



Asia/Pacific Group
ON MONEY LAUNDERING

APG 年度 態樣報告 2024

洗錢、資恐及資武擴之手法與趨勢

2024 年 11 月

亞太防制洗錢組織

目錄

| | |
|-------------------------------|-----------|
| 前言 | 3 |
| 方法論 | 4 |
| 1 - 法人濫用 | 5 |
| 1.1 概述 | 5 |
| 1.2 成員國對法人濫用所帶來的洗錢及資恐風險之認知 | 6 |
| 1.3 專業協助者 | 18 |
| 1.4 捍衛機制 | 25 |
| 1.5 共通之處 | 36 |
| 1.6 結語 | 38 |
| 2 - 洗錢及資恐之手法 | 39 |
| 2.1 澳洲 | 39 |
| 2.2 庫克群島 | 40 |
| 2.3 中國香港 | 41 |
| 2.4 印度 | 43 |
| 2.5 印尼 | 44 |
| 2.6 日本 | 45 |
| 2.7 韓國 | 47 |
| 2.8 中國澳門 | 47 |
| 2.9 馬來西亞 | 49 |
| 2.10 馬爾地夫 | 50 |
| 2.11 巴基斯坦 | 51 |
| 2.12 菲律賓 | 57 |
| 2.13 新加坡 | 60 |
| 2.14 中華臺北 | 63 |
| 3 - 洗錢及資恐趨勢 | 68 |
| 3.1 近期洗錢及資恐手法及趨勢之研究成果 | 68 |
| 3.2 新興趨勢、下降趨勢與持續趨勢之觀察 | 73 |
| 3.3 防制洗錢及打擊資恐立法、監理或執法措施之成效 | 82 |
| 4 - 資武擴之手法與趨勢 | 87 |
| 4.1 觀察員組織之倡議 | 88 |
| 4.2 近期有關資武擴手法及趨勢之風險評估、研究或調查報告 | 92 |

| | | |
|----------|---|------------|
| 4.3 | 金融機構、指定之非金融事業或人員（DNFBP）、虛擬資產服務提供商或其他相關產業之指引文件 | 94 |
| 4.4 | 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 | 97 |
| 4.5 | 資武擴—法人及專業協助者之濫用情形 | 99 |
| 4.6 | 船舶登記制度 | 100 |
| 5 | - 資產返還之方法與趨勢 | 103 |
| 5.1 | 資產追查，包括限制措施—鎖定及調查國內外犯罪所得、犯罪工具或同等價值之財產 | 105 |
| 5.2 | 管理凍結／扣押資產：關於資產管理案件之資訊，以及供資產管理機構使用之程序或作業手冊 | 113 |
| 5.3 | 資產沒入：刑事、民事或行政程序追討犯罪所得之經驗—成就與挑戰 | 114 |
| 5.4 | 被沒入犯罪所得之使用與共享：包括對其他司法管轄區取回或送出被沒入資產之案例 | 115 |
| 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 | 119 |
| 6.1 | 防制洗錢金融行動工作組織 | 119 |
| 6.2 | 加勒比海防制洗錢金融行動工作組織 | 124 |
| 6.3 | 歐亞防制洗錢與打擊資恐組織（EAG） | 124 |
| 6.4 | 東南非防制洗錢組織（ESAAMLG） | 126 |
| 6.5 | 拉丁美洲防制洗錢金融行動工作組織 | 127 |
| 6.6 | 中東與北非防制洗錢金融行動工作組織（MENAFATF） | 127 |
| 6.7 | 專家委員會防制洗錢措施之評估 | 128 |
| 6.8 | 亞洲開發銀行 | 128 |
| 6.9 | 國際貨幣基金組織 | 130 |
| 6.10 | 聯合國毒品犯罪辦公室 | 132 |
| 6.11 | 世界銀行集團 | 134 |
| 6.12 | 世界海關組織 | 135 |
| 7 | - 縮寫、首字母縮略詞、與貨幣匯率 | 141 |
| 8 | - 索引 | 143 |

前言

歡迎審閱《亞太防制洗錢組織（APG）2024 年度洗錢態樣報告》。

APG 成員國、觀察員組織及若干非觀察員機構，每年皆與 APG 秘書處通力合作，深入淺出且詳實地分析亞太地區乃至國際間當前及新興的洗錢、資恐及資武擴（ML/TF/PF）之態樣。

此等威脅與相關犯罪緊密交織，而且不斷增加，往往涉及複雜的跨國金融犯罪，但多數情況下仍以地方層面的影響最為明顯。防制洗錢金融行動工作組織（FATF）的建議對於在全球範圍內有效減輕此類威脅至關重要，而 APG 在協助其會員於亞太地區有效落實這些建議方面，亦扮演不可或缺的角色。

APG 營運委員會（Operations Committee），尤其是營運委員會共同主席，更是 APG 態樣分析計畫成敗的關鍵所在。本計畫得以成功推展，有賴即將卸任的印度籍共同主席 Pandey 的卓越領導（職務將由 Swain 接任），以及另一共同主席，薩摩亞央行總裁 Atalina 長期的卓越貢獻。

本報告使得 APG 年度態樣研討會，以及營運委員會之各項持續進行工作更加完善，展現出成員國致力於識別、及應對持續變化中各種洗錢態樣的不懈努力，特別是法人遭不當利用及專業協助者所扮演角色等相關議題。本報告亦指出，既有的防制洗錢、打擊資恐及打擊資武擴改革已見實施成效，大幅降低過去匿名帳戶及空殼銀行易受濫用之情事，

此正為成員國間合作互信精神的典範，也是 APG 成功應對區域挑戰及影響全球應對措施的關鍵所在。未來我們仍須秉持此一合作精神，確保態樣分析工作 APG 的整體行動緊密結合。

在此，我要誠摯感謝所有 APG 成員國及觀察員組織對本報告的寶貴貢獻，同時也要向非觀察員機構以及 APG 秘書處專業盡職的全體同仁表達衷心的謝意，感謝他們為本報告編纂所付出的卓越努力。

APG 秘書處對於能夠支援如此多元、專業且積極參與的成員國及觀察員組織感到無比自豪，本報告所體現的集體成就，堪稱已臻世界頂尖水準。

執行秘書 克里斯·布萊克博士（Dr Chris Black）

亞太防制洗錢組織



圖片：2023 年度 APG 態樣研討會，於印度新德里（New Delhi, India）舉行

方法論

亞太防制洗錢組織（Asia Pacific Group on Money Laundering, APG）是亞太地區的類 FATF¹ 區域性防制洗錢組織。APG 其中一項任務是發布區域性洗錢（Money Laundering, ML）、資助恐怖主義（資恐）（Terrorism Financing, TF）與資武擴（proliferation financing, PF）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、資恐與資武擴威脅的本質，並制定有效因應策略。當一連串洗錢、資恐與資武擴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 成員制定有效調查、並起訴洗錢、資恐與資武擴的策略，同時設計並落實有效的預防性措施。

APG 成員國及觀察員組織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，資武擴僅代表亞太地區及其他區域執法與情報機關偵查與防制洗錢、打擊資恐、及資武擴之少數成果。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。

為保護案例隱私，本報告已針對案件中涉案人與犯罪者之姓名、公司名稱及涉及其他轄區相關資訊，進行去識別化編輯處理，以匿名化案例內容。若 APG 會員提及該轄區及當地權責機關，則予以保留。個人多以「人士」稱呼並以字母標識，例如「A 人士」。於同一案例內之「A 人士」指同一人；但不同案例中之「A 人士」則往往代表不同個人。「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。貨幣除另行標註為美元（USD）外，均以提供案例之 APG 成員國當地貨幣顯示，第 7 節附有貨幣兌換表供參考。

APG 營運委員會（Operations Committee）負責督導態樣研究計畫；由薩摩亞央行總裁 Maiava Atalina Ainuu-Enari 女士及印度財政部 Smarak Swain 先生共同擔任主席。

¹ 防制洗錢金融行動工作組織（FATF）：<https://www.fatf-gafi.org/en/home.html>

1 - 法人濫用

1.1 概述

人們使用法人從事各種合法的商業活動，法人於各國經濟中亦扮演著不可或缺的重要角色。在大多數司法管轄區內，個人可以快速便捷地成立具獨立法律人格之法人，透過申報義務機構提供之金融產品（包括公司銀行帳戶、企業信用卡、貸款等），得以輕易進入全球金融體系。

Legal Persons (法人)

「法人」係指除自然人以外之任何實體，可與金融機構建立永久客戶關係或擁有財產，包括公司、法人團體、基金會、機構 (*anstalt*)、合夥關係或協會及其他類似實體。

隨著各司法管轄區落實防制洗錢、打擊資恐及資武擴 (AML/CTF/CPF) 改革，匿名個人銀行帳戶及空殼銀行（即在任何司法管轄區內均無實體業務之銀行）已大幅減少。於是，包括空殼公司在內之法人便成為犯罪分子從事洗錢、資恐及資武擴活動 (ML/TF/PF) 的主要工具。²

容易設立、以及易於掩飾其實質受益權與所有權，是法人的兩大關鍵弱點。由於法人結構複雜及／或不透明，權責機關往往難以取得正確之實質受益權資訊，因而妨礙釐清犯罪責任歸屬及追查資金流向與資產；尤其當實質受益人及／或專業協助者 (professional enablers，例如信託及公司服務業者 [TCSP]) 位於其他司法管轄區時，法人被濫用的風險將顯著增加，所造成的執法與監管困難也隨之加劇。³

更嚴謹的 FATF 標準

2022 年 3 月，FATF 強化第 24 項建議 (R.24) 及其相關之註釋，內容涉及法人之透明度及實質受益權。FATF 亦發布最新指引，以協助各司法管轄區落實強化第 24 項建議之要求。⁴

現行第 24 項建議要求各司法管轄區評估及處理法人帶來之風險，範圍不僅限於在該管轄區內成立之法人，亦涵蓋由外國人士成立、但與該管轄區具有充分經濟活動聯繫之法人。值得注意的是，第 24 項建議明確要求各管轄區採取多管齊下的方式，確保權責機關能及時取得透過不同機制所蒐集的實質受益權資訊。⁵

犯罪分子濫用法人或法人網路之原因可能包括：

- 與犯罪活動保持距離。
- 隱藏資產的真正所有權，包括重要政治性職務人士 (PEP) 的資產。
- 為大額資金移轉提供表面的合法商業理由。
- 將犯罪所得與合法資金混合。
- 以消費或投資方式處理犯罪所得。
- 達成貪污、詐欺及逃稅的目的。
- 轉移所收取的賄賂款項或所挪用之公款。
- 保護以犯罪所得獲取的資產。

² 世界銀行集團 (World Bank Group) - 《國家洗錢及資恐風險評估工具包》 (National Money Laundering and Terrorist Financing Risk Assessment Toolkit) : <https://star.worldbank.org/sites/default/files/2023-03/Legal%20Persons%20and%20Arrangements%20ML%20Risk%20Assessment%20Tool.pdf>

³ 新加坡銀行公會 (The Association of Banks in Singapore) 與新加坡金融管理局 (Monetary Authority of Singapore) 防制洗錢及打擊資恐產業合作計畫 — 《法人濫用態樣及最佳實務指南》 (Misuse Typologies and Best Practices) : <https://abs.org.sg/docs/library/legal-persons-misuse-typologies-and-best-practice.pdf>

⁴ FATF - 實質受益權 (Beneficial Ownership) : <https://www.fatf-gafi.org/en/topics/beneficial-ownership.html>

⁵ FATF - FATF 建議 : <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html>

今年 APG 秘書處邀請成員國分享法人濫用之經驗。各成員國提供了詳盡的回應，因此本章聚焦於法人濫用與洗錢行為之交集；並彰顯 APG 觀察員組織及其他政府／非政府組織在此領域之努力。成員國亦提供多達 138 個案例研究，描述最新的洗錢、資恐與資武擴手法及趨勢，包含法人濫用之案例。成員國有關法人濫用與資恐之資訊另列於第 2 章及第 3 章；法人濫用於資武擴及逃避金融制裁之資訊則於第 4 章。

1.2 成員國對法人濫用所帶來的洗錢及資恐風險之認知

評估洗錢及資恐風險，包括不同法人類型帶來之風險，是 FATF 要求各司法管轄區維護自身、及全球金融體系健全性的重要基礎。唯有充分識別各種洗錢及資恐風險，各司法管轄區方能有效地抵減並管理此等風險。各司法管轄區權責機關必須進行詳實的初步與持續風險評估，以識別自身弱點並實施有效的防制措施；此有助各司法管轄區理解犯罪分子如何在其管轄內或區域內濫用法人進行洗錢及資恐活動，藉此訂定更具精準性的法規與監理機制，以有效降低及控管相關風險。

根據 FATF 建議，各司法管轄區須依第 1 項建議評估洗錢、資恐與資武擴風險，並依第 24 項建議評估與法人相關之洗錢及資恐風險。第 24 項建議要求各司法管轄區評估在當地成立或管理之法人，以及與管轄區具有充分經濟聯繫之外國法人所涉之洗錢及資恐風險。APG 42 個成員國中，有 38 個（90%）已接受 2012 年更新 FATF 方法論。⁶ 下之相互評鑑。本報告以下列出這些相互評估報告之結果，惟應注意部分報告發表已數年，各管轄區在此後已有顯著改善。

成員國對法人濫用引發之洗錢及資恐風險之認知：

- 6 個成員國（14%）在接受相互評鑑時已評估過法人相關之洗錢及資恐風險。⁷
- 20 個成員國（48%）在相互評鑑當時已評估過法人相關之風險，但評鑑團隊認為該等評估仍存在諸多缺失，包括過於基礎或一般化、不夠全面、未涵蓋所有類型之法人、未同時評估國內及國際法人、或未評估洗錢與/或資恐風險。⁸
- 6 個成員國（14%）在接受相互評鑑時尚未評估法人相關之洗錢及資恐風險，但其後已進行評估。⁹
- 6 個成員國（14%）在接受相互評估時尚未評估法人相關之洗錢及資恐風險。¹⁰

儘管成員國對於洗錢及資恐風險之認知已有提升，但相關資料顯示，許多成員國仍在努力釐清與法人相關的洗錢及資恐風險。

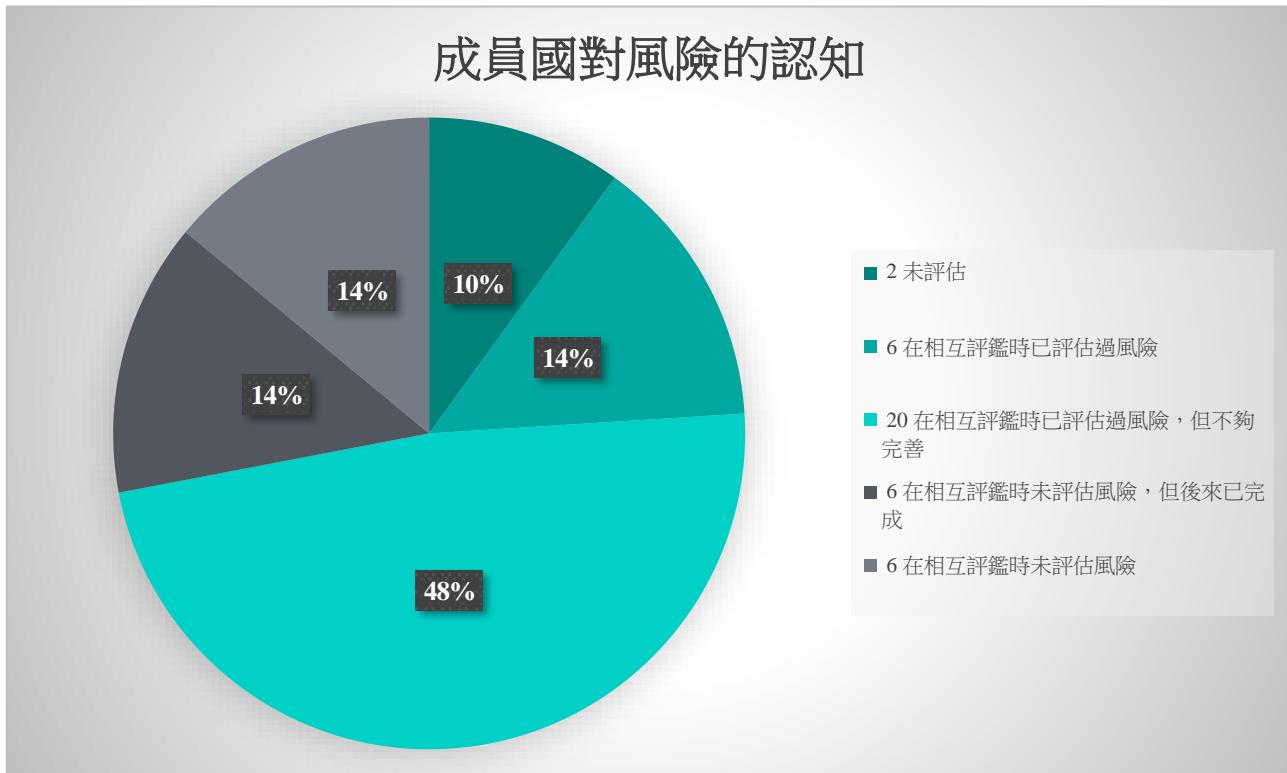
⁶ 馬爾地夫與紐埃（Niue）目前正在進行相互評鑑，而僅剩阿富汗與吐瓦魯（Tuvalu）尚未接受評鑑。

⁷ 加拿大、印度、印尼、韓國、紐西蘭及美國。

⁸ 孟加拉、中華臺北、庫克群島、中國香港、日本、中國澳門、馬來西亞、馬紹爾群島、蒙古、緬甸、諾魯（Nauru）、巴基斯坦、帛琉、薩摩亞、所羅門群島、東帝汶、泰國、東加、萬那杜及越南。

⁹ 澳洲、不丹、汶萊、菲律賓、新加坡及斯里蘭卡。

¹⁰ 柬埔寨、中國、斐濟、寮國、尼泊爾及巴布亞紐幾內亞。



部分成員國已透過重新進行國家風險評估（National Risk Assessment, NRA），或針對特定威脅及產業別的風險評估，以更新其對洗錢／資恐（及資武擴）風險的掌握與認識；以下列出若干相關計畫之範例。¹¹ 值得注意的是，一個成員國將境外金融部門內之法人與法律協議遭濫用情形評估為其境內最主要的洗錢及資恐威脅。¹²

澳洲

澳洲於其發布之《澳洲洗錢國家風險評估》（*Money Laundering in Australia National Risk Assessment*¹³）中，將法人與法律協議評定為**高度且持續存在的洗錢風險**。主要評估論據包括：

- 犯罪分子持續利用法人（及法律協議）與相關銀行業務安排，儲存及移轉大量犯罪所得資金，包括移往境外。
- 法人（及法律協議）設立相對容易，且能有效掩飾受益所有人之身分。
- 澳洲缺乏系統性蒐集、驗證及提供實質受益權資訊之全面性機制，因而限制政府機關透過法人結構偵測及調查洗錢活動之能力。此外，凍結及沒入公司或信託所持有之犯罪資產亦存在實務上的困難，且需要龐大與資源。
- 境外法人（及法律協議）可能進一步掩飾資金流向及實質受益權資訊，特別是當法人結構設立於秘密司法管轄區或跨越多個管轄區時，此一情況更為顯著。
- 專業服務業者在設立及管理被用以隱匿財富及洗錢之複雜法人與法律協議中扮演關鍵角色。

¹¹ 此外，其他會員國提供資訊指出：寮國正對所有法人進行洗錢及資恐風險評估，預計 2024 年底發表；馬來西亞即將完成第五版國家風險評估；馬爾地夫最近在國家風險評估中將法人評估為中等洗錢及資恐風險；新加坡目前正在更新法人洗錢及資恐風險評估，該風險仍維持為優先級別；越南亦已開始進行包含法人評估之洗錢及資恐國家風險評估。

¹² 《亞太防制洗錢組織 - 庫克群島相互評鑑報告》：<https://apgml.org/members-and-observers/members/member-documents.aspx?m=5c63cd37-73a2-4a45-aac3-f6e5b8ec0594>

¹³ 澳洲交易報告與分析中心（AUSTRAC）- 《澳洲國家洗錢風險評估》（*Money Laundering in Australia National Risk Assessment*）：<https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf>

值得注意的是，澳洲強調專業服務業者**持續協助**建立複雜商業結構及相關銀行安排，幫助個人洗錢及隱匿財富。¹⁴

加拿大

加拿大¹⁵近期發布《加拿大洗錢及資恐怖固有風險評估更新報告》，其中涵蓋法人、合夥組織及非營利組織（NPO）的洗錢及資恐風險評估。

- 加拿大將法人及合夥組織的洗錢及資恐風險分別評定為「極高」與「高」。

中國

中國近期對所有法人進行洗錢及資恐風險評估，涵蓋所有類型的境內法人，以及在中國境內營運的外國法人。

- 主要態樣包括透過法人實體**隱匿洗錢者身分**，以取得並洗白（launder）犯罪所得，或**透過空殼公司**或前台公司（front company）進行**虛假交易**。

印尼

印尼已完成《2022年法人洗錢及資恐風險部門評估報告》，該評估檢視2019年至2022年之資料，充分展現司法管轄區如何透過聚焦於特定部門與/或威脅情勢之評估，持續掌握洗錢與資恐風險之最新變化。主要發現包括：

- 就前置犯罪（predicate crime）類型而言，在法人中貪污及毒品犯罪是具高度洗錢風險的前置犯罪。
- 依據法人類型，國內持有及資金來源之有限責任公司（Limited Liability Companies, LLC）被視為具高度洗錢風險。
- 就產業類型而言，營造、貿易、投資及金融、採礦及物流業法人被認為具較高洗錢風險。
- 就申報單位產業而言，銀行業被認為是高度易於被法人利用為洗錢之管道。
- 就交易傳送管道而言，現金存款及跨境資金轉移被認定為具高度法人洗錢風險。
- 法人洗錢於之新興態樣，係利用不具海牙認證（apostille）¹⁶效力之國家簽發、用於投資目的之文書之漏洞，並藉由虛擬公司或虛擬辦公室掩飾身分。

中國澳門

中國澳門近期完成《2022年澳門特別行政區洗錢、資恐與資武擴風險評估報告》（Macao Special Administrative Region Risk Assessment Report on Money Laundering/Terrorist Financing/Financing of Proliferation of Weapons of Mass Destruction (2022)）中國澳門指出澳門金融情報辦公室（GIF）已密切監控法人或信託及公司服務業者（TCSP）服務遭濫用的可能性。

此外，隸屬GIF的金融資訊分析小組於2023年進行**特別策略審查**，識別部分**可疑空殼公司**，並將個案彙整結果送交監理機關—法律事務局（Legal Affairs Bureau）。目前澳門金融情報辦公室正以**可疑交易報告**（STR）資訊進行另一主題策略分析，以識別可能與空殼公司有關的信託及公司服務業者。該辦公室同時透過**公私部門夥伴關係**，定期向申報實體分享策略分析結果，以增強其風險防制及抵減措施。

¹⁴ 澳洲稅務局（ATO）所主導的跨機構「重大金融犯罪專案小組」（Serious Financial Crime Taskforce, SFCT）於其官網上指出，專案小組關注焦點之一為「專業協助者」（professional enablers）：<https://www.ato.gov.au/about-ato/tax-avoidance/the-fight-against-tax-crime/our-focus/serious-financial-crime-taskforce/how-the-taskforce-operates>

¹⁵ 加拿大政府《加拿大洗錢及資恐固有風險更新評估報告》（Government of Canada - Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada）：<https://www.canada.ca/en/department-finance/programs/financial-sector-policy/updated-assessment-inherent-risks-money-laundering-terrorist-financing-canada.html>

¹⁶ 一種文書驗證形式，旨在簡化公開文書之國際認證與法律化程序，使該等文書於國際間可被承認。

關於法人濫用之新興趨勢、下降趨勢與持續趨勢

關於法人濫用之相關趨勢，各成員國一致指出法人常被用於詐欺犯罪，包括電子郵件及電話詐欺、投資詐欺、企業電子郵件入侵及逃漏稅等。¹⁷

其他觀察到的前置犯罪還包括竊盜、侵占、貪污、賄賂及貪污、證券及市場操縱、走私、毒品販運及散布猥褻物品等。¹⁸ 觀察發現，法人被用於從事洗錢活動的情形相當普遍，其中以「貿易洗錢」（Trade-based money-laundering）最為明顯。¹⁹

部分成員國指出觀察到的趨勢具有跨國性質。庫克群島於 2023 年共接獲 9 起國際請求案，要求提供該司法管轄區內所註冊法人之相關資訊。日本則指出其境內詐欺案件常涉及境外司法管轄區。中華臺北觀察到，境外法人於境內設立子公司，以竊取營業秘密；而中華臺北國民亦透過於海外租稅天堂（tax havens）或境外金融中心設立公司，或經由管理公司、顧問公司等管道控制上述公司，以從事犯罪行為。

各成員國普遍指出，法人濫用的主要形式包括：利用空殼公司（shell companies）、以人頭董事/名義董事（stooge directors/nominees）作為掩護，以及使用企業帳戶移轉並混合資金，或建立貸款安排。印尼觀察到不法分子利用虛構法人、法律地位不明之法人（如缺乏營業執照或機構許可），以及以人頭戶（如登記之密切關聯人或家庭成員）隱匿法人背後真正受益所有人之身分。

日本亦指出，有時所涉法人根本未取得正式法律地位，或其法律地位不明確。日本提出的法人濫用之紅旗指標（red flag indicators）包括：初始資本極少（金額僅數萬至數十萬日圓）、經常變更地址或公司高階主管，以及從事業務範圍缺乏相關聯性、且營運模式可疑之公司。此外，日本與印尼均指出，被濫用之法人通常還伴隨其他法規問題，例如缺乏適當營業許可；日本則另外提及此類公司常違反有關接受捐贈、收受存款、或違反《貸金業法》（Interest Rates/Money Lending Business Act）等規範。

法人之風險評估方法論

數個技術援助提供機構已將重點放在，司法管轄區針對法人之風險評估所存在的缺口。以下為世界銀行集團與歐盟防制洗錢全球設施（EU Global Facility）就風險評估方法論，以及將其應用於司法管轄區時所面臨之挑戰，所提出之重要見解。

¹⁷ 庫克群島，中國香港，日本，新加坡。中華臺北，越南

¹⁸ 庫克群島，中國香港，日本，馬爾地夫，新加坡，中華臺北。

¹⁹ 馬爾地夫。

世界銀行集團 - 《國家洗錢及資恐風險評估工具包》(2022年)

2022 年，世界銀行集團的金融市場穩定與廉潔（FSI）部門，與聯合國毒品犯罪辦公室（UNODC）合作成立的追回被盜資產倡議（Stolen Asset Recovery Initiative，StAR）共同制定《國家洗錢及資恐風險評估工具包》（*National Money Laundering and Terrorist Financing Risk Assessment Toolkit*）²⁰（NRA Toolkit）。

各司法管轄區需透過結構化自我評估框架，方能有效理解及抵減法人濫用相關之洗錢及資恐風險；此有助各管轄區以識別威脅與弱點，並制定有針對性的風險抵減策略。《國家洗錢及資恐風險評估工具包》包括指導手冊、Excel 工作表、PowerPoint 簡報及其他輔助材料。

由於犯罪集團經常利用跨司法管轄區之法律漏洞，藉此隱匿其非法活動；在自我評估過程中，世界銀行集團所開發之工具，特別強調法人濫用問題之跨國性質。因此，各司法管轄區必須深入了解「輸出風險」（*exported risks*，即非居住民濫用本國司法管轄區內所設立之法人架構）及「輸入風險」（*imported risks*，即外國法人架構遭濫用並與本國司法管轄區產生關聯之情形）。

《國家洗錢及資恐風險評估工具包》明確要求各司法管轄區，應評估其對非居住之自然人及法人於境內設立法人之吸引力，包括該司法管轄區在法律、制度、經濟、監理及政治架構等各方面之特點，此等特點可能影響其提供公司設立服務（及相關專業服務）予非居住之自然人及法人之吸引力。

紅旗指標

在進行評估時，司法管轄區應考量紅旗指標，以協助辨識本國法律與監管框架之潛在缺口，防止犯罪集團利用這些缺口進行洗錢及資恐活動。此等紅旗指標包括：

- 設立與登記之便利性：法人登記要求寬鬆、成本低廉、處理迅速，可能更吸引犯罪分子利用。
- 實質受益權透明度：實質受益權資訊揭露規定不足或付之闕如，導致取得實質受益權資訊困難；且缺乏有效驗證機制，因而製造隱匿真正所有權與控制權的機會。
- 代名人安排：允許使用名義董事或股東，但缺乏適當管控及透明度，可能導致受益所有人身分遭隱匿。
- 不透明結構：司法管轄區若容許、或未能有效規範如無記名股票、信託及基金會等不透明結構，將增加洗錢與資恐風險。
- 國際合作：國際合作機制薄弱，包括資訊交換及刑事司法互助程序不足，妨礙有效調查與起訴跨國金融犯罪。
- 信託及公司服務業者（TCSP）之規範與監理：對信託及公司服務業者之規範與監理不足，可能導致其涉入協助非法活動。

司法管轄區考量上述紅旗指標後，即能識別自身防制洗錢與打擊資恐系統的特定弱點，並據此擬定更具精準性的風險抵減及管理措施，包括強化法律框架、改善資料蒐集與分享機制、加強監理措施，以及促進國際合作等。

²⁰ 世界銀行集團 - 《法人與法律協議之洗錢風險評估工具》：<https://star.worldbank.org/publications/legal-persons-and-arrangements-money-laundering-risk-assessment-tool>

歐盟防制洗錢全球設施（EU Global Facility）- 挑戰與區域性防制洗錢組織（FSRB）之支持

歐盟防制洗錢全球設施於提供技術支援協助夥伴國家落實法人與法律協議風險評估方法時，觀察到各國普遍面臨以下挑戰：

- **評估之全面性與風險評估方法之適切性**

FATF 在針對法人實質受益權之指引中，建議各司法管轄區應：收集法人登記統計資料；分析可疑交易報告（STR）與執法／檢控案件；識別最常見之態樣；調查信託及公司服務業者（TCSP）之作業方式；進行專家諮詢及其他必要措施，以深入理解各類法人所涉及之風險。此外，FATF 亦已修訂第 24 及第 25 項建議，納入可能涉及洗錢及資恐風險，並與該國有充分經濟聯繫之外國法人結構。為有效進行此分析，各司法管轄區需制定、或採用既有的方法論，明確說明評估國內外各類法人所帶來之威脅、弱點及抵減措施，並解釋所使用之途徑、方法及不同的風險評估標準。最重要的是，此方法論必須貼合管轄區自身的風險與背景，並涵蓋所有 FATF 之強制要求。

- **提供精確之風險評估工具**

各管轄區需使用精確的風險評估工具，此工具不僅必須完整反映該司法管轄區風險評估方法論（methodology）的全面性，更須能嚴格依循該方法論進行評估作業。

- **管轄區風險概況及現有預防措施與工具之風險評估方法論的彈性與適應性**

各司法管轄區的風險概況及所採用之抵減措施各不相同，因此難以設計一套通用之風險評估方法論供所有管轄區使用。目前有多種方法論與工具可供選擇，因此各司法管轄區須確認其所選取的方法論及工具是否具備充分彈性，允許各管轄區依據自身情境進行調整。

- **實務知識、經驗與協調**

最佳操作實務包括由各管轄區相關權責機關代表通力合作，組建風險評估工作小組。成員可能來自金融情報中心、執法機關、公司及實質受益權登記單位、稅務機關、反貪污機關、海關、信託及公司服務業者（TCSP）監管機關、防制洗錢及打擊資恐監管機構，以及金融與非金融部門等。所有工作小組成員應接受方法論教育訓練，並指定單一機關負責協調工作。

- **FSRB之強化指引與支援**

目前各司法管轄區於進行法人風險評估時普遍面臨經驗與知識不足之挑戰。因此，FATF 區域性防制洗錢組織（FSRB）可提供成員國額外指引與支援，協助管轄區發展風險評估方法論與工具，並於成員國間分享相關資源。例如，2022 年歐盟防制洗錢全球設施（EU Global Facility）協助東南非防制洗錢組織（Eastern and Southern Africa Anti-Money Laundering Group，ESAAMLG）制定法人與法律協議之洗錢及資恐風險評估工具，該工具整合歐盟防制洗錢全球設施之法人與法律安排風險評估方法論，並獲 ESAAMLG 正式採用與推薦。

實質受益權：



「隱匿實質受益權的目的很簡單：即確保資產或收入來源無法與真正的受益權人（owner）產生關聯。」

此觀察係來自亞太防制洗錢組織（APG）與澳洲稅務局（ATO）共同撰寫之亞太地區稅務犯罪與洗錢態樣相關研究報告。²¹ 該報告指出，實質受益權的不透明性可能導致應稅所得未能有效課徵，並阻礙後續犯罪所得之沒入或追徵程序進行。儘管該觀察係針對稅務犯罪與相關洗錢行為，但實務上亦適用於所有前置犯罪與獨立洗錢案件。使用公司與信託架構等複雜法人結構，並跨多個司法管轄區，為稅務犯罪與相關洗錢模式的常見特徵。例如，此類架構亦常用以掩飾涉及非法捕魚之船舶或相關公司的實質受益權。²²

此外，根據對 APG 成員國所進行之調查顯示，僅半數受訪國家要求將法人之實質受益權資訊登錄於中央登記處（central registry）。法人之基本資訊及實質受益權資訊往往出現無法取得、不完整或難以存取之情形，嚴重妨礙調查作業及資訊共享之效能。²³ 目前所能取得之實質受益權資訊，大多來自金融機構保存之資料。此外，亦有觀察指出，私部門普遍認為即使未能履行相關資訊申報要求，亦不致面臨具威嚇性之處罰措施。

法人實質受益權之透明化，可作為權責機關辨識法人濫用結構之犯罪者的重要工具，並於分析與調查過程中迅速取得相關資訊。²⁴ 因此，如能及時向權責機關提供法人之法定所有人及實質受益人、法人資產來源及其業務活動等資訊，將可大幅降低法人濫用之情形。²⁵

複雜的所有權結構

犯罪者常利用複雜的所有權結構，以多層次實體、境外實體或複雜的控制機制，以隱匿實質受益人身分，此為準確辨識法人之實質受益人的主要挑戰之一。一般而言，司法管轄區法律通常允許實質受益人依其需求設立複雜的所有權結構；各管轄區通常未限制層次數目、所有權鏈中參與實體之國籍或實質受益人之居住地。同樣地，各管轄區亦普遍未明確禁止循環所有權結構（例如 A 公司持有 B 公司之股權，同時 B 公司又反向持有 A 公司股權），儘管此類結構會妨礙實質受益人之辨識，及／或難以鎖定需負責的自然人。此外，在實務上權責機關可能難以辨識法人結構之複雜性，究竟係為刻意掩飾實質受益人身分，抑或係出於合法商業行為而形成（例如跨國公司透過併購其他公司而導致結構複雜化）。

...一個複雜的所有權結構
會將辨識受益所有人所需付
出的成本，由受益所有人
(不論公司結構簡單或複
雜，其設立費用可能相同)
轉嫁至轄區內權責機關及、
或申報義務機構。

²¹ 亞太防制洗錢組織（APG）與澳洲稅務局（ATO）合著《亞太地區與稅務相關洗錢》報告（*Money Laundering Associated With Tax Crimes in the Asia Pacific*）：<https://apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=5206>

²² 亞太防制洗錢組織 - APG 發表論文：《來自非法捕魚之非法金流》（*Illicit Financial Flows Generated from Illegal Fishing*）：<https://apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=6206#:~:text=The%20paper%20notes%20that%20illegal,to%20national%20and%20regional%20 security.>

²³ Ibid.與FATF - 《法人之實質受益權指引》（*Guidance on Beneficial Ownership for Legal Persons*）：<https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf>

²⁴ 亞太防制洗錢組織（APG）與澳洲稅務局（ATO）合著《亞太地區與稅務相關洗錢》報告（*Money Laundering Associated With Tax Crimes in the Asia Pacific*）：<https://apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=5206>

²⁵ FATF - 《法人之實質受益權指引》（*Guidance on Beneficial Ownership for Legal Persons*）：<https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf>

無論如何，法人結構複雜化將原本應由實質受益人負擔之成本（無論該法人結構簡單或複雜，設立登記費用並無差異），轉嫁予各該司法管轄區之權責機關及、或申報義務機構；因為後者在查證實質受益人時，必須耗費相當多的時間與資源，方能逐層查證法人結構中各層次之法律所有人及實質受益人。

至於何謂「複雜」（complex）的法人結構，則由各司法管轄區或申報義務機構自行判斷認定；此可能受到法人所屬之部門、產業、員工人數或營收規模等因素影響。舉例而言，跨國公司具有複雜結構可能屬於正常現象；但若重要政治性職務人士（PEP）僅為持有不動產資產而建立相似之複雜法人結構時，則容易令人起疑。

在歐盟防制洗錢全球設施所促成之討論中，²⁶ 專家群列出以下**指標及策略，可協助權責機關及申報義務機構辨識複雜的法人結構：**

- 所有權鏈的垂直及水平層級數目。
- 代名人（nominees）之使用。²⁷
- 外國實體的參與，尤其是來自高風險或黑名單司法管轄區的實體。
- 存在法律協議（信託）²⁸ 與其他法人結合使用之情形。²⁹
- 持有投資基金或上市公司的持股，尤其來自外國司法管轄區者。
- 持股比例稍低於實質受益權透明化的門檻（例如持股比例為 24.98%）。
- 登記資訊中揭露高階管理人員而非實質受益人資訊。
- 缺乏載明實質受益人的書面文件（例如僅由代名人與實質受益人口頭溝通，或透過授權書安排使實質受益人不持有股份，甚至不間接持有）。
- 公開文件中使用「通用術語」，例如：「約翰·史密斯指的是約翰·史密斯本人，或其家庭成員，或為約翰·史密斯本人或其家庭成員及其繼承人、遺囑執行人、遺產管理人、繼任者及法定代表人利益所設立之信託、合夥或有限責任公司」。

此外，專家建議各司法管轄區可透過下列措施降低複雜的所有權結構所衍生的隱匿風險。此等措施包括：

- 要求法人揭露完整所有權鏈（直至實質受益人及非實質受益人）。
- 分析並統計轄區內之法人，以確認「常見／正常結構」（此有助權責機關與申報義務機構更有效辨識異常結構）。
- 透過相互連結之登記資料庫，建立實質受益權資訊之公開資料以供大眾線上查詢。
- 對法人結構明顯過於複雜或風險過高者，實施加強盡職調查（enhanced due diligence），或拒絕其成立及開設銀行帳戶。
- 運用新技術如人工智慧（AI）及／或大數據，以連結不同資料庫（例如稅務資訊、居住資訊等）。
- 將舉證責任轉移至法人本身（即若法人結構受到質疑，法人須自行證明結構合法性，並確保所提供之資訊之正確性）。
- 落實吹哨者制度（whistle-blower programmes）。

²⁶ 歐盟防制洗錢全球設施 - 《實質受益權與複雜的所有權結構》（*Beneficial Ownership And Complex Ownership Structures*）：
<https://www.global-amcft.eu/wp-content/uploads/2023/01/BO-Series-1-Webinar-pages-2022.pdf>

²⁷ 非正式代名人（informal nominees）較難被發現，尤其當涉及非法金錢支付或脅迫，而非基於家庭關係時，情況更為嚴重。

²⁸ 許多國家並未要求信託（trusts）必須登記，因此可能無法取得信託存在或其相關資訊之記錄。

²⁹ 儘管信託通常要求所有信託相關方均應被辨識，且無設定門檻（thresholds），但若將公司加入作為信託之一方，則實務上會產生門檻效果（僅達到一定持股比例門檻者，才會被辨識為該公司之實質受益人，進而成為該信託之實質受益人）。

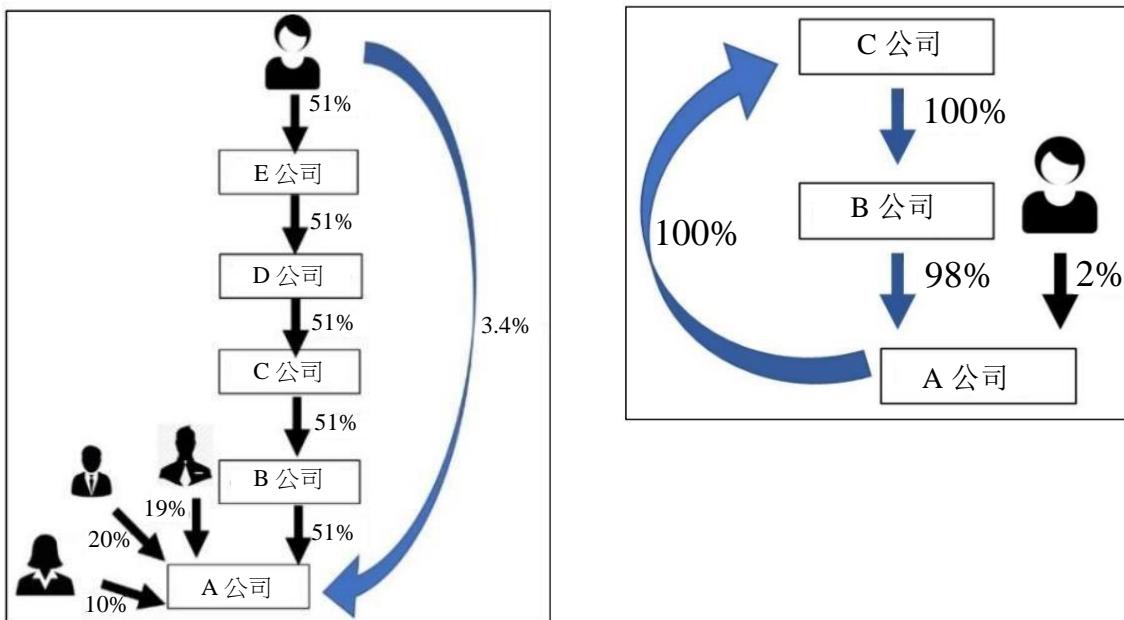
澳洲於《澳洲國家洗錢風險評估》報告³⁰中指出，以下一種或多種合法活動可能建構出複雜的所有權結構：

- 使用母公司與子公司間的實體結構。
- 設立信託、交易及營運用之商業帳戶。
- 使用「控股公司」（holding companies）、合資企業、合夥關係、當事方間「貸款」（inter-party loans）、服務協議及「信用額度」。
- 使用其他結構或安排，例如加盟店總部／加盟店結構、多層次傳銷組織、授權者／被授權者協議，以及財務與法律文書（例如授權書、契約書與合約）。

複雜的所有權結構亦可能透過「實質董事」（de facto directors）或「影子董事」（shadow directors）建立。實質董事，係指未列於公司登記權責機關記錄，但實際執行董事職能之人員，其職銜可能為「業務發展總監」、「主席」或「負責人」等。影子董事則透過傀儡或名義董事執行職務。在澳洲，法人使用實質董事或影子董事均屬非法行為。

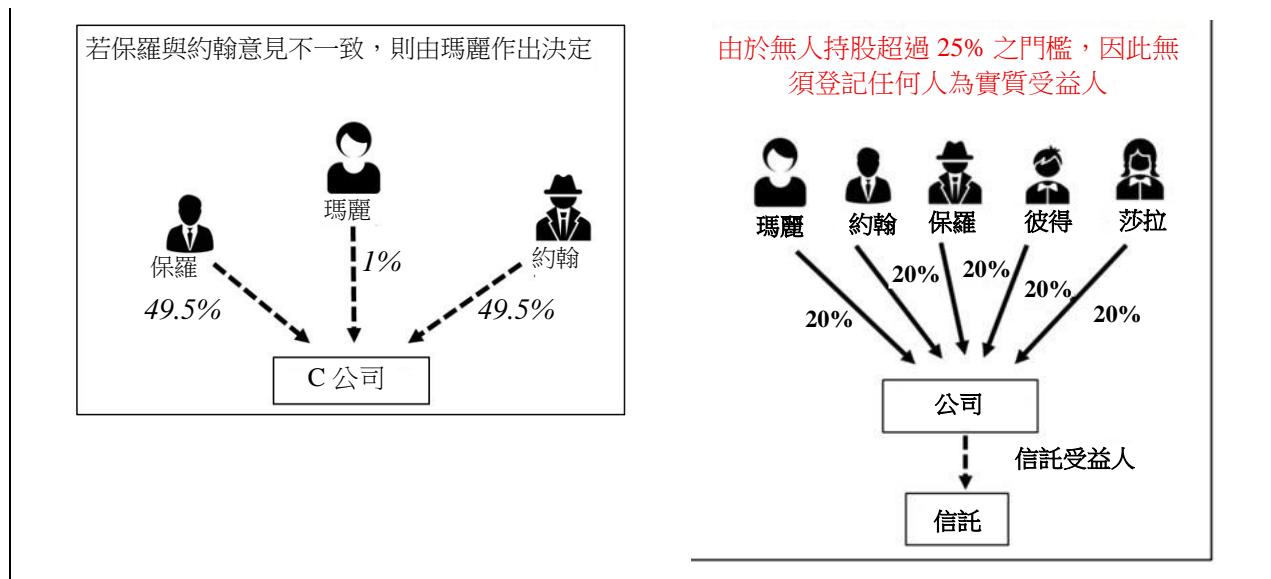
租稅正義網路（Tax Justice Network）—《複雜的所有權結構：實質受益權透明化之風險探討》（2020年）

2020 年，租稅正義網路與倫敦城市大學、國際企業稅務改革獨立委員會（Independent Commission for the Reform of International Corporate Taxation）、國際透明組織及財務透明聯盟（Transparency International, and the Financial Transparency Coalition）共同舉辦一場圓桌會議，探討複雜的所有權鏈結構及其在透明度與稅務濫用上的風險，以及相關的監管潛力。來自學術界、國際組織、公民社會、司法管轄區權責機關及私部門共 52 位專家與研究人員參與該圓桌會議。會議產出的簡報《複雜的所有權結構：實質受益權透明化之風險探討》（Complex Ownership Structures Addressing the Risks for Beneficial Ownership Transparency）³¹，包含有關常見複雜的所有權結構之圖示說明，例如：



³⁰ 澳洲交易報告與分析中心（AUSTRAC） - 《澳洲國家洗錢風險評估》：<https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf>

³¹ 租稅正義網路 —《複雜的所有權結構：實質受益權透明化之風險探討》：<https://taxjustice.net/wp-content/uploads/2022/02/Complex-ownership-chains-Reduced-Andres-Knobel-MB-AK.pdf>



代名人

代名人可以是自然人或法人，在法人內擔任代理人角色，依據對該法人具有較實質受益權及／或所有權主張之實質所有人（nominator）指示行事。通常，該實質所有人（nominator）即為該法人之實質受益人（beneficial owner）。儘管許多名義安排具有合法的商業目的，惟代名人可能被蓄意利用來規避實質受益權透明化措施，從而促成法人被濫用於洗錢及資恐目的。最常見的代名人類型包括名義董事與名義股東。³²

案例研究 #1：涉及哈瓦拉（hawala）之洗錢調查

詐欺，包括偽造；自我洗錢；金錢或價值移轉服務；使用法人與法律協議

2018 年，印度執法局（Enforcement Directorate, ED）依據 1999 年《外匯管理法》（*Foreign Exchange Management Act*）進行調查，發現一個犯罪集團的主謀及其共犯於印度境內外設立大量空殼公司（印度境內 450 家；主要位於杜拜及中國香港的 104 家；及以偽造文件成立的 102 家實體）。德里警方經濟犯罪調查組依據執法局的初步調查，對該案所涉之詐欺、偽造、文件造假及有組織犯罪共謀等情事展開前置犯罪調查。

該犯罪集團的作案方式包括為空殼公司招募掛名董事，並利用偽造的照片及身分文件創建虛構人員，用於設立公司、開設銀行帳戶及欺詐性交易。

主要共犯依據主謀指示管理辦公場所、招募員工及處理銀行交易。此外，該犯罪集團透過循環交易及提供空轉帳務服務以協助國內運作，並藉由空殼公司的多個帳戶製造虛構交易額。

主謀另成立虛設旅行公司，將資金匯往杜拜、中國香港及新加坡等海外司法管轄區，境外實體則透過偽造的外國旅客文件，向印度境內核准外匯經銷商提供偽造資訊，以便執行外匯匯款。

調查過程中，執法單位蒐集彙整公司事務部（Ministry of Corporate Affairs）入口網站資料、所得稅申報資料、來自移民局的護照及旅行記錄、金融情報中心提供的可疑交易報告及現金交易報告，以及銀行帳戶交易資料等。調查確認該集團透過洗錢活動處理之非法所得高達 56.5 億印度盧比（約 6,729 萬美元）。

裁定機關（Adjudicating Authority）確認對 8 億印度盧比（約 950 萬美元）的資產扣押處分，相關當局並已對主謀提出刑事指控，於 2020 年與 2022 年正式提交起訴書。包含哈瓦拉（hawala）業者在內的 16 名嫌疑人遭提起指控，法院於 2023 年召開審理庭確認指控內容，並進行保釋相關聽證，程序目前仍在進行中。

本案亦引發一連串後續調查，涉及至少其他兩家使用相似手法之匯兌業者及其共犯。

來源 - 印度

³² FATF - 《法人之實質受益權指引》 - <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html>

案例研究 # 2:洗錢犯罪集團**非法賭博/博弈；自我洗錢；使用法人與法律協議**

2022 年 11 月 10 日，中華臺北金融情報中心向刑事警察局通報一份金融情報報告。經深入分析，發現一個由 22 人組成的線上賭博犯罪集團，其中包括主嫌犯 A，利用數名人頭陸續成立 A、B、C 公司等多家空殼公司。自 2022 年 5 月起，該集團開始以此等空殼公司作為洗錢工具。

該犯罪集團在招募新進人員後，首先安排他們隱匿於高級住宅大樓內進行集中式培訓及管理。待新進人員熟悉集團之網路銀行轉帳流程且能迅速操作後，主嫌犯 A 即要求員工返回各自住處隱匿，等候接收通訊軟體傳送之訊息指示，以進行洗錢任務，並規避警方偵查。為隱匿大量非法博弈所得資金，集團員工透過眾多虛設銀行帳戶進行一連串交易。該集團幹部會要求員工定期透過聊天群組回報作業狀況，以計算各成員應分配之犯罪所得。

經過長期調查與廣泛蒐證後，專案小組於 2023 年 2 月及 6 月分兩波實施拘捕與搜索行動。第一次行動逮捕並移送法辦 13 人；第二次行動則逮捕包括主嫌犯 A 在內之 9 人。專案小組查扣行動電話、筆記型電腦、桌上型電腦、存摺等多項洗錢證物。全案犯罪所得高達 15 億臺幣（約 4,690 萬美元），查扣該犯罪集團名下之不動產價值 4,440 萬臺幣（約 140 萬美元）。此外，搜索過程中專案小組發現被作為洗錢用途的人頭帳戶內尚餘近 3,000 萬臺幣（約 93.8 萬美元），已立即通報檢察官並向法院聲請緊急扣押。

來源 – 中華臺北

以貿易為基礎之洗錢活動

以貿易為基礎之洗錢活動（Trade-based money laundering, TBML）一般定義為透過貿易交易掩飾犯罪所得及移轉資金，以合法化犯罪資金來源的行為（下稱「貿易洗錢」）。實務上，貿易洗錢常與其他洗錢活動及犯罪行為結合。

貿易洗錢通常透過海關、貨物稅與租稅徵收等高度專業化之全球性貿易環境運作。國際貿易體系固有諸多漏洞，易遭犯罪者利用。大量的全球貿易流動提供掩蓋單一非法交易之機會，尤其當交易與外匯交易或多元化之貿易融資安排結合時，此一風險更高。³³

世界海關組織（WCO）識別出以下兩種常見涉及法人濫用之貿易洗錢方式：

- 利用傀儡董事（straw directors）（代名人）及相關法人進行貿易洗錢。
- 法人實體在進行稅務詐欺的同時，透過無記名可轉讓金融工具（bearer negotiable instrument）洗錢，並於貨物出口至海外前謊報數量，以進行稅務詐欺。

傀儡董事與貿易洗錢

犯罪者在兩個司法管轄區成立兩家名稱相似之法人，此等法人名稱通常與知名公司極為近似。其中一個法人作為主要實體，另一個法人則作為過水帳戶（pass-through account）。法人之所有權再轉移至其他擔任傀儡董事的個人名下，但原董事實際上持續執行日常營運與帳戶管理活動。犯罪集團利用疑似犯罪所得購買貨物後出口至境外，並透過低報這些貨物的實際價值，將犯罪所得轉移至海外。

³³ 澳洲交易報告與分析中心（AUSTRAC） - 《澳洲國家洗錢風險評估》：<https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf>

迴轉式增值稅詐欺與貿易洗錢

犯罪集團將來源不明的資金（可能為犯罪所得）轉存至儲值卡（stored value cards），並利用該等儲值卡從零售通路購買高價電子產品，例如行動電話、吸塵器、電腦及遊戲主機等。隨後開立發票，將這些貨物虛假「銷售」予由彼此認識之犯罪集團成員所擁有及控制之法人。雖然實際上無任何貨物交付，但犯罪集團卻向稅務權責機關詐領根本未發生之貨物及服務稅（GST）的退稅款。隨後犯罪集團將這批高價電子產品以較低價格與較少數量報關出口至海外，藉此再度透過貿易洗錢（TBML）取得額外之洗錢與獲利機會。

案例研究

正如以下各成員國所提供之案例所示，犯罪分子透過法人濫用與貿易洗錢進行犯罪活動，而且日益猖獗。

案例研究 #3：以鑽石貿易為基礎之洗錢計畫

貿易洗錢；貴金屬及寶石交易商

2023年初，中國香港海關經與A司法管轄區進行情報交換後，偵破一起跨國貿易洗錢犯罪案件。該集團於2021年1月至12月期間，透過鑽石貿易進行達港幣5億（約6,400萬美元）的洗錢活動。該犯罪集團成立5家公司，向A司法管轄區出口低價的人造鑽石，假冒為高價天然切割鑽石，以達成洗錢目的。為轉移非法資金，該集團於貿易申報文件中高度誇大人造鑽石之價值。透過虛增申報價值，該集團隨後將犯罪所得由A司法管轄區轉入中國香港，作為鑽石交易之「合法貨款」。

該犯罪集團使用上述5家公司之企業銀行帳戶處理犯罪所得，並進一步將資金分散匯入逾100家當地公司，以進行後續交易。2023年12月至2024年2月間，中國香港海關成功瓦解該犯罪集團，逮捕5名涉嫌洗錢之人員，並查扣港幣100萬元（約13萬美元）。目前案件調查仍持續進行中。

來源 - 中國香港

案例研究 #4：以貿易為基礎之洗錢活動

貿易洗錢；公司組織形式濫用；偽造文件；稅務犯罪；資金多層化；結構化交易

權責機關發現4名具有多項違法紀錄之個人，成立並濫用公司組織形式及獨資企業，進行交易活動，疑似涉及貿易洗錢活動（TBML）。此4名嫌疑人透過銀行業務，包括網路銀行及境外匯款服務進行交易。嫌疑人為進行部分對外匯款交易，向銀行提交偽造或無效之文件。

本案係因銀行向馬爾地夫金融情報中心提交可疑交易報告（STR）而啟動調查；銀行提交STR的主因為客戶所進行之交易，與客戶盡職調查（CDD）及認識你的客戶（KYC）資訊明顯不符。目前本案仍由執法機關持續調查中。

來源 - 馬爾地夫

案例研究 #5：貿易洗錢與可疑實質受益權

以貿易為基礎之洗錢活動

申報義務機構對 C 人士及 D 人士兩人所擁有之 A 公司提交多筆可疑交易報告（STR）。A 公司從 B 司法管轄區進口太陽能板並於巴基斯坦當地銷售。該公司於不同銀行開設 5 個帳戶，並於三年間透過這些帳戶匯轉約 20 億盧比（約 700 萬美元）。公司之貿易發票顯示，進口太陽能板價值 20,150 美元，但海關機關評估之貨物實際價值卻高達 91,233 美元。此一明顯差異顯示公司明顯低報貨物價值，主管當局因此對交易真實性產生懷疑。

巴基斯坦金融監理單位（FMU）進一步分析發現，E 人士曾在 A 公司其中一個銀行帳戶內存入 5,000 萬盧比（約 179,573 美元）現金及 1,900 萬盧比（約 68,238 美元）之清算交易款項。後續分析亦揭露，E 人士係 B 公司之銷售員，且其亦曾透過多個帳戶向該公司存入超過 45 億盧比

（約 1,600 萬美元）現金。金融監理單位已先前向執法機關（LEA）提供有關 B 公司的金融情報，涉及 A 公司低報進口太陽能板價格與相關貿易洗錢活動。一個執法機關根據相關機構回饋資訊已針對 B 公司董事登錄第一資訊報告（FIR），並展開調查。

此外，F 人士（經查為 E 人士之兄弟）為 B 公司其中一個帳戶之簽署人。A 公司帳戶活動引發疑慮，可能涉及貝納米交易³⁴（以他人名義進行交易），也引發對公司實際實質受益權的懷疑。之後有不利媒體報導指出，政府稽核部門揭露有公司透過太陽能板進口業務進行大規模虛增發票價值，涉嫌貿易洗錢，藉以濫用太陽能板進口退稅制度。

稅務記錄亦顯示，A 公司於可疑帳戶活動期間僅繳納極少稅款。金融監理單位已將相關金融情報通報執法機關，以進一步調查其中之貿易洗錢情節，並追查經由 A 公司帳戶流動資金之最終受益人。

來源 - 巴基斯坦

1.3 專業協助者

在檢視法人濫用情形時，常見一個共同角色，即提供專業服務的個人、組織或網路，協助犯罪分子對犯罪所得進行洗錢。這類主體被稱為「專業協助者」（professional enablers）³⁵，其行為通常具有故意、罔顧後果、不當、不誠實，及／或未盡其專業與法規上應盡義務之特性。這些「犯罪化專業人士」在法人（及法律協議）之建立或運作時扮演關鍵角色，特別是在協助其犯罪客戶掩飾控制權及實質受益權方面。

專業協助者指提供專業服務，協助犯罪者以洗錢方式處理犯罪所得之專業個人、機構或組織網路。

FATF 於 2018 年發布「專業洗錢活動」（Professional Money Laundering）指引³⁶，辨識出專業協助者之關鍵特徵，包括：

- 洗錢之專業人士（個人）
- 洗錢之專業組織（機構）
- 洗錢之專業協作網路（聯繫人及合作網路）

³⁴ 非正式代名人安排

³⁵ 英國法律協會（The Law Society (United Kingdom)）- 專業協助者 <https://www.lawsociety.org.uk/topics/anti-money-laundering/professional-enablers#:~:text=%E2%80%9CA%20professional%20enabler%20is%20an,their%20professional%20and%20regulatory%20obligations.%E2%80%9D>

³⁶ FATF - 專業洗錢活動（Professional Money Laundering）：<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Money-laundering-fentanyl-synthetic-opioids.html>

此等專業協助者運用多種洗錢工具與技術，包括貿易洗錢、帳戶管理機制、地下匯兌及另類銀行平台等。他們與提供表面合法服務的貪污個人合作，如銀行人員、律師、會計師、不動產仲介等，為其活動披上合法外衣。

皇家聯合軍事研究所 - 《阻斷制裁規避的協助者》 (*Disabling the Enablers of Sanctions Circumvention*) : 政策簡報

2024 年 5 月，皇家聯合軍事研究所 (Royal United Services Institute, RUSI) 與金融安全中心 (Centre for Finance and Security, CFS) 發表政策簡報，³⁷ 指出專業服務業者 (如律師) 常規避制裁的共同行動機制。該簡報提出政策建議，呼籲各國政策制定者共同努力，降低協助規避制裁的風險，從而強化制裁之落實執行。

調查型記者 (包括「組織犯罪與貪污報導計畫」 (Organised Crime and Corruption Reporting Project, OCCRP) 所揭露之調查成果，提供了深入理解專業服務業者行為之寶貴洞見。為提煉有效政策建議，皇家聯合軍事研究所 (RUSI) 轄下的金融與安全中心 (CFS) 與組織犯罪與貪污報導計畫 (OCCRP) 攜手合作，分析逾百份報導，聚焦俄羅斯相關個人與法人實體如何倚賴專業協助者規避制裁之情形，並彙整自 2022 年 2 月俄烏戰爭爆發以來，美國、英國及歐盟對此類「專業協助者」所採取之行動。

主要發現與建議

金融與安全中心 (CFS) 分析調查報告發現，專業協助者為俄羅斯客戶提供「一站式」專業服務，包括法律、會計、投資、不動產、信託及公司設立等服務。由於協助者不侷限於傳統職業角色，《政策簡報》建議以態樣與活動方式對專業協助者分門別類，並加以監管。

《政策簡報》辨識出的專業協助者之五種主要活動類型包括：

- 藉由複雜企業架構與洗錢網路隱匿資產。
- 透過攤薄持股方式規避金融制裁之門檻。
- 透過利用監管寬鬆之司法管轄區進行全球化布局。
- 積極對抗試圖調查或關注其客戶事務之人士，以迴避外界之檢視。
- 最精明的協助者甚至在其客戶尚未遭受制裁前，即已先行採取各種預防及因應措施。

金融安全中心發現上述態樣在調查中反覆出現，顯示現有制度與實務仍存在缺口，讓專業協助者得以協助客戶不正當地保護其資產與利益，並規避制裁。

簡報最終提出十二項建議，旨在堵塞現有制度漏洞，並打擊專業協助者混淆視聽的策略，當中包括：

- 加強對專業協助者網路之執法行動，以提升嚇阻效果。
- 加強跨司法管轄區制裁名單之協調，並促進具相似法律體系之司法管轄區間相關規範與標準之調和一致性。
- 對金融及相關服務提供者，明確施加防制洗錢之義務。
- 建立更具包容性且全面的資訊共享機制。
- 提高實質受益權及控制權資訊的透明度。

³⁷ 皇家聯合軍事研究所 - 《阻斷制裁規避的協助者》：<https://www.rusi.org/explore-our-research/publications/policy-briefs/disabling-enablers-sanctions-circumvention>

世界銀行集團 - 簽名待售：犯罪化專業人士協助洗錢案例研究（2022年）

追回被盜資產倡議（Stolen Asset Recovery Initiative, StAR）所發布的《簽名待售》（*Signatures for Sale*）報告，³⁸探討公司服務提供商（CSP）如何透過提供代名人服務，藉由保護隱私的理由，協助個人隱匿在空殼公司的真實所有權，藉此有效對權責機關隱藏其真實身分。此報告強調公司服務提供商在協助非法活動的角色。此等協助者借助專業知識與技能，積極宣傳並提供代名人服務，常搭配其他增強隱密性的工具（如授權委任書）使用。

此報告係根據全球一項「神秘客」（mystery shopping）調查之超過 3,300 筆回應所撰寫，研究人員在調查中假扮成有意設立空殼公司之客戶進行調查。結果顯示，14% 公司服務提供商未受提示即提供代名人服務，15% 提及授權委任書或律師保密權。此顯示代名人服務普遍存在，尤以金融隱密度高之司法管轄區為甚。

