

APG年度態樣報告



亞太防制洗錢組織

2018

洗錢和資恐的方法和趨勢

亞太防制洗錢組織
2018年7月

目錄

內容.....	1
簡介.....	4
1. APG 在 2017 年至 2018 年進行的研討會和專案.....	6
1.1 APG 目前和將來可能的態樣專案.....	6
1.2 2017APG/FATF TREIN 聯合態樣與能力建構工作坊.....	8
2. FATF 和區域性防制洗錢組織態樣專案.....	10
2.1 FATF 態樣專案	10
2.2 EAG– 打擊洗錢和資恐歐亞小組	12
3. 洗錢和資恐的趨勢.....	15
3.1 APG 成員和觀察員對洗錢 / 資恐方法和趨勢進行的研究	15
3.2 洗錢或資恐類型與前置活動的關聯.....	21
3.3 新興的持續趨勢.....	29
4. 聚焦於透過網路助長的洗錢和資恐：網路洗錢.....	34
4.1 亞太地區網路犯罪的範圍.....	34
4.2 FATF 打擊洗錢、資恐、資助武器擴散和網路犯罪的 措施.....	35
4.3 打擊網路犯罪的現有努力和挑戰.....	40
4.4 透過網路漂白進行洗錢（網路助長的 ML/TF）	43
5. 洗錢和資恐的案例研究.....	55
5.01 資助恐怖主義.....	55
5.02 使用境外銀行、國際商業公司和境外信託.....	55

5.03	使用虛擬貨幣.....	57
5.04	貿易洗錢和移轉訂價.....	61
5.05	地下匯兌 / 替代匯款服務 /Hawala.....	68
5.06	使用網路（加密、存取 ID、國際銀行等）.....	75
5.07	使用新付款方式 / 系統.....	79
5.08	漂白稅收犯罪的收益.....	81
5.09	不動產（包括不動產仲介的角色）.....	85
5.10	人口販運和人員偷渡關聯.....	89
5.11	使用代名人、信託、家庭成員或第三方.....	93
5.12	賭博活動（賭場、賽馬、網路賭博等）.....	95
5.13	混合（商業投資）和投資詐欺.....	96
5.14	使用空殼公司 / 企業.....	101
5.15	與非法伐木有關.....	105
5.16	貨幣兌換 / 現金轉換.....	105
5.17	貨幣走私.....	108
5.18	使用信用卡、支票、本票等.....	110
5.19	分散交易（洗錢）.....	111
5.20	電匯 / 使用外國銀行帳戶.....	113
5.21	大宗商品交易（易貨交易，例如對非法毒品的再 投資）.....	118
5.23	使用假造的身分證件.....	119
5.22	寶石和貴金屬.....	122
5.23	購買貴重資產（藝術品、古董、賽馬等）.....	122

5.24	資本市場投資，使用經紀人.....	124
5.25	環境犯罪.....	125
5.26	毒品相關.....	126
5.27	直接根據可疑報告或門檻交易報告發展出的案例.....	127
6.	公私部門合作計畫.....	139
7.	縮寫對照表.....	142

簡介

背景

- 1 亞太防制洗錢組織（APG）是亞太地區的防制洗錢 / 打擊資恐（AML/CFT）區域機構。APG 編製有關洗錢（ML）和資恐（TF）技術和趨勢的區域態樣報告，協助政府和其他 AML/CFT 利害關係方進一步瞭解現有和新興洗錢和資恐威脅的性質，並致力尋求有效的策略因應威脅。態樣研究可協助 APG 成員實施有效策略，藉此調查和起訴洗錢和資恐，並設計和實施有效的預防措施。如果一系列洗錢或資恐以相似或相同方法進行，通常就會歸類為一種態樣。
- 2 APG 協同 FATF 和全球 AML/CFT 網絡的其他合作夥伴，共同進行態樣工作，包括執行聯合專案以及協調區域和全球優先領域的專案順序。
- 3 APG 年度態樣報告根據 APG 的策略性計畫，由 APG 營運委員會發佈，報告中包括對洗錢和資恐技術和方法的意見。APG 態樣報告旨在協助 APG 成員識別可疑的金融活動。本報告中的案例研究和指標將協助金融機構和非金融事業和專業（賭場、會計師、律師、信託及公司服務業者、不動產仲介等）發現並打擊洗錢和資恐。

4. APG 成員和觀察員每年都會提供有關洗錢和資恐案件、趨勢、研究、監管行動和國際合作的資訊。收集到的資訊不僅奠定了案例研究的基礎，還為選擇和設計深入研究特定態樣主題提供了依據，這類資訊亦為參與 APG 態樣工作的態樣專家網絡提供工作支援。
- 5 本報告中介紹的案例研究只是亞太地區和其他地區發現和打擊洗錢和資恐的一小部分成果，由於案件的敏感性或調查 / 司法程序仍在進行中，因此許多案件無法公開分享。本報告包含來自 APG 成員的報告以及開放來源中所收集而來的各種態樣範例個案。本報告中的部分案例發生在前幾年，但摘要資訊直到今年才發佈。

2017-2018 年的態樣

- 6 APG 委由 APG 營運委員會（前稱為「態樣工作小組」）進行態樣工作，該委員會目前由印度和紐西蘭擔任聯合主席。

1. APG 在 2017 年至 2018 年進行的研討會和專案

1 報告的本節簡述了 APG 在 2017 年 7 月至 2018 年 6 月之間進行的態樣相關工作。

1.1 APG 目前和將來可能的態樣專案

APG/MENAFATF 資恐和社群媒體聯合專案

2 APG/ 中東暨北非防制洗錢金融行動工作組織 (MENAFATF) 關於資恐和社群媒體的聯合專案，由馬來西亞和埃及共同主導。之所以發起此專案，是因為最近發現社群媒體成為資恐弱點，包括為恐怖組織和個別人士提倡宗旨、招募追隨者並為其活動籌集資金。為進一步理解此現象，2017 年 4 月向 APG 和 MENAFATF 成員和觀察員發放了一份問卷，旨在徵求濫用社群媒體進行資恐的案例研究及其因應措施。目前已據此撰寫一份報告，專案計畫預計於 2018 年 7 月結束。

人口販運和走私活動帶來的洗錢和資恐風險

3 據估計，人口販運可為犯罪集團帶來約 1,500 億美元的收益，走私人口也能夠帶來很可觀的犯罪所得，且持續為全球和各區域面臨的挑戰。APG 專案分為兩個階段，如下所示：

- a) 第 1 階段 – 打擊人口販運之 FATF/APG 聯合專案，於 2018 年 6 月結束；以及
- b) 第二階段 – APG 區域專案，以 FATF/APG 人口販運專案為基礎，考慮針對人口販運和人口走私的管理措施提供實施支援。

跨太平洋毒品路徑的風險和弱點

4 這件正在進行的專案由東加和萬那杜共同領導，預計於 2018 年 12 月完成。

APG/EAG 恐怖主義融資和犯罪所得（包括組織犯罪）

- 5 歐亞打擊洗錢和資助恐怖主義行為小組（EAG）將協同 APG 針對恐怖主義融資和犯罪所得（包括組織犯罪）展開一項聯合專案，聚焦於資恐使用犯罪所得的相關技術和趨勢（包括來自組織犯罪的收益）。
- 6 此專案網羅 EAG 和 APG 成員以及感興趣的觀察員提出貢獻和評論，各區域小組的轄區共同領導此專案。俄羅斯將領導 EAG 的專案，APG 的共同領導者則尚未確定，EAG 和 APG 秘書處將協調此專案。
- 7 此專案將包括：
 - a) 資訊收集階段，會採用問卷的方式獲取案例研究、態樣和最佳實務；在 EAG/APG 聯合態樣研討會（2018 年 12 月）上舉辦的會議中分享案例研究；
 - b) 待編寫的報告，其中包括專案的案例研究、態樣、

準則和建議，以供進一步考慮。

1.2 2017APG/FATF TREIN 聯合態樣與能力建構工作坊

8 每年，APG 態樣工作坊都會召集來自調查和起訴機構、金融情報中心（FIU）、主管機關、海關主管機關和其他機構的 AML/CFT 從業人員，目的是考慮洗錢和資恐風險和弱點的優先順序。近年來，APG 藉此機會結合態樣工作坊與能力建構 / 技術工作坊，分享從業人員在與洗錢和資恐相關優先主題上的經驗。這些活動旨在：

- 匯集 APG 從業者社群，互相分享經驗並建立合作網絡；
- 支援 APG 營運委員會正在進行的研究；
- 促進 APG 成員為由 FATF 和 FSRBs 領導的態樣專案做出貢獻；
- 分享實際應用 AML/CFT 措施的最佳實務和策略；
- 擴大公私部門與學術研究部門之間，在 AML/CFT 問題上的夥伴關係；以及
- 加強 AML/CFT 問題上的產業合作，並在選擇和進行洗錢和資恐態樣研究中借鑑產業經驗。

9 2017 年 APG/FATF TREIN 聯合態樣和能力建構工作坊於 2017 年 11 月 13 日至 16 日在大韓民國釜山舉辦，主辦單位為 FATF 培訓和研究所（FATF TREIN）。工作坊有 200 多名代表參加，其中包括私部門、非政府組織和民間社會的成員，該工作坊由印度和 FATF TREIN 共同主持。

- 10 工作坊包括全體會議和三場為期兩天的會議：（i）與人口販運和人口走私相關的洗錢；（ii）武器擴散融資；（iii）調查和起訴網路助長的洗錢和資恐。
- 11 態樣工作坊包括關於社群媒體和資恐的演講，以及最近發佈的 APG/UNODC 報告：「*繼續加強對 APG 地區野生動植物犯罪的非法資金流動的發現、調查和破壞*」。
- 12 透過工作坊識別以下共同主題、需求和建議：
 - 人口販運帶來了巨額犯罪所得，但相較於可能產生相當犯罪所得的許多其他罪行，洗錢防制相關的執法回應卻少之又少；
 - 制定有效和實用的紅旗警訊指標能夠有效輔助政府和私部門；
 - 政府、私部門和民間社會、研究機構和非政府組織之間的夥伴關係，對於進一步鎖定人口販運財務方面執法，可說是至關重要；
 - 許多司法管轄區對於識別和評估自身轄區內人口販運和相關洗錢風險，面臨挑戰；
 - 抵減洗錢風險需要進一步反映和回應已識別的人口販運和洗錢背景。

2. FATF 和區域性防制洗錢組織態樣專案

- 13 報告的本節簡述了 FATF 和其他 FSRBs 在 2017 年 7 月至 2018 年 6 月之間發布的態樣報告。

2.1 FATF 態樣專案

機構間 CT/CFT 資訊共享：優良實務和實用工具（非公開）

- 14 在國內各級機構之間有效地共享資訊和情報，對於打擊恐怖主義和資恐至關重要。提升適當機構間共享反恐（CT）和 CFT 資訊及相關情報產品，是 FATF 和 FSRB（包括 APG）成員的優先要務。
- 15 本報告旨在：
- 向決策者和營運專家告知國內 CT/CFT 架構所涉及的主要營運機構，以及這些機構收集的相關資訊；
 - 闡明這些主管機關在共享資訊時經常面臨的挑戰；以及
 - 重點介紹在國內實施的實用工具和優良實務實例，這些實例成功克服為打擊恐怖主義和資恐而發現的挑戰。
- 16 本報告著重於有效且及時的機構間資訊共享，認為這對於減少恐怖分子、恐怖組織、恐怖主義融資者、同情者和助長網絡之間的資金往來可說是至關重要。此外，本文還指出，鑑於國際層面的資訊共享是基於相

關資訊在國內層級的可用性和可及性，因此 CT/CFT 資訊的有效機構間資訊共享，對有效的國際資訊共享具有積極效應。

17 雖然國內資訊共享架構可能因司法管轄區而異，但識別挑戰、實用工具和優良實務具有附加價值，能有助於識別各機構如何有效地調整其國內法律和行政架構，進而促進機構間為 CT/CFT 目而共享資訊。

18 有興趣獲得此報告的 APG 成員請洽詢 APG 秘書處。

伊斯蘭國和蓋達組織及其附屬組織的財務更新（2017 年 10 月）– 非公開

19 2015 年 2 月，FATF 發表資助伊拉克和黎凡特伊斯蘭國綜合報告，自那時以來，FATF 每年根據自願貢獻進行三次非公開的定期更新，這些更新還涵蓋蓋達組織、伊斯蘭國和蓋達組織的附屬組織。有興趣獲得相關更新的 APG 成員請洽詢 APG 秘書處。

恐怖組織招募人員籌資

20 招募成員和支援者對於恐怖組織的存續至關重要，各恐怖組織都有不同的招募技術，具體取決於組織的規模，或是否為分散的個人網絡。

21 本報告利用從 FATF 全球網絡內各機構收集到的資訊，從而深入瞭解恐怖組織招募成員和支援者的資金需求。部分情況下，這些資金需求很少，但其他情況下，如果招募網絡與助長網絡互有連結，則財務情報和調查

的價值可能相當巨大。

22 本報告識別恐怖組織和恐怖組織使用的最普遍招募方法，以及與這些恐怖組織招募人員方法和技術相關的費用：

- 招募者以及維護招募 / 助長網絡基本基礎設施的個人需求
- 編製和分發招募資料
- 為促進新招募人員早日投入恐怖組織而支付的商品和服務，以及
- 直接向新招募人員或僱用傭兵或民事專家提供財務獎勵。

23 本報告闡明恐怖組織如何資助新成員和支援者的招募行為，本報告亦協助執法機關、金融情報中心和其他營運和安全機構，供其從一開始就擾亂恐怖分子的招募活動，防範更多個別人士投入恐怖組織。

2.2 EAG– 打擊洗錢和資恐歐亞小組

EAG 地區 FTF 的統一財務狀況

24 該專案的目的是總結 EAG 成員在識別資助外國恐怖主義戰士（FTF）態樣方面的經驗，以強調投入國際恐怖主義組織（包括伊斯蘭國）的個別人士及其作為支援者或本身為 FTF 之同夥的具體特徵。該研究著眼於潛在 FTF 的財務行為，旨在協助申報實體識別此類行為，

並盡可能減少 EAG 成員國面臨的威脅。

- 25 該報告旨在與私部門共同支援 EAG 成員國的金融情報中心，納入特殊指標，俾使信貸機構和其他國家的 AML/CFT 利害關係方，得以發現與恐怖主義相關的疑似洗錢或資恐交易。

透過保險公司洗錢

- 26 此專案由中國和俄羅斯共同主導，研究保險業中打擊洗錢的各種措施，包括疑似洗錢或資恐交易的風險特性和「紅旗警訊」（red flag）指標、共同挑戰和阻礙，以及典型的案例研究。該報告網羅來自許多公部門和私部門機構的資訊，包括監理機關、金融情報中心、執法機關等，該報告將於 2018 年 11 月發布。

識別協助恐怖主義組織的個別人士

- 27 金融情報中心的實務顯示，向恐怖分子提供援助的其中一種態樣，是為第三方的利益而購買機票。
- 28 有關購票事實的資訊可取自信用卡機構，有關旅客的資訊則在政府機關的資料庫中，但這些登記紀錄均沒有同步。
- 29 該研究的目的是為了瞭解各國如何針對基於第三方利益購買機票建立控管制度，該研究亦致力判定對於掌握購票者、用票旅客等資訊，何謂最有效的機制，並比較這些登錄的資訊。

跨境販毒和毒品收益合法化 - 電子支付工具和加密貨幣

- 30 根據毒品執法機構的經驗，販毒者密切監控並利用各種不斷升級的電子金融服務。犯罪者利用現代線上資產管理技術掩飾其非法活動，撇清犯罪所得與犯罪來源的關係，使其得以轉換和保留犯罪所得，最終規避起訴和罰則。
- 31 實務顯示，電子支付方式的廣泛可用性和可及性，加上識別國際電子支付系統客戶的相關法規不甚完善，阻礙了偵查毒品相關的犯罪行為以及犯罪者的身分，進而阻礙司法執行，允許組織販毒集團構建自身的「犯罪」能力。
- 32 研究團隊針對所採用的犯罪方法以及用於監管電子支付產業和加密貨幣的國家模型，彙整和分析 LEA 和金融情報中心可獲得的所有資訊。
- 33 擬議研究專案的結果可能成為制定舉措的資訊平台，這些舉措旨在協調 EAG 成員轄區的相關立法，以改善非法金融交易的遏制機制以及潛在制定 LEA 和金融情報中心的行動計畫。

3. 洗錢和資恐的趨勢

34 報告的本節簡述了洗錢和資恐的趨勢，包括有關 APG 成員和觀察員之研究的開放來源資訊。

3.1 APG 成員和觀察員對洗錢 / 資恐方法和趨勢進行的研究

汶萊和平之國（以下簡稱汶萊）

35 汶萊最近對 ML/TF 方法和趨勢的研究中，發現了 2017 年 STR 的趨勢，金融情報中心指出以下懷疑依據：

- 涉及個人或聯名帳戶（個人，而非公司）。
- 帳戶營業額（借 / 貸）超過個人的預期收入。
- 無明確目的但多次進 / 出資金移轉。
- 相似金額或相似金額範圍的交易。
- 涉及線上購買或電匯。

日本

36 JAFIC 發布一項風險評估，指出在日本金融情報中心（JAFIC）網站（日本 FIU）上發布了由企業經營者進行的每類交易的風險程度。JAFIC 年度報告包括 AML/CFT 統計資料、案例研究和趨勢，報告中反映的趨勢包括：

- 未註冊的放款業務和高利貸。
- 隱匿和接收透過詐欺罪獲得的犯罪所得。

- 透過網路提供的交貨服務擁有、轉讓非法藥品。
- 存摺走私、詐領福利和其他利益，以及與演唱會門票和手機電信合約銷售相關的詐欺。
- 使用他人非法獲得的現金卡，從 ATM 詐領現金以及從貨幣貸款進行勒索。
- 買賣股票的行為違反法律架構，進而改變了市場價格。

中國澳門

37 中國澳門的金融情報辦公室（GIF）在 2017 年 1 月至 6 月共收到 1,527 起 STR，其中博彩業共計 1,074 起 STR，金融業（包括銀行、保險和金融仲介）共計 414 起，其他產業共計 39 起。

38 從收到的 STR 中發現到常見的洗錢方法如下：

- 賭場籌碼轉換完全沒有 / 或僅有最少賭博活動；
- 代表第三方進行賭場籌碼轉換 / 籌碼贖回；
- 不定期領取大量現金；
- 嘗試交易但未成功；
- 使用 ATM、電話銀行業務、現金存款機；
- 可疑的地下銀行 / 替代匯款服務；
- 可疑電匯；
- 大量現金存款，但資金來源無法核實；
- 換匯 / 現金轉換；
- 無法提供身分證明 / 重要的個人資訊。

馬來西亞

39 馬來西亞已準備第三次國家風險評估（NRA2017），該評估將由國家協調委員會（NCC）在 2018 年中對防制洗錢發布。第三次 NRA 重點關注威脅和產業風險評估，其依據為增強和修訂的資料點，即（a）案例研究分析、（b）國內外製作的獨立報告、（c）統計資料和報告、（d）認知調查、（e）專家的觀點、（f）緩解過程。NRA2017 流程還考慮了最重要的宏觀因素（例如經濟、金融、政治和社會文化體系、治理層級和非正規經濟）以及犯罪和產業間的相互聯繫。除威脅和產業風險評估外，修訂後的國家風險評估還將納入其他獨立進行的風險評估作業，即非營利組織產業的國內評估和國家風險評估（DRRA）和納閩（Labuan）境外風險評估（LRA）。NRA2017 由 NCC 總結，預計將在 2018 年第二季度由高階 NCC 進行審議和認可。高階 NCC 簽核後，將與利害關係方（包括公眾）進行交流。

