發現，於是啟動平行之洗錢調查作業，並促成稅務機關與洗錢調查機關之密切合作及資訊共享。2022 年 5 月，A 某因觸犯稅務犯罪、詐欺罪，以及違反《貪污、販毒及其他重大罪行（沒收利益）法》（CDSA）第 47(1)(c) 條之洗錢罪，而遭法院判決有罪。2022 年 6 月，法院判處 A 某 9 個月有期徒刑，並處以罰金總額 253,195 新加坡元（約 186,000 美元）。

來源 - 新加坡

案例研究 #89 - 專業人士協助處理犯罪所得之案件

詐欺；境外前置犯罪；專業協助者（professional facilitators）

本案涉及一名專業協助者利用空殼公司處理詐騙之犯罪所得資金。

A 某擔任 4 家由外籍董事所設立之新加坡註冊公司之本地居民董事。惟其並未履行必要之客戶盡職調查（Due Diligence）義務，亦未曾聯繫該等外籍董事。公司服務提供商（corporate service provider）於接獲未經核實人士之指示後，即將銀行文件及網路銀行憑證（Token）寄送至不明海外地址。導致該 4 家公司銀行帳戶接收超過 55 萬美元之犯罪所得。經與外國執法機關合作，確認該筆犯罪所得資金涉及商務電子郵件詐騙及網路愛情詐欺，受害者遍及國內外。 A 某於 2021 年底依據《公司法》（Companies Act）被判有罪，此為洗錢罪之外之替代性刑事司法處置，法院判處其 6 星期有期徒刑，並禁止擔任公司董事職務 5 年。

來源 - 新加坡

案例研究 #90 - 犯罪集團涉及複雜洗錢活動案件

詐欺；第三方洗錢；金融機構；貴金屬及寶石交易商；現金交易

調查發現，一個犯罪集團利用 9 家休眠商業實體，詐領政府機關之培訓補助金，金額近 4,000 萬新加坡元（約 2,940 萬美元）。該等商業實體係由夫妻關係之 A 某與 B 某所成立。在 C 某協助下，該犯罪集團另招募 D 某等數人，擔任上述商業實體之名義董事（Nominee Directors），並將公司實質控制權交由犯罪集團運作。犯罪集團主嫌 A 某聘僱三名車手，協助兌現商業實體銀行帳戶所開立之支票。每次進行支票兌現作業時，A 某或犯罪集團其他成員均會陪同該 3 名車手前往銀行，將支票交付車手兌現後，於銀行附近領取現金，車手則以收取佣金作為報酬。

C 某則協助犯罪集團洗錢，陪同上述人頭董事，將商業實體帳戶及犯罪集團成員控制之銀行帳戶所開立之支票兌現，包括 D 某個人銀行帳戶內之支票。A 某並指示擔任銀行帳戶授權簽署人（Authorized Signatories）之人頭董事開立支票、並協助兌現部分支票，以將取得之現金交付 C 某。

此外，D 某自個人帳戶提領之現金亦轉交予 C 某，再由 C 某根據 A 某之指示，將資金交付 A 某、或由 A 某指定之犯罪集團內其他成員 犯罪集團成員將部分犯罪所得現金作為佣金支付予 C 某，由 C 某、數名人頭董事及 D 某共同分配。

此外，B 某數度自犯罪集團其他成員手中接收部分提領之犯罪所得。B 某將部分現金存放於其兄弟住處的保險箱內。該保險箱為 B 某依 A 某指示購置。

2017 年末，於調查啟動前，A 某、C 某、D 某及數名人頭董事相繼潛逃。C 某攜帶現金與 D 某共同離境，D 某則於離境前以犯罪所得資金購置珠寶。A 某潛逃期間，B 某依其指示，使用犯罪所得購買黃金。此外，為避免執法機關察覺，B 某依 A 某指示要求其兄弟將保險箱內之內容物取出，並交由他人保管。

經由 A 司法管轄區、B 與 C 之執法機關緊密合作與協助，上述所有潛逃嫌犯均已逮捕歸案。主要涉案人員 A 某、B 某、C 某及 D 某因共謀詐欺政府機關，並涉及多項洗錢罪行而被判有罪，該等罪行包括隱匿、轉換、移轉犯罪所得，取得犯罪行為之利益，以及將犯罪所得移出司法管轄區。各別因洗錢罪行判處 80 個月至 110 個月不等之有期徒刑。

此外，調查另發現 3 家貴金屬及寶石交易商（Precious Stones and Precious Metals Dealers, PSMDs）曾向 B 與 D 兩名人士出售黃金與珠寶，且購買行為主要以現金支付。這些業者未依規定進行必要的客戶盡職調查（CDD），亦未就單筆超過 20,000 新加坡元的現金交易提交現金交易報告（CTR）。最終，該三家業者遭起訴並被裁罰，罰金金額介於 9,000 至 40,000 新加坡元（約合 6,600 至 29,000 美元）不等。

來源 - 新加坡

案例研究 #91 - 海外毒品犯罪集團利用現金車手案件

毒品相關犯罪

2021 年 1 月至 5 月間，新加坡中央肅毒局（Central Narcotics Bureau, CNB）偵破一個以境外為基地之犯罪集團。該集團透過合法運輸貨物之車輛，將海洛因、大麻及甲基安非他命（俗稱冰毒）走私至新加坡境內，再供應予當地毒品販售人員。

為降低犯罪風險，避免毒品與毒品販售所得資金同時遭執法機關查扣，該犯罪集團設置多層次運作網路，透過毒品車手及車手，分別負責毒品運送與毒品販售所得資金之收取。

該集團除利用當地毒品據點人員收取毒品買家支付之現金，並直接轉交供貨集團成員外，亦利用其他車手將收取的毒品銷售所得匯出。負責匯兌的經許可之外幣兌換兼匯款服務業者（Licensed Moneychangers-cum-Remittance Service Providers）並未涉入毒品犯罪活動，乃於不知情狀況下遭犯罪集團利用。

其中 3 名協助將毒品販售所得現金交付車手、或透過匯款服務匯出犯罪所得之毒品據點人員，*已遭新加坡中央肅毒局逮捕，並依據《毒品濫用法》（Misuse of Drug Act, MDA）與《貪污、販毒及其他重大犯罪（犯罪所得沒收）法》（CDSA）同步展開調查*。

來源 - 新加坡

2.16 索羅門群島

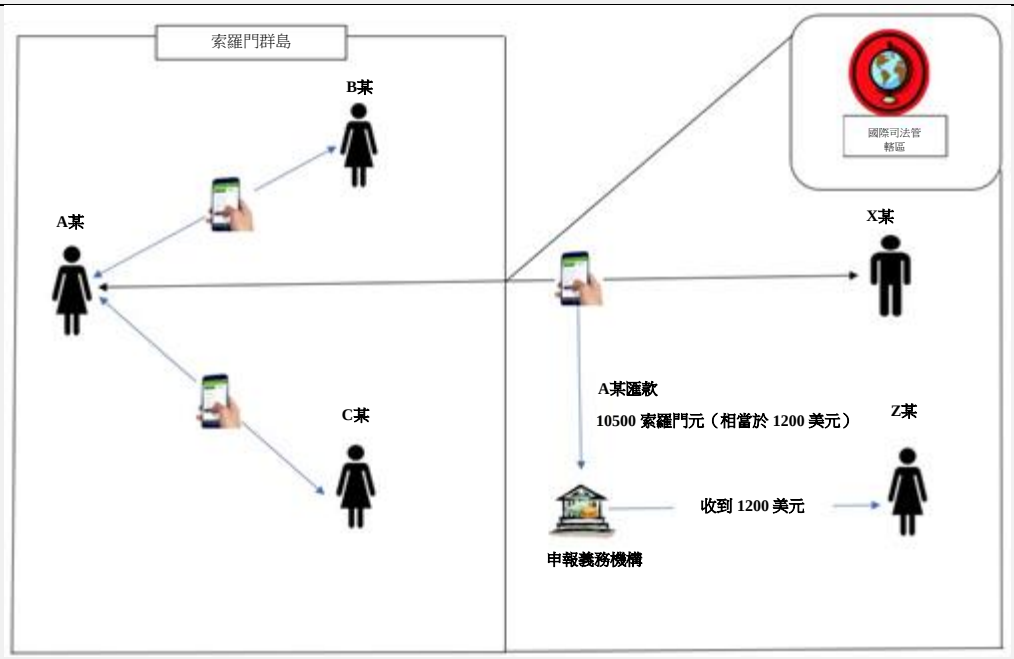
案例研究 #92 - 包裹詐欺

詐欺; 身分竊盜

2022 年 7 月至 8 月間，A 某於臉書上認識自稱居住於索羅門群島之B 某與 C 某。B 某隨後透過網路向 A 某介紹一個聲稱致力於協助全球身心障礙人士（disabled people）之組織。B 某並表示若 A 某有意加入，則可將其聯繫至該組織首腦，協助其完成註冊程序成為正式會員。隨後，A 某被轉介給 C 某，C 某宣稱其系統顯示 A 某已獲得 90,000 美元獎金。

但須事先支付 5,000 索羅門群島元（約 600 美元）才能取得該筆獎金。A 某被指示透過聯邦快遞（FEDEX）支付上述金額，並表示屆時將寄送包裹予 A 某。之後，A 某被要求聯絡 X 某處理獎金相關事宜。2022 年 7 月 29 日，A 某依據申報機構（Reporting Entity）指示匯出所要求之款項；2022 年 8 月 1 日，A 某再次接獲 X 某要求支付額外 5,000 索羅門群島元（約 600 美元）以進行包裹通關手續。A 某總計支付 10,500 索羅門群島元（約 1,200 美元），惟並未收到任何包裹。X 某後續再次聯繫 A 某，要求其支付更多款項以作為額外運費及相關手續費用。A 某遂向申報機構提出檢舉。該申報機構經初步分析後，確認該交易特徵符合典型消費者詐欺行為。並立即禁止位於 B 司法管轄區之 Z 某繼續使用其金融服務。

來源 – 索羅門群島



Case study #93 - 涉及國民將其金融卡寄往海外之詐欺案件

詐欺；結構化交易；現金；可疑交易報告；金融卡

某本地銀行帳戶於 3 個月內接獲數筆來自索羅門群島境內之大額現金存款及多筆行動轉帳，總金額約 20,000 索羅門群島元（約 2,400 美元）；每筆存入資金後皆立即於索羅門群島境內、及 B 司法管轄區進行現金提款。

索羅門群島金融情報中心接獲申報機構提交之可疑交易報告，內容涉及多個呈現類似異常交易

模式之銀行帳戶。初步調查發現，本地帳戶持有人透過網路認識外籍人士後，受其誘騙，將個人金融卡寄往海外，以換取承諾之豐厚商業投資機會。索羅門群島境內之大額存款與多筆行動轉帳，則來自於遭受上述外籍人士詐騙之多名受害人。

詐騙集團利用線上平台及社群媒體鎖定本地老年族群，誘導其將 Visa 金融卡寄予海外詐騙集團。同時，犯罪集團亦透過社群媒體誘騙其他民眾，將資金存入指定帳戶，以便自境外提領。

金融情報中心已深入分析前述可疑交易報告，並將分析結果轉介予相關執法機關續行偵辦。目前此案仍在調查中。

來源 – 索羅門群島

案例研究 #94 - 跨境稅務犯罪案件

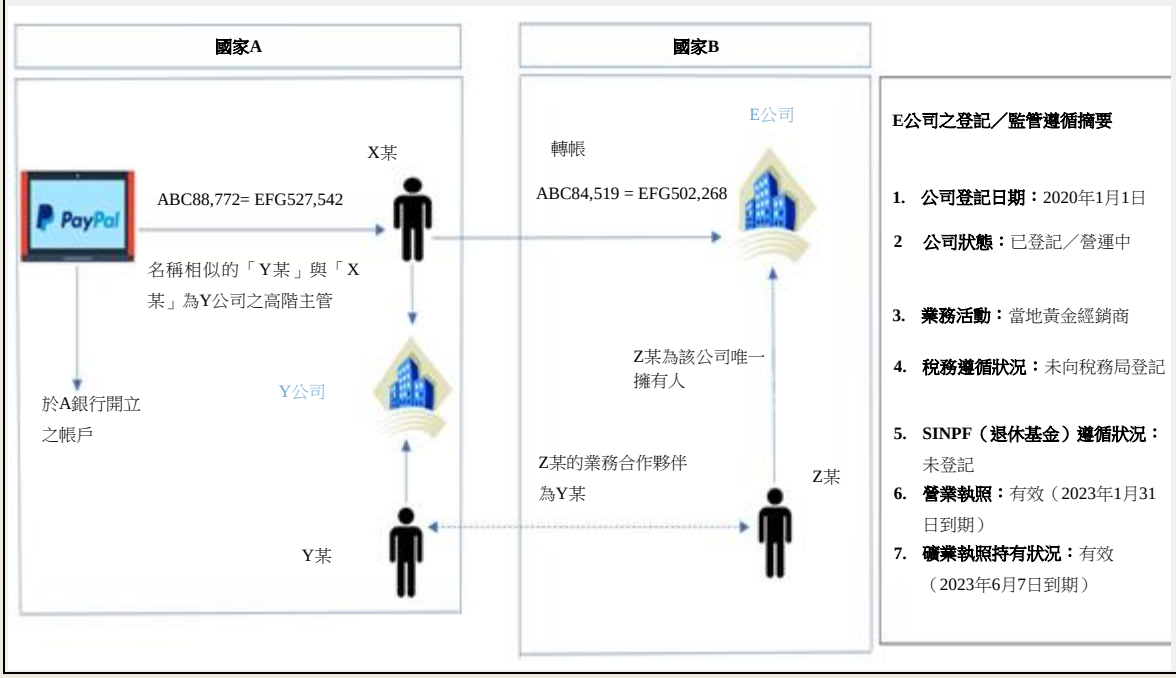
– 稅務犯罪；濫用法人及法律協議

金融情報中心接獲境外 A 司法管轄區提交之可疑交易報告，內容涉及索羅門群島籍國民 X 某（居住於 A 司法管轄區）多次自其個人帳戶向索羅門群島境內之 E 公司匯入大額資金，聲稱係用以住宅整修，金額約 502,268 索羅門群島元（約 60,000 美元）。惟金融情報中心經查證後發現，X 某於電子匯款表單所申報之資金用途，與實際收款之 E 公司業務性質明顯不符，該公司實際從事黃金等礦產開採業務，由 Z 某所持有。

進一步調查亦顯示，E 公司與 A 司法管轄區之 Y 公司存有商業合作協議，X 某與 Y 某則為 Y 公司之高階主管。X 某與 E 公司間有頻繁之資金往來，雖皆聲稱用以住宅整修，惟根據商業協議實際內容，上述資金實際用途係購買黃金以從事出口貿易，與所聲稱之用途明顯不符。金融情報中心研判此情事涉嫌透過虛假用途掩飾營業收入，以規避稅務申報。

已將本案調查報告轉介索羅門群島國稅局（Inland Revenue Division, IRD）進一步偵辦。

來源 – 索羅門群島



2.17 中華臺北

案例研究 #95 - 虛擬寵物詐欺案

詐欺; 使用網際網路

2020 年，中華臺北刑事警察局接獲檢舉，指出有一詐欺集團架設應用程式（App），其成員分別擔任平台管理人員、LINE 投資群組版主及投資活動講座主辦人等角色，以投資虛擬寵物為誘因吸引民眾加入該平台（LINE 為一種當地通用的通訊應用程式）。加入之會員購買虛擬寵物後，集團承諾可每日獲得所購買（認養）之虛擬寵物價值 2% 的獲利；另若會員成功推薦下線加入，還可額外取得下線所購寵物價值 5% 至 10% 不等的推薦獎勵。

集團要求會員必須將其個人電話號碼綁定至銀行帳戶，以供會員間進行虛擬寵物交易、購買應用程式平台上架之虛擬寵物，以及收受與匯出相關資金。該集團透過不定期於交易平台上推出新的虛擬寵物並販售予會員，以此獲取收益。然而該交易平台於 2020 年 4 月無預警關閉，導致多名會員蒙受財務損失。

經過近一年之監控調查後，發現該犯罪集團首腦為 A 某，其從境外司法管轄區購入該投資平台應用程式。B 某等人則擔任股東，共計設置五個 LINE 投資群組並擔任群組版主。其他集團成員則負責回覆會員諮詢、舉辦投資推廣講座，以及在 LINE 群組內鼓吹投資獲利。

蒐證完成後，警方分別於 2021 年 11 月 16 日及 2022 年 2 月 23 日展開兩波拘捕行動。共計逮捕 16 名涉案嫌疑人並搜索其居住處所。進一步調查發現，自該投資平台於 2019 年 8 月成立至 2020 年 4 月 2 日無預警關閉期間，共有 56 名被害人遭詐騙金額高達新臺幣 2,000 萬元（約合 620,000 美元）。該犯罪集團利用多個銀行帳戶接收會員資金，其中部分帳戶經查證為人頭帳戶。

16 名涉案人中，已有 6 人因涉嫌違反《銀行法》遭檢察機關提起公訴，目前案件仍在審理中。截至目前為止，尚未查扣任何相關資產。

來源 – 中華臺北

案例研究 #96 - 兩司法管轄區聯合偵破利用竊取連鎖咖啡店點數進行洗錢之偽卡犯罪集團

詐欺；偽造文書；組織犯罪；使用網際網路；信用卡／儲值卡

刑事警察局接獲 B 司法管轄區執法機關通報，指出該區多名被害人接獲假冒郵政機構寄發之電子郵件，謊稱包裹寄送失敗，要求被害人事先支付相關費用後，方得重新寄送。被害人點擊釣魚連結，依照假冒網站指示輸入信用卡號碼及一次性密碼（OTP）後，信用卡隨即遭綁定至「Apple Pay」行動支付，並立即用於購買中華臺北某連鎖咖啡店之儲值點數。

中華臺北與 B 司法管轄區聯合調查後，協助檢察署針對本案展開偵辦。經檢察署調查發現，首謀 A 某招募犯罪成員，架設釣魚網站，發送電子郵件或簡訊給被害人。誘騙被害人點擊連結。一旦被害人輸入信用卡或銀聯卡號碼及 OTP 密碼，其卡片資訊即遭竊取，用以製作偽造信用卡（偽卡）。

該犯罪集團成員隨後將偽造之信用卡／銀聯卡綁定於 Apple Pay 行動支付，並前往實體咖啡店，以偽造卡片購買大量儲值卡，再以折價方式轉售予第三方，以兌換現金。

該集團趁咖啡連鎖店推出促銷活動期間，更大量使用偽卡購買點數。短短一週內即獲取價值約新臺幣 100 萬元（約 31,000 美元）之儲值點數。並再折價出售予下游業者以從中牟利。由於儲值卡內之點數具現金價值，此犯罪模式得以進行跨境洗錢。一年內該犯罪集團即取得近新臺幣 1,000 萬元（約 310,000 美元）之犯罪所得，受害者遍及全球。2022 年 3 月 29 日，警方拘捕包含首謀在內之 5 名涉案人，現場查扣製作偽卡之設備、空白晶片卡、銀聯卡及儲值卡等證物。目前相關涉案人已由檢察署提起公訴，惟首謀 A 某已潛逃境外。

來源 – 中華臺北

案例研究 #97 - 地方政府機關首長涉嫌貪污

貪污賄賂；購置不動產；重要政治性職務人士

A 某為地方政府機關首長，長年來持續收受多家廠商提供之賄賂款項。A 某逃避 A 司法管轄區的調查、起訴及處罰。為逃避中華臺北司法機關之調查、起訴與處罰，A 某透過其一等親近親名義開設銀行帳戶，將賄賂與貪污所產生的犯罪所得進行洗錢，並自行掌控帳戶存摺與印鑑，將賄賂所得的資金存入帳戶。A 某並不時指示政府機關 內部職員使用前述借名帳戶存入或提領現金。此外，A 某亦透過上述近親名義，與友人合謀利用非法所得購置不動產。

A 某因違反《貪污治罪條例》及《洗錢防制法》遭檢察機關提起公訴，目前案件審理中。所收受之賄賂款項合計約新臺幣 1,000 萬元（約 310,000 美元）。

來源 – 中華臺北

案例研究 #98 - 涉嫌洗錢

貪污賄賂；使用信用卡；支票；現金；重要政治性職務人士；結構化交易

A 某為 I 縣縣長。自 2000 年起，A 某為隱匿來源不明之現金並避免遭查扣，遂與農會總幹事 B 某達成共謀協議。由雙方分別於同一日期開立同一金額之無記名支票（bearer cheques）相互交換。每當 A 某取得來源不明之新臺幣 100 萬元（約 31,000 美元）現金後，即透過其秘書 C 某交付 B 某一張新臺幣 100 萬元之無記名支票，而 B 某則回交一張到期日為隔日、同等金額之無記名支票予 A 某。

A 某接獲支票後，遂存入其友人 D 某及 E 某名下之銀行帳戶，惟上述帳戶實際仍由 A 某掌控並使用。當 A 某所開立之支票到期時，即由來源不明之 100 萬元現金存入 B 某帳戶，並於隔日以 B 某所開立之無記名支票兌現相同金額。秘書 C 某持用 D 某及 E 某帳戶之存摺與印鑑，自金融機構臨櫃提領款項後交付 A 某；D 某與 E 某則向 A 某收取所提領現金金額之 1% 至 3% 作為出借帳戶之報酬。秘書 C 某持用 D 某及 E 某帳戶之存摺與印鑑，每次臨櫃提領款項均未超過新臺幣 50 萬元,規避達到通報門檻之現金交易.