主要發現

- 公司服務提供商之代名人服務，有些屬例行合法用途，有些雖合乎用途但易遭濫用，而其他則主要用以隱匿受益所有人。
- 代名人安排乃隱藏空殼公司控制人身分最常見之方式，尤其常見於公司設立業中問題最嚴重之區塊。
- 目前各界對於代名人安排可能或實際遭到濫用的情形，仍未予以足夠重視，致使利用難以追蹤之空殼公司從事金融犯罪的漏洞依然存在，亟待改善。必須更積極地加強相關執法，特別是在實質受益權登記制度方面。
- 在非法應用端，對於意圖設立空殼公司之客戶，代名人服務常被明確作為賣點，成為避免受益所有人身分被公開登錄之工具。
- 代名人所建立之空殼公司網路，由於其既有跨司法管轄區之特性，對企業透明化構成重大威脅。然而現行單一轄區之法規監理架構，與此跨轄區威脅，二者存在根本性的落差與不足。
- 有效監管公司服務提供商（CSP）及代名人安排，對提升實質受益權透明度至關重要。

協助者

提供此類服務之公司服務提供商通常為律師，提供其簽名與身分，擔任名義董事或股東，以收取費用。亦可能擬定授權委任書，使受益所有人得以隱匿其控制身分。律師保密權更為其提供法律保護。不需揭露身分。部分公司服務提供商更提供附預設銀行帳戶與名義簽署人的「空殼公司」，令客戶得以立即使用金融系統而無需揭露身分。

使用代名人服務已造成防制洗錢之重大漏洞，這使犯罪分子得以有恃無恐地運作，對權責機關隱匿其身分與資產。此一現象已削弱實質受益權登記等透明制度之效用。

報告強調對代名人服務進行更嚴謹地監管與執法，包括：

- 提升透明度：要求代名人揭露其實質所有人及該安排之目的。
- 核准與監理：對專業代名人進行許可、核准與嚴格監理。
- 加強盡職調查：要求公司服務提供商（CSP）對其客戶及該代名人安排目的進行嚴密背景調查。
- 增進國際合作：強化國際合作機制，以因應代名人服務之跨司法管轄區特性。

針對上述漏洞採取有效措施，權責機關將能有效遏止代名人服務遭濫用，並防止「犯罪化專業人士」（criminalised professionals）藉此協助洗錢。

³⁸ 世界銀行集團 - 《簽名待售》（2022年），報告全文請參閱：<https://star.worldbank.org/publications/signatures-sale-how-nominee-services-shell-companies-are-abused-conceal-beneficial>

案例研究

APG 成員國及觀察員組織提供以下案例，說明地區內專業協助者如何濫用法人以進行洗錢及資恐活動。

案例研究 # 6：七人因涉國際網路詐騙被起訴

投資詐騙；使用法人；使用網際網路；使用虛擬資產；使用金融服務

S 司法管轄區向澳洲聯邦警察（AFP）主導之「聯合網路警務協調中心」（Joint Policing Cybercrime Coordination Centre，JPC 3）通報，一起詐騙案與澳洲有連結。澳洲聯邦警察遂與國外執法單位同步偵辦（代號「維克漢行動」〔Operation Wickham〕）。

此複雜詐騙案非法操控合法電子交易平台，某有組織集團以「殺豬盤」形式，透過交友網站、求職平台、通訊工具等社交工程技術，誘取受害者之信任，其後才提及投資機會。當受害者訂閱所謂投資服務後，該集團透過操作資訊，誘導追加投資，同時隱瞞該等資金已被竊取（成為犯罪所得）之事實。全球損失達 1 億美元以上，多數受害者位於 S 司法管轄區。

該犯罪集團利用居住於澳洲之外籍人士設立必要的帳戶等基礎設施，以進行詐騙活動。該集團亦以居住於澳洲之外籍人士登記澳洲公司並開設銀行帳戶，以洗錢方式處理犯罪所得。此等資金透過匯款公司進行洗錢，並經由與澳洲註冊企業相關之銀行帳戶進行多層交易。

其中一名罪犯在匯款公司工作，其與犯罪集團直接合作，為洗錢實體招募「影子董事」與「人頭帳戶持有者」，並設立虛假公司與銀行帳戶，以規避防制洗錢及打擊資恐之法規。

目前在「維克漢行動」中已有 7 人因涉嫌處理超過 1,000 萬澳幣（約 680 萬美元）犯罪所得遭起訴。此外，由澳洲聯邦警察主導之「犯罪資產沒入專責小組」（CACT），亦取得對該集團相關銀行帳戶之扣押處分（restraining orders），總金額超過 2,100 萬澳幣（約 1,400 萬美元）。

來源 - 澳洲

案例研究 # 7：澳洲公司被境外網路犯罪集團利用

詐欺包括商業電子郵件詐騙；法人濫用；使用虛擬資產（加密貨幣或其他虛擬資產）

澳洲金融情報中心（AUSTRAC）指出，一家澳洲註冊公司遭海外網路犯罪集團濫用，透過該公司將電子郵件詐騙所得資金轉移出境。犯罪集團利用境外空殼公司、數位貨幣及專業協助者（包括會計師）進行操作。該公司登記之董事疑為被盜身分之受害人、或人頭。

該帳戶曾收取 2020 年來自一起房地產交易相關電子郵件詐騙之 92,000 澳幣（約 61,424 美元）犯罪所得，該款項在被匯出境前已被凍結，並返還受害者。但該帳戶在 2020 年四個月內成功收受逾 290,000 澳幣（約 193,611 美元）來自多位海外受害者之款項，隨後進行多層化並轉出境外。

據判斷，該公司極可能利用數位貨幣（digital currencies）³⁹ 進行洗錢操作，亦即將資金存入數位貨幣交易商（DCE）⁴⁰ 並立即轉換為數位貨幣，再自交易商之託管帳戶提領出數位貨幣。透過數位貨幣交易商（DCE），該實體另外還連結兩個境外公司帳戶，這些帳戶極可能透過空殼公司⁴¹ 以洗錢方式處理犯罪所得。

來源：《澳洲洗錢國家風險評估報告》（內容略有調整）

³⁹ 虛擬資產

⁴⁰ 虛擬資產服務業者

⁴¹ 澳洲交易報告與分析中心（AUSTRAC） - 《澳洲國家洗錢風險評估》：<https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf>

案例研究 #8：透過空殼公司洗錢**法人濫用**

自 2019 年 4 月至 2021 年 4 月間，某犯罪集團 11 名成員成立約 340 間空殼公司，並建立約 900 個對應銀行帳戶。這些帳戶被「售予」犯罪分子，以管理及隱匿從經營非法賭博網站所獲取的非法資金。韓國檢察機關於 2012 年 10 月起訴該集團 11 名成員，並獲法院下達命令予以解散所有空殼公司。

來源 - 韓國

案例研究 #9：以虛假文件取得政府補助後提取現金**詐欺；自我洗錢；金融機構；現金；使用支票；新冠肺炎（COVID-19）；使用法人；可疑交易通報**

2021 年 12 月至 2023 年 2 月間，四名嫌疑人於五家澳門本地銀行替 140 餘家公司開設公司帳戶，並存入澳門政府針對中小企業及自由職業者（freelancers）疫情補助所簽發之支票。支票存入後不久，即全數以現金形式被提領，總金額約 200,000 美元。銀行於客戶盡職調查（CDD）程序中對其用途提出疑問，四人均表示資金用於業務。然而，金融機構仍併案申報可疑交易報告。澳門金融情報中心進一步調查後發現，多數公司共用通訊地址，隨即將案件移送至檢察院（Public Prosecutions Office）進一步偵辦。

來源 - 中國澳門

案例研究 #10：投資詐欺**投資詐欺；使用法人；跨國犯罪**

警方對一起投資詐騙案之調查引發多處突擊搜索行動，包括電話客服中心、公司與住宅處所。

該犯罪集團以馬來西亞為據點，運作僅數年，涉嫌累積高達近 2 億令吉（約 4,260 萬美元）之犯罪所得。雖然據點位於馬來西亞，集團成員卻來自多個國家，且利用馬來西亞當地人士作為協助者。

該集團透過社群媒體刊登廣告，提供虛假投資組合，誘騙受害人上當。此詐騙集團利用專業協助者（尤其是公司秘書）協助設立公司，使受害人誤以為投資於合法投資計畫，或購買真實公司的股份。

行動中有 4 名外籍人士遭以《刑事法典》中前置犯罪起訴、判刑並處以罰款，洗錢犯罪相關之資產沒入程序目前仍持續進行中。

來源 - 馬來西亞

案例研究 #11：逾 3,000 家公司網路之商業電子郵件詐騙**詐欺；境外前置犯罪；第三方洗錢；公司服務提供商；使用法人與法律協議；可疑交易通報**

2020 年期間，新加坡警察部隊商業事務局（Commercial Affairs Department, CAD）發現以新加坡公司為名的洗錢資金網路急遽增加，該資金係來自針對海外受害人的商業電子郵件詐騙針對海外受害者。調查顯示，逾 3,000 間疑似以洗錢為目的而成立之公司具有共同特徵。

體認到瓦解此犯罪集團的重要性，商業罪案調查科因此與銀行業等關鍵利害關係人合作，分享調查所得資訊及交換對該案的觀察與見解。並促請新加坡金融情報中心「可疑交易報告辦公室」（Suspicious Transaction Reporting Office, STRO）向銀行業發布針對此類新興犯罪模式之通報與建議。此類情資與意見交流，已被證實對加速調查極具助益；透過 STRO 接收並進一步傳遞可供執法行動之金融情報，有效協助商業事務局之調查作業。

調查發現，境外犯罪集團透過境外代理人，聯繫新加坡公司服務提供商設立公司，並由第三方個人擔任名義董事。此等董事名下持有 57 至 1,002 間公司職務，但實際允許境外代理人操作公司及公司銀行帳戶，被認定未善盡董事職責。

迄今，已有七位涉案人士經《公司法》判刑或罰款；另五人仍在審理中。

上述公司常見之共同特徵如下：

- 通常設有一位本地董事與一位外國董事，後者同時為該公司唯一股東。
- 多間公司共用相同登記地址或本地董事，且該董事通常同時擔任網路中多家公司董事。
- 多數公司成立於相同時期。
- 儘管交易金額龐大且交易頻繁，這些新成立的公司在網路上卻少有業務資訊，且各家公司所登記之營業性質彼此差異甚大。

來源 - 新加坡

案例研究 # 12：外匯詐欺

詐欺（包括電話、簡訊、電子郵件或社群媒體）；第三方洗錢；使用法人與法律協議

A 人士及其犯罪集團聲稱其為來自 X 司法管轄區之外匯交易商；成立 42 家空殼公司，分別經營非法外匯及期貨交易業務。該人等在多地設立分公司並雇用人員拓展業務，採取經紀人制度，透過經紀商或臉書、WeChat、QQ、Telegram 等網路平台推廣業務。同時提出「6% 紅利方案」保證獲利，藉此吸引大眾在該集團架設之詐騙網站上進行交易。自 2012 年至 2022 年 5 月期間，該集團詐騙金額累計高達 249.8 億臺幣（約 8.32 億美元）。

為追回犯罪所得，法務部調查局（MJIB）扣押了 A 人士名下共計 93 筆不動產，市值約 1 億 4,900 萬臺幣（約 460 萬美元）。透過追蹤境外資金流向，MJIB 發現 B 人士及其他人提供帳戶，供 A 人士轉移犯罪所得，涉及金額達 1 億 1,569 萬臺幣（約 373 萬美元）。經法院核准後，法務部調查局進一步扣押 B 人士名下價值約 130 萬臺幣（約 406,250 美元）之不動產。2023 年 3 月，法務部調查局將 A 人士及其犯罪集團移送檢察署偵辦，目前該案正在法院審理中。

來源 - 中華臺北

案例研究 # 13：澳洲史上最龐大、由澳洲聯邦警察主導之洗錢調查

有組織犯罪；貨幣兌換；金錢或價值移轉服務；國際合作；第三方洗錢；獨立洗錢

「Avarus-Nightwolf 行動」為一項由澳洲聯邦警察（AFP）主導、為期 14 個月的洗錢調查，由澳洲交易報告與分析中心（AUSTRAC）、澳洲邊境執法局（ABF）、澳洲刑事情報委員會（ACIC）、澳洲證券及投資委員會（ASIC）、澳洲稅務局（ATO）、以及美國國土安全部協助進行。

長江（Long River）洗錢集團七名成員及另一個涉嫌具全球影響力的澳洲有組織犯罪集團，因秘密經營澳洲境內一個交易規模高達數十億澳幣之重要匯款管道——「長江貨幣兌換」（Changjiang Currency Exchange）遭到調查與起訴。澳洲聯邦警察指出，為打造遵守法律的合法匯款公司形象，「長江貨幣兌換」甚至主動提供資源，以教育客戶認識澳洲防制洗錢法規（AML）。

2020 至 2023 年間，「長江貨幣兌換」經手進出澳洲境內的資金超過 100 億澳幣（約 68 億美元）。儘管這些資金大多來自合法交易客戶，澳洲聯邦警察指出該公司同時亦祕密處理非法獲得的資金。2020 至 2023 年間該公司涉嫌洗錢金額逾 2.28 億澳幣。

澳洲聯邦警察指控，該集團部分洗錢資金來自犯罪所得，包括網路詐騙及非法物品走私；並教導犯罪客戶如何製造虛假商業文件，例如偽造發票及銀行對帳單，以便在資金移轉受到權責機關注意時，犯案客戶與「長江貨幣兌換」得以虛偽證明其資金來源合法。

澳洲聯邦警察已起訴涉案的四名外籍人士及三名澳洲公民，並查扣價值超過 5,000 萬澳幣之房地產與車輛。2023 年 10 月，澳洲交易與分析中心（AUSTRAC）亦暫停六家匯款服務業者的註冊資格。

來源 - 澳洲

案例研究 # 14：股份有限公司之股票操縱與資產侵佔

詐欺；內線交易與市場操縱

A 人士及其共犯在一家股份有限公司（joint stock company）內進行股票操縱及侵佔資產。

A 人士創辦一家股份有限公司，為提升公司資本，其改制為在交易所上市之公開發行公司。相關審查中，多位前任公職領導人因涉嫌違反「在職濫用職權罪」遭起訴；另有官員因觸犯「在證券活動中發布不實訊息、或隱匿事實罪」被控。

被告已向國家支付 1,950 億越南盾（約 800 萬美元）以彌補犯罪行為所造成之損失；偵查機關亦扣押 9 筆不動產，全案估計損失總額達 1 兆 8,300 億越南盾（約合 7,550 萬美元）。

來源 - 越南

專業協助者面臨之主要挑戰：隱私權與律師保密特權

近期針對打擊不法資金流動的透明度改革，擴大了權責機關之間資訊蒐集與交換的範圍。此等新政策措施的範例包括：建立實質受益權資訊中央登記制度；全球銀行帳戶資訊自動交換機制；以及針對中介機構之強制揭露規範⁴²，要求揭露規避資訊交換、或隱匿實質受益人⁴³之相關安排。本次資訊蒐集、處理與各國間交換範圍之擴大，引發隱私權、資訊／資料保護權以及律師保密特權等方面之質疑。

其中最具影響力之發展為，歐洲法院（European Court of Justice）⁴⁴ 於 2022 年 11 月所作成之裁決認定，為防制洗錢而公開揭露實質受益權資訊之作法無效。主因與保障個人隱私權相關。此外，在隱私權的相關議題中，法律專業人士亦援引其當事人的律師保密特權（legal professional privilege）。例如，歐洲法院曾認可該特權，以撤銷依據歐盟理事會指令（The EU Council Directive）2011/16（即 DAC 6）所要求關於跨境稅務安排之強制揭露資訊。⁴⁵ 此外，歐洲法院之總檢察官（Advocate General）於 2024 年所提出之法律意見，⁴⁶ 也以律師保密特權為依據，拒絕提交特定設立公司之資訊，再次將其納入隱私權保障範疇。此等裁決引起民間團體之強烈批評。⁴⁷

FATF 及全球稅務透明與資訊交換論壇（Global Forum）已對此類發展提出警示，並主張應限制律師保密特權之範圍。例如，FATF 於 2019 年出版的《法律專業人員風險基礎方法之指引》（*Guidance for a Risk-based Approach Legal Professionals*）⁴⁸ 報告中指出：

「犯罪分子可能選擇法律專業人員（而非其他非法律專業）執行第 22 項建議中列舉之服務，目的是藉由專業特權之保密保護機制，隱匿其活動與身分，不受權責機關監管」（第 23 頁）。

同樣地，FATF 於 2013 年之報告《法律專業人員於洗錢及資恐面臨之弱點》（*Money Laundering and Terrorist*

⁴² 租稅正義網路（Tax Justice Network）- 《強制揭露規則：對付專業協助者的潛在利器》」部落格文章（*The unexploited silver bullet to tackle enablers: mandatory disclosure rules blog*）：<https://taxjustice.net/2023/07/14/the-unexploited-silver-bullet-to-tackle-enablers-mandatory-disclosure-rules/>

⁴³ 歐盟「行政合作指令」（DAC 2 與 DAC 6）（Directive Administrative Cooperation (DAC 2 and 6)）修正案，要求銀行帳戶資訊之自動交換，並強制中介機構揭露相關安排。

⁴⁴ 歐洲法院 - 新聞稿第88/22號 - 關於合併案件 C-37/20（盧森堡商業登記處，Luxembourg Business Registers）及 C-601/20（Sovim）之判決：<https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-11/cp20188en.pdf>

⁴⁵ InfoCuria 法律判例庫 - 大法庭對案件 C 694/20 之判決：

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=268430&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=27401>

⁴⁶ InfoCuria 法律判例庫 - 歐洲法院總檢察官 Kokott 於 2024 年 5 月 30 日就案件 C 432/23 提出之法律意見：

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=286580&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=7340756>

⁴⁷ 租稅正義網路（Tax Justice Network）- 《歐洲法院再度以人權為由對抗透明度及租稅正義》（*Another EU court case is weaponising human rights against transparency and tax justice*）部落格文章：<https://taxjustice.net/2024/06/28/another-eu-court-case-is-weaponising-human-rights-against-transparency-and-tax-justice/>

⁴⁸ FATF - 《法律專業人員風險基礎方法之指引》（*Guidance for a Risk-based Approach Legal Professionals*）：<https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Legal-Professionals.pdf.coredownload.inline.pdf>

*Financing Vulnerabilities of Legal Professionals)*⁴⁹ 中亦有類似論述：

「主張律師保密特權或專業保密，可能妨礙或延宕刑事偵查……在許多情況下，此類特權主張或專業保密必須由法院裁定，進而大幅延長偵查期限。鑑於時間對追查犯罪所得至為關鍵，此可能影響調查人員決定是否調查涉案法律專業人士，或改從其他來源尋求其當事人活動之證據。」（第 31-32 頁）

此外，此報告附錄列舉 45 個案例，顯示法律專業人士藉由設立公司、信託、使用不記名股票或擔任受託人來隱匿所有權。其中第 59 案涉及某法律專業人士設立複雜境外架構，並透過客戶帳戶轉移資金，主張保密特權以阻止調查人員發現其行動。

雖然各界對此議題仍存不同意見，但有人主張律師保密特權僅應適用於法律專業人士以法律職能所提供之通訊與資訊。舉例而言，《透明度與應要求資訊交換同行評審手冊》（*Handbook for Peer Reviews on Transparency and Exchange of Information on Request*）⁵⁰ 指出：

「當事人與律師、法律顧問或其他具資格之法律代表間之通訊，僅在該人士以其法律代表身分行事時適用特權。例如，若律師以登記代名人、受託人（trustee）、信託設立人（settlor）、公司董事或透過授權書代表公司處理業務，其因進行該等職能所產生之通訊或資訊，不得援用律師—當事人通訊保密特權予以保護」（第 88 段）。⁵¹

全球論壇（Global Forum）指出，所有權相關資訊原則上不屬於保密範疇。此外，作為資訊交換法律基礎之 2017 年《所得與資本模範稅收協定》（*Model Tax Convention on Income and on Capital*）⁵² 指出：

「提供予律師、法律顧問或其他具資格法律代表之文件或資料，若係為避免依法應揭露而提交，則不得予以保護。此外，個人如公司董事或實質受益人之身分資訊，通常不屬於保密通訊範疇。」（第 19.3 段）。

1.4 捍衛機制

權責機關可運用多種機制，以抑制專業協助者及法人濫用的現象。透過公開可查之登記制度，及時取得基本與實質受益權資訊，對權責機關掌握情資至關重要。此外，鑑於專業協助者通常為信託及公司服務業者（TCSP），各司法管轄區有效規範 TCSP，並搭配其他機制同步運作亦不可或缺。其他應施行的防制機制包括：採行相稱且具阻嚇作用之制裁、保障吹哨者權益，以及宣導公私部門夥伴合作關係。最後，因法人的受益所有人常具跨國特性，權責機關間之國際合作亦是重中之重。

本節彙整成員過及觀察員組織之作法、最佳國際操作實務以及執行上述機制之經驗教訓。

皇家聯合軍事研究所 - 《防制洗錢與專業服務業者》會議報告（2024年）

2024 年 4 月至 6 月間，英國皇家聯合軍事研究所（RUSI）轄下的金融與安全中心（CFS）舉辦了三場工作坊，探討防制洗錢之法規、監理及執法活動對於防範、偵測及懲處 律師與會計師等專業人士從事所謂「協助型行為」（enabling behaviour）方面所扮演的角色，並檢視英國與歐盟在宣導良好實務誘因（good practices incentives）方面的作用。

⁴⁹ FATF - 《法律專業人員於洗錢及資恐面臨之弱點》（*Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*）：<https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf.coredownload.pdf>

⁵⁰ 經濟合作暨發展組織稅務透明度與資訊交換全球論壇 - 《透明度與應要求資訊交換同行評審手冊》（*Handbook for Peer Reviews on Transparency and Exchange of Information on Request*）：<https://web-archive.oecd.org/tax/transparency/documents/handbook-for-peer-reviews-on-transparency-and-exchange-of-information-on-request.pdf>

⁵¹ 一般而言，在普通法系國家中，「律師保密特權」適用於律師與當事人之間為提供法律諮詢或訴訟所進行的保密通訊。然而，若該通訊係用於非法目的，該特權可能被剝奪。

⁵² 經濟合作暨發展組織 - 《所得與資本模範稅收協定》（*Model Tax Convention on Income and on Capital*）2017 年：<https://www.oecd-ilibrary.org/docserver/g2g972ee-en.pdf?Expires=1722597850&id=id&accname=guest&checksum=FA165AD67AA8EF4BE6F09EA6EB60E69F>

RUSI 與歐盟駐大不列顛暨北愛爾蘭聯合王國代表團 (*Delegation of the European Union to the United Kingdom of Great Britain and Northern Ireland*) 共同舉辦這些工作坊，邀集來自英國與歐盟的業界、監理機關、執法機關與學術界人士共同參與討論。2024 年 7 月，金融與安全中心發表《會議報告》(Conference Report)，⁵³ 綜合整理工作坊的主要討論成果。

每場工作坊皆聚焦於專業服務業者監理過程中不同面向之特定挑戰，包括監理成效、執法強度及誘因機制報告詳細列明每場工作坊的發現。三場工作坊均指出要求專業服務業者履行防制洗錢 (AML) 義務時，往往面臨以下共通挑戰：

- 部分司法管轄區內部與不同轄區之間缺乏一致之督導架構，阻礙跨境協調合作，並可能留下可供犯罪分子利用之漏洞。
- 必須強化整個體系內的資訊共享，尤其是針對可疑交易報告、與可疑活動報告；專業人員與監理機構都認為彼此反饋將極有助益。
- 監理機關須掌握多元監理工具，包括各種誘導專業服務業者履行防制洗錢義務之方式。此類工具亦應依專業服務業者之類型與司法管轄區特性而量身定製。

與會者一致認為，律師與會計師在防範與偵查洗錢行為方面扮演關鍵角色；惟目前面臨之挑戰不僅阻礙防制洗錢控制措施之有效實施，亦妨礙對違規專業人士、或專業服務業者進行有效執法。

聯合國毒品犯罪辦公室 (UNODC) 關於防範相關 專業協助者之預防措施

聯合國毒品犯罪辦公室 (UNODC) 正積極宣導與專業協助者相關之預防性措施。於第十四屆落實審議小組 (Implementation Review Group) 續會 (2023 年 9 月 4 日至 8 日) 中，針對聯合國大會特別會議 (UNGASS) 關於反貪污問題後續之第 6 項議程中，特別討論防制洗錢措施及中介機構 (intermediaries) 於犯罪所得轉移過程中所扮演的角色。聯合國毒品犯罪辦公室 (UNODC) 於會中提供以下最新進展：

「對犯罪所得進行洗錢並掩飾其來源乃一項結構複雜且持續演進之課題，嚴重威脅金融體系之誠信與法治精神。該行為使犯罪者得以隱匿非法所得之來源與所有權，並享受犯罪收益。中介或守門人經常在洗錢體系中扮演部分角色，無論是否明知其用途。其提供之服務包括設立空殼公司、開設銀行帳戶、轉移資產或辦理交易等方式，皆可能協助洗錢者掩飾資金之來源與去向。」

UNODC 依據成員國提出之挑戰及《聯合國反貪污公約》(UNCAC) 審查機制，聚焦以下重點議題：

- 修補法規與監理缺口，確保中介機構受到適當機關有效監督，並強化監督機關落實防制洗錢標準的能力與機制；
- 提升中介機構對其在防制與偵查洗錢行為中所承擔角色與責任的認知；
- 強化中介機構、執法單位與監理機關之合作與資訊分享；
- 確保提出可疑交易報告之中介機構免受報復或脅迫。

依照不同部門與專業特性設計適當之對應措施，是一大挑戰。當中介者易被納入洗錢活動時，預防為主之策略具有成效；但對於專業協助者，仍須更強制性之處置機制。

紐西蘭宣導專業協助者管制之進展

紐西蘭指出其專業服務提供者在提供代名人服務方面，存在易遭濫用的弱點。例如，一家紐西蘭信託及公司服務業者 (TCSP) 為外國客戶擔任逾 1,000 多家公司的名義持有人；另有犯罪者利用非正式代名人（如親屬或人頭）掩飾其實質受益權。

⁵³ 皇家聯合軍事研究所 (RUSI) - 《防制洗錢與專業服務業者》會議報告 (2024年) : Conference Report: <https://www.rusi.org/explore-our-research/publications/conference-reports/anti-money-laundering-and-professional-service-providers-conference-report>

因應此一風險，紐西蘭已採取多項措施，包括將信託及公司服務業者納入其防制洗錢與打擊資恐體系、建立「紐西蘭外國信託」（New Zealand Foreign Trusts）登記冊、設立專責「誠信與執法小組」（Integrity and Enforcement Team）維護公司登記制度之完整性，並修訂公司法（Companies Act）要求公司設置常駐董事。紐西蘭亦展開公司與合夥事業實質受益權揭露規範之諮詢作業。

實質受益權登記制度

一套有效之防制洗錢、打擊資恐及打擊資武擴制度應包括：

- 採取措施防止法人與法律協議被用於犯罪目的。
- 提高法人與法律協議之透明度。
- 確保可以隨時取得足夠、正確且最新的基本與實質受益權資訊。
- 實質受益權資訊應提供予權責機關查閱⁵⁴。
- 違反相關規範者，應依法受到有效、相稱及具阻嚇作用之制裁。

有效落實上述措施，將降低犯罪分子使用法人洗錢之誘因。⁵⁵

許多司法管轄區已建立、正在建立或考慮設立實質受益權中央登錄系統。實質受益權登記方式可以有多種樣式，各司法管轄區應依據制度環境及受記錄之法人種類彈性設計。

由成員國所提供之實質受益權資訊的資料顯示，此領域仍需大幅提升。整體而言，亞太地區法人之實質受益權資訊極為缺乏。即使某些成員國確實設有法人資訊之中央公開登記處，通常亦僅包含基本資料，並未涵蓋 FATF 標準所界定之實質受益權資訊。在全球範圍內，現有登記系統內的資訊品質通常未經查核，亦未及時更新；此外，法律架構甚至可能不要求法人本身揭露直接股東（immediate shareholders）以外的實質受益權資訊。

正面來說，不少司法管轄區已開始宣導改革，可作為其他轄區依其風險與背景適度借鏡之典範。

加拿大實質受益權登錄制度

加拿大於 2024 年 1 月 22 日啟動聯邦註冊公司（依據《加拿大商業公司法》〔Canada Business Corporations Act, CBCA〕設立）之公開實質受益權登錄系統。在加拿大，實質受益人亦稱作「具有重大控制權之個人」（Individuals with Significant Control, ISC）。此制度採用非政府組織「開放所有權組織」（Open Ownership）所制定之國際實質受益權資料標準（Beneficial Ownership Data Standard）。⁵⁶ 以建構資料結構，並提升與全球其他登錄系統之互通性，加速資料共享效率。依據規定，所有受《加拿大商業公司法》監管之公司，須向加拿大公司登記處（Corporations Canada）申報實質受益權資訊。公開揭露之資料項目包括：公開揭露之資料項目包括⁵⁷：

- 完整法人名稱。
- 成為或終止為「具有重大控制權之個人（ISC）」的日期（如適用）。
- 對具有重大控制權之個人（ISC）所持控制權之描述。
- 居住處所（若未提供送達處所（address for services），此住居地址將予以公開）。
- 送達處所（若有提供）。

⁵⁴ FATF - 《法人之實質受益權指引》 - <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html>

⁵⁵ FATF 《評估 FATF 建議技術遵循程度與防制洗錢及打擊資恐及資武擴體系有效性之方法論》（Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems） - <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-Methodology-2022.html>

⁵⁶ 開放所有權組織（Open Ownership）—《實質受益人資料標準》（Beneficial Ownership Data Standard）：

<https://standard.openownership.org/en/0.4.0/>

⁵⁷ 加拿大政府—具有重大控制權之個人（ISC）資料申報說明：https://ised-isde.canada.ca/site/corporations-canada/en/individuals-significant-control-file-your-information?utm_campaign=ised-isde-cc-isc-23-24&utm_medium=link&utm_source=notice

此外，魁北克省（Province of Quebec）於 2023 年 3 月 31 日啟動涵蓋在魁北克設立之公司及其他註冊營業之法人實質受益權公開登錄系統。卑詩省（Province of British Columbia）則於 2023 年 5 月 11 日通過法案，計畫於 2025 年建立公開實質受益權登錄處。

菲律賓公司登記改革措施

菲律賓近期啟動公司登記制度改革，強化並簡化執法機關取得實質受益權資訊之程序，該資訊主要來自菲律賓證券交易委員會（Securities and Exchange Commission, SEC）。具體作法如下：

- 證券交易委員會於公司設立程序中導入 eFAST 系統之自動註冊，並強制揭露實質受益權資訊；同時發布 2023 年第 19 號證交會備忘通函（Memorandum Circular, MC No. 19），依《修訂公司法》（Revised Corporation Code）第 21 條與第 177 條規定，訂定未依規定申報者之公司列為「違規（delinquent）」情形之處置準則。
- 截至 2024 年 4 月，逾 50 萬家有效註冊公司中，已有 68% 完成實質受益權揭露義務，剩餘 32% 公司已被列為「違規」狀態。根據證券交易委員會的一項範疇界定研究顯示，違規企業中其中 97% 屬於微型、小型與中型企業。
- 同時，證券交易委員會已暫停被監控、且八年未營運之 117,885 家公司註冊資格。值得注意的是，所有被暫停之公司於該期間均未從事或申報任何商業活動。
- 證券交易委員會亦與其轄下 19 個合作機關密切協調，截至目前已處理 734 件企業資訊請求，其中涵蓋實質受益權揭露資訊，涉及 4,989 家公司與 1,099 位個人。

澳洲擬建實質受益權登錄制度

澳洲政府於 2022 年 11 月開放諮詢，蒐集第一階段公開實質受益權登錄制度之設計要點。目的在於強化實質受益權透明化，遏制利用複雜的所有權架構逃避法令與隱匿稅負之行為；並同步支持針對稅務與金融犯罪更有力之監理與執法措施，協助外資申請程序，以及促進制裁措施之有效執行。

第一階段諮詢聚焦以下方案：針對受《公司法》（Corporations Act）規範之特定非上市實體，要求其維持準確、及時更新及公開揭露之實質受益權登錄資訊。未來諮詢階段將延伸意見蒐集，涵蓋透過其他法人工具（如信託）所持實質受益權之揭露機制，以及將全部資訊彙整於單一公開登錄平台之可行性。⁵⁸

經驗教訓：建置實質受益權登錄制度之最佳實務

根據歐盟防制洗錢全球設施（EU Global Facility）發表之《建立國家層級揭露制度發展藍圖》（Building a Country Roadmap for Beneficial Ownership Disclosure Regime）⁵⁹，報告，說明建構實質受益權登錄制度（Beneficial Owner Register, BOR）時的多項經驗與挑戰。主要最佳實務涵蓋：法律框架設計，政府部門間合作協調，科技整合提升資料串連效率，專業訓練等。

此報告亦指出在建立實質受益權登錄制度（BOR）時，須克服之主要挑戰包括：低估實施制度所需之時間與資源、法律規範不明確或模糊不清，以及因系統設計不夠健全以致產出資料品質低劣。

⁵⁸ 澳洲政府財政部網站（The Treasury）—《跨國稅務誠信：公開實質受益權登錄》（Public Beneficial Ownership Register）：<https://treasury.gov.au/consultation/c2022-322265>

⁵⁹ 歐盟防制洗錢全球設施 - 《建立國家層級揭露制度發展藍圖》：<https://www.global-amlcft.eu/wp-content/uploads/2024/05/BO-Country-Roadmap-vfinale.pdf>

聯合國毒品犯罪辦公室 - 東協成員國與東帝汶之實質受益權透明化落實情形之研究

2024 年，聯合國毒品犯罪辦公室（UNODC）發布一份報告⁶⁰，內容為東南亞國家協會（ASEAN）成員國與東帝汶（Timor-Leste）落實實質受益權所有權透明化之比較研究。此報告探討東協各國與東帝汶對實質受益權的法律定義，以及其實質受益權揭露架構的主要要素。研究與比較的主要項目包括實質受益權資料之蒐集與維護情形。UNODC 指出，東協成員國中已有六個國家建立登記系統，以蒐集與維護實質受益權資料，但各國間在涵蓋範圍上存在差異。其他研究與比較的要素包括未遵循法令時之制裁措施，以及東協與東帝汶各國實質受益權揭露制度所涵蓋法人之範圍。

信託及公司服務業者（TCSP）在實質受益權登記中的正面作用

當公司及其他法人透過信託及公司服務業者（TCSP）辦理相關業務，可能對實質受益權登記程序有所助益。相較於客戶（例如法人本身），信託及公司服務業者提供通常更能掌握並理解法律規範中關於實質受益權的要求。

若信託及公司服務業者屬該國防制洗錢與打擊資恐法規之申報義務機構（例如指定之非金融事業或人員，DNFBP），即須依照規定執行充分的客戶盡職調查（CDD）程序，包括辨識客戶之實質受益人。由於信託及公司服務業者在進行客戶盡職調查時已蒐集該等資訊，因此可更有效地向實質受益權登記處申報準確資料。此外，相較於公司登記處，信託及公司服務業者通常與客戶有更密切且深入的聯繫，因此更容易及時掌握客戶所有權或控制權的變動，協助實質受益權資訊的持續更新。值得注意的是，一個將信託及公司服務業者納入防制洗錢及打擊資恐系統內的成員國指出，2023 年，信託及公司服務業者總計向該國金融情報中心通報了 35 起可疑交易報告（STR）。

在信託及公司服務業者參與實質受益權登記的情形中，觀察到以下優點：

- 加強對實質受益權規範的理解與法令遵循能力。例如，比利時有 70% 的公司透過會計師登錄資訊，其他則直接透過其法律代表辦理。
- 宣導與訓練活動。從實質受益權登錄的角度，將訓練重點集中於參與實質受益權登記之信託及公司服務業者，比起直接針對所有法人或法律協議效率更高。
- 溝通協調。相較於直接處理所有法人或法律協議，實質受益權登錄僅需與相對較少的信託及公司服務業者溝通，可有效提供整合科技解決方案，例如安全線上入口網站與自動化資料傳輸系統（如 API），以便信託及公司服務業者與實質受益權登錄間無縫資訊共享。
- 資料查核。受客戶盡職調查規範之信託及公司服務業者亦需驗證實質受益權資訊之正確性。基於此查核結果，信託及公司服務業者可獲准（或依法）向實質受益權登記處通報所發現資訊不一致情形，以提升登錄資訊之準確性，如此即可啟動調查、要求提供額外資訊、修正錯誤資訊或採取執法措施。
- 人力資源。相較於政府權責機關編制之人力資源，信託及公司服務業者通常配置更多專職人員負責法令遵循與盡職調查事務，具備顯著的人力資源優勢。

然而，儘管信託及公司服務業者參與實質受益權登記有其優點，並不保證其等完全遵循。因此，實質受益權登錄處（BOR）應建立監督機制，如定期稽核、檢查，以及針對違規行為的處罰措施，以監督並確保信託及公司服務業者確實履行其把關之責任。

⁶⁰ 聯合國毒品犯罪辦公室 - 《東協會員國與東帝汶之實質受益權透明化落實情形之研究》（*Implementation of Beneficial Ownership Transparency in ASEAN Member States and Timor- Leste*）：

https://www.unodc.org/roseap/uploads/documents/Publications/2024/Implementation_of_Beneficial_Ownership_Transparency_in_ASEAN_Member_States_and_Timor-Leste.pdf

新加坡對公司服務提供商之監理措施

新加坡發現犯罪分子經常透過法人結構進行非法交易、控制或轉移不法資產。在新加坡，多數人透過公司服務業者（CSP）設立法人。公司服務業者在客戶設立法人前，必須執行客戶盡職調查（CDD），確認並核實客戶及其擬設法人之實質受益人身分。

新加坡會計與企業監管局（Accounting and Corporate Regulatory Authority, ACRA）負責監督與規範公司服務業者，並對未履行客戶盡職調查義務、或協助不當利用法人的公司服務業者採取監理行動。對公司服務業者可施以之制裁包括財務罰鍰、暫停、或撤銷註冊資格。會計與企業監管局（ACRA）並於網站公布被暫停或撤銷註冊的公司服務業者名單。

新加坡目前正在更新法人相關之洗錢及資恐風險評估（上次於 2019 年完成），且於 2024 年初，其公私合作平台「防制洗錢／打擊資恐產業合作夥伴關係」（AML/CFT Industry Partnership）發布《金融機構因應來自公司服務業者帶來之洗錢、資恐、資武擴風險最佳實務》報告（*Best Practices for Financial Institutions to Manage Money Laundering, Terrorism Financing and Proliferation Financing (ML/TF/PF) Risks Associated with Receiving Referrals from Corporate Service Providers*）⁶¹。

此外，於 2024 年 3 月，新加坡進行公開諮詢，以加強對公司服務業者的監理力度。提出加重公司服務業者與其高層在違反防制洗錢及打擊資恐義務時的罰則，並禁止非公司服務業者安排人員擔任名義董事，除非公司服務業者已評估該員適任。上述提案已納入《公司服務業者法案》（CSP Bill）以及《公司及有限公司合夥（雜項修訂）法案》（Companies and Limited Liability Partnerships (Miscellaneous Amendments) Bill），並於 2024 年 7 月 2 日獲得國會通過。

新加坡防制洗錢與打擊資恐產官合作 - 法人 - 濫用態樣與最佳實務(2018)

2017 年 4 月，新加坡設立「防制洗錢／打擊資恐產業合作夥伴關係」（AML/CFT Industry Partnership），由金融業、監理機關、執法機關及其他政府部門組成，協同識別、評估並抵減新加坡面臨之主要與新興洗錢及資恐風險。

於 2018 年 5 月，該產業合作夥伴關係發布《法人—濫用態樣與最佳實務》（*Legal Person - Misuse Typologies and Best Practices*）⁶² 報告。此報告揭示金融機構可觀察之可疑客戶行為或交易模式，並建議金融機構應採取之辨識與防範措施。

由於許多專業中介機構擔任法人設立與持續秘書服務的關鍵角色，因此其等構成與法人互動的第一道防線。報告重點包括：

- 律師事務所中的法人濫用案例：為潛在洗錢及資恐目的提供設立法人或安排的法律協助。在法人相關情境中，律師事務所經常代表法人行事，或受託協助設立法人或法律協議。

A 客戶向 A 律師提出洽詢，聲稱欲針對 A 律師執業之司法管轄區內某企業提起訴訟，並要求提供法律意見與協助。雙方會面時並未交換任何文件，但 A 客戶口頭說明爭議事實背景。會議後，A 律師依新客戶開戶程序（client on-boarding），識別 A 客戶的受益所有人並完成盡職調查篩查，未發現異常。

接著，A 客戶向 A 律師提出簽訂聘任契約並支付預付款項，該款項匯入 A 律師的客戶信託帳戶。不久後，A 客戶通知 A 律師表示該訴訟已和解，A 律師尚未執行任何實質法律服務，僅需扣除少額初步作業費用；A 客戶要求將剩餘款項返還，但指定匯往另一個與最初匯款來源不同的帳戶。

⁶¹ 新加坡金融管理局（Monetary Authority of Singapore）- 《金融機構因應來自公司服務提供商帶來之洗錢、資恐、資武擴風險最佳實務》：<https://www.mas.gov.sg/regulation/external-publications/best-practices-for-banks-to-manage-ml-and-tf-risks-associated-with-receiving-referrals-from-csp>

⁶² 新加坡銀行公會與新加坡金融管理局之防制洗錢與打擊資恐產業夥伴關係 - *Legal Persons* (法人) - 《法人—濫用類型與最佳實務》：<https://abs.org.sg/docs/library/legal-persons-misuse-typologies-and-best-practice.pdf>

A 律師不知情的是，A 客戶之訴訟純屬捏造。儘管 A 律師已依防制洗錢/認識你的客戶（AML/KYC）規定對 A 客戶完成篩查，但未發現任何負面資訊。若 A 律師將餘款退還給 A 客戶，將間接協助進行假訴訟型洗錢。然而，若 A 律師延遲退款，亦可能引起 A 客戶的猜疑。

- 信託及公司服務業者中的法人濫用態樣：雙重國籍

專業顧問（如顧問公司與稽核公司）在其業務過程中，也觀察到與法人有關之洗錢及資恐風險態樣。

A 客戶為 A 司法管轄區的外國護照持有人，委託信託及公司服務業者設立一家境外公司。若干時間後，A 客戶提出解散該境外公司，並同時要求以 B 司法管轄區頒發之另一外國護照名義，在東南亞設立一家名稱近似的公司。

- 公司服務業者面臨的洗錢及資恐風險管理

公司服務業者與法人互動之主要活動包括：設立公司（第一天）、公司架構變更（非定期、隨時進行）以及年報申報（週期性進行）。由此可見，客戶開戶（on-boarding）階段是公司服務業者面臨最重大洗錢及資恐風險的時點。

以下為成員國所分享關於公司服務業者，抵減相關洗錢及資恐風險的最佳實務範例：

- 辨識與核實控制人、實質受益人、股東、董事及/或授權簽署人
 - 對於設有名義董事之公司，可採取附加管控措施，例如由公司服務業者協助編製財務報表、或委由註冊會計師事務所審計。
 - 若公司服務業者在客戶盡職調查階段（CDD）未能查驗原始文件，得接受經合格人士（例如公證人、律師或註冊會計師）驗證為與原件相符之影本。
- 篩查控制人、實質受益人、股東、董事及/或授權簽署人
 - 公司服務業者於客戶開戶階段（on-boarding），可運用信賴度高之商業化篩查資料庫，以識別風險指標（如不利新聞、重要政治性職務人士等）。
- 了解客戶設立公司之目的、擬經營業務性質、控制人與/或最終實質受益人。
 - 公司服務提供者可透過面談，明瞭擬經營業務內容及設立公司之目的。
 - 可向客戶索取補充資料，以評估其風險層級，例如其主要客戶與供應商之地理所在地、實質受益人職業，以及資本之資金來源（SOF）。若涉及重大股權分配，亦可要求提供銀行對帳單或客戶的匯款憑證。
- 可疑活動指標／紅旗指標／門檻規定之程序
 - 公司服務提供者應制訂正式程序，透過可疑交易報告，向相關政府機關通報可疑活動。

英國 - 專業人士團體防制洗錢監理辦公室

英國專業人士團體防制洗錢監理辦公室（Office for Professional Body Anti Money Laundering Supervision, OPBAS）成立於 2018 年，為加強英國防制洗錢督導體系的一環，回應該國首次國家洗錢與資恐風險評估（NRA）所揭示之薄弱環節。OPBAS 目前監理 25 個法律與會計等專業團體監理機關（PBS），其任務為提升 PBSs 之防制洗錢督導效能，並強化與執法機關暨其他公部門間之資訊共享⁶³。

OPBAS 隸屬英國金融行為監理總署（Financial Conduct Authority, FCA），其監理方向與 FCA 及 FATF 規範一致，兼顧法令遵循（compliance）與實效。

除定期執行對專業團體監理機關（PBS）的實地風險導向監理評估外，OPBAS 亦宣導專案性主題督導工作，範圍涵蓋信託及公司服務業者（TCSP）⁶⁴與風險識別及驗證等相關作業⁶⁵。OPBAS 的督導涵蓋多個產業與細分職業群，包括訟務律師（barristers）、記帳人員（bookkeepers）、不動產交易代書（conveyancers）及稅務從業人員（taxation）。透過此種方式，OPBAS 能全面掌握各產業內潛在風險的相對程度，從而精準配置資源，最有效地打擊危害。

為防堵「專業協助者」（professional enablers）不論是知情或無意協助犯罪，OPBAS 與執法機關、中央政府及國際機構緊密合作，主動分享情報。為落實第二任務目標，OPBAS 亦已成立「情報共享專家工作小組」宣導 PBSs 與執法機關之資訊交流分享。例如，創建「情報分享專家工作小組」（Intelligence Sharing Expert Working Groups）^{66, 67}。

此外，英國於第 2 綜合經濟犯罪防治計畫（Economic Crime Plan 2）中⁶⁸，納入遏制專業協助者之行動，並為此發展出一套「專業投資者策略」（Professional Enablers Strategy）。⁶⁹ 該策略的行動包括強化公私部門間的互信與情報資訊共享程度，此為 OPBAS 之核心關注重點。

近期英國兩項重要的經濟犯罪相關法規：《2022 年經濟犯罪（透明化與執法）法》（Economic Crime (Transparency and Enforcement) Act 2022）及《2023 年經濟犯罪與公司透明化法》（Economic Crime and Corporate Transparency Act 2023），已建立具有突破性的立法，以提升企業透明度、改善實質受益權登錄制度，並防範法人濫用的情形。目前，OPBAS 正與英國公司登記處（Companies House）合作宣導並落實這些改革措施，以有效協助打擊上述濫用情形。

英國所採取的跨體系方法，彰顯公私合作之重要價值。英國已意識到各部門各自為政之運作方式無法有效防制洗錢風險，體系內各單位均應承擔降低洗錢風險之責任。此外，民間團體及學術界也被視為重要合作夥伴，可提供多元觀點、新的挑戰及專業技能。OPBAS 為一面向外界的組織，深刻體認風險具有跨境特性，因此積極在國際間分享英國經驗與良好實務，並向其他國家學習。

比例適當且具阻嚇作用之制裁

為確保權責機關能及時取得法人實質受益權資訊，各司法管轄區應對未依法維持或揭露實質受益權資訊之法人，進行比例適當且具阻嚇作用之制裁，此應持續適用於所有違反實質受益權資訊維護、與揭露義務之法人。

⁶³ 英國金融行為監理總署（Financial Conduct Authority, FCA）－專業人士團體防制洗錢監理辦公室（Office for Professional Body Anti-Money Laundering Supervision, OPBAS）：<https://www.fca.org.uk/about/how-we-operate/who-work-with/opbas>

⁶⁴ 英國金融行為監理總署，專業人士團體防制洗錢監理辦公室（OPBAS）- 多專業監管機構檢視報告，信託及公司服務業者風險之多專業專案報告）（Multi-PBS review, Multi-PBS project on TCSP risk）：<https://www.fca.org.uk/publication/multi-firm-reviews/opbas-multi-pbs-project-tcsp-risk.pdf>

⁶⁵ <https://www.fca.org.uk/publication/corporate/opbas-supervisory-update-risk-identification-verification.pdf>

⁶⁶ 英國金融行為監理總署，專業人士團體防制洗錢監理辦公室（OPBAS）- 會計業情報分享專家工作小組職權範圍（Accountancy Sector Intelligence Sharing Expert Working Group Terms of Reference）：<https://www.fca.org.uk/publication/opbas/accountancy-sector-isewg-terms-of-reference.pdf>

⁶⁷ 英國金融行為監理總署，專業人士團體防制洗錢監理辦公室（OPBAS）- 法律界情報分享專家工作小組職權範圍（Legal Sector Intelligence Sharing Expert Working Group Terms of Reference:）：<https://www.fca.org.uk/publication/opbas/legal-sector-intelligence-sharing-expert-working-group-terms-of-reference.pdf>

⁶⁸ 英國政府－經濟犯罪計畫二期（2023 至 2026 年）：2023-2026:

https://assets.publishing.service.gov.uk/media/642561b02fa8480013ec0f97/6.8300_HO_Economic_Crime_Plan_2_v6_Web.pdf

⁶⁹ 國家犯罪調查局（National Crime Agency, NCA）、國家經濟犯罪中心（National Economic Crime Centre, NECC）與專業人士團體防制洗錢監理辦公室（OPBAS）－《跨體系專業協助者策略》（2024 至 2026 年）（Cross-System Professional Enablers Strategy 2024-2026）：<https://www.nationalcrimeagency.gov.uk/who-we-are/publications/724-cross-system-professional-enablers-strategy/file>

巴基斯坦制裁改進作為 - 對未遵循實質受益權揭露規範之法人與法律協議

透過對未依規定揭露實質受益權資訊之法人、及法律協議實施具相稱性、與阻嚇作用之制裁，巴基斯坦近期在強化防制洗錢、打擊資恐及資武擴體系之有效性上，取得顯著進展。

巴基斯坦近日完成所有類型法人與法律協議之全面週期檢查，期間共對 54,593 個實體強制實行總計 23.8558 億盧比（約 8,560 萬美元）的制裁。這些實體多數為公司，亦涵蓋有限責任合夥、伊斯蘭法制（waqfs，慈善或公益基金會）、信託及合作社。巴基斯坦亦採取其他執法手段，例如暫停營業、撤銷登記等。此外，該國亦建置 WTC 資訊平台，以蒐集全國所有瓦克夫、信託與合作社之相關資訊，包括實質受益權資訊，供權責機關查閱。

中國澳門對法人之監督與制裁措施

2023 年，中國澳門發布《澳門洗錢、資恐與資助武器擴散風險評估報告（2022）》（*Risk Assessment Report on Money Laundering/Terrorist Financing/Financing of Proliferation of Weapons of Mass Destruction, 2022*）。中國澳門權責機關於 2024 年初發布此報告並進行推廣活動，涵蓋信託及公司服務業者（TCSP）領域（包括公證人及律師）。

中國澳門金融情報辦公室（GIF）持續密切監控法人或信託及公司服務業者服務可能遭受濫用之情形。2023 年，GIF 金融資訊分析小組執行特別策略性審查，並識別出若干可疑空殼公司。該小組彙整特定個案之調查摘要，並於 2023 年 8 月轉交該領域權責機關——法律事務局（DSAJ）。目前中國澳門金融情報辦公室正利用可疑交易報告資訊，進一步執行另一主題性策略分析，確認可能與空殼公司相關之信託及公司服務業者服務。該分析成果完成後將與相關權責機關分享。

透過中國澳門的公私部門協力合作，中國澳門金融情報辦公室亦定期向私部門分享策略分析結果，以強化其預防與風險抵減措施，防止法人濫用。在 2020 年及 2021 年新冠肺炎（COVID-19）疫情期間，中國澳門金融情報辦公室曾向金融機構分享可能為空殼公司之名單，以利其等執行風險抵減控管措施。中國澳門金融情報辦公室目前正準備與金融機構及監理機關共享之新名單。

根據第 2/2006 號法律《預防及遏止洗錢犯罪》（*Prevention and suppression of the crime of money laundering*）及第 3/2006 號法律（預防及遏止恐怖主義犯罪）（*Prevention and suppression of the crimes of terrorism*），中國澳門權責機關可以針對洗錢及資恐行為採取多種具比例性、且具嚇阻作用的制裁，包括罰款或司法解散。罰款金額介於澳門幣 1 萬元（約 1,250 美元）至澳門幣 2,000 萬元（約 250 萬美元）之間。若法人設立之目的即在從事洗錢或資恐、或其成員或管理階層經常性進行此類犯罪行為，顯示該法人係被用於此目的，法院得命令司法解散該法人。

此外，法人亦可能同時被課以多種附加刑罰，包括：

- 禁止從事特定活動，期間為 1 年至 10 年不等。
- 剝奪政府部門或公共機關所提供之補助或補貼。
- 停業，期間為 1 個月至 1 年。
- 永久停業。
- 法院禁制令（Judicial injunction）。
- 將判決公開（Publicity of the sentence）。

除洗錢及資恐行為之刑事責任外，未能遵守洗錢及資恐防制義務之實體，即使係出於過失，亦可能構成行政違規，行政違規可處澳門幣 10 萬元（約 12,500 美元）至澳門幣 500 萬元（約 625,000 美元）之罰鍰。此外，若犯罪行為所獲經濟利益超過該法規定最高上限之一半，則該上限應調高至該等利益之二倍。

跨轄區防禦

在防制法人濫用之洗錢行為時，若涉及跨境活動，執法機關往往面臨重大挑戰。犯罪集團為規避監管，常採用「跨司法管轄區分割」（multi jurisdictional splitting）策略，將公司設立、資產所有權、中介人及銀行帳戶等分散於不同司法管轄區。此碎片化手法使任何單一司法管轄區之權責機關難以掌握法人被濫用之全貌，必須透過國際資訊交換才能有效偵查、調查及起訴罪犯。此外，某些司法管轄區因受限於執法能量或政策取向，無法有效防制洗錢犯罪；此可導致包括無法確實評估犯罪規模及發現最新趨勢等的嚴重後果。

有效之預防措施與調查行動，均須仰賴國際合作。透過正式與非正式合作管道，能及時取得外國司法區實質受益權資訊，加速調查程序，並提升資金追查、凍結及沒入洗錢所得之能力，防止犯罪所得進一步流失。

FATF 建議的要素之一，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，以協助追訴犯罪及追繳相關資產。根據第 24 項建議，各司法管轄區應在法人基本及實質受益權資訊方面，開展迅速、建設性而有效且廣泛地國際合作。

聯合國毒品犯罪辦公室 – 《聯合國反貪污公約》（UNCAC）第四章：東協各締約國及東帝汶之國際合作執行情形

此報告概述東協各締約國及東帝汶在執行《聯合國反貪污公約》（UNCAC）第四章所面臨的挑戰及良好實務作法。該章節涵蓋國際合作機制，包括引渡、刑事司法互助、執法合作、聯合調查及特殊調查技術。未承認法人刑事責任及／或要求雙重犯罪（dual criminality）原則的國家，可能在提出涉及法人之刑事司法互助請求時面臨挑戰。

整體而言，由於各國法律框架、既有能力、國際合作經驗及既存國際安排各有不同，區域內執行情形出現明顯差異。區域內所獲得建議最多的是刑事司法互助，儘管部分國家可以針對法人所涉《聯合國反貪污公約》（UNCAC）犯罪提供刑事司法互助，但其他國家則並不明確。

案例研究

各成員國提供以下案例，作為如何運用防制洗錢系統之實例，包括如何運用國際合作回應法人濫用的情況（另一件涉及法律協議）。

案例研究 # 15：透過空殼公司洗錢

詐欺；跨國組織犯罪集團；境外前置犯罪

A 司法管轄區調查發現，兩名罪犯與其他犯罪集團成員共謀，以虛假資料及文件誤導投資人，聲稱該基金前景良好，導致多名受害人投資該基金。犯罪集團因此騙取超過 163 萬美元，並匯入該兩名罪犯於 A 司法管轄區之銀行帳戶內。權責機關最終逮捕上述罪犯，後續調查發現其等在中國香港利用多家空殼公司（金融及證券業）設立多個銀行帳戶，以洗錢方式處理部分犯罪所得。

經執行刑事司法互助請求後，大部分資金已返還 A 司法管轄區。2023 年，香港警方取得國內法院沒入命令，沒入仍留存於空殼公司銀行帳戶內之犯罪所得，總額達 250 萬港幣（約 347,850 美元）。

來源 – 中國香港

案例研究 # 16：成功將資金返還至 L 轄區

貪污；國際合作；自行洗錢；第三方洗錢；購置不動產；資產返還

2015 年，新加坡貪污調查局（Corrupt Practices Investigation Bureau, CPIB）接獲情資，指出來自 X 司法管轄區之飛機製造商 U 公司聘用 L 司法管轄區一名「顧問」，向該轄區國家航空公司官員行賄，以取得飛機及其引擎售後服務合約。調查發現，該名顧問為 A 人士，涉嫌收受賄款的官員則為 B 人士、C 人士及 D 人士，他們是該航空公司的高階主管。

貪污調查局亦接獲消息指出，上述人士皆在新加坡設有銀行帳戶，賄款可能經由新加坡金融系統支付及洗錢。資金追蹤調查顯示，A 人士透過其本人或其實質控制公司的帳戶，多層化匯款給 B 人士、C 人士與 D 人士。

X 司法管轄區、L 司法管轄區以及貪污調查局隨後展開聯合調查，以追查相關貪污及後續洗錢罪行。

帳戶與資產扣押

貪污調查局依據《刑事訴訟法》（Criminal Procedure Code）於 2017 年 1 月 16 日扣押 32 個相關銀行帳戶，並扣押登記在 B 人士名下一處私人不動產。該不動產的購置價格約為 260 萬新加坡元（約 190 萬美元）。

其他資訊

2017 年 1 月 17 日，X 司法管轄區權責機關與 U 公司達成延期起訴協議（Deferred Prosecution Agreement, DPA）。該協議暫緩的起訴罪名涵蓋 12 項，包括共謀貪污罪、虛假會計罪，以及未防止行賄罪。協議內容指出，上述貪污行為已持續約 30 年，涉及多個司法管轄區，包括 L 司法管轄區。

2019 年底，L 司法管轄區權責機關取得 D 人士配合，同意將其新加坡帳戶內剩餘資金交由權責機關處理。貪污調查局協調新加坡總檢察署（Attorney-General's Chambers, AGC）及 L 司法管轄區，最終於 2020 年 9 月 3 日成功自 D 人士位於新加坡之帳戶，自願將約 140 萬美元資金返還 L 司法管轄區。

2020 年 5 月 8 日，A 人士與 B 人士因貪污及洗錢罪於 L 司法管轄區被定罪。2021 年 4 月，新加坡接獲 L 司法管轄區權責機關針對上述私人不動產的外國沒入命令。目前新加坡權責機關正積極向高等法院申請沒入命令，以便將該不動產變現並返還款項至 L 司法管轄區。

來源 - 新加坡

案例研究 # 17：透過信託隱匿位於新加坡之資產

稅務犯罪；信託及公司服務業者；利用法人與法律協議；國際合作

2015 年，新加坡金融情報中心之可疑交易報告辦公室（STRO）主動向 X 司法管轄區之金融情報中心分享金融情報，指出 A 人士為設立於 Y 司法轄區兩個信託之受益人。此二信託在新加坡擁有兩個銀行帳戶，帳戶資金總額約為 7 億美元。此二信託之受託人係一家於境外設立之公司，即法人受託人（corporate trustee）。

調查期間，A 人士在 X 司法管轄區因涉嫌稅務犯罪與洗錢罪而接受調查，經查發現 A 人士於 2013 年至 2016 年間未向 X 司法管轄區申報其在新加坡之兩個銀行帳戶，以及透過位於 Y 司法轄區信託所獲得之相關收入。

新加坡權責機關為協助此調查，根據海外權責機關之請求，緊急處理並向 X 司法管轄區提供大量關於新加坡銀行帳戶的紀錄。此外，新加坡警察部隊商業事務局（CAD）與 X 司法管轄區執法機關密切合作。

2023 年 10 月，A 人士因一項詐欺及虛偽陳述罪名成立。A 人士與 X 司法管轄區達成和解，雙方同意 A 人士向 X 司法管轄區政府支付約 8.03 億美元的和解金。在兩地執法機關密切協調下，和解金成功支付。

來源 - 新加坡

1.5 共通之處

紅旗指標

對司法管轄區權責機關而言，有效防制洗錢、打擊資恐及資武擴的關鍵，在於能否即時取得可以採取行動之優質資訊。所謂優質資訊，係指詳盡、正確且即時的資訊。透過各權責機關於國內及國際間建立有效合作機制，以確保有效取得資訊；同時透過發布紅旗指標（red flag indicators），並對申報義務機構加強教育訓練，以提升所獲資訊之品質。

紅旗指標是用以顯示或暗示異常或可疑活動可能性的指標，有助申報義務機構瞭解、識別並向轄區「金融情報中心」（FIU）申報可疑金融活動，進而偵防犯罪。金融情報中心可使用所獲資料產製可供權責機關採取行動之可操作金融情資。為此，多數成員已訂定相關紅旗指標。

澳洲洗錢與資恐防制監理機構暨金融情報中心—澳洲交易報告與分析中心（AUSTRAC）最近重新修訂所有紅旗指標相關文件⁷⁰，同時其公私合作平台 Fintel Alliance 持續發布金融犯罪指引。

新加坡央銀暨綜合性金融監理機構—新加坡金融管理局（MAS）最近發布一份指導文件：《偵測及抵減法人濫用風險之有效實務》（Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons）⁷¹此文件明訂新加坡金融管理局對金融機構於防制洗錢及打擊資恐框架與控制面之監理期待，聚焦防制法人濫用之風險；同時列出多項案例與最佳實務，可供其他金融機構依風險導向及比例原則，自行制定因應方案。金融管理局建議金融機構應研讀該指引、並依其業務及客戶之洗錢及資恐風險特徵，適度採納上述指引之重點，包括：

- 強化金融機構識別能力，包括在客戶開戶（on-boarding）及後續監控作業的改進措施。
- 結合資料分析工具提升金融機構之檢測效率。
- 運用適切、有效且及時之風險抵減措施。

此外，亞太防制洗錢組織（APG）之觀察員近期亦完成與紅旗指標相關的重要工作。

世界銀行集團已完成一項關於法人與法律遭濫用之調查，並識別多項與其等所有權及控制權相關之紅旗指標。此等指標對於從事監理活動者極具助益，因為有助於辨識可能更易遭受洗錢活動影響的法律結構，從而針對該等類型進行監理，以確保其遵循法規並降低風險（如檢查或制定指引）。從執法角度而言，瞭解最常用於洗錢活動的法人類型，則有助於制定有效的調查策略從而分配資源。指標包括：

所有權及控制權

- 異常複雜的所有權/控制權結構：複雜的所有權結構，看似未具任何合法商業目的，主要設計用於隱匿真實所有權。
- 透過授權書進行控制：利用過於廣泛或缺乏明確目的的授權書安排，可能使難以辨識身分之個人取得控制權。
- 在所有權／控制權結構中使用信託或基金會：在所有權結構中使用信託或基金會，尤其設立於透明度較低之司法管轄區，可能導致實質受益權難以被察覺。
- 使用名義董事／名義股東／人頭：利用非實質受益人之個人擔任董事或股東，通常意圖隱藏實際控制者身分。
- 使用法人為公司董事：以法人作為董事，可能進一步模糊最終實質受益人之身分。
- 使用無記名股票（bearer shares）：持有人僅以股票憑證持有即被視為所有人，導致所有權難以追蹤。

與設立及營運有關之紅旗指標：

- 使用國際商業公司（IBCs）／豁免公司：利用國際商業公司或豁免公司以規避登記或揭露義務，可能隱藏非法活動及實質受益權。
- 使用虛構實體：利用未依法設立或登記且缺乏法律人格之實體，以便利洗錢或前置犯罪。