紐西蘭

40 紐西蘭於 2018 年 3 月發布了最新的國家風險評估（NRA），相關資料請見紐西蘭警察網站。NRA 審查國內外的主要洗錢威脅，以及其對紐西蘭金融、法律、不動產和零售產業構成的風險：

- 國內洗錢威脅：已知在國內產生洗錢的主要犯罪類

別是毒品犯罪、詐欺犯罪和稅收犯罪。

- 境外洗錢威脅：從境外到紐西蘭已知的三個關鍵威脅領域是：（1）與紐西蘭有聯繫的跨國組織犯罪集團，例如跨國毒品分銷網絡；（2）一般與紐西蘭無關的海外犯罪組織，但可能會透過紐西蘭及 / 或紐西蘭法律機構移轉資金；（3）專門的洗錢網絡，可能透過紐西蘭的金融體系或紐西蘭的法律結構來移轉資金。

41 NRA2018 評估了紐西蘭洗錢的主要弱點，在紐西蘭，提供洗錢機會的管道包括具有以下條件的金融、法律、會計、不動產和高價值大宗商品交易商：

- 為犯罪者提供匿名性；
- 可用於移轉大量且合法的資金，並為非法交易提供屏蔽；
- 國際上廣泛可用，且國際上對 AML/CFT 的控管不夠有力；以及
- 為現金密集型企業，特別用於掩飾毒品收益。

42 NRA2018 著重指出紐西蘭最應優先考慮的弱點：

- 國際電匯，此為與其他司法管轄區之間的電子交易。
- 替代付款方式：移轉價值和資金的替代支付方法非常容易使非法活動轉移到受管制產業以外之處。替代性匯款、國際交易轉帳和替代性銀行平台都已經成為弱點，這些移轉價值方法非常容易使非法活動轉移到受 AML/CFT 監督產業以外之處。

- 新技術：透過新技術進行濫用，與移轉價值和資金的替代方法弱點密切相關。紐西蘭對新式支付技術（包括數位貨幣）的瞭解程度，可能不及其他司法管轄區那麼高，儘管如此，支付技術的快速發展，創造了高度動態的環境，會讓弱點可能迅速顯現。
- 把關者專業服務：目前，紐西蘭專業服務供應商（律師、會計師、不動產仲介）對 AML/CFT 的控制層級很低，無法提供報告。由於識別紐西蘭公司、慈善機構和信託實質受益人方面面臨困難，使得這些弱點變得更加複雜。此弱點跟開啟了洗錢通道，專業人士可藉此促進犯罪交易，例如透過不動產領域。
- 現金收益：仍是國內毒品犯罪交易的主要手段，高價值大宗商品的交易商和賭場博弈仍然容易受到非法現金所得的影響。
- 商業產業：許多商業產業很容易作為洗錢的幌子，其中，現金密集型業務是建立現金收益表面化來源的常用方法。這類洗錢行為可能會產生反競爭效應，對合法競爭對手造成負面影響。
- 高價值商品：非金融資產會在洗錢的所有階段遭到濫用，其中，高價值的可運輸商品可用於儲存財富，或在犯罪者之間移轉價值。同樣地，不動產資產也容易遭受大型洗錢交易的濫用。

43 除了洗錢風險外，NRA2018 還評估恐怖主義風險，紐

西蘭的恐怖主義威脅比許多其他夥伴要來得低，因此，紐西蘭沒有針對資恐的起訴或定罪機制，而海外資恐者可能會因此濫用紐西蘭貪污程度低以及高度誠信的聲譽。此外，如果海外恐怖組織有以下作為，將可能對紐西蘭的聲譽造成重大影響：

- 利益紐西蘭的企業、公司、支付平台和慈善機構支援資恐，或
- 尋找當地的支援者協助資恐。

44 紐西蘭金融情報中心還完成以下其他策略性研究產品：

- 關於人口販運和人口走私的態樣研究報告。
- 虛擬貨幣態樣研究報告，審視虛擬貨幣兌換如何促進犯罪，與虛擬貨幣相關的新興風險，因應這些風險帶來的挑戰，以及對紐西蘭警察和申報實體的影響。該報告旨在協助開發和改良偵查、預防和破壞金融犯罪的策略。
- 幫派成員前往秘密轄區的風險態樣研究報告：這項風險評估從洗錢角度出發，評估幫派成員前往太平洋秘密轄區的風險以及對紐西蘭的影響。
- 儲值卡濫用態樣研究報告：該報告彙整 2016 年 1 月至 2017 年 1 月之間收到的儲值卡相關 STR 資訊。該報告描述紐西蘭犯罪實體濫用儲值卡的各種方式，識別儲值卡的主要弱點以及讓其得以繼續活動的風險。

- 關於另類匯款的態樣報告：此策略性報告聚焦於複雜的洗錢態樣，得以使組織犯罪集團用來移轉價值。該報告指出 AMLCFT 法規的漏洞，使其容易受到犯罪濫用，並識別讓該活動得以繼續進行的風險。
- 線上博彩態樣研究報告：此策略性報告聚焦於被本地毒品供應商 / 經銷商用於洗錢的境外線上博彩網站，該報告識別透過的洗錢指標，評估是否有助益防範透過線上博彩網站進行洗錢的法規。
- 關於在紐西蘭預防組織犯罪的文件：該文件聚焦於在策略層面上預防組織犯罪，重點是主動解決新興組織犯罪問題和足以助長組織犯罪活動的條件，而非關注活動本身。

3.2 洗錢或資恐類型與前置活動的關聯

阿富汗

45 阿富汗著重指出洗錢或資恐類型與恐怖組織和毒品走私相關的特定前置活動之間的聯繫。反映此關聯的案例如下：

支援恐怖主義組織

46 當事人 A 是 Konar 省的居民，遭控是塔利班（UNSCR1267/1998）和資恐的成員，於 2016 年 5 月在阿富汗 Nangarhar 省 Pacheer Agaam 區遭到逮捕。調

查過程中，發現嫌犯攜帶塔利班戰士的薪資表和分配表，還攜帶兩張價值 1,030 萬巴基斯坦幣（88,000 美元）的銀行支票，完成起訴後，案件移交初級法院，嫌犯遭定罪並判以下刑責：

- 根據打擊資恐法規，進行資恐應被判處五年半徒刑和罰款 AFN400,000（5,600 美元）；
- 根據《反恐怖主義犯罪法》加入塔利班成員應判 18 個月徒刑；以及
- 沒收資產和工具。

毒品走私

47 根據防制毒品司法中心（Counter Narcotics Justice Centre, CNJC）的要求，當事人 X 遭控將毒品走私到 A 轄區。

48 當事人 X 將毒品藏匿在其腹部試圖攜帶出境，但在喀布爾（Kabul）國際機場遭執法單位查獲和逮捕。對當事人展開身體搜索時，發現其擁有的兩張銀行帳戶卡與兩家商業銀行相關，該起毒品走私案已轉交 CNJC 起訴。

孟加拉

49 BFIU 收到財政部對 X 先生的投訴，表示其涉嫌參與資恐和反政府活動，收到投訴後，BFIU 向相關銀行收集該人的帳戶資訊，發現 X 先生在 2012-2013 年期間，從外國轄區的 7 名不同人士收到 58,672 美元的資金。

- 50 為進一步分析案件，BFIU 主動在匯款人和收款人之間建立關係，基於此理由和分析目的，BFIU 向相關外國管轄區的金融情報中心收集資訊。ABC 金融情報中心表示，其收到一起 STR，7 名匯款人中其中一個名為 Y 先生的人，出現在該起 STR 中，曾經多次透過 Western Union 向 X 先生匯款。根據公開消息，ABC 金融情報中心還發現 Y 先生是總部位於 ABC 首都的一個人道主義基金會的成員，該基金會主辦人道主義救濟活動，與 45 個國家和 32 個國際非政府組織合作，經發現，金錢會從轄區的不同區域存入 X 先生的帳戶，再透過 ATM 領取現金。
- 51 BFIU 根據調查結果編製了一份分析報告，並發送給孟加拉警察局的執法機關，執法機關根據報告逮捕 X 先生，指控其涉入資恐和反政府活動，並根據 ATA2009 7 (a) 起訴 X 先生。

中國香港

案例研究 1

- 52 香港海關調查一個走私集團後，發現該集團僱用一般商品經營者 (GMOs) 從中國將大量現金 (疑似為走私犯罪所得) 運往香港，然後再存入本地銀行帳戶。經過深入調查，香港海關在 2015 年識別了 8 名當地居民並展開逮捕行動，調查結果顯示，2011 年至 2012 年間，這 8 人從中國攜帶了大量現金，隨後分別以

100,000 港幣（12,800 美元）至 400,000 港幣（51,000 美元）的價格存入不同銀行分行；或以 5,000 港幣（641 美元）至 500,000 港幣（64,105 美元）安排轉帳，每次都透過個人銀行帳戶匯款至由該集團控制的同一銀行帳戶，且每筆交易可獲得 20 港幣至 100 港幣不等的獎勵。整個期間，經過漂白的金錢總額高達 5,400 萬港幣（690 萬美元）。

- 53 最終，所有嫌犯都因 2017 年的洗錢陰謀而遭定罪，並判處 12 至 48 個月不等的徒刑。

案例研究 2

- 54 2013 年初，香港海關與中國海關主管機關聯合調查一個集團，其涉嫌從香港向越南出口豪華左駕汽車，再偷運到中國，同時以迂迴的方式中國漂白犯罪所得後流入香港。
- 55 買主將車款支付到策劃者在中國持有的銀行帳戶，然後再將資金移轉到由香港貨幣服務營運商（MSO）持有的中國銀行帳戶中。策劃者最終安排在香港向 MSO 收取車款，主要是現金（即走私活動的犯罪所得），經過漂白的金錢總額高達 5,900 萬港幣（750 萬美元）。
- 56 2013 年 9 月，香港海關逮捕了策劃者，其洗錢罪名最終於 2018 年成立，被判處五年徒刑。

日本

- 57 日本強調在以下案例中，洗錢或資恐類型與特定前置

活動（如毒品和詐欺）的關聯：

與「日本暴力團體」相關的洗錢和詐欺案件

- 58 日本暴力團體，即 *Boryokudan*（包括 *Boryokudan* 成員、合伙和其他相關方）犯下多起洗錢和詐欺案件，犯罪者以放高利貸的方式，借出款項後計以超過法律上限的利息，藉此從還款獲取犯罪所得（包括以假名出售贓物所獲得的收益），並使用恐嚇或武力方式討債，這種高利貸的收益會隱匿在以另一方名義所開立的銀行帳戶。

隱匿販運興奮劑相關的毒品犯罪所得

- 59 一名從事興奮劑走私活動的男子使用送貨到府服務出售興奮劑，並安排客戶將總額約 120 萬日圓（11,000 美元）的款項匯入他人名義開設的帳戶，該名男子因違反《反毒品特別規定法》（隱匿毒品相關犯罪所得）而遭逮捕。

詐欺和洗錢案件

- 60 最近，日本經常接獲特定詐欺案件的通報，例如有些人藉由出售自身銀行帳戶支付娛樂費或生活費，而部分人則使用偽造身分證，以虛構身分或他人名義開立銀行帳戶，再將其出售給犯罪者，用以透過這些帳戶促進洗錢活動。

中國澳門

- 61 2017 年 1 月至 2017 年 6 月，公共檢察院共接獲 79 起

STR，這些案件主要與詐欺有關，司法警察則針對 74 起案件展開調查。

馬來西亞

62 洗錢調查會聚焦於在 NRA 中識別的高風險犯罪，即毒品、貪污、詐欺、走私和逃漏稅，如果有組織 / 集團犯罪，則會優先列入考慮，對恐怖主義的調查也已擴大至所有資恐要件。

巴基斯坦

貪污

63 某人從 ABC 交易所購買了大量外幣，但未如實揭露真實職業 / 資金來源，在分析過程中，發現該人已從政府組織的高層職位退休，且根據媒體消息，其在服務期間涉嫌貪污，他在 Alpha 銀行與家人共同持有多個聯名帳戶，並在特定時期內將高額資金記入所有帳戶。

64 帳戶明細顯示，這些資金投資在定期存款中，期限為一年，定存到期後，透過現金 / 清算從帳戶中領取資金，然後在公開市場購買外匯。嫌犯故意利用貨幣兌換交易以現金購買外幣，以中斷資金流向。

65 考慮到嫌犯的交易模式和不利的媒體消息，其很可能繼續涉嫌貪污 / 行賄，所有銀行帳戶和隨後貨幣兌換交易的資金來源也飽受懷疑，因此將情報與執法機關共享。

走私

66 X 先生和父親 Y 先生，兩人分別在不同銀行的不同分

行開設個人和聯名帳戶，他們從事布料和地毯生意。由於 A、B 和 C 銀行在帳戶中觀察到大量資金和異常交易方式，因此將這些帳戶呈報 FMU。

- 67 分析過程中，注意到大量資金以支票存入嫌犯帳戶，再透過不超過 CTR 門檻的現金交易立即領取相同金額，避免交易通報至金融情報中心。
- 68 X 先生和 Y 先生利用線上轉帳的方式互相移轉資金，或移轉到布料與相關領域業務的他人帳戶。在 FMU 的內部資料庫中經過一番搜尋後，還發現少數幾個嫌犯帳戶，其中都有類似的交易方式。有趣的是，儘管嫌犯在各自帳戶中進行高價值交易，但並未找到嫌犯的國家稅務編號，因為他們想藉由稅務機關不瞭解其業務性質，從而逃避稅收。
- 69 根據涉嫌走私和逃漏稅罪行，因此將金融情報轉發給執法機關。

泰國

- 70 泰國反映在以下案例中，洗錢或資恐類型與特定前置活動（如貪污、毒品、詐欺和現金走私）的關聯：

毒品販運

- 71 荷蘭國民 J 先生及其同夥從事毒品走私，構成跨國組織犯罪，檢察總署（OAG）收到荷蘭的請求，並將其轉發到洗錢防制辦公室（AMLO），請求對 J 先生及其同夥緊急實施資產扣押 / 凍結行動，其不願收回資產並同

意將資產由國家沒收。OAG、特別調查局（DSI）、緝毒警察和 AMLO 組成了一個聯合工作小組，根據《防制洗錢法》第 48 條，主管機關人員迅速採取行動，扣押 / 凍結價值超過 1 億泰銖（約 300 萬美元）的資產。目前已找到證據，有可能理由相信 J 先生及其同夥透過從事某種活動獲得資產，該活動構成毒品犯罪。

貪污

- 72 犯罪鎮壓部門和泰國皇家警察總署（RTP）要求 AMLO 檢查和進行財務分析，並限制 T 先生、U 女士及其同夥（前政府公職人員）的財務往來。犯罪者挪用國家教育機構的資金，並遭控犯下竊盜、偽造和使用偽造證件以及濫用職權。交易委員會下令沒收 T 先生及其同夥的資產，交易委員會還要求 AMLO 向檢察官提交此案，以向法院提交請願書，要求法院下達命令，強制返還犯罪行為的相關資產，或賠償被害人 2 億 7,100.08 萬泰銖（850 萬美元），此案正在民事法庭程序進行。

從事公共詐欺和現金走私的公司

- 73 AMLO 協同 RTP 共同對一公司集團及其高層主管（包括其次位當事人）提起公共詐欺訴訟，該公司的註冊記錄為具有三種產品的多層次傳銷公司。相關產品從未實際生產或銷售，但公司以高於泰國銀行規定的利率，付款或獎勵招募他人加入公司網絡的成員。
- 74 其中一大股東是馬來西亞國民，在馬來西亞遭到通緝

- 後逃往泰國，而後接受整容手術改變自己的外表，同時非法取得一位泰國死者的身分，以在泰國經營業務。
- 75 根據記錄，發現共有 12 萬多名成員，估計現金流量約為 380 億泰銖（10.73 億美元），其中泰國的成員數量可能高達 30 萬，估計損失達 1,000 億泰銖（28.24 億美元），成員收到的資金直接與大股東的銀行帳戶（代名人除外）共享。
- 76 後發現，被捕的各股東都將現金留在家中而不是存入銀行帳戶，並利用現金購買豪華汽車、豪宅和昂貴用品。
- 77 4 名遭控從泰國走私大筆現金到馬來西亞的快遞員遭到逮捕，各快遞員承認，其受僱在泰國 - 馬來西亞邊境的地區 Padang Besar 開設銀行帳戶，目的是為詐欺公司中其中一人提款，再將現金跨境攜帶至馬來西亞。一名快遞員承認，他為公司攜帶了超過 3 億泰銖（1,000 萬美元）的現金。

3.3 新興的持續趨勢

汶萊

- 78 汶萊觀察到，詐欺（詐騙）是 2017 年前置犯罪中的一項持續趨勢，識別出的騙局類型多以投資騙局為主，其他少數則為愛情騙局和其他形式的快速致富騙局。
- 79 2016 年以來，金融情報中心觀察到，未受監管的線上遊戲網站的相關活動有增加趨勢，移轉資金的便捷性

加上此類網站的無限制存取，使得這類活動得以繼續。

斐濟

- 80 斐濟注意到，偽造的銀行對帳單和聘書正在興起，斐濟金融情報中心注意到，使用假銀行對帳單和聘書以在各類金融機構獲得貸款的案件數量有增加趨勢。斐濟金融情報中心接獲來自各金融機構的 15 份通報，聲稱有 30 多人使用偽造銀行對帳單和不實聘書，申請無擔保的個人貸款。
- 81 斐濟金融情報中心接獲通報，有人偽造銀行電匯表格，以詐欺手段向海外供應商和客戶取得貨物。

新興趨勢：支票漂白

- 82 斐濟注意到「支票漂白」的新興趨勢，斐濟金融情報中心觀察到向多個零售商購買物品的「支票漂白」案件數量有增加趨勢，個人會購買少量的銀行支票，以「漂白」的方式修改金額和收款人欄位，用以購買大批酒精和肉類。
- 83 零售商直到將支票存入自身銀行帳戶前，才意識到銀行支票是偽造的。部分情況下，商品會打折出售給其他零售商以獲取現金。
- 84 斐濟注意到 ATM 側錄的持續趨勢，斐濟金融情報中心多次看到外國人進入斐濟，使用遭竊的信用卡提款。據觀察，這些人進入斐濟時帶著側錄裝置，並使用空白卡（包含被盜信用卡資訊）在轄區內多個 ATM 進行

多次提款。2017 年 12 月 8 日，三名保加利亞國民因持有側錄裝置和未經授權存取限制資料，而遭判一年監禁。2018 年 1 月 8 日，兩名賽普勒斯國民遭控 293 項洗錢罪，並意圖以欺騙手段在斐濟獲取財產，該案仍在斐濟法院審理。

- 85 斐濟注意到商業電子郵件攔截的持續趨勢，斐濟金融情報中心收到了六個實體的疑似洗錢或資恐交易報告，這些實體是 2017 年商業支付攔截詐騙的被害人，損失資金總價值約為 639,106，資金後流向澳洲、美國、加拿大和韓國。斐濟金融情報中心向其國外對等單位發布案件分發報，試圖追蹤最終受益人，找出流向以追討資金，但大多數情況下，此做法相當困難。
- 86 斐濟金融情報中心繼續宣導電子郵件相關詐欺的認知，請見此[連結](#)

日本

- 87 2016 年隱匿犯罪所得的案例，主要是犯罪者試圖以他人名義將資金移轉到銀行帳戶，這是日本在洗錢犯罪中常用的方法。
- 88 此外，犯罪者使用各種方法阻止調查機構追蹤資金流向，包括使用假名出售遭竊物品、掩飾獲取犯罪所得的原因等等。