上述提領之現金交由 A 某之子收藏，後者租用小型套房，將現金存放於保險箱內。透過開立表面為貸款用途之支票，使帳戶內循環流動，創造帳戶內僅餘新臺幣 259 元之假象。藉由上述交換支票、扣款兌現、使用他人之銀行帳戶、臨櫃分次提領現金及製作並開立支票以新債還舊債之手法，營造債務已清償之假象，以防止現金遭到查扣。

A 某已遭檢察機關以不明財產來源罪提起公訴。

來源 – 中華臺北

案例研究 #99 - A鄉長涉嫌收受賄賂案

貪污賄賂；不動產利用；重要政治性職務人士

2020 年，S 鄉鄉長 A 某於辦理聘用招募及遴選過程中，收受 B 某、C 某及 D 某提供之賄賂款項。其中，C 某透過 E 某交付 A 某新臺幣 60 萬元（約 18,600 美元）之賄款，C 某及 D 某則直接交付 A 某新臺幣 45 萬元（約 14,000 美元）賄款。

為隱匿上述賄款來源，A 某使用其母親名下之銀行帳戶，並指示鄉長辦公室助理 F 某代為存入及提領現金。2021 年 4 月至 5 月間，A 某將上述賄款與其他資金混和後， 再以其子名義進行投資，投入金額新臺幣 190 萬元（約 59,000 美元），與其友人共同出資購置價值新臺幣 570 萬元（約 177,000 美元）之土地。

A 某於 2022 年因違反《貪污治罪條例》及《洗錢防制法》遭檢察機關提起公訴。A 某已將所有犯罪所得交付檢察機關。

來源 – 中華臺北

案例研究 #100 - 投資詐欺及違反銀行法

詐欺；購置不動產

A 某為外國 B 司法管轄區 A 公司之實質受益人，聲稱具有多年期貨投資經驗。自 2013 年 4 月至 2021 年 7 月間，A 某設計期貨投資及海外貨幣基金投資方案，並招募投資人。

A 某及其共犯承諾在一定期間內代投資人進行期貨操作後，除返還本金外，更可提供不合理之高額利潤。在 A 某與投資人簽訂之投資合約中，投資人交付 A 某之資金係以投資資金或借款名義辦理。A 某要求投資人於期貨經紀商任職之共犯處開立期貨帳戶。

帳戶開立後，A 某即要求投資人提供網路交易帳戶密碼。惟 A 某僅將少部分資金投入期貨交易。大部分資金則遭 A 某提領，用於支付投資人利潤，以此繼續吸引更多投資人參與虛構之海外基金投資，以及海外期貨交易平台投資計畫。

此外，A 某以需匯一定金額至海外帳戶方能贖回原投資金為由，誘騙投資人持續加碼投資。自 2013 年至 2021 年間，A 某詐騙投資人之金額共計新臺幣 873,154,028 元（約 2,700 萬美元）。

為掩飾及隱匿犯罪所得來源，A 某及其共犯將犯罪所得用於購置不動產及購買人壽保險保單。調查過程中，檢方已查扣相關銀行帳戶、證券帳戶及不動產。目前 A 某及其共犯已遭提起公訴，案件審理中。起訴罪名包括違反《銀行法》、《刑法》、《期貨交易法》、《證券投資信託及顧問法》及《洗錢防制法》。

現已查扣 1 筆不動產、27 個銀行帳戶及 4 個證券 帳戶，合計價值新臺幣 2,880 萬元。

來源 – 中華臺北

案例研究 #101 - 透過第三方支付企業進行賭博與洗錢

賭博活動；新型支付方式；稅務犯罪；利用網際網路

2018 年 8 月，A 某與共犯設立公司並成立網路賭博博平台 專門招攬外國 A 司法管轄區之賭客，並於中華臺北境內 設置 3 間伺服器機房。由 B 某負責管理該等機房，另聘僱數名 客服人員。賭客申請帳號後，即可透過用戶名稱及密碼 登入該平台。並以 A 司法管轄區之貨幣兌換為 賭博點數，進行包括電子遊戲以及足球、 籃球等體育賽事之賭博投注。賭客若獲勝，則可透過位於 A 司法管轄區之第三方支付業者支付賭金 賭博點數儲值亦由第三方支付業者處理。

洗錢模式乃透過連接該賭博平台之內容管理系統（Content Management System, CMS）與第三方支付業者之系統而進行。賭客可透過便利商店付款、信用卡及虛擬帳戶進行儲值。相關資金首先透過第三方支付業者匯入人頭帳戶，接著客服人員再以網路銀行將資金於數個帳戶之間進行轉移，最終再將款項匯入該公司名下帳戶。當賭客要求將賭博點數兌換回 A 司法管轄區之貨幣時，亦透過第三方支付業者進行，之後資金以網路銀行方式將自 A 司法管轄區之人頭帳戶匯回賭客帳戶。透過此方式，犯罪所得之資金來源即遭掩飾及隱匿。

A 某及其共犯因涉嫌稅務犯罪與洗錢罪遭檢察機關提起公訴。為換取緩刑，A 某等人歸還犯罪所得新臺幣 2 億元（約 620 萬美元），並支付罰金新臺幣 8 億 5 千萬元（約 2,640 萬美元），且承諾連續兩年每年向財團法人犯罪被害人保護協會捐款新臺幣 1,000 萬元（約 31 萬美元）。

來源 – 中華臺北

案例研究 #102 - 平台G涉嫌違反《洗錢防制法》

詐欺；使用網際網路；使用虛擬資產

詐欺集團透過網路社群媒體，宣傳投資由平台 G 發行之虛擬資產「F 幣」。為吸引投資人，集團謊稱 F 幣之價值將穩定上漲。並於其網站捏造虛假投資獲利數據，再透過 LINE 等通訊軟體招攬投資人。詐欺集團起初誘使被害人小額投資並支付利潤以取得其信任。進而遊說投資人加碼投資。然而 2020 年 1 月，平台 G 突然告知投資人其帳戶遭凍結，暫停所有提領作業。

該詐欺集團由 A 某及其共犯所組成。A 某等人提供其所有金融帳戶資訊予詐欺集團，以接收資金並轉入被害人之投資帳戶，擔任詐欺集團之「人頭帳戶」。隨後再透過多家虛擬資產服務提供商之虛擬資產錢包，購入泰達幣（USDT）及其他加密貨幣，並將之轉入由不明人士控制之冷錢包（Cold Wallet）。該人等亦透過第三方支付業者協助移轉犯罪所得。犯罪所得總計新臺幣 111,291,972 元（約 345 萬美元）。

來源 – 中華臺北

案例研究 #103 - 加密貨幣竊盜案

竊盜; 使用虛擬資產

犯罪集團成員向虛擬資產服務提供商申請 4 個帳戶，利用該平台無法即時更新之時差漏洞，多次重複進行加密貨幣之兌換、出售及提領。2020 年底至 2021 年 1 月間，該集團以此手法不法取得超過 300,000 枚泰達幣（USDT）及 217 枚以太幣（ETH），市值超過新臺幣 2,500 萬元（約 77.5 萬美元）。該集團隨後將竊得之加密貨幣轉移至其他虛擬資產服務提供商之帳戶，以隱匿犯罪所得。

來源 – 中華臺北

案例研究 #104 - 加密貨幣搶劫案之國際合作調查

竊盜；國際合作

刑事警察局（CIB）接獲 A 司法管轄區執法機關通報，指出具雙重國籍之嫌疑人 A 某涉及於 2022 年 3 月 16 日搶劫、並竊取被害人持有之多種加密貨幣，價值約 300 萬美元。A 司法管轄區法院已於 3 月 23 日發布對 A 某之通緝令。

經調查發現，A 某於通緝令發布前已入境中華臺北。為查明該嫌疑人是否係意圖藏匿前述搶劫犯罪所得而入境，且是否於中華臺北境內從事其他犯罪活動，中華臺北與 A 司法管轄區展開刑事偵查合作。

A 某為 A 司法管轄區法院因涉重大犯罪案件所通緝之逃犯，其 A 司法管轄區之護照亦遭撤銷，故其入境中華臺北屬非法情事。此外，A 某於 A 司法管轄區涉及武裝搶劫、恐嚇、綁架、非法

拘禁等暴力犯罪，可能危害中華臺北之公共安全與社會秩序，因此刑事警察局積極透過多管道展開追查。5 月 31 日，檢察官核發拘票後，A 某遭到逮捕，並於 6 月 3 日依據移民法相關規定驅逐出 境。

本案涉及情資分享與整合。依據中華臺北與 A 司法管轄區所簽署之《刑事司法互助協定》（Mutual Legal Assistance in Criminal Matters Agreement），成功完成嫌疑人 A 某之拘捕及遣返。

來源 – 中華臺北

2.18 泰國

案例研究 #105 - 醫療器材與橡膠手套詐騙

詐欺；單獨洗錢案件；電子匯款；購置高價或具文化價值資產

AMLO與泰國皇家警察經濟犯罪防制處（Economic Crime Suppression Division of the Royal Thai Police）合作，共同調查涉及 A 公司之詐欺案件。該公司聲稱係瑞士公司 M 之醫療器材與設備及橡膠手套商標經銷商。並與 B 公司簽訂貿易契約，總金額為 260 萬美元。然至約定交貨日，A 公司卻未如期交付貨物。調查結果顯示，A 公司之實質受益人將詐欺所得用於購置資產。泰國防制洗錢辦公室已暫時查扣並凍結其車輛與銀行帳戶等資產。

來源 – 泰國

案例研究 #106 - 透過自動櫃員機交易進行資恐

可疑交易通報；資恐；現金

B 銀行提出可疑交易報告，A 某之金融交易明顯與其申報收入不符。A 某每月預期收入僅約 8,000 泰銖，然其卻於短時間內透過自動提款機進行多筆交易，總金額超過 600,000 泰銖（約 16,500 美元）。泰國防制洗錢辦公室調查發現，A 某與數起涉及簡易爆裂裝置（IED）案件有關聯。最終 A 某被列為指定制裁名單人士（Designated Person）。A 某之資產已遭凍結，目前並正式被列為資恐案件之涉案人。

來源 – 泰國

案例研究 #107 - 跨國人口販運

人口販運；現金； 電匯

泰國警方逮捕國際刑警組織（INTERPOL）發布紅色通報之嫌疑人 A 某。隨後將其引渡至原籍國 B 司法管轄區。B 司法管轄區法院根據該國刑事法律，判決 A 某人口販運及偷渡移民等罪名成立 A 某係以恐嚇、利誘及勒索手段，強迫外籍女子從事賣淫活動。AMLO展開金融調查，查扣 A 某及其相關人員名下之現金與銀行帳戶等 21 項資產，總值約 2,300 萬泰銖（約 632,000 美元）。目前相關資產沒收程序仍在法院審理中。

來源 – 泰國

案例研究 #108 - 公眾詐欺: 低價套裝旅遊行程。

詐欺；敲詐勒索；使用不動產；使用資本市場；金融機構

某旅行社透過社群媒體廣告，以低價販售國際旅遊套裝行程，吸引多名民眾購買。然而顧客購買後，卻無法出發旅遊。旅行社以簽證核發困難與資金周轉不靈為由，拒絕退款。

AMLO 調查發現，該旅行社透過其他多家公司進行複雜金融交易，並以此不法所得購置銀行帳戶、銀行彩券、不動產、股票、認股權證（Warrants）及衍生性金融商品等資產，價值約 7,500 萬泰銖（約 200 萬美元）。泰國防制洗錢辦公室已依法查扣並凍結上述資產，目前案件仍在法院審理中。

來源 – 泰國

案例研究 #109 - 非法線上賭博

賭博活動；使用虛擬資產；購置高價或具文化價值資產

泰國警方針對 A 某涉嫌經營非法線上賭博網站展開調查。隨後泰國防制洗錢辦公室（AMLO）亦啟動金融調查，已依法扣押並凍結 4 輛超級跑車、1 輛豪華轎車，以及多個銀行帳戶與虛擬資產交易帳戶。前述犯罪所得估計達 2 億泰銖（約 550 萬美元）以上。目前本案仍在法院審理中。

來源 – 泰國

案例研究 #110 - 資助簡易爆裂裝置

資恐；可疑交易通報

B 銀行提出可疑交易報告，A 某之金融交易明顯與其申報收入不符。A 某每月預期收入僅約 8,000 泰銖，然其卻於短時間內透過自動提款機進行多筆交易，總金額高達 600,000 泰銖（約 16,500 美元）。泰國防制洗錢辦公室調查發現，A 某與數起涉及簡易爆裂裝置（IED）案件有關聯，最終將 A 某列為指定制裁名單人士（Designated Person）。A 某之資產已遭凍結，目前並正式被列為資恐案件之涉案人。

來源 – 泰國

案例研究 #111 – 加密貨幣詐欺案

詐欺；使用虛擬資產

A 某自詡為「加密貨幣投資高手」，透過臉書與遊戲直播平台向大量被害人推廣比特幣（Bitcoin）投資組合。A 某聲稱投資人可獲得高達 30% 之高額投資報酬，並透過網路展示匯款記錄截圖取信被害人。初期投資人確實收到若干投資報酬，惟 A 某隨後宣稱銀行匯款出現問題，可能延遲支付投資收益，旋即關閉其臉書帳號及投資平台，導致大量投資人蒙受損失。受害人估計遭詐騙之總金額約為 220 億泰銖（約合 6 億 4,388 萬美元），並向泰國皇家警察報案。A 某已於 2019 年 1 月遭逮捕。

來源 – 泰國

3 洗錢與資恐趨勢

本節涵蓋會員國所提交的資訊，包括 3.1 部分的研究成果與研究報告、3.2 部分關於 2022 至 2023 年間會員國所觀察到之洗錢與資恐趨勢，以及 3.3 部分對防制洗錢及打擊資恐措施有效性之相關觀察。

3.1 近期洗錢與資恐手法及趨勢之研究成果

3.1.1 中國香港

《第二次香港洗錢及恐怖份子資金籌集風險評估報告》於 2022 年 7 月出版。此報告評估 2016 年至 2020 年間最新的洗錢及資恐趨勢。
（https://www.fstb.gov.hk/fsb/aml/en/risk-assessment.htm）

香港警務處財富情報及調查科（Financial Intelligence and Investigation Bureau of Hong Kong Police Force）目前正針對「空殼公司與現成公司」（Shell and Shelf Companies）及「未經主管機關許可之貨幣服務經營者」等領域之洗錢趨勢進行策略性分析。

3.1.2 日本

日本於 2022 年 12 月 1 日發布《國家風險評估追蹤報告 2022》（National Risk Assessment - Follow up Report 2022）。此報告英文版即將出版。

日文版網頁:
https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/nenzihokoku.htm

英文版網頁:
https://www.npa.go.jp/sosikihanzai/jafic/en/nenzihokoku_e/nenzihokoku_e.htm

3.1.3 寮國

寮國於 2022 年重新檢視其《國家風險評估》（National Risk Assessment）報告。指出該國現行常見之犯罪趨勢包括：詐欺、毒品犯罪、偽造或使用虛假文件、竊盜、偽造或使用假幣、非法製作或使用偽造支票或其他貨幣，以及環境犯罪。

3.1.4 中國澳門

2022 年 1 月至 12 月期間，澳門金融情報辦公室（GIF）共接獲 2,199 件可疑交易報告，其中博彩業佔 1,177 件、金融業（包括銀行業、保險業及金融中介機構）佔 765 件，其餘行業佔 257 件。

同期，金融情報辦公室共移送162件可疑交易報告至檢察院（Public Prosecutions Office），由執法機關進一步調查。相關案件多涉及犯罪集團及詐欺。

澳門接獲之可疑交易報告中，所發現之常見洗錢及資恐趨勢包括：

- 異常且大量的現金提款交易；
- 顯著的大額現金存款交易，但資金來源無法核實;
- 頻繁使用自動櫃員機、電話銀行或現金存款機；

- 使用支票或帳戶轉帳等方式進行資金移轉;
- 籌碼兌換交易顯著異常，且幾乎無進行任何賭博活動；
- 涉嫌可疑電匯交易；
- 使用網際網路銀行／網際網路；
- 客戶身分可能符合監控名單或其他黑名單；
- 疑似涉及非法金融活動。

3.1.5 馬來西亞

《納閩風險評估》（Labuan Risk Assessment）

馬來西亞納閩金融服務管理局（Labuan Financial Services Authority, LFSA）已採取多項措施辨識並評估納閩境外金融中心之洗錢與資恐威脅，對該境外金融中心實體進行風險評估。

納閩風險評估於 2021 年進行，並於 2022 年完成，主要目的為：
- 辨識一般與特定風險，以進一步強化金融犯罪風險管理措施
- 確認現行控管措施之有效性程度
- 確定金融部門的殘餘風險
- 提供指導並採取適當策略及措施，以因應已辨識之主要風險並改進政策文件

該風險評估涵蓋:
- 評估弱點與威脅，以確定金融產業之既有有風險
- 經許可（Licensed）及未經許可（Non-Licensed）金融機構

根據評估結果，納閩金融產業因其加強內部控管機制及密集的監理行動，被評為低風險部門。報告建議透過採用金融科技（fintech）優化監理行動、管控主要風險，並強化與利害關係人之互動及提升申報機構能力。此報告已於 2022 年 4 月經國家防制洗錢協調委員會（National Coordination Committee to Counter Money Laundering, NCC）通過，並已與包括NCC成員，及納閩各申報機構在內之相關利害關係人分享。

公告

馬來西亞國家銀行（Bank Negara Malaysia, BNM）於 2022 年持續對特定申報機構發布有關網路犯罪之公告，尤其針對勒索軟體、詐欺、洗錢及資恐趨勢與紅旗指標，以協助申報機構及早偵測、並提交可疑交易報告。該公告旨在因應國內外網路相關勒索犯罪手法之演變。

3.1.6 菲律賓

菲律賓－《資金人頭帳戶態樣簡報》（Money Mules Typologies Brief）
http://www.amlc.gov.ph/images/PDFs/PR2023/2022%20DEC%20TYPOLOGIES%20BRIEF%20MONEY%20MULES_For%20Publication.pdf
該研究係根據菲律賓防制洗錢委員會（AMLC）於 2016 年第一季至 2022 年間所接獲 821,979 件與資金人頭帳戶相關的可疑交易報告（STR）編製而成。該等可疑交易報告累計價值達 5,100 億菲律賓比索。報告指出，涉嫌參與洗錢活動的車手涉及以下行為：

- **透過自助服務終端機（Kiosks）進行之交易：**2019 年 2 月 1 日至 2020 年 9 月 4 日期間，申報義務機構 PQR 針對 2,508 名個人提出共 91,726 筆可疑交易報告（STR），該等帳戶透過設置於連鎖便利商店內之自助服務終端機進行異常頻繁之資金流入與流出交易，涉及金額總計約 5 億 9,396 萬菲律賓比索（約 1,074 萬美元）。由於資金經由數位支付平台快速流入，並透過線上轉帳功能迅速流出，顯示該等帳戶極可能用作過渡賬戶（pass-through accounts）。

- **使用連續編號之行動識別號碼（Mobile Identification Numbers, MINs）進行交易：**申報義務機構 PQR 亦針對 308 名個別客戶提交通報，該等個人於不到 7 個月內進行多筆資金移轉，合計達 6,319 萬 5 千菲律賓比索（約 110 萬美元）。該等款項匯往在另一國內銀行持有帳戶之 A 某。 PQR 發現多數涉案客戶係於 2019 年 11 月至 2020 年 3 月間開立帳戶。該人等及其交易相對人所使用之行動識別號碼（MINs）具連續性，且其「認識你的客戶」（Know Your Customer, KYC）影片背景雷同，因而推斷該人等可能係於同一地點開設帳戶。

- **連續性存提款交易**（詳見此報告第 2 節案例研究 #63）。

- **現金走私活動**（詳見此報告第 2 節案例研究 #67及 #69）。

報告第 3 節分析與資金人頭帳戶相關之可疑交易報告（STR）申報趨勢，發現截至 2022 年此類案件呈現逐年上升態勢。尤其是 2021 年，可疑交易報告（STR）申報量明顯激增，可能因於新冠（COVID-19）疫情期間及疫情後數位銀行與電子錢包之快速普及所致。

抽樣調查之 STR 案例中，有兩項可疑情事比例顯著偏高，分別為「缺乏法律或商業實質義務、交易目的或經濟合理性」及「所涉金額與客戶之營業或財務能力不相稱」。然而，若以涉案金額計，最常通報之可疑情形則為「客戶之身分未經妥善確認」。無論以通報案件數量或涉案金額計算，詐欺皆為最主要之前置犯罪（predicate crime）。

報告亦指出，菲律賓境內可疑資金人頭帳戶主要透過以下三種方式提領資金：電子現金卡、自動櫃員機、及臨櫃提領。此外，多數可疑資金人頭帳戶之持有者居住於馬尼拉都會區（Metro Manila）、黎剎省（Rizal）、新怡詩夏省（Nueva Ecija）、甲米地省（Cavite）、布拉干省（Bulacan）及拉古納省（Laguna）。

根據外匯申報表之彙整數據顯示，2015 年第 1 季至 2021 年第 3 季期間，有 3 人名菲律賓籍人士列名攜帶外幣進出菲律賓之最高額名單。公開資訊顯示，上述資金攜帶者姓氏均為 PQR，涉嫌於 2019 年 9 月至 2020 年 3 月間秘密攜入外幣現金。此等被稱為「PQR集團」人士曾於 2020 年接受國會委員會聽證調查，調查指出僅 2019 年 9 月至 2020 年 3 月期間，該集團未申報即攜入菲律賓境內之外幣金額即高達 6.33 億美元（約 320 億菲律賓比索）。