⁷⁰ 澳洲交易報告與分析中心（AUSTRAC） - 《可疑活動指標》（Indicators of suspicious activity）：

<https://www.austrac.gov.au/business/industry-specific-guidance/all>

⁷¹ 新加坡金融監理局 - 《偵測及抵減法人濫用風險之有效實務》（Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons）：[https://www.mas.gov.sg/regulation/guidance/effective-practices-to-detect-and-mitigate-the-risk\(風險\)-from-misuse-of-legal-persons](https://www.mas.gov.sg/regulation/guidance/effective-practices-to-detect-and-mitigate-the-risk(風險)-from-misuse-of-legal-persons)

- 使用私募投資基金／避險基金：透過私募投資基金或避險基金引導非法資金，以規避防制洗錢管控、進行洗錢、逃避制裁或投資犯罪所得。
- 使用大型專業機構：利用大型專業機構（如法律事務所、會計師事務所、信託及公司服務業者、銀行）設立或管理法人、開立帳戶、移轉資金或提供其他服務，可能藉此濫用專業特權或保密規定。
- 使用偽造身分證明文件設立／登記：於法人設立或開戶過程中提供虛假身分證明文件，以規避客戶盡職調查（CDD）及防制洗錢措施。
- 使用具欺騙性之法人名稱：刻意為法人取具誤導性之名稱，以混淆業務夥伴、法規遵循人員及其他人員，掩蓋法人真實性質及實質受益人之身分。

跨境活動相關紅旗指標：

- 拆分多重司法管轄區：將公司設立、資產所有權、專業仲介及銀行帳戶分散於不同司法管轄區，以規避監管。
- 與保密性司法管轄區相關聯：所有權或控制權與公司及金融透明度規則較低之司法管轄區相關，通常涉及不透明的境外結構。
- 與犯罪所得來源司法管轄區相關聯：與已知產生犯罪所得之司法管轄區存在關聯，顯示可能涉及非法活動。

其他考量因素：

- 涉及特定產業：某些產業如不動產、顧問服務、進出口及境外活動，可能較易遭受洗錢分子濫用。

貿易洗錢紅旗指標

FATF 已系統性完成紅旗指標之相關作業，包括貿易洗錢之紅旗指標。常見之貿易洗錢指標包括：

- 提單（bill of lading）與發票上所載商品描述顯著不符。
- 提單（或發票）上商品描述與實際裝運貨物顯著不符。
- 發票上所申報商品價值與該商品之公平市場價值顯著不符。
- 貨物運輸規模與出口商或進口商之正常業務活動規模明顯不符。
- 所裝運商品類型屬於洗錢活動之高風險商品。
- 所裝運商品類型與出口商或進口商之正常業務活動明顯不符。
- 該貨物之運輸缺乏經濟合理性。
- 貨品來自、或前往洗錢風險高之司法管轄區。
- 貨品運送經過一個或數個司法管轄區但缺乏經濟合理性。
- 支付方式與交易之風險特徵明顯不符。
- 交易涉及收受現金、或由其他與該交易無明顯關聯之第三方實體付款。
- 交易涉及多次修改或頻繁展延之信用狀。
- 交易涉及使用掛名公司（或空殼公司）⁷²。

2021 年，FATF 發布最新的貿易洗錢指引：《貿易洗錢：風險指標》（*Trade-Based Money Laundering : Indicators*）⁷³，該指引在上述基礎上更詳細列出紅旗指標。

⁷² FATF - 《貿易洗錢》（*Trade-Based Money Laundering*）：

<https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade%20Based%20Money%20Laundering.pdf.coredownload.pdf>

⁷³ FATF - 《貿易洗錢:風險指標》：

<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Trade-based-money-laundering-indicators.html>

1.6 結語

2024 年中，防制洗錢金融行動工作組織（FATF）、國際刑警組織（INTERPOL）與聯合國毒品犯罪辦公室（UNODC）的領導人共同呼籲 FATF 成員緊急加強打擊跨國組織犯罪所產生之巨額非法收益。⁷⁴ 跨國組織犯罪的主要方法之一即為法人濫用。

FATF 建議提供司法管轄區有效對抗法人濫用於洗錢、資恐及資武擴之工具。本章所列資訊旨在描繪法人濫用於洗錢及資恐的各種態樣，包括利用專業協助者及個人權利（如保護隱私權與律師保密特權）。本分析支持全球司法管轄區落實第 1 項建議之洗錢、資恐及資武擴風險要求；第 24 項建議所載法人透明化要求（以及法律協議適用之第 25 項建議）；以及第 40 項建議之國際合作要求的迫切需求。亞太防制洗錢組織（APG）代表團的意見亦闡述有效防制洗錢、打擊資恐及打擊資武擴體系之若干要素：例如實質受益權登錄；與信託及公司服務業者（TCSP）產業之合作；以及司法管轄區之國際合作，以共同應對法人濫用於洗錢、資恐及資武擴的風險。

⁷⁴ FATF - FATF, INTERPOL 與 UNODC 主管呼籲對洗錢與資恐採取緊急行動：<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/FATF-INTERPOL-UNODC-Call-to-action.html>

2 - 洗錢及資恐之手法

APG 成員提供之案例研究，依據司法管轄區來源以字母順序排列。每篇案例標題下均附有相關既存之前置犯罪、支付方式或其他情境相關術語，並於本報告第 8 節索引中予以引用。

2.1 澳洲

案例研究 # 18：成功阻止逾十億美元之欺詐性 GST 退稅

稅務犯罪；稅務或 GST 退稅詐欺；使用網際網路（社群媒體）

「防禦行動」（Operation Protego）是一項由澳洲稅務局（ATO）主導的調查行動，目的在於調查透過社群媒體大規模宣導之商品與服務稅（GST）退稅詐欺。澳洲稅務局於 2022 年 5 月 6 日宣布啟動「防禦行動」，以調查及阻止此大規模詐欺行為。

該詐欺行為首次於 2022 年初被發現，犯罪者分子透過虛構企業與澳洲企業號碼（ABN）申請，提交偽造的企業活動報表（BAS），意圖詐領 GST 退稅。詐欺推廣者透過社群媒體及其他管道招募參與者。澳洲稅務局將 Protego 行動轉介至由澳洲稅務局主導之「重大金融犯罪專案小組」（Serious Financial Crime Taskforce, SFCT），該小組為跨機關專責機構，負責處理最嚴重之金融犯罪案件。

截至目前，澳洲稅務局已對逾 56,000 名涉嫌犯罪者採取法令遵循行動，開出約 3 億澳幣（約 2.02 億美元）罰鍰，並成功阻止約 27 億澳幣（約 18.2 億美元）之欺詐性 GST 退稅流入企圖詐欺之個人手中。澳洲稅務局持續與澳洲聯邦警察（AFP）主導的「犯罪資產沒入專案小組」合作，以確保透過 GST 詐欺非法取得的資金，以及利用此類犯罪所得購置之財產均遭沒入。

成功起訴案例包括：

- A 人士於 2022 年 2 月 7 日重新啟用一個珠寶及銀器製造企業之澳洲企業號碼。2022 年 2 月 21 日至 2023 年 7 月 26 日期間，A 人士提交 63 份虛假的企業活動報表（BAS），詐領其無權獲得之 73,650 澳元（約 49,693 美元）。此外，A 人士亦企圖再詐領 192,983 澳元（約 130,201 美元）之 GST 退稅。A 人士最終被控四項以欺騙手段獲取利益之罪名，遭法院判處 1 年 8 個月有期徒刑。
- B 人士於 2021 年 10 月 22 日至 11 月 23 日期間提出虛假企業活動報表，詐領 834,437 澳幣（約 562,976 美元）之 GST 退稅，該企業並不存在。B 人士利用此款購置一間不動產與一部豪華轎車。經四項罪名認罪，包括「以欺騙手段獲取財務利益」、「企圖以欺騙手段獲取財務利益」和「處理犯罪所得」B 人士經法院判處有期徒刑 7 年 6 個月，5 年不得假釋。法院並命 B 人士賠償聯邦政府 834,437 澳幣（約 562,976 美元）。2024 年初，B 人士提出上訴，惟審理日期未定。
- C 人士曾於 2009 年 3 月 28 日至 2015 年 2 月 13 日期間註冊澳洲企業號碼（ABN），並於 2022 年 2 月 11 日重新註冊該企業號碼，意圖為不存在之企業提出企業活動報表（BAS），以申請從未進行之採購以申請 GST 退稅。因虛報資訊，C 人士不當獲得 109,278 澳幣（約 73,721 美元）。經認罪五項「以欺騙手段獲取財務利益」，法院判處 C 人士有期徒刑 2 年，服刑 12 個月後可獲釋，並須簽署為期 18 個月之良好行為保證令（good behavior bond）。同時命其賠償聯邦政府 109,278 澳幣（約 73,721 美元）。
- D 人士於 2022 年 1 月至 3 月間提出虛假企業活動報表，詐領其無權獲得之 282,914 澳幣（約 190,771 美元）之 GST 退稅。D 人士承認 11 項「以欺騙手段獲取財務利益」罪名，法院判處有期徒刑 3 年，服刑 10 個月後可獲釋，並須簽署為期 4 年的之良好行為保證令（其中包含 2 年監督式緩刑，須接受強制性戒毒／戒酒及戒賭課程）。法院同時要求 D 人士賠償聯邦政府 89,767 澳幣（約 60,531 美元）。
- 2022 年 2 月 17 日至 4 月 28 日間，E 人士使用虛假的企業活動報表，詐領其無權獲得之 246,463 澳幣（約 166,183 美元）之 GST 退稅。E 人士承認三項罪名，包括：「以欺騙手段獲取財務利益」、「企圖以欺騙手段獲取財務利益」及「合作實施該等欺騙行為之企圖」。法院判處 E 人士有期徒刑 3 年 4 個月，非假釋期為 1 年 9 個月。法院亦命其向澳洲聯邦政府賠償 180,095 澳幣（約 121,436 美元）。註：E 人士擬提出刑期上訴。

澳洲稅務局（ATO）同時已陸續寄發通知予超過 20,000 人，若不自願歸還詐領款項，將面臨嚴重後果。澳洲稅務局亦已強化控管機制，以防範此類詐欺並處置參與者。

來源 - 澳洲

案例研究 #19：打擊跨國犯罪集團對澳洲兒童的性影像勒索犯罪**性剝削（含兒童性剝削）；使用網際網路**

2022 年 6 月，澳洲權責機關展開「獵人行動」（Operation Huntsman），鎖定境外犯罪集團以經濟利益為目的，針對澳洲兒童的性影像進行勒索犯罪。作為行動一環，澳洲交易報告與分析中心（AUSTRAC）、澳洲聯邦警察（AFP）及其主導之「澳洲防制兒童剝削中心」（Australian Centre to Counter Child Exploitation，ACCCE）合作，打擊鎖定透過澳洲境內受害者之人頭帳戶，進而將非法款項轉移至國際犯罪組織之犯罪網路。

「獵人行動」的目標包括冒充青少年的跨國犯罪集團，透過網路強迫澳洲兒童提供具有性暗示之影像、錄影及金錢。當取得受害者資料後，犯罪集團便威脅恐嚇受害兒童匯款、轉帳禮物卡或遊戲點數，否則便曝光資料。如受害者無力支付，則被指使成為洗錢人頭，開立銀行帳戶協助犯罪組織洗錢。

截至目前，「獵人行動」已成功阻斷超過 1,000 名個人，涉及超過 1,500 個與跨國組織犯罪集團性勒索澳洲兒童相關的澳洲銀行、金融服務及數位貨幣帳戶。

澳洲交易報告與分析中心（AUSTRAC）正與金融服務提供商合作，以取得更多與跨國犯罪集團相關的澳洲銀行與金融服務帳戶資料，進一步對數百名協助非法資金流出澳洲的個人採取措施。

澳洲交易報告與分析中心、澳洲防制兒童剝削中心、與澳洲聯邦警察的情報單位持續鎖定澳洲境內外的犯罪分子，遏阻其透過針對及剝削澳洲兒童所獲資金移轉至海外。此外，澳洲交易報告與分析中心與澳洲聯邦亦持續與國內外執法機關合作，有數個相關調查仍持續進行中。

來源 - 澳洲

2.2 庫克群島

案例研究 #20：社會發展部詐欺案**偽造文書；以虛偽陳述獲取利益；洗錢**

2017 年 2 月，庫克群島金融情報中心向調查機關發布情報報告，通報一起疑似福利金詐欺案。該金融情報報告係依據金融機構提交之可疑交易報告（STR）所啟動之調查，涉及退休金支付至身故人士帳戶。

儘管該名退休金受領人已於 2011 年 1 月過世，並於 2011 年 4 月指定遺產管理人／執行人，紐西蘭社會發展部（Ministry of Social Development）仍持續支付退休金至該已故受領人帳戶，直至 2017 年 1 月停止支付為止；紐西蘭社會發展部共支付 116,002.32 紐西蘭元（約 71,808 美元）至該已故退休金受領人之帳戶。

庫克群島與紐西蘭當局於 2017 至 2018 年間展開調查。由於司法管轄權問題使案件複雜化，需取得法律協助。2021 年起，相關單位進一步展開可能涉及偽造法律文書之調查。

最終於 2023 年，兩名嫌犯在庫克群島高等法院認罪。嫌犯一為執法人員，亦為已故退休金受領人之姪子；嫌犯二則為嫌犯一之伴侶。兩名嫌犯均承認收受並提領退休金。

- 嫌犯一遭控以「偽造文書」及「以虛偽陳述獲取利益」之前置犯罪。法院判處嫌犯一有期徒刑 2 年 3 個月，並命其與嫌犯二共同支付 118,000 紐西蘭元（約 73,035 美元）予紐西蘭社會發展部。
- 嫌犯二遭控洗錢罪名。法院判處嫌犯二 9 個月緩刑，並命其與嫌犯一共同支付 118,000 紐西蘭元（約 73,035 美元）予紐西蘭社會發展部。

上述判決結果，使紐西蘭社會發展部得以恢復原有機制，讓返回庫克群島的居民繼續領取其退休金與福利，此機制曾於警方調查期間暫停運作。

來源 - 庫克群島

2.3 中國香港

案例研究 # 21：透過金融卡進行洗錢

[詐欺；跨國組織犯罪集團；境外前置犯罪](#)

2023年初，A司法管轄區查出來自當地發生的電話詐欺案、超過1億港幣（約1,280萬美元）的犯罪所得被送往中國香港，犯罪所得後續透過金融卡在中國香港以消費方式洗錢。A司法管轄區調查顯示，一個犯罪集團取得第三方（人頭）銀行帳戶及連結之金融卡，指示被害人將資金存入人頭帳戶內。當被害人將款項存入帳戶後不久，犯罪集團協調其成員使用實體金融卡於中國香港購買高價商品。案件仍在調查中。

香港警方於犯罪集團成員使用人頭金融卡交易時逮捕九名集團成員，並查扣人頭金融卡、名貴手錶及其他貴重物品。目前並查扣人頭金融卡、名貴手錶及其他貴重物品。目前該案件仍在調查中。

[來源 - 中國香港](#)

案例研究 # 22：透過加密貨幣洗錢犯罪所得

[第三方洗錢；詐欺；境外前置犯罪](#)

2022年，兩個執法機關交換情報後顯示，有人士控制一批位於中國香港的可疑個人銀行帳戶，在接收來自本地及海外詐欺犯罪所得款項後，頻繁透過自動櫃員機（ATM）提領現金。在犯罪期間，控制該批帳戶的人士共計洗錢逾1億1,100萬港幣（約1,420萬美元）的可疑資金。後續調查發現，本地一個洗錢犯罪集團利用人頭帳戶轉移犯罪所得。一旦犯罪所得匯入帳戶後，該犯罪集團立即指派成員透過自動櫃員機提領現金。犯罪集團以此方式累積大量現金，隨後用以購買加密貨幣，試圖隱匿資金來源。香港警方共逮捕10名集團成員，目前案件調查仍持續進行中。

[來源 - 中國香港](#)

案例研究 # 23：利用虛假網站進行陌生來電推銷貸款詐欺

[貸款詐欺；第三方洗錢](#)

2022年9月至2023年10月期間，一個犯罪集團透過陌生來電（cold call）推銷低息貸款的方式，在中國香港詐騙49名受害人。受害人被引導至假冒持牌貸款機構之虛假網站，並被要求將總額1,530萬港幣（約212.8萬美元）的保證金匯入111個本地個人銀行帳戶，以協助申請貸款。然而，沒有受害人收得任何貸款款項。調查行動已導致14人遭逮捕，其中包括虛假網站的註冊人與人頭帳戶持有人。目前案件調查仍持續進行中。

[來源 - 中國香港](#)

案例研究 # 24：跨境詐騙犯罪集團

[愛情詐騙；投資詐欺；援交詐騙；求職詐欺；第三方洗錢](#)

2023年初，A司法管轄區一項逮捕行動揭發一個進行裸聊詐騙的集團，該集團經營一個詐騙中心，中國與中國香港某洗錢犯罪集團有關聯，涉及149起詐騙案件，總金額達6,820萬港幣（約870萬美元）。A司法管轄區向香港警方提供情報，經調查確認中國香港境內有五名核心成員操作多個人頭銀行帳戶，接收、並以洗錢方式處理詐騙犯罪所得。香港警方逮捕九名出售銀行帳戶予該犯罪集團的人頭帳戶持有人，以及一名提供手機卡（SIM卡）供詐欺者聯絡受害者的手機卡登記人。其中兩名人頭帳戶持有人因「串謀處理明知或合理懷疑為可公訴罪行所得之財產」罪名遭起訴並判決有罪。其餘被捕人士的調查仍在進行中。

[來源 - 中國香港](#)

案例研究 # 25：劫持即時通訊應用程式帳號之詐欺**第三方洗錢；詐欺**

2023 年 10 月至 11 月間，一個本地詐騙集團透過劫持受害人親友之即時通訊帳號（instant messaging accounts），誘使 326 名本地受害人轉帳共計 396 萬港幣（約 550,995 美元）至人頭銀行帳戶。資金流向分析發現，犯罪所得被轉入 10 名人頭所持有的 18 個虛擬銀行個人帳戶，進一步調查顯示多個人頭帳戶由相同 IP 位址控制。警方採取行動，逮捕 13 名集團成員；目前案件調查仍持續進行中。

來源 - 中國香港

案例研究 # 26：透過儲值支付工具進行洗錢（註：此處「工具」一詞涵蓋電子錢包、預付卡等產品。）**第三方洗錢；詐欺**

2023 年 11 月至 12 月間，共計 143 名受害者通報收到偽裝成儲值支付工具（SVF）業者發送之釣魚簡訊，要求受害者登入虛假網站並輸入其 SVF 電子錢包、或信用卡登入資訊以兌換獎勵。受害者遵照指示後不久，即發現其電子錢包或信用卡遭未經授權轉帳或交易，共損失 680,335 港幣（約 94,662 美元）。當局查封 71 個與該等詐騙相關之虛假網站。2023 年 12 月，警方逮捕兩名接管受害者帳戶之嫌犯及五名人頭銀行帳戶持有者。目前案件調查仍持續進行中。

來源 - 中國香港

案例研究 # 27：深偽影片詐欺**詐欺；使用網路應用程式；第三方洗錢**

2022 年 9 月至 2023 年 7 月間，一個本地貸款詐騙集團利用受害者的遭竊或偽造之身分證件，並透過深偽技術（Deepfake）繞過臉部驗證程序，進行 144 次貸款或銀行帳戶申請。該集團成功申辦四筆共計 20 萬港幣（約 25,670 美元）的貸款及五個銀行帳戶，詐貸款項被轉入多個個人人頭帳戶。2023 年 8 月，警方展開公開行動，包括主謀在內的八名犯罪集團成員因涉嫌「串謀欺騙及詐欺」而被捕。目前案件調查仍持續進行中。

來源 - 中國香港

案例研究 # 28：境外架設之線上賭場**非法賭博；使用虛擬資產；第三方洗錢**

情資顯示，一個設於 A 司法管轄區之非法網路賭博網站，透過社群媒體平台向中國香港居民散播大量垃圾訊息，積極推廣線上賭博。參與賭博者必須以銀行轉帳、或加密貨幣購買賭博點數，每次贏取點數時需支付 5% 的佣金。調查發現，該犯罪集團實際上透過本地營運中心操控該平台，並於中國香港使用人頭帳戶進行儲值與提現操作。2023 年 8 月底，32 名中國香港居民因「串謀非法收受投注」罪名被捕，另有 15 人因「串謀洗錢」罪名被捕。2022 年 10 月至 2023 年 7 月期間，該集團共計洗錢約 3,850 萬美元，每月投注額估計約 330 萬美元。

來源 - 中國香港

案例研究 # 29：利用現金攜帶者之洗錢集團**跨境現金運送；有組織犯罪**

隨著 2023 年初跨境旅遊全面恢復，中國香港海關透過主動分析跨境現金、與不記名有價證券申報資料，於 2023 年 5 月至 6 月間，破獲一個利用現金攜帶者洗錢之犯罪集團，涉案金額約 7 億港幣（約合 8,970 萬美元）。自 2023 年 1 月起，中國香港海關發現一洗錢集團雇用現金攜帶者將大量美元運送進入中國香港。通關時，現金攜帶者聲稱其為 A 司法管轄區兩家公司員工，所攜帶現金係用於在中國香港採購珠寶鑽石。然而經調查後，其等無法提供採購明細，且透過艾格蒙聯盟（Egmont Group）與 A 司法管轄區交換之情報亦顯示，該兩家公司實際未從事珠寶鑽石交易。2023 年 5 月，中國香港海關破獲該洗錢集團，逮捕 23 人並扣押現金共 4,300 萬港幣（約合 550 萬美元），疑為犯罪所得。目前案件調查仍持續進行中。

來源 - 中國香港

案例研究 #30：以住宅作為犯罪作業中心**獨立洗錢；可疑交易通報**

經分析本地銀行提交之可疑交易報告（STRs），中國香港金融情報中心發現一個洗錢集團利用多家本地銀行帳戶進行交易，並頻繁透過一家不知情的貨幣服務業者提領現金，以處理來自多個可疑交易相對人之資金。2020 年至 2022 年間，該集團涉案可疑資金總額約 60 億港幣（約 7 億 6,700 萬美元）。調查顯示，該洗錢集團在一處大型私人住宅社區內租用住宅，藉此掩飾洗錢活動。2023 年 1 月，中國香港海關以洗錢罪名逮捕九人，並扣押現金共計 389 萬港幣（約合 50 萬美元）目前案件調查仍持續進行中。

來源 – 中國香港

2.4 印度

案例研究 #31：透過空殼公司洗錢**詐欺（含電話／簡訊／電子郵件／社群媒體）；自我洗錢；新型支付方式；使用法人與法律協議**

2021 年 1 月，印度海得拉巴邦（State of Hyderabad）警方接獲報案並展開搜查行動，揭發一個透過手機應用程式，以高額利率進行小額貸款的公司網路。調查發現，這些手機應用程式由外籍人士透過印度境內的多家空殼公司運作。這些應用程式提供高利貸予被害人，同時從被害人手機非法蒐集個資，藉此對被害人進行勒索，以追回貸款本息。其犯罪手法（Modus Operandi）包括：

- 外籍人士在印度設立空殼公司，以接收來自其所屬司法管轄區的資金；並聘用外國及當地印度籍董事。
- 此等空殼公司之後與印度境內的非銀行金融公司（Non-Banking Financial Companies, NBFCs）簽署合作備忘錄（MoU）。根據該備忘錄，空殼公司向非銀行金融公司支付保證金，NBFCs 再透過支付閘道為其開立多個商業識別碼（Merchant IDs），使空殼公司得以運行手機應用程式。這些應用程式登錄於各大主流手機應用商店（app stores）。
- 貸款透過應用程式發放，款項回收亦透過應用程式及支付閘道進行，並由 NBFCs 透過商業識別碼，扣除佣金後將款項轉回空殼公司。

經洗錢調查後，總共查扣 78 億印度盧比（約 9,300 萬美元），共起訴 521 名法人及自然人。目前案件調查仍持續進行中。

來源 – 印度

案例研究 #32 – 基於可疑交易報告所進行之資恐調查**恐怖主義，包括資恐；貿易洗錢；使用法人與法律協議**

2020 年 6 月，印度國家情報局（National Intelligence Agency, NIA）從印度金融情報中心收到關於 A 人士的可疑交易報告（STR）。一家金融機構因其負面媒體報導及不尋常交易模式而提交該 STR，理由是 A 人士所操作的商業帳戶僅有現金提款，未見任何實質商業交易活動。該金融機構在可疑交易報告中，提供 A 人士其他帳戶之資訊及相關識別資訊。

此 STR 促使印度國家情報局得以針對 A 人士（及其他）之商業活動進行調查，發現數名資助恐怖主義分子之幕後金主。這些資恐分子透過低報發票金額製造貿易不平衡以獲取利潤，以此支持真主穆斯林游擊隊（Hizbul Mujahideen）及虔誠軍（Lashkar-e-Tayyiba）等恐怖組織之生計與運作。上述資恐分子參與資金之籌集與分配，但未直接涉入恐怖活動。依 1967 年《防制非法活動法》（*Unlawful Activities (Prevention) Act, 1967*）之資恐罪名，其等正被起訴中。

來源 – 印度

2.5 印尼

案例研究 # 33：行賄造成國家財務損失

貪污與行賄；資金混合；金融機構

被定罪之法人（X 公司）於 2014 財政年度獲選為 Z 市政府一項專案之貨物／服務供應商，合約金額為 56 萬 7,000 美元。此專案應於 2014 年 4 月 1 日至 2014 年 12 月 1 日期間完成；但卻未依合約規定執行，X 公司卻於履約義務完成前即收到全額付款。稽核調查發現政府採購程序中，所提交的部分投標文件為虛假的資格證明文件。

稽核報告指出，被告作為專案貨物／服務供應商之行為，致使 X 公司不當得利，並對國家財政造成 23 萬 6,000 美元損失。犯罪貪污所得已由貨物／服務使用者轉入被告公司於銀行 C 開立之帳戶，使得此筆資金與原帳戶內既有資金混合，意圖隱匿並掩飾源自貪污犯罪之資產來源。X 公司已因貪污及洗錢罪名遭起訴，並被處以 4 萬 7,000 美元罰款。

來源 - 印尼

案例研究 # 34：行賄造成國家財務損失

貪污與賄賂；資金混合；金融機構；重要政治性職務人士

被告 B 公司與兩間關係企業，實際由重要政治性職務人士（PEP）官員 A 人士實質擁有與控制。A 人士利用 B 公司作為掩護，自政府專案合作夥伴收受賄賂，自政府專案合作夥伴收受賄賂，並從其主管的政府工程專案中獲取利益，其中 A 人士負責監管採購過程。2016 至 2017 年間，A 人士將 B 公司資金與關係企業帳戶混合，隨後提取資金供自身及其家人使用。當局對 B 公司的調查包括公司設立證書、公司章程及修訂文件、公司支票帳戶授權書、會計記錄及金融交易。調查發現，儘管法律上由一名員工負責控制 B 公司，但 A 人士實際為該公司控制人與實質受益人。

被告 B 公司被判洗錢罪，法院裁處 3,145 美元罰款，並判決沒入公司資產上繳國庫，金額分別達 22 萬 6,000 美元與 14 萬 4,000 美元，並禁止該公司在三年內參與政府貨物及服務採購投標。

來源 - 印尼

案例研究 # 35：假外匯交易之洗錢與詐欺

詐欺；自我洗錢；資金混合；虛擬資產服務提供商；使用虛擬資產（加密貨幣或其他資產）；購置不動產

2018 年，X 人士在網站「Y」註冊帳戶。「Y」為一種遊戲，玩家投注所選商品在特定時間內價格將上升或下降，其中一個商品為外國貨幣。若玩家投注正確，將獲得投注金額 80% 的收益；若投注錯誤，則損失全部投注金額。

X 人士之後成為「Y」的聯盟會員（affiliate），可推薦潛在玩家加入「Y」，並依營收比例獲取酬勞。X 人士製作「Y」交易相關教學影片，發布於個人 YouTube 頻道、Instagram 與 Telegram 帳號，並藉由個人推薦連結吸引玩家註冊。

為進一步使大眾相信「Y」為合法交易平台，X 人士另外成立經營教育業務的 Z 公司，並自任董事及主要股東。公司 Z 的業務活動包括開設課程或培訓，提供關於加密資產交易、股票、金融教育與電子遊戲之教學影片，學員須繳付 94 至 125 美元／年之課程費用，截至 2022 年初已吸引約 3,000 名學員。

X 人士透過社群媒體發布不實言論，如「值得信賴」、「Y 在印尼合法」與「Y 於 2015 年在印尼正式營運，迄今已有四年」等。實際上，「Y」的活動在印尼既不合法，也未經官方許可，更未獲商品期貨交易監理機構（BAPPEBTI）許可。X 人士的行為導致 144 名被害人損失約 520 萬美元。

作為「Y」聯盟會員，X 人士自「Y」分潤獲取利益，透過自己及他人銀行帳戶、虛擬帳戶支付閘道及比特幣（Bitcoin）、以太坊（Ethereum）等加密資產收取資金。2020 年 6 月至 2022 年 1 月期間，X 人士透過其虛擬資產服務提供商（VASP）帳戶接收了比特幣與以太坊的加密貨幣交易，共計 105 筆，總額達 395 枚比特幣（BTC）。X 人士將比特幣提領後轉入銀行帳戶，金額達 650 萬美元。X 人士以此收益購置房產、豪華汽車與名錶，並將資金轉予家人、女友與家人、第三方、自營公司 Z 及擔任董事的 B 公司。

經法律程序證明，X 人士犯下散播不實及誤導性訊息，致使消費者於電子交易中受損，並涉及洗錢等犯罪行為，罪證確鑿。法院判處 X 人士有期徒刑十年，併科罰金 615,000 美元。如未繳納罰金，則以額外十個月徒刑代替。

來源 - 印尼

案例研究 # 36：藥廠詐欺案

詐欺；新冠肺炎（COVID-19）

C 人士係 K 藥品公司之業務經理，該公司於機場提供新冠肺炎抗原快速篩檢（Rapid Antigen Test）服務。收取包括第三人銀行帳戶內之犯罪所得。C 人士指示多名員工重複使用達克綸（Dacron）拭子及試管，不法獲利約 22 億印尼盾（約 137,500 美元）。為掩飾其非法行為，C 人士另指示員工竄改新冠肺炎抗原快速篩檢報告，減少向相關機關通報之篩檢數量。C 人士將上述非法所得用於個人利益，並將資金置於包括員工帳戶在內之數個由其控制之銀行帳戶內。C 人士遭權責機關依違反健康相關法規、消費者保護法及洗錢罪起訴，法院判處有期徒刑 10 年，併科罰金印尼盾 10 億元（約 65,208 美元），並沒入包括第三人銀行帳戶內之犯罪所得。

來源 - 印尼

案例研究 # 37：透過銀行及網路貸款進行資恐

恐怖主義，包括資恐；金融機構

2019 年，警方於搜索 B 人士住處時發現，B 人士向 X 銀行及數家金融科技公司（網路貸款／點對點借貸）獲取貸款，單筆金額介於 37 美元至 628 美元間，合計 1,000 美元。B 人士將該資金用於資助恐怖組織（包括提供組織運作資金及分發予組織成員），並用於進行恐怖行動（購買用於恐怖攻擊之武器），其中 314 美元則用於個人用途。

來源 - 印尼

2.6 日本

案例研究 # 38：國際愛情詐騙犯罪所得偽裝為汽車銷售收入

詐欺；第三方洗錢；金融機構；可疑交易通報

日本金融情報中心（JAFIC）分析大量可疑交易報告之內容，發現報告常出現「長期不活動帳戶突然存入小額資金後，再由多個帳戶匯入大量資金」之關鍵語句。其中一起案件顯示，匯入 A 人士帳戶之資金係來自國際愛情詐欺與投資詐欺之犯罪所得。警方調查發現，A 人士將犯罪所得存入公司銀行帳戶，並偽稱該筆資金係汽車銷售所得。警方依詐欺及違反《有組織犯罪處罰法暨犯罪所得管制法》（隱匿犯罪所得）罪名逮捕 A 人士。

來源 - 日本

案例研究 # 39：透過匯款至高風險司法管轄區走私甲基安非他命 (methamphetamine)**毒品相關犯罪；走私；金融機構；電匯；可疑交易通報**

警方根據金融機構提交之可疑交易報告啟動調查，此報告內含「於同一日自多個分行匯款至具詐欺高風險之司法管轄區」、「依陪同人員指示申請國外匯款」及涉及可疑進口包裹等資訊。警方調查後鎖定多名不同國籍嫌疑人，涉嫌自國外走私甲基安非他命。警方依違反《麻醉藥品及精神藥物取締法等之特別規定及鼓勵非法行為等活動防制之其他事項法》（共同持有違禁藥物罪）（Act Concerning Special Provisions for the Narcotics and Psychotropics Control Act, and Other Matters for the Prevention of Activities Encouraging Illicit Conducts and Other Activities Involving Controlled Substances through International Cooperation）將嫌疑人逮捕。

來源 - 日本

案例研究 # 40：利用跳蚤市場應用程式販售名牌仿冒品**仿冒及盜版產品；自行洗錢；金融機構；新型支付工具；可疑交易通報**

日本金融情報中心分析多筆疑似可疑交易報告，發現關鍵詞例如「多個跳蚤市場應用程式之款項經由網路銀行轉帳至個人帳戶，但該帳戶使用目的與實際交易狀況不符」等情事，懷疑有個人販售仿冒名牌商品。警方進行調查後發現，A 人士販售名牌仿冒品，並從 B 人士處取得金融卡。警方依違反《商標法》（Trademark Act）及《犯罪所得移轉防制法》（涉及無償收受犯罪所得）（Criminal Proceeds Act (gratuitous receiving)）之罪，將 A 人士移送檢察官偵辦。

來源 - 日本

案例研究 # 41：透過加密資產將犯罪所得轉移至境外司法管轄區**詐欺、第三方洗錢、虛擬資產服務提供商、使用虛擬資產、可疑交易通報**

日本金融情報中心分析可疑交易報告內的關鍵詞，例如「於自動櫃員機存入大量現金後，再透過特定加密資產交易所將資金轉移至境外司法管轄區」以及「帳戶持有人涉及詐欺案件」。

日本警方調查後，於 B 人士通知警方詐欺取得款項的常用交付地點後，查明收取款項之人為 A 人士。A 人士指示其店內不知情的店員代收該筆款項，隨後將該筆款項兌換成加密資產後轉移至境外司法管轄區。日本警方以違反《組織犯罪處罰法》（Act on Punishment of Organized Crimes）（收受犯罪收益）罪名逮捕 A 人士。

來源 - 日本

案例研究 # 42：使用電子貨幣隱匿詐欺所得**詐欺；第三方洗錢；金融機構；新型支付工具**

詐欺集團成員 B 人士致電被害人，誘騙被害人交出銀行卡。詐欺集團另一成員 A 人士持該銀行卡於自動櫃員機提領現金後，以部分現金購買電子貨幣，並透過 Telegram 將電子貨幣的使用權（以電子貨幣使用代碼形式）轉移至 C 人士的帳戶。日本警方以違反《組織犯罪處罰法》（隱匿犯罪收益等）逮捕 A 人士。

來源 - 日本

案例研究 # 43：利用遠端控制應用程式進行電腦詐欺並隱匿犯罪所得**詐欺；自行洗錢；金融機構**

A 人士於 B 人士的電腦螢幕顯示偽造之資訊安全訊息，誘導 B 人士撥打螢幕顯示的電話號碼。A 人士接聽該通電話，並謊稱自己為資訊安全公司的員工，要求 B 人士下載遠端控制應用程式，並輸入其網路銀行之使用者名稱及密碼。C 人士（掌控以第三人名義開立之帳戶）收受自 B 人士帳戶未經授權轉帳之款項，遭警方以違反《組織犯罪處罰法》（隱匿犯罪收益等）逮捕。

來源 - 日本

案例研究 # 44：收受銀行現金卡以抵銷債務**詐欺；金融機構**

B 人士積欠 A 人士債務，因此 B 人士開設一個銀行帳戶，並將所欠金額存入該帳戶後，將連結該帳戶的現金提款卡交給 A 人士。B 人士保證自己不會使用該帳戶，藉此將債務償還給 A 人士。日本警方隨後以違反《有組織犯罪處罰法》（收受犯罪收益等）之罪名逮捕 A 人士。

來源 - 日本

2.7 韓國**案例研究 # 45：透過空殼公司進行貿易洗錢****稅務犯罪；貿易洗錢；電匯；使用信用卡／簽帳卡；購置不動產**

韓國海關透過蒐集與分析金融交易及貿易紀錄，發現 A 公司涉及可疑活動。位於韓國的 A 公司從事藥品包裝材料出口業務，並設立 B 空殼公司於 C 司法管轄區。A 公司透過偽造紀錄欺騙韓國海關，使其看似與空殼 B 公司進行相關貿易活動。A 公司直接將價值 1400 萬美元的產品出口至 D 司法管轄區，但僅向海關申報 1,200 萬美元。

A 公司將 200 萬美元轉移至位於 C 司法管轄區之 B 公司。這些被轉移的收益隨後透過 40 個未經揭露的帳戶（用以向韓國權責機關隱匿資金流向）以小額交易方式洗錢回流至韓國，並經由自動提款機提領現金。此 40 個帳戶皆以他人（例如熟人）的名義持有，而非犯罪者本人。

透過此種偽造貿易利潤行為，A 公司成功逃漏稅款。調查期間，韓國權責機關亦發現 A 公司代表另將部分轉移之資金用於購買房地產（公寓）。

2023 年 1 月，韓國權責機關依據大韓民國海關相關法規及犯罪收益隱匿相關法規，起訴 A 公司。韓國權責機關亦於起訴前，針對 A 公司代表持有之公寓提出假扣押聲請（provisional attachment），以防止其遭處分。目前司法程序仍在進行中。

來源 - 韓國

2.8 中國澳門**案例研究 # 46：前政府官員及商人涉及貪污與洗錢案件****貪污與行賄；濫用職權；重要政治性職務人士；第三方洗錢；不動產；電匯；公司股份**

中國澳門前政府官員 A 人士與 B 人士在職期間，濫用職權協助 C 房地產開發商、D 開發商及 E 開發商通過當地建築工程的審批程序，藉此獲取不法利益。作為回報，C 房地產開發商、D 開發商及 E 開發商透過低於、或高於市價買賣不動產、轉讓共同設立之公司股份，及透過他人提供各種利益等方式，非法向 A 人士與 B 人士行賄。在上述過程中，A 人士與 B 人士的共犯及家人協助收受及處置相關非法利益，藉以隱匿資產的非法性質及來源。

2022 年，中國澳門檢察院（Public Prosecutions Office）對 A 人士、B 人士、C 房地產開發商、D 開發商、E 開發商及其他犯罪同夥提出起訴，指控罪名包括不法行為之收受賄賂、行賄及洗錢罪。2023 年，經中國澳門初級法院與中級法院審理後，A 人士、B 人士、C 房地產開發商、D 開發商、E 開發商及其他相關人士被判決前述罪名成立，各被告分別被判處數年至 20 年不等之有期徒刑。

來源-中國澳門

案例研究 # 47：利用新型電子支付工具洗錢販毒犯罪所得**毒品犯罪；自我洗錢；第三方洗錢；現金；電匯；使用金融卡；新型支付方式**

2021 年，A 人士與 B 人士受指使在中國澳門從事販毒活動，為掩飾並隱匿犯罪所得，其等受指示安排銀行帳戶收取毒品買家付款。B 人士隨後與 C 人士協商，借用 C 人士銀行帳戶接收毒品買家匯款。

C 人士透過連結帳戶之簽帳金融卡提領犯罪所得後，以現金、或透過其他電子支付平台將犯罪所得轉交 A 人士。A 人士隨後與當地一家當舖員工聯繫，透過即時通訊應用程式之境外手機支付服務，將犯罪所得轉匯給位於 D 司法管轄區的毒品供應商。

中國澳門檢察院於 2023 年以洗錢罪起訴 A 人士、B 人士及 C 人士，其中 A 人士與 B 人士已於 2022 年被中國澳門初級法院判處有毒品犯罪及相關罪名。

來源-中國澳門

案例研究 # 48：破獲涉及有組織犯罪、詐欺與洗錢之非法賭博集團**跨國犯罪集團；非法賭博；詐欺；第三方洗錢；結構化交易 / 化整為零洗錢）；賭場；現金；虛擬資產（加密貨幣）**

2023 年 1 月，中國澳門司法警察破獲一跨國犯罪集團，該集團在中國、中國澳門與中華臺北經營非法線上賭博平台。該非法線上賭博平台提供多個賭博帳戶及各式網路投注選項，其後端伺服器設於中國澳門境外。該集團成員或旗下代理人負責招攬賭客。

該犯罪集團利用人頭帳戶或加密貨幣，以洗錢方式處理線上賭博的犯罪收益。此外，該集團亦將約 350 萬美元的犯罪收益轉移至集團成員的銀行帳戶，同時以化整為零方式將資金轉移至中國境內。中國澳門司法警察於行動中扣押約 130 萬美元現金，並以犯罪集團罪、非法賭博罪及洗錢罪將多名嫌疑人移送檢察院偵辦。

來源-中國澳門

案例研究 # 49：三名本地嫌疑人涉重大犯罪的洗錢、犯罪集團及詐欺被捕**電話詐欺；自我洗錢；第三方洗錢；金融機構；現金；使用簽帳金融卡；區域合作；購買高價商品**

2023 年 6 月，澳門司法警察反詐騙協調中心接獲情資，一宗中國境內電信詐欺案相關的犯罪所得 19 萬美元已轉至中國澳門，司警立即展開調查。

經調查後發現，該犯罪集團利用境外金融卡，以洗錢方式處理犯罪所得，再使用這些金融卡於中國澳門珠寶店購買奢侈品，交易金額超過 9 萬美元。司法警察成功於珠寶店內識別出集團成員，並立即通知中國執法機關。中國警方隔日逮捕該批集團成員。此外，司法警察亦成功攔截另外三名嫌疑人，扣押約 9 萬 3000 美元及一部車輛；並以犯罪集團罪、詐欺罪及洗錢罪將三名嫌疑人移送檢察院偵辦。

來源-中國澳門

案例研究 # 50：兩名嫌疑人涉虛擬貨幣詐欺及洗錢被捕**詐欺；自我洗錢；賭場；虛擬資產服務提供商；現金；使用虛擬資產；區域合作**

澳門司法警察接獲鄰近司法管轄區之情資及協助請求，涉及一起利用虛擬貨幣交易平台之重大詐欺案件；

於是立即展開調查，進一步資訊顯示該虛擬貨幣交易平台虛假聲稱為擁有多個場外貨幣兌換據點的有執照公司。為吸引投資者，該平台亦聘用知名人士在網路上進行宣傳，承諾提供不合理之高額投資報酬率。然

而，該平台發行的虛擬貨幣因流動性極低，無法在場外自由交易。此外，該平台向投資者收取提款手續費，且得任意調整費率。導致投資者無法取回本金。根據鄰近司法管轄區執法機關之資訊，截至 2023 年 9 月已有超過 2,000 名被害人向警方報案，涉案資金總額約達 1 億 9000 萬美元。

經調查後，司法警察在中國澳門確認兩名與該案有關之嫌疑人，並扣押其持有約 83 萬美元的賭場籌碼及約 9,000 美元現金。隨後凍結嫌疑人於賭場所設之前線存款帳戶，帳戶內約有 100 萬美元。

儘管嫌疑人拒絕透露相關細節，司法警察已查明此二人係涉及該虛擬貨幣交易平台詐欺案之核心成員，利用賭場前線存款帳戶轉移、隱匿，並以洗錢方式處理犯罪所得資金。澳門司法警察已依犯罪集團罪、電腦詐欺罪及洗錢罪將該兩名嫌疑人移送澳門檢察院偵辦。

來源-中國澳門

案例研究 # 51：透過合法博弈中介業務從事非法賭博及洗錢

犯罪集團；非法博弈業務；檯底投注(under-table bets)；境外線上賭場；詐欺；三合會(triad)；博弈中介公司

2021 年 11 月及 2022 年 1 月，執法機關於中國澳門就兩起刑事案件逮捕兩名商人及多名共犯，其中包括博弈中介公司之高階主管。上述兩名商人為中國澳門兩家大型博弈中介公司（junkets）的所有人，涉嫌透過有執照的博弈中介業務進行非法博弈活動。該非法博弈活動包括於澳門賭場內利用合法賭桌結果進行檯底投注（under-table bets），以及利用現有博弈中介公司在澳門之資源（包括員工、前線存款帳戶及客戶資源）經營境外線上賭場。

兩名商人利用博弈中介前線存款帳戶、博弈積分、中國澳門及境外公司（法人）以及銀行帳戶作為轉移非法博弈所得之管道。

2023 年 1 月至 2024 年 1 月期間，兩名博弈中介公司實際負責人因經營非法博弈（檯底投注及境外線上賭場）、領導三合會犯罪集團及加重洗錢罪，經中國澳門法院判處 18 年⁷⁵ 及 13 年⁷⁶ 有期徒刑。

來源-中國澳門

2.9 馬來西亞

案例研究 # 52：透過濫用非營利組織犯下背信罪及洗錢罪

貪污與行賄；自我洗錢；詐欺；背信罪；濫用非營利組織

馬來西亞反貪污委員會（Malaysian Anti-Corruption Commission, MACC）針對 A 人士、B 人士及 C 人士提出涉及洗錢、詐欺及背信罪的 164 項指控，相關金額約 3,950 萬令吉（約 820 萬美元）。

A 人士與 B 人士負責管理某非營利組織（NPO）資產，且同時擔任 A 公司之董事。他們涉嫌濫用非營利組織約 2,090 萬令吉（約 440 萬美元），該資金源自大眾捐款，卻未被提供給原定受捐對象。

A 人士與 B 人士涉及 2018 年至 2023 年透過銀行進行之匯款，各被控 52 項刑事背信罪。此外，其等共同被控 19 項詐欺罪，欺騙該非營利組織之信託董事會提取 3910 萬令吉（約 810 萬美元）現金，支付予 A 公司代購黃金，而 A 公司的購買價格遠超出市場價格。此外，A 人士與 B 人士以 A 公司董事身分，各自另面臨 19 項洗錢罪指控，涉及利用約 1,280 萬令吉（約 270 萬美元）購買豪華車輛、商店店面、倉庫及土地。調查顯示，該洗錢行為僅於國內，並無境外洗錢活動跡象。

⁷⁵ 2023 年 1 月，首宗刑事案件之博弈中介公司實際負責人被判處 18 年徒刑。來源：中國澳門初級法院，案件編號：CR2-22-0147-PCCh^{https://www.court.gov.mo/sentence/zh-9f8cd198757f3527.pdf} 2023 年 10 月，中國澳門中級法院支持檢察院意見，維持原有判決，該博弈中介公司實際負責人仍犯洗錢罪。來源：中國澳門中級法院，案件編號：162/2023，^{https://www.court.gov.mo/sentence/zh-6baa9952c1a81882.pdf}

⁷⁶ 2023 年 4 月，第二宗刑事案件之博弈中介公司實際負責人初審被判 14 年徒刑。來源：中國澳門初級法院，案件編號：CR1-22-0166-PCCh^{https://www.court.gov.mo/sentence/zh-27669220ca401221.pdf} 首次上訴後，2024 年 1 月，中國澳門中級法院將刑期減為 13 年。來源：中國澳門中級法院，案件編號：TSI-461/2023，^{https://www.court.gov.mo/sentence/zh-aac7e384f7a73fda.pdf}

同時，同為 A 公司董事的 C 人士，被指控涉及利用非法活動的犯罪所得共計 600 萬元令吉（約 130 萬美元），購置商店店面及倉庫，遭起訴三項罪名。目前案件仍在調查中。

來源 - 馬來西亞

案例研究 # 53：欺詐性層壓式推銷及未經許可之電子貨幣服務投資詐欺

投資詐欺

A 公司設立一系列子公司，在未取得直銷管理機關（controller of Direct Sales）頒發有效許可證下，即以電子交易方式進行直銷業務。該公司推廣一種層壓式推銷（pyramid scheme）架構，會員透過直接銷售會員套裝及招募下線成員以取得佣金或其他利益。

與此同時，A 公司積極推廣自家電子錢包應用程式，使用者購買以令吉計價之「電子券」，可於登記商家兌換商品或服務。A 公司透過促銷期間提供紅利券（bonus vouchers），鼓勵使用者購買電子券；這些紅利券亦可於註冊商家兌換商品及服務。A 公司承諾用戶可隨時將未使用之電子券金額提現。

當 A 公司停止讓用戶由已購買之電子券提領資金後，民眾開始向多個監理及執法機關提投訴。事實上，A 公司因懷疑執法機關對其營運展開調查，已關閉自身及其子公司之銀行帳戶。儘管成立時間相對較短，A 公司帳戶卻與眾多交易相對人有極高交易量，累積交易金額達數十億元。權責機關已對 A 公司及其董事，以未取得有效許可進行電子交易直銷業務、推廣層壓式推銷及洗錢等罪名提出起訴。目前案件仍在調查中。

來源 - 馬來西亞

2.10 馬爾地夫

案例研究 # 54：不動產詐欺案

詐欺；公司組織形式濫用；偽造文書；稅務犯罪；資金多層化；結構化交易（化整為零）；不動產

在媒體報導指出 A 人士在 A 司法官轄區從事不動產詐欺活動後，馬爾地夫金融情報中心（FIU）針對其金融活動、關係人及其在詐欺活動中使用的法人進行分析。金融情報中心發現，A 人士向多位個人收取鉅額資金，作為其 A 公司銷售豪華公寓之預付款。A 人士為 A 公司少數股東，並偽造公司文件，得以操作公司銀行帳戶。除了透過公司銀行帳戶將資金轉入 A 人士個人帳戶外，A 人士也直接透過現金或銀行轉帳向買家收取款項。A 人士甚至將同一間公寓重複出售給多位買家，並詐欺所有買家要求其等直接以現金支付預付款給自己，而非給 A 公司。A 人士另外設立多間公司，透過這些公司及相關人員對 A 公司資金進行多層化並轉移。

金融情報中心經分析財務記錄與其他資訊，發現 A 人士使用這些資金在馬爾地夫及 B 司法官轄區購置其他不動產，並購置部分奢侈品。金融情報中心成功追溯此等高價值不動產與奢侈品資訊，並提供給執法機關作後續調查及起訴。執法機關已就洗錢及相關前置犯罪起訴 A 人士及一名共犯，並扣押位於馬爾地夫的資產，同時已追溯其等在 B 司法官轄區的資產。目前，執法機關與檢察總長辦公室正就 A 人士位於 B 司法官轄區的資產進行扣押程序。

來源 - 馬爾地夫

案例研究 # 55：濫用非政府組織

[濫用非政府組織資金；非法外匯交易；濫用職權；稅務犯罪；資金多層化；結構化交易（化整為零）](#)

馬爾地夫金融情報中心分析當地一個知名非政府組織（NGO）之財務記錄及相關資訊，發現該非政府組織主席 A 人士濫用該組織資金以謀取私利，購買不動產。此外，A 人士亦使用部分非政府組織資金進行個人商業投資。A 人士濫用其作為非政府組織主席之職權，透過偽造文件，以美元買賣交易為名掩飾資金之真實用途。金融情報中心成功追溯其購買的不動產、商業投資交易及個人支出相關交易。

經相關執法機關調查後，檢察總長辦公室正準備就 A 人士涉不動產部分以洗錢及相關前置犯罪提起起訴。目前，檢察總長辦公室已就 A 人士洗錢及非法外匯交易提出起訴，該案件正在刑事法院進行審理。

來源 - 馬爾地夫

2.11 巴基斯坦

案例研究 # 56：協助境外貸款詐欺

[詐欺；逃漏稅](#)

巴基斯坦公司權責機關—巴基斯坦證券交易委員會（SECP）檢視了 A 有限公司（下稱 A 公司）最近三個財務年度之經審計年度帳目及相關季度帳目，初步證明（*prima facie*）該公司 2018 年及 2019 年之帳目存有重大錯報情形，遂向巴基斯坦金融監控單位（FMU）提交可疑交易報告（STR）。

三年期間內，A 有限公司及其董事與股東於不同銀行開立了共計 10 個帳戶，帳戶總貸方交易總額（credit turnover）達 15 億盧比（約 540 萬美元）。該資金主要匯入董事及其關係企業（包括姊妹公司）之帳戶，但這些帳戶並無任何與業務相關之交易活動。

2012 年，A 公司自境外 B 公司收取 110 萬美元股權申購預付款，但隨後並未向 B 公司發行股票，而是將此筆資金轉列為長期融資。截至 2019 年 6 月底，該筆 110 萬美元本金及 6 萬美元利息之融資未經適當考量（due consideration）即被註銷，僅提供投資公司已終止營業之通知。

同樣地，2016 年 A 公司向另一家境外 C 公司取得總額度 100 萬美元之貸款，其中 50 萬美元於 2016 年取得，餘額 50 萬美元則於 2017 年度取得。截至 2020 年 6 月底，A 公司再度未經適當考量即註銷該貸款。

審計報告顯示，A 公司已連續九年虧損，儘管如此，該公司仍聲稱自境外公司取得貸款，且該等貸款隨後亦未經適當考量即被註銷。

儘管 A 公司之主要業務持續虧損，關聯企業營業額也極低，但 A 公司之董事與股東於稅務申報中所申報的海外資產卻多年來大幅、且無法合理解釋地增加。這表明可能存在逃漏稅情事，且虧損可能為多年蓄意誤報。

此外，權責機關亦懷疑 A 公司及其關係企業之利潤可能透過未經申報管道非法轉移至海外。再者，自境外公司以貸款方式注入資金，似乎為將原先置於境外資產內之利潤或資金回流的手法。

上述調查結果已通報執法機關，並已展開調查，另透過巴基斯坦金融監控單位（FMU）向涉及境外公司所在地之外國司法管轄區金融情報中心提出非正式國際合作請求。

來源 - 巴基斯坦

案例研究 # 57：社群媒體之虛假廣告

透過社群媒體之詐欺

權責機關發現提供數位投資與外匯交易服務、名為 A Trade、B Trade 及 C Trade 的三個安卓（Android）應用程式。A Trade 為吸引投資人，偽造並廣告宣傳一張巴基斯坦總理之圖片。該圖片展示巴基斯坦總理站在外國人群中，被刊登於「Youtube.com」，廣告內聲稱以 5 盧比（約 0.02 美元）、50 盧比（約 0.18 美元）及 500 盧比（約 1.80 美元）等小額投資，兩三天內可獲得高額利潤，分別達 200 盧比（約 0.72 美元）、3,000 盧比（約 10.81 美元）及 40,000 盧比（約 144.10 美元）。然而，該總理圖片疑似修改自一張外國公司官員向巴基斯坦總理捐贈支票援助水災災民之真實照片。

截至 2023 年 4 月 5 日，民眾已下載這三個手機應用程式各超過 10 萬次。當選擇存款（投資）選項時，這些應用程式提供 500 盧比（約 1.80 美元）至 50,000 盧比（約 180.11 美元）不等的投資方案。然而，選擇任一方案後，資金通常被轉入個人帳戶，而非 A Trade、B Trade 或 C Trade 之商業帳戶。

每次透過應用程式進行存款操作，通常會產生一個新的個人帳戶。權責機關發現數百個此等無分行銀行帳戶，其中有多個帳戶彼此三個安卓應用程式共同使用。

權責機關分析總計 30 個主要帳戶，合計貸方交易金額超過 5 億盧比（約 180 萬美元）。分析顯示這些帳戶於相近時間開設、接收小額資金，且來自相同地區。帳戶持有人多為未滿 30 歲且不識字之個人，該等貝納米帳戶（benami accounts）係專門用以轉移該等投資款項。其中兩個帳戶已被執法機關調查。此外，此 30 個主要帳戶中的 11 個帳戶交易量最高，其中大多數資金以現金提領，權責機關懷疑此等帳戶持有人為詐欺案的最終受益人。

許多投資人向 Google Play 商店檢舉這些安卓應用程式涉及詐欺與騙局。

巴基斯坦金融監理單位已將金融情資提交給執法機關，目前該案件正在進一步調查中。

來源 - 巴基斯坦

案例研究 # 58：龐氏騙局

詐欺；使用法人及法律協議

根據巴基斯坦證券交易委員會針對 XYZ 集團發布的警示公告，建議大眾避免投資該集團的詐欺性投資計畫，巴基斯坦金融監理單位收到不同銀行提交多筆可疑交易報告（STRs）。

XYZ 集團（私人）有限公司（XYZ Group (Private) Limited，XYZ 集團旗下公司之一）的董事持股狀況如下：

| 序號 | 姓名 | 職務/身分 | 持股比例 % | 年齡 |
|----|------|---------|--------|------|
| 1 | A 人士 | 董事 / 股東 | 99% | 21 歲 |
| 2 | B 人士 | 董事 / 股東 | 1% | 24 歲 |

A 人士現年 21 歲，為 C 人士之女、D 人士之妹；B 人士現年 24 歲，曾任 XYZ 集團區域經理，目前為 XYZ 集團（私人）有限公司之董事。

XYZ 集團的商業模式與 LMN 集團公司相似，LMN 集團公司由 C 人士與 D 人士所有。執法機關已針對 LMN 集團涉嫌透過網站向大眾募集資金、並承諾提供高額回報展開調查；巴基斯坦金融監理單位（FMU）先前亦已就 LMN 集團提供金融情資予執法機關與監管機關-巴基斯坦證券交易委員會。

金融監理單位於資料庫內查詢 A 人士與 B 人士之電腦化國民身分證號碼（Computerized National Identification Numbers, CNIC），發現於 2023 年期間，A 人士涉及 491 筆現金交易報告（CTRs），總金額達 22 億盧比（約 790 萬美元）；B 人士涉及 413 筆現金交易報告，總金額達 19 億盧比（約 680 萬美元）。

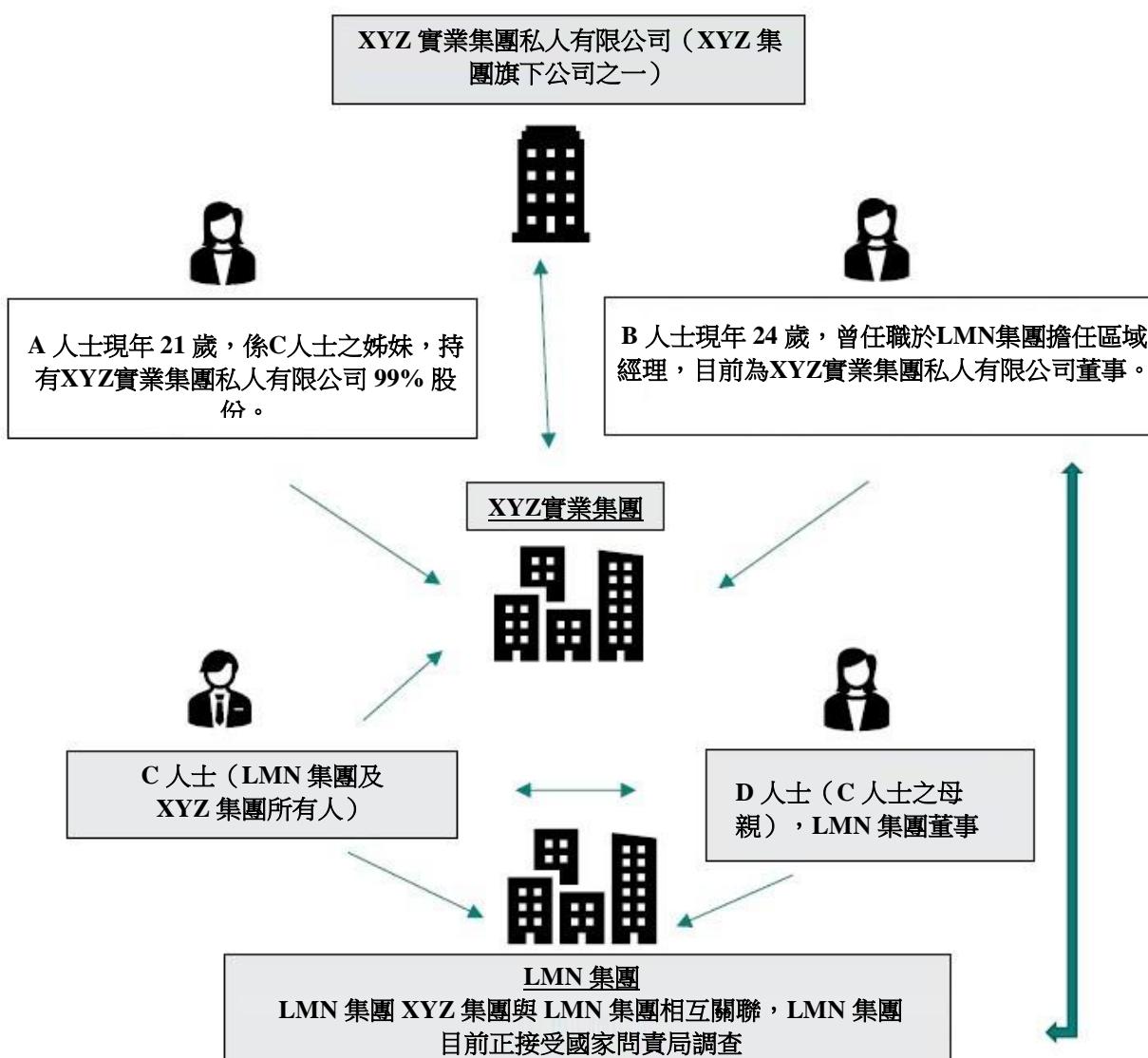
金融監理單位隨後向金融機構調取所有 XYZ 集團涉及可疑交易報告、及現金交易報告之帳戶資訊，發現帳戶於短時間內出現異常高額交易。FMU 發現四個銀行帳戶合計貸方交易總額超過 260 億盧比（約 9,300 萬美元）。XYZ 集團於 2022 年 12 月至 2023 年 2 月期間開設上述銀行帳戶。

金融監理單位發現四個銀行帳戶合計貸方交易總額超過 260 億盧比（約 9,300 萬美元）。XYZ 集團於 2022 年 12 月至 2023 年 2 月期間開設上述銀行帳戶。

金融監理單位另發現於公司登記機構的資料庫內，以 A 人士 CNIC 號碼註冊公司共有 15 家；以 B 人士 CNIC 號碼註冊公司則有 12 家。

A 人士及 B 人士皆非所得稅申報登記者。金融監理單位已向以下指定機構提供金融情資：

- 監管機關 - 巴基斯坦證券交易委員會（SECP），以採取監管措施；
- 三個執法機關，以進行實地調查（事實查證），偵辦涉及廣泛詐欺公眾及逃漏稅之行為。

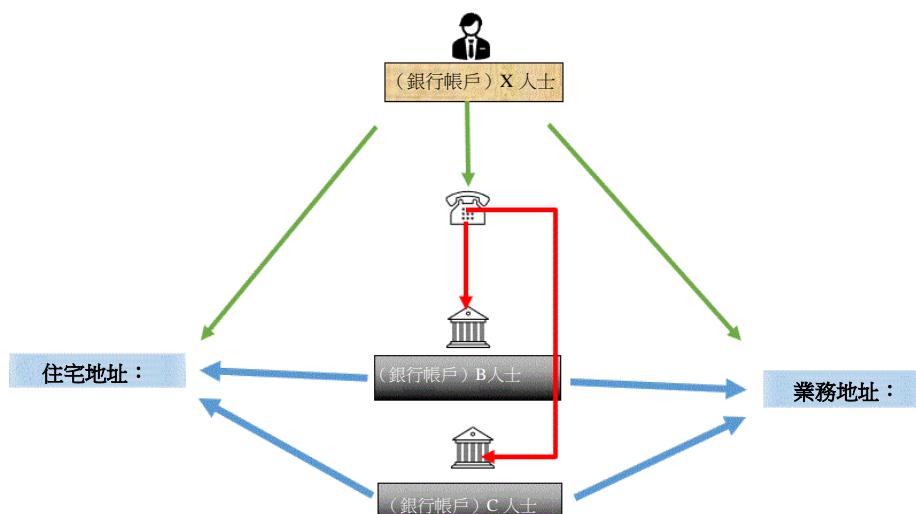


來源 - 巴基斯坦

案例研究 # 59：最終實質受益權影響之逃漏稅行為

逃漏稅；實質受益權

金融監理單位自申報義務機構收到可疑交易報告（STR）。此報告指出，一名客戶（化妝品業務）之高額交易與其商業概況明顯不符，該業務所有人为 X 人士。X 人士看似僅為一個企業的獨資經營者，但其聯絡電話亦被用於 B 人士及 C 人士之銀行帳戶資訊中。此外，申報義務機構亦發現 X 人士、B 人士及 C 人士各自銀行帳戶資料中的住宅地址及商業地址皆完全相同。基於申報義務機構比對不同資料庫後，發現有效聯絡電話、住宅地址及商業地址，X 人士極可能為其他多個帳戶之受益所有人。X 人士透過其申報帳戶及相關聯帳戶轉移超過 6 億 8389 萬盧比（約 245 萬美元）。另外，歷年稅務紀錄顯示，X 人士未曾繳納任何稅款。金融監理單位已將相關金融情資通報予相關執法機關，以就 X 人士業務及銀行帳戶之最終實質受益權，以及其涉及逃漏稅情事進一步調查。