寮人民民主共和國

- 89 走私毒品一直是 ML/TF 趨勢，尤其是每年預測的犯罪、

凍結、扣押和沒收相關資產以及寮國對販毒者制裁增加。

中國澳門

90 中國澳門注意到匯款詐欺的新興趨勢，接獲的疑似洗錢或資恐交易記錄的分析顯示，匯款詐欺行為不斷增加，這在過去幾個月中引起銀行業的特別關注。一般情況下，本地銀行帳戶接收海外匯款，然後立即將其匯入其他司法管轄區，受款銀行隨後從匯款銀行收到電報，或從被害人收到一封電子郵件，聲稱相關匯款與詐欺行為有關。

馬來西亞

91 STR 大量增加，可歸因於報告機構加強了對交易的監控，對貨幣服務營運商的認知也增強。報告機構通報的主要罪行是詐欺 / 詐騙、逃漏稅和行賄 / 貪污。

92 馬來西亞注意到以下持續趨勢：

- 現金交易仍然是轉移非法所得（接收、轉移和支出）的首選方法。
- 使用第三方帳戶（包括車手帳戶（mule account）持有人）接收和轉移犯罪活動的非法所得。
- 為恐怖主義活動籌集資金主要是為了資助外國恐怖主義戰士（FTF），而不是為恐怖主義團體本身提供資金。
- FTF 的資金通常經由社群媒體籌集而來。
- 使用第三方帳戶（包括車手帳戶）接收或轉移給

FTF。

巴基斯坦

93 巴基斯坦注意到以下情況：

- *新興趨勢*：與虛擬貨幣相關的可轉換債券。
- *持續趨勢*：2017 年收到 Hawala/Hundi 相關的 STR。

泰國

94 泰國注意到金融科技的新興趨勢，其中，加密貨幣多遭濫用為犯罪管道，TBML 成長尤其與毒品交易幫派有關。

95 泰國注意到使用境外銀行、第三方洗錢 / 代名人和地下銀行的持續趨勢。

4. 聚焦於透過網路助長的洗錢和資恐：網路洗錢

- 96 過去 10 年間，技術常用於實現金融犯罪的趨勢一直穩定成長，這是因為網路、社群媒體技術以及相關金融平台等的可用資訊和通訊技術（ICT），在種類和可及性有長足的進步。
- 97 網路助長的 ML/TF 可廣義理解為兩個問題：使用網路進行前置犯罪（網路犯罪）和使用網路洗錢或資助恐怖行動（網路洗錢）。
- 98 網路犯罪是犯罪持續演進的領域，網路犯罪領域下，犯罪者常利用網路的匿名性、速度和便利性，進行各種非法活動，這類活動多半不受限於實體或虛擬邊界，會對全球被害人構成真正威脅，甚至造成嚴重傷害，例如進行從銀行帳戶未經授權即撤離資金、支付卡詐欺等。
- 99 「2018 年 APG 態樣報告」聚焦於瞭解網路犯罪相關的新興風險、趨勢和背景問題，以及漂白非法所得的網路洗錢活動。

4.1 亞太地區網路犯罪的範圍

- 100 網路詐欺是該地區特別普遍的威脅。2017 年發布的最新調查¹發現，亞太地區日益成為詐欺目標，網路犯罪

¹ ThreatMetrix – a LexisNexis Risk Solutions Company, *Asia Pacific*

同比成長了 35%，主要集中在帳戶接管和付款詐欺。

101 該報告還指出，自 2015 年底以來，全球網路犯罪已增加近 100%，主要驅動力是新帳戶發起詐欺的情況增加，自 2017 年底以來，新帳戶詐欺增加了 30%。

4.2 FATF 打擊洗錢、資恐、資助武器擴散和網路犯罪的措施

102 FATF 標準包括與打擊網路犯罪相關的各種工具，其中，對洗錢和資恐的刑事定罪涵蓋了許多類別的犯罪，可應用於打擊網路犯罪的各個層面。

- 資助恐怖主義（包括恐怖主義）：當支援者尋求向位於海外的恐怖分子和恐怖組織提供資金時，資恐就可能會在網路和社群媒體上發生。請參見社群媒體和恐怖主義融資的 APG/MENFATF 聯合態樣報告。
- 性剝削（包括對兒童的性剝削）：對兒童的性剝削可能包括線上製作、散布和分發兒童剝削資料，每年足以產生數十億美元的犯罪所得。使用資通訊技術進行對兒童的商業性性剝削可增加犯罪者的潛在利潤，因為他們生產和分發資料的成本較低，且可

Cyberattacks up 35% Year on Year, As Global Organized Fraud Rings Turn Their Attention to Emerging Financial Services (隨著全球組織詐騙集團轉而聚焦於新興金融服務，亞太地區網路攻擊率同比成長了 35%)，(2017).

於線上爭取更大的潛在客戶群²。網路速度提高和行動裝置的取得性提高，導致兒童性虐待現象的增加，透過直播向觀眾收費，甚至會將錄製成果出售給他人³。

- 非法販運：FATF 標準涉及麻醉品和精神藥物的非法走私、非法武器走私以及遭竊物品和其他貨物的非法販運。毒品、武器和遭竊物品也可能透過全球網際網路於線上市場出售，或甚至匿名經由「暗網」（dark web）出售⁴。
- 詐欺、身分盜用和詐騙：這些在網路上已存在相當長的時間，且仍是成員司法管轄區面臨的一個普遍問題。
- 搶劫或竊盜：資通訊技術還促進助長搶劫和竊盜的新形式。
- 勒索：勒索亦可能透過資通訊技術進行，其方式與犯罪者線下向被害人勒索金錢類似。資通訊技術也促成部分新的勒索方法，例如勒索軟體，勒索軟體

² United Nations Office on Drugs and Crime (UNODC) (2014) Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children (新資訊技術對兒童虐待和剝削之影響研究), Vienna pp.18-19

³ UNODC (2014), p. 23

⁴ 暗網是存在於黑暗網路 (darknet)、覆蓋網路 (overlay network) 上的全球資訊網內容，只能用特殊軟體、特殊組態或特殊授權才能存取。

是一種惡意軟體，可以鎖定裝置或使用加密阻擋資料存取，直到付出贖金為止⁵。勒索軟體攻擊通常尋求以加密貨幣付款⁶（例如比特幣），款項須發送到特定地址才能解鎖帳戶⁷。

103 關於國際文書的 FATF 建議第 36 建議，鼓勵核准和實施 2004 年 7 月的《網路犯罪公約》（又稱《布達佩斯網路犯罪公約》或《布達佩斯公約》），該公約打破先例，首次藉由統一國家法律、改良調查技術以及加強國家間打擊網路犯罪合作，來解決網路和電腦犯罪⁸。

104 FATF 還針對商業網站和網路支付系統的洗錢和資恐弱點發布報告（2008 年），該報告著重於以下內容：

⁵ Richardson R & North M (2017). Ransomware: Evolution, mitigation and prevention (勒索軟體：演變、緩解和防範)。International Management Review, 13(1), p. 10.

⁶ 值得注意的是，洗錢網絡可能需要相對較高層級的技術才能使用加密貨幣進行洗錢計畫，但由於目前缺乏 AML/CFT 法規，因此仍視為具有很大風險，許多加密貨幣的匿名性質對犯罪者而言相當具有吸引力。

⁷ van Wegberg, R, Oerlemans, J and van Deventer O, (2018) "Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin" (比特幣洗錢：混合結果？：使用比特幣進行網路犯罪洗錢的探索性研究), Journal of Financial Crime, 25:2, p. 419.

⁸ Banks J (2011) European regulation of cross-border hate speech in cyberspace: the limits of legislation (關於網路空間中的跨境仇恨言論的歐洲法規：立法限制), European Journal of Crime, Criminal Law and Criminal Justice 19:1-13

- 商業網站和網路支付系統的弱點包括：使用者可能維持匿名、人為干預有限、交易速度、交易次數高、非面對面註冊、國際足跡、管轄權有限、傳統金融機構難以監控和偵查可疑金融交易，其結果就是，使用網路支付服務供應商時，發現可疑金融交易的能力可能會受到影響。
- 非面對面商業和金融交易以及交易基礎洗錢相關的許多 ML/TF 風險，同樣適用於網路支付系統和商業網站。大多數線上支付來自銀行帳戶或信用卡發起的金融交易；這些涉及到客戶識別、報告義務和交易記錄留存流程。由於低價值交易不一定代表低風險，因此仍受制於金融產業適用的監管控制。
- 需要線上身分驗證解決方案，例如特定轄區使用電子身分證，以在非面對面註冊以及使用者可能維持匿名的情況下，協助商業網站和網路支付服務供應商抵減犯罪活動風險。
- 如果網路支付服務供應商充分監控客戶的財務交易，能夠在監測到與客戶交易剖析發生偏差時直接採取對應措施，如此一來，縱使與商業網站和網路支付服務建立關係之初缺乏面對面的聯繫，但也不至於構成問題。
- 可比較的 AML/CFT 義務可用性，對於線上和線下零售商家和支付服務至關重要。

- 網路支付服務供應商和不同司法管轄區的商業網站，在打擊 ML/TF 方面所做的努力不至於因不同的隱私法規而受阻，相關法規可能會干擾服務供應商就可疑的 ML/TF 交換的客戶資訊量。

105 2013 年，FATF 發布*風險基礎方法指引原則報告：預付卡、行動支付和網路支付服務*。在全球，功能增強、成長快速加上新型支付產品和服務（NPPS）不斷普及，使得司法管轄區和私部門機構越來越難確保這些產品和服務不會遭洗錢和資恐濫用。司法管轄區致力藉著以下方式制定和實施 NPPS 的 AML/CFT 法規：

- 說明新式支付系統如何運作、哪些實體提供 NPPS、其職務 / 活動為何。
- 查驗哪些提供 NPPS 的實體已納入 FATF 建議之下（換言之，屬於 FATF 定義之金融機構）。
- 判定提供 NPPS 所涉及的風險，包括考慮相關的風險因素和風險緩解措施。
- 考慮監管對 NPPS 市場的影響，包括監管是否影響金融包容性以及將貨幣存款轉移到受監管金融機構的正面影響。

106 根據 NPPS 指引原則，FATF 在 2014 年發布一份報告，有關*虛擬貨幣：關鍵定義和潛在 AML/CFT 風險*。本報告提出一概念架構，可用於理解和因應其中一種與網路支付系統：虛擬貨幣相關的 AML/CFT 風險。具

體而言，該報告提出一通用的定義性術語表，該術語表根據不同的業務模型和操作方法，闡明何謂虛擬貨幣，並對各類虛擬貨幣進行分類，識別典型虛擬貨幣系統中的參與者。該報告還將 2013 年 NPPS 指引原則第四節（A）中規定的風險因素，應用於特定類型的虛擬貨幣，藉此識別潛在風險；另描述最近涉及虛擬貨幣的特定調查和執法工作；提供管轄區目前對虛擬貨幣監管方法的範本。

- 107 2015 年，FATF 發布*虛擬貨幣風險基礎方法指引原則*，該指引原則是 FATF 分階段方法中的一環，其依據是 2014 年虛擬貨幣報告和風險矩陣以及預付卡、行動支付和網路支付服務風險基礎方法報告最佳實務指引（2013 年 NPPS 報告）。實際上，虛擬貨幣支付產品和服務（VCPSS）的開發，以及 VCPSS 與其他新式支付產品和服務（NPPS）之間，甚至是與傳統銀行服務之間的交互作業，一再使得該指引大受歡迎，因為各方都需要保障全球金融體系完整性，免於遭受犯罪和網路犯罪（包括網路洗錢）。
- 108 該指引的重點是通往受監管金融體系的交會點，尤其是可轉換虛擬貨幣交易所。

4.3 打擊網路犯罪的現有努力和挑戰

- 109 近年來，網路助長的 ML/TF 和更廣泛的網路犯罪，

皆成為國際關注的焦點，在司法管轄區、區域和國際層級，皆分別展開許多活動，旨在進一步瞭解網路犯罪的性質、網路犯罪的預防策略以及調查和起訴犯罪者的工具。

監管加密貨幣

- 110 各司法管轄區除了簽訂《布達佩斯公約》，以期在各締約國間建立一致的法律架構和調查權力，除此之外還試圖使產業受到 AML/CFT 組織的監管，藉此解決加密貨幣相關的關鍵問題。
- 111 馬來西亞針對數位貨幣交易業者實施 AML/CFT 要求，將這些實體列入《2001 年防制洗錢及打擊資恐及非法活動所得法》附件 1 的「報告機構」⁹。這使得數位貨幣交易業者必須採取有效措施，防範與加密貨幣相關的 ML/TF 風險，同時也提高馬來西亞數位貨幣活動的透明度。此外，這些數位貨幣交易業者還須提供有關自身業務概況和活動的詳細資訊，並提交有關數位貨幣交易的每月報告。
- 112 澳洲根據《2006 年防制洗錢和打擊資恐法》下發布的「2018 年 AML/CTF 數位貨幣交易註冊政策原則」，對數位貨幣交易業者實施 AML/CFT 要求。除其他事

⁹ 更多詳細資訊請參見：http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4628&lang=en

項外，數位貨幣交易業者必須向 AUSTRAC 註冊、擬定 AML/CFT 計畫、申報疑似洗錢或資恐交易並留存充分記錄。¹⁰

司法管轄區面臨的挑戰

113 網路助長的 ML/TF 帶來許多挑戰，包括：

- 調查網路犯罪方面缺乏執法機關專業知識，負責調查網路犯罪與 ML/TF 的多個執法機關之間，若國內作業協調不善，將可能使情況更加複雜。
- 可能還缺乏針對網路犯罪或相關技術變更要件的法規。隨著技術演進，攻擊者的手法和攻擊者本身也不斷變化，網路威脅的性質因此不斷發展。¹¹
- 許多網路犯罪的跨國性質。一轄區中的個人，可使用託管於另一轄區的網路平台，對位於第三轄區的被害人犯罪。若要調查網路犯罪和相關的 ML/TF，有地緣關係或密切資通訊技術連結的不同轄區之間，須展開強而有力的國際合作。鑑於在網路空間中進行互動時，管轄權邊界之易滲透性，國際合作與協作對於打擊網路犯罪至關重要¹²。

¹⁰ 更多詳細資訊請參見：<http://www.austrac.gov.au/digital-currency-exchange-providers>

¹¹ Emerson R G (2016) Limits to a cyber-threat (對網路威脅的限制), *Contemporary Politics*, 22:2, p. 178

¹² Skopik F, Settanni G and Fiedler R (2016) A problem shared is a problem

- 網路犯罪和網路助長的 ML/TF 調查也需要與私部門強而有力的合作，私部門營運的線上基礎架構，開發過程通常不會將安全性和與執法機構合作列為優先事項¹³。如上所述，網路犯罪的跨國性質抑制了司法管轄區對外國私人公司執法的能力，反之，若採取合作方式，而非一味懲罰，試圖從社群媒體和電信公司等私營公司取得協助，可能會帶來更多好處。
- 對線上交易和一般交易的安全性缺乏信心，可能會限制司法轄區中的金融交易數量，因為客戶可能會轉往其他更安全的市場。

4.4 透過網路漂白進行洗錢（網路助長的 ML/TF）

孟加拉

案例研究 1

- 114 透過定期監控社群媒體，社群媒體監控和監測團隊（SMMST）識別了一個名為「X」的帳戶，該帳戶大肆宣傳激進意識形態，激發其他社群媒體使用者持續

halved: a survey on the dimensions of collective cyber defense through security information sharing（問題共享難度減半：透過安全資訊共享調查集體網路防禦維度），Computers & Security, 60. P. 157

¹³ Caveltly M D (2014) Breaking the syber-security dilemma: aligning security needs and removing vulnerabilities（打破網路安全困境：調整安全需求並消除弱點），Science and engineering ethics 20:3, p. 704

產生衝突，此外，該帳戶試圖募資以摧毀世俗化的孟加拉，改而建立哈里發制度，後來，該帳戶還宣布恐怖分子已到來，即將展開攻擊。

- 115 在此背景下，SMMST 尋求相關社群媒體公司的協助，識別該帳戶的擁有者，根據社群媒體公司提供的資訊和行動追蹤，SMMST 團隊順利逮捕該帳戶背後的擁有者。調查期間，SMMST 得知「X」是一個虛構名稱，由名為「Y」的個人實際操縱該社群媒體帳戶，調查人員還發現，「Y」是孟加拉政府指定實體名單中的活躍成員：Ansar Al Islam Bangla Team (ABT)。
- 116 BFIU 從調查機構獲得有關「Y」的資訊後，對其在金融產業的帳戶展開搜索，發現該人擁有 3 個銀行帳戶和多個行動金融服務 (MFS) 帳戶。這 3 個銀行帳戶都將該客戶識別為具有線上業務和關係企業行銷業務的客戶，但是，AOF 或 KYC 個人資料表格中，並未指明與之展開業務的線上業務實體、合作夥伴實體、帳戶或頁面。這些帳戶有著來自轄區不同地方的零星小額現金存款，MFS 帳戶的交易頻繁，大部分為現金，且帳戶多半用畢最多 MFS 交易限額，所有帳戶都保持在最低餘額。
- 117 根據 2009 年《反恐怖主義法》和 2006 年《資訊技術和通訊法》，已對該人提起訴訟。目前，調查人員正進一步調查以識別其同夥。

案例研究 2

- 118 以孟加拉政府資深公職人員的名義建立一臉書專頁，該專頁發布多則有關政府將經濟援助擴大到失業人員的貼文。為使專頁更受信賴，提出某些口號，如「脫離恐怖主義，恢復正常生活：政府將財政援助擴大到失業的貧困人口」。該專頁還貼出政府公職人員移交支票的圖片。該頁面提供電話號碼和電子郵件地址，指示有興趣的人主動聯繫以尋求經濟援助。
- 119 不少有興趣的人受到該臉書專頁的貼文吸引後，主動聯繫電話號碼和電子郵件地址，之後這些人收到電子郵件通知，表示已獲選為政府援助對象，政府公職人員不久後將把經濟援助支票交給他們。電子郵件中還指示這些人預先將 25% 的經核准援助存入援助計畫專案總監的銀行帳戶，以作為保證金，該銀行帳戶的收款人為「J 女士」。於是部分人根據指示將錢存入帳戶，但再也沒有收到所謂的政府部門回應。
- 120 此問題已引起相關部門關注，其將此問題通報執法機關、相關銀行和中央銀行。接獲該問題後，銀行提出疑似洗錢或資恐交易報告，中央銀行的不同部門而後將該問題轉發給 BFIU。BFIU 對問題進行分析，發現一群人使用臉書專頁和銀行帳戶進行詐欺，也確實騙到一部分民眾。該帳戶中存有 60 萬孟加拉幣，存入的錢在短時間內立刻提領一空，部分提款則再存

入另一個銀行帳戶，詐欺者的兩個銀行帳戶以及一個行動金融服務帳戶（餘額為 20 萬孟加拉幣）根據 MLPA2012 遭到凍結。負責單位編寫分析報告後傳達給執法機構。

汶萊

身分盜竊

121 犯罪者使用被害人的名字或身分犯罪，身分識別詳細資訊，如姓名、身分證字號、財務資訊（銀行帳號和 PIN 碼），可從多種管道（社交工程（Social Engineering））取得，包括透過電子媒體、語音電話或簡訊平台進行網絡釣魚。此類資訊會被用於詐欺，包括信用卡或 ATM 提款卡詐欺以及未經授權的線上銀行轉帳。

線上詐騙

122 犯罪者會利用社群媒體來獲得被害人的信任，最終透過提供產品、服務、商業投資、愛情騙局等方式欺騙被害人。例如，愛情騙局（也稱為詐騙郵件）是一種進階收費詐欺，例如要求被害人向犯罪者匯款，確保其可進入被害人的司法管轄區。