案例研究 #112 – 資金人頭帳戶涉入資恐案件

現金；資恐

菲律賓防制洗錢委員會（AMLC）資料庫顯示，168 筆資金流入交易、4 筆資金流出交易與 PQR 集團成員有關。該等資金流入與流出交易分別涉及金額 1 億 2 千 430 萬美元與 110 萬美元。據現有資料顯示，PQR 集團成員於 2019 年 9 月至 2020 年 3 月間頻繁自 A 或 B 司法管轄區往返菲律賓。依據機密情資，部分 PQR 集團成員與 C 司法管轄區國民 A 某有所聯繫，該名人士為 EFX 公司之擁有人。EFX 公司為設立於馬卡蒂市（Makati City）之外匯交易商，涉嫌參與資助與伊斯蘭國有關聯之茂德集團（Maute Group），該集團即為 2017 年菲律賓馬拉維市（Marawi City）圍城事件的幕後主導者。

基於上述情形，有理由認為 PQR 集團攜入菲律賓境內之資金可能被用以資助恐怖主義及／或其他不法活動。然而，鑑於 JKI 之外匯業務性質，亦不排除該等交易可能僅為 EFX 日常業務運作之一環。此一推測可由針對 EFX 業務模式蒐集之情報資料作為佐證，指出 EFX 係透過其聯絡人員，直接自位於 A 司法管轄區之 ABC 公司與 B 司法管轄區之 DEF 公司取得外幣現鈔。EFX 選擇以現金方式自境外公司採購美元之原因包括：匯率優惠（ABC 與 DEF 公司提供予 EFX 最低美元賣出匯率）、文件要求較低（相較於銀行，自 ABC 與 DEF 公司購買美元所需文件較少）、資金流動性佳（自 ABC 與 DEF 公司購買之美元可於隔日立即使用）。

AMLC 對 PQR 集團展開調查後發現，PQR-4 與 PQR-2 經常應商業合作夥伴 A 某之要求，運送大量外幣現金。經訪談 PQR-4 與 PQR-2 所得資訊亦證實該指控，顯示兩人曾於 2019 年 9 月 25 日之旅程中試圖隱匿隨身行李內所攜之外幣現金實際金額。

2019 年 9 月 26 日，PQR-6 抵達位於帕賽市（Pasay City）之尼諾伊・艾奎諾國際機場第二航廈（Ninoy Aquino International Airport Terminal II）時，未依法書面申報其攜入之 70 萬美元現金，亦未提供資金來源與運送目的相關資訊。進一步蒐集之情資顯示，PQR-6 曾為境外一家多層次傳銷公司成員，透過該公司累積資金，並於 2019 年與 PQR-4 及 JKI 合夥設立 GHI 公司。GHI 是菲律賓證券交易委員會（Securities and Exchange Commission, SEC）合法登記之公司，主要業務為經營與經銷治療神經及神經肌肉疾病之醫療設備。2021 年，PQR-6 再度投入另一家名為 JKL 之公司，該公司亦於菲律賓證券交易委員會登記，主要業務為批發販售機車防護裝備與設備，以及提供機車維修服務。AMLC 資料庫顯示，PQR-6 涉入最大之交易為 2021 年 7 月 12 日之 3 筆支票存款，總金額達 440 萬菲律賓比索。

來源 - 菲律賓

菲律賓 - 動物走私

菲律賓

案例研究 #113 – 動物走私

環境犯罪

MNO 銀行之客戶 B 某係一名學生，出生於 2006 年，申報之月收入為 1,000 菲律賓比索（約 18 美元），為 A 某之孫女。A 某則為 ABC 寵物用品公司之經營者，月收入約 5 萬菲律賓比索（約 880 美元）。公開資訊顯示，A 某多次遭菲律賓環境與自然資源部（Department of Environment and Natural Resources）、國家調查局（National Bureau of Investigation）及菲律賓國家警察（Philippine National Police）逮捕及起訴，罪名為違反《第 9147 號共和國法》（Republic Act No. 9147，野生動植物資源保育及保護法）。

MNO 銀行注意到，客戶 B 某之帳戶出現大筆金額異常交易，疑似被利用為資金人頭帳戶。根據銀行提供之資訊，B 某於 2017 年 12 月 12 日開設儲蓄帳戶，初始存款餘額即高達 1,983,088.89 菲律賓比索（約 35,000 美元）。其中 1,508,088.88 菲律賓比索被轉存至定期存款帳戶，該定期帳戶於此之前並無其他交易紀錄。此外，B 某與 A 某共同持有另一活躍之聯名帳戶。

B 某之儲蓄帳戶出入資金與其個人背景顯然不符。帳戶資金流入金額介於 10,000 至 620,000 菲律賓比索，流出金額則介於 10,000 至 1,070,000 菲律賓比索。鑑於 B 某於該可疑交易報告提出時年僅 13 歲，銀行推斷該帳戶之資金流動極可能係其祖父 A 某從事非法活動所得之款項。

來源 - 菲律賓

菲律賓 - 被用於暗網之帳戶

根據資料分析，有 24 個銀行帳戶隸屬於 19 名個人被舉報於「暗網」（Dark Web）販售，並作為人頭帳戶（Drop Accounts）使用。

銀行報告指出，該等帳戶可能已被詐騙者用來作為人頭帳戶，以接收其等盜取之憑證（帳號密碼），以及其他贓物販售所得款項。此外，不排除人頭帳戶持有人（money mules）透過該等帳戶接收駭客進行不法轉帳所得資金，並藉由自動櫃員機或匯款代理人（Remittance Agents）迅速將資金提現。

該等帳戶持有人在年齡、性別、資金來源或申報月收入等方面並無明顯共通之處。但郵寄地址則多集中於兩個特定地區。其中 47.36% 帳戶持有人為受僱人員，月收入介於 10,000 至 50,000 菲律賓比索（約 176 至 881 美元）；21.05% 帳戶持有人則為自營業者，月收入介於 10,000 至 250,000 菲律賓比索（約 176 至 4,406 美元）；另有 26.32% 帳戶持有人則聲稱無業，資金來源為津貼或生活費，金額介於 999 至 30,000 菲律賓比索。

其中一申報金融機構指出，某一帳戶之資金流入總額高達 107 萬菲律賓比索，主要來自線上付款、國內外匯款及現金存款。但該等資金亦隨即透過自動櫃員機提領。值得注意的是，該帳戶實際交易活動與持有人聲稱之開戶目的（個人儲蓄）明顯不符。

- ***X 司法管轄區國民詐欺集團之犯罪手法（Modus Operandi）***
- ***愛情詐騙。***
- ***資金快速移轉（Flipping of funds）。***

詳見此報告第 2 節之案例研究。

菲律賓 - 環境掃描：網路犯罪威脅及犯罪者

http://www.amlc.gov.ph/images/PDFs/2022%20SEP%20CYBERCRIME%20THREATS%20&%20PERPETRATORS.pdf

本研究乃根據 2009 年 1 月 1 日至 2021 年 12 月 31 日期間，各受規範金融機構（Covered Persons, CPs）所提交之 30,967 份可疑交易報告（STR）,與非洲大陸某司法管轄區國民所從事之犯罪活動有關，總交易金額達 32 億 6,110 萬菲律賓比索。研究指出，上述犯罪者主要從事以下活動：

- 疑似過渡賬戶
- 涉嫌與銀行駭客事件相關
- 招募資金人頭
- 包裹詐騙

詳見此報告第 2 節之案例研究。

由過去研究與近期報告之環境掃描分析發現，非洲大陸某司法管轄區之國民所涉網路犯罪正逐漸增多。2009 年以來的可疑交易報告（STR）通報案件數量及涉案金額，即可證明此一情形。2020 年受新冠（COVID-19）疫情影響，STR數量較前一年之 2,236 份大幅增加668.2%，達 17,178 份；總交易金額亦由 2019 年之 2 億 7,660 萬菲律賓比索增加 261.1%，達 9 億 9,860 萬菲律賓比索。然而，2021 年之數量及交易金額則略有回落。

依據金融機構提交 STR 之原因，可區分為「可疑情況」（Suspicious Circumstances, SC）及「前 置犯罪」（Predicate Crimes, PC）。值得注意的是，隨著數位化及網路犯罪連結增加，違反《2000 年電子商務法》（*Electronic Commerce Act of 2000*）之情事於數量及交易金額方面均居首位，分別為 7,573 份（佔24.5%）及 6 億 2,340 萬菲律賓比索（佔19.1%）。

此外，本研究依據涉案金額大小、疑似犯罪活動或計畫之通報頻率，以及所涉犯罪之嚴重程度，歸納出數種洗錢態樣（typologies），包括：與帳戶持有人商業背景不符之交易行為；透過過渡賬戶執行之包裹詐欺、網路愛情詐欺及彩券詐欺；未經驗證來源之資金存入；涉入非法毒品交易及非洲毒品集團活動；涉嫌銀行駭客事件'以及，招募資金人頭。

菲律賓 - 網路釣魚／駭客攻擊犯罪手法分析報告

http://www.amlc.gov.ph/images/PDFs/2022%20OCT%20TYPOLOGIES%20BRIEF%20PHISHING%20HACKING.pdf
本研究涵蓋自 2011 年至 2022 年 2 月期間，各受規範金融機構提交之 50,521 份可疑交易報告。主要涉及以下網路釣魚與駭客攻擊活動：

- 帳戶持有人接獲冒充銀行職員來電以套取資訊（電話詐欺範例）
- 帳戶持有人透過電話向第三方洩露資訊（電話詐欺之另一範例）
- 一群可能具有親屬或關聯關係之人員，代表某人收取國際匯入款項
- 客戶以現金提領款項，導致交易缺乏可供查核之軌跡
- 可疑指標：交易金額與客戶之財務能力不相稱
- 可疑指標：缺乏法律或商業實質之義務、目的或經濟合理性
- 涉及電子貨幣機構（EMI）電子錢包之帳戶遭非法接管
- 商業電子郵件詐騙
- 網際網路電子郵件駭客（另一商業電子郵件詐騙案例）
- 社群媒體平台使用者帳戶遭駭客入侵，詳見此

報告第 2 節之案例研究。

涉及網路釣魚/ 或駭客之案件數量，在可疑交易報告中，整體呈現增加趨勢，惟 2020 年則略有下降。提交可疑交易報告多數係基於下列原因：詐欺（swindling）（占 65%）及違反《2000 年電子商務法》（*Electronic Commerce Act of 2000*）（占 23%）。其他可疑指標，例如交易金額與客戶財務或業務能力明顯不相符，也被各受規範金融機構（Covered Persons, CPs）列為提報原因。觀察可疑交易中最常見之交易類型，包括帳戶間轉帳、電子現金卡加值、信用卡消費，以及電子現金卡提款等。

此外，值得注意的是，99.73% 的可疑交易為國內交易，僅 0.27% 為國際匯款交易。在所有境內交易中，有 50.45% 通報來自以下地區：馬尼拉首都圈（Metro Manila）、卡拉巴松大區（CALABARZON）、呂宋中部（Central Luzon）、中部維薩亞斯（Central Visayas）、伊羅戈斯大區（Ilocos Region）、達沃區（Davao Region）及西維薩亞斯（Western Visayas）；而 44.62% 的交易地點因資料不足，屬於不明或無法判定。至於國際匯款，則有 27.21% 交易涉及一個與菲律賓具有歷史淵源之大型司法管轄區。

菲律賓－《網路賭博產業 2020 年風險評估中，對可疑交易報告之詳細分析》（A Detailed Analysis of Suspicious Transaction Reports Captured in the AMLC's Year 2020 Internet-Based Casino Sector RiskAssessment）[21]

此報告為菲律賓防制洗錢委員會（AMLC）2020 年發布之網路賭博產業（Internet-Based Casino Sector, IBCS）風險評估報告之補充資料。該風險評估主要聚焦於，來自 IBCS 領域相關之可疑交易報告，所觀察到的洗錢犯罪類型及可疑指標。自 2013 年 6 月 14 日至 2019 年 10 月 28 日間，受規範金融機構提交之 IBCS 領域相關之可疑交易報告，共計 1,031 份，涉及金額達 140.1 億菲律賓比索（約 2 億 4,600 萬美元）。以下洗錢態樣係彙整自各通報機構所提出之疑似洗錢交易報告（STRs），以及上述已發布的網路賭博產業產業風險評估中之資訊：

- 貨幣服務業涉嫌違反《2000 年電子商務法》
- 缺乏法律或商業實質之義務、目的或經濟合理性
- 交易行為與客戶型態或過往交易明顯不符
- 交易金額與客戶之財務或業務能力明顯不相稱
- 客戶身分未經妥善驗證
- 詐欺（swindling）

詳見此報告第2節之案例研究。

[21] http://www.amlc.gov.ph/images/PDFs/PR2022/ANALYSIS%20OF%20STRS%20CAPTURED%20IN%202020 0%20INTERNET-BASED%20CASINO%20SECTOR%20RISK%20ASSESSMENT.pdf

根據 2013 年至 2019 年網路賭博產業之相關疑似洗錢或資恐交易報告（STR）逐年評估顯示，該期間內之 STR 呈現波動趨勢；2016 年達到高峰，共有 332 份 STR，涉及金額達 88 億菲律賓比索。2013 年至 2016 年間呈現持續上升趨勢，但自 2017 年起至 2019 年逐漸下降。從可疑情境觀察，提交 STR 的主要原因為「缺乏法律或商業實質之義務、目的或經濟合理性」，該項原因計 565 件，占 STR 總數 55%。若以交易金額觀察，則以違反《*2000 年電子商務法*》為主，共涉 49.4 億菲律賓比索，占本研究 STR 總金額之 35%。

此外，本評估發現幾乎所有網路賭博產業（IBCS）之子類別--包括網路賭博許可證持有人（IGL）、網路賭博服務及支援提供者（IGSSP）、菲律賓境外賭博營運商（POGO）以及服務提供商（SP）—均涉及潛在的可疑活動，其中又以服務提供商（SP）類別為最多。觀察到的可疑交易絕大部分為國內交易，主要涉及現金存款／提款、支票存款及匯入/匯出款。此這點引發重大疑慮，因為現金存提款之統計資料與現金交易本身所固有的洗錢風險相符，使用現金進行交易往往會掩蓋稽核軌跡。此外，考量網路賭博產業以網路科技作為其商業模式之本質，大量現金流動明顯偏離該產業之業務模式。

被辨識之交易實體的地理位置集中於馬尼拉市（Manila）、馬卡蒂市（Makati）及卡加延省（Cagayan），上述地區共計有 903 件可疑交易報告，交易總金額約 120 億菲律賓比索，分別占本研究 STR 總件數及金額之 87.58% 及 86.0%。此外，此等可疑交易報告亦涵蓋來自完全位於境外之網路賭博產業實體，以及具境內外雙重地址之外國實體。

菲律賓－《外匯申報制度偵測跨境非法資金流動之效益分析》（An Analysis of the Usefulness of Foreign Currency Declaration in Detecting Possible Cross-Border Transportation of Illicit Funds）[22]

本研究係菲律賓防制洗錢委員會（AMLC）針對 2015 年至 2021 年第一季間所收到之外匯申報書（Foreign Exchange Declarations）進行三階段研究之第一與第二階段結果分析。研究期間 AMLC 共接獲 7,619 份外匯申報書，其中個人旅客提交 5,059 份，法人旅客提交 2,560 份。此報告辨識出可能與洗錢及資恐（ML/TF）相關之可疑活動如下：

菲律賓－賭場相關交易

個人現金攜帶者相關資料顯示，以現鈔方式大量攜入、或攜出菲律賓之外幣資金與賭博產業有關。此結論係基於研究期間所蒐集之外匯申報表，按申報外幣折合美元價值排序之前四名個別現金攜帶者的交易情形分析得出。

該等現金攜帶者均來自國外司法管轄區。研究期間觀察到國外現金攜帶者於境內購買之外幣數量，與其外匯申報書所載之外幣總值間存在明顯落差 尤其涉入金額龐大，令人質疑大量現金走私（bulk-cash smuggling）之可能性。

[22] http://www.amlc.gov.ph/images/PDFs/USEFULNESS%20OF%20FX%20DECLARATIONS%20IN%20DET ECTING%20POSSIBLE%20CROSS-BORDER%20TRANSPORT%20OF%20ILLICIT%20FUNDS.pdf

菲律賓—異常頻繁之旅行

透過跨境外匯申報資料發現，有 5 名個人現金攜帶者於 2019 年 12 月至 2020 年 3 月間，共計入境菲律賓 38 次，該等人士於申報中表示所攜現金係用於賭場賭博。短短約 4 個月內，該 5 名現金攜帶者共計攜入金額約 6,090 萬美元（詳見此報告第 2 節案例研究 #78）。

菲律賓—申報資訊前後不一

資料庫顯示，2015 年至 2021 年間，一位位居前茅的菲律賓籍大額現金攜帶者，其所提交之資料存在顯著不一致性。其中最明顯的包括姓名拼寫差異，以及出生日期、住址與護照號碼不同。

另一種可疑交易模式來自前往 A 司法管轄區進行宗教朝聖活動之個別旅客。涉及於 2015 年兩個不同日期出發前往 A 司法管轄區的兩組、各 10 名居民。根據提交資料，該等旅行者於兩次旅程中，共攜帶沙烏地阿拉伯里亞爾（SAR）390 萬及科威特第納爾（KWD）50 萬。金融調查進一步顯示，其中部分人士於 ABC 銀行之帳戶曾有連續存款並於同日提領。外匯申報書所申報之金額高於其實際提款金額。

3.1.7 泰國

泰國防制洗錢辦公室（AMLO）於 2022 年 8 月透過官方網站公布《國家風險評估》（NRA）。報告全文請參閱：
https://www.amlo.go.th/amlo-intranet/media/k2/attachments/NRAYThailandYforYPublicationYEnglish_6112.pdf

泰國防制洗錢辦公室針對洗錢及資恐手法和趨勢進行研究，並向公共及私營部門發布相關報告與態樣分析，內容如下；

- 案例研究：Baan Eua Arthorn 公共住宅計畫詐欺案之洗錢模式。
- 態樣分析報告：跨國野生動物非法販運所得之洗錢手法。
- 案例研究：鐵路俱樂部儲蓄合作社（Railway Club Savings Cooperatives）詐欺案之洗錢行為。
- 案例研究：Mae Manee 龐氏騙局（公共詐欺）案之洗錢行為。
- 態樣分析報告：透過導遊業務以洗錢方式處理公共詐欺所得。
- 案例研究：膳食補充品與旅遊套裝行程詐騙案

3.2 新興趨勢、下降趨勢與持續趨勢之觀察

3.2.1 中國

中國報告指出，包括電信詐騙在內的網路犯罪案件日益猖獗，而與此等犯罪相關之洗錢手法呈現出跨國性與組織化犯罪交易之特徵。

此外，網路博弈已成為組織化賭博犯罪之主要形式，其犯罪模式涉及廣告、組織、博弈及資金結算等完整產業鏈。

地下匯兌（哈瓦拉匯款系統，Hawala）持續成為電信詐欺、網路賭博及貪腐等犯罪所得洗錢之管道。

3.2.2 庫克群島

庫克群島通報之新興犯罪趨勢包括：利用網路的金融犯罪、網路賭博、詐欺（未經授權之帳戶存取）、官員貪腐及臉書詐騙。持續觀察到之趨勢則包含：電子郵件詐騙與投資詐欺。

3.2.3 中國香港

香港通報之新興犯罪趨勢包括：
由於科技日新月異、電子金融服務普及及 COVID-19 疫情期間實施之社交距離措施，使用網際網路、電子郵件及社群媒體所為之前置犯罪（Predicate Offences）日益常見。

亦觀察到儲值支付工具（Stored Value Facilities, SVFs）遭濫用之情形日益增加：

- 犯罪分子利用盜用之身分證件申請開設儲值支付帳戶，以轉移犯罪所得。
- 儲值支付工具有時被賭博集團用於接收來自賭客之投注款項。

中國香港於 2020 年 3 月推出首家虛擬銀行。目前已有 8 家經許可之虛擬銀行，透過網路及其他電子管道提供零售銀行服務。然而，隨著遠端開戶程序之普及，虛擬銀行帳戶涉入犯罪活動之情形亦隨之增加：

- 犯罪分子招募人頭開設虛擬銀行帳戶。
- 部分洗錢集團或人頭使用偽造身分文件進行帳戶認證。

中國香港通報之持續趨勢包括：
詐欺相關犯罪仍為最常見之犯罪類型，其次為毒品犯罪。其他前置犯罪如境外逃漏稅、及境外貪腐案件之數量維持平穩。
銀行業仍為最常被用於洗錢活動之管道。透過第三方進行洗錢犯罪所得仍為常見手法：

- 洗錢集團招募非本地居民、學生及低收入人士作為「人頭」，以少量報酬利誘其開設銀行帳戶。
- 部分案件中，招募人頭之行為本身即屬於求職詐欺（employment fraud）。
- 近期亦發現外籍家庭幫傭被招募為人頭帳戶之情事。

衰退趨勢方面：

新冠（COVID-19）疫情期間跨境旅客人數顯著減少，導致跨境現金運輸活動亦隨之下降。

3.2.4 印尼

網路詐欺風險評估

印尼於 2022 年 6 月發布《網路詐欺犯罪洗錢之產業風險評估報告》（Sectoral Risk Assessment of Money Laundering on Cyber Fraud Crime）。該風險評估指出涉及網路詐欺之類型或特徵，包括商務電子郵件詐騙，以及私人企業、或個人所主導之投資詐騙。其中社交工程犯罪者（Social Engineers）被評為高風險肇事者。

與網路詐欺相關之洗錢樣態包括：

- 使用偽造之身分證明文件。
- 開設新帳戶以接收犯罪所得。
- 使用其他人（已知、未知或虛構人士）之人頭帳戶。
- 使用現金之交易模式。
- 以公司或個人名義接收匯款，偽裝成正常商業交易之情形