來源 - 巴基斯坦

案例研究 # 60：以果乾業務掩護之非法金錢或價值移轉服務（MVTS）

哈瓦拉（Hawala）；逃漏稅；實質受益權

多家銀行向巴基斯坦金融監理單位（FMU）提交多筆與 A 人士有關之可疑交易報告。A 人士為 B 市居民，經營一家獨資企業，從事果乾與一般食品業務。銀行對 A 人士與遠距離、不相關的交易相對人之帳戶交易產生懷疑。經分析各銀行之帳戶開戶文件發現，A 人士於國民身分證上的簽名清晰且適當，但其在開設銀行帳戶時則使用不成熟且易於複製之簽名，因此銀行對該等帳戶的實質受益權有所懷疑。金融監理單位分析財務帳戶資料後，發現 A 人士之帳戶交易總額達 34.8 億盧比（約 1,200 萬美元），且與其業務概況不符，交易對象相對人與其業務概況亦不一致。此外，A 人士之交易相對人位於遙遠地區，且帳戶資金經常存入後經常立即被提領，金融監理單位認為此交易模式普遍見於地下匯兌（hawala/hundi）業務。再者，A 人士歷年所得稅紀錄顯示其繳納稅款極少，與其銀行帳戶往來之巨額資金流量明顯不相稱。

基於以上發現金融監理單位將相關金融情資通報執法機關，針對 A 人士涉嫌逃漏稅、地下匯兌罪及潛在資恐活動展開調查。

來源 - 巴基斯坦

案例研究 # 61：透過開立多個帳戶方式洗錢、貿易洗錢及逃漏稅

哈瓦拉（Hawala）；逃漏稅；貿易洗錢

海關機關懷疑家族企業 A 公司透過高報價方式，利用境外 B 公司進口太陽能板以挪用資金（siphoning off funds）。海關機關針對 A 公司進口太陽能板的發票進行稽核，發現該進口業務並非公司實際經營範圍，並

確認 A 公司透過此種高報價格方式挪用 47.8 億盧比（約 17,169,485 美元）資金。2022 年期間，A 公司自位於不同司法管轄區的不相關交易相對人收取 2,200 萬盧比（約 78,973 美元）資金，引發權責機關懷疑該資金係挪用資金的一部分。此外，A 公司與多個不相關交易對手進行多筆交易。財務分析顯示，A 公司及其董事共開立 216 個公司及個人帳戶，透過這些帳戶將公司資金轉移至個人及獨資企業帳戶。所有帳戶之總交易額高達 770 億盧比（約 2.76 億美元），與公司業務概況不符。進一步分析 A 公司及其董事之所得稅繳納紀錄顯示，在相關財務活動期間僅繳納微量稅款。金融監理單位已將相關金融情資提供給執法機關，針對 A 公司高報價格及逃漏稅行為展開調查。目前該案正由執法機關持續調查中。

來源 - 巴基斯坦

案例研究 # 62：透過提供誘人投資回報之詐欺案

[透過社群媒體之詐欺；不動產](#)

2022 年，A 公司向巴基斯坦證券交易委員會（SECP）正式登記，聲稱其業務範圍為不動產相關活動。然而，與其所聲稱之業務範圍相反，公司三名董事透過網站及社群媒體帳號，向大眾非法募集投資及存款，承諾提供每年高達 60% 的固定高額回報。其等虛假聲稱所募得資金將投資於不動產、媒體、資訊科技與礦泉水等多個領域，而利潤將分配給投資者。經分析公司及其董事之帳戶發現，多名個人透過網路現金存款及網路轉帳向該公司帳戶匯入資金，明顯為向大眾集資。後續該公司帳戶被提領現金共計 600 萬盧比（約 21,572 美元），並被轉帳 30 萬盧比（約 1,079 美元）至兩名董事個人帳戶（兩項合計約 22,600 美元）。金融監理單位（FMU）在發現此類異常情形後，將金融情資通報執法機關及監管機構。最終巴基斯坦證券交易委員會（SECP）對該公司及其董事裁罰 30 萬盧比（約 1,079 美元），並撤銷相關董事之任職資格。

來源 - 巴基斯坦

案例研究 # 63：透過代名人帳戶逃漏稅

[走私；可疑實質受益權；哈瓦拉（Hawala）；貿易洗錢](#)

A 人士於位在巴基斯坦之家族企業 A 公司擔任董事職務，該公司主要從事液化石油氣（LPG）分銷業務。該公司曾尋求銀行協助透過陸路運輸自 X 司法管轄區進口液化石油氣，但因該司法管轄區被列入防制洗錢金融行動工作組織（FATF）「加強監控司法管轄區」（高風險司法管轄區名單），銀行拒絕其申請。

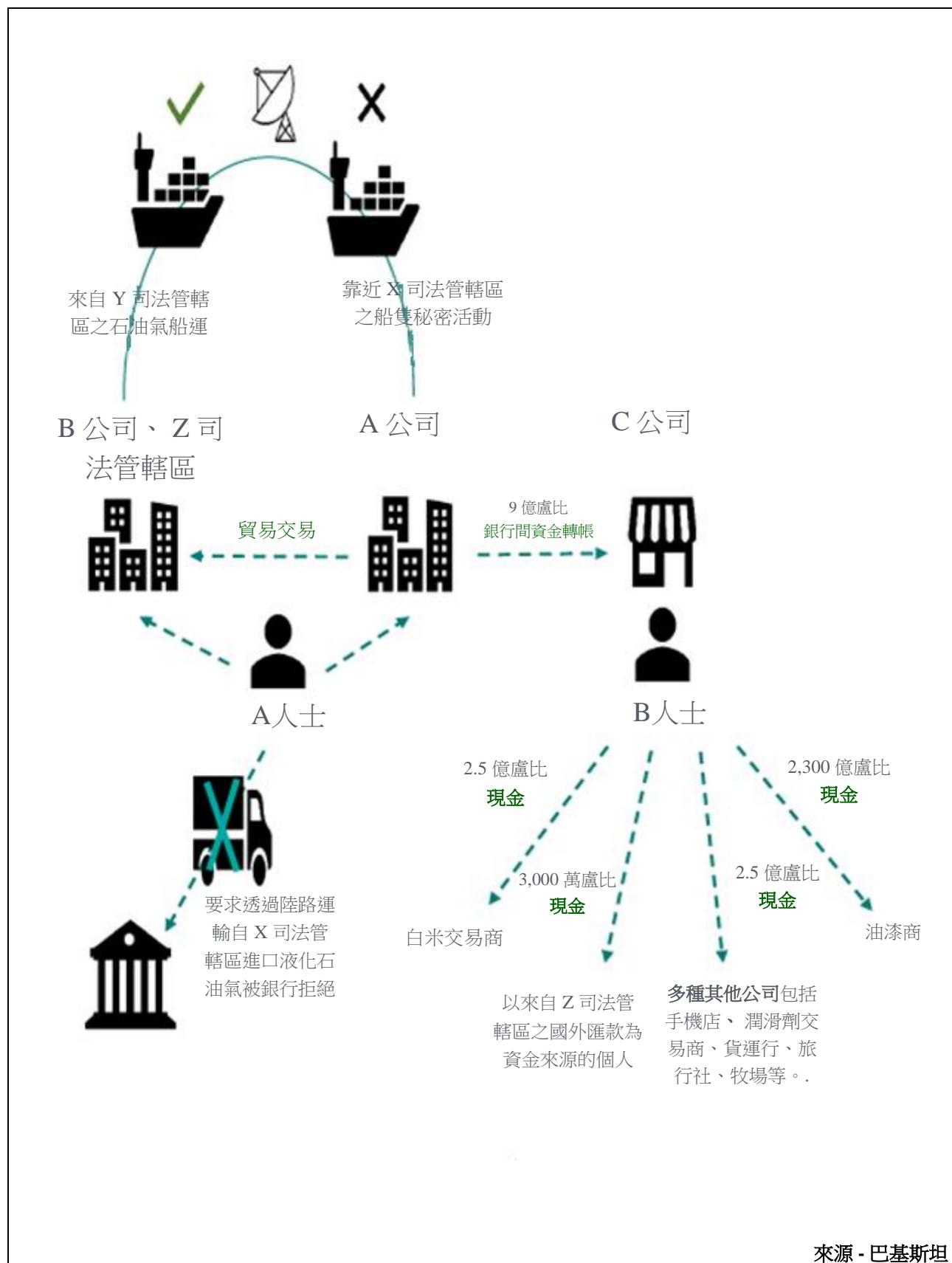
隨後，A 人士透過位於 Z 司法管轄區的 B 公司，自 Y 司法管轄區進口液化石油氣，A 人士同時為 B 公司董事。值得注意的是，A 公司與 B 公司皆為家族所有企業。

A 公司在不同銀行帳戶之業務往來累計貸方交易總額超過 1,000 億盧比（約 3 億 5,900 萬美元），大量涉及進口相關交易。

此外，A 公司將總計 9 億盧比（約 3,231,837 美元）資金轉移至位於巴基斯坦從事果乾業務之 C 公司（獨資企業）。該獨資企業之所有人为一名年輕個人（B 人士），該個人之身分證明文件與銀行文件簽名明顯不符，並以簽名補償書（銀行要求的簽名差異聲明文件）處理，導致對 C 公司之實質受益權產生疑慮，且 B 人士過去並無明顯金融活動記錄。該帳戶交易總額逾 10 億盧比，其中於一年內自 A 公司轉入已高達 9 億盧比（約 3,231,837 美元）。

由液化石油氣供應商轉資金給果乾商，此交易明顯缺乏經濟合理性。此外，C 公司亦向各類不相關實體，例如油漆商、手機商店、旅行社及稻米商支付資金，尤其是居住於 Z 司法管轄區且依賴海外匯款方之家庭成員。

基於上述調查結果，金融監理單位已將相關金融情資通報執法機關，懷疑 A 人士及 B 人士涉及走私與地下匯兌／匯票交易及貿易洗錢（TBML）活動。



案例研究 # 64：透過代名人帳戶逃漏稅**逃漏稅；可疑實質受益權；資金混合**

多家銀行提交數筆關於 A 人士的可疑交易報告（STR）。A 人士據稱作為某家族企業的人頭（front man），該家族企業由三兄弟經營管理。A 人士在該家族企業擔任會計，於 2016 年至 2019 年間在不同銀行開立共計 11 個個人及企業銀行帳戶。該會計將其雇主指定為帳戶繼承人（next of kin），並在三年間透過這些帳戶轉移約 60 億盧比（約 21,567,837 美元）。這些帳戶的整體金融活動達到 77 億 3,000 萬盧比（約 27,964,473 美元），顯著超出 A 人士之文件記錄上的資產概況及收入。此外，其家族成員經營多家公司，並共同開立 94 個額外的銀行帳戶，包括企業帳戶及個人帳戶。同期間稅務紀錄顯示，當這些可疑帳戶活動發生時，A 人士及其家族成員（其雇主）所繳納之所得稅極低。金融監理單位已將其金融情資移送執法機關調查涉嫌逃漏稅行為，並追查透過 A 人士多個帳戶流動之資金最終受益人身分。目前該案件仍由執法機關進一步調查中。

來源 - 巴基斯坦

2.12 菲律賓

案例研究 # 65：透過空殼公司進行稅務詐欺/ 逃漏稅**逃漏稅**

執法機關調查揭露一種名為「出售進項稅額憑證」（Input VAT Receipt for Sale）的詐欺手法。某有組織犯罪集團透過一間詐欺公司及數家幽靈或掛名公司，向大型納稅人（通常為公司，稱為「客戶」）出售虛假收據與發票，以規避向政府繳納應付稅款。據稱該非法活動已持續超過 15 年。

客戶向詐欺公司支付虛假收據及發票總金額約 0.4% 至 1.25% 的費用，以獲取虛假收據與發票。該等費用以支票支付，或由同一名信差或送貨員以現金收取，並將取得之收據或發票交付客戶；或透過詐欺公司提供的銀行帳戶以存款方式支付。客戶隨後利用這些虛假收據或發票，申報進項增值稅抵扣，或藉由虛增費用以減少所得稅。此案件由執法機關及菲律賓稅務權責機關持續調查中，部分案件已向司法部及法院提出訴訟。

來源 - 菲律賓

案例研究 # 66：宗教組織內之兒童性虐待**性剝削，包括兒童性剝削**

Z 人士為宗教組織 X 集團之負責人。⁷⁷ 申報義務機構注意到 Z 人士帳戶出現異常且可疑交易，包括大量且金額鉅大的現金交易，並與數家非 X 集團所屬產業之公司有交易往來。隨後，Z 人士因涉及詐欺案件而多次出現在負面新聞報導中，亦遭外國司法管轄區檢察機關以性販售活動提出起訴，並遭外國政府機關制裁，理由為其長達十餘年嚴重侵犯人權，包括系統性、且廣泛地對最小年齡 11 歲之女童施以性侵害及其他身體虐待行為。

據報導，Z 人士名下之美元及比索帳戶有大量無合理經濟目的之支票存款與資金轉帳，其個人帳戶內之貸方交易包括多筆現金存款，金額自 4,000 比索至 4,200 萬比索（約 70 美元至 73 萬美元）不等；及多筆資金轉帳，金額介於 1,000 比索至 1,650 萬比索（約 18 美元至 751,490 美元）之間。借方交易則包括金額介於 2,690 萬比索至 4,700 萬比索（約 481,488 美元至 841,102 美元）之對外匯款及資金轉出；另亦發現數筆現金提領，金額自 47 萬比索至 1,300 萬比索（約 8,408 美元至 232,598 美元）不等，以及開立支票，金額自 2,000 比索至 500 萬比索（約 36 美元至 89,440 美元）不等，據稱用途為電子稅款及帳單支付、營運支出、員工薪酬及

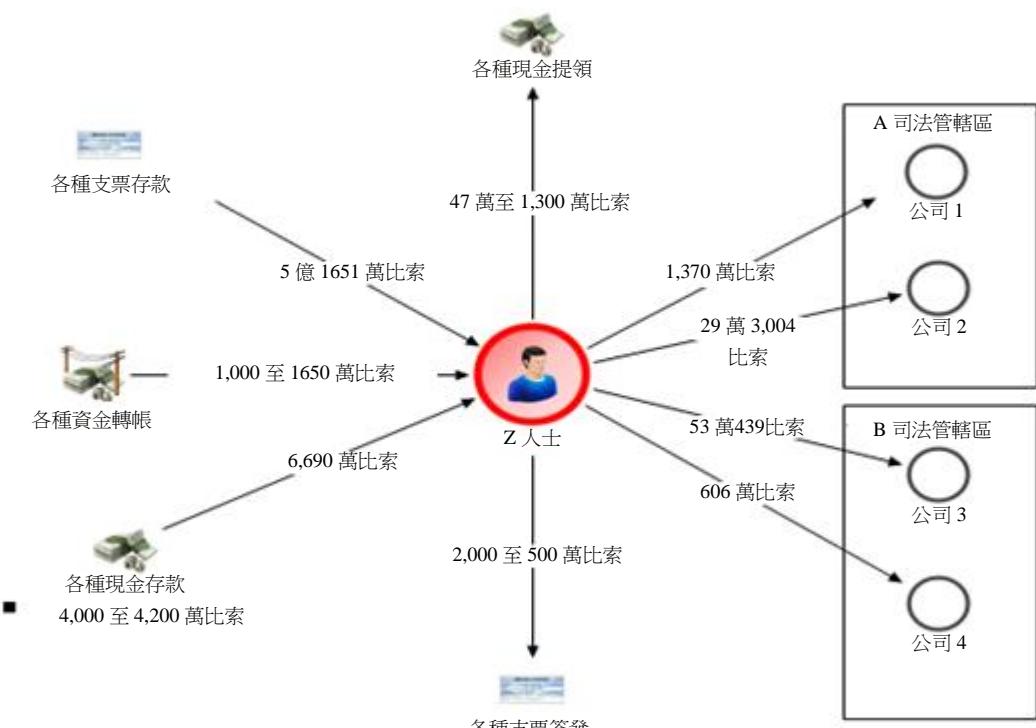
⁷⁷ 菲律賓防制洗錢委員會（Anti-Money Laundering Council）－《菲律賓兒童線上性虐待與性剝削：運用可疑交易報告（STR）資料之評估》（*Online Sexual Abuse and Exploitation of Children in the Philippines. An Evaluation Using STR Data*）：

<http://www.amlc.gov.ph/images/PDFs/Main/Online%20Sexual%20Abuse%20and%20Exploitation%20of%20Children%20in%20the%20Philippines.pdf>

持續進行中之 X 集團建設工程材料。此外，Z 人士另有四筆汽車貸款帳戶，分別於 2022 年、2024 年及 2025 年到期。Z 人士之帳戶已被義務機構納入內部監控名單，且待外國司法管轄區之訴訟有進一步進展後，可能建議予以關閉。

此外，據稱曾擔任外國司法管轄區教會管理層、負責收集全球教會營運財務資料之 Y 人士，亦涉入與 X 集團相關之可疑交易。據報，Y 人士於外國司法管轄區的負面媒體報導中，被指控參與一個高度危險且規模龐大的犯罪組織，涉及兒童性剝削、人口販賣、大額現金走私、洗錢、強迫勞動及移民詐欺等犯罪行為。外國司法管轄區已對 Z 人士與 Y 人士發出逮捕令，Y 人士之帳戶亦受申報義務機構嚴密監控，一旦遭起訴並判決有罪，將予以關閉。

圖 1. Z 人士不正常交易



來源 - 菲律賓

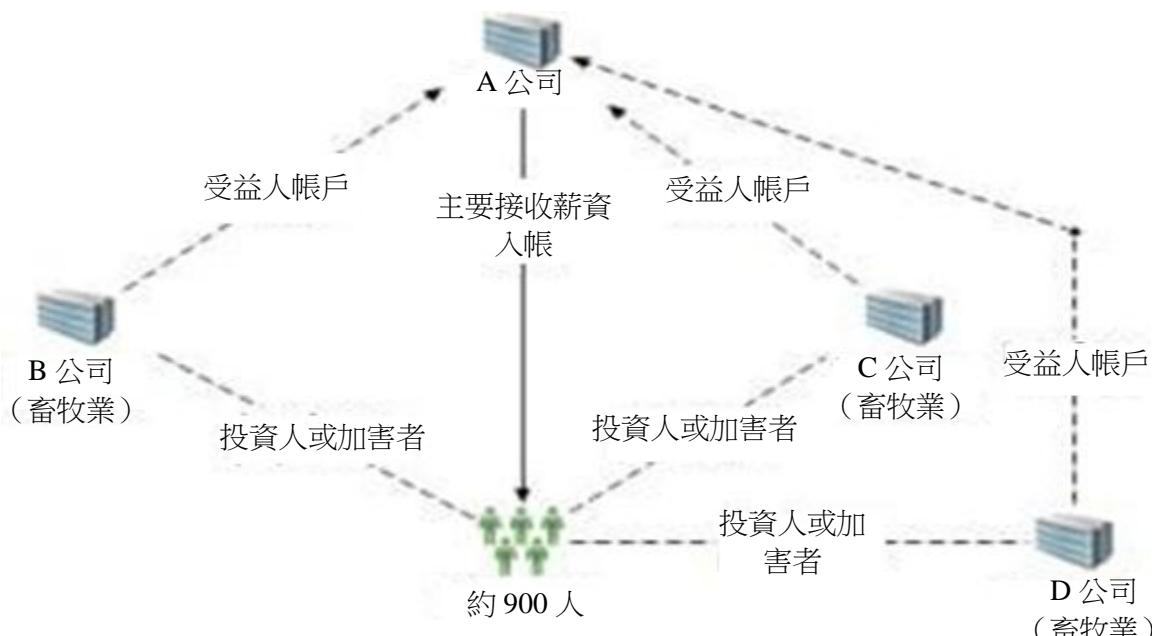
案例研究 # 67：未經授權之投資吸金公司

詐欺；投資詐騙；逃漏稅

約有 900 名個人涉及大量可疑交易，金額估計達 2 億 2,600 萬比索（約合 390 萬美元），相關人士疑似涉入未經授權且具詐欺性質的投資計畫⁷⁸。該計畫據稱涉及投資三家公司：A 公司、B 公司與 C 公司，以畜牧產品為投資標的，承諾在兩個月內提供 100% 的投資回報。近 900 名涉案人士之多數人係透過薪資轉帳方式自一家旅遊公司收到款項，據稱該旅遊公司帳戶係作為上述三家公司吸收投資款項之受益人帳戶。菲律賓證券交易委員會（SEC）於 2019 年發布公告，針對上述三家公司提出警告，提醒大眾停止對其進行投資。證券交易委員會進一步警告，涉案人士將被通報至稅務權責機關，以評估相應的罰款並課徵稅款。相關資訊已經提供予相關利害關係人，包括執法機關，以供進一步調查。

⁷⁸ 菲律賓防制洗錢委員會 - 《與稅務犯罪可能相關之疑似洗錢或資恐交易報告分析》（An Analysis of Suspicious Transaction Reports with Possible Links to Tax Crimes）：
<http://www.amlc.gov.ph/images/PDFs/2021%20ANALYSIS%20OF%20STRS%20WITH%20POSSIBLE%20LINKS%20TO%20TAX%20CRIMES.pdf>

圖 2.涉及法人之詐欺投資計畫



來源 - 菲律賓

案例研究 # 68：涉入犯罪集團之賭場中介公司

詐欺；投資詐騙

X 賭場通報數名個人係 ABC 犯罪集團成員⁷⁹。其中，已確認的 D 人士涉及多種業務，如建築業、化妝品分銷、及放款業務。此外，D 人士也是一家涉嫌經營龐氏騙局的公司高層，亦曾捲入有關賭場中介公司（junkets）運作的負面新聞報導。D 人士在國內某銀行擁有個人及公司帳戶，因警示交易問題未獲解決而遭關閉。此外，D 人士在國內另一家銀行開立支票，金額高達 1,050 萬比索（約合 187,830 美元），經查證為空頭支票。鑑於情況特殊，該筆空頭支票詐欺事件需提報可疑交易報告（STR），相關帳戶已被關閉。

與此相關的是，Y 賭場收到主管賭場之政府機關函文，指出 ABC 集團涉嫌投資詐騙，函文中指出，該集團由 D 人士主導，而 D 人士亦為 Y 賭場獎勵計畫之會員。D 人士涉嫌誘騙投資人簽訂貸款合約，以發放遠高於常理的回報或利息為誘餌，並開立未到期支票，最終因存款不足而跳票。ABC 犯罪集團聲稱其與私人賭場有仲介合作協議，資金用途係支付國際賭客之博奕活動。為營造合法組織之表象，ABC 犯罪集團冒用多家合法企業之名稱。相關資訊已通報給各利害關係人，包括執法機關，以供進一步調查。

來源 - 菲律賓

⁷⁹ 菲律賓防制洗錢委員會 - 《與賭場中介公司可能相關之可疑交易報告分析》（Analysis of Suspicious Transactions Associated with Casino Junkets）：
http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATED%20WITH%20CASINO%20JUNKETS_FINAL.pdf

2.13 新加坡

案例研究 # 69：公司依據《貪污、販毒及其他嚴重罪行（沒入利益）法》遭起訴

使用法人及法律協議

2022 年 9 月 29 日，A 公司依據 1992 年《貪污販毒及其他重大犯罪（沒入利益）法》（CDSA）相關罪名被法院起訴。依據 CDSA 第 47(3) 條，取得明知為他人犯罪所得之財產，A 公司被控 42 項罪名。於 2014 年至 2018 年 1 月間，A 公司透過旗下船隻接收總值 5,600 萬美元之船用柴油，而該等柴油乃不法侵占一家新加坡煉油設施所得。依據現行法律，A 公司每項罪名一旦成立，將面臨最高罰款 100 萬新加坡元（約 779,281 美元），或犯罪涉及財產價值的兩倍金額，以較高者為準。

該公司前任董事總經理亦因涉嫌同意接收侵佔之船用柴油，已另案遭法院起訴，該案亦仍在審理中。

A 公司主要營運海運業務，其取得被侵佔船用柴油之行為純係商業利益驅使，目前法院對 A 公司之訴訟仍在進行中。

來源 - 新加坡

案例研究 # 70：組織犯罪集團成員遭起訴

組織犯罪集團與敲詐；自我洗錢

2023 年 5 月與 10 月，總計 16 名個人因涉嫌參與非法遠端賭博活動之組織犯罪集團遭起訴。該等人士為警方在針對犯罪集團之行動中逮捕的 37 人之一。警方調查期間，扣押總值 453 萬新加坡元（約 353 萬美元）之現金與資產。

嫌疑人等人依據 2014 年《遠端賭博法》（*Remote Gambling Act, RGA*）及 2015 年《組織犯罪法》（*Organised Crime Act, OCA*）被起訴；其中三名男子與一名女子因以洗錢方式處理自身犯罪所得，另被依據《貪污、販毒及其他重大犯罪（沒入利益）法令》（CDSA）額外起訴。A 人士將犯罪所得隱匿於他人銀行帳戶，並以犯罪所得部分支付機車款項；B 人士將犯罪所得轉為其公司之貸款；C 人士則教唆 D 人士以犯罪所得支付其車輛分期付款。法院審理目前仍在進行中。

來源 - 新加坡

案例研究 # 71：12 名男子因涉及近期銀行相關惡意軟體案件遭起訴

涉及惡意軟體之詐欺；自我洗錢；第三方洗錢

2023 年 6 月至 8 月，新加坡發生一系列銀行相關惡意軟體案件，受害人銀行帳戶出現未經授權交易，且受害人並未向任何人洩露一次性密碼（OTP）。警方經廣泛調查，鎖定 12 名嫌疑人，於 2023 年 9 月展開全國性行動並予以逮捕。行動期間查扣現金超過 13,000 新加坡元（約 10,135 美元）、兩台筆記型電腦、32 張金融卡、23 台行動設備、毒品吸食工具及一把刀具。此外，當局凍結 60 個銀行帳戶，以防止進一步被遭濫用。

目前已有 9 人遭法院起訴，另有 3 人仍在調查中。涉及之罪名包括協助他人保有犯罪所得利益、持有及使用管制藥品、持有毒品施用器具、非法持有攻擊性武器、未經授權而存取電腦資料，以及參與非法社團及本地有關聯之組織犯罪集團等多項罪名。目前法院仍在審理上述 9 名被告相關案件。

來源 - 新加坡

案例研究 #72：以洗錢方式處理毒品犯罪所得**毒品相關犯罪**

2023 年 11 月 30 日，權責機關依據 1973 年《濫用毒品法》（*Misuse of Drugs Act, MDA*）逮捕 A 人士，罪名為販賣管制藥品。調查期間，權責機關凍結其銀行帳戶，帳戶餘額合計為 1,324.20 新加坡元（約 1,032 美元）。在金融調查中，A 人士表示只有 700 新加坡元（約 546 美元）為毒品交易犯罪所得。

2024 年 3 月 14 日，該名人士因涉及毒品前置犯罪及毒品洗錢罪名，被法院判處有期徒刑 5 年 8 個月 3 週，另處鞭刑 5 下。此外，檢方已向法院聲請沒入 700 新加坡元（約 546 美元）歸國庫所有，目前該沒入程序尚待法院裁定。

來源 - 新加坡

案例研究 #73：以洗錢方式處理毒品犯罪所得**毒品相關犯罪**

2022 年 5 月 5 日，執法機關依據 1973 年《濫用毒品法》（MDA）逮捕 A 人士，罪名為販運管制藥物。逮捕行動中，當局扣押 19,717.60 新加坡元（約 15,372 美元）現金及若干珠寶。調查期間，當局亦凍結其銀行帳戶，帳戶餘額為 358.03 新加坡元（約 279 美元）。在金融調查中，A 人士表示只有 1,100 新加坡元（約 858 美元）為毒品交易犯罪所得。

2023 年 9 月 26 日，A 人士因毒品前置犯罪及毒品洗錢罪，被判處 30 年有期徒刑。該 1,100 新加坡元（約 858 美元）已依法沒入歸國庫所有。

來源 - 新加坡

案例研究 #74：法人遭判決有罪**詐欺；第三方洗錢；使用法人及法律協議；境外前置犯罪；可疑交易通報**

新加坡可疑交易報告辦公室（STRO）收到涉及 X 公司之可疑交易資訊，該公司銀行帳戶因詐欺原因被提出多次資金撤回請求。STRO 分析後將金融情資提交新加坡警察部隊商業事務局（CAD），並展開對 X 公司及其唯一董事兼股東 Y 人士的調查。

調查顯示，位於 A、B 及 C 司法管轄區的四名投資詐欺與愛情詐騙案受害者被誘騙向 X 公司持有的兩個銀行帳戶匯入總額超過 11 萬新加坡元（約 85,759 美元）資金。儘管已收到資金撤回通知，Y 人士仍繼續使用這兩個帳戶收款，且未能提供一致且可信之解釋。Y 人士甚至試圖撤銷 X 公司登記，但遭權責機關拒絕。X 公司及 Y 人士隨後被控洗錢罪。2023 年 9 月，Y 人士最終被判有罪，處六個月徒刑；X 公司亦於 2023 年 9 月被判有罪，處罰金合計 3 萬新加坡元（約 23,389 美元）。

來源 - 新加坡

案例研究 #75：多案在身且拒不配合的洗錢人頭不守規章的車手??**詐欺；第三方洗錢；金融機構；匯款服務；可疑交易通報**

2021 年 2 月至 7 月期間，A 人士誘騙一名境外愛情詐騙案受害者，將約 7 萬 4,000 新加坡元（約 57,694 美元）轉入 A 人士自身銀行帳戶。新加坡警察部隊商業事務局調查發現，A 人士亦為人頭帳戶持有人其實是一名車手（money mule），曾協助身分不明之 B 人士接收詐騙所得資金。

調查亦顯示，2021 年 2 月另一起案件中，B 人士要求 A 人士協助接收來自身分不明之 C 人士的資金。C 人士聲稱想在 X 司法管轄區購買房地產，但不願將資金直接匯至 X 司法管轄區。A 人士對 B 人士的要求起疑，並要求提供房產相關證明文件，但 B 人士無法提供任何文件。儘管如此，A 人士仍繼續協助收受資金並將其匯往 X 司法管轄區的銀行帳戶。其中部分資金係透過新加坡一間有執照的貨幣兌換商匯往 X 司法管轄區。

A 人士於 2023 年 12 月被法院裁定違反《貪污、販毒及其他重大犯罪（沒入利益）法令》（CDSA），判處 7 個月有期徒刑。該新加坡法有執照的貨幣兌換商亦因明知資金有犯罪所得之合理嫌疑，卻未提交可疑交易報告（STR），被控違反 CDSA 相關規定，目前該案仍於法院審理中。依據 2002 年《犯罪所得法》（聯邦）的沒入程序仍在進行中。

來源 - 新加坡

案例研究 # 76：協助設立空殼公司以處理犯罪收益

詐欺；第三方洗錢；使用法人及法律協議

A 人士依據不明第三方的指示，設立 X 公司並為該公司開設企業銀行帳戶。約 150 萬美元被存入 X 公司銀行帳戶內，該筆資金係某外國司法管轄區一間銀行遭詐騙的 400 萬美元犯罪所得之一部分。

調查期間，身為 X 公司董事的 A 人士無法合理解釋 X 公司銀行帳戶內為何持有疑似犯罪收益的資金。由於 A 人士允許他人使用 X 公司銀行帳戶，且未善盡董事應有的合理謹慎義務。因此，於 2023 年 12 月，A 人士被控違反 1967 年《公司法》（Companies Act 1967）、CDSA 以及 1993 年《濫用電腦法》（Computer Misuse Act 1993）。目前該案仍在法院審理中。作為獨立法人之 X 公司，於 2024 年 3 月依據《貪污、販毒及其他重大犯罪（沒入利益）法》（CDSA）第 55 條規定，經法院判決洗錢罪名成立，處以罰鍰 5 萬新加坡元（約 38,980 美元）。

來源 - 新加坡

案例研究 # 77：逃漏稅洗錢

稅務犯罪；逃漏稅洗錢；金錢或價值移轉服務(MVTS)

新加坡警察部隊商業事務局（CAD）與新加坡稅務機關聯合調查一宗稅務詐欺案件，發現某唯一董事（sole director）利用兩家空殼公司，製造多筆虛假發票，以詐欺方式向稅務機關申報不實的商品及服務稅（GST）退稅請求，導致稅務機關錯誤向該兩家公司支付退稅款項。商業事務局後續進行之洗錢調查發現，該董事於犯罪期間居住於 C 司法管轄區，且無其他已知收入來源。2015 年 1 月 1 日至 2020 年 1 月 31 日期間，該兩家空殼公司的銀行帳戶每季固定收到詐欺性 GST 退稅款項。每季結束時，該董事回返回新加坡，並透過跨境匯款服務業者將詐欺所得之 GST 退稅款項匯至其本人及配偶於 C 司法管轄區之銀行帳戶。該董事亦將部分 GST 退稅所得資金存入新加坡中央公積金（Central Provident Fund, CPF）帳戶（新加坡強制性社會保障儲蓄計劃），並以其中一家空殼公司的名義存入，以製造空殼公司有真實商業營運之假象。透過此種方式，該唯一董事將逃漏之 GST 稅款從新加坡轉移出去，此行為構成洗錢罪。

2023 年 12 月，依據 1993 年《商品及服務稅法》（Goods and Services Tax Act 1993）第 62(1)(b) 條及第 62(1)(c) 條，該董事因涉及詐領 GST 退稅共計 660,114.97 新加坡元（約 514,630 美元），共 16 項罪名成立。該董事遭判刑共計 84 週有期徒刑，並須繳納罰款 1,980,344.91 新加坡元（約 1,543,853 美元），此罰款為逃漏 GST 稅額三倍。另有 33 項逃漏商品及服務稅（GST）之罪名，於量刑時一併納入考量。

此外，2023 年 12 月，該董事因透過將詐欺性 GST 退稅款項轉移海外及存入新加坡中央公積金（CPF）帳戶，共計 523,459.90 新加坡元（約 408,045 美元）涉及四項洗錢罪名成立，判處 15 個月有期徒刑。另有六項洗錢罪名納入量刑考量。

來源 - 新加坡

案例研究 # 78：成功逮捕涉嫌跨司法管轄區走私金條之嫌疑人**走私；貿易洗錢；貴金屬及寶石交易；國際合作**

新加坡警察部隊商業事務局（CAD）針對來自 A 司司法管轄區之數名人士進行長期情報調查，包括金融情報分析，發現其中兩名嫌疑人 A 人士及 B 人士於 2014 年至 2017 年間，自新加坡某珠寶批發商購入至少 2 萬 8,000 條金條，總價值達 15 億新加坡元（約 11 億美元）。其等涉嫌將該批金條藏匿於出口機械工具中，走私至包括 A 司司法管轄區及 C 司司法管轄區之海外目的地。新加坡定期召開與 A、C 司司法管轄區之執法機關虛擬案件討論會議，分享該集團之情報資訊，以利後續偵辦。

2023 年 12 月中旬，C 司司法管轄區海關扣押一批貨物，其中藏匿 15 條金條，該批貨物由涉嫌與 A 人士共謀之人士所寄送。同月的月底，A 人士在離境時遭新加坡警察部隊商業事務局逮捕，依據 1871 年《刑事法典》（Penal Code）第 417 條詐欺罪名遭起訴。截至目前，A 人士已另外被指控涉及 17,000 條 1 公斤重金條之案件，新增 4 項《刑事法典》第 417 條罪名。該案之調查與法院審理仍持續進行中。

來源 - 新加坡

案例研究 # 79：透過加密貨幣轉換手段轉移詐欺犯罪所得資金**詐欺；境外前置犯罪；第三方洗錢；使用虛擬資產**

新加坡警察部隊商業事務局（CAD）透過情報調查，發現一個由 A 人士協調之犯罪集團涉嫌透過轉換加密貨幣轉移超過 85 萬元新加坡元（約 662,598 美元）之詐騙所得。A 人士為 X 司司法管轄區之國民，協助身分不明之 B 人士進行以下活動：

- 尋找加密貨幣賣家；
- 購買來源不明人士之提款卡（ATM cards），用以接收 B 人士之資金，從而支付加密貨幣購買款項；
- 購買加密貨幣後，將其轉入 B 人士之加密貨幣錢包。

A 人士亦協助 B 人士在未經授權情形下存取新加坡某銀行帳戶，用以接收並轉移超過 50 萬新加坡元（約 389,764 美元）之詐騙犯罪所得。

2024 年 2 月，A 人士因多項違反《貪污、販毒及其他重大犯罪（沒入利益）法》（CDSA）及 1993 年《濫用電腦法》（Computer Misuse Act）遭定罪；判處有期徒刑四年六個月。此外，當局於調查期間自 A 人士處扣押 15,715 新加坡元現金（約 12,250 美元）。

來源 - 新加坡

2.14 中華臺北

案例研究 # 80：未上市股票詐騙**詐欺；現金；使用法人及法律協議**

某銀行向刑事警察局報案指出，該銀行櫃員發現 A 人士在多間分行提領大量現金，疑似為洗錢人頭帳戶持有者。經調查後，民眾亦陸續向警方報案，聲稱 O 公司假冒從事綠能產業，聲稱前景可期；許多被害人遭 O 公司詐欺性陳述誤導，購買其未上市股票。

2024 年初，調查本案之專案小組成立。經一個多月追蹤蒐證後，搜索 O 公司辦公室及 12 名相關人員住處，並逮捕相關嫌疑人（包括 A 人士），扣押電腦主機、筆記型電腦、行動電話、公司文件、公司大小章、股東私人印鑑、一疊公司宣傳文件、一疊股票憑證、一疊股利領取通知書存根聯、一疊股票過戶申請書、一疊納稅憑證、一疊公司合約，以及現金 32 萬餘臺幣（約合 1 萬美元）等證物。本案共有超過 1,300 人受害，涉案金額超過 4 億臺幣（約 1,250 萬美元）。

O 公司聲稱與多家上市公司及政府機關合作，從事熱裂解再生發電技術領域。然而，其等對外提供之資訊誇大不實，該公司實際上並無營運績效，且與無執照的證券業者合作，透過傳送簡訊及電話行銷向大眾推廣未上市股票。當被害人匯款購買這些未上市股票後，人頭帳戶集團（包括 A 人士）即前往銀行分行提領現金，再將現金交給無執照的證券商之首腦。

來源 – 中華臺北

案例研究 #81：公職人員涉嫌貪污案件

貪污與賄賂；現金；第三方洗錢

A 人士為 Y 縣議會議長，為隱匿收取賄款的事實，他要求廠商以沖刷保護工程（即在境外風力發電機基礎樁周圍堆置石塊，以防波浪侵襲的工程）為名，將資金匯入共犯 B 人士的公司帳戶。B 人士之後將款項提領現金並交付給 A 人士，藉此掩飾資金轉移及 A 人士收受賄賂之事實。A 人士共計收受犯罪所得約 25,404,899 臺幣（約 793,900 美元）。

來源 – 中華臺北

案例研究 #82：透過虛假交易掏空上市公司

詐欺；現金；使用支票；使用法人及法律協議

W 公司為主業從事營建工程之上市公司，由 A 人士擔任公司代表。自 2010 年起，A 人士與其配偶 B 人士透過 C 人士、D 人士及 E 人士名義設立 X、Y、Z 三間空殼公司，隨後利用這三家公司與 W 公司簽訂虛假工程銷售合約。事實上，這些工程實際上係由 W 公司人員或其他受委託公司所銷售，並無 X、Y、Z 公司之實際參與。隨後，X、Y、Z 公司偽造帳單文件，向 W 公司請款，導致 A 人士及 B 人士自 W 公司侵占 6 億臺幣（約 1,875 萬美元）。隨後，X、Y、Z 公司偽造帳單文件，向 W 公司請款，致使 A 人士及 B 人士得逞，自 W 公司侵占 6 億臺幣（約 1,875 萬美元）。

A 人士與 B 人士亦製作 X、Y、Z 公司的虛假會計文件，從這些公司帳戶提領現金，其中一部分存放於公司保險櫃內（後來由 B 人士取出供個人使用）。二人亦開立以 C 人士、D 人士及 E 人士為受款方的支票，存入這些個人帳戶後再全數提領此等資金。透過此方式，A 人士及 B 人士共以洗錢方式處理犯罪所得 395,183,223 臺幣（約 1,200 萬美元）。

2023 年 9 月，法務部調查局將 A 人士及 B 人士依涉嫌違反《商業會計法》、《防制洗錢法》、《證券交易法》及《刑法》罪嫌，移送檢察署偵辦。

來源 – 中華臺北

案例研究 #83：透過賄賂銀行員工進行洗錢

詐欺；賄賂；電匯；法人及法律協議使用

洗錢犯罪集團 A 透過仲介人取得人頭帳戶及空殼公司帳戶，其中法人帳戶價格高於個人帳戶。A 集團透過行賄銀行 X 之部分員工（包括 B 人士），以規避正當客戶身分盡職調查程序，申請多個人頭及空殼公司帳戶。此外，B 人士及其他涉案人員協助調整網路銀行轉帳限額，並為這些人頭及空殼公司帳戶設立指定之境外收款帳戶。B 人士及其他人根據所提供之不同收取相應費用，協助 A 集團轉移犯罪所得。A 集團從被害人取得詐欺資金後，透過多個帳戶進行資金多層化及轉移，最終將資金轉入指定之境外帳戶。A 集團共計取得及轉移犯罪所得 1 億 1,500 萬臺幣（約 350 萬美元）。

來源 – 中華臺北

案例研究 #84：殺豬盤詐騙案**虛擬資產服務提供商**

刑事警察局調查一宗國際殺豬盤詐騙案，發現嫌疑人自稱為伊拉克軍官、聯合國官員、或願意成為被害人妻子的網友⁸⁰，誘騙被害人進入虛假的戀愛關係後，將被害人帶往 J 公司（未完整填報防制洗錢合規聲明之虛擬資產服務提供商），以現金購買加密貨幣。J 公司與嫌疑人合作，以高於市場價格 10% 向被害人出售加密貨幣，隨後將加密貨幣轉入嫌疑人的海外錢包。

經蒐證後，刑事警察局於 2024 年初執行搜索，逮捕以主嫌犯 A 人士為首共 18 名嫌疑人，查扣現金 2,600 萬臺幣（約 81 萬 2,500 美元）、一輛保時捷汽車、23,912 枚泰達幣（Tether USDT）加密貨幣、一個保險箱、數部點鈔機、相關手機、電腦及文件等證物。

來源 – 中華臺北

案例研究 #85：政府官員收受賄賂**貪污與賄賂；現金**

A 人士為內政部某單位主管，負責督導若干專案之審查程序。於初審會議時，各地方政府及轄區之相關人員向 A 人士提案，由其挑選可提交內政部進行補助審批的計畫。B 人士為取得 A 人士核准及地方專案的大額補助款，透過立委辦公室執行長 C 人士向 A 人士行賄。

為掩飾賄款，A 人士要求以現金支付，並請 C 人士將現金存放於其辦公室內，以便 A 人士隨時取用。A 人士亦將部分現金藏於住家各處或茶葉罐內，並將部分資金拆分成小額存入本人及配偶、母親、兒子等人之銀行帳戶內。2017 年至 2023 年間，總計存入之現金超過 1,000 萬臺幣（約 31 萬 2,500 美元）。此外，A 人士以 B 人士名義購買一輛賓士轎車，並將部分資金存入由其友人 D 人士經營之 E 公司帳戶內。

2023 年 8 月，臺北地方法院檢察署依違反《貪污治罪條例》及《防制洗錢法》罪對 A 人士提起公訴。

來源 – 中華臺北

案例研究 #86：涉嫌洗錢**購置不動產**

Y 人士曾任地方警察局刑事偵查大隊偵查佐，D 人士則涉入有組織詐欺犯罪。Y 人士明知情況，仍協助 D 人士隱匿詐欺犯罪所得，以逃避司法機關之調查、起訴及處罰。Y 人士將 D 人士提供之犯罪所得現金存入其等本人名下之銀行帳戶，隨後以其等本人名義購置不動產，並支付房屋裝修費用。透過此方式，Y 人士在資金流動上製造斷點，共同隱匿 D 人士詐欺犯罪所得資金，總計 1,422 萬 700 臺幣（約 44 萬 4,400 美元）及其最終去向。

來源 – 中華臺北

案例研究 #87：A 人士、B 人士、C 人士涉嫌共同違反《貪污治罪條例》**貪污與賄賂；電匯**

A 人士、B 人士及 C 人士為某拘留所之警衛，涉嫌向收容人為掩飾賄款，收受賄賂。其等透過在 A 司法管轄區之 D 人士名義登記之手機號碼，聯絡收容人之親屬，要求將資金轉入 A 人士女兒，以及來自 B 司法管轄區之前收容人 E 人士之帳戶。A 人士、B 人士與 C 人士管理上述帳戶並持有存摺及相對應之私人印章，於 2020 年至 2023 年間將收受之犯罪所得存入此等帳戶。此外，A 人士、B 人士與 C 人士亦指示 A 人士的配偶及女兒不定期透過此等帳戶存取現金，藉此轉移或變更犯罪所得資金之流向。

透過上述手段，A 人士、B 人士與 C 人士共計隱匿、轉移及變更至少 810,100 臺幣（約 25,315 美元）之賄款及非法所得。中華臺北權責機關已成功將此案起訴。中華臺北權責機關已成功將此案提起公訴。

來源 – 中華臺北

⁸⁰ 透過網際網路認識的人

案例研究 # 88：侵占自非營利組織資金**自我洗錢；現金；電匯**

A 人士擔任 W 宮廟之主委，B 人士與 C 人士（均為 A 人士之親戚）分別擔任 W 宮廟的財務主管及總幹事。2019 年至 2020 年間，由於職務之便，A 人士、B 人士與 C 人士得以掌控 W 宮廟之存摺、印章與支票，且可自由存取宮廟資金。其等逐步將宮廟帳戶內的資金挪為個人用途，或轉移至三人經營之其他公司，包括透過現金存款或銀行轉帳方式在 W 宮廟與其他公司間轉移。

最終，他們將上述資金用以替 B 人士購買個人壽險、投資基金、美元存款，以及替 C 人士購置一輛豪華汽車。他們共計自 W 宮廟侵占 4,520 萬臺幣（約 141 萬美元）。此外，2016 年至 2022 年間，A 人士、B 人士與 C 人士亦偽造財務報表逃漏稅款，金額達 1,085 萬臺幣（約 33 萬 9,000 美元）。2023 年 11 月，A 人士、B 人士及 C 人士以違反《刑法》及《稅捐稽徵法》罪被提起公訴。

來源 – 中華臺北

案例研究 # 89：投資詐欺**詐欺；電匯**

A 人士、B 人士與 C 人士提供自身之銀行帳戶存摺、提款卡、提款卡密碼、及網路銀行帳戶密碼予身分不明之犯罪集團成員使用。2022 年 5 月起，該犯罪集團成員向被害人發送投資廣告連結，誘使被害人加入 LINE 投資群組。犯罪集團成員謊稱投資人加入「Z 應用程式」後可自行決定投資金額，由 Z 公司匯集投資資金，隨後透過「Z 應用程式」集體購買股票；並聲稱投資後股票將依投資金額分配至投資者之「Z 應用程式」帳戶，投資者亦可透過「Z 應用程式」參與股票增資或購買未上市股票。

如獲利，則投資人須另支付投資金額 20% 作為分潤，此誘使被害人誤信並匯款至 A 人士、B 人士與 C 人士的帳戶，總金額達 127 萬臺幣（約 39,688 美元）。該犯罪集團從未將被害人的資金投資於股票。A 人士、B 人士與 C 人士已依據《刑法》（詐欺罪）及《防制洗錢法》被提起公訴，目前案件正在審理中。

來源 – 中華臺北

案例研究 # 90：來自 A 司法官轄區之毒品販運案**毒品相關犯罪**

2021 年 1 月起，A 人士及其犯罪集團開始自 A 司法官轄區寄送包含愷他命（Ketamine）的包裹至 B 司法官轄區出售。為掩飾犯罪所得來源，A 人士使用其母親之銀行帳戶將 163 萬臺幣（約 50,937 美元）犯罪所得存入該帳戶後再轉出。A 人士因違反《毒品危害防制條例》及《防制洗錢法》罪名遭到起訴，目前案件審理中。

來源 – 中華臺北

案例研究 # 91：販運來自 B 司法官轄區之毒品**毒品相關犯罪**

自 2023 年 3 月起，A 人士及其犯罪集團開始從 A 司法官轄區寄送含有大麻之包裹至 B 司法官轄區販售。A 人士指示集團成員透過無摺存款方式將毒品交易所得 762,500 臺幣（約 23,828 美元）存入由 A 人士控制之 B 人士帳戶，隨後再轉匯給其他人。A 人士已因違反《毒品危害防制條例》及《防制洗錢法》罪嫌遭移送檢察署偵辦。

來源 – 中華臺北

資恐（資助恐怖主義）

以下為成員所提供之法濫用於資恐的範例：

案例研究 # 92：透過銀行及網路貸款進行資恐

恐怖主義，包括資恐；金融機構

2019 年，警方搜索 A 人士住宅，發現 A 人士計畫實施恐怖攻擊並需購置設備。為購買此設備，A 人士與其友人透過 X 銀行與數個線上貸款應用程式借款。X 銀行貸款條件僅需身分證及指紋掃描即可取得，其他小額線上貸款僅需身分證及銀行／ATM 存摺即可申請。A 人士自 X 銀行貸得 596 美元，並自數家金融科技公司（線上貸款）取得約 486 美元。此等貸款資金用於購買一把空氣步槍及其氣瓶與調節器，以進行恐怖行動（如攻擊政府、警察及軍事設施），並部分提供給 A 人士所屬恐怖組織作為組織資金。

來源 - 印尼

案例研究 # 93：與陳世憲（CHEN, Shih-Hsien）相關之外國法人

資恐（資助恐怖主義）

中華臺北法務部依據《資恐防制法》規定，於 2018 年 1 月 12 日召開資恐防制審議會。會中基於國際合作及聯合國決議，資恐防制審議會決議：

- 陳世憲（Chen, Shih-Hsien）
- 英屬維京群島註冊 Bunker's Taiwan Group Corporation
- 馬紹爾群島註冊 Billions Bunker Group Corporation
- 馬紹爾群島註冊 UMC Corporation Peru S. A.C.
- 馬紹爾群島註冊 Oceanic Enterprise Ltd.

（共計一名自然人及四家外國法人）被列入制裁名單

2019 年 6 月 22 日陳世憲逝世後，法務部於 2019 年 11 月 25 日宣布將其自制裁名單中移除。然而，上述四家外國法人仍在制裁名單中。

2020 年，陳世憲之遺孀聯繫法務部，表示希望解散上述四家外國法人，但迄今尚未提交任何相關解散文件。因此，該四家外國法人仍持續列於中華臺北指定制裁名單中。

來源 - 中華臺北

案例研究 # 94：與張永源（Tsang Yung-Yuan）相關之法人

資恐（資助恐怖主義）

2018 年 2 月 23 日，美國外國資產管制辦公室（Office of Foreign Assets Control, OFAC）對中華臺北籍人士 Tsang Yung-Yuan（張永源）進行制裁。依據 2018 年 3 月 30 日聯合國安全理事會第 1718 號決議，聯合國安全理事會將下列個人及法人：

- 張永源（Tsang Yung-Yuan）
- 馬紹爾群島註冊 Kingly Won International Co., Ltd.
- 薩摩亞註冊 Pro-Gain Group Corporation

列入聯合國安全理事會制裁名單。因此，中華臺北法務部於 2018 年 3 月 31 日將上述三名個人及法人納入中華臺北之制裁名單。

此項制裁意味著，任何中華臺北之個人或法人均不得向被制裁對象提供任何財產或財產利益，亦不得參與任何涉及被制裁對象財產或財產利益變更之行為。鑑於本案涉及聯合國安全理事會所發布之制裁措施，並經中華臺北法務部指定列入制裁名單，因此，未經聯合國安全理事會正式解除制裁程序，中華臺北不得自行將上述個人及法人自國內制裁名單中移除。截至目前為止，聯合國安全理事會尚未將此三名個人及法人自制裁名單移除，因此相關制裁措施於中華臺北境內仍持續有效。

來源 - 中華臺北

3 - 洗錢及資恐趨勢

本章節內容包括成員所進行之研究與調查（第 3.1 節）、成員就 2023 至 2024 年間所觀察到之洗錢與資恐趨勢報告（第 3.2 節），以及其等對防制洗錢／打擊資恐措施有效性之觀察（第 3.3 節）。

防制措施薄弱、或無效之司法管轄區，尤其容易成為洗錢者與資恐者的目標。此等犯罪分子藉由全球金融系統之複雜性、各國法律之差異性，以及資金跨境移動之迅速性，以隱匿其犯罪活動。⁸¹ 單一司法管轄區內之洗錢及資恐活動，可能對跨境乃至全球造成嚴重不利影響。多數司法管轄區仍以持續打擊資恐活動為其等反恐策略之核心。⁸²

3.1 近期洗錢及資恐手法及趨勢之研究成果

3.1.1 澳洲

《澳洲國家洗錢風險評估》⁸³ 評估產生犯罪所得之犯罪活動，以及在澳洲用以洗錢之手法與渠道。此報告亦檢視影響澳洲環境之國際與國內驅動因素，並評估澳洲如何降低及防制洗錢活動，包括可進一步改善之處。

此評估所呈現的核心主題為「持續性」：犯罪分子持續利用傳統管道洗錢（如銀行、匯款業者及賭場）；持續透過高價資產洗錢（如豪華手錶、車輛及不動產）；並持續透過專業服務提供者協助設立複雜企業結構及相關銀行安排，以協助個人洗錢並隱匿財富。

評估的另一個重要主題是犯罪分子之利用合法金融管道、資產與服務。澳洲國內經濟之核心要素，如現金、銀行帳戶、支付科技、企業架構及信託，亦被犯罪分子用以處置、多層化及整合犯罪所得。

澳洲許多洗錢活動的基礎特徵為不透明、匿名性及交易隱匿性。透過現金、信託、身分犯罪、人頭帳戶及第三方交易，以掩蓋身分、實質受益權或資金流動狀況，仍是犯罪分子持續採行的洗錢手法。主要發現：

- 澳洲經濟遭洗錢者剝削。合法之國內金融管道仍為洗錢者處置、多層化及整合國內外資金之重要途徑。
- 澳洲由於政治體制穩定、經濟開放自由、司法獨立、金融服務發達，而且房地產市場強勁，仍然是儲存與整合犯罪所得之誘人地點。
- 能產出最高價值、且必須以洗錢方式處理犯罪所得之犯罪行為，包括毒品犯罪（種植、製造及販運）、稅務犯罪，以及詐騙政府資助計畫等。
- 犯罪分子持續使用澳洲既有之洗錢渠道，例如現金、奢侈品、不動產、國內銀行、賭場及匯款業者等。
- 犯罪分子利用數位貨幣、數位貨幣交易所、未登記匯款業者及貴金屬交易商進行洗錢之情形日益增加。
- 近年來金融交易速度大幅加快，使得申報義務機構在資金離開帳戶前識別、並凍結可疑交易變得更加困難。若個人同時在多家金融機構開立帳戶，並使用多種金融產品進行交易時，情況則更加複雜。
- 犯罪分子在澳洲境內可建立不透明之法律架構，藉此隱匿其身分及非法活動。此等法律架構可能會限制、或遮掩法人、資產及金融基礎設施之最終實質受益人的可見度，造成澳洲執法機關及產業嚴重的洗錢漏洞。
- 專業服務提供者（無論是否知情）若協助建立、提供諮詢、或代為運作法人及金融基礎設施，亦會降低最終實質受益權的透明度，進而造成澳洲執法機關及產業之洗錢漏洞。

⁸¹ 國際貨幣基金組織 - 《國際貨幣基金組織與防制洗錢及打擊資恐》 (The IMF and the fight against money laundering and terrorism financing) : <https://www.imf.org/en/About/Factsheets/Sheets/2023/Fight-against-money-laundering-and-terrorism-financing>

⁸² 美國財政部 (Department of the Treasury) - 《2024 年國家資恐風險評估》 (2024 National Terrorist Financing Risk Assessment) : <https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf>

⁸³ 澳洲交易報告與分析中心 (AUSTRAC) - 《澳洲國家洗錢風險評估》: <https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf>

《澳洲國家資恐風險評估》（*Terrorism Financing in Australia National Risk Assessment*）⁸⁴ 評估資恐活動之手法與管道的相關風險；此報告亦檢視影響澳洲環境之國際與國內驅動因素，並評估澳洲如何降低及打擊資恐活動，包括可進一步改善之處。此國家風險評估指出以下情形：

- 近年來，具備意圖與能力在澳洲發動恐怖攻擊的暴力極端分子數量已經減少。然而，跨意識形態與宗教背景的暴力極端分子仍持續透過彼此聯繫而變得更加激進。任何恐怖攻擊最可能是由單獨行動的恐怖分子或小型團體所發動。
- 澳洲的資恐環境具有規模小、金額低的特性。國內恐怖攻擊事件不常發生，通常由獨立行動者（個別人士）發動，此等個體往往以自有資金資助行動，往往缺乏可偵測的金融活動軌跡。若資金流動存在，通常是由與嫌犯相關的人士直接提供武器或少量現金。
- 澳洲主要是向境外恐怖組織、及其相關團體提供小規模資恐金流的輸出者。最可能獲得澳洲人資金或支持的恐怖組織包括伊斯蘭國（Islamic State）、蓋達組織（al-Qa’ida）及其附屬組織，以及規模較小程度的哈馬斯（Hamas）與真主黨（Hezbollah）。隨著參與境外衝突的人數減少，用於支持外籍恐怖分子旅行的資金規模亦已降低。
- 恐怖分子及其資助者大多持續利用已建立的相同方式籌集資金。個人資金、及個別支持者捐款（通常以慈善捐贈掩飾）為國內及境外資金籌集提供可靠的來源。跨意識形態及宗教背景的暴力極端分子，則廣泛利用社群媒體、通訊及群眾募資平台進行招募及籌款活動。資恐分子仍偏好銀行、匯款及現金兌換等簡便且成熟之資金移轉方法，而非複雜的金融架構。儘管使用數位貨幣的情況有所增加，但無證據顯示在未來三年內該管道將超越傳統的簡便方法。
- 資恐行為往往不易偵測。透過受監管之金融管道進行的交易，通常與合法金融活動類似，極少引起懷疑。近年金融產品交易速度大幅提升，亦增加申報義務機構在資金離開帳戶前識別、及凍結可疑交易的難度。此外，資金亦可能透過較隱蔽之管道進行籌集或移轉，如現金或未註冊之匯款商。
- 澳洲在國內及東南亞區域之防制資恐體系、作業能力及調查成效近年已有大幅進展。各跨部門、與跨國界間之防制資恐工作小組透過分享情報並協調行動，為瓦解恐怖主義及資恐行動者提供重要工具。
- 金融情資工作已從以往主要監控可疑暴力極端分子、及支持相關調查之被動角色，發展為對抗暴力極端主義之主動角色。公私部門合作使國家安全機構及澳洲最大金融機構之成員得以近乎即時地分享機密資訊。此為預防和對抗暴力極端主義的關鍵要素，因為暴力極端主義行動可能快速且意外地升級為暴力事件。

3.1.2 中國香港

中國香港目前正進行第三次洗錢與資恐風險評估。依據最新的量化及質性資料，關於風險的主要發現包括：

- 頻繁濫用洗錢人頭帳戶。
- 前置犯罪與相關洗錢之犯罪手法（modus operandi）日益數位化。
- 使用虛擬資產的比例不斷增加

3.1.3 印尼

印尼完成《2023年人口販賣與移民走私之洗錢及資恐風險評估》（Risk Assessment of Money Laundering and Terrorism Financing from Human Trafficking and Migrant Smuggling 2023）（資料涵蓋期間為 2018 年 1 月至 2023 年 6 月）。主要發現：

⁸⁴ 澳洲交易報告與分析中心（AUSTRAC）-《澳洲國家資恐風險評估》：<https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Terrorism%20Financing%20NRA.pdf>

- 人口販賣、移民走私與勞工走私所涉及之洗錢犯罪趨勢、犯罪手法與組織及網路結構，並追蹤相關資金流向。
- 根據印尼金融交易報告與分析中心（PPATK）於 2017 年至 2023 年間的金融情報資料庫顯示，目前印尼境內源自人口販賣、移民走私及勞工走私相關之洗錢犯罪趨勢正逐漸增加，已累計達 159 件金融情報成果。PPATK 之金融情報資料顯示，人口販賣與移民走私存在多種剝削形式，包括兒童與性剝削、船員剝削、移民勞工／家庭傭工剝削、未經程序之兒童收養、器官買賣，以及強迫勞動（強迫參與線上詐欺）等。
- 根據資金流向及 2019 年至 2023 年上半年期間收到之可疑金融交易報告，PPATK 發現有 79 家申報單位申報，可疑交易金額達 530 萬美元。依據 PPATK 之移工仲介公司（含有執照及無執照）資料庫，有 59 筆疑似洗錢交易涉及 8 家狀態活躍之印尼移工安置公司（P3MI），及 5 家業務狀態不活躍之移工仲介公司，涉及之可疑金融交易總額達 250 萬美元。已確認之前置犯罪跡象包括人口販賣、詐欺／侵占及毒品犯罪；相關可疑金融交易之申報原因包括來自 PPATK 及／或執法機關之請求、負面媒體報導中所涉之人口販賣案件，以及金融交易異常、且明顯偏離帳戶資料登記檔案之情形。
- 根據印尼金融交易報告與分析中心（PPATK）資料庫及來自受訪申報單位的資料查詢結果，已確認未經許可之移工間存在非常龐大且顯著的金融交易活動，包括國內交易，以及由 37 家處於業務非活躍狀態的移工仲介公司所進行跨司法管轄區資金之流入與流出。此外，有數家移工仲介公司已被通報存在可疑金融交易，包括上述 37 家移工仲介公司，其總計資金流入額達 1.96 兆印尼盾（約合 1.29 億美元）。經深入分析與研究後，依照區域分布發現多個人口販賣與移民走私犯罪網路，其中以亞太地區及中東地區為主要犯罪發生區域，其手法包括傳統招募、社群媒體宣傳、求職網站刊登虛假資訊、以職業訓練機構名義掩護，以及透過經許可與未經許可之移工仲介公司進行之非正規移工安置等。
- 至於不同剝削類型的洗錢犯罪風險，涉及性剝削、使用身體及生殖器官，以及印尼籍移工之剝削案件屬於高度風險。尤其值得注意的是，透過網站及社群媒體進行之線上詐騙近年來迅速增加，已成為利用資訊科技之新興人口販賣手法與趨勢。
- 人口販賣及各類剝削活動的趨勢日益明顯，特別是針對境內外受害者的網路詐騙及投資詐欺（例如：殺豬盤）活動持續增加，並出現透過網站與社群媒體等資訊科技進行的新型態犯罪手法。