性勒索

123 被害人（通常是年輕人）遭誘拐進行視訊性愛，之後被害人為防止影片遭上傳和散布而被迫付款。

斐濟

為犯罪而進修

- 124 Manjeet Singh 先生和 Rajneel Chaudary 先生是在南太平洋大學（USP）進修的兩名友人，兩人密謀非法存取相關人士的網路銀行以竊取資金。Manjeet Singh 先生知道其房東將所有銀行帳戶詳細資訊保存在何處，並使用竊取來的詳細資訊為房東註冊網路銀行業務，而後，Manjeet Singh 先生進行三筆網路銀行轉帳，從其房東的帳戶將錢轉到自身名下的帳戶中（戶名為 Rajneel Chaudary 先生和 Arti Darshana Reddy 女士），金額共計 22,000.00 斐濟幣。Arti Darshana Reddy 女士是一位友人，Rajneel Chaudary 先生意圖使用其帳戶來支付學費，將資金轉帳至 Arti Darshana Reddy 女士的帳戶後，他使用她的 ATM 提款卡提領資金。
- 125 Rajneel Chaudary 先生假裝將資金存入該銀行的分行，並對另一名被害人的銀行帳戶提出詢問，Rajneel Chaudary 先生能夠獲取個人詳細資訊以存取被害人的帳戶，急著，Manjeet Singh 先生從被害人的帳戶進行三筆網路銀行轉帳，總計 4,340 斐濟幣。
- 126 2017 年 3 月，Manjeet Singh 先生以犯有三項洗錢罪行遭到定罪，並於 2017 年 4 月被判處 9 年徒刑；2017 年 4 月，Rajneel Chaudary 先生承認犯下三項洗錢罪後，被判處 8 年徒刑。

- 127 此案例研究是促成兩起洗錢定罪的首例國內網路犯罪案例，共謀和操縱銀行系統的程度顯而易見，這對斐濟的網路銀行系統產生了更廣泛的影響。

日本

- 128 日本金融情報中心（JAFIC）從策略性分析中發現，許多銀行帳戶收到來自網路賭博的犯罪所得，有關這些犯罪活動的資訊已分發給執法單位。

中國澳門

- 129 2017年8月，司法警察接獲一起詐欺通報，據稱，一名女性被害人遭詐騙巨額資金，其於2016年在網路上發布親身經歷。她當時與其中一名嫌犯結交為友，該嫌犯聲稱自己是同一案件的另一名被害人。2017年7月30日，上述嫌犯透過行動通訊應用程式接近被害人，自稱曾是一名資深警官，能夠藉助自己與法院的關係，以合法方式優先追討被害人丟失的錢財。其後，被害人在兩名冒充法院人員的詐欺者的指示下，一連20次以上將總計630,000澳門幣（78,000美元）的金額，電匯到指定銀行帳戶，最終她意識到自己上當了，於是向警方報案。

- 130 2017年11月8日，另一名類似案件的女性被害人向司法警察報案，稱她在2015年向當地一名男子借出55萬港幣（折合78,100美元）後，對方即失聯。一名自稱為貸款人的嫌犯，於2016年10月31日在社

群網路平台上聯繫被害人，聲稱願意還錢，但要求該被害人先解凍他的銀行帳戶，並預先支付手續費。被害人隨後收到由三名偽裝成公共檢察院和法院人員使用行動通訊應用程式發送的訊息，要求其親自進行銀行轉帳以支付處理費。該名被害人最終遭詐騙 10,000,000 港幣（1,300 萬美元）。

- 131 司法警察證實並確定上述案件的涉案人員來自同一詐騙集團，2017 年 11 月 11 日，在北區和中區的幾間公寓中逮捕了 8 名男女，連帶扣押了 240,000 港幣（31,000 美元）的非法資金和證據。
- 132 調查顯示，其中一名被捕婦女是案件的策劃者，其餘涉案人員偽裝成司法機關人員進行詐欺。策劃者使用其他涉案個人或策劃者本身的銀行帳戶接收並提領非法資金，並迂迴的方式移轉款項，這些款項最終存入了其在海外的銀行帳戶。
- 133 司法警察將這 8 名男女移送公共檢察院，以詐欺和洗錢罪名起訴，同時追究其他相關人士和犯罪所得。

馬來西亞

商業電子郵件攻擊 (BEC)

- 134 A 先生是組織內的高級會計師，收到一份專人親送、以電子郵件形式印出的指示，隨信附有一份據稱由高層主管寄來的發票，內容涉及變更受款銀行詳細資訊以進行預定付款，涉及金額為 120 萬美元。預期收款

人的銀行帳戶理應位於轄區 A，但變更為轄區 B 的另一家銀行，兩個帳戶持有人的姓名完全相同。

135 該名會計師相信了他手上的這份指示，因此填妥新的電匯（TT）表格以變更為新的受益人帳戶，交由相關主管核准後簽名。新填寫的 TT 表格已發送給銀行，開始轉帳至新的受益人帳號。

136 當天稍晚，A 先生接到監理機關的來電，表示其發行這筆 TT 是假的，高層主管與預定收款人之間的電子郵件往來遭到不名犯罪者攔截，進而變更受款銀行的詳細資訊。警方已提出通報，並立即發出指示要求撤回這筆資金。

137 此情況下，由於兩個轄區（被害人所在轄區和 B 轄區）的金融情報中心和相關執法機構根據艾格蒙聯盟 BEC 快速回應計畫迅速採取行動，因此成功阻止這次轉帳。

138 一般而言，涉及 BEC 案例的指標如下：

- 成立 / 使用的公司名稱（包括國際知名公司）與被害人的類似。
- 詐騙金額不高 / 在公司的正常範圍內，以免引起被害人懷疑。
- 不尋常的交易指示方法。
- 使用偽造文件。

- 資金立即以現金或透過轉帳到代理的方式從帳戶中提出。
- 帳戶行為不一致，包括轉帳目的變更。

紐西蘭

- 139 紐西蘭警方指出一起使用越南臉書社群專頁的案件，該專頁尋找毫無戒心的參與者，利用其身分為跨國犯罪網絡促進洗錢，該網絡涉及進口大量古柯鹼。
- 140 警方在調查大量古柯鹼進口時，正在監控犯罪者與一名知名洗錢人士的會晤情形，該名男性犯罪者將一袋現金交給女性犯罪者，女犯隨後與另一人（洗錢者（smurf））在銀行外頭見面，洗錢者隨後將 10 萬紐幣存入自己的銀行帳戶。
- 141 該洗錢者被捕時解釋，她已在越南當地臉書專頁貼文，表示想避開 Western Union 或銀行手續費將錢從越南匯入紐西蘭。一名男子回應並安排她與男子母親見面，其母親有意將錢退回越南，兩名女性在銀行見面時，洗錢者的母親正在越南的一家銀行存入 10 萬紐幣的等值資金到越南的銀行帳戶中，她告訴警方，這在越南是完全正常的做法，人們經常在臉書上發布類似的要求。
- 142 進一步調查後發現，最初的男性犯罪者與其母協同另外 8 人這麼做，而且都沒有提出任何問題，因為在那個背景下這是相當正常的現象。

143 最初的洗錢者以洗錢罪起訴，但當利用洗錢者的程度明朗後，該起訴隨後即撤銷。紐西蘭警方的資產追討單位限制 NZD100K 的流通，理由是這顯然仍是犯罪所得。

新加坡

國際電匯詐欺（車手）

144 2012 年初，商業事務部（CAD）發現一種犯罪趨勢，犯罪者侵入被害人的電子郵件帳戶，向被害人的銀行發送詐欺性指令，指示要將資金轉入新加坡的銀行帳戶。其他案例中，被害人受騙上當（包括網路愛情騙局）後，在犯罪者的指示下進行資金移轉。

145 CAD 的調查確定，海外犯罪集團是海外犯罪活動贓款的幕後黑手，新加坡的銀行帳戶持有人是與犯罪集團成員結交為友的當地人，雙方主要是透過社群網站交友。這些本地銀行帳戶持有人（稱為「車手」）有意或無意地應犯罪集團的請求，同意在其帳戶中接收匯出的資金，再將資金轉至他處，通常會轉至海外銀行帳戶，「車手」通常會因其在資金移轉中擔任的角色而獲得佣金。

146 下表詳細列出，CAD 與國外對等單位經由密切合作所識別的國外被害人銀行帳戶數量、從被害人帳戶轉出的金額，以及 CAD 成功扣押的犯罪所得金額。

CAD 已識別的銀行帳戶數量及扣押的犯罪所得

	2012	2013	2014	2015	2016	2017
識別的國外被害人銀行帳戶數量	129	264	148	64	37	44
確認已遭詐欺而從被害人帳戶轉入新加坡帳戶的總金額（百萬）	24.6	31.5	14.9	6.67	3.81	5.41
扣押的犯罪所得百分比	11	18	15	15.6	25.1	36

147 新加坡為打擊此趨勢投入許多努力，最後有效使得利用新加坡「車手」進行國際電匯詐欺洗錢的通報犯罪所得大大減少。國外被害人銀行帳戶數量下降了83.3%，從2013年高峰的264個帳戶下降到2017年的44個帳戶，自2015年以來，此數據的下降趨勢保持穩定。新加坡採取多管齊下的做法，CAD (i) 立即與相關利害關係方（包括外國金融情報中心和產業合作夥伴）共享資訊，(ii) 與各個司法管轄區的執法機關密切合作，以識別被害人的錢是否已詐欺性移轉到新加坡後再進一步移轉，從而在新加坡展開洗錢調查 (iii) 與總檢察署（AGC）合作，確保對錢車手採取強而有力的執法行動，以及 (iv) 加強預防犯罪和公共教育領域。

泰國

線上彩票騙局

- 148 來自中東地區某個國家的 W 先生聯繫 AMLO 開立一張支票，該支票立即以 Worldwide Express Courier Company（全球快遞公司）寄送，他聲稱這張支票來自 Yahoo 中獎彩票，AMLO 無權扣留，但與 AMLO 主管深談後，他意識到自己上當了，被偽裝成彩票計畫中的 Yahoo 協調員的人所欺騙。
- 149 W 先生與 AMLO 聯繫之前，經由 Western Union 將款項移轉給 S 先生，以開立其中獎彩票的支票，結果損失了 650 美元。該騙局利用 AMLO 的名稱已增加計畫的可信度。

社群媒體詐欺行為

- 150 被害人透過臉書與外國人 P 先生保持聯繫，她受騙並向犯罪者開設的多個銀行帳戶轉帳 11 次，損失超過一百萬泰銖（約 35,000 美元）。
- 151 被害人將 35 萬泰銖（約 10,000 美元）轉入 Y 女士在 T 銀行開設的帳戶（為 P 先生的合夥人），在此之前，銀行系統偵測到不尋常交易，因此通知銀行分行向帳戶持有人根據增強客戶審查流程徵求更多資訊。但是，分支機構無法聯繫該人。

5. 洗錢和資恐的案例研究

5.01 資助恐怖主義

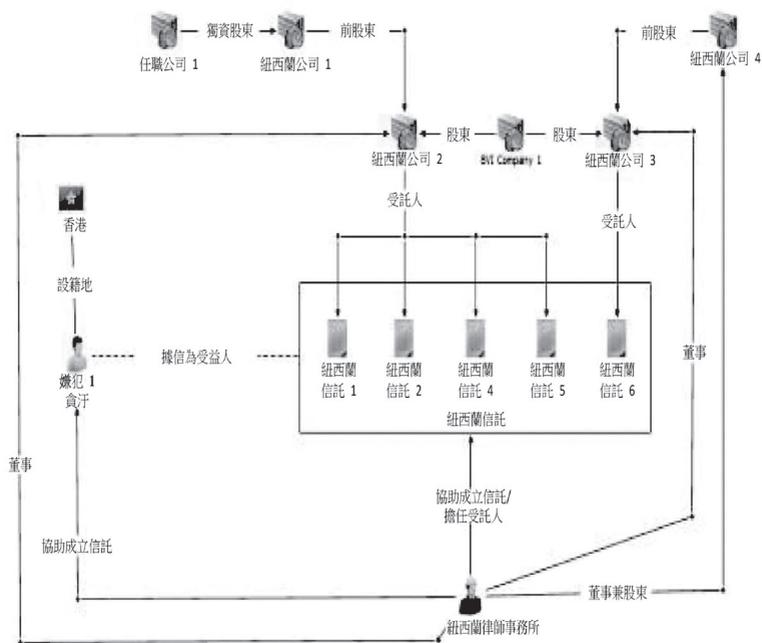
馬來西亞

- 152 有兩個人正在籌集資金，意圖資助前往敘利亞的外國恐怖主義戰士（FTF），這兩人透過部落格和被告的臉書帳戶籌集資金。
- 153 所有資金都被轉入其中一名被告的銀行帳戶，然後再移轉或交給 FTF 及其家人，以供支付旅費和津貼。
- 154 此案例中使用的方法包括：
- 使用代名人、信託、家庭成員或第三方等。
 - 使用現金
- 155 這些對象遭控犯下資恐罪名，最初，這些對象因籌集資金遭定罪，被判處 3 年徒刑，並因恐怖主義理由須賠償 2 年的資金。在檢察官對判決提出上訴後，各項指控的刑期均增至 15 年徒刑。

5.02 使用境外銀行、國際商業公司和境外信託

紐西蘭

- 156 媒體報導指出，A 人士挪用大筆金額後，使用犯罪所得購買高價值資產，紐西蘭一家律師事務所為 A 人士成立紐西蘭信託和公司，該律師事務所專門為境外客戶設立機構。



巴基斯坦

157 多起疑似洗錢或資恐交易報告都指向同一個人：Adam 先生，其曾是「Alpha 公司」的執行長，該公司是位於開曼群島「Beta 公司」的子公司。「Gama 公司」以 2.5 億巴基斯坦盧比的價格收購了「Alpha 公司」，而後，銷售收益從保留在 AA 銀行的 Gama 公司帳戶，轉移到保留在 BB 銀行的 Beta 公司帳戶。Adam 先生是操作 Beta 公司帳戶的唯一授權人，其將資金進一步轉移到自己在 CC 銀行的個人帳戶中，這是不尋常的

舉動。Adam 先生從自己的現金帳戶中提領出資金，然後向外匯公司購買外幣，再將現金存入其在 CC 銀行開設的外幣帳戶，最後將資金從轄區匯出到其在外國轄區 DD 銀行開設的個人帳戶。

- 158 Adam 先生的財務活動似乎很不尋常，他看似 Alpha 和 Beta 公司的實質受益人，並故意建立交易以免被發現。

5.03 使用虛擬貨幣

中華台北

- 159 「X」人士為一詐騙集團的成員，其在網路上廣泛研究比特幣，他將詐欺收益轉換為比特幣，再反覆轉移到電子錢包中，更設立了五道障礙，阻止警方追查這筆資金，並在一個月內成功漂白了新台幣 5,000 萬元。
- 160 X 首先使用偽造身分證件申請一個比特幣帳戶，將詐欺收益轉換為比特幣後，使用手機應用程式將比特幣轉移到另一個帳戶，最後再轉移至詐騙集團的帳戶。由於追蹤比特幣有一定困難度，導致 X 在一個月內成功漂白超過新台幣 5,000 萬元。在調查局的偵訊中，X 遭控違反法律。

斐濟

- 161 斐濟金融情報中心收到有關 X 夫婦的 STR，兩人在 18 天內收到超過 80,000 美元的匯入款項，斐濟金融

情報中心進行查驗，確定 X 女士是與外國人 X 先生結婚的當地國民，個人的旅行詳細資訊顯示，X 先生和 X 女士均居住在轄區 A。

162 對匯入款項的初步分析顯示，位於亞洲的一個店頭市場交易（OTC）比特幣團隊已將資金匯給 X 夫婦，斐濟 FIU 隨即透過艾格蒙聯盟安全網（ESW）向三個外國金融情報中心發送請求，要求進一步瞭解匯款給 X 夫婦之人的更多資訊，位於轄區 B 的一個外國金融情報中心識別資金匯款人之一（Y 先生），確定為其在該轄區內的利害關係人。

163 轄區 B 的金融情報中心多次接獲通報，表示 Y 先生時常涉入數位貨幣的買賣，Y 先生亦出現在逃漏稅報告中，並多次遭控在轄區 B 犯下電腦相關犯罪；相關報告已轉交斐濟的警察部隊和轄區 A 的金融情報中心，轄區 A 的金融情報中心並將斐濟金融情報中心的報告分發到下轄相關執法機構：

a) 可能犯行：

- 網路相關的犯罪
- 逃漏稅

b) 指標包括：

- 18 天內從無關的外國第三方匯出大量款項。
- 帳戶持有人不居住在司法管轄區。
- 其中兩名匯款人涉及虛擬貨幣。

日本

- 164 日本執法機關經手一起涉及比特幣的洗錢案件，其中一名嫌犯向比特幣交易所詐取一定數量的比特幣，將其結合從合法來源獲得的比特幣，接著，嫌犯兌現比特幣，再將資金轉移至他人名下的銀行帳戶，藉此掩飾資金來源。
- 165 嫌犯後來遭定罪，違反《刑法》第 246-2 條（電腦詐欺）和《組織犯罪懲治及犯罪所得和其他事項控制法》（隱匿犯罪所得）第 10 條。

巴基斯坦

- 166 多間銀行提出多起疑似洗錢或資恐交易報告，表示在不同人名下的多個帳戶中發現類似性質的交易。有人懷疑這些帳戶持有人涉入比特幣（虛擬貨幣）交易，這些帳戶中的交易方式顯示，資金透過 IBFT、INET、行動銀行記入，轉移到 ATM 後，以 ATM 和轉帳方式將現金提領一空。
- 167 在公開資料庫中搜尋後發現，這些人活躍於社群網站上，透過網路行銷影響民眾買賣電子貨幣，並為潛在比特幣客戶提供一平台。但巴基斯坦國家銀行並不承認比特幣等加密貨幣。
- 168 根據從 FMU 取得的 STR 資料庫資訊，參與加密貨幣業務的部分人士名下有其他帳戶，其中也觀察到類似的交易模式。根據分析結果與主管機關共享金融情

報，以考慮針對緊急以銀行帳戶使用數位貨幣（例如比特幣）採取適當措施 / 控制措施。

菲律賓

- 169 AMLC 收到了菲律賓執法機關要求提供 JD Cruz 銀行帳戶資訊的請求，該人涉嫌實施網路詐欺。JD Cruz 是 Cavite XYZ Trading and Services 的註冊所有權人，據稱該公司從事交易所交易。
- 170 JD Cruz 帳戶的已申報交易主要包括提款，提領金額從 Php509,000 到 Php420 萬不等，這顯示帳戶中的貸項低於申報門檻金額。
- 171 一虛擬貨幣交易所（VCE）對 JD Cruz 提交多起 STR，其於 2017 年 9 月進行兩筆現金存款交易，總計 100,000 菲律賓幣，另有一筆國內匯出款項，總計 78,000 菲律賓幣，VCE 認為交易與客戶的業務或財務能力不相符。
- 172 VCE 還對 JD Cruz 的合夥人 Brabo 提交 STR，指出有充分的跡象顯示 Brabo 的帳戶涉及詐欺。申報交易包括 2017 年 9 月的 122,000 菲律賓幣的現金存款和 92,000 菲律賓幣國內匯出款項。另一家銀行實體對 Brabo 提交數起 STR，指明其在 2017 年 8 月至 9 月期間進行多筆交易（即現金存款、資金轉帳、支票存款 / 現金），總金額為 2,702 萬菲律賓幣，該銀行認為這些交易沒有合法的交易所義務、目的和經濟理由。

173 分析結果已轉發給提出請求的執法機關，供其用於情報目的並協助其調查案件。

泰國

暗網上的非法毒品走私

174 C 先生是 25 歲的加拿大公民，應美國的要求在泰國被捕。泰國公職人員證實其為 Alphabay 的管理人員，Alphabay 是一個專門從事非法商品銷售的暗網，使用虛擬貨幣（如比特幣）避免被查獲。C 先生顯然在泰國過著奢侈的生活，在當地擁有三棟住在和四輛跑車。其遭控與麻醉品散布、身分竊盜和洗錢有關。