《印尼籍境外恐怖主義戰鬥人員資恐風險評估》（Risk Assessment of Terrorism Financing by Indonesian Foreign Terrorist Fighters）

印尼於 2021 年發布有關境外恐怖主義戰鬥人員（FTF）之資助恐怖主義風險評估。根據分析結果，提出以下結論：

- 募款模式包括：向他人募款、自行出售資產（例如房屋、汽車）及透過社群媒體進行募款。
- 資金移轉模式包括：攜帶現金、透過非銀行之有照資金移轉業者進行轉帳、國內現金提領以及使用銀行服務。
- 資金使用模式：資金通常由第三方或家庭成員使用，以協助相關人員之旅行。

貪腐風險評估更新

印尼於 2022 年更新針對貪腐的《部門風險評估》（Sectoral Risk Assessment）。前次貪腐部門風險評估於 2017 年完成。依據對各評估項目之威脅、弱點與影響後果等因素分析後，得出以下結論：

- 國家財政易受高度貪污風險影響。
- 具有高度風險從事透過貪污犯罪進行洗錢的個人行為人（individual perpetrators）包括，公務人員（含退休人員）、私人企業員工、企業家/商人，以及立法與政府機構官員。
- 具有高度風險從事源自貪污犯罪洗錢的商業實體特徵，主要為有限責任公司（PT）形式之公司。
- 銀行已被確認為易遭貪污犯罪行為人利用進行洗錢犯罪所得的高風險機構。
- 基礎建設領域具備源自貪污犯罪洗錢之高風險。
- 犯罪者之交易模式，包括帳戶記帳、購買或投資產品及透過手機銀行進行轉帳，皆屬用於貪污犯罪洗錢之高風險類別；
- 貪污犯罪行為人所使用之洗錢態樣包括：利用企業法人；使用人頭（借名）、信託、家庭成員或第三方；透過不動產（含房仲業者角色）；以及混合方式（將非法資金融入合法業務中）。

稅務風險評估更新

印尼於 2022 年更新稅務領域之《部門風險評估》（前次評估為 2017 年）。透過稅務系統辨識出的常見洗錢態樣包括：自行洗錢（Self-laundering），國內資金來源；將資產存放於銀行；購置房產；透過租賃方式購置車輛；投入商業資金。

持續存在之透過稅務犯罪洗錢風險包括：

- 濫用不實稅務發票（TBTS）／稅務發票。
- 虛假的年度稅務申報。
- 以非存款方式收取資金。

跨境現金攜帶之風險評估

印尼於 2022 年 7 月發布《跨境現金攜帶之洗錢與資恐風險評估》報告。該風險評估乃基於對貨幣關注點、交通運輸方式、現金攜帶之來源國與目的地國、現金攜帶者之特徵，以及監管跨境現金攜帶之主管機關所進行之分析。

根據各關切點之威脅、弱點與後果因素分析，研究結果如下：

- 新加坡元（SGD）與美元（USD）屬於跨境現金攜帶高風險貨幣，阿拉伯聯合大公國迪拉姆（AED）屬於中等風險貨幣。
- 空運方式帶來高度跨境攜帶現金之風險。
- 風險評估辨識出作為跨境現金攜帶來源或目的地的之高風險或中等風險司法管轄區。
- 外匯兌換公司及其員工為常見高風險跨境現金攜帶者，而私營貿易商員工、企業家及銀行業從業人員則屬於中等風險跨境現金攜帶者。
- 蘇加諾-哈達國際機場（Soekarno-Hatta International Airport）、巴淡島（Batam）渡輪碼頭及伍拉·賴國際機場（I Gusti Ngurah Rai International Airport）為跨境現金攜帶之高風險區 域。

非營利組織（NPO）被濫用作為資恐管道之風險評估更新

印尼於 2022 年 7 月更新非營利組織（NPO）之風險評估。上次風險評估為 2019 年。目前印尼在防範與消弭透過非營利組織資恐方面存在以下動態與挑戰：

- 越來越多非營利組織已取得法人資格。
- 非營利組織遭內外部濫用情形持續增加。
- 非營利組織透過社群媒體進行募款活動增加，且難以依據營運區域確認其等是否實際存在。
- 非營利組織財務管理問責性不足，尤其是其所管理之公共資金。

3.2.5 日本

日本已辨識出多起企圖進行洗錢之案件，犯罪者要求受害者透過國內匯兌交易，將款項匯入虛構或第三方名義之銀行帳戶，藉此快速且安全地轉移資金。

被濫用於洗錢之主要交易型態

年 \ 被濫用交易	國內匯兌交易	現金交易	存款交易	信用卡	電子貨幣（Electronic Money）	法人	加密資產	國際交易（例如換匯）	資金移轉服務	貴金屬與寶石	郵件代收服務（Postal receiving service）	法務/會計專業人士	外幣兌換	金融工具	總計（案件數量）
2019	160	61	31	15	12	14	2	14	6	3	3	1	0	0	322
2020	110	120	96	20	12	14	32	16	1	2	0	1	1	0	425
2021	208	72	40	40	23	16	9	9	9	2	0	1	1	2	432
總計（案件數量）	478	253	167	75	47	44	43	39	16	7	3	3	2	2	1,179

根據《特定毒品犯罪特別規定法》偵破之洗錢案件

2021 年依據《特定毒品犯罪特別規定*法*》*（Anti-Drug Special Provisions Law）*偵破之洗錢案件總數為 9 件。在部分案例中，透過毒品犯罪（例如興奮劑走私）所取得的資金被以洗錢方式處理。該等案例中，犯罪者要求客戶將支付非法毒品之款項存入以他人名義開立的銀行帳戶。

3.2.6 寮國

2022 年，寮國從申報機構收到的可疑交易報告顯示以下持續趨勢：

- 使用個人帳戶進行商業活動。
- 進行高額交易卻無充分理由。
- 未提供或迴避提供充足的資訊。

3.2.7 中國澳門

執法機關觀察到的洗錢與資恐趨勢：

洗錢趨勢

- 2022 年博弈相關犯罪有所減少，主因為旅客數量與博弈活動降低。
- 司法警察局（PJ）正密切關注：「練習券」詐騙手法的再度出現。
- 因應免檢疫通關措施全面實施、及國際航班逐步恢復，司法警察局持續關注可能再度出現利用人體夾帶及行李藏匿方式進行毒品走私之情事。
- 司法警察局自 2018 年開展專項網路犯罪調查以來，2022 年首次呈現案件數量下降趨勢。此下降趨勢，研判為一系列防範措施綜合發揮成效，以及民眾防制犯罪意識提升所致。其中，竊取信用卡資訊進行網路消費等電腦詐騙案件數量顯著減少。
- 然而，網路詐欺案件仍持續增加。涉及網購及色情服務陷阱的詐騙案件相對明顯增加，造成居民與商家損失。此外，色情勒索詐騙及電話詐騙案件的數量亦逐年增加–此逐年增加之趨勢可能與新冠（COVID-19）疫情期間社群媒體使用日益增多有關。

- 司法警察局於 2022 年採取多管齊下的方式，加強防範詐欺並改善反詐欺機制，期望為公眾提供更強有力的保護。司法警察局持續與本地銀行業合作，採取預防措施，於可疑匯款發生前即加以阻止，並與海外警察合作；截斷跨境詐欺資金的流動。

資恐趨勢

近年觀察到東南亞地區的非營利組織（NPO）遭濫用於資恐活動，引發關切。司法警察局對此保持警覺並持續進行威脅分析。除金融機構持續採取風險基礎方法以防制資恐及持續觀察可疑資金流動外，司法警察局於 2020 年 10 月成立專門的反恐調查部門，積極分析及調查匯往高風險司法管轄區的資金。截至目前，並未發現任何調查與資恐相關，整體趨勢保持穩定。

3.2.8 馬來西亞

馬來西亞仍持續面臨詐欺活動的風險，特別是電信詐欺。為因應電信詐欺案持續增加的趨勢，以及整體詐騙案件的同步上揚，馬來西亞於 2022 年 10 月 12 日成立國家詐騙應對中心（National Scam Response Centre, NSRC），旨在打擊線上金融詐騙，透過專門平台快速追蹤與攔截資金，讓受害者更容易通報案件。

國家詐騙應對中心（NSRC）是由 2021 年設於馬來西亞皇家警察（RMP）商業罪案調查部之「反詐騙中心」所升級成立之機構。其為馬來西亞皇家警察（RMP）、馬來西亞國家銀行（金融情報中心，FIU）、馬來西亞通訊與多媒體委員會、國家反金融犯罪中心（NFCC）、金融機構及電信業者共同合作成立；並作為一個全國性、多機關協調之公開溝通及詐騙應對協調平台。

透過設置專線服務並促進各合作機關之密切協作，該詐騙應對中心得以有效強化對線上詐欺/詐騙案件之即時應對能力。2022 年 10 月 12 日至 2023 年 1 月 31 日期間，國家詐騙應對中心共收到 16,752 件投訴，因此開立 751 件詐欺犯罪調查案卷，及 24 件洗錢犯罪調查案卷。

有關國家詐騙應對中心的進一步資訊可參考網站：
https://nfcc.jpm.gov.my/index.php/en/soalan/about-nsrc

3.2.9 索羅門群島

根據 2022 年收集的疑似洗錢交易報告，索羅門群島出現的新興趨勢之一，便是日益猖獗的身分盜用案件。大多數的身分盜用、或冒名案件與網路詐騙及透過網路進行的資金人頭活動有關。

金融情報中心於 2022 年持續觀察到被舉發的逃漏稅及網路詐騙案件。在逃漏稅案件方面，使用個人銀行帳戶進行商業交易，仍然是行為人規避稅務的常見手法。而在網路詐騙案件方面，最常見的情況是受害者透過社群媒體結識陌生人士，最終因各種詐騙手段蒙受大量金錢損失

3.2.10 菲律賓

菲律賓近期就洗錢與資恐之手法及趨勢所進行的研究與調查，包含新興、下降及持續趨勢之觀察。為求簡潔，上述內容已於此報告第 3.1.6 節摘要說明。

3.2.11 中華臺北

人口販運犯罪集團

近期中華臺北警察機關接獲多起報案，指稱境內犯罪集團與 A 司法管轄區的人口販運集團合作，透過臉書及其他社群媒體管道，以博弈客服、貸款服務、男性色情演員等高薪職務為誘餌，吸引民眾簽署勞動契約前往 A 司法管轄區工作。受害者抵達當地後即遭限制人身自由，並遭脅迫從事網路詐欺及電話詐騙等非法活動。警方調查，該集團運作模式係安排受害者入住指定飯店辦理相關文件後，再由集團成員陪同護送至機場，搭乘班機前往 A 司法管轄區。2022 年 5 月 5 日，警方於機場救出 3 名即將出境之受害者，並當場逮捕 3 名嫌疑人。經檢察官聲請，法院裁定羈押獲准。警方當場逮捕三名嫌疑人，經檢察官聲請羈押後，法院裁定准予羈押。

深入追查一個多月後，警方於 2022 年 7 月 5 日同步搜索 10 處犯罪據點，成功瓦解由 A 某領導之人口販運犯罪集團，當場逮捕 6 名嫌疑人。並扣押電腦 8 台、筆記型電腦 1 台、模擬槍枝 1 把、空包彈 100 發、點鈔機 1 部、A 司法管轄區之僱傭契約、銀行存摺、本票及借據（IOU）等證物。經偵查後，警方依涉嫌觸犯《刑法》第 297 條（意圖營利，以詐術使人出國外罪）及違反《*組織犯罪防制條例*》等罪嫌，將嫌疑人移送檢察署偵辦。該六名嫌疑人經法院裁定准予羈押。

LINE 群組投資詐欺案件

刑事警察局（CIB）經分析民眾通報資訊後發現，犯罪集團利用 Instagram（IG）、臉書及 YouTube 等社群媒體平台刊登投資廣告，附上投資平台連結與客服 ID，誘導民眾點擊觀看。犯罪集團以「投資規劃」、「被動收入」、「兼職賺錢」、「保證獲利不虧損」、「操作簡單，加入門檻低」及「輕鬆賺錢，邊玩邊賺」等宣傳口號，誘使民眾點擊連結並於即時通訊軟體加好友。受害人加入 LINE 群組後，詐騙集團成員便會主動私訊表示：「你需要錢嗎？我可以幫你賺錢」、「我可以教你如何投資賺錢」、「免費盈利專案」、「免費協助投資外幣」等。誘騙受害者註冊虛假投資平台，並加入 LINE 群組。其他詐騙集團成員會假扮投資者，在群組營造聽從「導師」或「首席導師」指導，進行加密貨幣、外匯、期貨投資即可輕鬆獲利的假象。受害者被蠱惑匯款投資後即遭詐騙。待其等發現受騙時，詐騙集團成員隨即封鎖被害人帳號，將之自 LINE 群組中移除，或不再回應訊息。該犯罪集團自 2021 年 10 月至 2022 年 1 月間運作約 4 個月。警方共接獲約 20 至 30 名受害人報案，初步估計詐騙金額超過新台幣 1,000 萬元，其中單一受害人最高損失達新台幣 260 萬元。

經過數月調查蒐證，警方於 2022 年 1 月 19 日同步搜索該詐欺集團據點（兩處機房）。13 名詐騙集團成員，包含假扮投資人及假扮指導老師之成員，當場遭警方逮捕並依詐欺罪移送偵辦。檢察官偵訊後向法院聲請羈押主嫌 A 某，經法院裁定後准予羈押。警方經近 3 個月追蹤、調閱

並分析數百支監視器畫面，同時針對全國多處可疑地點進行搜索及埋伏、夜間監控後，於 4 月初確認另一主嫌 B 某及其他嫌疑人藏匿於偏遠鄉間農舍。警方於 4 月 8 日取得搜索票後前往搜索，當場逮捕嫌疑人。B 某及另一名嫌疑人經檢察官偵訊後聲請羈押，並立即獲法院核准。

3.2.12 泰國

在洗錢犯罪方面，泰國觀察到虛擬資產相關詐騙、及利用虛擬資產洗錢成為新興趨勢。

持續趨勢包含：
- 利用人頭帳戶進行洗錢。
- 透過社群媒體進行龐氏騙局式詐欺。
- 以人頭或第三方名義購置不動產及奢侈品方式進行洗錢。
- 透過股票市場或共同基金進行洗錢。
- 利用未受監管之虛擬資產交易所進行洗錢。
- 透過現金攜帶者進行洗錢。
- 透過地下匯兌（underground banking）進行洗錢。
- 利用貿易活動進行洗錢。
- 經由電子貨幣（e-money）及電子支付服務進行洗錢。
- 透過空殼公司及合作社進行洗錢。

泰國指出，使用自身帳戶之線上銀行服務進行洗錢呈下降趨勢。

在資恐方面，泰國觀察到以合法來源自我籌資及利用網路、銀行成為新興趨勢：

持續趨勢包括:
- 透過社群媒體籌集資金。
- 透過犯罪活動籌集資金。
- 利用外國司法管轄區業務籌集資金。
- 透過非營利組織（NPOs）籌資。
- 利用第三方帳戶或第三方轉移資金。
- 透過現金運送者轉移資金。

泰國指出，利用空殼公司進行資恐之趨勢已呈下降趨勢。

3.2.13 越南

越南於 2022 年觀察到網路空間之前置犯罪明顯增加。其中包括財產侵占罪及組織賭博罪。

越南公安部發現多起涉及網路空間之犯罪路徑及洗錢案件，並於 2022 年 8 月偵辦一起涉外人士之「利用電腦網路、電信或電子方式侵占財產及洗錢」案件。此外，河內市警方亦偵辦另一起透過網路詐欺手法侵占財產及洗錢之案件。犯罪手法則以網路邀約方式，誘導民眾進行「輸入資料賺錢」活動，藉以洗錢。

隨著 4G 技術的發展，預期整體網路犯罪趨勢，特別是洗錢及資恐案件，將持續增加並更加複雜。

3.3 防制洗錢及打擊資恐法規與執法措施之成效

3.3.1 中國香港

由於金融機構持續強化客戶盡職調查（Customer Due Diligence, CDD）措施，提升對各類法人實質受益人資訊之掌握程度，透過境外公司進行洗錢活動之情形已逐漸減少。

3.3.2 日本

存款機構及信用卡業務機構，就其所受理之日本籍個人及法人之帳戶或相關交易（包含遭拒絕開戶或交易之情形），提出可疑交易報告（STR）情事包含：

- 客戶資料老舊長期未更新，卻接獲大量國際匯款轉入帳戶 之情形。
- 帳戶出現非預期之大量資金轉入，或自國外匯入大額資金。
- 自國外匯入資金時聲稱係合法交易，惟無法提出有效證明文件。
- 因涉及詐欺行為而收到外國銀行提出資金返還之請求。
- 該帳戶疑似涉入境外司法管轄區發生之詐欺案件。
- 該帳戶已遭主管機關列管凍結。
-

根據上述資訊，發現部分帳戶已涉及跨國詐欺案件。包括帳戶持有人在內之多名相關人士，因涉違反《有組織犯罪處罰法》*（Act on Punishment of Organized Crimes）*（隱匿犯罪程序）等罪名，已遭拘捕法辦。

用於調查目的之 STR 件數

	2019	***2020***	***2021***
調查使用的 STR 件數	***307，786***	***325，643***	***353，832***

4 資武擴之手法與趨勢

本節《態樣報告》來自聯合國專家小組（Panel of Experts）2022 年 9 月、 2023 年 3 月及 2023 年 9 月所發布報告之簡要概述，並彙整成員國提供之有關防制資武擴（Proliferation Financing, PF）風險評估、以及出版品與風險防制指引相關資訊。此外，成員國並提供四個實務案例供參考。

4.1 近期有關資武擴手法及趨勢之風險評估、研究或調查報告

聯合國專家小組 2022 年 9 月 7 日中期報告（文件編號：S/2022/668）

聯合國安全理事會發布專家小組（PoE）中期報告。

此報告指出，北韓（DPRK）持續加速推進其飛彈計畫，並宣稱已開發出「戰術核武」。專家小組亦觀察到，該國持續並發展新的非法石油進口與煤炭出口手法。報告檢視貨輪經改裝後用於運輸石油，並於北韓領海進行非法貨物的直接交付與船對船轉運（ship-to-ship transfers）之具體證據。

此外，非法網路活動亦為北韓另一重要收入來源。2022 年發生兩起重大網路攻擊事件，其中一起已確認為北韓所為，造成數億美元資金遭竊。此外，其他網路攻擊則以竊取機密資訊為目標，以支援北韓包括大規模毀滅性武器（Weapons of Mass Destruction, WMD）在內之違禁計畫。

此報告並提出 7 項建議，內容涵蓋教育宣導、資訊溝通、強化監管控制措施，以及促請成員國落實 FATF 有關虛擬資產之指引，以防制資武擴、洗錢與資恐活動。

聯合國專家小組 2023 年 3 月 7 日最終報告（文件編號：S/ 2023 /171）

2023 年 3 月 7 日，聯合國安全理事會發布專家小組 2022 年度最終報告。

2022 年，北韓持續發展聯合國禁止之彈道飛彈及核武計畫，全年至少發射 73 枚彈道飛彈及結合彈道與導引功能之飛彈，並宣布採行新的「核武先制使用」（first-use doctrine）政策，且宣稱其核武國家地位具「不可逆轉性」。

報告指出，北韓大幅加速取得貨輪及其他船隻，藉此直接及透過船對船轉運方式進口精煉石油，並出口煤炭，嚴重違反聯合國制裁規定。

北韓透過網路攻擊所獲非法收入超越歷年。2022 年北韓官方支持之網路威脅攻擊者透過勒索軟體（Ransomware）及惡意軟體（Malware）攻擊方式，竊取價值達 10 億美元之虛擬資產。此外，虛擬竊取非同質化代幣（Non-Fungible Tokens, NFT）亦逐漸成為北韓之新興非法收入來源。

除了重申先前提升「資安衛生」（cyber-hygiene）之建議外，另建議指名一位支持北韓違禁武器計畫之人士，擔任一個聯合國指定組織的主管職務；該組織涉及透過網路從事非法收益活動及敏感資訊之取得。

聯合國專家小組 2023 年 9 月 13 日中期報告（文件編號：S/2023/656）

2023 年 10 月 27 日，聯合國安全理事會發布專家小組 2023 年 9 月 13 日之中期報告。

此報告包含一系列個案研究與調查，內容涉及北韓持續違反、及規避聯合國對北韓制裁之情事，並涵蓋相關金融制裁面向。

報告指出，北韓持續違反聯合國安全理事會相關決議，透過各種非法金融操作，持續進入國際金融體系。聯合國專家小組查訪北韓境外之金融機構及國家代表（包括銀行機構代表）參與支援此類活動的情事。報告進一步提及，隨著邊境重啟，北韓國民以人工方式跨境攜帶現金及高價值物品之案件可能增加。專家小組調查多起涉及北韓國民違反制裁規定，在海外從事資訊科技、餐飲、醫療及建築等行業並取得收入之情事。此專家小組持續調查涉及北韓之合資企業、合作組織、非法商業活動，以及涉嫌輸出北韓軍用通訊設備、武器彈藥及其他商品之情事。最後，報告特別強調，北韓官方支持之駭客透過網路犯罪活動非法取得收入之手法更趨複雜，據報導，2022 年透過網路犯罪竊取之加密貨幣總額近 17 億美元。

中國香港

香港已完成第二次《洗錢及*資恐風險*評估》，並於 2022 年 7 月 8 日發表評估報告。此報告為中國香港第二次洗錢及資恐風險評估，亦為首次針對資武擴（Proliferation Financing, PF）所進行之風險評估。