紅旗指標

- 實體（行為人或當事方）：
 - 交易當事人來自未經許可之招募及就業安置機構。
 - 交易行為人為人口販賣案件之犯罪嫌疑人。
 - 犯罪者透過社群媒體、網站或缺乏可信度之求職平台，運用社交工程手法進行招募。
- 交易：
 - 交易訊息內含如下詞彙：印尼勞工費用、勞動、護照、不道德或色情字眼、印尼女性移工管理（handling TKW）、機票、gurda、nier、sinjang、勞動力、勞工等。
 - 接收來自未簽署合作協議、且未具勞工保護法規之司法管轄區勞動仲介機構所匯入之資金。
 - 資金流向多個高風險地區，這些地區作為勞工來源地及中轉地，或屬於未批准國際勞工保護規範的司法管轄區，例如未落實移工保護規定、移工社會保障規定；政權仍呈雙重狀態（如利比亞、伊朗、敘利亞）；處於衝突或戰爭狀態（如俄羅斯、烏克蘭、黎巴嫩）；或不歡迎外國勞工（如黎巴嫩）的司法管轄區等。
 - 使用銀行、匯款業者及貨幣兌換商之資金移轉與外匯服務。

- 交易呈過渡（pass-by）模式，與帳戶持有人的個人資料及業務領域不符。
- 採用資金混合（co-mingling）方式，將犯罪所得與合法企業、或投資產品收益混合。
- 透過自動櫃員機進行現金存取款，並呈現結構化（structuring）模式（即同一天內進行多筆交易）。
- 將資金存放於銀行保險箱內。
- 活動：
 - 大量且重複購買旅行機票。
 - 大眾媒體負面報導。
 - 就業培訓機構之行為人假冒來自勞工派遣單位。
 - 金融交易活動與通常或慣常交易特徵不符，特別涉及具有土地、海洋及航空管制權限之執法官員。
 - 使用印尼移工安置公司員工之帳戶。
 - 於國際邊境區域內大量現金提領。
 - 透過網路頻繁進行金融交易，以避免面對金融服務人員。

3.1.4 日本

日本已於 2023 年 12 月 7 日發布《國家風險評估後續報告》（National Risk Assessment-Follow up Report），並將於 2024 年底發布此報告之英文版本。

3.1.5 寮國

寮國於 2023 年進行第二次洗錢及資恐國家風險評估（NRA），旨在評估所有依據防制洗錢及打擊資恐法規定之前置犯罪的威脅、弱點、缺口、手法及趨勢。該評估將於 2024 年底完成並公開發布。此外，寮國亦針對銀行、賭場、不動產、虛擬資產服務提供商、非營利組織及法人等高風險領域進行產業別的洗錢及資恐風險評估。

3.1.6 馬來西亞

馬來西亞依據其 2020 年《國家風險評估》（NRA）指出，詐欺、貪污、非法毒品販運、有組織犯罪及走私仍是該國主要的境內犯罪活動。

馬來西亞目前正在進行 2023 年版國家風險評估，預計於 2024 年下半年完成。此次評估的主要目標在於辨識、評估並瞭解在司法管轄區境內的洗錢及資恐風險，涵蓋威脅、各產業既有風險、控管措施、相關新興趨勢，以及產業評估與威脅評估間的相互關聯。此國家風險評估亦將涵蓋自上一次國家風險評估後出現的新興趨勢與模式。

3.1.7 菲律賓

菲律賓防制洗錢委員會（AMLC）於 2023 年進行並發布下列有關洗錢與資恐之研究報告：

- 《菲律賓線上兒童性虐待與剝削報告》（*Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines*）⁸⁵（2023 年 5 月）。

⁸⁵ 菲律賓防制洗錢委員會 - 《菲律賓兒童線上性虐待與剝削報告》（*Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines*）：

<http://www.amlc.gov.ph/images/PDFs/Main/Online%20Sexual%20Abuse%20and%20Exploitation%20of%20Children%20in%20the%20Philippines.pdf>

- 《態樣簡報：洗錢人頭帳戶》（*Typologies Brief: Money Mules*）⁸⁶（2023 年 1 月）。
- 《與賭場中介公司相關之可疑交易分析》（*Analysis of Suspicious Transactions Associated with Casino Junkets*）⁸⁷（2023 年 1 月）。

3.1.8 新加坡

新加坡的主要風險仍涉及法人濫用、貪污、貿易和稅務相關之洗錢，以及集團式洗錢（包括網路詐騙）。作為金融中心，對財富管理產業潛在的洗錢風險。新加坡持續保持高度警覺。

案例研究 # 95：透過跨政府協調強化新加坡的防制洗錢與打擊資恐體系

有組織犯罪集團；詐欺；自我洗錢；金融機構

新加坡警察部隊（SPF）接獲可疑交易活動的資訊，包括銀行所提交關於偽造資金來源證明之可疑交易報告後，啟動一項全面協調的情報調查行動，此成為新加坡迄今規模最大的防制洗錢執法行動之一。2023 年 8 月，新加坡警察部隊對 10 名涉及以洗錢方式處理境外犯罪活動所得的嫌疑人提出指控，並扣押／禁止其等位於新加坡之資產。截至 2024 年 6 月，全部 10 名嫌疑人皆已被定罪，因涉及洗錢及偽造文書詐欺等罪名，各被判處 13 至 17 個月不等之有期徒刑。與其相關約 9.44 億新加坡元（約 7.34 億美元）資產（超過其被扣押／禁止資產之 90%）已被沒入歸國庫。

此案件提示新加坡，防制洗錢與打擊資恐體系必須與時俱進、鍥而不捨，以因應不斷演變的洗錢風險與態樣。借鑑此案，新加坡成立跨部會委員會（IMC），由多個政府部門及機構組成，以探討進一步強化新加坡防制洗錢與打擊資恐體系的各項措施。跨部會委員會的檢討工作廣泛涵蓋以下三個重點領域：

- 防止法人結構遭洗錢人士濫用。
- 加強金融機構控管措施及合作協調，以及指定之非金融事業或人員（DNFBP）對新加坡金融體系的保衛功能。
- 提升政府機關間之監控及資訊整合能力，以利早期偵測可疑活動，並促進後續情報分享。

跨部會委員會工作仍持續進行中。

來源 - 新加坡

2023 年 3 月，新加坡金融管理局（MAS）發布有關財富管理產業洗錢及資恐風險之通函⁸⁸，提醒所有金融機構（FI）務必對財富管理業務所涉及的洗錢與資恐風險保持警覺，並闡明金融管理局期待各金融機構檢視現有控管措施，以確保其等得以降低來自高成長領域的洗錢與資恐風險。金融管理局亦進行全行業之防制資恐控管措施調查，並透過一系列主題性檢視，以評估金融機構對資恐風險之理解，同時檢查其資恐相關控管措施的有效性。

2023 年 5 月，新加坡金融管理局發布《強化金融機構打擊資恐控管措施》（*Strengthening Financial Institutions' Countering the Financing of Terrorism Controls*）⁸⁹ 指引文件；此文件根據金融管理局針對整個產業進行之資恐控管措施調查，及主題性檢視之觀察結果編撰，闡明金融管理局的重要觀察，及其對金融機構的監理期望，金融機構應據此對照檢視自身的控管措施。金融管理局發布該指引文件後，建議金融機構以風險基礎（risk-based）且相稱的方式，參照文件所載之實務作法及監理期望，並進行缺口分析。

⁸⁶ 菲律賓防制洗錢委員會 - 《態樣簡報：洗錢人頭帳戶》：

http://www.amlc.gov.ph/images/PDFs/PR2023/2022%20DEC%20TYPOLOGIES%20BRIEF%20MONEY%20MULES_For%20Publication.pdf

⁸⁷ 菲律賓防制洗錢委員會 - 《與賭場中介公司可能相關之疑似洗錢或資恐交易報告分析》：

http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATED%20WITH%20CASINO%20JUNKETS_FINAL.pdf

⁸⁸ 新加坡金融管理局 - 《財富管理產業之洗錢與資恐風險》：<https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/anti-money-laundering/countering-the-financing-of-terrorism/circular--mltf-risks-in-the-wealth-management-sector-3-mar-2023.pdf>

⁸⁹ 新加坡金融管理局 - 《強化金融機構之打擊資恐控管措施》：<https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidance/amld/strengthening-fi-cft-controls/strengthening-fi-cft-controls.pdf>

為確保金融機構持續對制裁風險環境的變化保持警覺，金融管理局亦於 2023 年 8 月發布《確保有效偵測制裁相關風險》（*Ensuring Effective Detection of Sanctions-Related Risks*）通函⁹⁰，特別鼓勵金融機構繼續強化董事會與高階管理層對相關制裁風險的監督，並提升偵測制裁風險之能力，包括運用資料分析。

此外，新加坡各產業監管機關與執法機關亦積極與業界合作，共同辨識、評估及降低洗錢及資恐風險。其中，由新加坡警察部隊商業事務局（CAD）及新加坡金融管理局（MAS）共同主持的「防制洗錢／打擊資恐產業夥伴聯盟」（AML/CFT Industry Partnership，ACIP）即為此類公私合作計畫之一。ACIP 於 2023 年 7 月發布《業界觀點：數位資產連結之客戶關係的洗錢、資恐及制裁風險管理最佳實務》（*Industry Perspectives on Best Practices - Management of Money Laundering, Terrorism Financing and Sanctions Risk from Customer Relationships with a Nexus to Digital Assets*）文件⁹¹；2024 年 2 月再發布《金融機構管理來自公司服務業者引介業務之洗錢、資恐及資武擴風險的最佳實務》（*Financial Institutions to Manage Money Laundering, Terrorism Financing and Proliferation Financing Risk Associated with Receiving Referrals from Corporate Service Providers*）文件⁹²。

3.1.9 越南

越南於 2024 年完成洗錢及資恐國家風險評估，並制定降低高風險與中等風險之行動計畫。依據針對法人實施之洗錢及資恐風險評估結果顯示，

越南因法律規範之因素，包括對外國投資與稅務之嚴格規定，對來自外國司法管轄區之公司而言，越南並不具吸引力。越南目前正檢討國內法人之刑事責任，並提議修改企業法，以納入實質受益權之相關義務。

3.2 新興趨勢、下降趨勢與持續趨勢之觀察

聯合國毒品犯罪辦公室（UNODC）— 東亞與東南亞地區之賭場、洗錢、地下匯兌與跨國有組織犯罪：一個隱密且加速中的威脅

跨國有組織犯罪與非法經濟活動為東南亞地區帶來前所未之挑戰，近年來該地區更成為新技術的試驗場。基本上，該地區因為非法經濟的擴張，迫使地下匯兌（underground banking）系統經歷革命性的變革。

東南亞蓬勃發展的賭場產業，其後衍生的博奕中介（junkets）、線上賭場、電子博彩中介（e-junkets）以及日益猖獗的非法但監管不足的加密貨幣交易所，已成為有組織犯罪集團所運用之銀行架構的基礎組成部分。賭場與相關產業已證明其等能有效、且不易被察覺地轉移及洗錢大量的法定貨幣與加密貨幣，藉此創造管道將數十億美元的犯罪所得有效整合進入正式金融體系。

與此同時，可擴展且數位化的解決方案快速發展，使東南亞尤其是湄公河地區的犯罪商業環境更為活躍，也為以此區域作為營運基地的犯罪分子創造新的機會。此現象進一步吸引犯罪網路、創新者及服務業者於區內聚集、相互支持並從各種非法市場中獲利，同時地下匯兌需求亦日益高漲。

聯合國毒品犯罪辦公室透過一年以上的詳盡調查與分析，包括刑事起訴書、案件紀錄、金融情報、法院文件及相關公開資訊，以及與國際及區域執法及犯罪情報夥伴之磋商，完成此報告。此報告是對區域地下匯兌運作機制、複雜性及宣導因素的一次獨特嘗試。報告提出若干廣泛建議，旨在協助區內司法管轄區解決已發現之問題及漏洞，最終提高東南亞尤其是湄公河地區各國政府、監管機關及執法單位的意識、理解與能力。

⁹⁰ 新加坡金融管理局 - 《確保有效偵測制裁相關風險》：<https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/amld/circular---ensuring-effective-detection-of-sanctions-related-risks.pdf>

⁹¹ 防制洗錢／打擊資恐產業夥伴聯盟 - 《業界觀點：數位資產連結之客戶關係的洗錢、資恐及制裁風險管理最佳實務》：[https://abs.org.sg/docs/library/acip-best-practices-for-the-management-of-ml-tf-and-pf-risks-from-customer-relationships-with-a-nexus-to-digital-assets_100723-\(publish\).pdf](https://abs.org.sg/docs/library/acip-best-practices-for-the-management-of-ml-tf-and-pf-risks-from-customer-relationships-with-a-nexus-to-digital-assets_100723-(publish).pdf)

⁹² 防制洗錢／打擊資恐產業夥伴聯盟 - 《金融機構管理來自公司服務提供商引介業務之洗錢、資恐及擴散融資風險的最佳實務》：<https://abs.org.sg/docs/library/acip-best-practices-for-banks-to-manage-ml-tf-pf-risks-associated-with-receiving-referrals-from-corporate-service-providers.pdf>

防制洗錢金融行動工作組織（FATF）- 透過群眾募資進行資恐

近年來，群眾募資活動日益增長，專家預測未來將持續擴張。2020 年全球群眾募資市場規模估計達 172 億美元，預計 2026 年將達 346 億美元⁹³。FATF 曾有研究顯示，透過線上群眾募資是進行資恐的方式之一。

此報告⁹⁴深入研究個別恐怖分子、恐怖組織與暴力極端主義者透過群眾募資為各種恐怖活動進行籌資的手法與技術；並建立對各種群眾募資活動之共同認識，特別重點關注資恐風險最高之各類活動。

此專案團隊由加拿大與西班牙專家共同領導，FATF 秘書處提供支援。團隊成員由來自 FATF 全球網路之 12 個會員與 1 個觀察員組織組成，包括：加拿大、歐盟執委會、法國、希臘、印度、義大利、日本、菲律賓、西班牙、土耳其、聯合國（CTED）與美國。

此報告研究結果基於以下內容：回顧現有文獻及公開來源資料，包括 FATF、區域性防制洗錢組織（FSRB）、以及 FATF 成員國與觀察員組織的報告；來自 FATF 全球網路問卷調查之結果。40 個代表團提供有關風險指標及群眾募資進行資恐的案例研究資訊；FATF 成員國與觀察員組織、學術界、智庫及私部門於 FATF 印度聯合專家會議（2023 年 4 月）以及西班牙反制資恐研討會（2023 年 9 月）上分享之討論與觀點；以及私部門及非營利組織全球聯盟針對 FATF 提供的書面意見。

主要發現與建議

報告指出，群眾募資平台被濫用進行資恐目的之四種主要方式；實務上，恐怖分子與暴力極端主義者通常會透過多種手段募集資金，並可能結合使用不同的方法與各種技術。雖然部分司法管轄區及業界參與者，積極實施各種措施以降低此等風險，但全球防制洗錢與打擊資恐法規並不一致。根據全球網路的司法管轄區所述，以捐贈為基礎的群眾募資因其特性，而最易被濫用於資恐用途，且經常不在防制洗錢與打擊資恐規範之內。其中原因之一是許多司法管轄區未系統性地評估群眾募資活動相關風險，因此仍普遍缺乏相關濫用情形的全面性數據。群眾募資產業的多樣性、所使用的多種募資模式，以及支付技術快速演進的本質，亦說明現今各司法管轄區在監管上的不同方式。

報告強調政府機關與群眾募資生態系統利害關係人，在偵測及遏止資恐活動時面臨的挑戰。執法機關在調查與群眾募資相關的資恐疑案時，經常難以證明資金被用於與恐怖主義相關的犯罪行為。群眾募資運作的複雜性、缺乏數據及匿名化技術的使用，更增添執法機關、申報單位和監管者追蹤資金的難度。提供群眾募資服務的中介平台因其員工缺乏足夠的訓練與資恐專業知識，且往往未設立適當的申報機制，以致難以在其網站上辨識資恐活動。各公司在移除非法內容的行動力度也不一致。

一些司法管轄區提供部分最佳實務案例來應對這些挑戰，例如加強對國內群眾募資產業性質和規模的理解，並將群眾募資納入國家風險評估。在群眾募資領域進行外展活動，也被證明能有效加強辨識與申報潛在資恐活動。穩健的國內與國際資訊分享機制，以及公私部門的合作，也構成有效反恐以及防制洗錢／打擊資恐行動的基礎。

此報告建議司法管轄區及所有涉及群眾募資產業的利害關係人，辨識並瞭解與此活動相關的資恐風險，並採取符合聯合國安理會第 2462 號決議的風險基礎且相稱的措施，以降低潛在的濫用風險。鑑於群眾募資具全球性，司法管轄區應體認此募資活動的跨境性質，並防範自身管轄區被利用於境外資恐。此外，司法管轄區應考量此產業持續演進，資恐風險可能與時俱進。

司法管轄區應將公私部門間之資訊分享作為優先事項，並持續對私部門利害關係人進行相關外展與宣傳活動，以增強對潛在資恐活動的偵測，促進對產業及控管機制的共同理解，並確保合法的群眾募資活動不受限制。考量群眾募資與其他金融及非金融領域有所關聯，司法管轄區應全面落實與虛擬資產、非營利組織、及金錢或價值轉移服務（MVTS）有關的 FATF 標準，避免將群眾募資視為獨立領域處理。最後，在制訂群眾募資相關風險抵減策略時，司法管轄區應採取涵蓋權責機關、私部門、民建團體、及學術界的利害關係人共同參與方式，以確保符合人權盡職調查，避免妨礙合法募資活動的進行。

報告亦包含風險指標清單，以協助公私部門及一般大眾辨識與群眾募資相關的可疑活動。

⁹³ 市場資料預測（Market Data Forecast）-《全球群眾募資市場研究報告》（Global Crowdfunding Market Research Report）：www.marketdataforecast.com/market-reports/crowdfunding-market

⁹⁴ FATF 《打擊資武擴最佳實務與指引－強化權責機關採取行動之能力》（Best Practices and Guidelines on the Fight against Proliferation Financing - Strengthening Authorities for Action）：<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Speech-psi-political-meeting-may-2018.html>

3.2.1 加拿大

新興趨勢：在加拿大，有組織犯罪集團利用網路大麻藥房非法銷售大麻的灰色市場，因為大麻合法化迎來更多機會。此等公司利用電子資金轉帳系統，透過專業洗錢人士（PMLs）擁有的多個空殼公司，向 PMLs 隱匿資金來源，同時有效地透過資金多層化，以防止全部資金遭到沒入。

持續趨勢包括：加拿大持續將包括甲基安非他命、吩坦尼（fentanyl）和古柯鹼在內的非法毒品販運視為與洗錢有關的主要前置犯罪，相關洗錢手法包括透過不具名公司將犯罪所得投資於合法經濟之不動產購置、利用結構化及布穀鳥式洗錢（cuckoo Smurfing）方式將犯罪所得整合進金融機構，以及透過非正式價值轉移系統（Informal Value Transfer System, IVTS）轉換、或移動大量現金。

跨國重大有組織犯罪集團持續利用加密貨幣進行大量非法毒品的批發採購及轉售，同時也用於接收客戶支付的款項。與此相關的是新興的人工智慧及深偽技術（deepfake），犯罪者透過此類技術偽造身分證件，以逃避虛擬資產服務提供商的客戶身分確認措施。

3.2.2 庫克群島

庫克群島指出毒品販運、詐欺及貪污等前置犯罪的趨勢仍然不變。

3.2.3 中國香港

新興趨勢：近年來虛擬資產市場迅速發展，虛擬資產已成為犯罪販子以洗錢方式處理犯罪所得的途徑。有時部分被捕人士聲稱，其帳戶中之交易是其真正的加密貨幣交易所得，並否認知悉資金來源為犯罪所得。

某些案件中，洗錢集團或人頭帳戶持有人使用假身分證件或深偽技術進行身分驗證。目前此類案件數量仍然較少，但已引起相關單位注意。

此外，新的跨境支付機制使得中國香港與其他司法管轄區之間的金融交易增多，但另一方面，也使中國香港面臨潛在跨國洗錢風險，例如跨境多層化（cross-border layering）。犯罪集團藉由在中國香港與其他司法管轄區之間轉移犯罪所得，製造多層化跨境支付，往往造成執法機構在追蹤資金流動上的重大延誤。

持續趨勢：詐欺相關犯罪仍是最常見的前置犯罪，其次是毒品相關犯罪。其他在中國香港的前置犯罪，包括境外逃漏稅及境外貪污案件，則保持穩定。銀行業仍洗錢活動的主要管道。

使用第三方以洗錢方式處理犯罪所得的行為持續盛行：

- 洗錢集團招募非居民、學生及低薪人士開立銀行帳戶，以小額金錢作為報酬。
- 在某些情況下，招募人頭帳戶持有人亦涉及就業詐騙。犯罪分子聲稱代表不同類型業務的公司（公司甚至可能不存在）聘用員工，指示求職者開立銀行帳戶（通常為個人帳戶）。受害者被告知此等帳戶係被用於處理與業務相關的交易及資金，但事後證實該等資金為詐欺案件的犯罪所得。
- 近期亦發現外籍家庭幫傭被招募為人頭帳戶之情事。

銀行日益普及的遠端開戶程序，使得傳統及虛擬銀行帳戶持續高度涉入犯罪活動：

- 犯罪者亦招募人頭帳戶持有者設立虛擬銀行帳戶。

近年來，隨著科技進步及電子金融服務的普及，涉及網路、電子郵件和社群媒體的前置犯罪越趨普遍。

濫用儲值支付工具（SVF）的行為仍然盛行：

- 犯罪者以盜用的身分證件開立儲值支付帳戶，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。

衰退趨勢：隨著申報單位強化客戶盡職調查（CDD）規範，以辨識各類公司的實質受益人，利用境外公司進行洗錢活動的情況已逐漸減少。

3.2.4 印尼

印尼持續進行洗錢與資恐風險評估，並確認相關風險與新興趨勢，包括：

- 法人：
 - 洗錢與法人領域的新興趨勢包含使用易遭濫用之公證認證文件進行投資，特別是來自不具海牙認證（apostille）效力之司法管轄區，以及使用虛擬公司或虛擬辦公室之認證文書。
 - 使用虛構實體、法律地位不明確之公司，例如未持有營業執照或機構許可，並利用名義持有人、掛名人或親屬等掩飾受益所有人的身分，進行資金混合。
- 金融科技（FinTech）
 - 詐欺是金融科技領域中具有高度洗錢風險的前置犯罪類型，侵占、賭博和貪污則屬中等風險。
 - 具有高度洗錢風險的產業包括商品期貨交易、加密資產、匯款業務、銀行業，以及電子貨幣和電子錢包服務提供商。

金融科技在投資、匯款及支付領域面臨高度風險，以及下列新興洗錢即資恐之趨勢：

| 支付與匯兌 | 借貸 | 群眾募資 | 投資 | 其他 |
|--|--|--|---|--|
| <p>交易過程涉及複雜的多層化手法，例如存款與支付交易非直接使用銀行帳戶，而是透過多種交易服務（包括電子錢包、貨幣兌換網站等）。</p> <p>濫用電子錢包儲存及轉移線上賭博所得。</p> <p>現金提領與現金存入用以切斷金流。</p> <p>iv.跨境QR付款。</p> | <p>線上貸款之資金提供者與資金接收者相互勾結。</p> <p>ii.以虛擬帳戶支付的線上貸款交易並未使用線上貸款帳戶所記錄的帳戶。</p> | <p>對於群眾募資活動，目前未從受訪者取得新的洗錢或資恐威脅案例，但在選舉背景下，我們已辨識出透過社群群眾募資機制收集選舉資金的潛在風險。</p> <p>群眾募資可能掩蓋資金來源，因資金來源來自大眾，且可能超過個人捐款上限。</p> | <p>透過市場外的加密貨幣交易（私人區塊鏈交易、點對點（P2P）直接交易）。</p> <p>利用境外加密貨幣交易所進行交易。</p> <p>以電子商務進行投資例如線上共同基金投資、與電子商務平台合作的黃金投資。透過社群媒體進行電子錢包/電子貨幣交易合約(通常用來購買並售出加密資產)。</p> <p>非同質化代幣（NFT）。</p> <p>由第三方進行投資支付。</p> | <p>設立虛假公司（商戶）帳戶用來洗錢。</p> <p>ii. 犯罪者濫用「先買後付」（buy now, pay later）服務購買商品。</p> |

3.2.5 日本

日本提供以下表格：

(依據《有組織犯罪處罰法》及《毒品特別法》所偵破之洗錢案件數量與比例，按前置犯罪分類)

| 年 | 被濫用交易 | | | | | | | | | | 總計(案件數量) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|--------|------|------|----------|-----|------|-----|-----|-----|----|----------|-----|----|----|----|----|----|----|----|-----|-----|----|-----|-----|-----|-------|----|----|----|---|---|----|----|---|---|---|---|---|---|---|-----|-----|-----|-------|
| | 國內匯兌交易 | | | | | 現金交易 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | 2020 | 2021 | 2022 | 總計(案件數量) | 110 | 208 | 266 | 584 | 120 | 72 | 105 | 297 | 96 | 40 | 55 | 39 | 71 | 20 | 40 | 160 | 115 | 11 | 9 | 16 | 57 | 36 | 32 | 14 | 16 | 9 | 7 | 32 | 20 | 5 | 3 | 1 | 1 | 0 | 2 | 2 | 424 | 430 | 530 | 1,384 |
| 總計(案件數量) | 584 | 297 | 160 | 115 | 11 | 9 | 16 | 57 | 36 | 32 | 14 | 16 | 9 | 7 | 32 | 20 | 5 | 3 | 1 | 0 | 2 | 2 | 424 | 430 | 530 | 1,384 | | | | | | | | | | | | | | | | | | |

(主要交易 被濫用於洗錢等)

| 比例 | 案件數量 | 前置犯罪 | 總計 |
|------|------|--|--------|
| 34.7 | 701 | 竊盜 | 2,021 |
| 34.2 | 691 | 詐欺 | |
| 10.9 | 220 | 電腦詐欺 | |
| 3.3 | 67 | 違反《投資法》/《資金業法》 (Money Lending Business Act) | |
| 1.9 | 38 | 經常性賭博／以營利為目的經營賭場 | |
| 1.7 | 34 | 違反《出入國管理及難民認定法》 (Immigration Control and Refugee Recognition Act) | |
| 1.6 | 33 | 毒品相關犯罪 | |
| 1.3 | 26 | 違反《風俗營業法》 (Amusement Business Act) | |
| 1.3 | 26 | 違反《商標法》 | |
| 1.2 | 24 | 偽造文書罪 | |
| 1.0 | 20 | 恐嚇罪 | |
| 1.0 | 20 | 散布猥褻物品罪 | |
| 0.9 | 18 | 違反《防制賣淫法》 (Anti-Prostitution Act) | |
| 0.8 | 17 | 侵佔罪 | |
| 0.6 | 13 | 持械搶劫罪 | |
| 0.6 | 12 | 未經授權製作私用電磁紀錄罪 | |
| 3.0 | 61 | 其他 | |
| | 100 | 總計 | (案件數量) |

日本分析遭逮捕之洗錢犯罪案件及可疑易報告資訊，觀察如下：

- 境內匯兌交易共有 584 筆（約佔 42.2%），其次為現金交易 297 筆（約佔 21.4%）與存款交易 160 筆（約佔 11.6%），此三類交易佔利用存款金融機構之商品及服務進行洗錢的主要部分。
- 許多案件中，有洗錢意圖之人士透過能快速可靠轉移資金的境內匯兌交易，將犯罪所得轉入以他人名義開設的虛設帳戶內。最終透過境內匯兌交易、或存款交易存入帳戶內的犯罪所得，會再轉換為現金，導致資金後續追蹤極為困難。
- 隨著信用卡詐欺案件增加，被濫用於洗錢的信用卡數量也不斷增多。
- 支付方式的多樣化，例如信用卡、預付支付工具、加密資產及資金移轉服務遭到濫用情形的增加，導致主要交易類型被濫用的情況更趨普遍。

3.2.6 寮國

寮國指出，2023 年由可疑交易報告（STRs）中所辨識出的持續趨勢（指標）如下：

- 使用個人帳戶進行商業活動。此為逃漏稅之指標；客戶未使用企業銀行帳戶，而改用個人銀行帳戶進行交易。
- 進行大額交易卻缺乏充分理由，且／或交易與客戶的身分描述資料不符。
- 詐欺案件：大部分從可疑交易報告中發現的詐欺案例涉及社群媒體詐騙、電話詐騙中心及網路犯罪，多屬於點對點（P2P）詐欺。

3.2.7 中國澳門

中國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：

- 未參與或僅極少參與賭博活動即兌換籌碼。
- 異常大額現金提領。
- 貨幣兌換／現金轉換。
- 存入大額現金且資金來源無法查證。
- 代第三方兌換籌碼／兌換貸款憑證（marker redemption）／進行賭博。
- 使用自動櫃員機、電話銀行及現金存款機。
- 使用支票／帳戶轉帳等方式移轉資金。
- 可疑電匯交易。
- 使用網路銀行／網際網路。
- 可能符合監控系統之觀察名單或其他黑名單。

2023 年 1 月至 12 月期間，金融情報辦公室（GIF）共接獲 4,614 件可疑交易報告（STRs），其中博彩業占 3,431 件、金融業（含銀行、保險及金融中介業）占 887 件，其他產業占 296 件。同期間內，金融情報辦公室將 116 件 STR 案件轉交檢察院（Public Prosecutions Office），由執法單位進一步調查。這些案件主要涉及犯罪集團及詐欺活動。相關案件多涉及犯罪集團及詐欺。

洗錢趨勢：儘管多數犯罪（包括毒品、賭博相關犯罪及竊盜罪）相較於前一年有所增加，但仍低於 2019 年水準。2023 年，網路犯罪及電信詐騙持續攀升，達到高於新冠疫情前的水準。中國澳門司法警察局（PJ）遵循三大方針，以因應犯罪環境之變化。此等方針著重於：強化打擊與賭博相關犯罪、深化防制詐騙工作，及強化執法單位部署以因應日益增加的跨境犯罪風險。司法警察局亦採取多項防制犯罪措施，此等措施已證明能有效保護社會安全及大眾之合法權益。

資恐趨勢：中國澳門注意到近年來東南亞地區內非營利組織遭濫用於資恐活動，引發各方關切。司法警察局持續對此狀況保持警覺，並持續進行威脅分析。目前為止，司法警察局未發現任何與中國澳門相關之資恐活動。亦未發現中國澳門境內存在任何本土恐怖組織，更無任何外籍恐怖分子前往中國澳門。除此外，除金融機構已執行以風險為基礎之打擊資恐措施並持續監控可疑資金流動外；司法警察局於 2020 年 10 月成立專責之反恐調查處，積極分析與調查匯往高風險司法管轄區之資金。截至目前為止，並未發現任何與資恐相關之案件，整體趨勢維持穩定。

3.2.8 馬來西亞

根據馬來西亞國家詐騙應變中心所通報之案件，犯罪分子最常使用的詐騙手法仍以假求職、投資詐騙、電信詐騙及電子商務詐騙為主：

- 假求職詐騙：詐騙集團通常以誘人的高報酬為誘因，聲稱能迅速輕鬆賺取金錢，例如訂閱 YouTube 頻道、提供反饋意見或購買商品。
- 投資詐騙：受害人被吸引加入不存在的投資計畫，該計畫宣稱能以極少或無風險的方式獲取高額且迅速的回報。
- 電信詐騙：電信詐騙集團常見手法為冒充官方機構，增加其詐騙的可信度，利用受害人對法律機關的恐懼，從而掌握受害人個資以取得信任。
- 電子商務詐騙：在節慶期間與節日相關的電子商務詐騙明顯增加。此類詐騙包含多種欺騙手法，例如偽造商品、假促銷活動以及針對積極尋找節慶商品之消費者的網路釣魚詐騙手法。

3.2.9 馬爾地夫

2023 年，金融情報中心針對 2022 年 1 月至 2023 年 3 月期間達申報門檻（現金與電子資金交易金額超過 20 萬盧非亞（MVR），約 12,970 美元）之交易進行了策略分析。金融情報中心辨識出銀行客戶進行與貿易洗錢相關交易呈現增加趨勢，與 2023 年可疑交易報告（STR）分析結果一致。

金融情報中心將此觀察結果告知銀行、執法機構及監理機關，並指示銀行強化客戶身分確認（即「認識你的客戶」，KYC）及客戶盡職調查（CDD）措施，以防制貿易洗錢活動。金融情報中心之策略分析及對銀行的指示，使得 2023 年第四季與貿易洗錢有關的可疑交易報告數量下降。

2023 年可疑交易報告觀察到的其他趨勢包括：

- 前置犯罪：稅務犯罪、詐欺與詐騙、侵佔、貪污與濫用職權、非法外匯交易、偽造文書、毒品犯罪及有組織犯罪活動。
- 犯罪所得涉及不動產（公寓）。
- 濫用法人實體。

3.2.10 菲律賓

菲律賓兒童線上性虐待與剝削（OSAEC）情況⁹⁵（2023 年 5 月）

截至 2022 年底，通報機構（CP）提交與 OSAEC 有關之可疑交易報告數量整體呈增加趨勢，由 2015 年的 204 件增至 2022 年的 92,200 件。申報理由包括：兒童色情（94.47%）、人口販賣及人口走私（0.69%）、照片及影片濫用（0.75%），以及其他情況（4.05%）。值得注意的是，約 73% 之 OSAEC 相關可疑交易報告，是由通報機構透過內部篩查及／或客戶交易調查後，主動揭露為符合 OSAEC 典型態樣之交易；其餘 27% 則為通報機

⁹⁵ 菲律賓防制洗錢委員會 - 《菲律賓兒童線上性虐待與剝削報告》（*Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines*）：

<http://www.amlc.gov.ph/images/PDFs/Main/Online%20Sexual%20Abuse%20and%20Exploitation%20of%20Children%20in%20the%20Philippines.pdf>

構被動回報，多數由菲律賓防制洗錢委員會（AMLC）轉介所觸發。

《與賭場中介公司可能相關之可疑交易報告分析》⁹⁶（2023 年 1 月）

該研究強調博彩中介系統因其交易量及金額龐大，易受洗錢與資恐風險影響的既有弱點。2009 年以來的可疑交易報告（STRs）通報案件數量及涉案金額，即可證明此一情形。

資料集 1（Dataset 1）⁹⁷ 中可疑交易報告（STRs）分析顯示，自 2021 年起，STRs 通報數量呈上升趨勢。奇怪地，儘管資料集僅涵蓋該年最初 18 天，但 2023 年 STRs 數量最高。進一步分析發現，這些 STRs 由 4 家通報機構針對 17 名個人提出（其中 11 名菲律賓籍、4 名來自 B 司法管轄區、2 名來自 C 司法管轄區）。通報機構指出，這些個人：(1) 涉嫌參與犯罪集團，遭調查涉及龐氏騙局、或層壓式推銷詐騙；(2) 進行現金存入及籌碼兌換交易，但未參與任何博奕活動；(3) 進行與個人背景資料不相稱的銀行交易；或 (4) 缺乏文件佐證交易之合法性。

另一方面，博奕中介相關洗錢或資恐報告的年度總價值似乎每三年激增一次，自 2016 年開始。其中最大規模的激增發生於 2022 年，當年度博奕中介相關 STR 總金額達到 96.8 億比索（約佔資料集 1 中 STRs 總價值之 54.42%，約合 1.68 億美元）。2022 年 STRs 價值劇增之原因，來自 13 筆涉及博奕中介玩家將賭場籌碼存放於賭場財務部門保管，金額介於 1 億至 3 億比索之間。

在交易數量與金額方面，資料集 1 中大部分博奕中介相關之可疑交易報告（STRs）均係依據修訂後菲律賓《第 9160 號共和國法》列舉之可疑情況所提交。可疑情況：「無基礎之法律或貿易義務、目的或經濟理由」（SI1）即佔樣本一半以上，分別佔總 STR 數量的 58.71% 及總 STR 金額的 54.04%。此等 STRs 主要涉及帳戶持有人缺乏支持性文件，無法證明其帳戶交易的合法性。

在樣本 STRs 中所列之前置犯罪中，以「違反《2000 年證券管理法》之詐欺行為與其他違規事項」案件數量最多，約佔 STR 總數的 2.24%。在交易金額方面，「詐欺罪」排名首位，涉及金額達 1,584 萬比索（約佔總 STR 金額 0.09%）。

與資料集 1 類似，資料集 2 中絕大部分的可疑交易報告（STRs）亦係基於可疑情況提出，尤其是可疑指標 1：「缺乏合法或商業上的義務、目的或經濟合理性」。儘管資料集 2 中的前置犯罪整體占比相對較低，但高風險綜合型度假村卻報告了 16 種其他前置犯罪類型，此等類型未見於博奕業之外其他通報機構所提交的 STRs。

3.2.11 新加坡

新加坡的主要風險仍涉及法人濫用、貿易洗錢，以及集團式洗錢（包含網路詐騙）。作為金融中心，新加坡持續對財富管理領域潛在的洗錢風險保持高度警覺。

如財富管理領域洗錢與資恐風險通告所述⁹⁸，金融機構應對高風險客戶與交易保持警覺。尤其是在處理以法人或法律協議為受益對象之財富管理法律結構或安排（例如信託安排）時，應察覺額外的洗錢與資恐風險。此外，金融機構應注意潛在客戶因無法、或不願提供必要的客戶盡職調查（CDD）資訊而撤回申請的情形；並持續監控留意與第三方之間或聲稱商業目的而產生的異常交易量激增、及意外的資金流動，尤其是涉及高風險司法管轄區的交易。

⁹⁶ Anti-Money Laundering Council - Analysis of Suspicious Transactions Associated with Casino Junkets:

http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATED%20WITH%20CASINO%20JUNKETS_FINAL.pdf

⁹⁷ 研究使用來自防制洗錢委員會資料庫所擷取的兩套不同資料集。資料集 1，由敘述欄位中包含關鍵字「博奕中介（junket）」之 STR 所構成，共計 3,308 筆。資料集 2，由四家綜合型度假村（integrated resorts）提交之 STR 構成，共計 4,110 筆，該四家度假村係依據博奕業相關權責機關之更新風險矩陣（涵蓋期間為 2021 年 12 月至 2022 年 9 月），被認定為具有最高洗錢／資恐風險之機構。

⁹⁸ 新加坡金融管理局 - 《財富管理產業之洗錢與資恐風險》：<https://www.mas.gov.sg/regulation/circulars/circular-on-money-laundering-and-terrorism-financing-risks-in-the-wealth-management-sector>

此外，如新加坡《國家資恐風險評估報告》所述，新加坡容易受到境外恐怖分子／恐怖組織／恐怖活動募集與移轉資金之資恐威脅。極端化個人持續對新加坡帶來顯著的資恐威脅。金融機構亦應注意透過勒索軟體（ransomware）、藝術品與古董，以及線上群眾募資機制等新興國際資恐態樣。

新加坡特別注意到群眾募資因其可觸及廣泛的國際群眾籌集資金，成為新興的資恐手法。恐怖分子可能以慈善、或人道援助目的偽裝募集資金，誘使不知情的受害者無意中捐助資恐活動。就此，新加坡於擔任防制洗錢金融行動工作組織（FATF）主席任期期間（2022 年至 2024 年），宣導與群眾募資相關資恐風險的專案，最終於 2023 年 10 月由 FATF 發表《資恐目的之群眾募資》（*Crowdfunding for Terrorism Financing*）報告。

3.2.12 中華臺北

第三方洗錢：近年來，民眾廣泛使用第三方支付業者，由支付服務提供商擔任線上交易買賣雙方之中介機構。除了提升買賣雙方交易之安全性、公平性與可靠性之外，第三方支付業者也為小規模電子商務賣家提供便利的信用卡與虛擬帳戶支付服務，達成普惠金融（financial inclusion）與電子商務發展之目的。然而，第三方支付業者近年來也遭濫用作為洗錢之渠道。犯罪者利用人頭帳戶或空殼公司向第三方支付業者申請金融服務，誘使被害人將資金匯入第三方支付業者提供的虛擬帳戶，作為收取線上交易款項之用途。當資金轉入犯罪者控制之帳戶後，再透過多個帳戶多次轉移，或透過人頭提領現金，藉此產生資金流向之斷點，增加調查追蹤資金流向之困難度。自 2019 年起，涉及第三方支付業者之可疑交易報告（STRs）數量便逐年增加。（2019 年：462 件，2020 年：504 件，2021 年：496 件，2022 年：702 件，2023 年：1,186 件）。（2019 年：462 件，2020 年：504 件，2021 年：496 件，2022 年：702 件，2023 年：1,186 件）

可疑活動指標包括：

- 違反規定：第三方支付業者違反《第三方支付服務業防制洗錢及打擊資恐辦法》之規定，與其他第三方支付業者簽訂合約作為付款方或收款方。
- 快速提領現金或資金轉移：第三方支付業者將資金轉入賣方帳戶後，賣方迅速提領現金或轉移資金，且通常由疑似人頭帳戶之多名個人提領。
- 資本額偏低及營業地址相同：涉及異常交易之第三方支付業者通常資本額異常偏低，且與其他類似公司登記於相同營業地址，引發使用空殼公司之疑慮。
- 缺乏真實線上交易：客戶聲稱經營網路商店，但所提供之網站連結經常無效、或是虛假網站、缺乏購物下單系統，或不願提供網路商店網址。

線上遊戲平台：使用具有交易性遊戲幣的線上遊戲平台，為洗錢開闢新的途徑；犯罪分子以洗錢為目的，藉此利用遊戲內之支付系統購買、和販售虛擬物品或貨幣。

毒品犯罪：毒品相關交易主要涉及現金支付，若涉及跨境或國際交易，犯罪分子則使用另類匯兌系統，例如地下匯兌及人頭帳戶等。犯罪分子與職業洗錢人士亦使用現金走私技巧，如利用旅客跨境攜帶現金交付。為確保安全、降低犯罪集團內部衝突風險及規避執法機關偵察，犯罪集團通常會將人員、毒品與資金之流動分開處理。

在國內毒品交易中，也以現金交易為主，極少數案件涉及以物易物的毒品交換方式。雖然警方常於毒品查緝現場扣押現金，但鮮少有足夠證據證明罪嫌違反《洗錢防制法》。唯當執法機關能證實相關資金係毒品犯罪所得、且資金已流入人頭帳戶時，始能構成隱匿犯罪所得來源之犯罪要件，進而起訴犯罪嫌疑人涉及洗錢罪。然而，若犯罪嫌疑人未轉移或改變毒品犯罪所得，或其行為未有效隱匿犯罪所得來源，則難以依洗錢罪名起訴。

執法人員於查緝行動中扣押證實為毒品犯罪所得之資金。2020 年，調查局扣押 196 萬 9,350 臺幣（約 61,542 美元）及 4 萬 5,673 馬幣（約 9,718 美元）。2021 年，調查局扣押 1,755 萬 3,856 臺幣（約 548,558 美元）及汽車 2 輛。2022 年，調查局扣押 609 萬 8,520 臺幣（約 190,579 美元）及遊艇 1 艘。2023 年，調查局扣押 632 萬 1,400 臺幣（約 197,544 美元）、美元 402 元、汽車 6 輛及遊艇 1 艘。

3.3 防制洗錢及打擊資恐立法、監理或執法措施之成效

3.3.1 加拿大

加拿大於 2023 年修訂《犯罪所得（洗錢）與資恐法》，明確規定以意圖欺騙申報機構之方式結構交易，以致申報機構未向加拿大金融情報中心通報金融交易的行為屬犯罪。此項修法促使加拿大展開新一輪的洗錢案件調查。

3.3.2 庫克群島

2022 年，庫克群島於毒品調查行動中，發現數名作為人頭帳戶的個人將資金分別存入三個不同帳戶，存款金額皆低於現金交易申報門檻 1 萬紐西蘭元（NZD）。這些交易揭露現行申報門檻存在的漏洞，促使政府與銀行業界討論降低現金交易申報門檻。降低現金交易申報門檻之提議已獲得銀行業界、西聯匯款（Western Union）及沃達豐（Vodafone）行動銀行的支持。

3.3.3 中國香港

2023 年中，中國香港建立虛擬資產服務提供商（VASP）之執照制度及監管要求。目前已有兩家已核可的虛擬資產交易平台透過執照升級，得以向零售投資者提供比特幣（BTC）及以太坊（ETH）之交易服務。已核可平台受到證券及期貨事務監察委員會（Securities and Futures Commission, SFC）嚴格的監管，可提供投資者充分保障。此外，證監會亦維持一份「可疑虛擬資產交易平台名單」，列出被認定針對中國香港本地投資者、或宣稱與中國香港有關聯、但未於中國香港取得執照之機構。此名單可作為投資者之早期預警服務，亦有助於提高大眾警覺性。

考量到詐騙集團曾大量使用人頭帳戶收取詐欺款項並進行洗錢，香港警務處（HKPF）與律政司（DOJ）合作，精簡證據蒐集及起訴程序，以加快司法程序。此外，香港警務處與律政司亦制定加重刑罰之適用規範。自此規範施行以來，香港警務處成功使人頭帳戶持有者之判刑平均提高約 20%。

3.3.4 印尼

印尼在其法律審查報告《優化專業通報機構對金融交易報告與分析中心之可疑金融交易報告義務的執行》(Optimizing the Implementation of the Obligation to Report Suspicious Financial Transaction Reports by Professional Reporting Parties to the Financial Transaction Reporting and Analysis Center) 中，辨識出反制措施需要改進的領域。

主要發現

此法律審查辨識出以下問題：專業通報機構在提交可疑金融交易報告時遭遇之障礙；影響通報義務執行最佳化的因素；所需之政策方向。

專業通報機構註冊 GOAML 應用程式遭遇的障礙包括：(i) 印尼金融交易報告與分析中心（PPATK）缺乏權限對專業通報機構實施撤銷許可之制裁措施；(ii) 對律師通報機構而言，因有多個律師協會或組織具有指派律師的權限，使得註冊程序在實務運作上遭遇障礙；(iii) 對財務規劃通報機構而言，目前缺乏明確規範財務規劃師

之任命程序，以及核發執業許可或任命財務規劃師之權責機關；(iv) 財務規劃通報機構中存在以金融服務資訊科技形式營運的財務規劃業者，現行法規對此缺乏明確規範。

影響專業通報機構向 PPATK 通報可疑交易報告的義務，最佳化之因素可分為內部與外部兩類。內部因素與 PPATK 作為監理機關對特定專業通報機構（如律師通報機構及公證人通報機構）之制裁權限不足有關。目前 PPATK 僅能對上述機構實施警告制裁，難以產生直接的嚇阻效果。因此，需要賦予 PPATK 更強的制裁權限，例如撤銷營業執照或相關資格。

最佳化專業通報機構向 PPATK 通報可疑交易報告之政策方向包括：(i) 辦理培訓與宣導，以統一專業通報機構間對相關通報義務之認知；(ii) PPATK 與（有權任命專業通報機構之）監管機關或專業協會加強合作，以落實相關制裁措施；(iii) 建立明確的法律基礎，以監理財務規劃相關業務；(iv) 擴大專業通報機構對服務使用者進行「認識你的客戶」（KYC）之範圍；(v) 研議於專業通報機構所提供之服務活動中，引入以受託人（trustee）概念為基礎之相關法規的可行性。

3.3.5 日本

日本實施之反制措施已促使可疑交易報告（STR）及洗錢案件數量穩步增加。

日本指出，2020 至 2022 年間已偵破的洗錢案件數量持續上升。

已偵破之洗錢案件數

| 類別 | 年度 | | 2020 | | 2021 | | 2022 | |
|--|------|------|------|------|------|------|------|----|
| | 案件數量 | 比例 | 案件數量 | 比例 | 案件數量 | 比例 | 案件數量 | 比例 |
| 已偵破之洗錢案件數 | 600 | — | 632 | — | 726 | — | | |
| 組織犯罪處罰法（Act on Punishment of Organised Crimes） | 597 | 99.5 | 623 | 98.6 | 709 | 97.7 | | |
| 《毒品特別規定法》（Anti-Drug Special Provisions Law） | 3 | 0.5 | 9 | 1.4 | 17 | 2.3 | | |

日本指出，2020 至 2022 年間，受監管機構提交之可疑交易報告數量亦持續增加。

權責機關所提交之STR數量（依業務類型）

| 類別 | 年度 | | 2020 | 2021 | 2022 |
|------------|------|------|---------|---------|---------|
| | 報告數量 | 報告數量 | 報告數量 | 報告數量 | 報告數量 |
| 金融機構 | | | 402,868 | 495,029 | 542,003 |
| 存款機構 | | | 342,226 | 411,683 | 435,728 |
| 銀行及其他 | | | 319,812 | 390,381 | 414,651 |
| 信用金庫、信用合作社 | | | 19,793 | 18,461 | 18,520 |
| 勞動金庫 | | | 300 | 318 | 316 |
| 農林中央金庫等 | | | 2,321 | 2,523 | 2,241 |
| 保險公司 | | | 2,635 | 3,458 | 3,939 |
| 金融商品業者 | | | 17,933 | 19,718 | 19,032 |

| | | | |
|-------------|---------|---------|---------|
| 資金業者 | 25,255 | 35,442 | 45,684 |
| 資金移轉服務業者 | 6,040 | 10,499 | 20,271 |
| 加密資產交換服務業者 | 8,023 | 13,540 | 16,550 |
| 商品衍生性金融商品業者 | 320 | 388 | 318 |
| 貨幣兌換業者 | 252 | 201 | 430 |
| 電子貨幣債權記錄機構 | 5 | 7 | 0 |
| 其他 | 179 | 93 | 51 |
| 融資租賃業者 | 123 | 163 | 71 |
| 信用卡業者 | 29,138 | 34,904 | 41,106 |
| 不動產仲介業者 | 7 | 4 | 11 |
| 貴金屬與寶石交易商 | 63 | 48 | 124 |
| 郵件代收服務業者 | 2 | 0 | 1 |
| 電話代接服務提供業者 | 0 | 0 | 0 |
| 電話轉接服務提供業者 | 1 | 2 | 1 |
| 總計 | 432,202 | 530,150 | 583,317 |

3.3.6 中國澳門

2023年防制洗錢與打擊資恐相關立法與監管措施之發展：

《金融體系法律制度》(Financial System Act , FSA)之修訂：中國澳門於 2023 年修訂之《金融體系法律制度》(FSA) 已於 2023 年 11 月 1 日生效，旨在促進金融業發展，並與國際監理標準接軌。從防制洗錢與打擊資恐觀點而言，該修訂進一步強化金融業洗錢與資恐風險之防制措施，包括強化核准（執照）規定，明確董事會成員、監察人及實際負責業務管理人員，須符合防制洗錢與打擊資恐相關之適格性 (fit-and-proper) 先決條件。此外，亦加重包含防制洗錢與打擊資恐相關違規行為在內之行政罰則，以達成更有效之嚇阻效果。未經核准擅自接受公眾存款、或其他可償還資金之行為已明訂為犯罪，並提高刑度，以有效打擊非法金融活動。

《博奕信貸法律制度》之修：訂為進一步促進新一輪博奕專營權業務的安全及健全發展，中國澳門政府於 2024 年 4 月透過第 7/2024 號法律，加強博奕法律架構。此法修訂博奕業之信用制度，同時廢止先前之第 5/2004 號法律。主要修訂內容包括完善博奕業提供信用之原則、明確博奕業者之法定記錄保存義務、及風險管理機制，並具體規定違規之行政制裁規範，包括罰鍰及限制措施（例如禁止違規業者於最長一年內提供博奕信用）。新法將於 2024 年 8 月 1 日起施行。

《打擊非法博奕法》修訂草案（立法中）：2023 年 12 月，中國澳門政府已向立法會提出《打擊非法博奕法》修訂草案，目前仍處於審議階段，預計於 2024 年內通過。該草案旨在因應博奕相關活動帶來之重大犯罪威脅，透過強化刑事程序，促進博奕業之健全發展。主要修訂內容包括：更明確界定涉及中國澳門博奕結果之非法博奕犯罪行為（例如場邊投注、代理人投注及線上博奕）；擴大對非法網路博奕經營活動之犯罪化範圍（即使相關設施未實體設立於中國澳門）；同時亦加強執法機關對此類犯罪活動之調查權限及執法能力。此次修訂之最終目的在於因應中國澳門博奕業最新犯罪趨勢，提供更有效之刑事嚇阻效果，尤其提高相關犯罪行為之有期徒刑年限。

3.3.7 馬來西亞

修訂版防制洗錢／打擊資恐／打擊資武擴政策文件之發布

馬來西亞國家銀行（Bank Negara Malaysia，馬來西亞中央銀行）近期修訂針對金融機構、指定之非金融事業及人員（DNFBPs），以及非銀行金融機構（NBFIs）之防制洗錢／打擊資恐／打擊資武擴政策文件，並已於 2024 年 2 月正式生效。

此項修訂旨在與防制洗錢金融行動工作組織（FATF）標準接軌，並進一步明確對申報機構之相關要求。主要修訂內容如下：

- 要求申報機構辨識、評估及減輕資武擴之風險，以因應全球逐步增加的大規模毀滅性武器與資武擴之威脅，並確保申報機構不會在不知情的狀況下支持被指定制裁之人士。
- 擴大對金融集團之定義，新增對DNFBP（指定之非金融事業或人員）團體及其他DNFBP架構之定義，並要求DNFBP團體應採用集團層級方案，以辨識並管理其洗錢／資恐／資武擴風險。
- 強化對貨幣服務業法人客戶之非面對面業務關係相關要求，以確保有效辨識及驗證法人客戶身分。

作為馬來西亞迅速有效打擊線上金融詐欺行動之一環，該國於 2022 年 10 月設立國家詐騙應變中心（National Scam Response Centre，NSRC）。

截至 2023 年 12 月，NSRC 已辨識出逾 60,000 個疑似人頭帳戶，金融機構因此得以迅速採取措施，防止詐欺資金進一步遭層層轉移與分散。透過與金融機構合作，皇家馬來西亞警察（RMP）已針對線上金融詐欺的詐欺犯罪開立 8,754 件調查案件，並凍結疑似詐欺收款帳戶內共計 6,900 萬馬幣（約 1,460 萬美元）。

為深化 NSRC 之功能，馬來西亞將透過與銀行及馬來西亞支付網路有限公司（Payments Network Malaysia Sdn Bhd, Paynet）合作，推出國家詐欺入口網站（National Fraud Portal, NFP），作為馬來西亞的共享支付基礎設施。該入口網站將配備進階功能，可快速追蹤被盜取資金，並建立完整的人頭帳戶資料庫。透過更全面且高品質的資訊存取，此功能預期將提高金融機構分析、與辨識人頭帳戶之能力，協助決定適當的應對措施。

3.3.8 新加坡

自 2023 年起，為有效因應不斷變化之犯罪形勢，新加坡已強化其防制洗錢／打擊資恐（AML/CFT）相關立法措施。

新加坡於 2023 年修訂了《貪污、販毒及其他嚴重罪行（沒入利益）法》（Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, CDSA）及《濫用電腦法》（Computer Misuse Act, CMA）。此次修訂新增多項規定，以強化執法機關防制洗錢之能力。新法授權執法機關針對涉及洗錢計畫之人頭帳戶持有者、以及協助他人保留犯罪活動與毒品犯罪所得之人士，採取法律行動。此修訂旨在嚇阻任何協助或促使他人實施犯罪行為之人士。

案例研究 # 96：強化新加坡針對防制洗錢／打擊資恐措施以打擊詐欺相關之人頭帳戶犯罪

網路詐騙犯罪

2024 年 9 月，40 位人士因涉及與詐欺相關之人頭帳戶活動，依據 2023 年修訂之 CDSA 及 CMA 所新增之罪名，而遭到法院起訴。這些新罪名目的在遏止協助詐欺、轉移犯罪所得以及濫用新加坡數位身分服務「Singpass」之行為而設，並於 2024 年 2 月正式生效；主要針對將本人銀行帳戶控制權、或其 Singpass 證資料交付或揭露予他人，以致他人得以利用該帳戶或認證資料進行詐欺及洗錢行為之人士。

此外，新加坡判刑諮詢團（Sentencing Advisory Panel）亦發布指引，建議對涉及將銀行帳戶或 Singpass 認證資料交付他人使用以進行詐欺犯罪之行為，應常態性地判處較重之監禁刑責。

來源 - 新加坡

2023 年《網路犯罪危害法》（*Online Criminal Harms Act*）：該法案授權新加坡警察部隊（SPF）阻斷犯罪者透過網路招募人頭帳戶，以進行洗錢之行動。新加坡警察部隊被授權得要求線上服務業者，阻止可疑詐欺帳戶（或內容），與新加坡境內使用者互動或接觸。

2024 年《防制洗錢與其他相關事務法》（*Anti-Money Laundering and Other Matters Act*）：此法進一步加強跨部門間之資訊共享，以更有效地偵測洗錢、資恐及資武擴活動；允許執法機關對國外發生的嚴重環境犯罪之洗錢行為展開調查；增強執法機關追查及起訴洗錢罪行之能力；並允許法院在符合以下三種情形之一時，得以下令出售與可疑犯罪行為相關聯之被扣押或限制處分財產：

- 各方當事人同意拍賣。
- 財產價值可能減損，或維護財產將涉及不合理成本。
- 拍賣符合司法利益。

2024 年《防範詐欺保護法案》（*Protection from Scams Bill*） 此法案授權新加坡警察部隊（SPF）向銀行發出限制令（Restriction Orders, ROs），對於正在遭受詐欺但拒絕相信自己已遭詐欺之目標個人，暫時限制其銀行交易。限制令將包括以下銀行服務。限制令初始有效期間為 28 天，以為新加坡警察部隊提供充足時間採取後續行動（例如繼續與當事人及其親屬溝通、蒐集進一步證據說服當事人，或促使當事人採取必要的銀行防護措施）來阻止持續之詐欺行為。於 28 天限制期屆滿後，若警方評估認定該人士仍有遭詐欺之風險，則可將限制令逐次延長最多 28 天。受限制之銀行業務包括：從該受害人銀行帳戶轉出之所有資金轉移（包含網路銀行、行動銀行以及臨櫃交易），資金將無法轉出至其他帳戶。此外，新加坡亦將推出一套機制，允許受限當事人向新加坡警察部隊申請使用本人帳戶內資金，以支付正當用途之需求（如日常生活開銷及繳納帳單）。

4 - 資武擴之手法與趨勢

本節之態樣報告提供包括聯合國區域間犯罪與司法研究所（United Nations Interregional Crime and Justice Research Institute, UNICRI）在資武擴相關工作之概要簡介；亦涵蓋電子期刊《1540 指南》（1540 Compass）之報告，以及其就東南亞地區資武擴問題所撰寫之觀察研究報告。此外，本節亦包含亞太防制洗錢組織（APG）成員所執行之資武擴風險評估，以及其為降低相關風險而發布之相關出版品與指引資訊。

資武擴

籌集資金是武擴活動的核心環節。犯罪分子經常利用不同司法管轄區法律與實務系統中的漏洞，以募集並移轉資金，進而執行相關金融交易。資武擴的行動者亦使用相同方式進行資金流動。金融措施是司法管轄區用以對抗武擴活動最有效的工具之一：

- 預防性措施可增加犯罪分子募集與移轉資金的難度，進而抑制武擴網路的量能。
- 金融情資可預警非法移轉敏感物資之企圖。透過金融機構提交之可疑交易報告，可及時偵測並攔截相關貨物之運送。
- 每一筆貨物移動皆伴隨相關金融交易：透過金融調查可追蹤資金流向，進一步核實交易申報內容，分析武擴網路，並辨識相關協助者。

FATF 有關打擊資武擴之建議，透過明訂各司法管轄區須落實之具體要求，使聯合國安全理事會各項決議之金融制裁規定更具可執行性。各司法管轄區必須建立必要的法律授權，並指定負責即時落實及執行目標性金融制裁（TFS）之權責機關。⁹⁹

FATF 建議各司法管轄區針對自身所面臨之特定威脅情境，資武擴量身訂定資武擴風險評估及相關風險抵減策略。此等威脅可能來自該司法管轄區自身環境，亦可能因為與高風險司法管轄區接觸所引發。完整掌握該等動態，可以幫助各司法管轄區辨識可能面對之資武擴態樣，並進一步確認需要強化管控之高風險之產業或通路。

目標性金融制裁（TFS）適用於下列人士、或實體：

- 代表或依據指定制裁之個人、或實體指示行事。
- 由指定制裁之個人、或實體所擁有或控制。
- 協助指定制裁之個人、或實體規避制裁或違反決議條款。

實施目標性金融制裁後，意圖規避制裁者可能利用金融與貿易服務以隱匿其等涉入武擴活動之事實；包括利用貿易融資產品、乾淨付款（clean payment）服務，以及資金匯款服務等，以便採購並支付武擴敏感物資。

⁹⁹ FATF執行秘書 David Lewis 關於「打擊資武擴之最佳實務與指引－強化權責機關之行動」之講話紀錄：<https://www.fatf-gafi.org/en/publications/Fatfgeneral/Speech-psl-political-meeting-may-2018.html#:~:text=Financial%20intelligence%20provides%20advance%20warning,transaction%20by%20financial%20institutions.>

4.1 觀察員組織之倡議

皇家聯合軍事研究所（Royal United Services Institute，RUSI） - 《銀行業打擊資武擴與制裁管控之挑戰》

皇家聯合軍事研究所之《銀行業打擊資武擴與制裁管控之挑戰》（*Challenges for Counter-Proliferation Finance and Sanctions Control in Banking*）報告¹⁰⁰ 探討全球金融體系因國際制裁與資武擴議題，所面臨日益複雜之挑戰。各國政府必須建立監管架構以打擊資武擴、並維持金融體系完整性，但有效落實這些規範則是金融機構之主要責任。

然而，金融機構在落實過程中亦面臨若干主要挑戰：

- 監管期望與實務落實間之落差 - 金融機構的實際操作與監理要求之間仍有距離，往往無法清楚掌握如何在其營運範圍內有效適用國際及國內制裁規定。
- 資料品質不足及資訊取得受限 - 金融機構因缺乏取得高品質資料之管道，導致難以有效偵測、及防止資武擴及制裁規避行為。因此，金融機構迫切需要提升資訊共享機制，並採用如分散式帳本技術（Distributed Ledger Technology, DLT）等先進科技，以強化資料透明度。
- 專業知識不足 - 銀行業往往缺乏必要的專業能力，因應複雜且不斷變化的制裁情勢。金融機構必須持續接受權責機關之教育訓練與指導，才能應對快速變動的監管要求，並確保法令遵循。
- 銀行業資武擴與制裁風險評估之差異性 - 不同銀行對資武擴及制裁相關風險之評估與管理方式缺乏一致的標準，此等差異可能使全球金融體系暴露潛在弱點，進而影響制裁措施之有效執行。