5.04 貿易洗錢和移轉訂價

阿富汗

案例研究 1

175 阿富汗金融情報中心對與電匯詐欺相關的 11 起 STR 的分析顯示，兩貨幣服務供應商（包括貨幣兌換服務供應商）涉入不當使用國際轉帳，協助進行貿易洗錢。

176 X 集團遭查獲欲向國外移轉資金，但卻提不出充分的電匯佐證文件。從轄區 A 購買紡織品和太陽能的商業發票被標記為詐欺。金融情報中心識別的關鍵紅旗警訊指標如下：

- 商業發票的電子郵件地址與原始供應商的電子郵件地址不同，發送到發票上不實電子郵件地址的所有

驗證電子郵件，都回覆確認發票為正本。

- 不實發票從轄區 A 的相關業務中挑選業務類型、地址和聯繫方式，意圖使不實發票看似合法。
- 原始業務交易也與詐騙發票混在一起，使法遵人員難以識別。
- 發票上的手機號碼似乎與銷售代理人勾結，準備向銀行人員提供正面意見回饋。

移轉的金額與實際進口的商品之間，發現有超過 70% 的落差，發票開低於是成為證明此落差的關鍵紅旗警訊。

177 阿富汗金融情報中心於 2016 年將此案移送重大犯罪工作小組，調查過程中，兩名嫌犯（貨幣服務提供者的所有權人）試圖賄賂調查人員。反貪污司法中心初級法院宣判兩名涉嫌提供回扣的嫌犯有罪，分別判處 18 個月徒刑，其洗錢行為也正面臨起訴。

案例研究 2

178 金融情報中心自發性地向調查機構揭露貿易洗錢活動，共 11 家企業（包括貨幣服務供應商（MSP）和 FXD）涉嫌使用偽造且不充分的佐證文件將 X 美元轉移至國外，目的是購買和進口商業貨品至當地轄區。

179 根據商業銀行申報的 STR，當事人已向國外轉移 X 美元，以便購買和進口商業商品至阿富汗，但該等企業所提交的部分海關文件未經海關部門認證或認可。另外，根據 A 銀行提交的 STR，其中一個對象提議每月

向銀行人員提供回扣，以協助進行海外交易。

180 分析結果從帳戶簽名人和業務活動判定，其中部分業務經由家族關係互相有關聯，所識別的紅旗警訊指標和可疑事項如下：

- 未經法律許可提供外匯服務；金錢
- 提供偽造發票以進行 FTT；
- 所進行的多筆交易與月營業額相互抵觸；
- 提議回扣；
- 有多個公司銀行帳戶。

181 聯合工作小組完成自發性揭露的調查後，就以下指控移送檢察總署提起公訴：

- 洗錢；
- 逃漏稅；
- 偽造文書；
- 隱匿資金的非法來源；以及
- 提議回扣。

澳洲

商品發票開低

182 A 公司是廢金屬和機械的國內出口商，其客戶群位於亞洲，其國際資金移轉說明（IFTI）價值和向邊境主管機關申報的出口價值對不起來，顯示 A 公司可能涉及 TBML。在其中一個會計年度內，A 公司從亞洲訂

購客戶收到與廢金屬和機械出口相關的 IFTI，總額為 250 萬澳幣，而出口報關總價值為 310 萬澳幣。該公司使用交易融資的行為也令人懷疑，公司 A 為從歐洲進口的機械申請價值 137,500 美元的交易融資，但並未提出與購買相關的任何 IFTI 或顯示已收到產品的記錄。此外，該公司向邊境主管機關申報的實物出口價值小於向澳洲稅務局（ATO）申報的出口銷售價值，顯示該公司故意增加所主張的商品暨服務稅抵免額。

商品發票開高

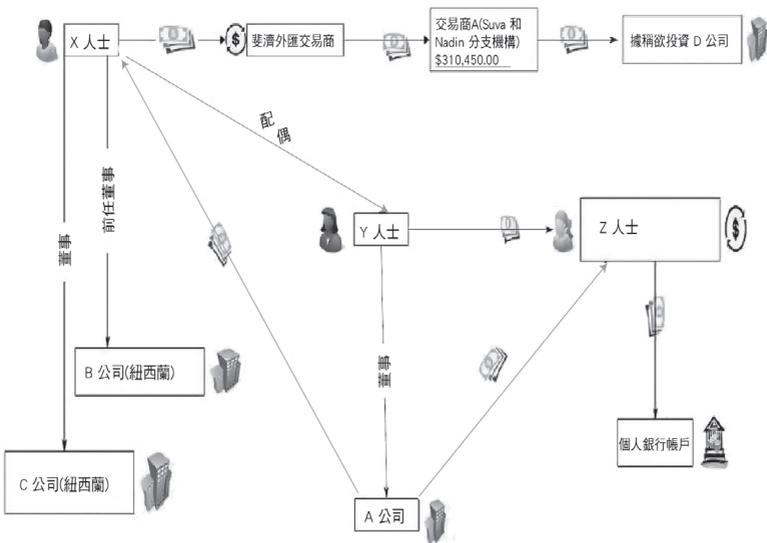
183 三間公司（A、B 和 C）組成的澳洲出口商網絡，向香港、新加坡和阿拉伯聯合大公國出口電信裝置和其他電子產品。出口和交易記錄顯示，B 公司和 C 公司申報的出口價值大致符合其向海外買家收到的 IFTI。相反地，A 公司的記錄卻有發票開高的跡象，A 公司申報的出口總值略高於 1,100 萬澳幣，但收到的資金約為 3,360 萬澳幣。大約 2,300 萬澳幣的剩餘資金（與同等的出口交易無關）已匯往海外給原始訂購客戶。

斐濟

184 斐濟金融情報中心收到一起 STR，一雙重國籍公民（斐濟和紐西蘭）X 人士涉嫌販運毒品，據稱，X 人士在 2016 年 11 月至 2017 年 11 月期間，共六次遭當地外匯交易商和銀行提交 STR。X 人士一開始是因兌換大筆紐西蘭幣而引起斐濟金融情報中心的注意。

- 185 斐濟金融情報中心進行財務檢查後，認定 X 人士在入境時未於邊界申報紐西蘭幣。外幣兌換可折合 91,640 斐濟幣，斐濟金融情報中心無法判定其最終用途。兌換貨幣前，X 人士已在 A 銀行開設一個銀行帳戶，還曾在另一家本地 B 銀行開設帳戶。
- 186 X 人士從紐西蘭向位於斐濟的 Z 人士匯出大量資金，Z 人士從 X 人士及其位於紐西蘭的配偶 Y 收到匯款。X 人士和 Y 人士同為紐西蘭 A、B 和 C 公司的董事。Z 人士還從紐西蘭的 A 公司收到匯款，Z 人士與 X 人士或 Y 人士之間沒有明顯的關係。
- 187 X 人士表示，兌換大量貨幣的原因是因為其欲在斐濟成立一家公司，D 公司後來在斐濟成立，X 人士委請他人代其進行貨幣兌換。
- 188 斐濟金融情報中心還發現，X 人士在紐西蘭有不良旅行記錄，一份案件分發報告首先傳遞給紐西蘭金融情報中心（NZFIU），由其調查嫌犯在紐西蘭涉嫌逃漏稅和洗錢的情況，同份報告而後依要求提供給斐濟過渡犯罪單位（TCU）查驗毒品相關犯罪，隨後也將 STR 傳遞給 TCU。斐濟稅務和海關總署也發布了同份報告，供其邊境進行分析：
- a) 可能犯行包括：
- 貿易洗錢行為
 - 海關相關的罪行

- 逃漏稅
- b) 指標包括：
- 在沒有任何明顯交易關係的情況下，本地和海外實體之間出現大量資金交換。
 - 向斐濟多名人士匯款
 - 未於邊界申報即進行大量貨幣兌換。



巴基斯坦

189 Alpha 銀行針對 A 先生提交 STR，A 先生經營一家獨資企業「M/SZXY」，根據負面媒體消息，嫌犯捲入一起騙局。對 STR 的分析顯示，該人投入藥品進口業務，擁有多個銀行帳戶，但發現其帳戶中的活動有異

常，其在過去幾個月中發生高流動性周轉、現金提取和國外匯款，但是，其個人稅收狀況與帳戶中金融活動的程度不符。

- 190 結果發現，嫌犯向海關報關時提交不實進口發票和其他假證件，藉此壓低進口貨物的實際交易價值，而相關資金則經由 Hawala/Hundi 匯往國外的。基於異常帳戶活動和不利的媒體新聞，情報最初與執法機關共享以採取必要措施。

泰國

- 191 財政部和國家審計委員會合作檢查了 30 多個廢金屬出口公司的不實增值稅退稅。調查發現，此案涉及國稅局的 18 名公務員（包括資深公務員），所涉金額共 41 億泰銖（約 1.5 億美元）。國家審計委員會協同特別調查部（DSI）、國家反貪腐委員會（NACC）和 AMLO 擴大調查範圍。
- 192 DSI 的調查發現，犯罪者付錢給窮人 200-500 泰銖（7-15 美元），以便借用其身分證副本並向社會安全局進行註冊。此外，犯罪者還租用偽裝成法人公司的工作場所，調查該工作場所後卻只發現一個空房間，沒有任何員工或設備。此外，有文件顯示，金屬的成本為每公斤 600 泰銖，高於市場價格，所犯的罪行牽涉出口後不實要求增值稅退稅。

5.05 地下匯兌 / 替代匯款服務 /Hawala

澳洲

- 193 執法機關接獲 AUSTRAC 轉報情資，針對兩名犯罪者經營的兩家未註冊匯款業務展開調查。執法單位根據搜索令進行搜索後，將犯罪者逮捕歸案，經過內部調查，AUSTRAC 將公司和董事移交執法單位進行刑事調查。AUSTRAC 在調查之前和調查期間積極向執法單位提供金融情報報告，著重於公司和相關實體的報告和交易活動。
- 194 2016 年 10 月，犯罪者對未註冊的匯款服務和洗錢行為表示認罪，並分別被判處 24 至 26 個月的緩刑，此外還根據執法調查結果扣押了超過 200 萬美元的資金。
- 195 請參見：「AUSTRAC 轉報協助逮捕未經註冊的匯款業者」（<http://www.austrac.gov.au/case-studies/austrac-referral-helps-catch-unregistered-remitters>），發布於 2017 年 9 月 22 日。

中華台北

案例研究 1

- 196 2013 年 3 月起，馬來西亞籍「Y」人士使用在中華台北和海外的許多帳戶來營運地下銀行系統，為在中華台北工作的印尼、泰國、越南和菲律賓的客戶提供通訊服務。Y 使用本地公司帳戶接收資金，將資金轉換為美元，再匯到外國公司的海外銀行單位（OBU）帳

戶，然後將資金移轉到不同司法管轄區的聯絡窗口帳戶中，確認金額後，聯絡窗口即依客戶需求將資金以不同幣別轉入指定帳戶。Y 收取的服務費取決於匯款金額。

- 197 2013 年 3 月至 2016 年 12 月期間，Y 經手的總金額約為新台幣 566 億元，其中賺取的交易費約為新台幣 7 億元。2017 年 4 月，台中地檢署以 Y 違反《銀行法》和《洗錢防制法》為由起訴 Y，並向法院聲請宣告沒收犯罪所得約新台幣 7 億元。

案例研究 2

- 198 「X」人士經營非法地下銀行集團，該集團利用行李箱內的衣服藏匿和運輸大量現金（每次運送新台幣 1,500 萬元）。根據調查，X 為印尼籍，在中華台北經營一家出售印尼商品的商店，其與丈夫和婆婆一起經營這家商店。除了出售印尼食品和補給品外，這家商店還私下接受請求，協助印尼勞工匯款至印尼。其在未取得適當執照的情況下賺取佣金和匯差做為報酬。迄今，該集團已賺得新台幣 800 萬元。
- 199 執法機關發起搜索，最終逮捕了 8 名嫌犯，警方在 X 隨身攜帶的 3 件行李中發現新台幣 14,545,000 元的現金，另起獲犯罪通訊、交易記錄和居留證等的證據。X 遭控違反《洗錢防制法》和《銀行法》。

中國香港

案例研究 1

- 200 2013 年 9 月至 2014 年 3 月期間，據稱有身分不明的犯罪者為三名位於中華台北的被害人提供對香港股票投資的豐厚報酬，誘使他們將 80,000 美元匯入持牌貨幣服務營運商（MSO）的本地銀行帳戶。被害人隨後與犯罪者失聯，此案通報中華台北的一個主管機關後，該主管機關於 2014 年 8 月將案件移送香港警察（HKP）進行調查。
- 201 香港警察向 MSO 的負責人查詢後發現，其客戶（後稱被告）安排將所得款項從中華台北轉移至 MSO，被告親自前往 MSO，要求將共計 91 萬美元（包括被害人的 80,000 美元）的款項匯往中國的三個帳戶，供用於其友人在 2014 年 1 月至 2014 年 4 月間在中國的建築業務。被告還從 MSO 提取 7,200 美元現金作為報酬。
- 202 被告後遭逮捕，並遭控訴洗錢罪名；2017 年 9 月，被告定罪；2017 年 10 月，法官裁定被告罪行嚴重，涉及國際要件，因此後被判處 3 年 9 個月徒刑。

案例研究 2

- 203 2013 年 11 月至 12 月間，據稱有身分不明的犯罪者為兩名位於中華台北的被害人提供對香港股票投資的豐厚報酬，誘使他們將 14,103 美元匯入本地銀行帳戶。

被害人隨後與犯罪者失聯，此案通報中華台北的一個主管機關後，該主管機關於 2014 年 8 月將案件移送香港警察進行調查。

- 204 香港警察的調查顯示，共有 74,359 美元（包括被害人的 14,103 美元）從中華台北匯入本地銀行帳戶，存款後，立即從 ATM 將 69,231 美元移轉給持照 MSO。MSO 的負責人說，其客戶（後稱被告）聲稱已存入 69,231 美元，被告親自前往 MSO，要求 MSO 將其於 2013 年 11 月至 12 月間共 10 次匯款的款項匯往中國的三個帳戶，以供進行交易業務。
- 205 被告漂白其在中華台北的一項投資騙局所獲得的 69,231 美元犯罪所得，其於 2017 年受審後被判洗錢罪名成立，被判處 1 年 3 個月徒刑。

馬來西亞

- 206 馬來西亞主管機關截獲一群非法匯款營運商的活動，這些營運商疑似在 5 年內從馬來西亞非法匯款到鄰國超過 30 億美元。據信，這些非法匯款活動是由一個聯合集團展開，該集團透過非正規的匯款網絡和以人體攜帶現金方式走私到鄰國轄區，協助將馬來西亞的資金移轉。
- 207 大部分款項被轉移到國外，以協助本地商人與外國供應商之間的交易支付，為外籍勞工進行匯款以將錢匯回其本國司法管轄區，以及將非法所得移轉到海外。

208 此案的作案手法涉以下內容：

- 外籍勞工 / 本地公司與非法匯款營運商進行交易。
- 非法匯款營運商使用轄區 C 的網路銀行設施將資金移轉給轄區 C 的收款人，透過非法匯款營運商與集團負責人之間的預備資金（pre-funding）安排實現此資金移轉。
- 從客戶收取的資金接著移轉到由該集團控制的銀行帳戶中，經由監控和金融情報分析顯示，該集團使用代理人營運部分公司和銀行帳戶。交易分析顯示，大量現金從各個存款人存入帳戶，隨後，該集團會在同一天或次日從帳戶提取現金，使帳戶中的餘額保持低位。
- 該集團隨後將這些錢從集團匯出或走私到馬來西亞，運往鄰近的轄區 S，後者是這些貨幣的轉運點。
- 來自轄區 C 的車手取走轄區 S 的款項後，將有形貨幣走私到轄區 C。
- 轄區 C 的集團存入款項，補足轄區 C 用於從馬來西亞非法匯款到轄區 C 的帳戶餘額。

209 目前正在調查該集團的洗錢和前置犯罪，包括尋求相關司法管轄區之間的司法互助。所使用的洗錢方法包括：

- 貿易洗錢行為。
- 地下銀行 / 替代匯款服務 /Hawala。
- 利用網路（網路銀行）。

- 使用代名人、家庭成員或第三方。
- 貨幣走私（包括隱匿和安全問題）。
- 換匯 / 現金轉換。
- 分散交易（洗錢）。

巴基斯坦

案例研究 1

- 210 兩家不同銀行分別對 AB 先生提交 STR，其在 A 銀行和 B 銀行的多間分行擁有大約 10 個帳戶，散布於不同城市，各自經營不同業務，包括一般訂單供應商、汽車零件、代理、乾果、麵粉和石油、煤炭和鉻鐵礦、鋼鐵廠等。
- 211 在 FMU 內部資料庫進行搜尋後，識別多起相互關聯的可疑貨幣交易報告，指明各項交易都有共同的手機號碼和營業地址。這些相互關聯的 STR 也提及另一名「CD 先生」，其先前因涉嫌在 Hawala 進行前置犯罪而將 STR 傳遞給執法機關。
- 212 提交申報的銀行要求取得有關 AB 先生交易對象的詳細資訊以作進一步分析，隨後識別其兩名交易對象 EF 先生和 GH 先生的兩起 STR，懷疑這兩人的理由，是由於其帳戶中的營業額過高，而且是與無關聯的交易對象進行交易。該銀行還收集有關這些嫌犯的市場資訊，證實這些嫌犯與 Hawala 業務有關。
- 213 該資訊已與執法機關和主管機關共享，供其採取必要

的措施。

案例研究 2

- 214 Z 先生在 ABC 銀行持有一個名為「XYZ 企業」的獨資企業帳戶，嫌犯在 XYZ 企業帳戶進行的交易量大且性質不一致，高價值資金以現金和轉帳記入，大部分轉入巴基斯坦不同城市無關的交易對象。
- 215 嫌犯還在多個銀行開立多個帳戶，並與這些帳戶中無關的交易對象進行高價值交易。嫌犯帳戶的交易對象從事不同業務，例如水果業務、穀物交易商、零件交易商、財產交易商、電腦和硬體交易商、建築業務和一般交易商。檢查 Z 先生的納稅狀況時，發現嫌犯並未註冊國家稅務編號（NTN）。考慮到嫌犯及其交易對象業務之間的差異，懷疑其從事 Hawala/Hundi 業務，因此將本案以涉嫌 Hawala/Hundi 罪行移交執法機關。

泰國

- 216 中國向 AMLO（泰國金融情報中心）提出請求，希望調查並搜集有關 38 歲中國公民 Z 先生及其同伙的證據，其涉嫌誘使 30,000 名中國人投資一項計畫，並承諾在當年歸還高達 10 億泰銖的價金。Z 先生有意透過購買泰國的不動產來洗錢，其同夥 B 先生建議其透過地下匯兌系統將這筆錢從中國轉移到泰國。
- 217 要轉移這筆現金的價值，但沒有到目的地司法管轄區

的實際貨幣轉移，Z 先生向 B 先生發送有限的資訊，以完成電子轉帳請求，其中包括泰國的收款人帳號和人民幣金額，然後 B 先生將與擁有曼谷不動產經紀公司的 P 先生聯繫。P 先生透過微信應用程式或 Gmail 告知 B 先生中國的受款人帳號清單以及不同帳戶中的金額。之後，B 先生會將此資訊發送給 Z 先生的同夥，以將資金轉入中國的這些帳號。透過地下銀行進行的交易總計為 1.09 億元人民幣。