本次報告根據以下重要調查結果，評估中國香港於資武擴威脅及弱點之風險等級為中低度：

- 截至 2021 年底，聯合國安全理事會及其相關委員會之制裁名單未列入任何居於、或登記於中國香港之個人或營運企業。執法機關深入調查後，亦未發現中國香港境內存在資武擴之證據。
- 儘管如此，中國香港作為國際金融、貿易及運輸中心，且鄰近北韓與伊朗，亦認識其可能暴露於外部資助擴散威脅之下。
- 透過完備的反資助擴散制度，包括健全之法規體系，以及涵蓋政府機關、監理機關及私部門之制度架構，以有效降低任何可能存在之弱點。

可以在此下載《風險評估》報告: https://www.fstb.gov.hk/fsb/aml/en/risk(風險)-assessment.htm

除風險評估外，香港聯合財富情報組（Joint Financial Intelligence Unit）亦定期發布可疑交易報告（STR）季度分析報告與紅旗指標。該等專題策略分析報告促進資武擴（PF）之情資交流，協助執法機關採取行動，並提供制定資助擴散防制政策及法規之重要參考。

印尼

印尼於 2020 年進行資武擴風險評估，考量其與北韓及伊朗既有之外交與經貿往來，判定該國面臨中等程度之風險。此等關係涵蓋外交層級之政治互動、商業合作及人際往來。

印尼已採取多項措施降低風險，包括對指定個人及實體資產之凍結權限；目前印尼整體風險與弱點評估為低。

新冠（COVID-19）疫情期間，印尼進一步辨識出涉及醫療、化學及生物材料跨境交易量遞增之風險。

雖尚未發現與制裁名單上之指定個人或實體有直接關聯的案件，但 2018 年至 2022 年間，印尼海關總署（DGCE）已對與伊朗及北韓進出口交易相關之資武擴案件採取執法措施，共計 113 次，扣押資產總價值達 26.8 億印尼盾。

中國澳門

澳門於 2022 年參照皇家聯合軍事研究所（RUSI）「資武擴快速風險評估工具」（Proliferation Financing Rapid Risk Assessment Tool），完成資武擴風險評估。

該評估考量下列因素：

- 聯合國安全理事會（UNSC）專家小組關於北韓及伊朗之相關報告。
- 其他司法管轄區之資武擴風險評估結果。
- 人口統計及地理鄰近性分析。
- 疑似洗錢交易報告以及涉及資武擴相關犯罪案件分析。
- 所扣押之化學品、武器及彈藥統計數據。
- 進出口資料及軍民兩用物資之分析。
- 既有法律架構與控制措施。

自中國澳門於 2016 年實施《資產凍結制度》（第 6/2016 號法律）（Asset Freezing Regime Law no. 6/2016）以來，迄今未曾執行與資武擴相關之資產凍結措施，亦無任何涉及資武擴之案件遭提起公訴。

《資產凍結制度》要求金融機構及指定之非金融事業或人員（DNFBPs）對列名於資武擴制裁名單之個人及法人，依法採取資產凍結管制措施。監理機關已就資產凍結要求，與金融業及博弈產業建立有效溝通機制。

迄今未發現中國澳門境內有違反、未落實或規避 FATF建議第 7 項所規定之目標性金融制裁相關義務之情事。

整體而言，中國澳門之資武擴風險評估結果為低，既有風險暴露程度低，且現行控制措施足以有效降低相關風險。

菲律賓

菲律賓已辨識出在執行資武擴之針對性金融制裁（Targeted Financial Sanctions）措施方面之若干缺口，包括缺乏針對資武擴之盡職調查分析程序、相關情報蒐集與處理程序，以及專門調查方法等。菲律賓 亦認為有必要針對特定對象，包括指定之非金融事業或人員（DNFBPs）、出口商及經紀業者，進一步推廣宣導並提升其認知。此等措施對於未來相關法規正式施行後，能有效落實在資武擴上之目標性金融制裁，至關重要。

戰略貿易管理辦公室（Strategic Trade Management Office, STMO）已與洗錢防制理事會秘書處（AMLCS）合作，依據防制洗錢金融行動工作組織（FATF）建議第 7 項，提出具體執行機制。具體而言，已提出防制資武擴之立法建議，但仍需建立相關法規及作業機制，以監督遵循情形並對違規行為實施制裁。

新加坡

新加坡於 2013 年進行洗錢／資恐風險評估時，已納入資武擴風險考量，並持續透過跨部門「風險與態樣跨部會工作小組」（Risks and Typologies Inter-Agency Working Group, RTIG）對相關風險進行檢討與評估。RTIG 於 2017 年成立，專責辨識與檢視新加坡洗錢、資恐及資武擴之風險。相關主管機關透過與產業界之交流互動、及主管機關發布之指引，傳達資武擴之主要風險。

因應 FATF 標準之修訂，新加坡正透過國家級資武擴風險評估（Proliferation Financing National Risk Assessment, PF NRA）更新其對該風險之理解。為確保該風險評估涵蓋 FATF 建議之各項要素，新加坡將此風險評估納入 RTIG 跨部門框架執行，參與單位涵蓋執法機關、金融情報單位及主管機關，並參考產業界回饋及公私部門間之資訊交流之資訊。此外，新加坡在防制洗錢及打擊資恐產業合作架構（AML/CFT Industry Partnership）下成立專責工作小組，特別向金融機構（如銀行及保險業）、及指定之非金融事業或人員（如公司服務提供商）徵詢意見。

中華臺北

自 2017 年 1 月至 2022 年 10 月，中華臺北檢察機關共偵辦 11 起涉及違反聯合國對北韓制裁之案件。其中 5 起判決有罪、3 起判決無罪，另 3 起案件未予起訴。涉及資武擴最常見之犯罪態樣，是由中華臺北石油公司所控制之第三司法管轄區船舶，在公海上將石油轉運予北韓籍船舶，或先轉運予第三司法管轄區船舶後，再由該第三司法管轄區船舶轉售予北韓籍船舶。此外，亦發現中華臺北國籍人士違反聯合國制裁，自北韓購買無煙煤（煤炭），再轉售至其他國家之案例。

石油產品仍為中華臺北國籍人士違反聯合國制裁規定交易最常見之商品。依中華臺北法律，於公海上交易油品本身並不違法。然而，包括外國人士在內的船務公司代表或實質受益人，以及各種中介機構與複雜商業結構之參與，經常以合法交易掩飾非法油品轉運之行為。此外，犯罪分子亦透過提供虛假出口資訊，並利用境外公司及帳戶妨礙資金追蹤。

依據《資恐防制法》第 9 條第 1 項第 1 款之主觀構成要件，須證明被告對象係「明知」與受制裁標的進行交易，但因中介人介入，使該要件之證明相當困難。

雖已發現涉及違反中華臺北《貿易法》對伊朗相關規定之案件，惟該等案件僅係廠商出口未經許可之戰略性高科技商品，並無發現涉及資武擴之情形。

泰國

泰國之《國家風險評估》於 2022 年發布關於資武擴的風險評估。此報告判定泰國之資武擴風險屬於低級別。主要潛在之資武擴手法包括規避制裁、以及涉及軍民兩用物資之相關商業活動。泰國現已建置有完整的防制資武擴法規架構。

4.2 關於金融機構、指定之非金融事業或人員（DNFBPs）、虛擬資產服務提供商或其他相關產業之指引文件

日本

日本財務省發布《外匯檢查指引》（Foreign Exchange Inspection Guideline），規範金融機構依據《外匯及外國貿易法》（Foreign Exchange and Foreign Trade Act）應盡之經濟制裁義務、必須採取之措施、與降低資武擴風險之方法。

文件連結
:https://www.mof.go.jp/policy/international_policy/gaitame_kawase/inspection/e_g_zenbun.pdf

菲律賓

菲律賓戰略貿易管理辦公室（STMO）發布下列金融及相關產業之指引文件：

- 《國家戰略物資清單》（National Strategic Goods List, NSGL）。於該清單附錄三明訂禁止與北韓及伊朗進出口之國家管制物資。文件連結: https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Policies/Annex%20III.pdf
- 菲律賓貿易暨工業部（DTI）第 20-13 號備忘錄通函，採行聯合國安全理事會（UNSC）之綜合制裁名單作為STMO之「禁止用戶名單」（List of Prohibited Users）。文件連結: https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/e-library/Laws+and+Policies/140420_MC20_13.pdf
- 菲律賓貿易暨工業部第 21-06 號備忘錄通函,規定仲介（brokering）及融資（financing）之實施指引，以符合聯合國安全理事會第 1718 號決議（2006 年）、第 2231 號決議（2015 年）及後續相關決議要求。
  文件連結: https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/Laws+and+Policies/Memorandum+Circular+No.+21-06+Implementation+of+FInancing+and+Brokering+Under+Republic+Act+No.+10697.pdf
- 依據菲律賓洗錢防制委員會（AMLC）第 1 號監管發布，戰略貿易管理辦公室（STMO）可協助提供授權，以使凍結資產於符合條件下用於支付先前契約款項。惟相關契約須經STMO認定並未涉及聯合國安全理事會第 2231 號決議（2015年）及後續決議所禁止之項目、財務援助、仲介或服務，且相關支付未直接或間接由制裁名單之個人或實體接收，方得進行。
  文件連結:
  http://www.amlc.gov.ph/images/PDFs/Guidance%20for%20Delisting%20and%20Unfreezing%20-%20PF%20TFS%20v2.pdf

此外，菲律賓戰略貿易管理辦公室亦進行以下風險意識提升及強化盡職審查活動：

- 對受監理之利益相關方進行宣導，提醒其與遭制裁之個人或實體進行交易可能產生之不利影響。宣導形式包括戰略貿易管理辦公室進行一對一之輔導、針對特定產業之宣導，以及政府與產業利益關係人共同參與之公開說明會等。
- 此外，戰略貿易管理辦公室亦提供「終端使用者商務諮詢」（end-user business advice），協助企業遵循制裁國家之相關規範。截至目前，戰略貿易管理辦公室已處理逾 10 起涉及未來商務活動、或與新外國商業夥伴契約之諮詢案件。

  文件連結:
  https://dtiwebfiles.s3-ap-southeast-amazonaws.com/STMO/Announcements/STMO+Advisory_Sanctioned+Individual+and+Entities.pdf

  https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Publications/red+flags.pdf

  https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Publications/restricted-party-screening-2.pdf

新加坡

新加坡金融管理局（Monetary Authority of Singapore, MAS）對金融機構發布相關指引，協助其防制資武擴之風險：

- 金融管理局針對銀行業進行系列關於防制資武擴之風險監理訪查後，發布一份指引文件。該文件內容涵蓋訪查期間所觀察之重要發現、及優良作業實務，金融機構被要求據此作為基準，以強化其既有內控措施。
- 金融管理局於此防制洗錢及打擊資恐指引中，提供防制資武擴相關方針，包括可能涉及資武擴之可疑跡象。

此外，金融管理局亦與新加坡銀行公會（Association of Banks in Singapore, ABS）合作，將防制資武擴列為 ABS 年度「金融犯罪研討會」（Financial Crime Seminar）之固定議程項目。ABS 金融犯罪研討會為新加坡重要之防制洗錢及打擊資恐產業宣導活動之一，經常吸引逾 500 名新加坡及鄰近地區之專業人員參與。歷年來有多位來自新加坡及海外專家受邀於 ABS 金融犯罪研討會演講，從而提升產業界對資武擴及其風險降低措施之認識。

中華臺北

中華臺北保險業洗錢防制及打擊資恐聯合工作小組發布保險業防制洗錢、打擊資恐、及防制資武擴風險相關之海上保險指引文件：

- 《保險業防制洗錢及打擊資恐最佳實務指引—主題：貨物保險及相關險種防制洗錢、資恐與資武擴之實務作業程序》。該指引針對產物保險業者提供實務性建議，確保其於貨物保險及船體保險之招攬、核保及理賠程序中能有效落實防制洗錢及打擊資恐措施，並針對涉及高風險地區之權宜船旗（flags of convenience, FOC）漁船保險業務，提出具體之核保實務作業建議。

泰國

泰國防制洗錢辦公室（AMLO）定期向金融機構、與指定之非金融事業或人員（DNFBPs）發布有關資武擴之資訊及指引。並舉辦多場宣導研討會，向包括商業部及易受資武擴影響之業者推廣如何辨識、評估及降低資武擴風險；同時提供針對涉及軍民兩用物資之業務所需辨識、評估及降低資武擴風險之具體指引。

4.3 涉及違反、未落實或規避資武擴目標性金融制裁之案例研究

案例研究 #114 - 船對船轉運及利用第三方司法管轄區

資武擴；濫用法人及法律協議

一家國際公司（以下稱「該公司」）於庫克群島信託事務所成立登記，並作為一艘船籍註冊於 B 司法管轄區之船舶之「船東」。該公司實際業務運作地點位於 C 司法管轄區，而設於 A 司法管轄區之註冊辦公室與駐地秘書並未參與該公司任何營運活動、業務或財務交易，亦未與該公司唯一所有人兼董事有任何往來紀錄。

經提交之疑似可疑活動報告（SAR）揭露，該船舶因涉及與懸掛北韓（DPRK）船旗之船隻進行非法船對船轉運，而於 B 司法管轄區遭停權並除籍。

該活動已構成違反聯合國之目標性金融制裁，導致該公司亦被列入制裁名單，並遭 A 司法管轄區撤銷登記。

來源－庫克群島

案例研究 #115 - 中央銀行拒絕公司與受制裁司法管轄區潛在夥伴之合作申請

資武擴；濫用法人及法律協議

中央銀行作為主管機關，針對 A 公司申請與潛在夥伴建立業務關係一事進行評估。經中央銀行協調與審查後發現，A 公司欲合作之潛在夥伴為 FATF 所認定之高風險受制裁司法管轄區之法人實體。中央銀行隨即要求 A 公司就該潛在夥伴提出進一步說明及補充資訊。惟 A 公司無法達到中央銀行之資訊要求，因此主管機關決定拒絕 A 公司提出之合作申請。

來源－印尼

案例研究 #116 -「智慧誠實號」- 利用第三方司法管轄區之船對船轉運

資武擴

「智慧誠實號」（The Wise Honest）為一艘散裝貨輪，在 2016 年 11 月至 2018 年 4 月間違反聯合國目標性金融制裁措施，從事北韓與其他司法管轄區之間的進出口貨物轉運活動。參與此活動之人士試圖在航運文件中以虛假之船籍與煤炭來源地資訊，掩飾該船與北韓之關聯性。

2018 年，印尼接獲 A 司法管轄區提出之刑事司法互助請求，調查「智慧誠實號」與來自 B 司法管轄區之船隻可能進行非法船對船轉運之情事。經印尼國家情報局（State Intelligence Agency, SIA）調查，發現一個涉及該計畫之印尼及北韓籍人士所組成之犯罪網路。國家情報局隨即將相

關情資通報印尼金融情報中心（PPATK）進行並行之金融調查。前述各項調查最終促成「智慧誠實號」被成功遣返 A 司法管轄區，印尼當局並裁罰該船船長 4 億印尼盾（約合 26,000 美元）。

來源 – 印尼

案例研究 #117 - 拉撒路集團

資武擴

日本境內虛擬貨幣交易服務商遭受一系列網路攻擊，攻擊方式與據稱受北韓政府支持之網路犯罪組織「拉撒路集團」（Lazarus Group）的攻擊手法高度相似。基於前述情形，研判日本相關產業已持續數年成為該集團攻擊之目標。

來源 – 日本

5 資產返還之方法與趨勢

本節內容依據各會員國提供之資產返還相關資料與案例分析彙整而成。

5.1 澳洲

案例研究 #118 - 利用毒品犯罪所得購買奢侈品與貴金屬

毒品犯罪；購置不動產；購買貴重物品；金融機構、濫用法人及法律協議；電匯

2020 年，澳洲邊境執法局（ABF）查獲藏匿於機械設備內之毒品。隨即將案件移交澳洲聯邦警察（Australian Federal Police, AFP）進行刑事偵查與資產沒收程序。雙重調查顯示，涉案之 A 某具雙重國籍，涉及國際銀行電匯、可疑現金存款，透過不動產經紀業者及律師信託帳戶收取銀行轉帳，並利用境內公司購置資產，包括取得無抵押不動產、貴金屬及古董車。

2022 年 4 月警方執行控制下交付行動（controlled operation）後逮捕 A 某。A 某經法院判處有期徒刑 11 年，6 年不得假釋。法院同時扣押 44 輛汽車、現金及黃金、白金與白銀等貴金屬，總價值約澳幣 500 萬元（約 320 萬美元）。前述財產隨後於 2022 年 10 月依據澳洲聯邦《2002 年*犯罪所得法*》（Proceeds of Crime Act 2002 (Cth)）規定自動沒收。

來源 – 澳洲

5.2 中國

2017 年至 2022 年間，中國權責機關透過「天網行動」（Skynet）返還得資產總額約人民幣 327.86 億元（約合美元 45 億元）。該行動特別針對逃亡中之貪腐官員犯罪所得。

5.3 中國香港

香港警務處（HKPF）轄下之反詐騙協調中心（ADCC）與聯合財富情報組（JFIU）加強與金融機構合作，透過與 14 間本地銀行建立全天候聯絡機制，以降低詐欺受害人損失。當接獲符合一定標準之詐欺或相關洗錢活動通報後，反詐騙協調中心立即通知銀行，由銀行評估並決定是否進行止付作業。

此外，反詐騙協調中心與國際刑警組織金融犯罪科（Financial Crimes Unit of INTERPOL）於 2019 年 10 月共同建立「國際止付機制」（International Stop-Payment Mechanism）。當接獲涉及境外金融機構受款帳戶之詐欺通報，且符合特定標準時，反詐騙協調中心將聯繫國際刑警組織啟動該止付機制。同樣地，國際刑警組織若收到涉及香港境內受款帳戶之案件，亦將通報反詐騙協調中心以攔截犯罪所得。

鑑於加密貨幣交易日益普及，與其遭犯罪集團利用作為洗錢工具之潛在風險，香港警務處於 2021 年 3 月另行建立「加密貨幣止付機制」（Cryptocurrency Stop Payment Mechanism）。該平台可迅速追查、並攔截犯罪所得資金。該平台

為加密貨幣相關利害關係人，包括支付平台與加密-自動櫃員機服務提供商提供一個協調與合作的管道。當接獲疑似詐騙通報時，此機制有助於香港警務處系統性地協助追蹤相關資金流向、提出止付請求及攔截詐欺匯款，以有效降低被害人損失。

在中國香港最常見遭凍結及沒收之資產包括銀行帳戶內之現金、不動產及由經許可機構或銀行所持有之證券。其他資產尚包括貴金屬、寶石、珠寶、名錶及實體現金。約 60% 之資產係登記於第三人名下，或由公司共同持有。

案例研究 #119 - 成功止付境外戀愛詐騙匯款

詐欺； 金融機構；境外前置犯罪

2022 年中旬，一名來自 X 司法管轄區之女性受戀愛詐騙誘導，分四次匯出合計 377 萬美元（約 2.96 億港幣）至中國香港某銀行帳戶。該名女性隨後向香港警方報案，香港警方立即與該銀行聯繫以攔截匯款。最終成功攔截全部款項並全數退還予被害人。

來源 – 中國香港

案例研究 #120 - 成功止付商務電子郵件詐欺匯款

詐欺； 金融機構

2022 年中旬，香港某股票投資公司經理依據詐騙集團偽冒公司董事所發送之電子郵件指示，從公司銀行帳戶匯出 986 萬港幣（約 130 萬美元）至當地一個銀行帳戶。隨後真實之公司董事收到銀行之簡訊通知，始揭發此宗詐騙案件。案件經向香港警方報案後，該銀行帳戶內詐欺資金已被全數凍結，目前正進行後續之返還程序。

來源 – 中國香港

案例研究 #121 - 以洗錢方式處理毒品販運所得

毒品相關犯罪；現金；金融機構；可疑交易報告

A 某於 A 司法管轄區因毒品販運罪成立，被判處終身監禁。金融情資顯示，其於中國香港之銀行帳戶內共計有 69 筆現金存款，總額達 2,900 萬港幣（約 370 萬美元）。A 某遭逮捕後不久，其香港銀行帳戶內合計 1,200 萬港幣（約 150 萬美元）之資金，透過電話銀行轉入其妻子名下之帳戶。其妻子居住於 Y 司法管轄區。2021 年底，法院裁定核發沒收令，沒收 A 某及其妻子名下之資產共計 880 萬港幣（約 112.6 萬美元）。

來源 – 中國香港

案例研究 #122 - 沒收加密貨幣資產

詐欺；境外前置犯罪；可疑交易報告；使用虛擬資產

2022 年中旬，Y 司法管轄區某加密貨幣公司發生倒閉事件後， 中國香港聯合財富情報組（JFIU）接獲與該公司創辦人 A 某 相關之可疑交易報告，懷疑 A 某涉及詐欺金額 500 萬港幣（約 6,400 萬美元）。警方成功阻止 A 某及其兩名同夥自數位資產帳戶移轉價值超過 1 億 5,700 萬港幣（約 2,000 萬美元）之加密貨幣。目前 Y 司法管轄區之執法機關正配合相關請求，啟動資產返還程序。

來源 – 中國香港

5.4 印尼

案例研究 #123 - 大規模貪污所得之複雜資產管理

賄賂與貪污、國際合作

A 某與 B 某利用位於雅加達之國營企業 A 公司，透過貪污侵占資金，並利用該企業及其他公司與帳戶進行洗錢，涉案金額合計達 16.8 兆印尼盾。同時以嫌犯本人、第三方及其他公司名義購置車輛，藉此掩飾犯罪所得。犯罪所得亦被用於賭博及購置海外資產，相關情事透過正式及非正式之國際合作揭露。