建議

為解決上述挑戰，此報告提供以下建議措施：

- 監理指引與支援 - 權責機關應向金融機構提供清楚且務實之指引，以協助金融機構解讀並落實制裁規定；包括分享最佳實務範例、逐步說明落實流程，以及提供產業特定建議，協助銀行有效遵循複雜法規。
- 促進資訊共享與科技應用 - 報告建議宣導採用分散式帳本技術（DLT）及其他先進科技，以改善資料品質及取得能力。此外，權責機關亦應考量強制使用「協調制度（Harmonised System, HS）編碼」標註軍民兩用貨品，以協助金融機構偵測可疑交易活動。
- 培育專業能力 - 權責機關應投注資源，加強金融機構內部專業能力培訓，包括提供產業特定指引，並協助交易監控工具之參數設定與校準。
- 風險評估之標準化 - 銀行業對資武擴與制裁之風險評估亟需標準化指引，權責機關應透過檢視分析，確認銀行間之差異，並宣導一致性之風險管理方式。

結語

此報告強調政府與金融機構間之合作，對強化打擊資武擴及制裁管控之效能至關重要。透過有效因應報告中所辨識之挑戰，並落實所提出之建議措施，金融機構將更能保障全球金融體系免受資武擴與制裁規避之風險。

¹⁰⁰ 皇家聯合軍事研究所 - 《銀行業打擊資武擴與制裁管控之挑戰》<https://www.rusi.org/explore-our-research/publications/special-resources/challenges-counter-proliferation-finance-and-sanctions-control-banking>

聯合國區域間犯罪與司法研究所（UNICRI）-《1540指南》

聯合國安全理事會第 1540 號決議（UNSCR 1540）於 2004 年 4 月 28 日被一致通過，為維護全球和平與安全的關鍵基礎。然而，各國在理解、落實及適應該規定上仍存有歧見。有鑑於此，聯合國區域間犯罪與司法研究所（UNICRI）重新啟動《1540 指南》（1540 Compass）電子期刊。¹⁰¹

《1540 指南》是一份致力於推廣聯合國安理會第 1540 號決議（2004 年）（UNSCR 1540）及其後續決議之目標、提高認知與落實措施的電子期刊。該期刊旨在成為防制大規模毀滅性武器（WMD）擴散議題上可信賴之知識來源、分析平台及對話管道；促進聯合國成員國、學術專家、政策制定者、實務工作者，以及所有關注 1540 決議相關議題之人士，共同分享深入的知識交流、精闢的分析及有意義的對話。

《1540 指南》對於參與防制武器擴散工作的政策制定者、實務工作者與學術界人士而言，是寶貴的參考資源。該期刊的目標是透過提供知識交流與對話平台，支援聯合國安理會第 1540 號決議之持續落實，並為全球安全盡一己之力。

2024 年 4 月號

2024 年 4 月出版之《1540 指南》適逢聯合國安理會第 1540 號決議通過 20 週年。該決議為全球防止非國家行動者取得大規模毀滅性武器（WMD）及運載工具的重要國際性文件。由聯合國區域間犯罪與司法研究所（UNICRI）重新啟動的此期刊，旨在促進各界對話，分享該決議執行的最佳實務經驗。

主要內容及主題：

- 本期刊登多篇文章、專訪及時間軸回顧，探討 1540 號決議過去 20 年在防制武擴工作上的影響及實施上的挑戰。
- 專訪首任「1540 委員會」主席 Mihnea Motoc 大使及現任主席 José Javier De La Gasca 大使，提供有關決議歷史沿革及未來方向之觀點，討論決議通過時的地緣政治背景、施行過程的挑戰，以及面對全球威脅演變下，提升決議成效的策略。
- 本期亦探討 1540 號決議與其他防制武擴倡議之間的關聯性，凸顯其間之協同作用及可進一步改進之處。此外亦審視「1540 委員會」在協助成員國司法管轄區、提升透明度、與宣導技術援助之角色。

挑戰與建議：

- 執行 1540 號決議的過程面臨諸多挑戰，包括各成員國之間需加強協調，軍民兩用（dual-use）技術管理之複雜性，以及非國家行動者持續造成的武擴威脅。
- 強化決議效能的建議措施，包括改善資訊共享、加強國際合作、並在各國國內宣導更完善的法律架構。此外，亦強調向開發中司法管轄區提供技術協助與能力建構的重要性。

2024 年 9 月號

2024 年 9 月出版之《1540 指南》包含三篇與資武擴相關的文章：

- 第 1540 號決議（2004 年）與資武擴之關係

第 1540 號決議（2004 年）及其後續決議確立安理會在打擊資武擴議題上的基本要求。打擊資武擴（CPF）對於防制大規模毀滅性武器（WMD）擴散至關重要，惟 2022 年綜合審查報告顯示，各國在 2022 年資武擴規定的落實程度並未較 2016 年明顯提升。儘管「1540 委員會」尚未提供此方面之具體指引，但安理會在後續多個 1540 號決議中均肯認 FATF 之指引，顯示 FATF 可望於此領域扮演重要角色。因此，發表一份 1540 號決議之資武擴執行指引將會是好的開始。

¹⁰¹ 聯合國區域間犯罪與司法研究所（UNICRI）-《1540指南》：<https://unicri.it/Publications/Magazine-1540%20Compass>

- 認識資武擴風險評估

防制洗錢金融行動工作組織（FATF）第 1 項建議之修訂，使國際社會重新關注對大規模毀滅性武器（WMD）擴散活動之資金支持相關風險的評估工作，這代表從過去以規則基礎（rule-based）轉型為以風險基礎（risk-based）防制方法的重要轉折點。文章指出，儘管資武擴風險評估之議題本質複雜且製作風險評估面臨諸多挑戰，各國權責機關及民間部門仍不應僅限於滿足 FATF 標準之合規要求，而應更廣泛地進行資武擴風險評估。雖然 FATF 第 1 項建議著重於聯合國針對 WMD 擴散的目標性金融制裁措施，但其他可能存在的資助 WMD 計畫之風險，包括違反聯合國安理會第 1540 號決議（2004 年）之情形，亦不容忽視。

- 聯合國安理會第 1540 號決議（UNSCR 1540）與間接資武擴

在過去二十年間，聯合國安理會第 1540 號決議（UNSCR 1540）對防止非國家行動者取得 WMD 之擴散活動扮演重要角色。然而，該決議對於資助 WMD 擴散活動之規範不夠清晰與具體，尤其是對奢侈品貿易等間接資助行為的處理上更顯不足。為提高該決議之實質效能，有必要針對上述模糊地帶作出明確規範，並在 1540 號決議框架下，擴展資武擴之涵蓋範圍，以強化國際間合作及能力建構等倡議。

此外，本期內容亦肯認公民社會在防制大規模毀滅性武器擴散所扮演之關鍵角色，並特別刊載兩篇文章，探討產業界與學術界等利害關係人如何與政府及國際組織合作，以確保該決議之有效落實。

聯合國區域間犯罪與司法研究所－《化學、生物、放射性及核子武器（CBRN）資武擴：東南亞觀察》

聯合國區域間犯罪與司法研究所（UNICRI）所發表之《化學、生物、放射性及核子武器（CBRN）資武擴：東南亞觀察》，（*CBRN Proliferation Financing:A Perspective from Southeast Asia*）報告¹⁰²是 UNICRI 透過專案形式執行的結果，旨在提高各方對化學、生物、放射性及核子武器（CBRN）資武擴風險之理解，增強對相關國際規範的認識及遵循，並辨識國家及區域層級的優先行動，以增強各司法管轄區有效應對資武擴風險之能力。此報告整合UNICRI的研究及各方諮詢之成果。

報告共分兩大部分：第一部分概述東南亞地區正暴露於資武擴風險，尤其著重於大規模毀滅性武器（WMD）採購計畫、WMD 擴散網路，以及規避防制武擴制裁計畫之資金募集活動相關之威脅。資武擴第二部分則提出資武擴風險抵減之建議措施。

報告指出東南亞地區在北韓（DPRK）WMD 擴散野心下處於獨特之風險位置。地理上東南亞鄰近北韓，且具備廣闊的海域邊界，使該地區容易被北韓之武擴網路利用。此外，東南亞經濟體日益發展的貿易與金融中心，加上各國積極宣導核能計畫、化學及生技產業，均吸引 WMD 擴散者試圖利用企業經營者提供之服務及技術協助達成犯罪目的。資武擴行動者亦藉由區域內某些司法管轄區缺乏先進之防制資武擴措施，在東南亞地區秘密從事相關活動。

此報告亦簡略說明航運業資武擴之情形。衛星圖像及各成員國提供的資訊顯示，北韓持續違反聯合國安理會所訂定之貿易限制規定，特別是超額進口精煉石油產品，並出口受制裁商品如煤炭與砂石等。航運進出口業務中所使用之複雜規避策略包括船對船轉運（ship-to-ship transfers）、濫用船舶自動識別系統（AIS）、使用偽造文件、及規劃企業架構以掩蓋船舶管理或所有權等。

報告強調，當某司法管轄區有公司之董事或股東參與經營、或擁有從事違反制裁活動之船舶時，即暴露於資武擴風險。此外，提供船舶營運所需之各項服務，如保險服務、船員供應服務、船舶分級或認證服務等，亦將該司法管轄區暴露於資武擴風險之中。依據國際法規定，船舶必須註冊，而登記船籍之國家（船旗國）決定船舶之國籍，進而允許該船舶航行國際。船籍登記機構須認證船舶符合特定之航行標準。向受制裁之指定船舶，或與指定個人或實體有關聯之船舶，提供此類型之技術援助，已成為非法貿易活動及北韓（DPRK）籌措資金之重要手段。

¹⁰² 聯合國區域間犯罪與司法研究所（UNICRI）-《化生放核武器（CBRN）資武擴：東南亞觀察》：<https://unicri.it/sites/default/files/2023-10/CBRN%20Proliferation%20Financing.%20A%20Perspective%20from%20Southeast%20Asia.pdf>

路易斯·戴寇克 (Louis de Koker) - FATF 打擊資武擴標準：私部門執行上的挑戰

路易斯·戴寇克為澳洲樂卓博 (La Trobe) 大學法學院法學教授及該校LawTech研究團隊協調人。

此研究¹⁰³探討受規範之機構在落實 2020 年防制洗錢金融行動工作組織 (FATF) 標準修正案時所面臨的挑戰，該修正案旨在加強打擊資助大規模毀滅性武器 (WMD) 之擴散。修正後之資武擴標準要求各司法管轄區與通報機構執行風險評估，並對風險較高所在，進一步強化其風險控制措施。

本研究辨識出四大類挑戰：

- 「資武擴」不同定義之間的落差與協調。
- 在威脅資訊不足、地緣政治與地緣經濟能力不足的情況下，資武擴如何進行資武擴之風險評估與風險抵減。
- 在缺乏商品資訊情況下，如何有效監控貿易相關交易，以避免資武擴的目標性金融制裁 (PF-TFS) 活動。
- 在不允許於風險較低情況下簡化法令遵循措施情形，如何有效率並有效果地打擊資武擴之目標性金融制裁。

此外，此研究亦指出一個核心挑戰，即欠缺關於新措施實施之目的及策略目標之周全政策考量。

此研究建議，各國 PF-TFS 國家策略應包含以下要素：

- 採用適合國家整體防制武擴政策的「資武擴」明確定義。
- 採取分階段推行方式，首階段先聚焦於經挑選、具備相應能力之高風險機構。
- 採用協作式方法，資武擴將特定機構與涉及資武擴之相關政府權責機關集合，共同探索最佳實務，以支持有效及有效率之法令遵循措施。
- 適當運用 FATF 之低風險豁免規定，使低風險機構得以免除 PF-TFS 風險管理義務。
- 透過支援部門別風險評估及合規技術發展，促進 PF-TFS 合規作業。
- 基於機構擁有資訊之有限性，調整法令遵循要求。
- 監測實施成效及其預期（與預期外）之影響，並就進展定期回報。

打擊資武擴 (CFP) 是一項複雜任務，目前焦點主要集中於協助各司法管轄區落實 FATF 建議及進行資武擴風險評估。但對於私部門在執行有效果且有效率的合規措施時所面臨的兩難處境卻關注不足，而通報機構在以風險為導向之資武擴目標性金融制裁 (PF-TFS) 中卻扮演重要角色。因此，監理機關現階段應更深入了解私部門所面臨的實際限制，以及提供其等有效果且有效率地履行職責所需之協助，才能避免對企業營運造成不當干擾，或為顧客及社會製造不合理的額外成本負擔。

FATF 建議為最低標準，各司法管轄區與受規範機構因此得採行高於此標準之政策、規定及法令遵循實務，以服務更廣泛之打擊武擴與裁軍目標。鑑於當前全球大規模毀滅性武器風險上升，此作法實值得各界認真考量。

¹⁰³ The FATF's Combating of Financing of Proliferation Standards: 資武擴；濫用法人與法律協議 Private Sector Implementation Challenges: APG成員國落實FATF虛擬資產要求之狀況 https://link.springer.com/chapter/10.1007/978-3-031-59543-1_6

4.2 近期有關資武擴手法及趨勢之風險評估、研究或調查報告

4.2.1 澳洲

澳洲於 2022 年發表《澳洲資武擴國家風險評估》（*National Risk Assessment on Proliferation Financing in Australia*），指出澳洲目前面臨的主要資武擴威脅包括：

- 濫用澳洲金融服務及金融基礎設施，以取得軍民兩用物資（dual-use goods）並規避制裁。
- 濫用設立於澳洲之公司架構，以協助資武擴及規避制裁。
- 利用澳洲籍或第三國籍人士，協助資武擴行動並規避制裁。
- 利用澳洲公民資武擴行動者獲取及輸出敏感技術與知識。
- 使用指定之非金融事業或人員（DNFBPs）協助資武擴及規避制裁。

4.2.2 日本

日本於 2024 年 3 月發布首份《資武擴國家風險評估報告》（*National Risk Assessment of Proliferation Financing*），此報告由日本防制洗錢／打擊資恐／打擊資武擴跨部會委員會（Inter-Ministerial Council for AML/CFT/CPF Policy）所編纂。主要發現包括：

- 日本承認自身可能暴露於以下威脅：
 - 行動者透過貿易、服務及網路攻擊竊取資金。
 - 行動者透過軍民兩用物資交易及非法船對船轉運，竊取敏感技術與物資。
 - 行動者利用複雜結構與不透明的實質受益人（beneficial owner）規避監管。
- 日本之弱點因素包含與北韓地理位置接近，且為全球重要的國際金融中心、工業重鎮，且為開放經濟體。
- 透過相關立法，以及政府機關與私部門、外國與國際機構間的緊密協調等方式的抵減措施，日本致力降低前述風險。

4.2.3 馬來西亞

馬來西亞於 2021 年完成首次《資武擴風險評估》（Proliferation Financing Risk Assessment, PFRA），目前正透過國家防制洗錢協調委員會（National Coordination Committee to Counter ML）修訂並更新 2023 年度版以防制洗錢。此次更新《資武擴風險評估》旨在透過辨識金融業與指定之非金融事業或人員（DNFBPs）等部門可能遭利用以進行資武擴、或規避聯合國安理會制裁的主要漏洞。此外，此評估亦透過制訂適當的策略與建議措施，以抵減所發現的風險與弱點，強化馬來西亞整體打擊資武擴的架構。

4.2.4 菲律賓

菲律賓貿易暨工業部戰略貿易管理辦公室（Department of Trade and Industry - Strategic Trade Management Office, DTI-STMO）及防制洗錢委員會（AMLC）目前正與其他政府及執法機關合作，即將完成首次《資武擴國家風險評估》（PFNRA）。此評估旨在透過檢視洗錢前置犯罪引發之威脅、部門特定威脅、及部門特定弱點，以評估菲律賓國內整體資武擴風險。涵蓋範圍包括四個主要部門，即政府、戰略性貨品出口業者、金融機構（FI）及指定之非金融事業或人員（DNFBP）。

4.2.5 新加坡

資武擴風險仍為新加坡之重要優先關注議題，其中尤以濫用空殼公司、及掛名公司為關鍵風險領域。此外，其他風險領域還包括使用虛假文件，以及新加坡作為國際運輸與轉運中心所帶來的潛在弱點。

新加坡持續透過「風險與態樣跨機構小組（Risks and Typologies Interagency Group, RTIG）」辨識與檢討洗錢、資恐及資武擴之風險。相關權責機關亦會透過產業座談及權責機關發表之指引文件，向產業界傳達資武擴風險之重要訊息。

目前，新加坡亦正透過「資武擴國家風險評估」更新對資武擴風險的瞭解，預計於 2024 年公布。為確保國家風險評估之全面性並符合 FATF 建議之要素，此次評估邀集相關執法機關（包括金融情報中心）及監理機關參與。

此外，新加坡「防制洗錢／打擊資恐產業夥伴計畫（AML/CFT Industry Partnership）」旗下特別成立一個工作小組，徵求金融機構（FIs）及指定之非金融事業或人員（DNFBPs）意見，以協助本次資武擴國家風險評估。該工作小組亦預定於 2024 年發布一份有關資武擴之最佳實務指引，以提升產業界對資武擴風險的瞭解與應對能力。

4.2.6 中華臺北

在中華臺北既有與北韓（DPRK）相關之資武擴案件中，最常見之態樣為透過中華臺北油品公司掌控之第三國籍船舶，在公海上將石油轉運給北韓船舶，或將石油販售予其他司法管轄區之船舶，再由該船舶轉售予北韓受制裁船隻。此外，亦曾有中華臺北國民自北韓購買無煙煤，再轉售予其他司法管轄區以進行資武擴之案例。

資武擴在中華臺北國民涉及之資武擴案件中，石油產品仍為最常交易之商品。此等人士通常為船運公司之代表或實質受益人，在報關出口申報時，常提供虛假出口資訊（如虛假目的港）。石油產品則於公海進行交易，或運載至公海後透過船對船轉運移交予北韓相關船隻。

繼「北斗星號」（Polaris）油輪案之後，財政部關務署設立「ZZZ99」作為公海交易報關代碼。許多從臺中自由貿易港區出發之船舶將石油運往公海。因此，自 2023 年 7 月 1 日起，中華臺北對於從自由貿易港區出口石油產品至公海實施全新之報關規定。當業者在公海進行油品交易且無法確認船舶最終目的地之司法管轄區時，若於完成出口報關時已知交易對象，即須提供相關石油交易資訊，包括油品交貨之時間與位置（經緯度）、船舶名稱及 IMO（國際海事組織）船舶識別編號。若出口時尚未確認交易對象，則業者須於返港後補充申報相關交易資訊，供權責機關進一步查核。

分析相關資武擴案例顯示，由中華臺北油品公司掌控之船隻，在中華臺北、北韓附近或公海進行油品轉運活動時，主要交易對象為非北韓籍船隻。這些船隻本身並未受制裁，且許多船員亦非中華臺北國民。案件主謀通常具有國際貿易經驗，並運用境外公司掩蓋交易事實，因此其企業結構通常高度複雜。此外，犯罪分子亦利用合法貿易掩飾非法交易活動。多數被查獲之涉案人曾成功與北韓進行至少一次交易，並利用境外帳戶轉移貨款，以避免資金遭執法機關追查。中華臺北執法機關面臨之一大挑戰，在於《資恐防制法》第 9 條第 1 項第 1 款存有主觀認定要件，需證明嫌疑人係「明知」與受制裁對象交易，然而使用中介人之情形卻增加此認定之困難度。

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

4.3.1 庫克群島

庫克群島向金融機構及指定之非金融事業或人員（DNFBP）、虛擬資產服務提供商、或其他部門（如航運業）之指引資料，以協助辨識、評估及降低規避制裁與資武擴風險。

金融情報中心透過庫克群島外交與移民部（Cook Islands Ministry of Foreign Affairs and Immigration），向金融機構及指定之非金融事業或人員（DNFBPs）提供聯合國制裁之個人與實體名單。

4.3.2 中國香港

聯合財富情報組（JFIU）定期向通報機構發布可疑交易報告（STR）之季度分析及警示訊息，並發表資武擴主題策略分析報告，促進情資交流，宣導執法行動，並提供制定資武擴法規與政策之參考。

4.3.3 日本

日本於 2024 年 3 月公布其首次《資武擴國家風險評估報告》¹⁰⁴。依據此報告規定，包括銀行、資金移轉服務業者在內之相關法規涵蓋部門，須考量此報告內容，針對自身暴露於資武擴風險之情形，執行風險評估。此外，包含指定之非金融事業或人員（DNFBP）在內的其他私部門，亦應辨識上述風險並的風險抵減措施。

4.3.4 菲律賓

在貿易管制方面，菲律賓貿易暨工業部戰略貿易管理辦公室（DTI- STMO）發布以下指引：

- 公布《國家戰略性貨品清單附錄 3》¹⁰⁵：《國家戰略物資》（Nationally Controlled Goods），規範基於國家安全、外交政策、反恐、犯罪控制及公共安全之單邊管制貨品。附錄 3 涵蓋聯合國安理會決議 1718 號決議（2006）、2231 號決議（2015）及其後續決議所列貨品，為禁止與北韓（DPRK）及伊朗（Iran）進出口之物項。
- 發布貿易暨工業部《備忘錄通告第 20-13 號》（DTI Memorandum Circular 20-13）¹⁰⁶，採用聯合國安理會（UNSC）之「個人與實體綜合名單」，作為戰略貿易管理辦公室（STMO）之「禁止交易對象名單」（List of Prohibited Users），有效禁止任何人與該名單所列對象進行戰略性貨品貿易。
- 菲律賓貿易暨工業部第 21-06 號備忘錄通函¹⁰⁷，規定中介（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。

¹⁰⁴ 日本財務省 - 《日本資武擴國家風險評估》(暫譯): https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/20240312.html

¹⁰⁵ 貿易暨工業部 - 《國家戰略性貨品清單附錄 3》: <https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Policies/Annex%20III.pdf>

¹⁰⁶ 貿易暨工業部 - 《備忘錄通告第 20-13 號》https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/e-library/Laws+and+Policies/140420_MC20_13.pdf

¹⁰⁷ 菲律賓貿易暨工業部 - 《備忘錄通告 21-06》: <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>

- 菲律賓貿易暨工業部戰略貿易管理辦公室（DTI-STMO）依據菲律賓防制洗錢委員會（AMLC）第 5 號監理公告《解除名單登錄與解凍程序指引》（Regulatory Issuance No. 5 – Guidance for De-Listing and Unfreezing Procedures）¹⁰⁸，授予存取遭凍結資產之授權，俾使當事人得以履行先前簽訂契約之應付款項。此項授權僅限 DTI-STMO 確認該契約並未涉及聯合國安理會決議第 2231 號（2015）及其後續決議所列之禁止物項、融資協助、中介經紀或其他服務，且該付款亦非直接或間接支付予受上述措施制裁之個人或實體時，方得准許。

在宣導活動與提升盡職調查方面，DTI-STMO 發布以下資料：

- 舉辦多場宣導活動，提醒受規範之利害關係人，與受制裁之個人或實體進行交易可能面臨之潛在風險。此類宣導活動包括 DTI-STMO 一對一輔導會談、特定產業之專門宣導，以及政府與產業共同參與之公開座談會。
- 此外，DTI-STMO 亦針對終端用戶提供商業諮詢建議，以確保企業符合制裁實施國所要求之規定。截至 2023 年為止，DTI-STMO 已提供超過 10 宗未來商業活動、或新外國業務夥伴相關契約之諮詢服務。
- 部分公告及通知已發布於貿易暨工業部官方網站，包括：
 - 2023 年 10 月公告 - 《「出口執法五國」發布聯合指引反制俄羅斯規避制裁行為》¹⁰⁹。
 - 2022 年 3 月 8 日公告：《有關特定國家單邊實施之制裁措施。》¹¹⁰。
 - 對可能與受制裁之個人或實體交易之所有人士發布之警示公告¹¹¹。
 - 《企業交易常見紅旗指標之指引，協助公司審查交易並確保遵守《戰略貿易管理法》(Strategic Trade Management Act) 規定》¹¹²。
 - 《受限交易對象名單查核指引》，為 DTI-STMO 《備忘錄通告 20-13 號》（2020 年）《禁止終端用戶名單》之補充指引¹¹³。

在強化涉及資武擴之目標性金融制裁相關人員與機構能力方面，已進行以下活動：

- 打擊武器擴散調查方法與菲律賓戰略貿易管理法執行工作坊（Counter-Proliferation Investigative Methods and Enforcing Philippine Strategic Trade Management Act Workshop）
- 目標性金融制裁執行工作坊（TFS Implementation Workshop）
- 資武擴金融情報中心打擊資武擴研習：處理俄羅斯規避制裁之金融活動
- 防制北韓（DPRK）武器擴散及制裁規避論壇（Forum on Countering Democratic People's Republic of Korea (DPRK) Proliferation and Sanctions Evasion）
- 北韓制裁執行情境桌上演練（Tabletop exercise of DPRK-related sanctions implementation）

菲律賓防制洗錢委員會（AMLC）亦發布 2021 年版《制裁指引》（Sanctions Guidelines）¹¹⁴，主要針對恐怖主義、資恐與資武擴相關之目標性金融制裁，該指引詳述適用於資恐與資武擴之各項制裁措施與法律規定。

¹⁰⁸ 菲律賓防制洗錢委員會 - 《監理公告第 5 號 - 解除名單登錄與解凍程序指引》：

<https://dtiwebfiles.s3.ap-southeast-1.amazonaws.com/Advisories/Guidance+for+De-listing+and+Unfreezing++PF+TFS.pdf>

¹⁰⁹ 貿易暨工業部 - 2023 年 10 月公告 - 《「出口執法五國」發布聯合指引反制俄羅斯規避制裁行為》：<https://dtiwebfiles.s3.ap-southeast-1.amazonaws.com/STMO/Announcements/October+2023+-+Sanctions+Advisory.pdf>

¹¹⁰ 貿易暨工業部 - 2022 年 3 月 8 日公告 - 《關於部分國家之單邊制裁》（On unilateral sanctions imposed by certain states）：

<https://dtiwebfiles.s3.ap-southeast-1.amazonaws.com/STMO/Announcements/SanctionsMarch2022.pdf>

¹¹¹ 菲律賓貿易暨工業部 - 《對可能與受制裁個人及實體交易之所有人士之警示公告》：https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Announcements/STMO+Advisory_Sanctioned+Individual+and+Entities.pdf

¹¹² 菲律賓貿易暨工業部 - 《交易常見紅旗指標指引：協助企業審查交易並遵守戰略貿易管理法》：<https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Publications/red+flags.pdf>

¹¹³ 菲律賓貿易暨工業部 - 《受限交易對象名單查核指引：DTI-STMO 備忘錄通告 20-13（2020 年）禁止終端用戶名單之補充指引》DTI-STMO 備忘錄通告 20-13（2020 年）禁止終端用戶名單之補充指引]：<https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Publications/restricted-party-screening-2.pdf>

¹¹⁴ 菲律賓防制洗錢委員會 - 《2021 年制裁指引》<http://www.amlc.gov.ph/images/PDFs/2021%20SANCTIONS%20GUIDELINES.pdf>

此外，菲律賓防制洗錢委員會於 2021 年 2 月 1 日發布實施「防制大規模毀滅性武器擴散及資武擴之目標性金融制裁指引」（*Targeted Financial Sanctions related to Proliferation of Weapons of Mass Destruction and Proliferation Financing*）¹¹⁵，包含聯合國安理會決議第 1718 號與第 2231 號之相關制裁名單。

4.3.5 新加坡

近年來新加坡金融管理局（MAS）已發布多項指引，協助金融機構打擊資武擴風險，具體措施包括：

- 金融管理局於對銀行執行一系列防制資武擴監理訪查後，發布《防制資武擴之有效實務》（*Sound Practices to Counter Proliferation Financing*）¹¹⁶ 指引文件，其中載明訪查發現之重要議題及所觀察之有效防制實務，供金融機構參考以強化現行內控措施。此外，金融管理局亦發布其他指引文件：《偵測與降低法人濫用風險之有效實務》（*Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons*）¹¹⁷ 及《強化法人／法律協議與複雜結構遭濫用之防制洗錢與打擊資恐防制措施》（*Strengthening AML/CFT controls on risks of misuse of legal persons/arrangements and complex structures*）¹¹⁸ 針對法人濫用之風險（此為資武擴之常見手法之一）提出有效防制之實務作法。
- 金融管理局亦在其針對金融機構發布之防制洗錢與打擊資恐指引文件中，提供防制資武擴之指引，包括可能的資武擴跡象指標。
- 2023 年 8 月，金融管理局發布《有效偵測與管理制裁相關風險通函》（*Circular on ensuring effective detection of sanctions-related risks*）¹¹⁹，供所有金融機構參考，以協助機構將該通函所述建議納入內部程序，有效辨識與管理制裁相關之風險。

此外，金融管理局亦與新加坡銀行公會（ABS）合作，將打擊資武擴列為銀行公會年度「金融犯罪研討會」（Financial Crime Seminar）之固定議程項目。銀行公會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士參與。歷年來，來自新加坡及其他國家（如美國）之專家在研討會中發表演說，提升金融業者對資武擴風險及其防制措施之認識。此外，金融管理局亦已展開宣導活動，提升其他產業（如金錢或價值移轉服務業者（MVTS）及虛擬資產服務提供商）之資武擴風險意識。

4.3.6 中華臺北

中華臺北已向金融機構、指定之非金融事業或人員（DNFBP）、虛擬資產服務提供商或其他部門，提供辨識、評估與降低規避制裁／資武擴風險之相關指引資料：

2022 年 1 月 20 日，財政部於其官網發布《記帳士暨記帳及報稅代理人執行防制洗錢及打擊資恐業務指引手冊》（*Operation Guide on Anti-Money Laundering and Counter-Terrorist Financing for Certified Public Bookkeepers and Bookkeeping and Tax Return Filing Agents*）¹²⁰（僅有中文版本）。

數位發展部數位產業署發布《第三方支付服務業防制洗錢指引手冊》，以防制洗錢、打擊資恐及打擊資武擴。該指引說明第三方支付業者應如何在不同業務層面辨識與評估洗錢/資恐/資武擴風險，並制定防制洗錢、打擊資恐及打擊資武擴計畫。第三方支付業者須採取風險基礎方法（Risk-Based Approach），進行風險評估，針對

¹¹⁵ 菲律賓防制洗錢委員會 - 《防制大規模毀滅性武器擴散及資武擴之目標性金融制裁指引》：<http://www.amlc.gov.ph/un-sanctions-list/notice-on-tsfs-obligations-on-proliferation-financing-of-wmd>

¹¹⁶ 新加坡金融管理局 - 《防制資武擴之有效實務》：<https://www.mas.gov.sg/regulation/guidance/sound-practices-to-counter-proliferation-financing>

¹¹⁷ 新加坡金融管理局 - 《偵測與降低法人濫用風險之有效實務》：<https://www.mas.gov.sg/regulation/guidance/effective-practices-to-detect-and-mitigate-the-risk-from-misuse-of-legal-persons>

¹¹⁸ 新加坡金融管理局 - 《強化法人／法律協議與複雜結構遭濫用之防制洗錢與打擊資恐防制措施》：

<https://www.mas.gov.sg/regulation/guidance/amlcft-controls-on-risks-of-misuse-of-legal-persons-arrangements-and-complex-structures>

¹¹⁹ 新加坡金融管理局 - 《有效偵測與管理制裁相關風險通函》：<https://www.mas.gov.sg/regulation/circulars/circular-on-ensuring-effective-detection-of-sanctions-related-risks>

¹²⁰ 財政部 - 《記帳士暨記帳及報稅代理人執行防制洗錢及打擊資恐業務指引手冊》：

<https://www.mof.gov.tw/download/6c9319f86c0b41079f47bf13fb2f0085>

洗錢、資恐及資武擴風險制定防制與降低風險措施，合理配置資源，建立內部控制制度，並落實防制洗錢、打擊資恐與防制資武擴相關之政策、程序及控管措施。考量第三方支付業者規模與營運模式差異，該指引特別為第三方支付業者訂定風險評估表，將客戶風險、產品、服務及交易風險、支付管道及商業實務風險、區域風險等分為四個構面，並就控管措施之執行提出具體建議，作為業者遵循相關法規之依據。

2021 年 8 月，經濟部商業司於「全國商工行政服務入口網」發布《銀樓業防制洗錢與打擊資恐簡介》¹²¹（僅提供中文版本）。

金融業相關公會則訂定以下指引，協助金融機構評估洗錢、資恐及資武擴之風險：

- 《銀行評估洗錢及資恐風險及訂定相關防制計畫指引》
- 《電子支付機構評估洗錢及資恐風險及訂定相關防制計畫指引》
- 《證券商評估洗錢及資恐風險及訂定相關防制計畫指引》
- 《信用卡業務機構評估洗錢及資恐風險及訂定相關防制計畫指引》

上述指引提供金融機構參考作法，說明如何在各業務領域辨識與評估洗錢、資恐及資武擴風險，並制定防制洗錢、打擊資恐與防制資武擴相關計畫。

銀行公會則另制定《銀行防制貿易洗錢之實務參考》，為銀行在貿易融資業務辨識、評估洗錢/資恐/資武擴風險及制定相關控管措施提供實務參考。

2021 年，內政部地政司擬訂《地政士及不動產經紀業防制洗錢及打擊資恐指引手冊》，提供予地政士公會全國聯合會，並置於官網，供業者遵循及瞭解其監理方法（僅提供中文版本）。此手冊包含中華臺北國家風險評估中所辨識之洗錢、資恐與資武擴的威脅、弱點及部門風險相關資訊。

4.4 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

在這些案例研究中，APG 成員國發現，規避目標性金融制裁（TFS）的方式，除了原有的船對船轉運石油等實體走私活動外，近期更有逐步轉向透過網路途徑進行的趨勢。此外，也觀察到法人實體遭濫用的情形日益增加，值得特別留意。

4.4.1 日本

**案例研究 #97：北韓IT工作者涉及資武擴
使用網際網路（包括加密及取得身分認證）**

日本發現，疑似北韓籍 IT 工作者冒充日本國民身分，透過日本企業提供之線上工作平台承接工作，藉此獲取收入。依據聯合國安理會第 1874 決議（2009 年）所設立之專家小組報告指出，北韓 IT 工作者所賺取之收入，用於資助北韓核武與飛彈計畫，因此涉及資武擴行為。

針對此情形，日本政府已發布警示公告，說明北韓 IT 工作者之運作模式，以提升相關企業意識，並鼓勵平台業者採取措施，如嚴格審核身分認證文件，以降低相關風險。

來源 - 日本

4.4.2 中國澳門

2023 年，中國澳門金融情報辦公室（GIF）統籌跨部門防制洗錢/資武擴工作小組各成員機關，彙整各產業檢視報告與威脅分析報告之內容（包含資武擴風險分析、整體資武擴風險評估及各產業別個別風險分析），完成

¹²¹ 經濟部商業司 - 《銀樓業防制洗錢與打擊資恐簡介》：<https://gcis.nat.gov.tw/mainNew/subclassNAction.do?method=getFile&pk=252>

《澳門 2022 年洗錢、資恐及資武擴風險評估報告》，並於 2024 年第一季派發予各利害關係人。綜合評估結果顯示資武擴，中國澳門整體資武擴風險偏低，主因係其既有之資武擴風險暴露程度較低，同時目前已有足夠有效之控管措施減輕相關風險。

自 2016 年起，中國澳門依據《資產凍結制度》（Asset Freezing Regime）（第 6/2016 號法律）之規定執行聯合國安全理事會相關資產凍結措施；惟截至目前，澳門並未針對境內之任何自然人、法人或實體，實施相關之資產凍結措施。此外資武擴，中國澳門亦未偵辦或起訴任何涉及資武擴之案件；亦未發現有違反、未落實或規避 FATF 第 7 項建議所規定之目標性金融制裁之情事。

依據《資產凍結制度》之規定，金融機構與指定之非金融事業或人員（DNFBP）須依法對列入聯合國安全理事會資武擴制裁名單之個人與法人實施資產凍結措施。為確保相關措施之有效性，中國澳門權責機關已與金融業及博弈業建立有效之溝通協調機制，以共同落實資產凍結措施。

另為持續提升各產業界對風險評估之認知，澳門金融管理局（AMCM）已透過發送調查問卷方式，掌握金融機構在資武擴方面之風險情形，及所採行之相關控管措施。

4.4.3 新加坡

案例研究 #98：非法向北韓供應柴油

資武擴

2019 年 9 月至 11 月期間，A 人士涉嫌與其他五名身處海外的人士合謀，於七個不同場合向北韓非法供應約 12,260 公噸柴油（gasoil）。其中，前六次的交貨係透過船對船轉運方式進行，第七次則於北韓境內一個港口進行，此違反新加坡《2010 年聯合國（制裁—北韓）條例》的相關規定。

為促成與北韓的柴油買賣交易，A 人士涉嫌四次利用他所擔任董事的 X 公司銀行帳戶進行相關款項支付；並涉嫌兩次偽造 X 公司的文件。此外，A 人士亦涉嫌五次利用其控制的另一間公司（Y 公司）之銀行帳戶，收取非法供應柴油予北韓之款項。新加坡可疑交易報告辦公室（STRO）發現該些交易可能涉及制裁活動，遂將分析報告呈交予新加坡警察部隊商業事務局（CAD）。

在商業事務局的調查過程中，A 人士涉嫌向調查人員作出虛假陳述，並銷毀與其非法供應柴油予北韓的相關證據。此外，A 人士亦未向商業事務局告知另一艘船隻於 2019 年 2 月非法供應柴油予北韓之情事。

2023 年 12 月，新加坡執法當局依據《2010 年聯合國（制裁—北韓）條例》、新加坡《刑事法典》（Penal Code，1871 年）及《貪污、販毒及其他重大犯罪（沒入利益）法》（CDSA），對 A 人士提出多項控狀。此外，作為獨立法人實體的 X 公司，被控四項依據《2010 年聯合國（制裁—北韓）條例》第 12(1)(b) 條並結合第 16(1) 條之規定，轉移可能促成受禁止活動之金融資產的罪名；Y 公司則依據《貪污、販毒及其他重大犯罪（沒入利益）法》第 47(3) 條規定，被控五項從犯罪行為中獲取利益之罪名。

來源 - 新加坡

4.4.4 中華臺北

案例研究 # 99：非法轉運油品予北韓船舶

資武擴

A 人士、B 人士二人與 C 人士、D 人士等人共同出資經營海上加油業務，使用多艘外籍油輪，於出口時虛報油品出口目的港，並於北韓港口附近海域為受聯合國制裁之北韓籍船舶「SAE BYO」號進行非法海上加油作業。中華臺北檢察機關 2022 年 12 月依據《資恐防制法》起訴 A 人士、B 人士、C 人士、D 人士等人，目前該案正在審理中。

來源 – 中華臺北

案例研究 # 100：違反《貿易法》

資武擴

S 項貨品係列屬中華臺北經濟部管制之戰略性高科技貨品，出口業者應在出口前向經濟部國際貿易署或其指定、委託之機關申請出口許可。然而，A 公司為規避該規定，於出口報關時虛報海關稅則號列，謊稱 S 項貨品非屬戰略性高科技貨品，以規避海關查驗，並將該貨品運往受管制之 B 司法管轄區。

2023 年 6 月，A 公司及其負責人 A 人士因違反《貿易法》，經權責機關移送檢察署偵辦，嗣後獲檢察官核准緩起訴，並向公庫支付 10 萬臺幣（約 3,138 美元）。

來源 – 中華臺北

4.5 資武擴－法人及專業協助者之濫用情形

由多個洗錢及資武擴案例可見，規避制裁之行為經常涉及濫用空殼公司及通匯銀行帳戶關係，以跨國移轉資金並掩飾最終實質受益人之身分。此種情形特別常見於在高風險司法管轄區設有海外分行之銀行，易遭利用進行高風險資金轉移活動。

4.5.1 案例研究

下列案例闡明法人濫用、利用第三方以掩飾實質受益權資訊，規避制裁之情形：

案例研究 # 101：利用空殼公司與藝術品顧問規避制裁

制裁；使用法人及法律協議

兩名遭美國財政部外國資產控制辦公室（OFAC）¹²² 制裁之個人，在制裁指定後仍可透過空殼公司及第三方藝術品顧問掩飾實質受益權，持續進入美國金融體系及藝術品市場。

2014 年，上述受制裁個人在被 OFAC 指定後，仍以數千萬美元向知名拍賣公司及其他藝術市場業者購入藝術品。交易透過第三方藝術品顧問代理完成，報告指出，至少某些拍賣行內部專業人員知曉實際買家的身份。¹²³

來源：防制洗錢金融行動工作組織（FATF）《藝術品與古物市場之洗錢及資恐風險報告》

¹²² 請注意：儘管所提及之制裁為特定司法管轄區之制裁，但用於規避此類制裁之方法凸顯資武擴中常見的制裁規避技術類型。

¹²³ FATF - 《藝術品與古物市場之洗錢及資恐風險報告》：<https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.html>

案例研究 #102：資武擴行動者濫用指定之非金融事業或人員（DNFBP）**制裁；使用法人及法律協議**

一家¹²⁴位於中國香港、專門從事境外公司註冊及提供公司秘書服務之會計師事務所，涉嫌協助一名澳洲居民設立掛名公司及空殼公司（X 公司及 Y 公司），用以便利進行高風險金融交易，向位於俄羅斯之受益人（包括一家遭美國金融制裁之實體）匯款。

2018 年，某外國銀行向澳洲交易報告與分析中心（AUSTRAC）提交一份可疑事務報告（SMR），此報告指出 X 公司申報之主要營業地點位於中國大連（鄰近北韓邊境，被視為制裁規避與資武擴活動高風險地區）。X 公司接收多筆來自位於中國香港與中國之船務公司的匯款，並試圖將此等資金匯往位於俄羅斯海參崴（Vladivostok）之不明受款方。

同年，另有一家大型銀行也提交了一份有關 Y 公司之可疑事務報告，該公司於澳洲註冊，但公開資訊有限。報告指出，Y 公司試圖將資金匯往俄羅斯境內一名遭美國制裁之受款方。

來源：《澳洲資武擴國家風險評估》

成員國提供下列案例：

案例研究 #103：違反制裁法律**制裁；使用法人及法律協議**

2021 年，新南威爾斯州最高法院判處一名外國出生的澳洲籍人士因違反澳洲對北韓之制裁法律，被判處三年六個月有期徒刑。該名人士利用境外銀行帳戶及一系列設立於澳洲之掛名公司，與北韓從事煤炭、石墨、銅礦、黃金、原油（包括代表北韓購買伊朗石油）、飛彈及飛彈相關技術等多種貨品之交易居間活動。此案係澳洲首度就違反北韓相關制裁而起訴之案件。

來源 - 澳洲

4.6 船舶登記制度

武擴網路經常利用全球商業供應鏈規避偵查，並藉此籌措資金，以取得受管制物資。船務公司及船舶經常涉入規避制裁及違反出口管制之行為，透過掛名公司與空殼公司掩飾其實際控制者身分，更導致海運部門成為武擴活動濫用的管道。根據 2020 年 3 月 FATF 發布之《全球海事警示》（Global Maritime Advisory）¹²⁵，伊朗、敘利亞與北韓等國經常透過偽造船廠文件、更換船旗國（Reflagging）及關閉自動識別系統（AIS）等方式，規避非法轉運貨物過程中的監控與偵查。¹²⁶

FATF 第 7 項建議，及方法論直接成果（Immediate Outcome）11 中特別強調，依據聯合國安全理事會決議實施之目標性金融制裁（TFS）。此包括要求各司法管轄區凍結指定個人及實體所擁有、或控制之財產，以及由其所有、或控制之其他人或實體之財產。此項義務亦適用於提供船舶註冊與船籍登記服務之個人或實體，因為船舶、船舶執照及船籍權利皆屬於財產或資產之一部分。

亞太防制洗錢組織（APG）在進行相互評鑑時，會依據 FATF 有關資武擴（PF）及相關資恐（TF）之建議，考量各司法管轄區船舶登記制度可能存在的漏洞。評估有效性時，評鑑人員需了解船舶登記機構在發現與制裁對

¹²⁴ 澳洲交易報告與分析中心（AUSTRAC）-《澳洲資武擴國家風險評估》：https://www.austrac.gov.au/sites/default/files/2022-12/AUSTRAC_Proliferation_Financing_in_Australia-National_Risk_%20Assessment_Web.pdf

¹²⁵ 美國國務院美國財政部外國資產管制辦公室及美國海岸防衛隊 -《因應非法航運與制裁規避行為之指引》（Guidance to Address Illicit Shipping and Sanctions Evasion Practices）：<https://ofac.treasury.gov/media/37751/download?inline>

¹²⁶ 美國財政部—《國家資武擴風險評估報告》（National Proliferation Financing Risk Assessment）：<https://home.treasury.gov/system/files/136/2022-National-Proliferation-Financing-Risk-Assessment.pdf> :

象相符之情形時，可採取哪些資產凍結行動，尤其須留意避免任何涉及指定船舶之交易，包括禁止變更所有權或船籍登記。更廣泛而言，APG 亦注意到船舶利用權宜船旗（Flags of convenience）可能涉及跨國犯罪及相關洗錢風險，因其可能被濫用於運送受禁物資。

此外，下列亞太防制洗錢組織（APG）成員國的兩個船舶登記制度案例顯示，若一司法管轄區將船舶登記管理委託給商業機構，可能產生額外的漏洞。雖然此種做法本身並無問題，但若商業機構與司法管轄區的權責機關之間缺乏充分的溝通、理解及問責機制，便可能滋生事端。

4.6.1 馬紹爾群島共和國（Republic of the Marshall Islands）

馬紹爾群島共和國（下稱馬紹爾群島）擁有規模龐大且管理完善之開放式船舶登記制度。該國為全球許多大型航運公司的法律註冊地，登記船隻數量全球排名第三（截至 2024 年 1 月 31 日，註冊船舶已超過 5,600 艘）。船舶登記及非居民國內實體（Non-resident Domestic Entities, NRDEs，約 41,000 個實體）提供之收入，成為該國第三大收入來源。

馬紹爾群島之國家風險評估指出，船舶登記與非居民國內實體登記在資武擴風險上屬於中度風險。國家風險評估特別提及，馬紹爾群島登記之船舶或非居民國內實體可能提供用於運送、轉運或交付核武、化武或生物武器相關材料的資產或金融服務，因而產生資武擴相關之防制缺口。儘管國家風險評估已將法人實體、航運業、登記制度及實質受益權列為幾大功能性弱點之一；但卻低估非居民國內實體（NRDEs）相關風險，因在該地法人設立容易，且在實質受益權之透明度與控制方面仍是一大挑戰。

馬紹爾群島信託公司（The Trust Company of the Marshall Islands Inc., TCMI）是該地非居民國內實體登記機關及海事管理機關。鑑於與航運相關的非居民國內實體增加，資武擴之風險隨之升高，TCMI 已於船舶登記程序實施多項措施，以應對及減輕資武擴及規避目標性金融制裁（TFS）之風險。TCMI 透過與聯合國專家小組等國際組織及外國政府合作，已充分理解此等風險，尤其針對航運公司之風險更為透徹。

TCMI 之海事管理單位利用商業資料庫，對非居民國內實體及海事交易涉及之所有已知當事人進行嚴格審查。該資料庫涵蓋聯合國、美國、歐盟等國際與國內制裁名單，亦包括公開被指控、調查、拘捕、起訴、正式提訴、拘留、訊問或接受審判等任何與犯罪活動相關名單。此外，TCMI 對船舶登記之所有當事人（含所有權人、實質受益人及營運者）、所有船舶識別資訊及船員，皆使用商業篩查資料庫，與聯合國安理會制裁名單及其他國內外制裁及犯罪名單比對篩查。該系統每 12 至 24 小時自動檢核所有已知當事人，並依據詳盡方法排除誤報（false positives），且設有逐級核准機制。該公司亦會視需要蒐集身分文件、居住證明、警方無犯罪紀錄證明等其他文件，以排除可能之匹配情形。此一系統持續篩查上述人員、船舶識別資訊及船員資料；若上述人員或船舶後續被列入制裁名單，或公開被指控、調查、拘捕、起訴、正式提訴、拘留、訊問或接受審判等任何與犯罪活動（包括與資武擴有關之犯罪活動）相關之司法程序，系統將自動通知法令遵循人員。

此外，海事管理單位主動透過船舶定位監控系統，監察船隻潛在的制裁規避行為，並發布關於非法航運及制裁規避實務之指引及通告。所有馬紹爾群島登記之船舶均須接受定期檢查，包括由專屬馬紹爾群島航海檢察官每年執行之檢查。

若 TCMI 必須根據聯合國制裁而被要求凍結或扣押實體，其可將相關船舶自船舶登記名冊中除名、撤銷其航行許可或撤銷公司註冊。曾有一家馬紹爾群島登記公司（Kingly Won International Co., Ltd.）因列名聯合國制裁名單而遭 TCMI 主動偵測並強制解散，解散之時間點早於聯合國安理會實施制裁。

馬紹爾群島海事登記制裁違規資訊共享機制：

馬紹爾群島船舶登記機構於 2019 年為船舶登記資訊共享契約（Registry Information Sharing Compact, RISC）之創始成員，建立了一個旗國間資訊通報系統，當船舶因疑似制裁相關活動而遭拒絕登記或除籍時，各旗國可互通報。透過 RISC，馬紹爾群島可取得非其登記船隊之資訊，協助規模較小、且較易受制裁規避風險影響之旗國。RISC 之成員目前掌控全球商船總噸位之比例超過 40%。

4.6.2 庫克群島

庫克群島於 2015 年之國家風險評估中，將自身面臨之資武擴（PF）風險評為低級別，其與北韓及伊朗之聯繫微乎其微，且並未查獲或凍結任何制裁名單中指定個人或實體之資金或資產。庫克群島金融業與北韓、或伊朗並無任何直接貿易往來，且依法禁止與北韓進行商業活動；但若與伊朗進行商業活動，則須採取加強客戶審查及監控措施（包括提交可疑交易報告）。自 2010 年以來，權責機關曾因發現數次涉及北韓及伊朗之船務活動。

2015 年，某銀行提交了一份可疑交易報告，原因是收到來自伊朗、與庫克群島船舶登記機構的船舶註冊有關。2016 年，金融監理委員會（FSC）於審查某保險公司之執照申請過程中，發現申請人於 2005 年曾為北韓船舶提供保險服務。金融監理委員會向申請人提出查詢後，確認該公司早已停止相關業務。

庫克群島於 2017 年進行之風險檢視指出，因為船舶登記制度的缺失，可能讓該國暴露於資武擴風險之中。交通部（MoT）將大部分行政業務外包給私人承包商，即庫克群島海事服務公司（Maritime Cook Islands, MCI）。交通部對目標性金融制裁之義務並不熟悉，並認為自身角色僅限於監督船舶登記機構之承包商，以確保其行使之授權符合國際海事組織（IMO）標準。MCI 則表示，其瞭解其契約義務包括代表交通部進行制裁名單之篩查，並與庫克群島政府機關協調受制裁船舶應採取之適當措施。

截至 2017 年 11 月，庫克群島船籍登記冊上共有 566 艘船舶登記，其中約半數為私人擁有之遊艇。船舶登記之擁有者通常為法人公司，來自 65 個不同司法管轄區，其中以馬紹爾群島、庫克群島、新加坡、英屬維京群島、俄羅斯及美國最為多。

2016 年 12 月，海事庫克群島公司（Maritime Cook Islands, MCI）開始訂閱一家專門針對航運與貨運領域機構之商業制裁篩查服務。MMCI 於船舶註冊或重新註冊時，透過此軟體對船舶之「控管主體」（即船舶經理人、光船承租人或其他營運人；若前述皆不適用，則為船東）進行制裁名單篩查。此外，MCI 亦每日持續針對與船舶相關之實體進行制裁名單篩查，並追蹤船舶是否涉及高風險活動。MCI 於註冊前亦會檢視船舶之歷史移動紀錄，透過船舶追蹤訊號判斷是否曾前往高風險區域，以辨識可能違反聯合國安理會決議（UNSCR）之情形。惟 MCI 似乎並未對船舶之控管主體以外之實質受益人或控制人（例如與船舶具直接或間接關聯、但非控管主體之實質受益人）進行制裁名單篩查。此外，在 2016 年 12 月前，未有證據顯示庫克群島航運登記機構依據 UNSCR 第 1373 號決議、或第 1267 號及後續決議進行目標性金融制裁篩查。

針對庫克群島航運登記機構潛在之資武擴風險，國家防制洗錢／打擊資恐策略中已納入相關措施，以強化庫克群島針對資武擴之目標性金融制裁制度。其中一項措施即訂定規範，要求 MCI 對其登記船舶進行盡職調查，以確認是否與任何受制裁實體具任何關聯。2017 年 11 月，庫克群島發布《2017 年金融交易通告（海事庫克群島）規範》（*Financial Transaction Reporting (Maritime Cook Islands) Regulations 2017*, 以下簡稱「MCI 規範」），「MCI 規範」指定 MCI 為申報機構，其義務範圍有限，包括於特定船舶登記前對控管主體進行客戶盡職調查（包含制裁名單篩查），並負有提交可疑交易報告（STR）之義務。然而，控管主體以外，MCI 規範並未要求 MCI 對其他人員進行制裁名單篩查。MCI 規範亦指定金融情報中心作為 MCI 執行此類義務之權責機關。此外，庫克群島政府內部亦有高度共識支持相關規定之執行，國家防制洗錢協調委員會於 2016 年即已通過資武擴行動計畫。目前並未發現有任何受制裁實體於庫克群島境內運作、或透過庫克群島移轉資金或資產。

案例研究 # 104：受制裁之註冊船舶遭查扣

制裁

2024 年 5 月，金融情報中心接獲兩起可疑活動通報，涉及四艘於庫克群島海事服務公司（MCI）註冊掛旗之船舶。上述船舶因涉嫌運送伊朗無人機至俄羅斯，而遭美國財政部海外資產控制辦公室（OFAC）列入制裁名單。¹²⁷ 目前該四艘註冊船舶已遭註銷登記，相關違規行為之調查仍在進行中。

來源 – 庫克群島

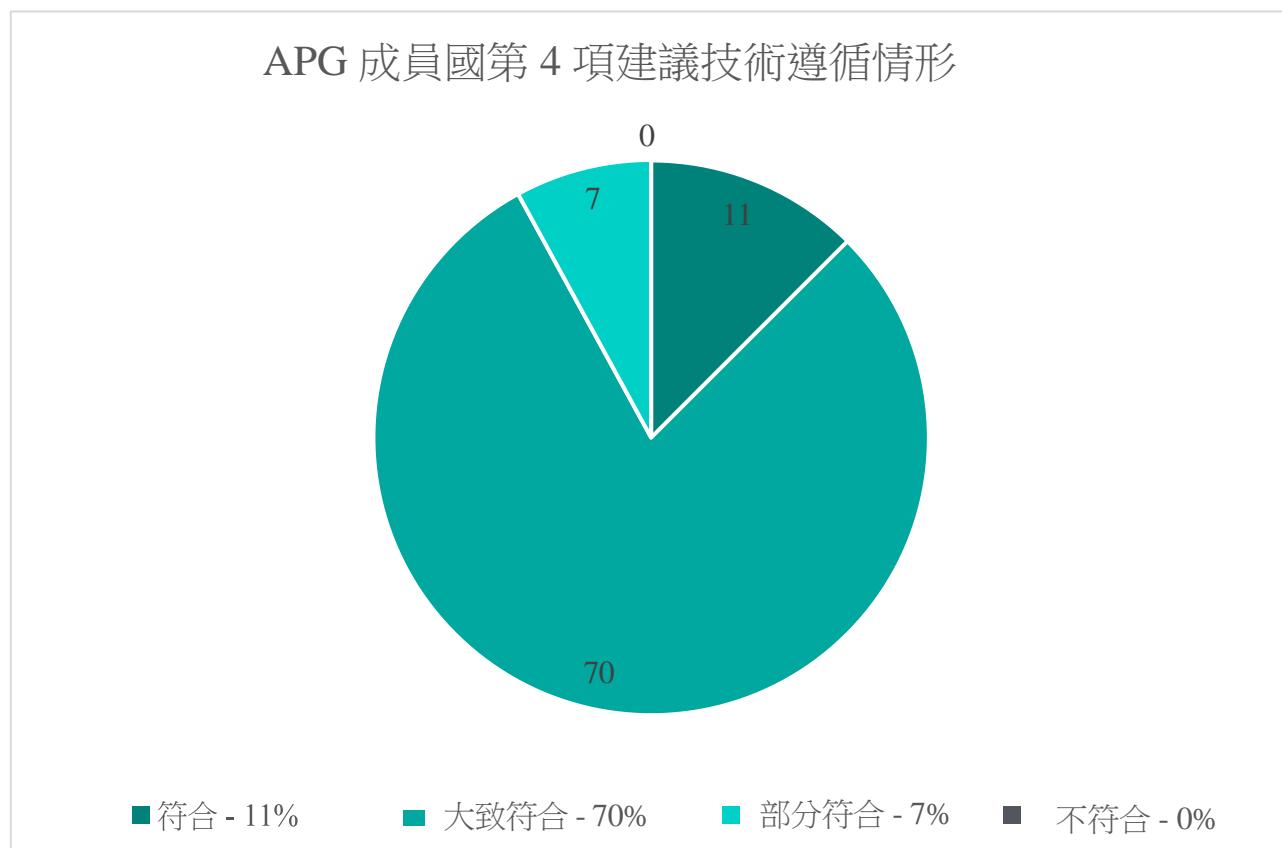
¹²⁷ 請注意：儘管上述提及之制裁措施為特定司法管轄區所實施，但所使用之規避制裁方法，凸顯出資武擴活動中常見的規避制裁類型。

5 - 資產返還之方法與趨勢

本節內容聚焦於亞太防制洗錢組織（APG）成員國就資產返還工作所提供的相關數據及案例研究。

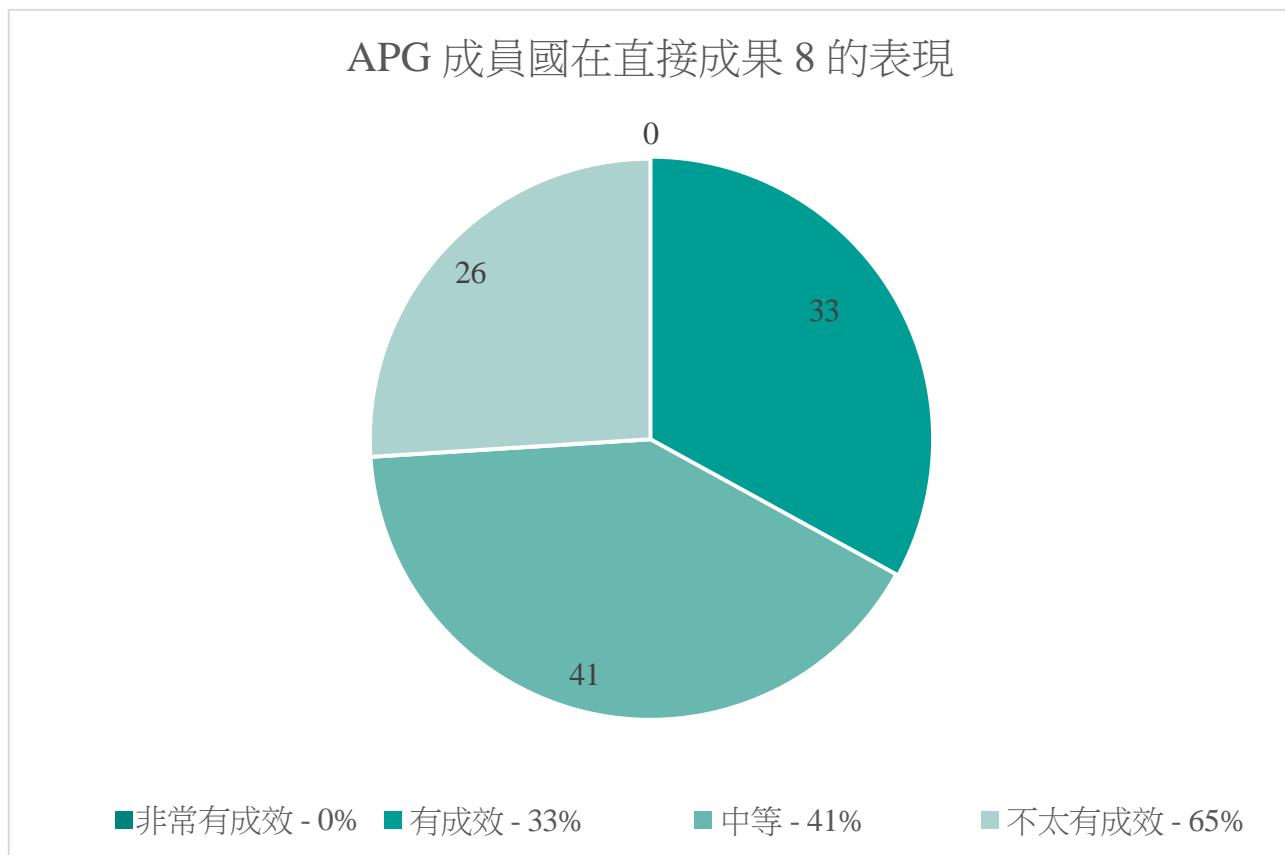
隨著 APG 即將完成第三輪相互評鑑（轄內僅三個司法管轄區尚待評鑑）¹²⁸，現階段已可從中擷取有關成員國司法管轄區遵循及有效落實 FATF 有關沒入及臨時措施（建議第 4 項、直接成果 8）與國際合作（建議第 38 項、直接成果 2）的統計數據。

FATF 第 4 項建議：沒入及臨時措施



FATF 直接成果 8 : 没入犯罪所得與犯罪工具

¹²⁸ 阿富汗、紐埃（Niue）及吐瓦魯（Tuvalu）



如圖表所示，儘管 APG 多數成員國對 FATF 建議的技術遵循程度普遍良好¹²⁹，但在達成原先設定之成效方面，成員普遍表現不佳。

同樣地，儘管多數 APG 成員國已建置資產追查、凍結、沒入及資產共享的國際合作法律框架，但實際運作成效仍僅屬中等水準。

鑑於亞太防制洗錢組織（APG）第四輪相互評鑑已於 2024 年展開，並將於 2032 年完成，各成員應特別注意 FATF 對第 4 項建議及第 38 項之相關修訂，並更加注重跨司法管轄區之非正式合作管道，同時強化正式程序之精簡與效率。

APG 亦鼓勵各司法管轄區積極參與並利用以下國際合作管道，包括國際刑警組織（Interpol）、艾格蒙聯盟（Egmont Group）、亞太區追討犯罪所得機構網路（Asset Recovery Interagency Network Asia Pacific，ARIN-AP）、太平洋金融情報機構通訊網路（Pacific FIU Communications，PFIC）及太平洋律師組織網路（Pacific Islands Lawyers' Organisation Network，PILON）等。

追回被盜資產倡議（StAR）之「資產返還觀測資料庫」

追回被盜資產倡議（StAR）之「資產返還觀測資料庫」（Asset Recovery Watch）¹³⁰，是一個公開資料庫，追蹤全球各司法機關追討貪污所得資產之情形。StAR 資產返還觀測資料庫的主要目的在於，蒐集、並系統化具國際層面的貪污所得資產返還案件資訊，包括已完成及進行中的相關案件。

¹²⁹ FATF - FATF 建議. <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html>

¹³⁰ 追回被盜資產倡議（StAR）—資產返還觀測資料庫 <https://star.worldbank.org/asset-recovery-watch-database>

追回被盜資產倡議 (StAR) - 《被扣押與沒入之資產管理：實務工作者指南》

此指南¹³¹ 旨在為資產管理實務工作者提供指引，涵蓋扣押前規劃、資產保管期間的價值維護，以至資產處分時價值最大化等各個階段。指南期能協助實務工作者建立有效之資產管理機制，並逐步擴充其資產管理能力，以處理更為複雜之資產。因此，本指南蒐羅國際研究之建議、並自資產管理專家訪談、以及實務操作案例之優良作法截取經驗。此外，實務工作者亦可從不同司法管轄區採行方法之討論、案例實例，及針對特定資產管理細節之說明中獲益。