- 218 在中國完成交易後，Z 先生的同夥將轉帳證明發送給 B 先生，B 先生再將結果發送給 P 先生，後者立即通知其在泰國的地下匯兌網絡，以向 Z 先生及其同夥在泰國的帳號移轉泰銖計價的資金。不同帳戶中的每筆交易金額都不超過 100 萬泰銖。
- 219 此過程花了一到兩天，P 先生藉由匯差和營運成本（100 萬泰銖的百分之一）獲利。

5.06 使用網路（加密、存取 ID、國際銀行等）

孟加拉

- 220 J 先生是住在利比亞的孟加拉籍外籍人士，他來到孟加拉開設兩個銀行帳戶，一個以自身名義開戶，另一個以其妻名字（K 女士）在 B 銀行開戶。幾天後，大量金錢從該轄區的不同地方透過線上轉帳方式被轉入 J 先生的帳戶。某天，某人來到 B 銀行的 F 分行將錢

存入 J 先生的帳戶，銀行人員發現存錢人面色蒼白，因此問他存錢目的，經詢問，發現此人在利比亞工作的兄弟最近被綁架，綁架者要求支付贖金，因此，他必須以將錢存入的方式支付贖金，才能釋放被綁架的兄弟。獲悉此事後，銀行針對 J 先生及其妻 K 女士的帳戶提交 STR。

221 孟加拉金融情報中心（BFIU）分析員收集了有關 J 先生和其妻 K 女士的相關文件和資訊，經過分析後發現巨額存款（一次存入 10 萬至 15 萬孟加拉幣），分別從不同分行轉入 J 先生和其妻的帳戶。根據帳戶對帳單中提供的存款人資訊，BFIU 識別存款人並收集相關資訊，得知所有存入這些帳戶的錢都是贖金。根據被害人的陳述，BFIU 通知其他銀行帳戶（A、S 和 M 銀行的另外三個帳戶），其中被害人的親屬依指示將贖金存入這些帳戶。收集這些銀行帳戶的詳細資訊後，BFIU 獲得有關帳戶持有人的更多資訊，瞭解到這些帳戶被用於向在利比亞被綁架的人的親戚勒索贖金，此外，也發現其中一個帳戶持有人是 J 先生的姐夫，另一帳戶持有人則是其員工。

222 BFIU 凍結這五個帳戶，阻止資金流動，BFIU 根據調查結果編寫了一份分析報告，緊急傳遞給執法機關進行進一步的調查和法律程序，執法機關立即逮捕了該集團，對他們提出洗錢指控。

斐濟

223 本地商業銀行對 X 人士提交了 STR，X 人士經識別可能是網路銀行詐欺車手，X 人士的銀行帳戶顯示有四筆交易，該帳戶收到總計 2,900 的金額後，隨即進行三次提款，總計 2,890 斐濟幣，如下：

- 2017 年 7 月 28 日，X 人士從 A 人士的帳戶收到 1,000 斐濟幣的信用轉帳。
- 2017 年 7 月 31 日，X 人士從 A 人士帳戶收到兩筆信用轉帳，總計 1,600 斐濟幣。
- 2017 年 7 月 31 日，X 人士的銀行帳戶從 B 人士的銀行帳戶收到信用轉帳，總計 300 斐濟幣。
- 2017 年 7 月 31 日，X 人士從三個不同地點的當地 ATM 提領三筆現金，總計 2,890 斐濟幣。

224 相關資金轉移是以詐欺手段從 A 人士和 B 人士的銀行帳戶進行，其並不知道這些交易的詳情。指標包括：

- 對象對交易不知情
- 被害人與被告之間沒有關係

中國澳門

225 2012 年 4 月至 2013 年 3 月期間，一名香港居民竊取了至少 6 名香港被害人的重要個人資料，偽造他們的簽名，並非法移轉總計約 772 萬港幣的銀行存款。證據顯示，相關贓款已流入澳門，因此，香港警方要求司法警察在 2013 年底經由國際刑警組織追蹤調查。

- 226 司法警察經過深入調查後，發現涉案男子已將贓款轉移至數個銀行帳戶，並透過處置（placement）和分層化（layering）將部分非法資金移轉至澳門。司法警察識別涉案男子的同時，也發現其已於 2014 年 1 月被香港警方逮捕，其被香港法院判處 52 個月徒刑，服刑結束後於 2016 年底獲釋。
- 227 由於涉案男子在澳門進行洗錢活動，司法警察於 2017 年 9 月 21 日在男子抵達外港客運碼頭時再次逮捕他，同時還扣押現金 24 萬港幣及價值 20 萬港幣的手錶。該男子坦誠犯罪，被司法警察移交公共檢察院起訴。

菲律賓

- 228 設在菲律賓作為機房的實體涉嫌參與大規模投資詐欺，騙局手法如下：機房使用「Magic Jack」裝置，可插入個人電腦 USB 連接埠，「Magic Jack」裝置分配了美國主要城市的對應區號，包括芝加哥、紐約、聖地牙哥和邁阿密。這些裝置可撥打居住在美國的年長者，讓被害人以為來電者位於美國，但實際上他們都位於菲律賓。
- 229 此外，機房營運商在美國有合作夥伴，特別是來自加州聖地牙哥和佛羅里達州哈倫代爾的同夥，其向被害人郵寄詐欺性行銷資料和客戶對帳單。2011 年 2 月至 2013 年 8 月期間，至少 40 位美國居民受害於該詐騙計畫，累積資金超過 300 萬美元。被害人依據指示開

立個人支票，再由聯邦快遞取貨；支票隨後轉發給菲律賓 Muntinlupa 市的 ADV。AMLCS 能夠驗證疑似遭存入資金的特定帳戶。

泰國

230 泰國協助美國偵查使用惡意軟體侵入許多轄區銀行帳戶的問題，泰國皇家警察總署就此事逮捕了兩人，並扣押嫌疑犯的 56 個銀行帳戶。AMLO 協同 DSI 對洗錢提出刑事訴訟。目前此事由檢察總署（OAG）起訴洗錢被告，並由法院審理中。

5.07 使用新付款方式 / 系統

孟加拉

231 根據投訴，BFIU 分析師搜尋一名低階警官 X 人士的銀行帳戶，結果發現，X 在 6 家銀行（A、B、C、D、E、F）持有 30 個帳戶（4 個儲蓄帳戶、1 個活期帳戶、1 個貸款帳戶和 24 個存款計畫），另在非銀行金融機構（NBF1）持有帳戶 G。Y 女士（X 先生的配偶）在 B 銀行有兩個帳戶（1 個儲蓄帳戶、1 個存款計畫），在 G 銀行則有 1 個貸款帳戶。這對夫妻在 F 銀行也有兩個聯名帳戶（儲蓄和貸款）。

232 經過分析，發現經常有少量現金存款（總計 2,810 萬孟加拉幣）會存入 X 先生和 Y 女士（在 A、B、C、E、F 銀行）的儲蓄或活期帳戶，而後再頻繁經由 ATM 提

款，也會從這些帳戶進行銷售點轉帳（POS）付款。如果這些帳戶有大量餘額，資金就會被轉移到同一家銀行的開放固定存款收據（FDR）、存款計畫或定存收據（TDR）帳戶。X 先生選用現金存款在 A 銀行開設一個存款計畫帳戶，在 B 銀行開設兩個 TDR 帳戶以進行現金存款（109 萬孟加拉幣）。

- 233 X 將存款計畫 /FDR 帳戶的金額新增到 A 銀行中的儲蓄帳戶。他和妻子分別向非銀行金融機構（NBFI）‘G’ 貸款 150 萬和 250 萬孟加拉幣，用以購買公寓，並將此金額轉入 X 先生在 A 銀行的儲蓄帳戶。X 先生隨後會簽發支票（628 萬孟加拉幣）給予 Q 和 R 先生，以在 D 銀行開立兩個 FDR 帳戶，並提領來自 A 銀行的現金（270 萬孟加拉幣），此外也透過電子資金轉移（EFT）在 NBFI ‘H’ 開設兩個 TDR 帳戶（110 萬孟加拉幣）。
- 234 X 先生和 Y 女士共同從 F 銀行貸款 300 萬孟加拉幣，作為公寓貸款，並使用 Y 女士在 NBFI ‘G’ 中存款償還貸款，X 先生從其在 A 銀行的儲蓄帳戶轉帳 50 萬孟加拉幣、從 B 銀行的儲蓄帳戶轉帳 64 萬孟加拉幣、從 NBFI ‘G’ 的 TDR 帳戶兌現 31 萬孟加拉幣，來償還自己的貸款。
- 235 X 以自身名義在 B 銀行購買了兩張 200 萬孟加拉幣的儲蓄單，另以其妻的名義購買四張 350 萬孟加拉幣的

儲蓄單。Y 女士自己也以自身名義買了一張 100 萬孟加拉幣的儲蓄單。

- 236 X 提及自己的職業和收入來源是服務業，其配偶則是家庭主婦，但兩人帳戶中的複雜交易與各自職業並不相符。BFIU 分析師懷疑貪污和行賄收益可能已轉入其帳戶。此案已分發給執法機關進行進一步調查，執法機關決定對涉嫌人士提起訴訟。

5.08 漂白稅收犯罪的收益

斐濟

案例研究 1

- 237 斐濟金融情報中心收到有關 X 夫婦的 STR，原因是其收到大筆匯款，並在其企業和個人銀行帳戶之間進行轉帳。斐濟金融情報中心發現 X 先生收到的匯款交易額超過 100 萬斐濟幣，X 女士收到的匯款額為 300,000 斐濟幣，所有匯款均來自中國。
- 238 X 先生是斐濟 UVWLtd 和 XYZLtd 兩家公司的董事，X 女士是斐濟 RSTLtd 公司的董事。進一步查驗後，發現 X 夫婦以及這三家公司均未提交任何納稅申報表。X 先生擁有兩個個人銀行帳戶，其中一個帳戶餘額超過 100 萬斐濟幣；X 女士擁有一個個人銀行帳戶，餘額約為 30 萬斐濟幣。一份報告已傳遞給稅務機關，認為可能有稅收犯罪問題。指標包括：

- 其個人帳戶有巨額餘款。
- 未向稅務機關提交納稅申報表。
- 收到大量匯入款項。

案例研究 2

239 斐濟金融情報中心收到有關 A 人士的 STR，據稱該人將商業資金轉入個人銀行帳戶。A 人士是三個大型製造和硬體公司 X、Y 和 Z 公司的董事，斐濟金融情報中心進行財務檢查後，發現 A 人士在個人銀行帳戶中收到大量現金和支票存款。已確定大多數支票是來自屬於 X 公司的商業帳戶。

240 斐濟金融情報中心進一步確定，平時少有大量存款存入 X 公司和 Y 公司的銀行帳戶，這與他們一般業務活動不符。斐濟金融情報中心進行進一步查驗，注意到 X 公司和 Y 公司有未繳稅款，於是針對可能涉及稅法和洗錢犯罪向稅務機關傳遞一份報告。指標包括：

- 未向稅務機關提交納稅申報表。
- 將業務資金存入個人帳戶

案例研究 3

241 X 公司是一家汽車經銷商，2017 年為避稅而低報銷售收入，因而被課徵約 800 萬斐濟幣的稅款和罰款，X 公司一直超時處理其銷售記錄。該資訊是由洩密者提供的，當稅務局進行詳細調查時，發現該公司的納稅申報表和銀行帳戶中申報的銷售額顯示重大異常情況。

X 公司的董事 X 先生似乎也參與其他業務，擁有的投資物業也有銷售收入低報的問題。X 先生和 X 公司因逃漏稅被起訴並受罰。指標包括：

- 營業額可觀，但出於稅收目的，未向稅務機關如實申報適當收入。

案例研究 4

242 稅務機關對六家公司進行調查，發現涉嫌逃漏稅，金額超過 1500 萬斐濟幣，這些公司從事進口交易，據稱為低估其商品價值以逃避關稅，據稱這些公司還低估自己的所得以逃避稅收。

243 此外，還因上述犯罪而受調查的三家公司，遭罰款 2500 萬斐濟幣，後已全額繳納稅款和罰款。

a) 可能犯行包括：

- 逃漏稅；和
- 逃避關稅。

b) 指標包括：

- 營業額可觀，但出於稅收目的，未向稅務機關如實申報適當收入

巴基斯坦

244 根據開戶表格，HN 先生在巴基斯坦農村地區擁有農業用地，並在伊斯蘭堡從事建築業務，根據申報資訊，其收入來源是農業用地和建築業。

245 其帳戶收到名為 EG 的實體之國外匯款，該實體在國

外司法管轄區註冊，從事一般交易，這筆交易引起銀行懷疑。由於帳戶活動與 HN 先生的業務性質不符，因此就 HN 先生的所有帳戶向金融監控中心（FMU）提交可疑交易申報。

246 FMU 分析該帳戶並搜尋公共領域資料後，發現該實體 -EG（匯款人）的所有權人是 HN 先生本人，且 EG 的主要業務是進出口和貿易。經審查其帳戶對帳單後，發現自 2015 年 7 月至 2016 年 2 月，期間 HN 先生的個人帳戶曾 10 次收到總計 68,880 美元的款項，以及 3 次總計 115,664.90 歐元的匯入款項。

247 調查發現，HN 先生的稅務狀態為活躍，但截至 2015 年底，當年僅繳納微薄稅款。由於 HN 先生繳納的稅金與帳戶對帳單所反映的營業額不相符，因此將此事呈報稅務機關。

248 收到 FMU 的情報通報後，稅務機關對此案展開調查，HN 先生聲稱其為 EG 實體的合夥人，該實體在國外司法管轄區中註冊為自由區實體，並稱在帳戶中收到的匯款是他從轉介業務中獲得的利潤分紅，後將其用於在巴基斯坦購買不動產。

249 根據 2001 年《所得稅條例》第 101（16）條，所有外國所得均須如實申報，然此案例並未遵守此條規定，因此，2013 年至 2016 年納稅年度的匯入外幣金額，應列為 HN 先生的股利所得，連同罰款和罰金，其應

補繳共 1,241.9 萬盧比（約合 115,000 美元）。

- 250 詢問時得出的結論是，納稅人以為因為匯款是來自阿拉伯聯合大公國的業務營收，因此透過銀行通路收到匯款可免稅。

5.09 不動產（包括不動產仲介的角色）

中華台北

- 251 X 是 K 公司和其他公司的董事長，這些公司經營不善，狀況不佳。為欺騙民眾投資 K 公司，X 偽造合約和採購訂單，假裝 K 公司處於良好的營運狀態，X 還以年利率 24% ~ 54% 的承諾吸引投資人。
- 252 為擴大業務規模，X 以高額佣金僱用 H 和其他 8 名人員來協助吸引投資人。2013 年 4 月至 2017 年 3 月期間，X 使用 K 公司、其他公司和員工的帳戶接收投資，總投資額超過新台幣 149 億元。為隱匿犯罪所得，X 以其員工和親戚的名義購買不動產、汽車和高價值產品；2017 年 3 月，X 指示其員工從其帳戶中提領約新台幣 3,000 萬元現金給他。
- 253 調查過程中沒收了新台幣 370 萬元現金。執法單位調查完畢後，全案於 2017 年 8 月依違反《銀行法》、《洗錢防制法》以及偽造文書和詐欺罪移送嘉義地檢署提起公訴。

斐濟

- 254 斐濟金融情報中心收到當地執法機關請求提供資訊，執法機關表示有意對 P 人士和 E 公司建檔，因為發現他們可能因貪污行為收到無法解釋的財富。
- 255 斐濟金融情報中心發現，P 人士於 2010 年以外籍勞工的身分進入斐濟，而後一直在政府機關工作。P 受僱於政府時成立了 E 公司和 F 公司，E 公司是一家不動產開發公司。斐濟金融情報中心發現 P 人士、E 公司和 F 公司共擁有 16 個銀行帳戶，而 P 人和 E 公司為 10 個物業的所有權人。
- 256 P 人士疑似利用其在政府部門的僱傭關係收受特定回扣和賄賂，P 人士再透過 E 公司購買物業以掩飾這些非法資金。

馬來西亞

- 257 A 先生曾在其中一州的一家公共事業機構擔任董事，負責價值超過 10 億美元的基礎設施專案開發，A 先生濫用權力將專案授予與他有關係的特定承包商。相關交易的回扣以現金和其他誘因的方式提供給 A 先生，整起計畫由 A 與其妻和主管共謀犯案。
- 258 回扣大部分是現金或其他形式的奢侈品，現金被存放在他的房屋和辦公室內不同處，或用以購買物業、汽車或奢侈品。
- 259 調查過程中，發現除土地、豪華汽車、珠寶和配飾外，

還查獲涉案人士身上有約 4,700 萬美元的現金，隨即扣押這些現金。

260 A 先生、其妻和兩名資深公職人員遭控犯下洗錢罪，目前已受審，扣押的部分資金則依民事沒收規定進行扣押。

261 已向相關司法管轄區尋求司法互助，旨在追討流入海外銀行帳戶的可疑非法所得。使用的洗錢方法包括：

- 使用現金；
- 購買有價值的資產；
- 使用代名人和第三方；以及
- 電匯 / 使用外國銀行帳戶。

巴基斯坦

262 X 先生是政府承包商，據媒體報導，嫌犯涉嫌經由不同住房騙局，從無辜者手中竊取價值數百萬盧比的財產。嫌犯在不同銀行擁有多個個人和商業帳戶，其帳戶的平均每月營業額以及借貸總金額非常高，據觀察，最近三年中，嫌犯從不同銀行的不同帳戶移轉資金。

263 嫌犯使用不同的交易方式（例如現金和清算），經由其帳戶移轉高額資金。據觀察，以支票存入的資金隨後立刻以現金提領一空。嫌犯還在採用分散交易的方式，意圖避免 CTR 的最低申報門檻。此外，審查嫌犯美元帳戶的帳戶明細（SOA）時，發現以現金存入

的資金，很快就以外國電彙和外國即期匯票的形式，移轉或開立給多個不相關人士。此外，嫌犯將高價值的資金轉用於外國不動產專案，目的是在該轄區內購買物業。

264 此案因涉嫌詐欺和挪用公款罪而移送執法機關。

新加坡

265 2017 年 11 月，一名不動產仲介和一名產權轉讓律師遭控未能向主管機關通報可疑財產交易，案主是涉嫌在中國因犯金融詐欺罪而遭定罪的中國女商人。

266 調查顯示，不動產仲介和產權轉讓律師應可合理懷疑中國女商人在聖淘沙灣購買物業時，使用的超過 500 萬星幣可能是其犯罪所得。許多國際和本地媒體大肆報導這名中國女商人因參與中國其中一起最大的龐氏騙局而遭逮捕。儘管客戶申報不利消息，但兩人仍未就上述私有財產購買提交任何疑似洗錢或資恐交易報告。

267 不動產仲介和產權轉讓律師分別於 2018 年 4 月和 2018 年 6 月遭定罪併科罰款 10,000 星幣。

泰國

268 一名資深警官 C 和其同夥犯下濫用職權、非法賭博業務等罪行，並從想要購買職位的警察收受 3-5 百萬泰銖的賄賂，警官更要求警察每月支付 10,000-200 萬泰銖的金額。2011-2014 年期間，C 警官更每月從石油

走私集團收賄，金額高達 2-5 百萬泰銖。泰國皇家警察總署、稅務局、NACC、陸軍和 AMLO 對涉及該網絡的 30 多人展開金融調查和分析。

269 調查發現，犯罪所得用於購買 111 項土地、汽車、古董、銀行存款等以進行洗錢，價值總計約 5.6 億泰銖（1,750 萬美元）。

5.10 人口販運和人員偷渡關聯

斐濟

270 2017 年 3 月，斐濟金融情報中心收到斐濟警察部隊請求提供已定罪的重罪者 A 先生的資訊。A 先生是斐濟人，居住在紐西蘭，於 2016 年 12 月在紐西蘭被判販運人口罪。斐濟警察部隊的請求提供 A 先生子女的財務背景查核資料，即 2007 年 9 月 13 日出生的女兒 S 和 2014 年 6 月 17 日出生的兒子 X。當時兩位兒童分別為 10 歲和 3 歲，視同未成年人，但進一步查驗後，證實其在當地一家銀行開設了銀行帳戶。銀行支票確認，在兒子 X（3 歲）的銀行帳戶中總計發生 13,900 斐濟幣的存款交易和 13,000 斐濟幣的提款交易。