印尼總檢察署（Attorney General's Office, AGO）於 2020 年成立一支獨立於原調查團隊之外之資產追查小組。該小組自印尼境內多個主管機關（如稅務總局、不動產及車輛登記機關，以及印尼肅貪委員會〔Commission of Eradication of Corruption, CEC〕）取得金融情報，並行使調查權向銀行調取金融交易資料，以建構嫌疑人之特徵，並追查犯罪所得與相關資產之間的關聯。由於涉案人士運用公司結構層層掩飾不法資金流向，總檢察署另與印尼金融服務監理局（Financial Service Authority, FSA）協調取得相關股票資訊；並與印尼法律與人權部（Ministry of Law and Human Rights, MLHR）合作調取公司登記資料。

2020 年 10 月，檢方扣押 3 間公司之資產、21 輛汽車、1 部機車、多件奢侈品、多張保單、不動產以及 110 億印尼盾現金。為維持資產價值，資產返還中心（Asset Recovery Center, ARC）經評估後拍賣土地、股票及豪華車輛。其中一艘尚未建造完成之豪華遊艇經拍賣後得款 55 億印尼盾。無法出售之資產則由資產返還中心管理。股票之拍賣及 A 公司之重整，亦與財政部密切合作謹慎執行，以避免資產價值減損。為彌補侵占公款行為對國家所造成之損失，資產返還中心正評估追討犯嫌名下之股票資產，以及礦業經營許可執照，作為等值返還資產。

透過國際合作機制，印尼亦積極追討犯罪所得於區域內第三國家以第三人名義購買之資產。總檢察署亦透過刑事司法互助向 B 司法管轄區取得銀行交易及股權資料，以利調查。該等資訊並用於對犯罪嫌疑人提起公訴。目前印尼政府已正式透過刑事司法互助提出凍結資產之請求，並非正式地請求相關國家協助，提出法院聲請扣押及沒收犯嫌名下資產。

來源－印尼

5.5 日本

警方依據國家公安委員會（National Public Safety Commission）之規則，以及警察廳（National Police Agency）發布之證物保管及管理指引，查扣相關資產。此外，檢察廳（Public Prosecutors Office）依據其內部《行政證據管理規則》（Administrative Rules of Evidence）處理證據，涵蓋從接收、移送至變現處分犯罪所得之完整程序。

案例研究 #124 - 大麻販運案件提起公訴前，針對毒品犯罪所得聲請暫時限制處分以利後續沒收

毒品相關犯罪

A 某在其住宅與林地內種植大麻，並透過宅配服務販運大麻給多名買家。本案依違反《毒品特別規定*法*》（Anti-Drug Special Provisions Law）偵辦。法院已針對 A 某因販賣大麻所得之 570 萬日圓（約 38,000 美元）現金裁定暫時限制處分（Temporary Restraining Order），以利後續沒收程序。

來源 – 日本

案例研究 #125 -透過社群媒體販運毒品案，於提起公訴前聲請沒收與毒品相關的犯罪所得核發暫時限制處分

毒品相關犯罪；金融機構

嫌疑人利用社群媒體尋找毒品買家，並透過郵寄包裹服務於全國寄送興奮劑與大麻。毒品交易所得資金則匯入其控制之第三人名下銀行帳戶。本案經警察機關偵破，認定為構成違反《毒品特別規定*法*》之犯罪案件。經法院核准對本案源自毒品販運所得之現金 129 萬日圓（約 8,600 美元）及銀行存款 18 萬日圓發出暫時限制處分，以利後續沒收。

來源 – 日本

5.6 蒙古

案例研究 #126 - 濫權及洗錢案件

重要政治性職務人士、購置不動產、濫用法人與法律協議

蒙古前高階重要政治性職務人士 Y 某，濫用職務之便，於簽訂投資合約時偏袒 A 公司。隨後，A 公司執行董事 Z 某，將公司大筆資金轉移至其本人於境外司法管轄區成立的 X 境外公司名下。該 X 境外公司再於同一司法管轄區內，以 Y 某親屬名義購置不動產。

本案偵辦過程中，金融情報中心及執法機關廣泛與國內權責機關及申報機構合作，並積極與外國對等單位及金融情報中心進行資訊交流及合作。同時透過艾格蒙聯盟（Egmont Group），向外國對等金融情報中心發出多項資訊請求，以取得相關資料，並向境外司法管轄區之主管機關提出司法互助請求，以蒐集證據。

Y 某及 Z 某隨後遭提起公訴並經法院判決有罪。於 2020 年經法院裁定「濫用職權罪」及「洗錢罪」罪名成立。2021 年，法院裁定兩人應返還犯罪所得，總計約 600 萬美元。

來源 – 蒙古

案例研究 #127 – 侵佔公款

重要政治性職務人士、購置不動產、濫用法人與法律協議

國際調查記者同盟（International Consortium of Investigative Journalists, ICIJ）報導指出蒙古國境內若干重要政治性職務人士（PEP）於境外司法管轄區設立公司，引發後續調查。調查相關境外公司活動期間，發現一家國營企業與境外公司簽訂採購合約時，成交價格明顯高於市場價格，且涉案之公職人員及重要政治性職務人士濫用職權，批准相關合約。國營企業向境外公司付款後，其中部分資金透過涉案人士同夥之銀行帳戶，轉回上述公職人員與重要政治性職務人士之帳戶。該等資金之後被用以購置土地與不動產，以掩飾犯罪所得之來源。

調查期間，金融情報中心及執法機關廣泛與國內權責機關及申報機構合作，並與外國對等機關協調。共向外國金融情報中心提出 1 次資訊請求，另向外國司法管轄區提出 1 次刑事司法互助請求以蒐集相關證據。

本案依據《刑法》之簡易程序於 2021 年結案，沒收土地及不動產之價值共計 74.112 萬美元。

來源 – 蒙古

5.7 新加坡

案例研究 #128 – 沒收非法賭博所得

賭博活動；組織犯罪；敲詐勒索

2022 年 7 月 27 日，新加坡高等法院針對 A 某經營非法賭博網站案，裁定沒收其約 125 萬新加坡元（約 92.2 萬美元）犯罪所得；A 某因本案判處有期徒刑 4 年 12 個月，並處罰金 50 萬新加坡元（約 36.8 萬美元）。A 某所涉罪名包含於新加坡境內經營遠端賭博服務、收受非法彩券投注、轉移犯罪所得利益、加入組織犯罪集團及相關組織犯罪行為等。深入調查 A 某財務狀況發現，其多年累積財富與其已知合法收入來源顯不相稱。

來源 – 新加坡

案例研究 #129 – 沒收用於購買奢侈品與不動產之犯罪所得

賄賂與貪污；使用不動產；購置高價或文化資產

2022 年 3 月 31 日，一宗涉及從石油設施盜取油氣資源的共謀案件中，三名涉案人之一被判處 29 年有期徒刑。涉案人 A 某同時被控兩項洗錢罪。金融調查發現，A 某所涉犯罪所得至少達 560 萬新加坡元，其犯罪所得被用於購置精品手錶、汽車及境內外不動產。法院對 A 某核發財產處分令（disposal order），命其返還現金 331 萬新加坡元（約合美元 250 萬元）、及以購置價值計算之資產 29 萬 9,922 新加坡元，返還予該石油設施。另兩名共謀者目前仍在審理中。

來源 – 新加坡

案例研究 #130 – 迅速跨國追回 7,000 萬美元犯罪所得

詐欺；第三方洗錢；境外前置犯罪；電匯

被害人 C 某於一起網路愛情詐案中，受騙將其公司資金 陸續轉帳至多個國家、及地區之多家企業與個人帳戶，其中匯入新加坡之銀行帳戶金額即超過 1.35 億美元。新加坡警察部隊商業事務局（Commercial Affairs Department, CAD）接獲通報後，迅即查扣並返還近 7,000 萬美元，來自涉案之多個銀行帳戶。該局並透過國際刑警組織、金融情報中心及各國警察間之直接合作管道，追查並確認資金去向，所查獲之資金於扣押後一年內返還被害者之公司。

來源 – 新加坡

案例研究 #131 – 運用隱匿所得分析（Concealed Income Analysis）成功沒收非法所得

走私；獨立洗錢；現金；金融機構

2019 年 7 月，新加坡海關逮捕涉嫌香菸逃漏稅款之 A 某。行動中，新加坡海關查扣超過 300 箱、價值逾 87,000 新加坡元之菸品。所逃漏之稅捐加上商品與服務稅（GST）合計超過 90,000 新加坡元。調查期間，新加坡海關發現A某擁有來源不明之財產，且無法做出合理解釋，因此將案件移送商業事務局（CAD）進一步偵查。

商業事務局立即對 A 某展開全面金融調查，經與新加坡多家商業銀行合作清查後，查扣 A 某名下兩個銀行帳戶內約 112,000 新加坡元。為釐清其財務狀況，調查人員深入訊問 A 某，要求其申報資產、負債、支出、合法收入及其他收入來源。經「隱匿所得分析」（Concealed Income Analysis）計算結果顯示，A 某於 2018 年 10 月至 2019 年 7 月間，累積所得達 92,750.83 新加坡元，但無法提供合理來源證明。

2021 年 5 月，A 某因違反新加坡《海關法》（Customs Act）第 128I(1)(a)(ii) 及 128I(1)(b) 條之規定，被判處 3 個月有期徒刑，併科罰金 10 萬新加坡元（未繳交則處以額外 3 個月徒刑）。2022 年 1 月，調查人員依據新加坡《貪污、販毒及其他重大罪行（沒收利益）法》（CDSA）第 5 條第 1 項規定，沒收 A 某之隱匿所得 92,750.83 新加坡元（約 67,561 美元）。

來源 – 新加坡

案例研究 #132 –沒收毒品販運之犯罪所得

毒品相關犯罪

A 某於 2010 年因觸犯新加坡 1973 年《毒品濫用法》（Misuse of Drugs Act）之毒品交易罪遭逮捕。並於 2015 年 2 月 4 日判處死刑。警方逮捕 A 某當時，同步扣押其所持現金 70,295 新加坡元。另於金融調查期間，進一步限制處分（restrained）A 某名下共 4 個銀行帳戶，帳戶內餘額合計 211,260 新加坡元。金融調查證實，A 某遭扣押之資金來自毒品交易及非法放貸活動的犯罪所得。

為釐清 A 某因毒品交易所取得之總犯罪所得，調查人員進一步運用「隱匿所得分析」（Concealed Income Analysis）進行計算。結果顯示，A 某名下無法合理解釋之隱匿所得達 167,429 新加坡元，明顯高於其合法收入來源。此為被告無法就其財產累積情形提出合理說明，且與其已知收入來源顯不相當之部分。2020 年 2 月 17 日，法院根據新加坡《貪污、販毒及其他重大罪行（沒收利益）法》（CDSA）第 4 條規定，針對 A 某毒品交易所得，核發沒收令（Confiscation Order），沒收 167,429 新加坡元（約 124,000 美元）犯罪所得。

來源 – 新加坡

5.8 中華臺北

2016 年 7 月 1 日起，中華臺北正式施行《刑法》沒收相關規定。截至 2022 年 4 月止，法院裁定沒收之犯罪所得總金額 已達新臺幣 271 億元（約 9.204 億美元）。

案例研究 #133 - 拉法葉艦採購弊案

賄賂與貪污

中華臺北最知名之沒收案例，涉及自境外 Y 司法管轄區採購 6 艘海軍巡防艦之貪污賄賂犯罪所得。法院針對該案所裁定之犯罪所得沒收金額高達 9 億 2,039 萬 7,000 美元（新台幣 271 億 6,091 萬元）。

Y 司法管轄區透過其前身部分國營之 A 公司支付賄款，以確保巡防艦順利出售予中華臺北。該批巡防艦經 Y 司法管轄區之 B 公司出售予中華臺北海軍，雙方於 1991 年簽訂合約，交易總價約 28 億美元，據稱該金額已包含協助促成交易之回扣與賄款。前述不法回扣由中華臺北籍武器仲介商 A 某及其家人收取。經追查發現，此犯罪所得資產最終流向數個歐洲國家。

中華臺北於 2001 年起尋求司法協助，Z 司法管轄區於 2006 年 9 月積極回應並凍結相關非法所得資金。A 某及其家人於同年遭到檢方以貪污罪名起訴，但涉案人士已潛逃境外，目前仍遭通緝中。A 某雖於 2015 年死亡，惟本案仍持續就其遺產及家庭成員進行追訴。

依據中華臺北最高法院於 2019 年及 2021 年之判決，允許沒收 A 某繼承人持有之犯罪所得（約 4 億 8,700 萬美元）。中華臺北法務部及檢察機關持續與 Z 司法管轄區保持密切聯繫，以求返還遭凍結於該管轄區內之資產。

法院經審理後，於 2022 年作成裁定，認定犯罪所得之沒收屬公平性措施，性質近似不當得利之返還，而非刑事處罰。

2022 年，Z 司法管轄區同意將上述犯罪所得資產返還予中華臺北。為感謝 Z 司法管轄區之長期協助與支持，中華臺北主管機關經雙邊協商後，同意與該管轄區共享該批資產。本案進入 Z 司法管轄區之不法資金約新台幣 2,000 萬元，在扣除訴訟費用及與 Z 司法管轄區共享後，中華臺北成功追回逾 1,000 萬美元之犯罪所得。此為中華臺北與其他司法管轄區首次進行之資產共享案例。

來源 – 中華臺北

案例研究 #134 – 國際合作返還犯罪所得

走私；洗錢；國際合作

2014 年 9 月，中華臺北收到 X 司法管轄區提出之刑事司法互助請求，請求協助限制或扣押 A 某涉嫌從事洗錢與走私犯罪所得存放於中華臺北境內銀行帳戶內之資金。中華臺北據此協助扣押 A 某銀行帳戶內約 1,500 萬美元之犯罪所得。

在案件程序進行期間，A 某於 X 司法管轄區認罪並與該司法管轄區達成認罪協商，同意自願將遭中華臺北扣押之資金 返還 X 司法管轄區。據此，X 司法管轄區於 2020 年 5 月進一步提出補充請求， 請求中華臺北解除資金之限制及扣押措施，以便將銀行帳戶內之犯罪所得匯回 X 司法管轄區。

於新冠（COVID-19）疫情期間，經 X 司法管轄區、中華臺北法務部、國內相關銀行、A 某及相關協助機關持續協商與協調後，於 2022 年 3 月中華臺北成功協助將該筆約 1,500 萬美元之犯罪所得 匯至 X 司法管轄區指定之銀行帳戶。目前中華臺北與 X 司法管轄區仍就資產分享及相關國內程序持續協商中。

來源 – 中華臺北

5.9 泰國

案例研究 #135 – 國際合作返還犯罪所得

詐欺；國際合作

美國聯邦調查局（FBI）向泰國防制洗錢辦公室（AMLO）請求提供金融資料，以調查一起美國民眾遭詐欺並將資金匯入泰國之案件。泰國防制洗錢辦公室調查發現所有接收美國資金之銀行帳戶皆由泰國籍 A 某擁有或控制，該等帳戶共計接收美國匯入資金 2,662,035.70 泰銖（約 7.3 萬美元）。泰國民事法院最終裁定沒收上述款項，並將上述款項返還予美國以賠償被害人。

來源 – 泰國

案例研究 #136 – 自國外返還賄賂貪污之犯罪所得

賄賂與貪污；重要政治性職務人士

泰國政府官員 A 某及其共犯涉嫌自境外商人處收受總額約 6,000 萬泰銖（約合 150 萬美元）之賄賂與回扣，作為取得政府採購合約之交換條件。前述資金透過銀行本票及國際資金匯款方式，匯入 A 某女兒及其他人頭帳戶，資金流入多個國外司法管轄區。

泰國國家反貪污委員會（National Anti-Corruption Commission, NACC）依貪污罪及財產來源不明罪起訴 A 某與其共犯。泰國最高法院嗣後判處 A 某及其女兒有期徒刑，並裁定沒收其資產，包括位於境外多個司法管轄區之資金。泰國隨後透過刑事司法互助（MLA）程序，向五個不同司法管轄區申請協助執行泰國法院之裁定，以追回犯罪資產。

嗣後發現其中一個司法管轄區尚有其他資產後，NACC另請求泰國防制洗錢辦公室（AMLO）協助向泰國民事法院聲請沒收該筆資產，並透過刑事司法互助程序，請求該境外司法管轄區協助執行沒收裁定，將約 50 萬美元犯罪所得資金返還泰國。目前資金返還程序正在進行中。此外，A 某及其共犯另因涉及洗錢犯罪而遭到起訴，相關刑事審判程序仍持續進行中。

來源 – 泰國

6 FATF 、區域性防制洗錢組織及觀察員組織之研究專案與出版報告

本節概要說明防制洗錢金融行動工作組織（FATF）、區域性防制洗錢組織（FSRBs）及觀察員於 2022 至 2023 年間發布之相關態樣報告。

6.1 FATF 2022 至 2023 年間洗錢、資恐及資武擴風險態樣報告

6.1.1 *虛擬資產／資助勒索軟體相關風險*

報告全文請參閱：
https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html

主題概述

FATF 於 2022 年 6 月針對各司法管轄區在虛擬資產及虛擬資產服務提供商（領域中落實 FATF「國際轉帳規則」（Travel Rule）之情形，發布專題更新報告。
此報告係 FATF 於三年前將防制洗錢與打擊資恐（AML/CFT）措施擴及虛擬資產領域後，為持續防範此領域遭犯罪及恐怖份子濫用所進行之後續追蹤評估。本次更新報告延續先前評估成果，除更新各司法管轄區落實 FATF建議第 15 項之現況外，亦探討新興風險及市場最新發展情形。

研究／專案合作夥伴名單
本專案由「虛擬資產聯繫小組」（Virtual Assets Contact Group, VACG）主導，由日本與美國共同擔任召集人。報告亦透過該小組與私人部門持續進行交流，以取得相關業界之意見。

主要發現與建議

報告指出各國迅速落實 FATF建議第 15 項的必要性，特別是落實「國際轉帳規則」之要求。「國際轉帳規則」指虛擬資產服務提供商（VASPs）與其他金融機構於進行虛擬資產交易時，應同步提供匯款人與 受款人相關資訊。然而，報告發現各司法管轄區於執行該規則方面進展有限。 FATF 報告亦強調，目前已有若干技術解決方案可協助業者遵循「國際轉帳規則」，但私人部門仍需進一步提高各技術解決方案及跨境間之相容性。

針對市場最新發展及新興之洗錢及資恐威脅，報告特別強調各司法管轄區及 FATF 需持續關注去中心化金融（DeFi）、非同質化代幣（NFTs）市場，以及無託管錢包（unhosted wallets）之成長趨勢及相關風險。

6.1.2 *打擊資助勒索軟體（2023 年 3 月 14 日發布）*

報告全文請參閱：
https://www.fatf-gafi.org/en/publications/Methodsandtrends/countering-ransomware-financing.html

主題概述
近年來，勒索軟體（Ransomware）犯罪在全球範圍內規模持續增長。勒索軟體與虛擬資產之間的緊密關聯亦相當明顯，犯罪者所要求支付之贖金幾乎均以虛擬資產進行。

本研究再次強調 FATF 及虛擬資產聯繫小組（VACG）[23] 宣導全球迅速落實 FATF 對虛擬資產與虛擬資產服務提供商相關建議之重要性。各國權責機關在面對涉及虛擬資產之犯罪活動時，亦應確保具備必要之專業技能及能力，以有效調查及防制相關洗錢犯罪。

目前各國通報勒索軟體攻擊案件之情形普遍不足，此或致使主管機關缺乏相關洗錢資金流向之調查經驗。此外，虛擬資產所具有之去中心化與跨國特性，更進一步增加執法機關於跨境資金追查及資產返還之困難。

勒索軟體犯罪本質屬於一種勒索行為，依據 FATF建議第 3 項，各司法管轄區應將其列為洗錢罪之前置犯罪（predicate offence）。但實務上，多數國家將勒索軟體犯罪視為電腦犯罪，而電腦犯罪並未明列入 FATF 所指定犯罪類別。但這似乎並未阻礙勒索軟體相關洗錢犯罪之調查或起訴。

研究／專案合作夥伴名單

本專案係由以色列與美國之專家共同領導。

另由以下司法管轄區及單位作為專案團隊成員參與：澳洲、加拿大、歐盟執委會、法國、德國、日本、盧森堡、墨西哥、菲律賓、新加坡、南非、西班牙、瑞士、土耳其、英國、亞太防制洗錢組織（APG）及艾格蒙聯盟（Egmont Group）金融情報中心。

本專案團隊共計收到逾 40 個代表團之意見與建議。

主要發現與建議

近年來，與勒索軟體攻擊相關之全球資金流動規模大幅增長。據業界統計，相較於 2019 年，2020 年至 2021 年間勒索軟體攻擊支付金額成長高達四倍。各種新手法亦提升犯罪集團採之攻擊之獲利性及成功率。包括專門鎖定具高資產價值之大型企業及機構，或透過「勒索軟體即服務」（Ransomware-as-a-Service, RaaS）模式，由犯罪者向其下線（affiliates）出售易於操作之軟體工具包。勒索軟體攻擊之後果相當嚴重，可能對國家安全構成威脅，包括對關鍵基礎設施與重要服務之破壞及干擾。

此報告旨在提升全球各司法管轄區對勒索軟體相關資金流動之認知，並指出各國與私營部門應對此威脅時之最佳操作實務。此外，此報告亦提供相關風險指標，供各國主管機關與私營部門偵測此類資金流動參考運用。本研究成果廣泛整合公、私部門之經驗與專業意見，亦納入 FATF 全球網路逾 40 個代表團提供之意見與案例研究。