追回被盜資產倡議 (StAR) - 《貪污之資產受害者：追回賠償》

此報告¹³² 旨在概述現有國際法律框架，並引導討論重要議題，包括受害人尋求補償之途徑、受害人之界定、法律地位之認定，以及損害賠償額度之確定等。此報告提出若干值得探討之做法，冀圖能適當協助貪污被害人取得賠償。

5.1 資產追查，包括限制措施 — 鎖定及調查國內外犯罪所得、犯罪工具或同等價值之財產

5.1.1 澳洲

案例研究 # 105：國際聯合行動沒入逾 225 萬美元非法資金與財產

購置不動產；犯罪所得；國際合作

「巴辛行動」（Operation Bassing）目的在鎖定並沒入澳洲境內外之犯罪所得，是澳洲境內外相關機關與產業共同合作的專案。此國際聯合洗錢及稅務詐欺調查行動，最終沒入約值 300 萬澳幣之資產。

「巴辛行動」係源於澳洲交易報告與分析中心（AUSTRAC）發現可疑帳戶活動，並偵測到西澳洲與 X 司法管轄區間之銀行帳戶間存在大筆國際資金移轉。儘管相關帳戶係以公司或其他個人名義開立，實際上均涉嫌與一名居住於西澳洲之人士有所關聯。

AUSTRAC 遂將此金融情資轉介予澳洲聯邦警察。2020 年，澳洲聯邦警察主導之刑事資產沒入專案小組（Criminal Assets Confiscation Taskforce, CACT）利用 AUSTRAC 提供之情資，與 X 司法管轄區警方展開國際聯合調查。調查發現相關帳戶餘額與涉案個人向澳洲稅務局所申報之個人與企業收入顯不相稱，顯示資金來源可疑。

CACT 進一步向 AUSTRAC 提供金融情資報告，並行使法定之資訊蒐集權力，向通報機構蒐集更多資訊以支援本次調查。

經詳盡調查及民事訴訟程序後，西澳洲最高法院於 2022 年根據《2002 年犯罪所得法》（Proceeds of Crime Act 2002）裁定，沒入約 245 萬澳幣（約合 169 萬美元）非法資金，以及位於柏斯市、價值約 58 萬 5,000 澳幣（約合 40 萬 4,533 美元）之公寓，歸澳洲聯邦政府所有。此外，在 X 司法管轄區警方及該地金融情報中心協助下，另有約 100 萬澳幣（約合 69 萬 1,569 美元）資金遭到凍結。

來源 - 澳洲

¹³¹ 追回被盜資產倡議 (StAR) - 《被扣押與沒收之資產管理：實務工作者指南》：<https://star.worldbank.org/publications/managing-seized-and-confiscated-assets-guide-practitioners>

¹³² 追回被盜資產倡議 (StAR) - 《貪污之資產受害者：追回賠償》：<https://star.worldbank.org/publications/victims-corruption-back-payback>

5.1.2 加拿大

加拿大皇家騎警（RCMP）近年致力於提升追查非法虛擬資產（包含加密貨幣）之能力。為此，加拿大皇家騎警從私部門購得相關授權，獲取掃描與搜尋區塊鏈交易記錄之權限，以追蹤非法虛擬資產流向。此外，加拿大皇家騎警亦與供應廠商密切合作，由技術面掌握追蹤工具之運作模式，深入理解廠商如何辨識交易、蒐集資訊，並確保相關作業流程符合法院要求之證據標準。

為妥善使用上述工具，皇家騎警特別設計培訓課程，協助調查人員掌握追蹤非法虛擬資產之技能，以支援刑事調查，並編製適用於法院審理之虛擬資產追蹤宣誓書。

5.1.3 庫克群島

案例研究 # 106：美國證券交易委員會詐欺案

詐欺犯罪（電匯、投資詐騙）

2021 年 6 月 24 日，庫克群島金融情報中心接獲金融機構通報之可疑活動報告。報告指認一名擔任庫克群島多家公司的董事及控制人，而相關公司之銀行帳戶內有 130 萬美元存款。該名涉案人士為美國公民，涉嫌在美國證券交易委員會（US-SEC）管轄範圍內參與投資詐騙活動。

隨後，金融情報中心收到美國司法部來函證實該名涉案人士已在美國遭逮捕，美國司法部並要求申請緊急資產凍結令。根據《2015 年金融情報中心法》（FIU Act 2015），金融情報中心負責人有權申請資產凍結令。

2021 年 6 月 25 日，庫克群島高等法院依據《2015 年金融情報中心法》第 35 條發布資產凍結指令（Freeze Instruction），凍結將該金融機構帳戶內 130 萬美元，有效期間為 60 日（至 2021 年 8 月 24 日屆滿）。由於涉案人士透過其律師要求自該帳戶匯出 125 萬美元至美國，以支付保釋金並獲釋，因此法院緊急發布凍結令，以防資產遭移轉或分散。

初步調查發現，涉案公司帳戶係於 2021 年 1 月 27 日開立，申報用途包括國際支付、金融投資、可轉換債務投資，以及支付與收取服務款項等業務活動。金融情報中心已向美國證券交易委員會（主要調查機關）及相關外國對等單位提出情資報告。

2023 年 11 月 16 日，庫克群島高等法院首席法官頒布經蓋印之判決令（sealed judgment order），批准將凍結資金返還美國，並於 2023 年 12 月開始執行返還作業。該最終返還令係依美國刑事司法互助請求，並經庫克群島金融情報中心依《2015 年金融情報中心法》成功三度延長凍結令後，由法院核發。凍結令延長指示係由金融情報中心依該法規定下達予通報金融機構，法院之相關呈請由庫克群島皇家法律辦公室（Crown Law Office）代表金融情報中心提出。

來源 - 庫克群島

5.1.4 中國香港

2023 年底，香港警務處（HKPF）成立「反詐騙聯盟」（Anti-Deception Alliance, ADA）平台，由 10 家主要銀行之代表，與香港警務處商業罪案調查科轄下的「反詐騙協調中心」（Anti-Deception Coordination Centre, ADCC）共同合作。該聯盟旨在即時支援香港警務處打擊詐欺犯罪活動，例如加速處理止付請求，以有效提升反詐欺機制之運作效率。

案例研究 # 107：成功攔截企業電子郵件涉及公司銀行帳戶的詐騙**詐欺；金融機構；境外前置犯罪**

2023年初，A司法管轄區公司之經理收到公司董事的電子郵件指示後，從公司帳戶匯出1,100萬美元至中國香港另一公司之銀行帳戶。然而，該封郵件實際為駭客入侵董事郵件帳號所發出。經理察覺公司董事的電子郵件被駭客入侵後，向警方報案。警方接獲通報後，成功凍結該詐騙集團銀行帳戶內之830萬美元，避免該筆款項進一步遭移轉或分散。目前遭詐騙資金之返還程序仍在進行中。

來源 – 中國香港

案例研究 # 108：成功攔截企業電子郵件涉及公司銀行帳戶的詐騙**詐欺；金融機構**

2023年，本地一間貿易公司的會計收到一封偽造電子郵件，該電子郵件冒充公司的業務夥伴，詐騙者利用電子郵件欺騙手法（spoofing）發送訊息。會計隨後將公司銀行帳戶中的680萬美元匯入位於A司法管轄區的一間公司帳戶。當會計聯絡真正的業務夥伴核實後，詐騙行為被揭露。此案已報警至香港警察，詐騙者帳戶中的全額款項已被凍結，防止進一步轉移。目前，被騙款項的追回工作仍在進行中。

來源 – 中國香港

5.1.5 印度

案例研究 # 109：以洗錢方式處理透過多起詐欺案取得之犯罪所得**詐欺（包含偽造文書）；竊盜；金融機構；使用法人及法律協議**

印度執法當局於2015年至2016年間，針對A人士及其共犯提出數起犯罪檢舉。經查證，A人士等人涉嫌透過犯罪共謀，以欺詐手段向一家由銀行主導的聯貸案取得貸款；並將非法取得的部分資金透過空殼公司移轉至印度國內外，再將之轉換為不動產與其他資產。

印度執法局（Enforcement Directorate, ED）偵辦後確認涉案犯罪所得總額約達1,129.1億印度盧比（約13億美元），並於2016年依據兩道臨時扣押令（provisional attachment orders）扣押約504.27億印度盧比（約6.01億美元）。同年，A人士因逃離印度，被宣告為「通緝犯」（proclaimed offender）。印度當局亦根據刑事訴訟法典第83條（CrPC Section 83），扣押A人士名下價值約169.42億印度盧比（約2.02億美元）之資產，無須證明其與特定前置犯罪之關聯性。

2016年至2020年間，印度執法局透過艾格蒙聯盟（Egmont）及司法互助途徑，向8個司法管轄區提出共21項調查請求（Egmont requests及Letters Rogatory），以確認A人士位於境內外之資產。相關請求導致數筆資產遭到扣押，包括一處位於法國、價值約160萬歐元（約180萬美元）之不動產及其他位於印度國內外之資產。

截至目前，A人士尚未於印度受審，並於2019年被宣告為「逃亡經濟犯」（Fugitive Economic Offender）。同年，印度當局批准自英國引渡A人士，但由於英國相關司法程序仍持續進行，尚未完成引渡程序。

受害之聯貸銀行團依據印度《2022年防制洗錢法》（Prevention of Money Laundering Act 2022），向法院提出申請，要求歸還由印度執法局扣押之財產。2021年，印度特別法院裁定，在刑事案件審理終結前，將約1,413.13億印度盧比（約18億美元）的動產與不動產返還聯貸銀行團。該返還金額較已確認的犯罪所得高出25%，並包含資產遭印度中央政府控管期間之利息收入。上述財產係直接返還予聯貸銀行團，而非納入印度政府收入。

來源 – 印度

5.1.6 印尼

案例研究 # 110：合作社侵吞社區資金

詐欺

2007 年至 2014 年間，C 合作社自約 23,193 名合夥人處募集約 4.7 兆印尼盾（約 3.08 億美元）資金。此等合夥人投入的資金（參與資本）未用於擴展合作社的業務活動，而是用於向 2007 年至 2014 年間到期之 8,414 名合夥人支付利息與本金，支付金額達 1.5 兆印尼盾（約 9,800 萬美元）。此外，相關資金亦遭被告（合作社管理委員會主席）及數家公司挪作私人用途。被告行為導致整體社區資金損失約 3,264,688,621,100 印尼盾（約 2.136 億美元），為 14,779 名合夥人之存款或投資總額。最終，被告遭法院判處 2 年有期徒刑，罰金 50 億印尼盾（約 327,237 美元），其名下多處土地資產亦遭沒入並拍賣，以償還債權人；剩餘款項按比例交付予受害人協會。

來源 - 印尼

5.1.7 馬來西亞

案例研究 # 111：逃漏稅 - 低報收入

逃漏稅

A 人士為某主權財富基金公司（A 財富基金）之前執行董事，該基金係為促進經濟發展而成立。A 人士亦擔任安排人角色，執行涉及外國銀行及避稅天堂司法管轄區之聯貸交易。

調查過程中，調查人員發現 A 人士個人銀行帳戶內，收到來自 A 財富基金的大筆資金，此情形與可疑交易報告所列之指標吻合。此外，馬來西亞國家稅務局（IRBM）採用淨值法調查 A 人士之未申報收入，發現 A 人士涉嫌逃漏稅，刻意隱匿其收到的款項。

國家稅務局隨後對 A 人士之銀行帳戶發出凍結令，法院亦對 A 人士名下兩輛汽車及銀行帳戶內的 26,000 馬幣（約 5,400 美元）現金發布沒入令（forfeiture order）。

來源 - 馬來西亞

案例研究 : # 112:大麻產品

毒品相關犯罪

2022 年 6 月，在馬來西亞金融情報中心主動提供資訊後，馬來西亞皇家關稅局（RMCD）針對一個涉嫌透過網路銷售大麻產品之犯罪集團，執行控制交付（追蹤包裹）行動。

該犯罪集團自境外供應商以每公斤 3,500 馬幣（約 700 美元）的價格購買壓縮大麻，並加工製成大麻花與大麻餅乾。其等之後積極透過 Telegram 行銷，接受客戶訂購上述產品。

行動中，皇家關稅局逮捕三名嫌犯，凍結其等名下合計 19 個銀行帳戶，總計 50 萬馬幣（約 104,000 美元）。另外查扣一輛汽車，以及製作大麻花與大麻餅乾之器具與設備。三名嫌犯彼此為親屬關係，馬來西亞皇家關稅局已依據 1956 年《危險毒品法》（*Dangerous Drugs Act*）第 39B 條向法院提出指控。本案目前仍在審理中。

來源 - 馬來西亞

案例研究 # 113：打擊涉及毒品犯罪之私菸酒走私犯罪集團案**走私（走私酒）、毒品犯罪、自我洗錢**

作為馬來西亞打擊走私違禁品行動之一，馬來西亞皇家警察（Royal Malaysian Police, RMP）查獲逾 7,000 箱走私酒類，並在現場發現搖頭丸（MDMA）毒品及若干疑似用於小型毒品製造實驗室的機器及實驗設備。

經調查，A 人士與 B 人士涉嫌共同經營此走私違禁品犯罪行動，並利用該場所加工毒品，之後銷往當地市場。隨後馬來西亞皇家警察透過金融情報及資產追蹤進一步偵辦，最終查扣包括豪華汽車、銀行帳戶、珠寶及現金等資產，總價值約達 300 萬馬幣（約 625,000 美元）。此外，皇家警察亦查明 A 人士利用數家公司帳戶進行洗錢活動，以隱匿非法收益。

皇家警察已依據 1952 年《危險毒品法》對 5 名涉案人士提起毒品販運罪名指控。所有被查扣資產正根據 1988 年《危險毒品（財產沒入）法》進行相關沒入程序，目前該程序仍在進行中。

來源 - 馬來西亞

5.1.8 新加坡

案例研究 # 114：針對遠端博奕集團營運者之不明財富沒入**犯罪類型：有組織犯罪；勒索詐欺**

自 2014 年起，某犯罪集團透過線上平台提供彩票、足球與賽馬等非法遠端博奕服務；A 人士及其他 9 名嫌疑人被捕。新加坡警察部隊調查顯示 A 人士為主要上游代理人，負責為 6 名共犯於不同遠端非法賭博網站開立投注帳戶，並負責收付非法賭注。2018 年 7 月 12 日，A 人士因違反《2014 年遠端博奕法》（Remote Gambling Act 2014）被判處 26 個月徒刑與 160,000 新加坡元的罰款（約合 124,395 美元）。

金融調查顯示 A 人士多年累積之不明財富與已知收入來源不符。A 人士經法院定罪後，新加坡警察部隊依據《貪污、販毒及其他重大罪行（利益沒入）法》（CDSA）第 7(1) 條之規定，向法院申請沒入令，以沒入 A 人士從犯罪行為中獲取之利益。2023 年 3 月 13 日，高等法院核准該沒入令，追繳 A 人士犯罪所得約 110,332.67 新加坡元（約 85,768 美元）。

來源 - 新加坡

案例研究 # 115：查扣疑似無照放貸及洗錢犯罪所得之資產犯**無照放貸罪**

2020 年 6 月至 10 月期間，被告 A 人士涉嫌在新加坡未經許可經營放貸業務，以買賣及租賃二手手機業務作為掩護，實際進行非法放貸活動。調查過程中，執法當局凍結 A 人士與其犯罪活動相關之 5 個銀行帳戶，並查扣資產總額超過 700,000 新加坡元（約合 544,186 美元）。2024 年 1 月 22 日，A 人士因涉嫌違反新加坡《2008 年放債人法》（Moneylenders Act 2008）及《貪污、販毒及其他重大罪行（利益沒入）法》（CDSA）之規定，被新加坡法院起訴，目前法院對 A 人士之案件審理仍在進行中。

來源 - 新加坡

案例研究# 116：沒入毒品販運犯罪所得**毒品相關犯罪**

2015 年 3 月 18 日，A 人士因違反《濫用毒品法》（Misuse of Drugs Act, MDA）（1973 年）販運管制毒品而遭逮捕，2017 年 12 月 14 日，其因上述毒品前置犯罪而遭判處強制性死刑。

A 人士被捕時，執法機關扣押現金共計 25,218.30 新加坡元（約 19,614 美元）；調查期間，亦凍結其兩個銀行帳戶，帳戶餘額共計 18.45 新加坡元（約 14.35 美元）。A 人士聲稱，遭扣押之款項中，僅 1,000.00 新加坡元（約 778 美元）係毒品販運所得，其餘則來自合法來源。

為釐清 A 人士從毒品販運活動中所取得利益之規模，當局進行隱匿收入分析（concealed income analysis），結果顯示 A 人士隱匿之所得達 46,199.81 新加坡元（約 35,872 美元），可變現資產為 25,236.75 新加坡元（約 19,629 美元），此為 A 人士無法合理說明之累積財富，明顯超過其已知合法收入來源。

2023 年 2 月 20 日，依據《貪污、販毒及其他重大罪行（沒入利益）法》（CDSA）第 6 條規定，法院頒布沒入令，裁定沒入 A 人士自毒品販運所獲利益共計 25,236.75 新加坡元（約 19,629 美元）。

來源 - 新加坡

案例研究 # 117：沒入毒品販運犯罪所得**毒品相關犯罪**

2012 年 3 月 14 日，A 人士因違反《1973 年濫用毒品法》（Misuse of Drugs Act, MDA）販運管制毒品首次遭到逮捕，並於 2014 年 8 月 6 日因毒品販運罪名被判處 11 年有期徒刑。

首次逮捕期間，執法機關扣押現金共計 26,974.10 新加坡元（約 20,978 美元）及 10 汶萊幣（約 7.78 美元）；調查期間另凍結一個銀行帳戶，帳戶餘額為 228.20 新加坡元（約 177 美元）。金融調查期間，A 人士聲稱遭扣押之款項均為合法來源所得。

於 2013 年 4 月 30 日第二次逮捕期間，當局再次扣押現金共計 5,899.20 新加坡元（約 4,588 美元）。金融調查期間，A 人士聲稱僅 1,749.20 新加坡元（約 1,360 美元）為毒品犯罪所得。

為確認 A 人士自毒品販運活動取得之利益規模，當局進行隱匿收入分析，結果顯示 A 人士隱匿所得達 365,514.32 新加坡元（約 284,264 美元），可變現資產則為 35,347.66 新加坡元（約 27,491 美元）。此為 A 人士無法合理說明之財富累積，明顯超過其已知合法收入來源。

2023 年 8 月 7 日，法院依據《貪污、販毒及其他重大罪行（沒入利益）法》（CDSA）第 6 條規定，裁定頒布沒入令，沒入 A 人士因毒品販運所獲利益共計 35,347.66 新加坡元（約 27,490 美元）¹³³。

來源 - 新加坡

案例研究 # 118：貨幣兌換業者透過現金攜帶者走私現金**走私；貨幣兌換／現金兌換；現金**

新加坡跨境現金移動申報制度規定，凡旅客出入新加坡時，攜帶實體貨幣及不記名可轉讓票據總值超過 20,000 新加坡元（約 15,554 美元）時，必須向權責機關完整且正確地申報。

2023 年 6 月，A 人士入境新加坡時僅申報攜帶約 505,500 新加坡元（約 393,143 美元），但實際上攜帶約 198 萬新加坡元（約 1,539,906 美元）之現金。此情形係經新加坡樟宜機場之執法人員進行檢查時發現。經新加

¹³³ 最終沒收金額尚未確定，目前仍待拍賣程序完成。

坡警察部隊商業事務局（Commercial Affairs Department, CAD）調查後發現，A 人士係 A 司法官轄區之貨幣服務業者，以隨身攜帶方式將現金帶入新加坡進行外幣兌換用途。調查另發現，A 人士此前於 2023 年 6 月另一次入境新加坡時亦曾作出不實申報，僅申報攜帶 458,000 新加坡元（約 356,200 美元），惟當時實際上所攜現金達約 100 萬新加坡元（約 777,706 美元）。

針對上述二次違規行為，A 人士於 2023 年 11 月被法院依據《貪污、販毒及其他重大罪行（沒入利益）法》（CDSA）第 60 條結合 1871 年《刑事法典》（Penal Code 1871）第 108B 條之規定，裁定犯下二項共謀將超過規定數額（20,000 新加坡元）之現金攜入新加坡、且未向主管官員完整準確申報之罪行，合併判處罰金共計 30,000 新加坡元（約 23,329 美元）。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。法院並依檢察官之聲請，依據 CDSA 第 64 條規定頒布沒入令，裁定沒入款項 400,000 新加坡元（約 311,051 美元）歸國庫所有。

來源 - 新加坡

案例研究 # 119：沒入處理私菸所得利益

[走私；自我洗錢；現金](#)

新加坡海關（Singapore Customs）經調查後逮捕涉嫌處理超過 800 公斤未完稅香菸之 A 人士，其逃漏消費稅及其他稅賦金額超過 400,000 新加坡元（約 311,051 美元）。A 人士隨後經法院審理，依據 1960 年《關稅法》（Customs Act 1960）第 128I(1)(b) 條等罪名成立，遭判處 37 個月有期徒刑。

由於 A 人士遭逮捕時，被查獲持有超過 160,000 新加坡元（約 124,412 美元）之現金，且無法就其來源提出合理解釋，新加坡海關遂將本案移送新加坡警察部隊商業事務局（CAD）進行金融調查。2023 年 8 月，法院依據《貪污、販毒及其他重大罪行（沒入利益）法》（CDSA）第 5 條規定，最終裁定沒入 A 人士犯罪所得之約 110,000 新加坡元（約 85,531 美元）。

來源 - 新加坡

5.1.9 中華臺北

案例研究 # 120：拉法葉艦採購弊案

[貪污與賄賂](#)

引起中華臺北高度關注之「拉法葉艦案」涉及軍火掮客 A 人士收受非法回扣。2001 年，歐洲媒體披露 A 人士家族有大量資金異常流入歐洲多個司法管轄區。經法務部協助，最高檢察署向多個司法管轄區提出刑事司法互助請求，凍結 A 人士家族於境外之資產。2001 年至 2003 年間，A 司法官轄區陸續凍結 A 人士家族控制之 27 個銀行帳戶；本 2006 年，B 司法官轄區亦同意提供協助，凍結該家族之海外銀行帳戶。依據《貪污治罪條例》，共同被告 B 人士等人因共同收受回扣而遭起訴，A 人士家族成員則因協助收受回扣遭起訴。A 人士及其家族長期逃亡國外，法院雖發布通緝令，審判仍無法實質進行。由於 A 人士家族擁有龐大犯罪所得，且其帳戶及資產分布於多個司法管轄區，跨境追討犯罪所得行動極為困難。

2016 年 7 月 1 日刑法沒入制度修正施行後，最高檢察署立即聲請沒入宣告。最高法院分別於 2019 年及 2021 年裁定本案應沒入之犯罪所得本金總額超過 4 億 8,719 萬美元，奠定法務部向其他司法管轄區請求沒入 A 人士家族海外犯罪所得之法律基礎。隨後，法務部積極聯繫並協助臺北地方檢察署，向 B 及 C 的司法管轄區要求返還已凍結之 A 人士家族資產。在兩司法管轄區之協助下，B 司法官轄區於 2023 年 2 月已返還約 1,103 萬美元，C 司法官轄區則於 2023 年 7 月將 1 億 3,804 萬美元移轉回中華臺北。經過法務部、外交部及駐 C 司法官轄區臺北文化經濟代表團之努力協助，歷時 20 餘年之刑事司法互助終於取得具體成果。為妥適回應社會大眾期待，法務部將持續宣導國際合作，追討所有藏匿於境外之犯罪所得，以徹底取回犯罪所得不法利益，維護社會公平正義。

來源 - 中華臺北

案例研究 # 121：A 司法管轄區資產之返還**詐欺**

2019 年，中華臺北接獲 A 司法管轄區提出之刑事司法互助請求，要求返還其國民遭詐欺所得之犯罪資產。該筆犯罪資產移轉至中華臺北後已遭扣押。兩地司法管轄區歷經數年偵查，相關權責機關多次磋商後，中華臺北最終要求 A 司法管轄區提供相關證據。經中華臺北權責機關協助安排，A 司法管轄區之法務部派遣其調查官及助理前往中華臺北，於中華臺北檢察署收回遭扣押之犯罪所得資產，總金額約為 34,000 美元現鈔。此為近年來 A 司法管轄區與中華臺北首次成功完成之跨境資產返還案例。

來源 - 中華臺北

5.1.10 越南**案例研究 # 122：利用電腦網路、電信網路及電子媒體進行詐欺與侵占資金****詐欺，包括利用社群媒體犯罪**

八名被告利用電腦網路、電信網路及電子媒體犯下詐欺與侵占財產罪行，涉及約 657,353,973,788 越南盾（約 27,115,207 美元）。

本案被告所屬公司開發網站、應用程式及電子商務平台，透過此類軟體招募投資人，以多層次傳銷（Multi-level marketing）方式誘導投資者購買所謂「去中心化」股票。被告以多層次方式募集投資，高額利息的承諾實際上是以新進投資者的資金來支付早期投資者的佣金及紅利，亦即侵占後期投資人資金。

調查期間，調查機關已凍結並扣押 A 公司及被告之銀行帳戶內之犯罪所得，共計 179,686,704,902 越南盾（約 7,411,900 美元）。此外，調查機關亦扣押 12 處房屋與土地（A 公司各代表辦公室所在地），以及 A 公司所有並供部分代表辦公室主管使用的 5 輛汽車，均視為犯罪所得。

來源 - 越南

案例研究 # 123：發生於股份有限公司之財產侵占詐欺**竊盜；利用資本市場**

本案涉及於股份有限公司及其關係企業所發生之財產侵占詐欺案件。

被告 A 人士與外國投資經紀人 B 人士合作，進行多家公司股票買賣交易。A 人士直接從 B 人士及其合作夥伴處收取資金，並與 B 人士簽訂買賣 C 公司股票之合約，以侵占 B 人士約 77,577,600,000 越南盾（約 3,200,000 美元）之資金。

A 人士家屬已支付現金 20,000,000,000 越南盾（約 824,980 美元）以彌補犯罪損害，檢察機關並已查扣三筆不動產。

來源 - 越南

5.2 管理凍結／扣押資產：關於資產管理案件之資訊，以及供資產管理機構使用之程序或作業手冊

5.2.1 日本

日本指出，其國家警察廳（NPA）依據國家公安委員會（National Public Safety Commission）規則，以及其《證物之保管與管理指引》（Guideline for the Storage and Management of Material Evidence）執行扣押資產之管理工作。

5.2.2 中國澳門

中國澳門之資產扣押機制與程序主要依據《刑事訴訟法典》（Criminal Procedural Code）之規定。根據法律規定，司法機關得批准或命令扣押曾用於、或準備用於犯罪之資產，或屬於犯罪行為所產生之物品、收益、價金、報酬及其他可視為證據之資產。被扣押之資產應附於案卷，若無法附卷，則交由負責該程序之司法人員、或指定保管人保管。如被扣押之資產可能遺失、損毀或具危險性，司法機關得視情況，命令將該等資產出售、銷毀或用於社會公益。

為在訴訟程序中更系統化、有效率地管理經檢察院依法扣押之資產，檢察院已建置「扣押資產管理系統」（Seized Assets Management System），並備有使用手冊。檢察院亦規劃逐步與各警察部門建置扣押資產資訊之結構化傳輸格式，並持續討論及宣導系統性之資訊交換。

5.2.3 菲律賓

依據經修正之《防制洗錢法》（Anti-Money Laundering Act, AMLA）第 7(16) 條之規定，菲律賓防制洗錢委員會（AMLC）負有依凍結令（Freeze Order）、資產保全令（Asset Preservation Order）及沒入判決（Judgment of Forfeiture）保存、管理或處分資產之職責。

為落實此項職責，AMLC 透過其資產管理組（Asset Management Group）確保所有經凍結、保全與沒入之資產，均依據凍結令、保全令及沒入判決進行監控、維護、保存，必要時進行處分，並移轉予菲律賓國家政府。

待決民事沒入案件資產統計（2003 年至 2023 年）

截至 2023 年 12 月 31 日，共有 119 件民事沒入案件待決，待保全資產總額為 9,143,220,299.09 比索（約合 1.59 億美元），包含銀行資產、保險資產、其他股票投資及不動產等。詳細內容如下表：

| 表格 9 待決民事沒入案件資產依資產類型統計 (2003 年至 2023 年) | |
|--|---------------------|
| 案件數量 | 119 |
| 銀行資產 ¹³⁴ | 3,900,448,592.34 比索 |
| 其他貨幣工具 ¹³⁵ | 277,568,924.03 比索 |
| 保險資產 ¹³⁶ | 236,517,787.22 比索 |
| 不動產（仍登記於被告名下） | 4,630,036,333.00 比索 |
| 機動車輛估價 | 98,648,662.50 比索 |
| 總計 | 9,143,220,299.09 比索 |

¹³⁴ 汇率轉換為比索

¹³⁵ 汇率轉換為比索

¹³⁶ 汇率轉換為比索

此外，下表列示待決民事沒入案件依犯罪類型區分之資產分布：

| 待決民事沒入案件資產依非法活動類型統計 | | | |
|---------------------|------------|------------------------|------------|
| 排序 | 非法活動 | 金額 | 佔全額百分比 (%) |
| 1 | 貪污 | 3,925,751,560.30 菲律賓比索 | 42.94% |
| 2 | 非法毒品 | 3,013,789,505.13 菲律賓比索 | 32.96% |
| 3 | 其他犯罪 | 904,378,702.96 菲律賓比索 | 9.89% |
| 4 | 詐欺 | 815,870,084.83 菲律賓比索 | 8.92% |
| 5 | 資恐（資助恐怖主義） | 483,430,445.86 菲律賓比索 | 5.29% |
| | 資產總額 | 9,143,220,299.09 菲律賓比索 | 100% |

5.3 資產沒入：刑事、民事或行政程序追討犯罪所得之經驗—成就與挑戰

5.3.1 中國香港

中國香港最常被限制與沒入之資產包括銀行帳戶內資金，以及存放於有執照企業或銀行之保險與證券資產。其他被沒入資產尚包含貴金屬、寶石、珠寶、手錶及實體現金。

案例研究 # 124：以洗錢方式處理電子郵件詐騙犯罪所得

詐欺；境外前置犯罪

2011 年，多個司法管轄區的公司因商務合作夥伴之電子郵件詐騙，遭誘騙匯款逾 500,000 港幣（約 69,570 美元）至一個由人頭在中國香港開設之銀行帳戶。隨後之調查顯示，該人頭在開設帳戶後已迅速離境。2023 年，香港警方成功阻止該犯罪所得資金之散逸，最終取得本地法院之沒入令，沒入該人頭帳戶內剩餘之犯罪資金。

來源 – 中國香港

案例研究 # 125：利用銀行帳戶洗錢

毒品相關犯罪

情報顯示，一對夫妻涉及以洗錢方式處理毒品相關犯罪收益。金融調查發現，2014 年至 2016 年間，該對夫妻透過 5 個個人銀行帳戶清洗犯罪收益高達 1,400 萬港幣（約 1,948,000 美元）。調查人員注意到的洗錢特徵包括頻繁、且大量的帳戶交易，與其收入明顯不相符。經調查後，該對夫妻遭控以洗錢罪，並於 2023 年法院審理後定罪，並沒入其名下價值 150,125 港幣（約 19,311 美元）之資產。

來源 – 中國香港

案例研究 # 126：洗錢集團利用外籍家庭幫傭工作為人頭帳戶

詐欺；跨國組織犯罪集團；境外前置犯罪

2021 年 4 月，香港聯合財富情報組 (JFIU) 與 A 司司法管轄區進行情報交流，發現一名外籍家庭幫傭在中國香港所持銀行帳戶涉入發生於 A 司司法管轄區之愛情詐騙未遂案件。進一步調查揭露，有超過 20 名外籍家庭幫傭將個人銀行帳戶售予洗錢集團。該集團再將帳戶用於接收來自多個線上詐騙案件所得資金，隨後立即透過自動櫃員機提領現金。香港警方逮捕兩名負責提領現金之集團核心成員，以及 24 名出售銀行帳戶之外籍家庭幫傭。其中，兩名核心成員及 6 名人頭帳戶提供者遭法院以洗錢罪名定罪，分別判處 8 個月至 30 個月不等之有期徒刑。法院亦核准沒入令，沒入總計 204,598.42 港幣（約 26,319 美元）、200 美元及 20 比索（約 0.35 美元）。其餘人頭帳戶涉案者仍在訴追中。

來源 – 中國香港

5.3.2 中國澳門

有關沒入犯罪工具及犯罪所得，中國澳門《刑法典》（Penal Code）特別設有專章規定犯罪所得之財產或權利之喪失，另規範被用於、或將被用於犯罪之財產，以及透過犯罪直接、或間接取得之報酬、物品、權利或利益，均得沒入。若某些犯罪所得無法以實體方式扣押，犯罪行為人須向中國澳門支付相應金額作為補償。

5.3.3 馬來西亞

馬來西亞在執行犯罪資產之沒入或充公時經常面臨以下挑戰：

- 難以建立犯罪資金或資產之軌跡或連結。
- 難以追蹤、聯絡被告，或被告已潛逃。
- 若資產已移轉海外，進行跨國資產返還往往困難重重（例如，不同法律架構差異、牽涉諸多司法管轄區等等）。
- 資產價值可能減損或折舊。

5.3.4 中華臺北

中華臺北《刑法》有關沒入之規定自 2016 年 7 月 1 日施行，截至 2024 年 2 月止，法院裁定沒入犯罪所得之總金額已超過 1,695 億臺幣（約 53 億美元）。

2023 年 11 月 17 日，憲法法庭就《毒品危害防制條例》第 19 條第 3 項之規定舉行辯論，並於 2024 年 1 月 26 日裁定。憲法法庭宣告，擴大沒入犯罪所得之規定與一般沒入目的相同，均旨在將非法取得財產回復其合法狀態，並非施加刑罰；此並不違反罪刑法定原則（*nulla poena sine lege*）、罪責原則（*culpability*）、無罪推定原則（*presumption of innocence*）及法律明確性原則（*the intelligible principle*）。此裁定認定，擴大沒入犯罪所得之規定係基於公共利益，與防制毒品犯罪之目的間具有合理關聯性，符合比例原則。

5.4 被沒入犯罪所得之使用與共享：包括對其他司法管轄區取回或送出被沒入資產之案例

5.4.1 中國

案例研究 # 127：跨境資產返還

國際合作

2015 年 10 月，中國湖南省公安機關針對一個犯罪集團展開調查。該集團成員超過 10 人，以網路購買境外商品及股票為誘因，要求參與者支付人民幣加入。參與者若能招募更多會員或購買更多產品，即可獲得佣金。此傳銷騙局波及 18 個省份，參與者近五萬人。

2015 年 12 月，該犯罪集團的首腦遭到逮捕，隨後因組織、領導傳銷活動罪被判刑。與此同時，湖南省公安機關在公安部「獵狐行動」辦公室指導部署下，與境外警方合作進行資產追繳作業。該犯罪活動所得透過地下匯兌網路（非法跨境匯兌業者）洗錢轉移。經過協商，2023 年，中方與外方司法管轄區達成資產分享原則協議，雙方各自從沒入資產中追回部分金額，外方司法管轄區分享並返還的資產總值約 1.66 億元人民幣（約 2,280 萬美元）。

來源 - 中國

5.4.2 日本

案例研究 # 128：基金投資績效造假詐欺之犯罪所得

詐欺；洗錢；沒入；徵收等值金額

被告 A 人士、B 人士、C 人士三人合作，以 A 人士擔任執行長之 A 公司所管理之基金，向某退休基金提出虛假投資績效報告，藉此詐得約 248 億日圓（約 1.58 億美元）。法院審理後判決三名被告有罪，並命其沒入及追徵與犯罪所得等值金額。

法院判決後，日本權責機關向 B 司法管轄區提出刑事司法互助請求，要求沒入存於 B 司法管轄區境內銀行帳戶之資金。2023 年 5 月，B 司法管轄區將約 7.17 億日圓（約 459 萬美元）移轉返還給日本。日本現正將此筆資金分配予被害人。

來源 - 日本

案例研究 # 129：以洗錢方式處理外匯交易詐欺犯罪所得

詐欺；洗錢；徵收等值金額

被告 A 人士與 B 人士兩人合作，透過一投資教室詐騙從事外匯交易之投資人，犯罪所得約 19 億日圓（約 1,200 萬美元）。法院審理後判定被告 A 人士與 B 人士有罪，並裁定沒入及追徵與犯罪所得等值之金額。

法院判決後，日本向 A 司法管轄區提出刑事司法互助請求，沒入被告 B 人士存於 A 司法管轄區銀行帳戶內之約 1.2 億日圓（約 76.9 萬美元）。收到 A 司法管轄區返還該筆資金後，日本已將此款項分配給被害人。

其餘約 17.8 億日圓（約 1,120 萬美元）之犯罪所得則已匯至其他司法管轄區之銀行帳戶。

來源 - 日本

案例研究 # 130：投資詐欺與洗錢

詐欺；獨立洗錢

馬來西亞金融情報中心接獲外國 FIU 通報之可疑活動報告（SAR），指出兩名馬來西亞籍人士於虛擬資產服務提供商帳戶內存有大量虛擬資產。

馬來西亞皇家警察（RMP）經調查後發現，外國金融情報中心通報之虛擬資產或許與馬來西亞境內一宗先前運作之龐氏騙局有關。該龐氏騙局係以比特幣（Bitcoin）投資計畫為主軸，透過社群媒體吸引投資人參與，承諾每日發放投資報酬，並提供推薦佣金誘使投資人引介更多新參與者加入該計畫。

馬來西亞權責機關隨即採取行動，提出刑事司法互助請求，透過外國司法管轄區協助扣押存於相關虛擬資產帳戶內之資產，總價值約 3,450 萬美元。目前案件調查仍持續進行中。

來源 - 馬來西亞

5.4.3 新加坡

案例研究 # 131：成功將資金返還至 L 司法管轄區

貪污；國際合作；自行洗錢；第三方洗錢；購置不動產；資產返還

2015 年，新加坡貪污調查局（CPIB）接獲通報，得知 X 司法管轄區之航空製造公司 U 聘用 L 司法管轄區之「顧問」，向該司法管轄區之國家航空公司高層官員支付賄款，以取得飛機供應及飛機引擎售後服務等相關合約。經調查後發現，該「顧問」即為 A 人士，涉嫌收受賄賂之航空公司官員分別為：總裁兼執行長 B 人士、維修及機隊管理執行副總裁 C 人士，以及資產管理副總裁 D 人士。

新加坡貪污調查局亦接獲通報，指出上述涉案人員均於新加坡擁有銀行帳戶，且相關賄款可能已透過新加坡銀行體系支付及洗錢。貪污調查局經追查資金流向後發現，A 人士將資金透過其本人、或其實質控制之公司帳戶層層轉移，支付予 B 人士、C 人士及 D 人士。

X 司法管轄區、L 司法管轄區以及新加坡貪污調查局於是對上述貪污及洗錢犯罪展開聯合調查。

帳戶與財產之扣押

2017 年 1 月 16 日，貪污調查局依據《刑事程序法典》（Criminal Procedure Code），扣押涉案之 32 個銀行帳戶，以及登記於 B 人士名下之一處私人不動產。該不動產之購置價格為 2,626,140 新加坡元（約 1,944,000 美元）。

其他資訊

2017 年 1 月 17 日，X 司法管轄區之權責機關與公司 U 達成暫緩起訴協議（Deferred Prosecution Agreement, DPA）；該協議涵蓋 12 項罪名，包括共謀貪污、偽造帳目及未防止賄賂罪。依該協議所述，相關貪污行為歷時達 30 年，涉及數個司法管轄區，包括 L 司法管轄區。

2019 年底，L 司法管轄區權責機關取得 D 人士之合作，同意將其於新加坡銀行帳戶內剩餘資金繳交給 L 司法管轄區當局。

2020 年 9 月 3 日，新加坡貪污調查局協調律政司（AGC）及 L 司法管轄區權責機關，成功將 D 人士存於新加坡銀行帳戶內之 1,402,125.49 美元資金，以自願返還方式轉移回 L 司法管轄區。

2020 年 5 月 8 日，B 人士與 A 人士於 L 司法管轄區被法院裁定貪污與洗錢罪名成立。

2021 年 4 月，新加坡接獲 L 司法管轄區提出之私人不動產外國沒入令（Foreign Confiscation Order）。新加坡權責機關目前正向高等法庭（High Court）申請核發國內沒入令，並將在法院批准後執行該不動產之處分程序，將所得資金返還至 L 司法管轄區。

來源 - 新加坡

案例研究 # 132：成功沒入資產

貪污；可疑交易交易通報；國際合作；自我洗錢；資產返還

2017 年，新加坡貪污調查局接獲資訊指出，S 司法管轄區某國營鐵路公司前總裁 A 人士，因涉嫌收受約 3,400 萬美元賄款，正遭 S 司法管轄區權責機關調查。A 人士及其妻子在 S 司法管轄區權責機關執行逮捕前潛逃出境，並疑似將賄款洗錢至美國、澳洲、賽普勒斯、聖克里斯多福及尼維斯、中國香港、中國及新加坡等地。

新加坡可疑交易通報辦公室（STRO）經分析發現，2017 年 3 月，有疑似犯罪所得資金匯入以 A 人士妻子名義於新加坡某投資平台開設之帳戶，遂將此資訊通報予貪污調查局。

貪污調查局根據通報資訊展開調查，以確認該投資平台是否觸犯《貪污、販毒及其他重大罪行（沒入利益）法》（CDSA）相關罪行，並依據《刑事訴訟法》（CPC）職權扣押 500,028 美元資金。經深入調查，證實該投資平台並未涉入犯罪。

經 2018 年 3 月至 2020 年 1 月期間，CPIB 與 S 司法管轄區權責機關密切合作，以維護所扣押之 500,028 美元資產。S 司法管轄區權責機關提供充分證據，證明相關資金確實來自貪污犯罪所得。

2020 年 1 月，S 司法管轄區法院頒布沒入令，沒入位於新加坡之上述資產。經由目前新加坡權責機關正進行資產變現程序，預計於 2024 年將相關資金返還 S 司法管轄區。

來源 - 新加坡

案例研究 #133：與外國司法管轄區密切合作成功定罪並沒入資產

貪污；國際合作；自我洗錢；第三方洗錢；購置不動產；資產返還

2016 年，新加坡貪污調查局針對兩名新加坡籍人士 A 人士與 B 人士（兄妹）展開調查，兩人涉嫌協助 S 司法管轄區的兩家貨運公司取得某大型硬碟製造商 X 公司的貨運合約。A 人士為 X 公司資深總監，其向 B 人士洩漏機密資訊，由 B 人士協助上述兩家貨運公司取得相關合約。貨運公司取得合約後，以支付佣金為名，將賄款支付予位於 T 司法管轄區、由 B 人士男友所持有之 Y 公司，賄款總額約為 160 萬美元。上述「佣金」匯入 B 人士男友於 S 司法管轄區之個人銀行帳戶。隨後 B 人士將資金提領至其本人於 S 司法管轄區之帳戶內；A 人士則利用 B 人士的提款卡於新加坡提領現金，並以 B 人士名義購置新加坡的不動產。

新加坡權責機關向 S 司法管轄區提出刑事司法互助（MLA）請求，取得銀行帳戶及相關交易明細，S 司法管轄區亦協助約談兩家貨運公司代表人。自 S 司法管轄區取得之證據對案件審理至關重要，證實 A 人士提領 703,480 新加坡元（約 547,082 美元），支付不動產購置及相關法律費用。該不動產購置價格為 112 萬新加坡元（約 871,005 美元），新加坡貪污調查局已對該不動產設定中止轉讓申請（caveat）。

2023 年，A 人士及 B 人士遭法院裁定貪污及違反 CDSA 相關罪名成立，新加坡最終成功沒入其犯罪所得資產約 220 萬新加坡元（約 170 萬美元）。

來源 - 新加坡

5.4.4 中華臺北

案例研究 # 134：拉法葉艦採購弊案

國際合作

由於 A 與 B 司法管轄區對前述拉法葉艦案之協助逾 20 年，考量《聯合國反貪污公約》（UNCAC）精神及國際實務慣例，中華臺北已與 A 及 B 司法管轄區 分享相關返還資產，以促進長期國際協力合作。

來源 - 中華臺北

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（FSRB）及觀察員組織於 2023 至 2024 年間發布之相關態樣報告。

6.1 防制洗錢金融行動工作組織

FATF 發表以下報告，揭示部分最新的防制洗錢與打擊資恐方法及趨勢。

《網路詐騙之非法資金流動報告》（*Illicit Financial Flows from Cyber-enabled Fraud*）¹³⁷

透過網路進行之詐欺與騙局，已逐漸成為網路犯罪的主流。若未能有效遏止，此等犯罪手法將更趨複雜，並在更多組織性犯罪集團涉入並利用新科技（如生成式人工智慧）創造的機會後，形成更大的威脅與風險。

此報告主要著眼於源自「網路詐騙」（Cyber-enabled fraud, CEF）之非法資金流動，此類犯罪活動係透過網路環境進行，並具備以下特徵：

- 涉及跨國犯罪行為，例如跨國犯罪者與跨境資金流動。
- 涉及欺騙性社交工程技巧（亦即操縱受害者以取得機密或個人資訊）。

此報告旨在強化各國權責機關對網路詐騙威脅的風險認知，並建構於 FATF 與其他國際組織（包括艾格蒙聯盟、歐洲刑警組織及國際刑警組織）現有的研究成果之上，並試圖辨識能進一步加強風險認知的重大、及新興發展趨勢。

本專案由新加坡（代表 FATF）、香港金融情報中心（代表艾格蒙聯盟）及國際刑警組織（INTERPOL）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：亞塞拜然、巴西、比利時、加拿大、中國、歐洲理事會、歐盟執委會、歐洲刑警組織、德國、西非政府間防制洗錢組織（GIABA）、印度、義大利、以色列、日本、馬來西亞、墨西哥、歐洲理事會防制洗錢與打擊資恐評估專家委員會（MONEYVAL）、巴基斯坦、葡萄牙、沙烏地阿拉伯、多哥、英國及美國。

此報告之研究發現奠基於以下基礎：審視既有文獻與公開來源資料-包括艾格蒙聯盟及國際刑警組織所提供之數據及研究成果；向 FATF 全球網路及艾格蒙聯盟（分別涵蓋逾 200 個司法管轄區及 170 個金融情報中心）徵詢有關風險、執法架構與策略、國內及國際合作協調機制等資訊，專案團隊總共收到超過 80 個代表團提供之意見與資料；2023 年 4 月於 FATF 聯合專家會議及 2023 年 5 月私部門諮詢論壇中所分享之討論與觀點，包括與私部門之特別會談。

主要發現與建議

網路詐騙（CEF）是逐漸成長的跨國組織性犯罪活動，此種犯罪集團通常具備結構嚴密、專業分工明顯之特性，包括專業洗錢團體。這些團體亦可能以較為鬆散、及去中心化的方式分散於不同司法管轄區，使調查網路詐騙活動工作變得更加複雜。此外，網路詐騙集團亦被發現與其他類型犯罪活動有所關聯，特別是涉及人口販賣與網路詐騙電話詐騙中心內之強迫勞動、以及與北韓進行之非法網路活動相關之資武擴犯罪行為。

洗錢團體及專業協助者（professional enablers）皆參與網路詐騙相關洗錢流程。此類洗錢通常涉及人頭帳戶，但亦可能包括空殼公司或合法企業。洗錢網路亦會利用各種不同類型的金融機構，包括銀行、支付及匯款服務業者，以及虛擬資產服務提供商等。為進一步隱匿其非法收益之資金流向，犯罪分子會採用多種洗錢手法相互搭配，例如使用現金交易、貿易洗錢（TBML）、未被核准的金融服務等伎倆。

數位化宣導下，「網路詐騙」（CEF）犯罪分子進行非法活動的規模、範圍及速度也隨科技增加。其等利用各種工具與技術，透過詐術欺騙受害者，或操縱其心理狀態及情緒，以達到盡可能榨取資金之目的。網路詐騙犯罪集團也利用科技發展，得以更輕易、更快速地以洗錢方式處理犯罪所得。虛擬服務（如線上遠端開立帳戶）

¹³⁷ FATF - 《網路詐騙之非法資金流動報告》：<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html>

使犯罪分子得以輕易設立海外帳戶，透過跨境金融交易迅速清洗犯罪所得。此外，犯罪分子還透過社群媒體與通訊平台，大規模跨境招募人頭帳戶，並迅速利用新興數位金融機構、電子商務、社群媒體及影音串流平台等非傳統金融部門之漏洞。

為更有效遏止網路犯罪，各司法管轄區必須：採取措施增加受害者通報並強化可疑交易報告；有效分析大量資訊流；因網路犯罪犯罪具有跨領域性質，各國內部須建立強而有力的協調機制，整體防制網路犯罪與相關洗錢活動。

網路犯罪之前置犯罪發生地通常與資金洗錢地點不同。犯罪所得可迅速透過跨國、多重帳戶之網路洗錢，各司法管轄區必須採取多邊協作，迅速有效地攔截跨境清洗的網路犯罪所得；並應利用並支持現有（及未來可能出現）的多邊機制（如國際刑警組織的 IGRIP 計畫、艾格蒙聯盟之 BEC 專案），以迅速達成國際合作及資訊交換，提升打擊網路犯罪之效能。

最後，此報告亦提供風險指標清單及反詐騙之相關要求與控管措施，協助公私部門識別並防制網路犯罪及相關洗錢活動。

《濫用投資取得公民與居留權計畫》¹³⁸

每年全球有數萬人透過投資移民計畫，成為非其出生地的公民或永久居民。此類政府主導之「投資取得公民權與居留權」（Citizenship and Residency by Investment，CBI/RBI）計畫可謂雙贏政策，除促進地主國經濟成長（例如擴大外國投資管道）外，亦方便富裕人士快速取得公民權或居留權及其相關權利，免去一般耗時的移民程序。這些計畫吸引之客戶眾多，其中多數合法取得財產且目的單純。然而，亦存在部分犯罪分子濫用此類計畫，清洗、隱藏犯罪所得或從事新的犯罪行為，包括金融犯罪，破壞此計畫之原訂目標。

此報告係 FATF 與經濟合作暨發展組織（OECD）聯合撰寫，整體檢視投資移民計畫之洗錢與金融犯罪風險，包括海外行賄、詐欺及貪污相關風險，以及其他涉及公共廉政、稅務及移民政策考量。

此專案由美國與英國專家共同主持，OECD 及 FATF 畘處提供支援，專案團隊包括 FATF 全球網路之 19 個成員及 3 個觀察員組織：安地卡及巴布達、巴哈馬、加拿大、中國、多明尼加、歐盟執委會、希臘、格瑞那達、印度、愛爾蘭、馬爾他、墨西哥、奈及利亞、葡萄牙、聖露西亞、千里達及托巴哥、土耳其、英國、美國，加勒比海防制洗錢金融行動工作組秘書處、國際貨幣基金組織（IMF）及 OECD。

此專案參考 FATF 全球網路中 36 個司法管轄區提供之間卷調查結果、以及 FATF 於 2023 年 4 月專家聯合會議。此外，報告內容亦包括 OECD 公共廉政資深官員工作組（SPIO）所發送之間卷調查結果，以及來自 2023 年 5 月 FATF 私部門諮詢論壇中，與私部門投資移民業務及金融業從業人員之討論成果。亦參考學界、政府及非營利組織研究論文之觀點。

主要發現與建議

犯罪分子利用投資移民計畫中的多項漏洞，實施大規模詐騙，並透過這些漏洞將價值數十億美元之犯罪及貪污所得進行洗錢；同時亦將資產藏匿於法令遵循程度較差、或執法較弱之司法管轄區，從而助長有組織犯罪活動並逃避執法機關追查。公民權投資（CBI）計畫尤其脆弱，因其讓不法分子更易跨國移動；其等取得新身分文件後可於其他國家開設銀行帳戶、成立空殼公司，隱匿真實身分或逃避稅務及其他金融義務。

公民與居留權投資計畫（CBI 及 RBI）可能為擁有犯罪所得之富裕人士提供多種便利，包括將資產及家人安置於海外，以阻撓資產追繳、合理化可疑的大額交易，及便利大筆非法資金之跨境流動。此類投資計畫成為參與者進入其他大小司法管轄區乃至區域金融市場的入口，讓取得新公民或居留權者享有其原籍國或原居地原本無法取得之金融服務及市場准入，並且因身為國內人士（而非外國人）而受到較寬鬆之金融審查。

¹³⁸ FATF - 《濫用投資取得公民與居留權計畫》：<https://www.fatf-gafi.org/en/publications/Methodsandtrends/misuse-CBI-RBI-programmes.html>

投資移民計畫通常極為複雜及國際化，涉及許多中介機構參與計畫設計與推廣，及政府多個機關協調運作之需求，因此可能在協調、執行與監管等面向面臨諸多挑戰。這此類計畫亦易受到「專業協助者」（professional enablers）及詐欺集團濫用，以藉機牟利。例如犯罪、不盡責或共謀的房產經紀、財富管理公司、移民代理商、行銷公司及禮賓服務公司等都可能助紂為虐。前述人員往往未能進行盡職調查（due diligence）及金融犯罪通報義務，甚至協助客戶向權責機關提交虛假或誤導性文件，以達成犯罪目的。

尤其當政府缺乏對計畫的有效治理時，更易產生濫用機會。例如公共部門與私部門角色分工不明確、利益衝突未妥善處理，以及資源不足以有效監督執行成效時。若內部缺乏有效的控制與稽核機制，且政府機關之間及跨境間之協調不足，前述問題會進一步惡化。此外，若投資移民計畫出現遭犯罪濫用之情形，可能導致第三國取消免簽證待遇，進而損害國際商業與外交關係。

為協助政策制定者與計畫權責機關強化計畫治理、解決洗錢及金融犯罪風險，此報告提出多項風險控管措施，審慎分析洗錢及貪污風險、設定明確計畫目標，並於設計及實施階段納入廉政措施，可以為投資移民計畫奠下穩固基礎。此外，國內執法機關、移民權責機關與金融情報中心之間有效協調，也至關重要。由於此類風險可能超出投資計畫所在司法管轄區，亦有必要透過多邊合作迅速交換資訊，並促進相互間之執法機制之協調支援。

許多允許私人部門參與投資的司法管轄區日益面臨詐欺風險，不僅需監控資金來源，更須注意資金後續去向。

政策制定者、計畫權責機關、金融機構及執法單位皆應提高警覺，不僅關注申請人本身，也需注意參與投資移民交易之專業協助者及中介機構可能涉及的洗錢與金融犯罪風險。明確劃分公私部門的角色與責任，對於防止私人利益不當滲透投資移民計畫之執行是重中之重。

《透過跨機構網路返還國際犯罪所得》¹³⁹

此報告旨在探討追討犯罪所得機構網路（Asset Recovery Inter-Agency Networks, ARINs）之角色與功能，供全球政策制定者及執法機關參考。ARINs 協助各國執法機關跨越司法管轄區，共同追蹤包括洗錢及相關犯罪所得之非法資金。此報告提供 ARINs 之整體回顧，包括其全球影響、角色、管理、所面臨之挑戰，以及與其他國際組織的合作狀況。

此報告旨在協助政策制定者更深入了解 ARINs 的角色與功能，並指出其在改善作業實務、強化績效監督及深化與國際組織合作等方面的潛力與方向。此外，此報告亦強調建立健全的資料蒐集與通報機制之重要性，以彰顯 ARINs 在打擊全球金融犯罪中不可或缺的價值與貢獻。

此報告係防制洗錢金融行動工作組織（FATF）所宣導專案之一部分，目的在提升與 ARINs、其等秘書處、及其他相關全球資產返還國際組織之合作。

主要發現與建議

追討犯罪所得跨機構網路（ARINs）於資產追討過程中，能提供非正式的協助，包括資產辨識、追蹤、扣押、凍結、沒入及返還作業。然而，儘管 ARINs 扮演重要角色，政策制定者對 ARINs 之本質，及其對全球犯罪資產追討所作之貢獻，往往缺乏清晰的認識。ARINs 的使用亦未普及或系統化，全球僅少數調查透過這些網路促成。

ARINs 在建立執法機關從業人員間的互信方面發揮關鍵作用，亦與相關國際組織合作，並可擔任與其他區域性網路之聯繫橋樑。然而，ARINs 與其他國際組織之間的協調往往不足，因而限制促進員國司法能力的機會。

雖然 ARINs 覆蓋範圍已逐步擴大，但在中東、北非及中非地區仍存有區域性缺口。目前，ARINs 共有 178 個成員國司法管轄區，其中包括 FATF 全球網路 205 個司法管轄區中的 159 個成員國。

¹³⁹ FATF - 《透過跨機構網路返還國際犯罪所得》：[https://www.fatf-gafi.org/en/publications/Methodsandtrends/recovering-international-proceeds\(犯罪所得\)-crime-inter-agency-networks.html](https://www.fatf-gafi.org/en/publications/Methodsandtrends/recovering-international-proceeds(犯罪所得)-crime-inter-agency-networks.html)

各個ARIN獨立運作，均設有自己的治理架構、職責範圍及指導方針。儘管參與 ARIN 並非強制性，但事實證明這些網路能有效促進調查人員與資產追討辦公室間的聯繫，強化跨境溝通及互信。透過ARINs的協助，各司法管轄區得以成功取得重要且關鍵的資產資訊，包括疑似犯罪人與洗錢者在其他司法管轄區所持有之銀行帳戶、企業、房地產及登記財產。強化跨境溝通及互信。透過ARINs的協助，各司法管轄區得以成功取得重要且關鍵的資產資訊，包括疑似犯罪人與洗錢者在其他司法管轄區所持有之銀行帳戶、公司、房地產及登記財產等。

雖然 ARINs 在許多案件中扮演重要角色，但仍面臨資源不足的挑戰。根據估算及質量分析回饋顯示，部分主要的 ARINs 每年可能需處理數百甚至上千筆來自成員國的資產追蹤請求。儘管並非所有 ARINs 皆面臨此情況，但這些數據凸顯其在國際調查中可能扮演的重要角色。然而，大多數 ARIN 的秘書處人力不足，各網路間資源配置差異甚大，普遍面臨難以有效協助成員國司法管轄區、及後續追蹤調查請求的困難，影響整體資產追討的效能。此外，如何維持 ARIN 秘書處職能財務的長期永續性，也是共同面臨的一大挑戰。語言及文化障礙亦為影響 ARINs 效能的重要因素。

ARINs 與各 FATF 型區域組織（FSRBs）的關係因地區而異，某些地區協調密切，但也存在完全缺乏合作的情況。

虛擬資產：《針對虛擬資產及虛擬資產服務提供商落實FATF標準之重點更新》¹⁴⁰

2019 年，FATF 將其全球防制洗錢及打擊資恐標準延伸適用於虛擬資產及虛擬資產服務提供商。為強化第 15 項建議（R.15）之實施，FATF 於 2023 年 2 月採納一份路線圖。作為此路線圖一部分，FATF 公布一份表格，載明各成員國、及其他具實質重要資產服務提供商活動之司法管轄區，對第 15 項建議實施情況之現狀。FATF 及其虛擬資產聯繫小組（VACG）將持續進行宣導，並提供協助，以支持全球符合第 15 項建議之要求，並將於 2025 年更新該表格。

此報告係 FATF 針對虛擬資產、及虛擬資產服務提供商（包括「轉帳規則」）之第五次專題實施檢視，並此項工作由「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聯合主席。此報告部分資訊來自 VACG 與私部門之持續討論。

主要發現與建議

根據 2023 年的調查結果，部分具有實質且重要虛擬資產服務提供商活動之司法管轄區，已逐步宣導、或已完成防制洗錢與打擊資恐相關法規的建置工作。然而，由於全球對 FATF 相關標準的落實程度仍顯不足，導致虛擬資產與虛擬資產服務提供商仍存在遭受濫用的風險，且整體標準的落實程度仍落後於其他金融領域。因此，此報告針對公共與私部門提出需加強改善的主要領域、及具體建議。

虛擬資產持續被用於資助大規模毀滅性武器擴散（PF），並成為詐騙集團、恐怖組織及其他非法行動者的工具。北韓（DPRK）持續透過竊取或勒索等手段獲取虛擬資產，且其洗錢手法日益複雜。此外，虛擬資產也逐漸成為恐怖組織重要的資金來源，尤其是伊斯蘭國（ISIL）在亞洲及敘利亞境內的恐怖團體，更常使用穩定幣（Stablecoins），並嘗試採用具備強化匿名性的加密貨幣。

在虛擬資產聯絡小組（VACG）的溝通交流中，私人部門利害關係人報告市場最新發展情況，包括穩定幣被用於洗錢、資恐與資武擴用途比例日漸增加，以及去中心化金融（DeFi）架構持續遭駭客攻擊等。此外，某些利害關係人也指出在運用智能合約（smart contracts）進行風險抵減措施方面已有一定進展。若干司法管轄區在法規、監理與執法方面亦有進步，例如針對穩定幣服務提供商實施防制洗錢、打擊資恐與打擊資武擴法規，包含轉帳規則（Travel Rule）要求，對去中心化金融架構採取監管與執法措施，並對去中心化金融及未託管錢包（包括點對點交易）進行風險評估。

¹⁴⁰ FATF - 《虛擬資產：針對虛擬資產及虛擬資產服務提供商落實FATF標準之重點更新》：<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vaps-2024.html>

《「守門人」與貪污相關的技術遵循水平檢視》¹⁴¹

貪污與洗錢之間存在密不可分的聯繫，貪污行動者必須透過洗錢程序才能享有其等之犯罪所得。作為金融體系的把關者，非金融專業人士可能有意或無意地促成高層級貪污行為。

為降低此類風險，防制洗錢金融行動工作組織（FATF）於 20 多年前即已採取措施，要求全球司法管轄區對律師、會計師、信託及公司服務業者（TCSP）及不動產經紀人等守門人實施防制洗錢與打擊資恐措施。上述措施旨在降低相關行業遭受洗錢與貪污威脅的弱點，透過向專業人士提供必要的專業知識，使其具備辨識可能犯罪跡象的能力。然而，若這些專業人士未依據 FATF 標準進行有效監管，則仍可能暴露於嚴重的犯罪風險中，且缺乏可協助他們察覺洗錢相關警訊的必要措施。

為評估目前施行現況，FATF 展開此次水平檢視（Horizontal Review），並識別成員國需進一步優先改善的領域。此為深度檢視涵蓋成員國司法管轄區，針對守門人落實 FATF 建議要點所採取的措施。

此次 FATF 水平檢視的範圍包括成員國司法管轄區對第 22 項建議（準則 1 至 3）、第 23 項建議（準則 1、2 與 4）及第 28 項建議（準則 2 至 5）的遵循情形，並聚焦於以下非金融專業人士：不動產經紀人、律師、公證人、其他獨立法律專業人士、會計師及信託及公司服務業者。這些專業人士作為守門人，在預防及偵測洗錢、及包括貪污在內的前置犯罪行為中扮演關鍵角色，惟亦可能故意助長貪污及相關洗錢行為。

主要發現與建議

表面上看來，此次水平檢視的結果是正面的——超過半數的 FATF 成員國得分超過 80%。然而，考量七個得分低於 50% 之 FATF 成員國司法管轄區所處的背景及其重要性時，整體情況就不容樂觀。此等司法管轄區占全球 GDP 一半以上。

儘管一般認為法律專業界的防制洗錢與打擊資恐規範較其他守門人行業更為寬鬆，但本次水平檢視發現律師、會計師、信託及公司服務業者（TCSP）及不動產經紀人等四個被檢視的守門人行業間，在規範涵蓋程度上的差異並不顯著。

此外，本次檢視發現，某些 FATF 建議中的關鍵義務的遵循程度，仍落後於其他義務。這些核心義務包括進行客戶盡職調查、實施內部控管措施，以及確保主管機構具備足夠權限進行風險導向的監理等，均為有效解決守門人行業易受洗錢及貪污威脅之重要要求。