271 此外，銀行支票還確認，在女兒 S（10 歲）的銀行帳戶中總計發生 38,268 斐濟幣的存款交易和 37,000 斐濟幣的提款交易。A 先生顯然一直利用其子女的銀行帳戶進行疑似洗錢或資恐的交易。

272 斐濟金融情報中心向斐濟警察部隊發布一份報告，協助其對所謂的銀行帳戶受益人進行調查。指標包括：

- 利用未成年人帳戶進行高額存款和提款交易。

日本

案例研究 1

273 一名從事情色交易業務男子從一家成人商店以銀行轉帳的方式收取總計 180 萬日圓的現金作為佣金，其因違反《組織犯罪懲治法》（收受犯罪所得）而遭逮捕。

案例研究 2

274 嫌犯在其農場僱用外國勞工負責農務，然後滯留這些外國勞工，即使居留期限屆期也不讓勞工離開，並剝削其在農場或其他地方繼續勞動。（該行為構成了促進非法勞動的刑事罪行）。嫌犯經由促進非法勞動而獲得可觀數量的農作（構成本案的犯罪所得），接著以不實名義將農作出售給善意第三方，藉此掩飾農作的處置。

275 此案中，嫌犯被判處有期徒刑併科罰款，此外還沒收因犯罪所得和財產所獲得的金錢索償，共計約 400 萬日圓（36,500 美元）。

紐西蘭

276 2016 年 9 月，高等法院裁定 46 歲的 F.A 先生犯有 15 項將斐濟勞工販運到紐西蘭的罪名，其中一項不實承諾是每週採摘水果的薪資為 900 紐元。F.A 先生向勞

工收取高昂費用，在勞工抵達時剝削他們，迫使勞工非法勞動，甚至居住在人滿為患的環境中，短付薪資，更威脅勞工如果遭到投訴就會將其驅逐出境。F.A 先生還因協助和教唆他人非法進入或居住在轄區內等 16 項罪名而遭定罪，其對剝削罪認罪，包括未能向勞工支付最低薪資或假日薪資，以及協助和教唆勞工違反簽證規定。F.A 先生是紐西蘭第一個因販運人口遭定罪的嫌犯，最後被判入獄 9 年半。

巴基斯坦

- 277 A 先生被列入 FIA 高度通緝的人口販子名單，該嫌犯自 2006 年以來持續從事人口販運活動，FIA 在 2006 年 1 月將他逮捕，但當時沒有羈押。嫌犯的名字更列入 World Check 資料庫中，各新聞報導也都提及該人是其中一名頭號通緝的人口販子。
- 278 嫌犯在 ABC 銀行、DEF 銀行和 GHI 銀行等各個分行開設帳戶，其中有巴基斯坦盧比和歐元帳戶，此外，還發現嫌犯持有獨資企業帳戶。
- 279 B 女士是嫌犯的其中一個主要交易對象，因使用個人帳戶進行商業交易而遭通報 FMU 違規情況。
- 280 A 先生和 B 女士因涉嫌涉入人口販運，因此將其帳戶詳細資訊通報執法機關。

泰國

案例研究 1

- 281 一人口販運網絡經由商業銀行進行匯入匯出款項，嫌犯及其代孕公司的同夥分別以各自名義開立 5 個銀行帳戶，帳戶類型包括儲蓄帳戶、固定帳戶和外幣帳戶。
- 282 該網絡將資金轉入中華台北的銀行帳戶以向泰國經理支付薪資，在泰國的支出也都是以現金支付。
- 283 員工機票和驗孕的醫師診療費，都由中華台北銀行發行的信用卡支付，代孕婦女的薪資會從國外轉移到員工的個人帳戶，其他員工的薪資則在公司以現金支付。

案例研究 2

- 284 泰國皇家警察總署人口販運小組（RTP）對將非法移民偷渡到泰國的案件展開調查，並於搜查車輛之後發現兩名嫌犯欲將 98 名非法移民運送到該轄區內。RTP 在進行金融調查時尋求 AMLO 的協助，期望藉助 AMLA 擁有的權力。
- 285 由於 RTP 和 AMLO 之間密切合作並運用其金融調查技能，加上銀行積極配合，主管機關得以查獲龐大的犯罪網絡，其中涉入走私、融資和洗錢活動。透過銀行對帳單和電匯明細，AMLO 利用被捕嫌犯的財務交易追溯到其他關鍵嫌犯，並發現想利用同夥和家庭成員的銀行帳戶進行金融交易。對嫌犯的同夥和家庭成員進行廣泛的金融調查後，最終成功追溯到主要犯罪者的犯罪所得。拍到嫌犯提領和存入現金的監視攝影記錄、電話記錄、過往人口販運案件，加上銀行大力

給予援助，成功將調查範圍擴大到更大的網絡。

286 大約 70% 的調查都以金融情報為依據。RTP 和 AMLO 之間的聯合金融調查發現有兩個主要帳戶，一個是犯罪者的姐妹，另一個是合夥人，這兩帳戶的營業額非常可觀，其中有 3.8 億泰銖（約合 1,350 萬美元）。上述帳戶下的相關交易都是發生在邊境地區（例如，Padang Besar、Sungai Kolok、Sadao 和 Hatyai）的資金移轉，這相當不尋常。銀行已提交 STR，表示懷疑交易與客戶的個人資料不符，最後，主管機關找出犯罪集團的主謀，並識別出涉案的高階公職人員和其他人。

5.11 使用代名人、信託、家庭成員或第三方

中國香港

案例研究 1

287 在 2007 年至 2011 年之間，一位女性不動產仲介向無辜者作不實陳述，稱一家投資公司將收購多棟老舊舊物並重建，該仲介要求投資人提前付款以預購建物，以便轉售給投資公司獲取利潤。投資人將款項匯付至物業代理人指定的銀行帳戶，包括其男友在香港的銀行帳戶，總計 8,500 萬港幣（約合 1,090 萬美元），但後來部分地主並未收到租金付款時，投資人才發現這是不實的收購消息，並於 2011 年 11 月通報香港警察。

- 288 香港警察對 8,500 萬港幣的犯罪所得進行金流分析後發現，被告已兌現約兩千萬港幣（約合 260 萬美元）。2017 年 7 月，被告認罪，裁定 7 項洗錢罪名，並判處 42 個月徒刑。

案例研究 2

- 289 從一起肅貪調查中發現，被告的未婚夫是一所國際學校的助理招生人員，其向入學學生的父母尋求捐款。被告的未婚妻作不實陳述，聲稱被告是學校的資深主任，如果希望孩子能優先入學，父母須捐款，學童父母因此支付了 210 萬港幣。
- 290 2017 年 5 月裁定被告犯洗錢罪，並判處 24 個月監禁，被告的未婚夫亦裁定犯詐欺罪，被判入獄 34 個月。

巴基斯坦

- 291 多起 STR/CTR 報告中提及四兄弟 A、B、C 和 D，其中 A、B 和 C 先生是知名商人，經營 XYZ 公司，而 D 先生非本地居民。這組家庭成員從事貨幣兌換交易，透過分散交易和利用不同兌換公司，故意規避巴基斯坦國家銀行規定一天內購買外幣的門檻。四兄弟在不同銀行持有多個本地貨幣和外幣帳戶，採用特殊的交易方式，即從不同銀行的 PKR 帳戶中提領資金，再分批從公開市場購買美元，然後將錢存入同一家銀行的外幣帳戶，最後將資金從轄區內匯出到他們的個人帳戶。

- 292 此外，還注意到，較年長的 A 和 B 先生將大量資金贈予非本地居民的胞弟 D 先生，此外，根據家庭成員的納稅記錄，儘管帳戶營業額很高，但並沒有依規定繳納所得稅。
- 293 此情報已與執法機關和主管機關 SBP 共享，供其採取適當的行動。

泰國

- 294 泰國主管機關調查一名販毒者和位於泰國 / 緬甸邊境附近的一家大型毒品生產工廠，主管機關發現，被告付錢給山上部落的居民，由居民將毒品運送給最終顧客，其中一名顧客被捕後認罪。隨後對被告及其情婦進行調查，發現被告已將錢轉給了情婦。

5.12 賭博活動（賭場、賽馬、網路賭博等）

日本

- 295 Boryokudan（日本暴力團體）一名資深成員從賭場經理那裡取得 90,000 日圓現金作為保護費，此成員曉得這筆錢來自慣性賭博的犯罪所得，其因違反《組織犯罪懲治法》（收受犯罪所得）而遭逮捕。

泰國

- 296 AMLO 從一家銀行接獲一起 STR，發現 Z 先生的金融交易額約為 10 億泰銖，但其每月收入不足 10,000 泰銖。Z 先生將總計 4,500 萬泰銖的資金移轉到 M 先

生的銀行帳戶，且這比交易企圖規避申報義務。調查發現 Z 先生是線上博彩網站的所有權人或受益人。檢察官指控 Y 先生、D 女士和 L 女士犯有《賭博法》規定之罪行，法院下令判處監禁和沒收財產。在法院訴訟程序期間進一步發現，有關賭博玩家銀行帳戶和網站代理人銀行帳戶之間資金移轉的更多資訊。偵訊官針對 Z 先生及其 10 名同夥安排線上博彩（足球博彩）提交訴狀，主管機關人員檢查相關人員和犯罪者的財務記錄後，發現財務記錄和 STR 之間存在關聯。

- 297 此外還發現 Z 先生及其同夥前往監獄探視 D 女士和 L 女士。主管機關人員審問線上博彩網站的管理員後，確認 Z 先生及其同夥是網站所有權人，其利用非法所得在股票市場上購買資產、投資和證券，並購買巨額的人壽保險。

5.13 混合（商業投資）和投資詐欺

汶萊

- 298 X 因在 2015 年 2 月至 2016 年 10 月期間向多人提供不實投資騙局，而遭控犯有 20 項洗錢罪和 17 項詐欺罪，皇家汶萊皇家警察商業犯罪調查部發現 X 欺騙多名被害人，共計詐騙 147,581 美元。
- 299 一起事件中，X 在當地美食廣場遇到一名被害人，其當場向被害人宣傳，只要支付最低金額 500 美元，就

能夠終其一生每月獲得 3000 美元的投資收益，被害人立刻就加入這個不實的投資計畫並向 X 支付現金，接著，被害人被告知自己支付的款項低於規定投資額，於是不久後又與 X 會面，交出兩個金手鐲和三個金戒指以補足不足額的投資。X 告知被害人，這些物品估值為 600 美元，並向被害人保證其可享有終生每月 6,000 美元的利潤。

300 另一起事件中，X 和另一人在一家餐館遇到另一名被害人，其向被害人宣稱，只要支付 6,350 美元即可成為投資計畫的正式成員，他們告訴被害人，加入後即可獲得賓士轎車 S280、20 萬美元現金、終生享有每月 60,000 美元現金、價值 40 萬美元的房屋、勞力士手錶、進行「朝聖之旅」的旅遊獎勵，還有一張環球 VIP 卡，據說可在全球任一地點的任何 ATM 提領高達 200,000 美元的現金，此後 15 年內還可每月拿到 3,000 美元現金。

301 其他事件中，犯罪者則向被害人推廣一個名為「Dana Pelaburan Amal Jariah」（慈善投資基金）的慈善計畫。

302 犯罪者大多都是透過私人朋友、X 的前同夥或另一人的面對面網絡與被害人取得聯繫。調查結果發現，X 已透過一家知名匯款服務供應商將資金匯往外國轄區給另一個人。X 於 2017 年 4 月 8 日遭起訴，後因洗

錢罪被判處兩年徒刑，並因詐欺罪判處三年徒刑。

中華台北

- 303 X、Y 和 Z 分別是 W 公司的董事長、監察人和董事，2015 年 11 月至 2016 年 3 月間，為尋求犯罪所得並增加股權，X 安排 W 公司向三人所持有的 S 公司和其他 3 家公司購買模具和設備。這些並非必要產品，對 W 公司而言的經濟利益頗低，W 公司於是向 S 公司和其他三家公司支付約新台幣 4 億元。這些資金隨後在 X 的指示下轉移到 F 公司和其他兩家公司的帳戶中，X 從上述巨額款項中配置了新台幣 3 億元，並向放款人借貸新台幣 3 億元，用以購買 W 公司的新台幣 6 億元增資股份，其他資金則用於從其他投資人購買股票。
- 304 新購入的股票分別為 X、Y 和 Z、F 公司和其他兩家公司等，接著這些股份被轉移給 H 公司和 X 所控制的另外三家公司，剩餘資金則由 X 作個人用途。2016 年 6 月，X 使用相同手法使 W 公司向 X 所控制的公司支付約新台幣 5 億元，以購買無用的模具和設備，隨後指示一名員工將付款轉移到 F 公司和其他兩個公司的帳戶中。其他資金則用於從其他投資人購買 W 公司的股票。
- 305 X 從 W 公司挪用的資金被用於購買和增持其在 W 公司的股份。W 公司共籌集新台幣 6 億元的新資金，但

由於 X 的行為致使 W 公司無法獲得足夠的資金，因而蒙受巨大損失。

- 306 為償還 2017 年 1 月到期的新台幣 3 億元貸款，X 安排由 X 控股的 H 公司籌集新台幣 3 億元，然後安排 W 公司及其子公司分別認購新台幣 2.55 億元和 4,500 萬。資金已於 2017 年 1 月轉入 H 公司的帳戶，X 並指示員工將資金作為還款轉移到放款人指定的帳戶中。
- 307 執法單位調查完畢後，全案於 2017 年 9 月依違反《證券交易法》、《洗錢防制法》移送桃園地檢署提起公訴。

馬來西亞

- 308 馬來西亞主管機關針對聯合集團非法和詐欺性投資計畫（稱為「資金盤」）協調展開一場聯合調查，這些團體持續在短期內提供高報酬，藉此吸引國內外民眾參與財務計畫。
- 309 這類計畫中，投資的資金會用於購買可兌換積分的「虛擬硬幣」，30 天後「虛擬硬幣」的價值將增加三倍，同時會根據波動的單價加上所獲得獎勵積分的數量進一步成長。稍後，投資人可在線上市場出售「虛擬硬幣」，以換取現金或向合作商家購買商品和服務。
- 310 聯合調查聚焦於提供金字塔騙局和非法電子貨幣業務相關規定的違反行為，調查過程中，共凍結超過 5,000 萬美元的銀行帳戶和其他資產。
- 311 調查過程中，發現經由該計畫獲得的犯罪所得，被用

於支付律師等專業服務和購買物業，部分作國內和國際轉帳至第三方帳戶，但都沒有明確的經濟目的。調查人員還發現犯罪所得與不動產開發的商業投資收益混合在一起。

312 對聯合集團洗錢和前置犯罪的調查正在進行中。使用的洗錢方法包括：

- 使用虛擬貨幣；
- 使用專業服務（律師）；
- 使用網路（國際銀行、投資平台）；
- 使用新付款方式 / 系統；
- 不動產；
- 使用代名人和第三方；
- 混合（商業投資）；以及
- 電匯 / 使用外國銀行帳戶。

泰國

313 一聯合集團在泰國南部經營販運業務，包括與鄰國進行非法跨境交易，海關人員逮捕 4 名嫌犯，起獲並扣押 13.4 萬顆安非他命、3 輛汽車、珠寶、豪華家電和 600 萬泰銖現金，此外還扣押一棟房屋和三間公寓等資產。海關人員發現，該集團在曼谷開設一家豪華汽車經銷企業，作為漂白非法所得和促進直接交換毒品付款的場所。

5.14 使用空殼公司 / 企業

中華台北

314 A 先生是 J 公司的董事長，該公司並無任何業務活動。2015 年，A 先生分別向國籍為 K 轄區的 LP 先生和個人資訊不明的 P 先生提供其在 C 銀行的個人帳戶和在 E 銀行的 J 公司帳戶，2015 年 5 月、6 月和 10 月，P 先生使用被害人的身分向金融機構發送電子郵件，意圖誤導金融機構並將資金從被害人帳戶轉移到 J 公司帳戶，確認交易後，LP 先生即指示 A 先生提領現金，再將資金交付給 LP 先生。從詐欺被害人帳戶轉移的資金總額約為 1,900 萬新台幣。桃園地檢署於 2017 年 8 月起訴 J 公司、A 先生和 LP 先生犯下詐欺罪以及違反《洗錢防制法》。

中國香港

315 從肅貪調查中得知，被告根據其友人的要求購買了一家空殼公司，受任命為該公司的唯一董事兼股東，被告同時也是該空殼公司銀行帳戶的唯一授權簽署人。2005 年 1 月至 2008 年 12 月期間，空殼公司透過信用狀詐欺收到的犯罪所得共計 250,450,000 港幣，並在同一時期向多家公司和個人支付了 250,440,000 港幣。

316 2017 年 3 月裁定被告判犯有洗錢罪，被判處三年徒刑。

紐西蘭

案例研究 1

317 一家位於萬那杜的紐西蘭信託公司成立了一家紐西蘭空殼公司，該空殼公司代表一個未知的海外客戶進行註冊，這是利用代名人隱藏實質受益人的身分。空殼公司的實際業務並不明確，從公司名稱也看不出來，公司註冊簿上列出的地址與在奧克蘭註冊為 TCSP 的虛擬辦公室相同。代名人董事居住在塞席爾，代名人股東是 TCSP 持有的代名人持股公司，代名人持股公司本身實質上是一家空殼公司，是 TCSP 註冊的其他數百家空殼公司的提名股東。新聞報導指出，授權書將董事職務轉讓予一位俄羅斯國民，其出售自己的護照資料並在拉脫維亞開設銀行帳戶。與幾家烏克蘭公司（包括國有武器交易商）進行交易往來，但資金移轉後，合約隨即遭取消，並退還給不同的第三方境外公司。此外，與同一 TCSP 註冊的其他三家紐西蘭空殼公司進行數起交易，其使用的代名人董事、代名人股東和虛擬辦公室地址都與 Tormex 相同。新聞報導指出，4 間空殼公司全涉入墨西哥錫那羅亞販毒集團的洗錢活動，涉案金額達 4,000 萬美元。

案例研究 2

318 萬那杜 TCSP 在紐西蘭註冊、由紐西蘭公民經營的公司，涉嫌充當在國外司法管轄區協助犯罪的空殼公司。TCSP 擔任代名人股東，並為居住在萬那杜、巴拿馬和塞席爾等轄區的代名人董事，提供被聘為董事

的員工（以 A 公司而言），員工多半不瞭解正在發生的活動，因為過去從未參與過任何 TCSP 活動。犯罪行為包括走私非法貨物、武器走私、稅收詐欺、投資詐欺和洗錢。A 公司是 TCSP 設立的一家公司，該公司出租飛機，但後來遭查獲被用於走私武器。TCSP 在紐西蘭註冊的 73 家公司涉嫌充當在國外司法管轄區促進犯罪的空殼公司。犯罪行為包括走私非法貨物、武器走私、稅收詐欺、投資詐欺和洗錢。

菲律賓

- 319 聲稱擔任投資顧問的個人主動聯繫 X 先生（澳洲公民也是 Y Ltd. 的所有權人），誘使 X 先生在 Z and Z Co.（一家空殼公司）開立交易帳戶，該公司是在澳洲成立的一間合法投資公司，提供美國證券的諮詢和經紀服務。X 先生投入股票買賣，但事後發現該股票完全不存在，6 個月內他損失了大約 180 萬美元。
- 320 X 先生將付款匯到 F Ltd（另一家空殼公司和虛擬經紀人帳戶），該公司位於香港，據稱為 Z and Z Co. 提供證券交割服務。X 先生向 F Ltd 的匯款部分發現是撥到 DRR（同為空殼公司），這是在菲律賓 SEC 註冊的實體。從被害人（X 先生）到 F Ltd，再到 DRR 的資金流向顯示這是「境外分層化」活動，匯入 DRR 的資金，在收到電匯資金後立即提領一空。
- 321 DRR 還從多個線上論壇（包括參與鍋爐室騙局）標記