勒索軟體攻擊係屬勒索性質之犯罪行為，依據 FATF 標準，各司法管轄區應將此犯罪行為納為洗錢罪之前置犯罪。此報告發現，勒索軟體犯罪所得之支付及後續洗錢程序幾乎均透過虛擬資產進行。犯罪者利用虛擬資產之跨國特性，以實現大規模、近乎即時之跨境資金流動，有時甚至無須經由已設有防制洗錢與打擊資恐（AML/CFT）計畫之傳統金融機構。犯罪者更透過複雜多層次交易方式，以增加執法機關資金追蹤及資產追回之困難。 犯罪者在洗錢過程中通常使用強化匿名性的技術、手法與代幣（tokens），例如匿名加密貨幣（anonymity enhanced cryptocurrencies）及混幣器（mixers）等技術。

[23] 虛擬資產聯繫小組

由於勒索軟體相關洗錢幾乎完全透過虛擬資產進行，因此更凸顯迅速落實防制洗錢金融行動工作組織（FATF）建議第 15 項之重要性。建議第 15 項 要求各司法管轄區制定相關措施，以降低虛擬資產之風險，並對虛擬資產服務提供商產業進行有效監管。此一措施之落實攸關防制犯罪者利用防制洗錢及打擊資恐控制措施薄弱、甚至缺乏的司法管轄區內之虛擬資產服務提供商，而輕易洗錢並掩飾犯罪所得。

此外，此報告發現勒索軟體攻擊普遍通報不足，其原因包括私營企業在偵測攻擊上的困難、受害企業擔憂通報攻擊事件會對業務產生負面影響，以及受害者恐懼犯罪分子報復等因素。此現象亦部分解釋目前在調查與勒索軟體相關洗錢犯罪時，缺乏實務經驗的原因。各司法管轄區應進一步強化對勒索軟體之偵測與通報來源。主管機關須迅速採取行動收集重要資訊，並應具備有效追蹤及返還虛擬資產之必要工具與技能。

勒索軟體跨越眾多領域，且可能涉及傳統防制洗錢及打擊資恐主管機關以外之其他單位，例如資安及資料保護機構。因此，有效對抗勒索軟體及其相關洗錢活動，必須採取跨領域（multi-disciplinary）合作模式。此外，由於虛擬資產具備去中心化及跨國特性本質，必須建立並善用現有之國際合作機制，方能成功打擊與勒索軟體相關之洗錢活動。

為強化全球對勒索軟體及其相關洗錢犯罪的應對， FATF 建議各司法管轄區採取以下行動：

- 落實 FATF 相關標準，包括對虛擬資產服務提供商之監管與偵測能力，
- 強化金融調查與資產返還力度、
- 採取跨領域合作模式，以有效應對勒索軟體犯罪、
- 鼓勵並深化與私部門之合作夥伴關係、
- 提升國際合作效能

6.1.3 *藝術品與古物市場之洗錢與資恐活動*

藝術與古物市場長期以來遭洗錢及資恐集團濫用。 FATF 於 2023 年 2 月發布一份針對此類犯罪模式之報告，報告全文請參閱：

https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.html

主題概述

全球藝術品、古物及其他文化物品（統稱文化藝術品）交易之市場規模達數十億美元。根據 2021 年數據顯示，全球藝術及古物市場銷售金額達 651 億美元，較前一年成長 29% [24]。該行業在市場規模、營運模式與地域分布上均高度多元。

儘管與文化藝術品相關之洗錢與資恐活動已引起國際關注，但防制洗錢與打擊資恐（AML/CFT）社群歷來鮮少針對該市場所涉之威脅與弱點進行專門評估。

[24] 克萊兒·麥坎德魯 2022 年（Clare McAndrew，2022），《環球藝術市場報告》2022 年（The Art Market 2022），巴塞爾藝術展與瑞銀集團, Art Basel and UBS
https://d2u3kfwd92fzu7.cloudfront.net/Art%20Market%202022.pdf

犯罪分子、有組織犯罪集團與恐怖份子已知曾濫用藝術品、古物及其他文化物品市場進行洗錢並為其活動籌資。高價藝術品、古物及其他文化物品的買賣，容易淪為犯罪分子利用的溫床。高價文化藝術品容易以現金交易，具有匿名性，交易過程常透過第三方中介、空殼公司及其他複雜企業結構完成，極容易被不法份子濫用。

儘管部分司法管轄區與市場參與者已主動採取風險緩解方法，但許多地區仍尚未採取有效的因應措施。本 FATF 報告為首份專注於藝術品、古董及其他文化物品市場洗錢與資恐的研究，指出多數司法管轄區需強化對該市場之風險認識與防制能力，並提出因應弱點之建議。

研究／專案合作夥伴名單

本專案由美國與歐盟委員會共同領導。
專案小組成員來自以下 27 個司法管轄區與國際組織：阿根廷、比利時、巴西、中國、哥倫比亞、歐盟委員會、法國、德國、希臘、瓜地馬拉、冰島、印度、義大利、墨西哥、挪威、秘魯、俄羅斯聯邦、新加坡、瑞士、英國、美國，及以下國際組織：歐洲刑警組織（Europol）、國際貨幣基金（IMF）、國際刑警組織（INTERPOL）、聯合國毒品和犯罪問題辦公室（UNODC）、聯合國反恐委員會執行局（UNCTED）與世界海關組織（WCO）。

本專案利用 FATF 全球網絡中 25 個司法管轄區與兩個國際組織所提供之資訊、案例與資料，並參考 2021 年 12 月 13 日 FATF 聯合專家會議（JEM）特別場次討論內容，同時收集自 2022 年 8 月至 12 月回覆草案之市場參與者、學界、藝術與古物業者協會與非營利組織之意見。

主要發現與建議

藝術品、古物與文化物品市場在規模、營運模式及地域分布上多樣化。大多數為小規模，參與者多與非法活動無關。然而過去十年已有案例顯示，該市場易被犯罪分子利用，包括洗錢者。該等物件往往高價、保值、可代他人以現金購買，並可在個人及企業間低調轉移後，再出售以取得「乾淨資金」。高價值小型物件，如古錢幣等，因其易於跨境攜帶的特性，亦是洗錢犯罪者青睞的工具。

不法資金多來自貪污、毒品販運、金融犯罪等嚴重影響社會的違法行為。此報告指出隱藏或轉移非法犯罪所得的典型洗錢方式包括：隱匿買受人身分、高報或低報物件價格、假買賣或虛假拍賣等等。此外，在此類市場中還發生數種產生犯罪所得的犯罪行為，包括偽造藝術品、詐欺、竊盜及非法販運。

資恐是文化藝術品市場從業人員面臨的另一項重大風險。伊斯蘭國（ISIL）過去曾大肆掠奪敘利亞和伊拉克的重要考古遺址，並傾力銷售掠奪所得的文物，同時對挖掘者課徵稅款，以籌措資金。儘管 ISIL 現已失去原本控制的領土，但該組織及其附屬機構仍控制著世界其他地區的部分領域。此意味著其等可能仍能進入文化遺產地點、或取得文物，並藉以籌措資金。其他恐

怖組織，包括蓋達組織（Al-Qaeda）及其附屬機構，也曾在中東、北非及亞洲部分地區採取類似手法掠取資金。在若干案例中，跨國組織犯罪集團亦曾與恐怖組織合作，從衝突地區取得此類文物並進行走私。該等犯罪集團通常使用常見的洗錢技巧，包括利用空殼公司與現金交易，以掩飾或隱藏文物的真正來源。

要有效解決藝術品、古物及其他文化物品市場的洗錢及資恐問題，存在許多挑戰。此等挑戰大致可分為兩大類。第一類為與物品種類及市場本身特質相關的弱點相關。第二類則為偵查追緝上的困難。

為因應此等挑戰，部分國家已採取監管措施，以降低所確認的洗錢及資恐風險。有些國家成立專注於藝術品、古董或其他文化藝術品市場之專門單位與偵查訓練計畫。另有國家建立相關資料庫，並促進與專家及考古學者合作，以協助追蹤、辨識、調查並返還相關文物。

司法管轄區與相關企業是否能正確辨識、並理解不同文化藝術品與市場參與者的特定風險，至關重要。例如，來自恐怖組織活動區域、或其周邊地區的文化藝術品，可能特別容易被利用為資恐工具。藝術品交易商、顧問、拍賣行與倉儲設施等此類市場業務的從業者亦可能面臨多種風險。數位藝術、非同質化代幣（NFTs）以及藝術品金融服務提供商，因其各自具有特定的內在特性，而面臨不同的洗錢與資恐風險。

此報告特別強調迅速辨識、追蹤涉及洗錢及資恐之文化藝術品的重要性，以利相關物品的扣押與沒收，並追查相關非法所得。此外，此報告亦鼓勵各界與市場參與者合作，包括提供訓練課程、指導方針與道德規範等。公私部門資訊分享可協助克服偵查追緝之困難。其他建議做法則包括建立跨領域專家網路、強化國內外資訊分享、以及與博物館合作以管理被查扣的藝術品與古物等。

最後，此報告另列舉數項風險指標，可協助公私部門機構辨識與文化物品相關的可疑活動。

6.1.4 *吩坦尼及合成鴉片類藥物之相關洗錢活動 2022 年 11 月 29 日*

每年鴉片類藥物走私為有組織犯罪集團帶來數百億美元收益，並導致數萬人過早死亡。 FATF 於 2022 年 11 月發布報告，探討由製造與走私合成鴉片類藥物（Synthetic opioids）所產生之利潤如何進行洗錢。

來自吩坦尼及合成鴉片類藥物之相關洗錢活動 2022 年 11 月 29 日:

https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Money-laundering-fentanyl-synthetic-opioids.html

主題概述

合成鴉片類藥物的非法生產及走私活動，每年為有組織犯罪集團帶來數百億美元的收益，[25] 同時也導致每年數萬人因藥物濫用而死亡。[26].有效截斷合成鴉片類藥物走私的犯罪收益，是解決這項日益嚴重的跨國犯罪，及某些國家面臨之公共衛生危機的最有效手段之一。

有組織犯罪集團亦為合成鴉片類藥物危機推波助瀾，過去十年間已造成數十萬人死於藥物過量。

在北美地區，非醫療用途之吩坦尼濫用已成為鴉片類藥物過量使用、與相關死亡案件激增的主因。在非洲部分地區，曲馬多（Tramadol）濫用正對公共健康造成嚴重衝擊，而亞洲多個國家亦通報案例數量逐漸增加。

此報告旨在：(1) 協助執法機關與其他主管機關有效進行針對非法合成鴉片類藥物走私所得資金之金融調查及起訴；(2) 提升各界對合成鴉片類藥物走私所造成嚴重危害之認識，並進一步充實相關領域的研究文獻。此報告基於過往案例經驗提供風險指標及建議，以協助執法機關與相關利害關係人偵測、並處理合成鴉片類藥物走私之資金流。並提供操作實務及政策選項與工具，協助各國偵測、調查及破壞有組織犯罪集團與相關專業洗錢者之財務活動。本研究結果來自 40 個國家的案例及最佳操作實務，加上專案團隊與執法單位、民間團體討論所獲得之資訊。

此報告亦分析有組織犯罪集團如何以洗錢方式處理合成鴉片類藥物走私所得資金。方法包括，大額現金走私、現金攜帶者、貿易洗錢及虛擬資產（加密貨幣），以及空殼公司與專業洗錢者提供之服務。

研究／專案合作夥伴名單

本研究專案由加拿大與美國專家共同領導。

專案小組由 10 個國家與 2 個觀察員組織所構成：澳洲、加拿大、印度、墨西哥、俄羅斯、新加坡、南非、土耳其、美國、烏克蘭；觀察員組織為國際刑警組織、及聯合國毒品與犯罪問題辦公室（UNODC）。

專案小組於 2022 年 5 月收集來自 25 個防制洗錢金融行動工作組織（FATF）與區域性防制洗錢組織（FSRBs）之問卷調查結果（澳洲、德國、加拿大、墨西哥、奈及利亞、比利時、愛沙尼亞、希臘、塞席爾、盧森堡、挪威、荷蘭、瑞典、日本、塞內加爾、俄羅斯、塞爾維亞、新加坡、斯洛伐克共和國、斯洛維尼亞、南非、西班牙、瑞士及土耳其）。2022 年 5 月至 7 月間，專案領導人與被認定為對本專案具有高度風險或高度相關之司法管轄區及觀察員組織——印度、荷蘭、芬蘭、國際刑警組織、歐洲刑警組織（Europol、聯合國毒品與犯罪問題辦公室 UNODC）——進行了一系列雙邊會談。

[25] 歐洲檢察官組織（Eurojust）（2021）,《Eurojust 藥物販運案件通報》（Eurojust Reporting on Drug Trafficking）

[26] 美國疾病控制與預防中心2022年《理解藥物過量流行病》（Understanding the Drug Overdose Epidemic）；加拿大（2022）《加拿大鴉片類及興奮劑相關危害》（Opioid- and Stimulant-related Harms in Canada）；以及歐洲毒品與毒癮監測中心（EMCDDA, 2022）《歐洲藥物過量死亡情形》（Drug Overdose Deaths in Europe）。

主要發現與建議

合成鴉片類藥物之供應鏈多元複雜，犯罪所得之洗錢手法亦組雜多變。並無單一、全球性之「商業模式」。犯罪集團會因司法管轄區或特定毒品之差異而採取不同的方式。

從事此類毒品販運之組織犯罪集團，使用多種方式跨境轉移非法所得。包括：散裝現金走私、現金攜帶者、貿易洗錢、未經授權之資金或價值移轉服務或銀行體系，以及透過外匯經紀商（money brokers）等。犯罪集團亦透過暗網販售藥物，有時利用增強匿名特性的虛擬資產收取款項。並迅速將此等虛擬資產兌換成法定貨幣。毒品販運者經常利用空殼公司及掩護公司（front companies）來清洗犯罪所得，亦可能利用此等犯罪所得採購藥物、前驅化學品（precursor chemicals）及生產設備。

過去吩坦尼通常可以直接向化學品製造商取得，但由於多數吩坦尼相關物質如今被全面列管（class-wide scheduling），犯罪集團轉而使用前驅化學品自行製造吩坦尼等藥物。此種近期趨勢，增加偵查相關可疑金融活動之困難度。

與其他毒品交易類似，專業洗錢網路亦為毒品販運者及組織犯罪集團提供服務。例如，有證據顯示，亞洲地區的洗錢組織透過無須直接跨境匯款的方式（例如鏡像交易〔mirror transfers〕、哈瓦拉〔hawala-style transfers〕及其他金錢或價值移轉服務〔MVTS〕等）處理犯罪所得。

多數主管機關尚未完全理解對鴉片類藥物相關的全球資金流向，或無法有效辨識可能用於採購化學品、實驗室設備及其他特殊生產設備之活動。在某些司法管轄區，相關主管機關及銀行、金錢或價值移轉服務商（MVTS）等申報單位，傾向從國內角度觀察鴉片類藥物販運，但實際上此類非法交易涉及龐大的跨國組織犯罪集團，及專業洗錢團體。

儘管多數國家均認定毒品販運為重大洗錢前置犯罪，但有關合成鴉片類藥物販運所得的洗錢犯罪，調查與起訴案件仍偏少。此報告旨在提高各國對鴉片類藥物貿易（包含前驅化學品使用）、及其相關全球金流之認識。並提出最佳偵查與打擊犯罪網路之建議。這些活動包括：

- 促進對該領域風險之理解，包括供應鏈、及製藥產業角色，制定更健全的法律及監管架構，以打擊非法鴉片類藥物交易。
- 強化對檢察官及相關主管機關之培訓，以提升其金融調查能力，並涵蓋前驅化學品供應鏈之調查技巧。
- 透過既有國際合作機制，促進原料來源國、轉運國及目的地國之間合作，辨識並瓦解合成鴉片類藥物供應鏈。
- 運用公私部門合作，提升對暗網市場及虛擬資產（加密貨幣）之風險認知，分享紅旗指標資訊，以協助私營部門更有效地辨識、並通報可疑活動。

此報告亦提供相關風險指標，以協助辨識可能涉及非法合成鴉片類藥物販運之活動。

6.1.5 *伊斯蘭國（ISIL）、蓋達組織（Al-Qaeda）及其附屬機構之資恐活動*

主題概述

2015 年起，防制洗錢金融行動工作組織（FATF）持續蒐集並分析由區域性防制洗錢組織（FSRBs）成員提供之資料，內容包括伊斯蘭國（ISIL）、蓋達組織及其附屬機構的資金來源。公共部門專家如有意取得金融行動工作組（FATF）於 2023 年 2 月通過之最新報告，應洽其所屬 FATF 代表。
FACT相關連結:

2022 年 6 月 - https://fact.fatf-gafi.org/official-document/FATF/RTMG(2022)10/REV2/en
October 2022 - https://fact.fatf-gafi.org/official-document/FATF/RTMG(2022)20/REV1/en
February 2023 - https://fact.fatf-gafi.org/official-document/FATF/RTMG(2023)9/REV2/en

6.2 區域性防制洗錢組織（FSRBs）與觀察員組織專案 2022-2023 年

6.2.1 *加勒比海防制洗錢金融行動工作組織*

加勒比海防制洗錢金融行動工作組織（CFATF）發布定期教育文獻，概述犯罪類型與洗錢態樣分析。2022–2023 年間，該機構發表關於「現代奴役／人口販運」、「環境犯罪與非法野生動物貿易之金融偵查」、「空殼公司與實益所有權之角色」等多篇報告。

詳情請見 CFATF 研究專區（Research Corner）。https://www.cfatf-gafic.org/home/cfatf-research-corner

6.2.2 *歐洲理事會防制洗錢及打擊資恐評估專家委員會*

2023 年 5 月，歐洲理事會防制洗錢及打擊資恐評估專家委員會（Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism，簡稱MONEYVAL）通過了一份由曼島（Isle of Man）領導之專家團隊所擬定之報告，內容針對虛擬資產及虛擬資產服務提供商所涉之洗錢及資恐風險進行深入評估。

《虛擬資產世界之洗錢與資恐風險》（Money Laundering and Terrorist Financing Risks in the World of Virtual Assets）報告全文請參閱：https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4

此報告檢視 MONEYVAL 成員國在 FATF標準建議第 15 項中，針對虛擬資產之遵循情形，並評估各國對虛擬資產服務提供商之監管架構，以及執法機關與虛擬資產服務提供商間相互配合之情況。
同時指出與虛擬資產相關的各項風險特徵，並提出各國在面對此一複雜領域時，採用風險基礎方法（Risk-based approach）之最佳操作實務。

6.2.3 *歐亞防制洗錢及打擊資恐組織（Eurasian Group）*

1) 由歐亞防制洗錢及打擊資恐組織（EAG）成員國與祕書處組成之工作團隊負責執行，由《歐亞地區洗錢／恐怖主義融資風險評估》（連結至 EAG 網站）。於 2022 年 6 月通過。

根據本次專案所使用之「可觀察洗錢／資恐手法評估方法論」，若某一洗錢或資恐風險同時具備以下特徵：(1) 在歐亞防制洗錢及打擊資恐組織（EAG）中兩個以上成員國顯現共通性及特徵；(2) 涉及跨境性質，即認定其為「區域性風險」。然而，歐亞地區內的洗錢及資恐風險並非完全一致。因此在評估時特別考量東歐、歐亞經濟聯盟（EAEU）及中亞等次區域之差異性，尤其在判斷既有威脅、弱點與風險時，予以區分考量。此報告除採用 EAG 成員國及觀察員組織所提供之資料外，也比對來自其他可信來源之資訊、與私營部門會談過程中取得的情報，以及涉入跨境洗錢與資恐活動之司法管轄區所提供之資料。本區域風險評估主要涵蓋 2017 年至 2020 年間情況，但報告中也納入部分國家稍後觀察到之洗錢／資恐趨勢，例如 2021 年阿富汗局勢惡化後的情形。

洗錢之威脅

依據本方法論，「洗錢威脅」係指個人從事犯罪活動，因而產生犯罪所得，且該等犯罪所得涉及洗錢過程之情形。當此類犯罪活動由有組織犯罪集團或犯罪組織所為時，所帶來之威脅層級則顯著提升。

在歐亞區域層級已辨識出下列最相關之洗錢威脅：

#	威脅類別
1	逃漏稅與其他必須支付費用等相關稅務犯罪，含操縱加值型營業稅（VAT）（詐欺）
2	賄賂及其他與貪污相關之犯罪（含濫用國家預算資金）
3	詐欺行為（含濫用國家預算資金）
4	非法販售麻醉藥品、精神藥品及其等之前驅物
5	逃漏關稅與其他海關犯罪
6	金字塔騙局活動（多層次傳銷）
7	非法商業活動
8	組織非法移民偷渡活動

經整合對上述各項威脅、弱點及相關制度因素之分析，確認出以下區域性洗錢風險，及其於複雜洗錢模式中所涉及之重要構成要素：

需高度關注並加強風險緩解措施之區域性風險	
1.1	利用人頭公司／受控公司或個體戶
1.2	將犯罪所得投資於法人之經濟活動，包括設於第三國之法人實體
1.3	利用不動產及其他財產之境內外買賣計畫（含虛構交易方案）
1.4	利用銀行帳戶進行「過境」（Transit）金融交易

1.5	進行「提領現金」（Cash-out）操作
1.6	將犯罪所得移轉至區域外，隨後以合法商業投資方式回流至區域內
1.7	使用境外公司（境外公司）
需持續監控並加強風險緩解措施之區域性風險	
2.1	濫用證券市場，包括涉及證券買賣交易
2.2	使用電子支付工具及虛擬資產
2.3	使用不需開設帳戶之資金匯款系統
需標準風險緩解措施之區域性風險	
3.1	透過執行工具（enforcement instruments）將資金匯往境外