在這些方面仍有不足之 FATF 成員國司法管轄區，應盡速加強改進，以符合 FATF 長期以來對此領域的相關建議。此報告之調查結果、分析或結論，不影響或預判未來任何相互評鑑報告之結果。

¹⁴¹ FATF - 《「守門人」與貪污相關的技術遵循水平檢視》：<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Gatekeeper-TC-Corruption.html>

FATF 區域性防制洗錢組織

6.2 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（The Caribbean Financial Action Task Force，CFATF）已發布以下兩項研究專案報告。

CFATF 大麻專案報告 (Cannabis Project Report) ¹⁴²

此專案探討大麻合法化對防制洗錢與打擊資恐帶來的影響。旨在協助會員司法管轄區理解大麻去刑事化、合法化或採取混合方式所產生的防制洗錢與打擊資恐風險。此專案重點在掌握各司法管轄區採用的不同作法、辨識相關風險，並提出風險抵減策略之建議。

CFATF 《2023年去風險更新報告》 (De-Risking Update 2023) ¹⁴³

此次更新為 2018-2019 年間對 CFATF 成員國司法管轄區去風險（de-risking）情況評估的延續，聚焦於中央銀行及金融機構為減輕「去風險」影響所實施的措施。此外，報告亦說明去風險對區域的負面影響以及相應的應對措施，並詳述 2019 年至 2022 年間觀察到的去風險做法。

6.3 歐亞防制洗錢與打擊資恐組織（EAG）

歐亞防制洗錢與打擊資恐組織完成以下態樣專案。

《EAG 防制洗錢與打擊資恐金融調查指引》

根據 EAG 第 34 次全體會議決議，態樣及打擊資恐與犯罪工作小組（WGTYP）專案團隊編製《EAG 防制洗錢與打擊資恐領域金融調查組織與執行方法建議》文件。（*EAG Methodological Recommendations on Organising and Conducting Financial Investigations in the AML/CFT Sphere*）¹⁴⁴ 參與本專案團隊的司法管轄區與組織包括：EAG 成員國（白俄羅斯、印度、哈薩克、中國、吉爾吉斯、俄羅斯、塔吉克、土庫曼與烏茲別克）、EAG 紘書處，以及 EAG 觀察員組織（FATF 紘書處、APG、獨立國協反恐中心（CIS ATC）、反綁架與組織犯罪辦公室（BKBOP）、歐亞經濟委員會（EEC）、集體安全條約組織（CSTO）、上海合作組織地區反恐機構（SCO RATS）、中亞區域資訊協調中心（CARICC））。

文件涵蓋了以下議題：防制洗錢與打擊資恐金融調查之法律規定、執行金融調查之基礎、取得資訊之類型與金融調查成果之運用、特定類型金融調查的特性、私部門參與金融調查之情形、國內及國際合作、團體（整合）金融調查，以及相關問題與建議行動。此文件於 EAG 第 39 次全體會議通過。

主要發現與建議：

- 金融調查是確保國家資金流動、與財產流通透明化之有效工具，因此應在法律體系的基本架構內，儘可能廣泛地涵蓋金融調查所涉及之領域與任務。
- 應透過明確界定具體任務之權責機關及其職權範圍，以完善金融調查機制並提高其效能。
- 為提高金融調查的效率，應積極推進金融資訊與其他相關資訊數位化，並確保執行金融調查之機關能直接、順暢地取得資訊。
- 持續提供針對金融調查人員的專業化培訓，並改善金融調查人員的遴選與組織。

¹⁴² 加勒比海防制洗钱金融行動工作組織（CFATF）專案報告: <https://www.cfatf-gafic.org/documents/resources/22443-cfatf-cannabis-project-report/file>

¹⁴³ 加勒比海防制洗钱金融行動工作組織 - CFATF 去風險更新報告 2023 年: <https://www.cfatf-gafic.org/documents/resources/22442-cfatf-de-risking-update-2023/file>

¹⁴⁴ Eurasian Group on Combating Money Laundering and Financing of Terrorism - 《EAG 防制洗錢與打擊資恐金融調查指引》 (EAG AML/CFT Financial Investigation Guidance) : https://eurasiangroup.org/files/uploads/files/Public_typerology_reports/FI_Guidence_eng.pdf

《貪污犯罪及侵害公共服務利益犯罪所得之洗錢行為》¹⁴⁵

此態樣研究專案旨在透過防制洗錢的視角分析貪污威脅，進一步瞭解貪污行為的機制與弱點，從而辨識在貪污案件中被用於洗錢的工具與方法，並掌握目前趨勢、新興威脅、漏洞與態樣，以提升對貪污案件及後續洗錢行為的警覺與及早偵測之機會。此研究成果旨在供執法機關、金融情報中心、防制洗錢與反貪污主管機構、銀行與金融業界及私人部門參考運用。本專案由印度共和國主導，所有 EAG 會員均參與其中。此文件於 EAG 第 39 次全體會議通過。

主要發現與建議：

- 對於貪污與洗錢案件調查隸屬不同機構的成員國，應在調查貪污罪行時，同步進行金融調查，以探索或調查可能涉及的洗錢罪行。
- 加強對重要政治性職務人士（PEP）之客戶盡職調查措施。
- 推廣建立實質受益權（beneficial ownership）登記制度，並可能要求法人及法律協議必須公開其最終受益所有人。
- 宣導國際合作：提出清楚簡潔的合作請求，並在刑事司法互助（MLA）請求中，提供充足的輔助資訊；在正式送出請求前，頻繁有效地利用非正式溝通管道，以確保正式管道提交之請求能及時有效執行；對起草與提交請求的相關人員與調查人員提供定期訓練與協助；發展與推行刑事司法互助電子交換平台。
- 強化調查與執法能力：提供足夠資源、訓練及技術協助予負責調查及防制洗錢的執法機關與金融情報中心，使其專業技能與金融領域的科技發展並駕齊驅。此外，應鼓勵企業落實健全的內控措施、風險管理系統及員工訓練計畫，以有效辨識洗錢風險及企圖。
- 加強資產返還能力：可設立專門負責追討非法資產的單位或機構，以集中精力於追討犯罪所得、或被盜資產工作。
- 數位化與科技解決方案：新冠肺炎疫情促進包括金融領域在內的各個產業的數位化進程。數位平台與線上交易則提供各國政府透過科技解決方案有效偵測、及防制洗錢與貪污行為的機會。先進數據分析、人工智能與機器學習演算法，可以更有效地辨識可疑的交易模式與行為。

以洗錢方式處理非法毒品與前驅物之犯罪交易所得¹⁴⁶

本專案旨在辨識以洗錢方式處理非法販運麻醉藥品犯罪所得之類型、方法與工具，以增進執法機關、金融機構及其他相關利害關係人對此議題之理解，冀能更有效地打擊此類犯罪活動。專案團隊研究洗錢活動之各面向，包括犯罪分子採行之方法及技術、現有法律與金融架構，以及國內外針對此類非法活動而制定之有效法律規範。本專案由印度共和國主導，所有 EAG 會員共同參與。此文件於 EAG 第 39 次全體會議通過。

主要發現與建議：

- 強化司法管轄區與國際組織間資訊共享及合作，以更有效偵測、進而破壞跨國毒品交易洗錢活動。
- 探討如何防止人頭帳戶濫用金融卡與電子錢包，並考慮對蓄意提供自己金融工具供他人使用（即「出租」銀行帳戶或工具）的公民追究法律責任之可行性。
- 提升執法機關人員、金融機構及其他相關組織對於毒品犯罪所得洗錢的辨識能力。
- 發展與落實可能被用於毒品犯罪所得洗錢之加密貨幣之交易監控機制。
- 檢視並調整機構內部控制規範的要求。
- 強化風險管理計畫。

¹⁴⁵ 歐亞防制洗錢與打擊資恐組織 - 《貪污犯罪及侵害公共服務利益犯罪所得之洗錢行為》：

[https://eurasiangroup.org/files/uploads/files/Public_typerology_reports/WGTYP_\(2023\)_7_rev_1_eng.pdf](https://eurasiangroup.org/files/uploads/files/Public_typerology_reports/WGTYP_(2023)_7_rev_1_eng.pdf)

¹⁴⁶ 此文件不對外公開，僅發佈於EAG網站之安全專區，供會員及觀察員使用。

<https://eurasiangroup.org/d.php?doc=69e98753d860c28af3bda71f1eff93ea>

《辨識涉嫌洗錢目的之資金追討訴訟標準》¹⁴⁷

首輪 EAG 區域風險評估報告¹⁴⁸指出，一項需要採取標準措施以抵減之區域性風險，即透過強制執行程序將資金轉移至境外，這種情形在實務上通常表現為利用基於虛假事由而作成的法院判決。在執行司法或其他裁定的階段，辨識可疑行為時存在重大挑戰與風險，可能導致犯罪所得流失。為減輕上述區域洗錢與資恐風險，EAG 秘書處制訂識別用於洗錢目的之可疑資金追討訴訟標準。此專案由 EAG 秘書處主導，所有 EAG 成員國參與。此文件已於 EAG 第 40 次全體會議獲得通過。

主要發現與建議：

- 在執行司法或其他裁定階段識別可疑行為時，存在重大挑戰與風險，可能導致犯罪所得流失。
- 在強制執行階段極難識別洗錢計畫，因為此程序階段不涉及對證據的實質審查，只有在明顯的情況下才可能識別可疑特徵。而洗錢案件中普遍採用的較隱蔽手法，在執行程序階段幾乎無法被察覺。
- 涉及隱蔽洗錢計畫之案件的法院或其他裁定通常以最快速度執行，因為犯罪者希望儘快合法化資金，避免曝光並使資金脫離權責機關掌控、或隱藏其後續去向。
- 司法、執法及執行機構相關人員能否及早發現可能的洗錢計畫至關重要。

EAG 預計於 2024 年 11 月通過以下態樣專案。

《EAG 成員國辨識涉嫌洗錢目的之資金追討訴訟程序指南》

- 本專案依據 EAG 成員國提出的建議，延續識別涉嫌洗錢目的之資金追討訴訟標準的制定工作；旨在建立辨識洗錢目的之資金追討訴訟的示範程序，以促進權責機關間的合作，並提出在司法程序中及對此類訴訟實質內容進行處理時可採取之行動。
- 本專案由 EAG 秘書處主導，並由 EAG 成員國代表團參與進行，相關內容依據 EAG 成員國法規分析制定。
- 此專案文件預計於 2024 年 11 月舉行的第 41 次 EAG 全體會議上通過。

成員國新風險營運環境監測報告

- 在第 37 次全體會議中，成員國通過「EAG 成員國新風險營運環境監測機制」（Mechanism to monitor the operational environment in the EAG Member States in terms of new risks）之發展階段。此文件係根據成員國於第 41 次全體會議召開前所提供之資料與資訊，所彙整而成的監測機制摘要先導版本。
- 此專案由 EAG 秘書處主導，並以 EAG 成員國提供之資訊為分析基礎。
- 此專案文件預計於 2024 年 11 月舉行的第 41 次 EAG 全體會議上通過。

虛擬資產用於犯罪目的之風險監測

- 此專案旨在識別 EAG 成員國使用虛擬資產所涉及的風險、威脅與漏洞，並提出相應的抵減方式。
- 此專案由俄羅斯聯邦代表團主導，並以 EAG 成員國提供之資訊為分析基礎。
- 此專案文件預計於 2024 年 11 月舉行的第 41 次 EAG 全體會議上通過。

6.4 東南非防制洗錢組織（ESAAMLG）

¹⁴⁷ 歐亞防制洗錢與打擊資恐組織 - 《辨識涉嫌洗錢目的之資金追討訴訟標準》：

https://eurasiangroup.org/files/uploads/files/Public_typology_reports/Criteria_for_identifying_suspicious_money_recovery_lawsuits_eng.pdf

¹⁴⁸ 歐亞防制洗錢與打擊資恐組織 - 《辨識涉嫌洗錢目的之資金追討訴訟標準》：https://eurasiangroup.org/files/uploads/files/Summary_RRA.pdf

東南非防制洗錢組織發表以下兩份報告：

《黃金、鑽石、紅寶石非法交易及相關洗錢與資恐活動》¹⁴⁹

此報告旨在描述 ESAAMLG 地區內促使黃金、鑽石、紅寶石非法交易，及相關洗錢與資恐活動的資金流動情形。報告列出風險指標與案例研究，有助於區域內相關機構辨識與調查貴金屬及寶石市場的非法活動，並強調迅速辨識與追蹤涉及洗錢與資恐的珍貴金屬及寶石之重要性。

由於貴金屬及寶石非法交易的豐厚收益，使此類犯罪活動成為洗錢與資恐的絕佳途徑。此類非法交易為有組織犯罪集團提供一種將非法現金轉換成穩定、匿名且易於交易資產的機制，便於實現、或投資來自犯罪活動的收益。貴金屬及寶石在查緝與沒入等刑事程序中不易被追蹤，已被作為購買禁運、或限制貨品的替代貨幣，例如黃金兌換古柯鹼、鑽石兌換武器；亦是儲存非法活動所得的工具之一。

貴金屬與寶石亦自原產地被走私至消費國，包括用於資助武裝衝突。此外，貴金屬及寶石的高價值，可能吸引相關權責機關官員在採掘與交易各階段索賄或受賄。若 ESAAMLG 地區內貴金屬與寶石持續被用於非法活動的，將對該地區的經濟與政治穩定構成嚴重威脅。

因此，各司法管轄區已積極努力，保護該產業免於被犯罪分子濫用的風險。為有效因應此類問題，該地區亟需更深入理解這些犯罪的本質，及其與地區特殊性之間的關聯。

報告中包含 ESAAMLG 成員國為應對挑戰而採取的最佳操作實務，包括設立專責單位、使用相關資料庫，以及與專家合作以協助辨識、追蹤和調查涉及貴金屬與寶石的非法金融活動等。

《ESAAMLG 25 週年紀念報告：回顧打擊金融犯罪與進步的傳承》（1999年-2024年） (Celebrating a Legacy of Fighting Financial Crimes and Progress) ¹⁵⁰

此報告紀念並深入評估 ESAAMLG 過去 25 年的運作成果，著重介紹該組織在東部及南部非洲地區取得之成就、面臨之挑戰及其所產生之影響。

6.5 拉丁美洲防制洗錢金融行動工作組織

拉丁美洲防制洗錢金融行動工作組織（GAFILAT）（The Latin American Financial Action Group）發布以下報告。

《2021-2022 區域態樣報告》¹⁵¹（以西班牙文出版）

GAFILAT 發布了 2021-2022 年度區域態樣報告，作為 2023 年雙年度區域態樣研究的成果。此報告旨在辨識洗錢與資恐的新模式、涉及的金額、與先前態樣報告相比出現的變化或變異、分析態樣與最近區域威脅更新之間的一致性，以及此等犯罪行為對 GAFILAT 成員國造成的影響。

6.6 中東與北非防制洗錢金融行動工作組織（MENAFATF）

《中東和北非地區法人及法律協議用於洗錢與資恐活動》報告

MENAFATF 成員國表示，願意落實一項法人及法律協議用於洗錢及資恐活動之態樣報告。此落實專案係依據初步研究與相關調查結果，指出全球非法金融活動持續利用法人與法律協議的情形，防制洗錢金融行動工作組

¹⁴⁹ 東南非防制洗錢組織 - 《黃金、鑽石、紅寶石非法交易及相關洗錢與資恐活動》：

https://www.esaamlg.org/index.php/methods_trends/readmore_methods_trends/15

¹⁵⁰ 東南非防制洗錢組織（ESAAMLG）- 《25 週年紀念報告：回顧打擊金融犯罪與進步的傳承（1999 年 -2024 年）》：

https://www.esaamlg.org/index.php/all_news/readmore_news/476

¹⁵¹ 拉丁美洲防制洗錢金融行動工作組織 - 《2021-2022 區域態樣報告》：<https://biblioteca.gafilat.org/?p=6966>

織（FATF）之互評報告（MERs）亦指出，各司法管轄區在防制上述濫用行為上仍有明顯不足，強調各國應全面有效落實 FATF 標準。

中東和北非地區之互評報告顯示，該地區之司法管轄區在防範法人與法律協議遭濫用於洗錢及資恐活動之相關標準遵循上，明顯存在缺口。許多受評司法管轄區在此方面需進行大幅度甚至根本性的改善，以避免與法律協議遭濫用的情形。

為有效解決此問題，FATF 已修訂第 24 項與第 25 項建議，強化法人實體所有權透明度，降低法人實體遭濫用之風險。FATF 亦發布詳盡指引，協助各司法管轄區有效執行上述標準。此態樣報告專案之目的在於評估法人實體於金融犯罪中遭濫用之風險，並提出具體建議以提升國際標準之遵循成效。

此專案之主要目標包括掌握法人實體涉入非法金融活動之風險、辨識相關威脅指標、分析實務案例，並建議可行措施，以提升國際標準之落實成效。此報告將分享最佳實務經驗，促請司法管轄區加速落實 FATF 之修訂標準，以應對偵測、及防制法人與法律協議遭濫用的相關挑戰。

此報告目前尚未公開發布，其內容亦參考來自 FATF、國際貨幣基金組織（IMF）、世界銀行、經濟合作暨發展組織（OECD）及稅務正義網路（Tax Justice Network）等機構之相關文獻。

6.7 專家委員會防制洗錢措施之評估

防制洗錢措施和資恐問題評估專家委員會（MONEYVAL）

《虛擬資產世界之洗錢及資恐風險》態樣報告¹⁵²

此報告旨在綜合呈現 MONEYVAL 成員國在虛擬資產與虛擬資產服務提供商領域所面臨的洗錢與資恐風險概況，包括各司法管轄區針對虛擬資產服務提供商所採取的規範及監管措施，並探討犯罪分子如何利用虛擬資產服務提供商與虛擬資產，進行犯罪所得之洗錢活動。MONEYVAL 成員國在落實金融行動工作組織（FATF）第 15 項建議上仍有困難，約有 80% 的受評估成員國在此項標準上僅部分符合、或完全未符合要求。

此報告亦探討執法機關是否擁有足夠的權力與工具，以調查、追蹤及採取暫時性措施處理虛擬資產，並列舉犯罪分子使用虛擬資產平台支援金融犯罪活動之類型與權責機關調查之實際案例。此外，報告也特別指出在對此領域實施風險導向監理時所面臨的良好操作實務與挑戰。

觀察員組織

6.8 亞洲開發銀行

亞洲開發銀行（Asian Development Bank，ADB）發表下列報告：

《國際統一私法協會數位資產與私法原則之重要面向》（Key Aspects of UNIDROIT Principles on Digital Assets and Private Law）¹⁵³

此報告為亞洲開發銀行宣導強化東協加三（ASEAN+3）司法管轄區金融市場基礎建設之努力之一，旨在增進相關各方對數位資產的理解，並提升國際法律適用於跨境交易之確定性。此報告以國際統一私法協會

¹⁵² 專家委員會防制洗錢措施之評估 - 《虛擬資產世界之洗錢及資恐風險》態樣報告：<https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4>

¹⁵³ 亞洲開發銀行 - 《國際統一私法協會數位資產與私法原則之重要面向》：<https://www.adb.org/publications/unidroit-principles-digital-assets>

(UNIDROIT) 發布之《數位資產與私法原則》為核心，介紹該原則所涵蓋的 19 項涉及數位資產相關私法議題之原則，並說明此等原則不受司法管轄區及機構組織之限制，並探討各國應如何調整其國內法律以適應數位資產之交易需求。

《數位資產導論》¹⁵⁴

鑑於目前尚無全球統一之數位資產定義，此報告介紹各司法管轄區及國家標準之制定機構，並說明如何制定自身規範以界定並監理數位與加密資產此報告亦詳述國際統一私法協會（UNIDROIT）所制定的全面性且技術中立之原則，並說明此原則如何適用於現有及新興之數位資產，以及如何協助提高相關交易之安全性與效率。

《打造包容性經濟體：中小企業與數位支付在提升經濟平等中的角色》¹⁵⁵

此研究聚焦於中小企業（SMEs）與數位化金融工具如何改善取得融資的機會，藉此打造更具包容性的經濟體。報告強調科技發展，特別是數位支付系統，有助於持續促進普惠金融（financial inclusion）的實踐。然而，在實務執行層面上仍存在長期挑戰，尤其在開發中國家更為明顯。此研究探討中小企業對國內生產毛額（GDP）的貢獻、數位支付之運用，與吉尼係數（Gini coefficient）顯現的現存經濟不平等現象之間的關聯性。研究歸納兩項核心發現：

- 中小企業對降低經濟體內的不平等有顯著助益。
- 數位支付作為數位轉型的一環，能縮減東南亞地區經濟體內不平等差距。

報告最後提出結論性觀察、政策建議及未來研究方向之建議。

《以法治途徑打造更具韌性的制度：司法獨立、司法問責與全球經濟活動》¹⁵⁶

此報告強調司法機關公正性的重要，尤其是司法獨立與問責機制，其等對穩定全球供應鏈與金融體系更是不可或缺。報告第一部分從兩篇研究論文歸納出三項核心政策意涵：第一，強調獨立任命法官對於提升決策品質與經濟誠信（economic integrity）的重要性。依據專業能力（merit-based）而非政治偏好進行法官任命，有助於增強公眾信任並防範司法受政治干預。第二，提倡理解文化規範與政治制度之間的互動關係，此論文提出若干措施，以有效區隔宗教與政治權力，包括在宗教教育地區宣導積極性的平權措施，以及促進官僚體系的世俗化改革。第三，呼籲建立司法遴選程序，以杜絕法官遴選受政治干預，確保司法體系之獨立性與問責性。

《以法治途徑建構更具韌性的全球供應鏈與金融架構》¹⁵⁷

此報告探討法治原則與規則導向方法（rule-based approach）之運用，以及如何有效強化全球供應鏈與金融架構之韌性。報告主要論點如下：

- 確保全球供應鏈與金融系統的穩定性，對各國經濟與社會至關重要。
- 「法治」（rule of law）與「規則導向方法」（rule-based approach）在概念上有區別。
- 法治是治理的基礎原則，能確保問責、公平與透明，亦延伸至國際貿易與全球金融活動中。
- 規則導向方法則強調可預測性、透明性、一致性與問責性，對建構韌性與促進經濟永續成長具有關鍵作用。
- 落實法治原則與規則導向方法，能有效提升全球供應鏈與金融架構的穩定性及韌性。

¹⁵⁴ 亞洲開發銀行 - 《數位資產導論》：<https://www.adb.org/publications/introduction-digital-assets>

¹⁵⁵ 亞洲開發銀行 - 《打造包容性經濟體：中小企業與數位支付在提升經濟平等中的角色》：<https://www.adb.org/publications/imagining-an-inclusive-economy-the-role-of-sm-es-and-digital-payment-in-elevating-economic-equality>

¹⁵⁶ 亞洲開發銀行 - 《以法治途徑打造更具韌性的制度：司法獨立、司法問責與全球經濟活動》：<https://www.adb.org/publications/the-rule-of-law-approach-for-more-resilient-institutions-judicial-accountability-and-independence-and-global-economic-activities>

¹⁵⁷ 亞洲開發銀行 - 《以法治途徑建構更具韌性的全球供應鏈與金融架構》：<https://www.adb.org/publications/rule-of-law-approach-for-more-resilient-global-supply-chains-and-financial-architecture>

《金融科技風險管理：政策與監管之涵義》¹⁵⁸

此論文舉例說明各經濟體如何因應金融科技（Fintech）蓬勃發展，闡述監管機關迫切需要採取靈活的政策，以有效監管新興金融產品及服務業者。報告勾勒金融科技整體發展情勢，並說明各經濟體如何在鼓勵創新的同時，加強國際合作，以盡可能隔絕新興科技帶來的金融、營運及網路安全等風險。

《亞洲地區中央銀行數位貨幣最新發展與影響》¹⁵⁹

此報告探討全球中央銀行數位貨幣（CBDC）的發展現況及新興趨勢，並指出健全的數位基礎設施、強有力的公私部門合作、及金融科技的普及教育，對於確保中央銀行數位貨幣（CBDC）有效宣導數位經濟轉型至關重要。

《中央銀行數位貨幣在普惠金融中的角色：2022 年亞太普惠金融論壇報告》¹⁶⁰

此報告探討中央銀行數位貨幣（CBDC）可以如何善用數位金融科技，對未享有金融服務（unbanked）之民眾提供正式金融產品及服務的覆蓋面與價值；並分析宣導此一目標所面臨之挑戰及其解決方式。報告針對政策制定者與監管機構提供若干建議，包括如何設計中央銀行數位貨幣（CBDCs）、建構推行 CBDCs 所需的前置條件、及有效管理相關風險。此外，報告也分享來自「亞太普惠金融論壇」（此為亞太經濟合作會議（APEC）財長會議政策倡議）的重要觀察與見解。

6.9 國際貨幣基金組織

國際貨幣基金組織（IMF）發表下列報告：

《中央銀行數位貨幣的資料使用與隱私保護》¹⁶¹

此報告提出一套框架，協助司法管轄區引導應對 CBDC 數據使用與隱私保護之間的權衡取捨，並提供相關管理工具。報告主要針對零售 CBDC，因為批發 CBDC 環境下的數據使用與隱私考量，與傳統即時總額結算系統（real time gross settlements）類似。報告強調制度安排、數據蒐集、存取及儲存政策、設計方案及科技解決方案之重要性。在一定的隱私保護偏好前提下，中央銀行可透過強化透明度與問責機制、健全政策，以及審慎採用「設計即隱私」（privacy-by-design）之方法，包括使用強化隱私的相關技術，促使 CBDC 數據得到更好的運用。

《2023年國際貨幣基金防制洗錢與打擊資恐策略檢視》（2023 Review of The Fund's Anti-Money Laundering and Combating The Financing of Terrorism Strategy）¹⁶²

此報告檢視國際貨幣基金組織（IMF）為維護金融誠信所採取的行動，並對未來防制洗錢與打擊資恐策略提出發展方向。國際貨幣基金組織逾二十年來持續強調，有效的防制洗錢與打擊資恐框架，及更廣義的金融誠信，對於維護金融體系的健全性與穩定性具有關鍵作用；並可避免金融犯罪對成員整體經濟造成負面的總體影響。因此，IMF 逐步將此項工作融入其所有核心職能及各項政策之中。此報告回顧國際貨幣基金組織自 2018 年以來執行防制洗錢與打擊資恐策略的成果，並建議未來應更深入整合金融誠信議題，並強化對洗錢與資恐相關議

¹⁵⁸ 亞洲開發銀行- 《金融科技風險管理：政策與監管之涵義》：<https://www.adb.org/publications/managing-fintech-risks-policy-regulatory-implications>

¹⁵⁹ 亞洲開發銀行 - 《亞洲地區中央銀行數位貨幣最新發展與影響》：<https://www.adb.org/publications/central-bank-digital-currency-developments-asia-implications>

¹⁶⁰ 亞洲開發銀行 - 《中央銀行數位貨幣在普惠金融中的角色: 2022 年亞太普惠金融論壇報告》：<https://www.adb.org/publications/asia-pacific-financial-inclusion-forum-2022>

¹⁶¹ 國際貨幣基金組織 - 《中央銀行數位貨幣的資料使用與隱私保護》：<https://www.imf.org/en/Publications/fintech-notes/Issues/2024/08/30/Central-Bank-Digital-Currency-Data-Use-and-Privacy-Protection-554103>

¹⁶² 國際貨幣基金組織 - 《2023年國際貨幣基金防制洗錢與打擊資恐策略檢視》：[https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Funds\(資金\)-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542015](https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Funds(資金)-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542015)

題的總體經濟影響之關注。

《2023 年國際貨幣基金防制洗錢與打擊資恐策略檢視 - 背景文件》¹⁶³

此背景文件旨在支持國際貨幣基金組織（IMF）2023 年對其防制洗錢與打擊資恐（AML/CFT）策略之回顧分析及未來策略方向建議。文件包含五篇背景分析，深入探討以下主要議題：

- 非法資金流動
- 洗錢對金融穩定性之影響
- 金融誠信（financial integrity）議題與 IMF 其他政策及工作的加乘效果
- IMF 與關鍵合作夥伴在全球防制洗錢與打擊資恐政策架構中之協作情形
- 利害關係人對 IMF 執行防制洗錢與打擊資恐成效的看法

《中央銀行數位貨幣—初步考量》¹⁶⁴

此報告向 IMF 執行董事會介紹中央銀行數位貨幣（CBDC）的初步考量事項，包括一套指引各司法管轄區探索 CBDC 的框架，以及 CBDC 對貨幣政策傳導、資本流動管理措施及普惠金融之潛在影響。

《國際貨幣基金組織之中央銀行數位貨幣能力建構方針》¹⁶⁵

全球央行目前正積極探索發展中央銀行數位貨幣（CBDC），此一趨勢可能對國內外經濟與金融穩定性帶來深遠影響。國際貨幣基金組織現階段針對 CBDC 的工作，主要著重於促進成員國之間的相互學習交流，並建立分析基礎，以協助 IMF 人員向成員國提供政策建議。此文件勾勒一套多年期策略，以回應各界對 CBDC 經常提出之問題，並概述 CBDC 指引手冊的制定流程，該手冊將記錄新獲得的經驗教訓、分析成果及政策觀點。

《加密資產有效政策之構成要素》（*Elements of Effective Policies for Crypto Assets*）¹⁶⁶

此報告說明各國應如何因應加密資產的興起及其衍生之風險。報告依據加密資產的基本特徵定義並分類，同時說明加密資產宣稱的效益與潛在風險。報告提出一套針對加密資產的政策框架，以達成總體經濟穩定性、金融穩定性、消費者保護及市場與金融誠信等主要政策目標，此框架概述實現這些目標所必須具備的關鍵要素。但上述框架無法修正加密資產本身設計之根本性缺陷。

《支付與合約平台之興起》（*The Rise of Payment and Contracting Platforms*）¹⁶⁷

此報告探討，為強化符合公共政策目標之跨境支付所設計的平台及其治理方式。儘管近年來的創新多數較侷限於改善終端用戶的使用障礙，此報告的願景則奠基於國際貨幣基金組織（IMF）的使命 – IMF 係由 190 個會員司法管轄區之中央銀行與財政部共同治理。跨境支付為全球金融體系之基礎，其運作由 IMF 監督。

《中央銀行數位貨幣於促進普惠金融之角色》¹⁶⁸

普惠金融（financial inclusion）為各國中央銀行（尤其是新興、與低所得司法管轄區）宣導零售型中央銀行數位貨幣（CBDC）之重要政策目標。若 CBDC 之設計能有效解決阻礙普惠金融推展的各項障礙，則有機會提高未享有金融服務族群對數位支付的接受度，使 CBDC 成為進入更廣泛正式金融體系的途徑。CBDC 具備若干有

¹⁶³ 國際貨幣基金組織 - 《2023年國際貨幣基金防制洗錢與打擊資恐策略檢視 - 背景文件》：<https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Fund-s-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542020>

¹⁶⁴ 國際貨幣基金組織 - 《中央銀行數位貨幣—初步考量》：<https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/11/14/Central-Bank-Digital-Currency-Initial-Considerations-541466>

¹⁶⁵ 國際貨幣基金組織 - 《國際貨幣基金組織之中央銀行數位貨幣能力建構方針》：<https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/04/12/IMF-Approach-to-Central-Bank-Digital-Currency-Capacity-Development-532177>

¹⁶⁶ 國際貨幣基金組織 - 《加密資產有效政策之構成要素》：<https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092>

¹⁶⁷ 國際貨幣基金組織 - 《支付與合約平台之興起》：<https://www.imf.org/en/Publications/fintech-notes/Issues/2023/06/16/The-Rise-of-Payment-and-Contracting-Platforms-534794>

¹⁶⁸ 國際貨幣基金組織 - 《中央銀行數位貨幣於促進普惠金融之角色》：[https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/22/Central-Bank-Digital-Currency\(貨幣\)s-Role-in-Promoting-Financial-Inclusion-538728](https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/22/Central-Bank-Digital-Currency(貨幣)s-Role-in-Promoting-Financial-Inclusion-538728)

利於宣導普惠金融的特性，包括作為無風險且廣受接受的數位貨幣形式、支援離線支付、可以降低使用成本、及提高使用便利性等。然而，CBDC 並非宣導普惠金融的萬靈丹，仍須累積更多實務經驗，方能充分瞭解其潛在影響。

《中央銀行應如何探索發展中央銀行數位貨幣？》¹⁶⁹

經濟數位化帶來挑戰與機遇，中央銀行必須確保其能於數位時代持續達成政策目標。在此背景下，中央銀行數位貨幣（CBDC）的評估變得至關重要。若設計得當，中央銀行數位貨幣（CBDC）將可協助中央銀行實現支付系統現代化，並確保中央銀行貨幣在數位化的速度與形式持續演進下，仍能適應未來需求。然而，是否宣導CBDC 的探索與發行，必須依據各司法管轄區的經濟數位化程度、法律與監管框架，以及中央銀行內部能力進行個別評估。此報告提出一套動態決策框架，協助中央銀行在不確定性下做出決策，透過階段式與循序漸進的方法，中央銀行可隨著國內外環境的變化，調整CBDC專案的速度、規模與範圍。

《外國加密資產對小型開發中經濟體之總體金融影響》¹⁷⁰

為探討數位貨幣的相關風險，此報告以小型開放經濟體模型模擬大規模採用加密資產之假設情境。模型指出，以外幣計價之穩定幣（Stablecoin）可能在面臨負面衝擊時，加劇貨幣替代及資本外流的情形。此外，此現象亦將削弱貨幣政策的傳導效力，迫使中央銀行必須在遭遇衝擊時更積極地調整利率。倘若資本流動管理措施（CFMs）未有效限制加密資產的流動，將進一步誘使家庭部門為規避限制而持有外國穩定幣，加劇加密資產採用對整體經濟之負面影響。此研究凸顯，廣泛採用加密資產可能會限縮各國政府應對外來經濟衝擊的政策空間，甚至導致經濟問題從一國蔓延到其他國家（cross-country spillovers）。

《數位時代的資本流動管理措施（二）：中央銀行數位貨幣之設計選擇》¹⁷¹

此金融科技報告探討如何透過中央銀行數位貨幣（CBDC）實施資本流動管理措施，並分析其中可能產生的效果、風險及複雜性。研究分析得出以下幾項要點：首先，CBDC 生態系統的設計應具備實施資本流動管理措施的功能；其次，得益於數位科技賦予支付基礎建設可程式化的特性，某些資本流動管理措施在 CBDC 系統內的實施效率及效果可能高於傳統系統；第三，資本流動管理措施之有效實施，仰賴各國中央銀行在實務操作與標準上共同合作；最後，透過 CBDC 實施的資本流動管理措施必須與傳統的資本流動管理措施並行，且互相配合。

6.10 聯合國毒品犯罪辦公室

聯合國毒品犯罪辦公室（UNODC）發表下列報告：

《法人之法律責任：聯合國反貪污公約之執行情形，聚焦馬來西亞之案例》¹⁷²

《聯合國反貪污公約》（UNCAC）於 2005 年生效，透過公共部門與私部門參與預防措施、執法及國際合作的整體性方法，致力於打擊貪污犯罪。

法人對貪污犯罪負有法律責任，已成為廣泛接受的國際標準。此代表法人（相對於自然人）須對其涉及的貪污行為承擔法律責任。之所以強調法人責任，是因為重大且手法複雜的犯罪經常透過公司、企業或慈善機構等法人進行。由於企業結構複雜、決策層級眾多，加上涉案自然人可能居住海外，法人內部個別涉案人士的行為往往難以追查。UNCAC 第 26 條要求締約國採取措施，規定法人須對依公約定罪之犯罪行為承擔法律責任。

¹⁶⁹ 國際貨幣基金組織 - 《中央銀行應如何探索發展中央銀行數位貨幣？》：<https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/08/How-Should-Central-Banks-Explore-Central-Bank-Digital-Currency-538504>

¹⁷⁰ 國際貨幣基金組織 - 《外國加密資產對小型開發中經濟體之總體金融影響》：<https://www.imf.org/en/Publications/fintech-notes/Issues/2023/12/05/Macro-Financial-Implications-of-Foreign-Crypto-Assets-for-Small-Developing-Economies-541440>

¹⁷¹ 國際貨幣基金組織 - 《數位時代的資本流動管理措施（二）：中央銀行數位貨幣之設計選擇》：<https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/15/Capital-Flow-Management-Measures-in-the-Digital-Age-2-Design-Choices-for-Central-Bank-538509>

¹⁷² 聯合國毒品與犯罪問題辦公室 - 《法人之法律責任：聯合國反貪污公約之執行情形，聚焦馬來西亞之案例》：https://www.unodc.org/roseap/uploads/documents/Publications/2024/Liability_of_Legal_Persons_-Implementation_under_UNCAC_with_a_focus_on_Malaysia_Sep_2024.pdf

《落實聯合國反貪污公約第三章：東協成員國與東帝汶之刑事定罪與執法》¹⁷³

此報告針對聯合國反貪污公約（UNCAC）第三章：「刑事定罪與執法」條款在東協（ASEAN）成員國及東帝汶的執行情況進行全面性分析；上述各國皆為 APG 會員。本報告亦概述落實 UNCAC 第三章條款的主要挑戰與良好操作實務。

挑戰

各國執行 UNCAC 第三章規定時，往往面臨立法與執行層面的挑戰。在立法方面，許多司法管轄區缺乏完整的法律框架，或相關法律過於分散，無法完全符合 UNCAC 規定。在某些情形下，國內法律設定之標準高於 UNCAC 要求，使得貪污行為之辨識、調查與起訴程序更加複雜。現行制裁措施通常不足或規定不完備、不一致，削弱執法成效。在執行方面，許多司法管轄區普遍缺乏資源，包括技術設備、人員訓練及相關能力，另缺乏區域性辦事處，也影響反貪污措施的有效性。此外，資源不足也造成跨部門協調，及貪污犯罪相關統計資料蒐集的困難。

最佳操作實務

儘管面臨上述挑戰，報告亦指出各國在落實第三章規定上所採取的若干良好操作實務。有些司法管轄區已成功制定完整且貼合 UNCAC 標準的立法，進而有效宣導貪污行為的辨識、調查與起訴程序。此外，報告亦提出具體建議，例如制定平衡的裁量權規定，並落實涉及貪污之公務人員的停職具體程序。有些司法管轄區已建立透明且有效的資產申報制度，以打擊不法所得，提升政府官員的問責性。此外，加強對遭凍結、扣押或沒入資產之管理措施，也被視為有效提升反貪污措施成效的良好實務之一。

技術援助需求

此報告指出多項重要技術援助需求，包括：

- 良好實務與經驗教訓之彙整：報告共提出超過 40 項需求，希望能彙整良好實務及相關經驗教訓，以提升各司法管轄區對反貪污措施的理解與執行成效。
- 示範法規：報告提出逾 20 項需求，請求提供示範法規以協助各國立法草擬工作，並使國內法規與聯合國反貪污公約（UNCAC）規定接軌。
- 法律諮詢與能力建構：報告提出約 20 項需求，希望取得法律諮詢及能力建構方面的協助，以提升各司法管轄區的反貪污專業知識與能力。
- 立法草擬協助：報告中提出 20 項涉及立法草擬的支援需求，凸顯司法管轄區在發展完整法律框架方面所需的技術協助。
- 資訊科技與數據系統：司法管轄區亦經常提出希望取得資訊科技與數據系統方面的技術協助，以改善貪污相關資料的管理與分析能力。

整體而言，此報告發現區域內司法管轄區在私部門貪污行為的刑事定罪規範方面仍存在落差，包括私人部門內的賄賂與財產侵佔罪。此外，法人責任規範在本區域內亦未統一落實，透過 UNCAC 執行審查機制，一些締約國特別指出此為優先處理的領域。

¹⁷³ 聯合國毒品與犯罪問題辦公室 - 《落實聯合國反貪污公約第三章：東協成員國與東帝汶之刑事定罪與執法》：

https://www.unodc.org/roseap/uploads/documents/Publications/2024/Implementation_of_UNCAC_Chapter_III_-_ASEAN_States_parties_and_Timor-Leste_March_2024.pdf

《東南亞UNCAC快速落實區域平台再振興之區域路徑圖（2024 年 -2027 年）》*Regional Roadmap to Reinvigorate the Regional Platform to Fast-Track the Implementation of UNCAC in Southeast Asia (2024-2027)*¹⁷⁴

聯合國毒品犯罪辦公室（UNODC）持續支持區域平台之設立，以加速落實 UNCAC。區域平台的方法具有催化作用，旨在找出既有反貪污努力中的缺口，並協調及整合各種技術援助資源，同時促進區域間的協調與合作。2024 年 2 月，汶萊、柬埔寨、印尼、寮國、馬來西亞、蒙古、菲律賓、泰國、東帝汶及越南等國代表於泰國曼谷召開「東南亞 UNCAC 快速執行區域平台再振興會議」。各司法管轄區在會議上評估其執行 UNCAC 的情形，檢視成功經驗與所面臨之挑戰，並分析宣導後續執行所需的改革方向。報告明確指出各國共同認定的重點主題領域，作為宣導區域反貪污行動的指引框架，包括發展與強化實質收益權透明化、及法人責任之法律框架等。

《落實聯合國反貪污公約第三章：東協成員國與東帝汶之刑事定罪與執法》¹⁷⁵

UNCAC 第 26 條規定，各締約國須依照其法律基本原則採取必要措施，使法人負起法律責任。此類法律責任可包括刑事、民事或行政責任。同時，第 26(4) 條要求各國制定之制裁措施必須有效、合乎比例且具嚇阻效果。此報告同時聚焦東協各國在 UNCAC 第 26 條之落實情形。

《東協成員國、蒙古與東帝汶之資訊取得權》¹⁷⁶

此報告就東協各成員國、蒙古及東帝汶，概述資訊取得權於國際法下之相關規範，並彙整各國宣導資訊取得權之法律架構與實務案例，包括優良實務經驗，並提出強化資訊取得權相關立法及機制之建議及未來發展方向。

**《東南亞跨國有組織犯罪與網路詐騙、地下匯兌及科技創新的交匯：威脅局勢的變遷》
(Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape)¹⁷⁷**

報告指出，東南亞跨國有組織犯罪之威脅局勢正以前所未有之速度急遽演變。此變化尤以合成毒品之生產與販運、網路詐騙之成長最為顯著，均係由高度專業化之犯罪集團與複雜之洗錢、人口販賣網路，以及不斷增加之其他服務業者與協助者所驅動。儘管執法力度持續加強，網路詐騙卻日益猖獗，2023 年針對東亞及東南亞受害者之詐騙案件所造成之財務損失，估計介於 180 億至 370 億美元之間。

6.11 世界銀行集團

世界銀行集團發表以下報告：

《實質受益權登錄：落實經驗洞見與新興前沿》*(Beneficial Ownership Registers:Implementation Insights and Emerging Frontiers)*¹⁷⁸

此報告彙整奈及利亞、北馬其頓、肯亞及英國宣導實質受益權登錄之關鍵落實啟示。上述法域之經驗，對於全球宣導提升實質受益權透明度之改革，提供寶貴借鏡。

¹⁷⁴ 聯合國毒品犯罪辦公室 - 《東南亞UNCAC快速落實區域平台再振興之區域路徑圖（2024 年 -2027 年）》：
https://www.unodc.org/roseap/uploads/documents/Publications/2024/2024-2027_UNCAC_Implementation_Roadmap_in_Southeast_Asia.pdf

¹⁷⁵ 聯合國毒品犯罪辦公室 - 《落實聯合國反貪污公約第三章：東協成員國與東帝汶之刑事定罪與執法》：
https://www.unodc.org/roseap/uploads/documents/Publications/2024/Implementation_ofUNCAC Chapter III - ASEAN States_parties_and_Timor-Leste_March_2024.pdf

¹⁷⁶ 聯合國毒品犯罪辦公室 - 《東協成員國、蒙古與東帝汶之資訊取得權》：
https://www.unodc.org/roseap/uploads/documents/Publications/2024/Right_to_Information_in ASEAN Member States Mongolia_and_Timor-Leste_Sep_2024.pdf

¹⁷⁷ 聯合國毒品犯罪辦公室 - 《東南亞跨國有組織犯罪與網路詐騙、地下匯兌及科技創新的交匯：威脅局勢的變遷》：
https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

¹⁷⁸ 世界銀行集團 - 《實質受益權登錄：落實經驗洞見與新興前沿》：<https://openknowledge.worldbank.org/entities/publication/43aa154d-eb9c-49ea-b952-6811755b94da>

《貪污對永續發展之影響》(The Impact of Corruption on Sustainable Development)¹⁷⁹

貪污助長惡性循環：氣候變遷引發糧食安全、人口及資源壓力，進而促使貪污加劇。G20 反貪污工作小組於本篇論述中，探討打破此循環之可行途徑。

6.12 世界海關組織

世界海關組織防制洗錢打擊資恐計畫

觸手專案 (Project TENACLE)

「觸手專案」自 2019 年啟動以來，已成為世界海關組織於防制洗錢及打擊資恐領域之重要礎石。該專案由世界海關組織主導，並與艾格蒙聯盟（Egmont Group）及國際刑警組織（INTERPOL）共同宣導，致力於打擊大量現金走私，以及寶石與貴金屬之非法貿易；貿易洗錢（TBML）亦為重點項目之一。該計畫透過全球性之作業及教育計畫，已有效擴展影響力至亞太、拉丁美洲、非洲、中東及東歐等區域。

能力建構始終為「觸手專案」之核心。於 2023 至 2024 年間，該專案已經由教育訓練，協助並提升 630 名前線執法人員、調查人員及分析師之專業能力。相關工作坊與實作訓練聚焦於可疑活動/交易通報、作業與策略分析、貿易洗錢調查、及資恐防制。此類訓練除提升參與者之實務技能，亦促進跨機關合作，並分享有組織犯罪集團最新之活動趨勢與犯罪手法。相關專案推展已遍及亞太、東歐、拉丁美洲及地中海等地區。

「觸手行動」（Operation TENACLE）亞太地區第二階段執行成果顯著，查獲及扣押價值逾 2,000 萬美元（以多種貨幣及貴金屬形式呈現），成效超越以往標準。專案行動揭露出一套極為複雜之犯罪網路，包括多個設於中東之哈瓦拉（hawala）系統，與緬甸甲基安非他命走私組織間之連結。上述發現突顯一項創新之交換模式，即以黃金直接交換非法藥物，有別於傳統區域內與毒品犯罪相關之金流方式。

2,000 萬美元（黃金與貨幣） 扣押「觸手行動」亞太地區

- ★ 116 次黃金扣押 – 266.3 公斤金條、153 顆金幣及 122 件珠寶
- ★ 153 次貨幣扣押 – 336 萬美元現鈔
- ★ 1 次野生動物扣押：69 隻巨嘴鳥與金剛鸚鵡
- ★ 1 個貿易洗錢案例與高關稅消費品與酒類有關
- ★ 29 只手錶 (4 只勞力士)

2023 至 2024 年期間之成果，無論於執法層面或情資層面，對全球打擊複雜洗錢機制均產生重大影響。

亞太地區女性攜帶者 (female couriers) 趨勢：本年度觀察發現，亞太地區女性作為黃金及現金攜帶者之比例上升。針對此特定族群遭徵用之情形，應強化重點查核及預防機制，以維護其合法權益並防止被犯罪集團不當利用。

寶石扣押：資料缺口與區域執法

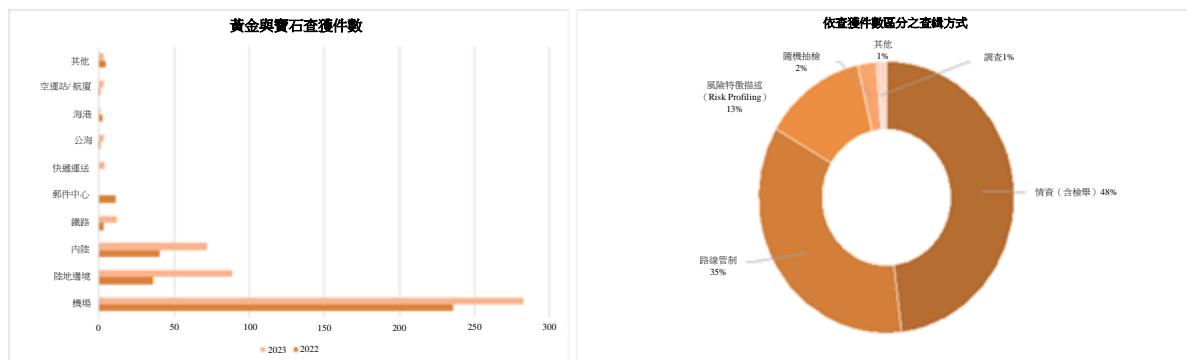
資料挑戰：報告指出，寶石查扣相關數據顯著不足，多數地區通報案件數量有限，難以支持全盤性分析。寶石本身具高度鑑別困難，進一步提升打擊走私執法之複雜度；資料缺口亦成為制定策略與宣導國際合作之重

¹⁷⁹ World Bank Group - *The Impact of Corruption on Sustainable Development*: https://www.unodc.org/corruption/uploads/documents/Corruption_sustainable_development_C.pdf

大阻礙。

資源與執法區域現有資料顯示，寶石查扣主要來自亞太地區、東歐及中歐之司法管轄區，東非及南非則為主要來源地。此情形顯示需針對特定區域路線制定精準執法策略。

戰術啟示：大多數黃金查扣案件發生於機場及陸路邊境，可見人員運輸為主要走私手法。此趨勢提醒相關單位，應於上述關鍵節點強化海關執法及科技偵查能量，以提升查緝成效。



扣押黃金：量化與區域觀察

數量顯著增加：與 2022 年相比，2023 年黃金查扣量出現顯著增長，查扣黃金重量年增率高達 623%，案件數亦增加 36.8%。此不僅反映走私活動日益猖獗，同時也顯示全球各地海關機關查緝能量及執法作為明顯提升。

區域熱點：亞太地區通報的查扣黃金重量占全球總量之 81%，顯示該地區為黃金走私活動的關鍵熱點。此類黃金的主要來源地為中東與北非地區，顯示不法集團慣用該區域作為走私通道，藉以滿足亞太市場對非法黃金的高度需求。

案例研究：世界海關組織防制洗錢與打擊資恐計畫

案例研究 # 135：印度稅收情報署

非法販運贓物及其他貨物

在「亞太區觸手行動第二階段」（Operation TENTACLE Asia/Pacific II），印度稅收情報署（Directorate of Revenue Intelligence, DRI）聯合印度海岸防衛隊（ICG）在坦米爾納德邦（Tamil Nadu）攔查兩艘漁船，並於兩起個案中查扣逾 32 公斤黃金。基於情資顯示，自斯里蘭卡經由拉姆納德韋德萊海岸（Vedhalai coast in Ramnad）走私外來黃金，稅收情報署及印度海岸防衛隊人員遂加強沿海巡查。

經識別可疑船隻並展開海上追緝後，稅收情報署及印度海岸防衛隊人員成功攔查其中一艘可疑漁船。雖然船上人員試圖棄置走私物品，印度海防隊潛水員仍於海床成功尋獲一包重達 11.6 公斤的外來黃金，稅收情報署及印度海岸防衛隊人員亦依法查扣該走私船隻。

稅收情報署人員搭乘印度海關巡邏艇靠近第二艘漁船，目擊有包裹轉交給岸上兩名男子。該二人察覺被監視後試圖攜帶非法黃金逃逸，最終遭稅收情報署海關人員當場查獲。



照片提供 - 印度稅收情報局：行動中查扣之金條



照片提供 - 印度稅收情報局：自斯里蘭卡走私至印度之漁船，現已遭查扣

案例研究 #136：摩洛哥海關

非法販運贓物及其他貨物

2023 年 10 月 15 日至 11 月 15 日，世界海關組織防制洗錢與打擊資恐計畫（AML-CTF Programme）實施「觸角行動地中海第三階段」（Operation TENTACLE Mediterranea III）。本次行動共查獲約 120 萬美元之走私現金及約 68.6 萬美元之走私黃金。

在本次行動期間，摩洛哥海關單位共查獲五起大額現金走私案件，總金額約為 269,467 美元；其中大部分為旅客將現金藏於隨身行李中所致。摩洛哥海關針對性查緝亦查扣八條總重 10.215 公斤、總值約 68.6 萬美元之金條。上述黃金條係於 Guerguarat 邊境檢查站自一輛小客車查獲，該批黃金條被藏匿於車輛行李廂與油箱之間。



照片提供 - 摩洛哥海關

案例研究 # 137：孟加拉海關

非法販運贓物及其他貨物

於「觸角行動亞太區第二階段」期間，孟加拉海關查扣超過 36 公斤金條。該批黃金條由 3 名孟加拉籍男性自中東地區走私入境，其等自阿拉伯聯合大公國杜拜搭機抵達 Hazrat Shahjalal 國際機場。後續偵訊結果顯示，案中涉及一個以中東為據點之哈瓦拉（hawala）網路，該網路與緬甸毒品（安非他命）走私集團具有關聯。進一步調查亦發現，此批走私黃金乃用於毒品交易支付，及結算非正式貿易款項。



照片提供 - 摩洛哥海關

於另一港口，孟加拉海關於行動期間查獲一個以中國為基地之貿易洗錢（TBML）犯罪網路。該集團以化學品貨櫃作掩護，夾藏高關稅消費品，包括 1,688,000 顆一次性電池及 16,824 公升酒精，藉由持續虛報品項之手法進行非法洗錢。此次查緝及後續調查，進一步查出 1 名哈瓦拉地下匯兌業者（hawaladar），及 1 名涉案貪瀆銀行人員，兩人均涉及資金結算、及非法洗錢活動。



照片提供 - 孟加拉海關（電池與酒類）

案例研究 # 138：日本海關

非法販運贓物及其他貨物

於「觸手行動亞太區第二階段」期間，日本海關於成田機場（Narita Airport）查獲一名女性旅客，其所穿鞋履中夾藏兩塊金條。查驗時，檢查人員注意到該鞋重量異常，經解構鞋底，發現有兩條用絕緣膠帶包裹、經塑形後貼合鞋內襯的黃金條。該隱匿手法突顯黃金易於重塑為日常物品，以規避邊境查緝機關查驗，亦反映黃金常被用作洗錢工具。



照片提供 - 日本海關

近期學術研究

世界海關組織（WCO）強調下列兩篇與防制洗錢相關之最新學術論文：

《影響洗錢手法之選擇因素：APPT 架構》（Factors Influencing the Choice of Technique to Launder Funds : The APPT Framework）¹⁸⁰

此研究探討犯罪集團選擇洗錢手法時所考量的因素，並提出一套名為 APPT 的新分析架構。APPT 架構分別代表影響洗錢手法選擇的四大要素：（A）行動者（actors）、（P）前置犯罪（predicate crime）、（P）洗錢目的（purpose of laundering）、（T）科技創新（technological innovations）。本研究旨在提升對洗錢行動者動機與手法選擇背後原因的認知，並提出有助於金融犯罪調查及防制洗錢之實務啟示主要發現。

主要發現

涉案之行動者：此架構強調犯罪與非犯罪行動者的角色，並指出其專業能力及所需洗錢手法之複雜程度，均會影響最終所選用的洗錢方式。

前置犯罪：前置犯罪的種類及嚴重性，會直接影響所選擇的洗錢手法，愈複雜的前置犯罪通常會採用更高階的洗錢方式。

洗錢目的：洗錢所得最終用途—納入合法經濟體系，或資助後續犯罪行為—會影響所選擇之洗錢模式。

科技創新：科技進步為洗錢活動帶來新契機，也驅使現行防制洗錢架構不斷推陳出新。

建議：此研究建議，防制洗錢工作應採取全面性、風險導向之作法，跳脫僅以法令遵循為基礎之傳統模式，轉向更富彈性、與更動態之架構，以因應金融犯罪不斷演變之特性。

《運用圖形資料庫平台強化防制洗錢：宣導大規模採用》（Using Graph Database Platforms to Fight Money Laundering: Advocating Large Scale Adoption）¹⁸¹

此研究主張，應大規模宣導圖形資料庫平台（graph database platforms）於洗錢活動偵查與查緝之應用，尤其針對涉及空殼公司等複雜案件。研究指出，圖形資料庫有助於揭露非法企業網路中的隱匿關聯，提升辨識、與防制洗錢行為之效率。此研究亦探討該項技術之理論基礎與實務應用，並視其為防制洗錢之有效解決方案。

主要發現與建議

強化偵測效能：導入圖形資料庫可顯著增進洗錢行為之偵測能力，協助辨識實體間之複雜網路及隱藏關聯。

大規模採納技術：此報告強調應於銀行、公司登記機關及查緝單位等防制洗錢相關部門全面推廣圖形資料庫技術之應用。

實務應用：圖形資料庫在實際案件（如巴拿馬文件 Panama Papers）已成功被運用，顯示其有望革新金融犯罪偵查模式。

未來研究：此研究建議持續深入探討圖形資料庫如何更廣泛地應用於防制洗錢策略，並鼓勵未來發展更精密之偵測模型。

¹⁸⁰ F 《影響洗錢手法之選擇因素：APPT 架構》經濟犯罪學期刊（Journal of Economic Criminology），1, 100006 -

<https://doi.org/10.1016/j.jeconc.2023.100006>

¹⁸¹ 《運用圖形資料庫平台強化防制洗錢：推動大規模採用》洗錢控制期刊（Journal of Money Laundering Control），26(3), 474-487.

<https://doi.org/10.1108/JMLC-03-2022-0047>

7 - 縮寫、首字母縮略詞、與貨幣匯率

| | |
|----------|--------------------|
| ABF | 澳洲邊境執法局 |
| AFP | 澳洲聯邦警察 |
| AML | 防制洗錢 |
| AMLC | 防制洗錢委員會 |
| 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 |
| 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（打擊資助恐怖主義） |
| CTR | 現金/貨幣交易報告 |
| 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 | 加強盡職調查 |
| 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 |
| FMU | （巴基斯坦）金融監控中心 |
| FSRB | FATF 區域性防制洗錢組織 |
| GIABA | 西非政府間防制洗錢組織 |
| GIF | （澳門）金融情報辦公室 |
| HKD | 港幣 |
| IDR | 印尼盾 |
| IIFTI | 國際資金移轉指示 |
| INTERPOL | 國際刑警組織 |
| JPY | 日圓 |
| KYC | 認識你的客戶 |
| LEA | 執法機關 |
| MENAFATF | 中東與北非防制洗錢金融行動工作組織 |
| MLA | 刑事司法互助 |
| ML | 洗錢 |
| MONEYVAL | 防制洗錢措施和資恐問題評估專家委員會 |
| MOP | 澳門幣 |
| MVTS | 金錢或價值移轉服務（MVTS） |
| MYR | 馬來西亞令吉（貨幣代號） |
| 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 | 資本擴 |
| PHP | 菲律賓比索 |
| PKR | 巴基斯坦盧比 |
| PPATK | （印尼）金融交易報告與分析中心 |
| PPP | 公私夥伴關係 |
| RMB | 中國人民幣 |
| RM | 馬來西亞令吉（貨幣符號） |
| SEC | （菲律賓）證券交易委員會 |
| SGD | 新加坡元 |
| 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（資助恐怖主義） |
| UNODC | 聯合國毒品犯罪辦公室 |
| USD | 美元 |
| VAT | 加值型營業稅 |
| 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網站所提供之資料，於 2024 年 7 月至 10 月不同時間點之匯率。本資料雖力求正確，惟僅為參考資料。

8 - 索引

索引詞彙後方之數字為本報告內之案例號碼。

犯罪型態：

有組織犯罪與敲詐勒索

13, 29, 48, 51, 70, 95, 114

恐怖主義，包括資恐

32, 37, 92, 93, 94

性剝削，包括兒童性剝削

19, 66

毒品相關犯罪

39, 47, 72, 73, 90, 91, 112, 113, 116, 117, 125

非法販運贓物及其他貨物

135, 136, 137, 138

搶劫，竊盜

109, 123

貪污與賄賂

16, 33, 34, 46, 52, 55, 81, 83, 87, 120, 124, 126, 131, 132, 133

詐欺包括，但不限於：

- 電話/簡訊/電子郵件詐欺/社群媒體
- 身分詐欺或愛情詐騙
- 偽造，以及
- 商業電子郵件詐騙

1, 4, 6, 7, 9, 10, 11, 12, 14, 15, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 31, 35, 38, 40, 41, 42, 43, 44, 48, 49, 50, 51, 52, 53, 54, 56, 57, 58, 62, 67, 68, 71, 74, 75, 76, 80, 82, 83, 89, 106, 107, 108, 109, 110, 121, 122, 128, 129, 130

非法賭博/博奕

2, 28, 48, 51

偽造（含貨幣偽造）及商品侵權（盜版）行為

40

走私（包括貨幣走私，以及涉及關稅及稅捐之相關走私行為）

63, 78, 118, 119

稅務犯罪（直接稅與間接稅）

117, 18, 45, 77

內線交易與市場操縱

14

境外前置犯罪

11, 15, 21, 22, 74, 79, 107, 124, 126

洗錢之種類：

自我洗錢

1, 2, 16, 31, 35, 40, 43, 47, 49, 50, 52, 70, 71, 88, 95, 113, 119, 131, 132, 133

獨立洗錢

13, 30, 130

第三方洗錢

11, 12, 13, 16, 22, 23, 24, 25, 26, 27, 28, 38, 41, 42, 46, 47, 48, 49, 71, 75, 76, 79, 81, 131, 133

以貿易為基礎之洗錢活動

3, 4, 5, 32, 45, 61, 63, 78

分散交易（Structuring）/化整為零（smurfing）/混合交易（mingling）

4, 29, 33, 34, 35, 48, 54, 55, 64

管道：

金融機構

9, 33, 34, 37, 38, 39, 40, 42, 43, 44, 49, 75, 92, 95, 107, 08, 109

賭場，賭廳

2, 28, 48, 50, 51, 68, 70, 114.

貴金屬與寶石交易商

3, 7, 8

地下匯兌（underground banking）／替代性匯兌服務／哈瓦拉（hawala）

1, 60, 61, 63

貨幣兌換/現金兌換

7, 13, 50, 118

金錢或價值移轉服務

使用資本市場

虛擬資產服務提供商

6, 7, 25, 28, 35, 41, 48, 50, 79, 84, 130

支付方式：

現金

65, 66, 70, 73, 80, 81, 82, 84, 85, 86, 87, 88, 113, 116, 117, 118, 119, 126

電匯

39, 45, 46, 47, 83, 87, 88, 89, 106

使用虛擬資產（加密貨幣或其他虛擬資產）

7, 22, 28, 35, 41, 48, 79, 84, 130

使用信用卡/金融卡，支票，本票（promissory notes）等

9, 21, 26, 45, 47, 49, 65, 66, 68, 82, 88

貴金屬與寶石交易

3, 29, 78

新型支付方式

31, 40, 42, 47

內容:

國際合作

3, 16, 17, 49, 50, 78, 105, 127, 131, 132, 133, 134

跨國組織犯罪集團

15, 21, 26

重要政治性職務人士

34, 46

使用網際網路（加密，存取ID，國際銀行等）

6, 18, 19, 27, 97

購置不動產

16, 35, 45, 46, 54, 62, 86, 105, 131, 133

濫用非營利組織

52, 55

新冠肺炎疫情（COVID-19）

9, 19

濫用法人與法律協議（包括國際商業公司，境外公司或信託，信託及公司服務業者等）

1, 2, 4, 6, 7, 8, 9, 10, 11, 12, 17, 31, 32, 54, 58, 69, 74, 74,
76, 80, 82, 83, 101, 102, 103, 109

可疑交易通報

9, 11, 30, 38, 39, 40, 41, 74, 75, 132

購置高價或具文化價值資產（藝術品，古物，賽馬，車輛等）

49