區域性資恐風險

專案小組分析辨識出區域特有之資恐風險如下：

- 利用網路進行線上募資；
- 由恐怖份子親屬募集並轉移資金，以滿足恐怖份子基本生活需求；
- 利用銀行帳戶與金融卡轉移資金；
- 使用實體現金方式移轉資金；
- 使用無需開設銀行帳戶之資金匯款系統或電子支付工具轉移資金；
- 以提供物資、物品、制服及服務等形式，使用資金支援恐怖組織成員。

2) 《稅務及經濟犯罪所得之洗錢行為分析》（Laundering of the proceeds from tax and economic crimes）-（連結至 EAG 網站）由吉爾吉斯共和國主導，2022 年 11 月通過。

本專案針對各國打擊稅務及經濟犯罪之防制洗錢及打擊資恐（AML/CFT）制度之現況進行分析，內容涵蓋相關法律規範之檢視、現行可用之制裁措施、權責機關的職責與角色分工，以及此類犯罪偵防調查之特性。此外，專案主導國亦就金融情報中心（FIU）在打擊此類涉及洗錢犯罪之實務角色進行探討，包括紅旗指標、可疑交易報告（STR），以及各種用以偵測此類犯罪之工具與情報來源。最後，此報告亦透過若干實務案例，列舉相關犯罪者採用之洗錢手法與工具，供各界參考。

3) 合法化網路犯罪所得（洗錢）及以該類犯罪所得資恐（包含透過電子貨幣或虛擬資產及相關服務提供商之基礎設施）之研究報告–（連結至EAG網站）由俄羅斯聯邦主導，2022 年 11 月通過。

此報告重點探討近年來各國針對虛擬資產與虛擬資產服務提供商之立法發展情形，並分析私營部門在相關領域中所扮演之角色，以及歐亞防制洗錢及打擊資恐組織（EAG）各成員國對 VASPs 的分類方法。此外，此報告亦提供各種洗錢態樣，及相關偵測與調查技術之整體性資訊，並舉例說明若干涉及虛擬資產之資恐模式與方法。

6.2.4 *東、南非洲防制洗錢組織（ESAAMLG）*[27]

東、南非防制洗錢組織區域《黃金、鑽石、紅寶石等貴金屬及寶石之非法交易與相關洗錢及資恐情形》報告

https://www.esaamlg.org/reports/ILLICIT_DEALING_SEPT_2022.pdf

東、南非洲防制洗錢組織（ESAAMLG）於 2022 年 9 月發布此報告，探討貴金屬與寶石（PMS）市場之洗錢及資恐趨勢。本研究報告由史瓦帝尼（Eswatini）及尚比亞（Zambia）共同主導，並獲得 6 個成員國與聯合國毒品與犯罪問題辦公室（UNODC）之協助。

報告指出，貴金屬與寶石為犯罪分子提供將非法現金轉換為穩定、匿名且易於流通資產的管道。此類資產亦曾被用為購買武器、或毒品的替代貨幣。使用貴金屬與寶石資恐的風險明顯可見。

此報告提供多個相關案例研究，並總結出關鍵發現及建議，包括有必須強化區域內金融情報中心（FIUs）的能力，並改善各司法管轄區間的資訊交流。[28]

6.2.5 *西非政府間防制洗錢組織*[29]

西非政府間防制洗錢組織（GIABA）評估報告（2022 年）,《西非實質受益權資訊與資產返還框架》（Beneficial Ownership Information and Asset Recovery Framework in West Africa）GIABA，達卡（Dakar），塞內加爾（Senegal）：
https://www.giaba.org/media/f/1296_Beneficial%20Ownership%20Information%20and%20Asset%20Recovery%20Framework.pdf

此報告檢視選定成員國有關實質受益權（beneficial ownership）資訊之法律、監管與遵循架構，及其所涉之洗錢與資恐風險。並審視相關成員國之資產返還（asset recovery）及資產管理制度。GIABA 專案小組向各公私部門主要利害關係人進行研究調查，並與 FATF 、美國財政部及世界銀行等發展出合作夥伴關係。

此報告結論認為，西非地區各國因未能有效辨識公司、信託及其他法人之受益所有人，因此易受洗錢及資恐威脅。缺乏足夠的實質受益權資訊導致調查困難，起訴與定罪案例寥寥可數。此外，資產返還機制在該區幾乎不為人知且罕被使用，更進一步加劇該區域所面臨之洗錢及資恐風險。

報告提出之建議包括：

- 進行風險評估。
- 制訂實質受益權資訊揭露法規，並建立國家級登記冊以記載相關資訊。
- 成立專責資產管理機構，建立專屬資料庫登錄資產及不動產，並集中管理返還之資產。
- 參與培訓課程及技術支援活動。

[27] 以上摘要係由亞太防制洗錢組織（APG）秘書處依據公開資訊整理而成。
[28] 以上摘要係由亞太防制洗錢組織（APG）秘書處依據公開資訊整理而成。
[29] 以上摘要係由亞太防制洗錢組織（APG）秘書處依據公開資訊整理而成。

《2022西非地區透過貪腐洗錢與資恐態樣報告》（GIABA Typologies Report (2022) Money Laundering and Terrorist Financing through Corruption in West Africa）GIABA，達卡（Dakar），塞內加爾（Senegal）：

報告全文請參閱：
https://www.giaba.org/media/f/1300_Money%20Laundering%20and%20Terrorist%20Financing%20through%20Corruption.pdf

此報告指出，貪腐仍然是西非經濟崛起的一大障礙。尤其涉及公共機關之貪腐行為，更是形成斂財與洗錢活動之主要來源。

此報告透過蒐集成員國提供之相關資料，並與公私部門利害關係人深入會談後，識別出 8 種類型之洗錢模式，並佐以具體案例研究。此 8 種態樣分別為：

- 貪腐成為防制洗錢及打擊資恐之障礙。
- 重要政治性職務人士之洗錢行為。
- 公職人員涉貪所得之洗錢行為。
- 對犯罪所得進行洗錢濫用職權、非法致富及侵占公款之犯罪所得。
- 公共服務收費所得之洗錢行為。
- 利用法人與法律協議處理貪腐所得之洗錢行為。
- 透過「開門者」（Door Openers）或「守門人」（Gatekeepers）處理貪腐所得之洗錢行為。
- 透過慈善組織處理貪腐所得之洗錢行為。

此報告並提出 15 項策略建議與 14 項實務建議，強調應宣導立法改革、強化防制洗錢與打擊資恐相關機構、提升金融情報中心（FIUs）與政府主管機關之能力，並促進各機構間之資訊共享。

另可參考：GIABA（2021）《西非地區洗錢及資恐案件調查、起訴與審判所面臨挑戰之評估》研究報告（An Assessment of the Challenges Associated with the Investigation, Prosecution and Adjudication of Money Laundering and Terrorist Financing in West Africa），GIABA，達卡。

報告全文請參閱：https://www.giaba.org/media/f/1302_An%20Assessment%20of%20Challenges.pdf

此報告提供西非地區防制洗錢及打擊資恐之現況概述，以及在政策與實務執行層面所面臨之挑戰；此研究計畫亦獲 FATF 之技術援助。

此研究緣起於西非各成員國面對日趨複雜之犯罪情勢，刑事司法反應普遍不佳之背景。

整體而言，報告發現：

- 儘管西非國家積極防範其境內成為犯罪分子之溫床，但由於邊界管控不嚴密、現金交易經濟盛行，以及行政服務數位化程度低，以致防制洗錢與打擊資恐成效不彰。
- 雖然已宣導多項立法改革、設立新機構及進行能力建構措施，但在調查與起訴洗錢及資恐方面之執法措施，仍未能產生有效嚇阻效果。

在政策層面，此報告發現：

- 防制洗錢及打擊資恐架構未考量各司法管轄區之個別風險狀況。

- 政治力介入執法程序，尤其當涉及重要政治性職務人士時，更衝擊執法機關之廉正性與獨立性。
- 刑事司法系統對防制洗錢及打擊資恐認知不足。
- 跨機關合作效能不足
- 金融情報中心之自主權不足或未受保障。
- 國際合作與刑事司法互助機制效果不彰，犯罪所得之沒收亦非優先項目。

實務運作層面，此報告指出：

- 洗錢與資恐案件之司法審理統計偏低，與前置犯罪數據不符。即使已發布沒收裁定，卻因欠缺執行文書障礙重重，資產追還成效不彰。
- 司法從業人員與相關專家對國際合作機制不熟悉，往往使用效率低落之協助渠道。
- 缺乏支援地籍或民事身分資料之科技系統，妨礙蒐集法院受納之證據。
- 法官及檢察官對於洗錢防制與打擊資恐法律體系經驗不足，執意要求前置犯罪之證明。
- 司法體系、檢察單位及其他法律人員之金融情報力不足。
- 刑事司法人員對洗錢態樣（typologies）認識不足，調查人員亦鮮少進行金融調查以支持洗錢案件起訴。

8 項關鍵建議與實施策略如下：

1. 提供資源並提升能力予涉案之調查、起訴及審判機構，特別是金融情報中心、刑事調查人員、法官與地方法官、執達員、反貪機關、資產返還主管機關及司法機關
2. 強化所有參與洗錢及資恐案件調查、起訴與審判機關之能力
3. 增進一般大眾，尤其是法官與地方法官，對國家防制洗錢與打擊資恐法律之理解，特別是洗錢或資恐案件中證據的司法處理方式。
4. 儘快系統化地促進跨機關合作，以共同對抗洗錢與資恐。
5. 強化政府對整治刑事領域內的貪腐，以及對防制洗錢與打擊資恐犯罪之政治承諾。
6. 優先提升刑事司法體系各崗位對區域內洗錢與資恐手法及技術之理解。
7. 強化區域內對洗錢與資恐案件之調查、起訴及審判合作機制。
8. 加強司法體系對洗錢及資恐犯罪案件之專責審理能力。

6.2.6 *中東及北非防制洗錢金融行動工作組織* [30]

(1) 中東及北非防制洗錢金融行動工作組織（MENAFATF）2022年兩年期態樣報告（第5版）（Biennial Typologies Report 2022 – fifth edition）

此報告依據會員國提供之 44 個案例研究，分析該區域內洗錢及資恐之主要類型及趨勢。報告全文請參閱：https://www.menafatf.org/information-center/menafatf-publications/menafatf-biennial-typologies-report-2022

[30] 摘要報告已經中東及北非防制洗錢金融行動工作組織（MENAFATF）核准。

此報告中第一類案件涉及多種態樣。犯罪類型如下：

1. 以洗錢方式處理貪腐所得（共 8 案）。
2. 以洗錢方式處理稅務犯罪所得（共 4 案）。
3. 以洗錢方式處理毒品販運之犯罪所得（共 4 案）。
4. 以洗錢方式處理人口販運及非法移民走私之犯罪所得（共 3 案）。
5. 使用虛擬貨幣/虛擬資產（共 2 案）。
6. 使用新型支付方式（例如 T Pay）（共 3 案）。
7. 以貿易方式洗錢（共 2 案）。
8. 使用假公司（空殼公司）（共 2 案）。
9. 地下（平行）銀行系統／替代性匯兌服務／哈瓦拉（共 2 案）。
10. 貨幣走私（共 2 案）

第 2 類態樣（各僅涉及單一案例）：

1. 賭博活動。
2. 寶石交易（珍珠）。
3. 扭曲市場競爭及破壞投資環境（金字塔騙局）
4. 透過社群媒體從事資恐（透過社群媒體募捐，透過郵政帳戶以小額支付方式進行）
5. 使用境外非居民銀行、國際商業公司及信託（Trusts）
6. 投資資本市場並透過中間人（例如，利用嫌疑人之未成年子女）
7. 黃金走私（利用駱駝運輸）

此報告並提供相關案例所利用之機構實體資訊，以及正在調查、已移送起訴或法院審理之案件數量。

此外，此報告從案例分析中歸納出 30 項重要之可疑活動指標。

(2) 《非營利組織（NPOs）遭濫用於資恐活動之態樣專案報告》（Typologies Project Report on the abuse of NPOs in TF Activities）- 2022 年 11 月

此報告旨在分析與探討成員國非營利組織被資恐活動濫用之風險程度，並找出防範此種濫用之最佳操作實務，同時避免影響合法非營利組織之正常運作。

報告全文請參閱：https://www.menafatf.org/information-center/menafatf-publications/typologies-project-report-abuse-npos-tf-activities

MENAFATF 秘書處透過兩份問卷蒐集資訊，一份來自公部門（包括金融情報中心、執法機關、非營利組織之主管機關），另一份則來自私部門及非營利組織自身。報告亦廣泛蒐集成員國提供之案例研究，並引用 FATF 及 APG 相關公開報告及資料。

非營利組織面臨之洗錢與資恐風險來自 2 個面向。合法非營利組織被不當利用；虛假非營利組織被用來從事非法活動。

報告詳述案例包括，一名資恐組織成員被安插於非營利組織之董事會。犯嫌企圖以虛假非營利組織名義設立銀行帳戶。

某慈善組織名義上致力於兒童福利，實際卻將募得資金挪轉至協會主席個人，導致兒童遭受虐待和經濟剝削（從事農業與建築工作），同時也被灌輸極端主義思想。

艾格蒙聯盟（Egmont Group）[31]

《金融情報中心－金融科技合作與相關網路犯罪態樣與風險》（FIU – FinTech Cooperation and Associated Cybercrime Typologies and Risks）

艾格蒙聯盟於 2022 年 7 月發布報告，探討金融科技（FinTech）領域，以及新型支付相關服務與產品的威脅與風險。

報告全文請參閱：
https://egmontgroup.org/wp-content/uploads/2022/11/2022-Report-on-FIE-FinTech-Cooperation-and-Assoc.-Crimes.pdf

金融科技泛指用於支援、或提供銀行與金融服務之電腦程式與技術工具。

包括網際網路與行動銀行、數位或電子貨幣、匯款平台、非面對面投資（機器人技術）、群眾募資平台（crowdfunding platforms），以及虛擬資產服務提供商。

金融科技是金融服務未來的樣貌，但報告發現多數金融情報中心對金融科技產品底層機制了解有限，亦未充分掌握其可能引發之洗錢與資恐風險。儘管 FATF建議第 15 項要求各司法管轄區積極因應新興科技所帶來的風險，但並非所有金融科技業者均屬於法規所定義之申報義務機構。

此艾格蒙聯盟專案目的包括：
- 了解金融科技實體如何與各國金融情報中心合作；
- 分析相關法規環境；以及
- 擬訂與金融科技產業互動之潛在最佳實務。

此專案涵蓋全球 41 個成員國之參與，透過 16 個案例研究，說明金融科技產業遭濫用的多種方式，以及金融情報中心在解讀所獲資料、追蹤或取得於境外司法管轄區成立之金融科技企業相關資訊時所面臨的挑戰。

常見態樣包括詐欺、利用虛擬資產與空殼公司銀行帳戶進行洗錢等。

報告總結指出，多數司法管轄區尚未建立對虛擬資產服務提供商與區塊鏈技術之相關監理規範；即使已有規範的地區，對服務及產品的分類亦不盡相同，導致應對風險措施存在差異，進而增加追查國際資金流向的難度。

報告建議金融分析人員應具備對金融科技產品及服務運作機制的基本認識，並理解如何解讀金融情報中此等產品及服務的資料。

報告亦建議強化金融情報中心間即時資料交換機制，以促進跨境執法，並確保此領域風險之適當緩解。金融情報中心需與金融科技業者及相關部門合作，共同制訂一套標準通報格式。

[31] 以上摘要係由亞太防制洗錢組織（APG）秘書處依據公開資訊整理而成。

《開放來源情報在金融情報中心作業與策略分析之應用》（*Use of Open-Source in FIU Operational and Strategic Analysis*）報告全文請參閱： https://egmontgroup.org/wp-content/uploads/2023/07/202302-IEWG-Report-Use-of-OSINT-in-FIU-Operational-and-Strategic-Analysis-Sanitized-Version_FINAL3.pdf

艾格蒙聯盟資訊交換工作小組（Information Exchange Working Group）發布此報告，探討開放來源情報（open source intelligence, **OSINT**）在金融情報中心作業及策略分析中之運用現況。此報告透過來自 61 個金融情報中心蒐集之質化與量化資料，進行主題式及描述性統計分析。研究結果涵蓋以下重點：

- 使用開放來源情報之金融情報中心數量。
- 開放來源情報之實務運用方式。
- 開放來源情報與金融情報之整合方式。
- 開放來源情報所使用之資訊類型。
- 開放來源情報資訊可靠性之評估方法。
- 專責開放來源情報團隊之設置情形，及相關工具之開發現況。

報告結論指出，開放來源情報對於發展犯罪態樣、進行洗錢與資恐之宏觀趨勢分析，以及偵測自然人、法人與其他活動或對象間之關聯性，提供重要且寶貴之資訊來源，惟此類資訊通常難以透過可疑交易報告（STR）取得。

7 縮寫、首字母縮略詞、與貨幣匯率

ABF	澳洲邊境執法局
AED	阿拉伯聯合大公國迪拉姆
AFP	澳洲聯邦警察
AML	防制洗錢
AMLA	防制洗錢法
AMLC	防制洗錢委員會
AMLO	（泰國）防制洗錢辦公室
APG	亞太防制洗錢組織
ASIC	澳洲證券與投資委員會
ATM	自動櫃員機
ATO	澳洲稅務局
AUSTRAC	澳洲交易報告與分析中心
BND	汶萊元
CAMLMAC	中國防制洗錢監測分析中心
CDD	客戶盡職調查
CFATF	加勒比海防制洗錢金融行動工作組織
CFT	打擊資恐
CTR	現金交易報告
DNFBP	指定之非金融事業或人員
EAG	歐亞防制洗錢及打擊資恐組織
EDD	加強盡職審查
ERWTF	極右翼資恐
EUR	歐元
FATF	防制洗錢金融行動工作組織
FI	金融機構
FIU	金融情報中心
FJD	斐濟元
FMU	（巴基斯坦）金融監控中心
FPTBTS	虛構稅務發票（印尼）
FSRB	區域性防制洗錢組織
GIABA	西非政府間防制洗錢組織
GIF	（中國澳門）金融情報辦公室
HKD	港幣
IDR	印尼盾
IFTI	國際資金移轉指示
INTERPOL	國際刑事警察組織（簡稱國際刑警組織）
IPOA-IUU	預防、制止和消除非法、未報告及不受規範捕魚之國際行動計畫非法、未報告、不受規範（IUU）捕魚行為
JAFIC	日本金融情報中心
JPY	日圓
KYC	認識你的客戶
LEA	執法機關
MENAFATF	中東及北非防制洗錢金融行動工作組織
MLA	刑事司法互助
ML	洗錢
MLO	洗錢組織
MNT	圖格里克，蒙古官方貨幣

MONEYVAL	歐洲理事會防制洗錢及打擊資恐評估專家委員會
MoJ	法務部
MOP	澳門幣，中國澳門之官方貨幣
MVTS	金錢或價值移轉服務
MYR	馬來西亞幣
NCC	（馬來西亞）國家防制洗錢協調委員會
NGO	非政府組織
NPO	非營利組織
NRA	國家風險評估
NZD	紐西蘭元
OECD	經濟合作暨發展組織
PEP	重要政治性職務人士
PF	資武擴
PHP	菲律賓比索
PKR	巴基斯坦盧比
PoE	專家小組
PPATK	（印尼）金融交易報告與分析中心
PPP	公私部門合作機制
RBF	斐濟儲備銀行
RFMO	區域漁業管理組織
RMB	中國人民幣
RM	馬來西亞幣
SBD	索羅門群島元
SEC	（菲律賓）證券交易委員會
SGD	新加坡元
SIMP	美國海產品進口監控計畫
STR	可疑交易報告
STRO	可疑交易報告辦公室，新加坡之金融情報中心
SVF	儲值支付工具
TF	資恐
THB	泰銖
UNCLOS	聯合國海洋法公約
UN CTED	聯合國反恐委員會執行局
UNODC	聯合國毒品與犯罪問題辦公室
USD	美元
VAT	加值營業稅
VND	越南盾
WMD	大規模毀滅性武器

貨幣兌換表

除非提交案例之司法管轄區選擇將其國內貨幣價值轉換為約略之美元價值（USD），否則本報告中之金額一律以該司法管轄區之國內貨幣價值表示。以下貨幣兌換表採用 XE 網站所提供之 2023 年 11 月 8 日單一時間點之匯率。「轉換為美元」欄位代表每單位相應貨幣可兌換之美元金額。

司法管轄區	貨幣（單位）	縮寫	轉換為美元（USD）
澳洲	澳幣	AUD	0.643
孟加拉	孟加拉塔卡	BDT	0.009
中國	中國人民幣	CNY	0.137
庫克群島	紐西蘭元	NZD	0.593
歐盟	歐元	EURO	1.069
中國香港	港幣	HKD	0.127
印尼	印尼盾	IDR	0.000063
日本	日圓	JPY	0.006650
大韓民國	南韓圜	KRW	0.000766
中國澳門	澳門幣	MOP	0.124
馬來西亞	馬來西亞幣	MYR	0.214
蒙古	蒙古幣	MNT	0.000289
巴基斯坦	巴基斯坦盧比	PKR	0.003
菲律賓	菲律賓比索	PHP	0.017
新加坡	新加坡元	SGD	0.738
索羅門群島	索羅門群島幣	SBD	0.118
中華臺北	新台幣	TWD	0.031
泰國	泰銖	THB	0.028

8 索引

索引詞彙後方之數字為本報告內之頁碼。