的海外實體獲得資金，匯款人分別為 GCo.（香港）、CBP（澳門）、A Group（美國）和 SM Brokerage（美國）。

- 322 X 先生的法律顧問進行調查後發現，與 Z and ZCo. 相關的個人，所發送電子郵件的網路通訊協定（IP）幾乎位於菲律賓的一個主要城市。

泰國

案例研究 1

- 323 U 公司註冊為直銷業務，但實際上並沒有按註冊資料營運，相反地，其經由線上系統以 U-TOKEN 的名義提供單位信託，該公司誘使投資人，承諾以高額報酬提供貨幣或其他資產，但此報酬源於尋求更多成員和 U-TOKEN 增值，卻沒有出售任何商品。U 公司的活動構成公共詐欺罪，而且 U 公司的業務非常複雜，使用涉及跨國網絡的多間子公司為跨國組織犯罪集團運作，該集團將資金轉入和轉出泰國，並利用不正當收益購買土地、物業、汽車等，藉此漂白從犯罪獲得的資產。

案例研究 2

- 324 J 先生（荷蘭國民）及其同夥涉入跨國組織犯罪集團並從事毒品交易，目前已找到證據，有可能理由相信 J 先生及其同夥透過從事某種活動獲得資產，該活動構成毒品犯罪，是洗錢防制法的前置犯罪。他們開了

一家咖啡連鎖店作為非法活動的幌子業務，年收入為 600-800 百萬泰銖。

5.15 與非法伐木有關

泰國

- 325 C 女士過去曾因涉嫌將老虎從馬來西亞經寮國販運到泰國最後進入越南而被捕，但從未實際起訴，後來，其兄弟 K 先生在曼谷北部的森林中被捕，根據線索，K 先生經營一個重要網絡，涉嫌將保育的泰國紅木（Thai Rosewood）走私到中國，其他網絡涉及的走私品包括象牙和活體穿山甲。逮捕人員發現 K 先生擁有大量現金，表面上是要用來購買紅木的。AMLO 向越南的金融情報中心尋求協助，以解密 K 先生複雜的企業、同夥和跨轄區匯款網絡，據估計，K 的網絡在 2011 年至 2014 年之間使用不同且複雜的方法漂白了多達 3,500 萬美元。
- 326 主管機關發現，K 先生的姐姐 D 女士在泰國擁有一個老虎動物園，被作為走私的幌子。
- 327 K 先生和其妻遭控串謀犯有非法砍伐和販運暹羅紅木的意圖，並意圖賄賂公職人員和進行洗錢。D 女士被控洗錢罪名。

5.16 貨幣兌換 / 現金轉換

阿富汗

328 一外匯交易商於 2016 年 12 月在巴格蘭 (Baghlan) 省被捕，罪名是挪用 A 銀行 24,415,811 阿富汗幣的資金以串通銀行員工以及洗錢 6,740,000 阿富汗幣。反貪污司法中心初審法院裁定被告洗錢罪名成立，判處兩年徒刑，併科罰金 50,000 阿富汗幣，並支付相當於洗錢資金的罰款。

汶萊

329 2016 年 6 月 21 日至 23 日，來自外國轄區的 5 人以社訪簽證抵達汶萊，隨身帶來偽造的 ATM 提款卡。

330 2016 年 6 月 24 日至 25 日間，5 人同時前往多個 ATM 使用偽造的提款卡及隨附的個人身分識別碼 (PIN)，存取 ATM 內的電腦程式，一旦獲得存取權限，就透過多次交易提領大量現金。

331 汶萊皇家警察部隊 (RBPF) 根據 ATM 的監視錄影證據，於 2017 年 6 月 25 日在汶萊國際機場的登機閘口逮捕這 5 個人，調查發現，由於交易嘗試失敗，在其中一台 ATM 機上遺留了 43 張偽造的 ATM 提款卡。

332 其中三個人利用持照的貨幣交易業者將非法獲得的現金兌換成總計 34,550 美元的金額，RBPF 已收回所有轉換後的現金。

333 根據《電腦濫用法》(第 194 章)和《刑法典》第 22 章，於 2017 年 8 月 26 日將這些人判處 4 至 13 年不等的徒刑，檢察官進一步根據《2012 年犯罪資產追討

令》提起訴訟，要求沒收這五個人竊取的資金。

巴基斯坦

- 334 一起針對 A 先生和 B 先生的 STR 指出，兩人是堂兄弟，A 先生定居國外，B 先生則在巴基斯坦管理商業物業。一家找換公司提出 STR，表示以分散交易的方式進行高價值的貨幣兌換交易。分析過程中，發現這兩個人從公開市場購買了大量美元，嫌犯在 ZXY 銀行擁有多個巴基斯坦盧比和美元聯名帳戶，而帳戶交易方式顯示，大量資金透過清算和內部轉帳記入其 PKR 帳戶。資金是以現金交易的方式從 PKR 帳戶中提領，然後向不同的兌換公司購買美元，再存入嫌犯的外幣帳戶，最後，資金匯出管轄區。
- 335 進一步調查中發現，A 先生出售其物業，相關資金存入 PKR 帳戶，但金融活動的層度遠高於出售物業的所得，因此懷疑其低報銷售合約以逃避稅收。此外，B 先生的職業也令人起疑，因為嫌犯提供的業務證明與公司的位置和存續互相矛盾，內部資料庫還發現，B 先生是持有帳戶所屬銀行的員工。在所有聯名帳戶中，開戶帳戶的權限均為「任一或倖存者」，這表示任何人都可以獨立操作帳戶，A 先生疑似為實際所有權人，所在位置不在轄區內，而負責交易的人則由 B 先生進行。
- 336 此外，其個人稅收狀況與帳戶中金融活動的程度不符。

- 337 結果發現，他們故意採用這種交易方式和行為，目的是規避主管機關，然後利用銀行管道和找換公司以分散交易和其他策略，將大量資金匯出轄區。
- 338 根據異常帳戶活動可得出結論，兩人涉入未經授權的資本逃避和逃漏稅行為，此情報與執法機關共享。

泰國

- 339 緊急情況下，OAG 接到荷蘭大使館的請求，要求 AMLO 凍結和扣押 J 先生及其同夥的資產，因這些人可能轉移、處置、隱匿或隱藏犯罪相關資產。J 先生及其同夥透過其在荷蘭的公司網絡（實為組織犯罪集團）販運大麻（一種麻醉藥品），該集團漂白銷售麻醉藥品的犯罪所得，將資金從海外法人的銀行帳戶移轉至泰國，再以實體跨境運送、銀行存款、幌子公司、土地出售以及由代名人持有貨幣或財產等方式，持有資金或財產。

5.17 貨幣走私

阿富汗

案例研究 1

- 340 2017 年 1 月 22 日，某人（X 人士）從轄區 Y 直飛到喀布爾（Kabul）國際機場，海關發現其持有的未申報現金超過機場海關允許的門檻，進行全身搜查後，總共發現 X 人士隨身攜帶了 23,000 瑞士法郎、

238,700 美元、141,500 印度盧比和 95,910 歐元，經徹查後，裁定對該人罰款，罰金佔扣押現金總額的 15%（即 3,569,282 阿富汗幣，約合 52,313 美元）。

案例研究 2

341 2017 年 6 月 8 日，在喀布爾機場對一名嫌犯（A 人士）的行李進行實物搜查，發現其中有 4 包重達 11.724 公斤的金條。在機場接受偵訊時，A 人士表示：「我在鞋子內放金條，過海關的 X 光機後，我坐在椅子上，將包裹從鞋內拿出來進了手提包，然後就將手提包交給航空公司」，但檢查機場的監視攝影機之後，發現 A 人士進入機場航廈時只有一個行李，第二件行李則是由另一人帶到航廈。據發現，兩個人先後進入候機室的洗手間，當他們從洗手間出來時，其中一人前去航空公司的櫃檯交出行李，另發現，將行李交給航空公司櫃檯後，A 人士即進入航廈大廳，而 B 人士離開機場航廈。權責機關對案件進行徹底調查之後，裁定當事人罰款 4,980,93 阿富汗幣 0（72,558 美元）。

案例研究 3

2016 年 12 月 12 日，某人（X 人士）購買直航商業機票欲從喀布爾國際機場飛往轄區 Y，該人完全無意向授權人員申報他隨身攜帶的 28,750 美元現金。根據程序，當事人在機場的離境海關被攔下進行行李搜查，理由是懷疑藏匿未申報現金，且金額超過規定門檻，在機場第一個海關對當事

人進行搜查時，海關人員發現嫌犯的鞋子、旅行袋和褲子中藏有 19,250 美元，夾克口袋則藏有 9,500 美元。經調查後，因該人違反規定而遭海關裁定罰款 288,712 阿富汗幣（4,310 美元）。

斐濟

342 2017 年 8 月 14 日，一名 35 歲的商人 Buren Randolph 先生協同其妻乘坐 Tarawa FJ230 航班抵達香港，其並未依規定申報價值 37,719.18 斐濟幣的貨幣（澳幣和美元貨幣），這筆錢在其中一個手提箱中查獲，而 Randolph 先生本人無法以英語讀寫。

343 Buren Randolph 先生因違反 BCR 申報要求而遭判有罪，勒令支付 4,000，斐濟幣其他未申報的現金則予退還。

泰國

344 寮國國籍的 M 女士將一筆 3,000 萬泰銖的現金藏在皮卡車中，意圖走私進寮國，海關人員在泰寮 2 號友誼大橋的海關逮捕 M 女士。AMLO 仍在調查相關洗錢網絡。

5.18 使用信用卡、支票、本票等

斐濟

345 兩名賽普勒斯國民於 2017 年 12 月 12 日從香港抵達斐濟，兩人於 2017 年 12 月 19 日因使用偽造信用卡 / 簽帳卡在 ATM 進行交易而遭斐濟警察部隊逮捕。

Loizos Petridis 先生和 Cleanthis Petrides 先生共同遭
起訴 293 項洗錢罪以及意圖透過詐騙手段獲取財產。

日本

- 346 一名男子從事非法放款業務，向存款機構提供本金和利息借貸、過帳票據或支票，以將資金移轉到以他人名義開立的帳戶。涉及洗錢行為的罪犯濫用票據或支票，以快速轉移犯罪所得或將犯罪所得偽裝為合法資金。

新加坡

- 347 一名前銀行人員利用其團隊經理的帳戶，將自己的信用卡臨時額度從 15,000 星幣提高到 106,500 星幣，還未經授權退還信用卡 9,300 星幣的餘額。
- 348 該銀行人員藉著信用額度提高買下金條，再立即以 30,150 星幣的價格售出，還利用提高的額度購買價值 65,834.08 星幣的賭場籌碼，隨後將其用在海外賭場賭博。該人使用現金和信貸餘額退款資助自己的賭博惡習，以此償還欠銀行和無照放款人的債務。
- 349 該人遭判犯有濫用電腦和洗錢的罪名，被判處 41 個月徒刑。

5.19 分散交易（洗錢）

阿富汗

- 350 阿富汗銀行機構的申報門檻為 1,000,000 阿富汗幣（14,500 美元），如果連續兩天內發生的任兩項或多

352 儘管已將 2,600 萬阿富汗幣（382,000 美元）存入銀行系統，但由於經過嚴密組織性的分散交易（38 筆存入），因此未就大量現金交易向金融情報中心提交報告。除了分散交易外，還發現其他可疑行為，因此將案件轉交給執法單位進行調查。

5.20 電匯 / 使用外國銀行帳戶

汶萊

2017 年 10 月 29 日，外國人 Z 依《2006 年稅務令》第 146（1）（d）條遭控持有違禁品，另根據《2012 年犯罪資產追討令》第 3（1）（b）條被控三項洗錢罪名。Z 承認自己未經許可即持有 118 包和 2,058 條香菸，以及三箱裝有酒精飲料，調查過程中，Z 承認其從外國轄區購買所有違禁品。

353 調查發現 Z 涉入洗錢行為，2016 年 1 月至 2017 年 10 月之間，其將銷售違禁品所賺取的獲利 2974 美元，匯給位於外國轄區的某人。根據《2006 年稅務令》，Z 被裁定應付罰款 1,600,000 美元，併科 3 年監禁，同時各項洗錢定罪應各判處 6 個月監禁。

中華台北

354 LH 先生曾任 T 公司的董事長。2007 年到 2008 年，LH 先生在海外成立了 P 公司和另外 6 家公司，並為這些公司開設了帳戶，為獲得犯罪所得，LH 先生與 24 名員工簽署股份管理合約或技術性股份分配合約，

聲稱由於擔心公司未來收入過低，因而需協助員工管理獎金。這些合約載明 T 公司正式管理員工最初持有的股份和獎金，LH 先生指示員工在特定時間和價格售出股票，員工扣除必要費用後，將交割收益轉移到 P 公司在香港的帳戶。資金總額約為一億元。

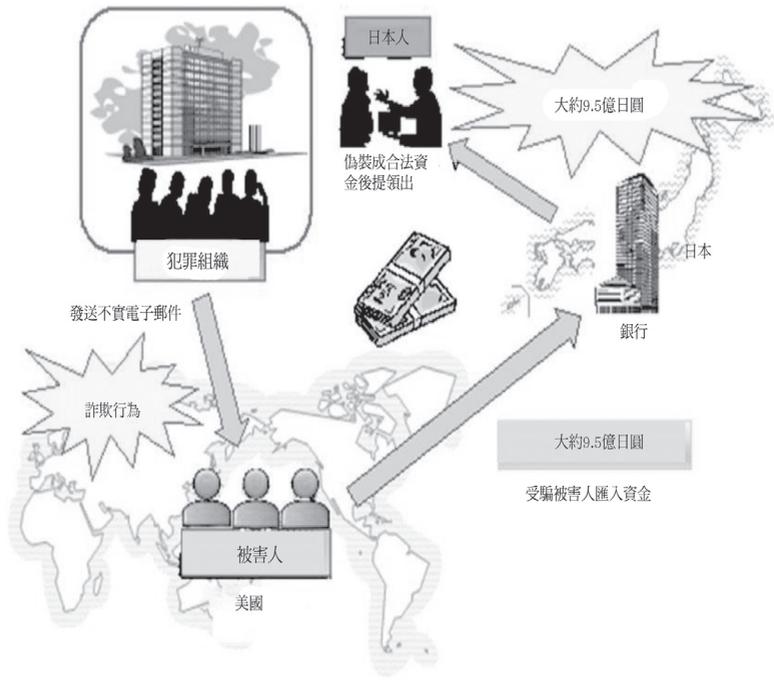
- 355 為避免遭執法機構進行調查，LH 先生指示一名員工將資金分配到 LH 先生控制的多個法人帳戶。執法單位調查完畢後，全案於 2017 年 7 月依違反《證券交易法》、《洗錢防制法》移送士林地檢署提起公訴。

斐濟

- 356 斐濟金融情報中心收到針對一家工程公司（Y 公司）的兩起 STR，原因是其進行大量的定期現金和支票存款交易，斐濟金融情報中心進行分析後，確定該公司在三個月內進行了多次不尋常交易。
- 357 根據發現，Y 公司在兩間不同銀行共擁有 5 個商業銀行帳戶，調查進一步發現，過去兩年間，這兩個銀行帳戶中的存款交易總額約為 450 萬斐濟幣。
- 358 斐濟金融情報中心還確定，Y 公司在過去兩年中未向稅務機關提交任何納稅申報表，一份報告已傳遞給稅務機關，認為可能有稅收犯罪問題。指標包括：
- 多次存款交易，但都低於 10,000 斐濟幣的申報門檻。
 - 未向稅務機關提交納稅申報表。

日本

- 359 日本男子向美國被害人發送偽造交易電子郵件，促使被害人將約 9.5 億日圓（約合 900 萬美元）的資金匯入以他人名義開立的日本銀行帳戶。
- 360 犯罪者提領資金時向銀行人員提供不實陳述，表示這些資金來自一般商業交易相關的匯款，意圖將資金偽裝成合法商業利潤。最後其因違反《組織犯罪懲治法》（隱匿犯罪所得）和詐欺行為而遭逮捕。



菲律賓

- 361 根據國家調查局（NBI）報告，某些菲律賓人正使用不實美國國稅局（USIRS）和菲律賓政府的印鑒和文件假設虛擬網域，並在該網站上徵求投資。該網站建議被害人將預付款和手續費移轉至銀行帳戶 1 和銀行帳戶 2。銀行帳戶 1 屬於「ABCD Trading system」的帳戶名稱下，地址在宿霧市，此帳戶中的交易多為國際匯款（來自英國、澳洲、挪威和瑞典等個人以及印尼實體），且這些匯款匯入後都立即被提領一空。一名匯款人還向設在宿霧的 CD and Associates、USR Trading 和 XYZ Trading Services 匯出資金；另一名匯款人則將資金移轉到位於班詩蘭省（Pangasinan）的 NL Distribution and Logistics。AMLC 資料庫顯示 CD and Associates、USR Trading、XYZ Trading Services 和 NL Distribution and Logistics 帳戶中的交易模式，皆與與 ABCD Trading 帳戶中的交易模式相同。
- 362 一家銀行因一名中國匯款人的投訴，而向 USR Trading 提交疑似洗錢或資恐交易報告，該報告中指出，投訴人據稱依據財政部國稅局的建議匯出款項，以將稅款支付到 USR Trading 的帳戶（與提早投資的收益有關）。

泰國

案例研究 1

- 363 AMLO 協同 DSI、泰國皇家警察總署打擊犯罪部（CSD）和 SEC，共同展開一項公共詐欺、逃漏稅和洗錢調查，其中涉及 E 先生及其同夥，E 先生為加拿大國民，是一家健身公司的前任所有權人。
- 364 該健身公司在泰國破產法院被一家泰國銀行提起訴訟，要求償還 7,200 萬泰銖的貸款以及 400 萬泰銖的利息，因此，該公司最後將收掉其在泰國的 8 間連鎖店中的 7 間。
- 365 該公司的行為模式導向公共詐欺和逃漏稅行為，包括向股票市場提供自 2003 年以來持續持續虧損的可疑不實陳述，以及縱使提出虧損報告但仍不斷進行可疑的海外匯款。
- 366 該公司在泰國的業務基本上是非法貨幣交易業務，會員獲得的服務品質極差、損失會費，還導致股東利益損失和泰國營收損失。

案例研究 2

- 367 主管機關懷疑一名被告捲入毒品相關的案件，並據此展開了調查，後發現被告利用其子女和他人的帳戶，從他處將資金轉入這些帳戶。主管機關發現被告對這些帳戶擁有完全控制權，儘管檢方無法證明毒品犯罪，但法院發現，被告利用這些帳戶其實是為了隱匿資金的真實來源，因而裁定被告洗錢罪成立。

5.21 大宗商品交易（易貨交易，例如對非法毒品的再投資）

紐西蘭

368 以下案例研究已發布在紐西蘭金融情報中心 2015-16 年第三季度態樣報告中，請參見：<http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q3-2015-16-predicate-offending.pdf>

狡猾行動：毒品犯罪

369 威靈頓秘密行動小組和中央資產追討單位聯合對一起家庭大麻的商業銷售案件展開調查。該集團種植大麻和也向其他種植者採購大麻，然後再行出售，該集團從中賺取可觀利潤，前後 7 年間該集團內各家庭成員的銀行帳戶總計存入約 116 萬美元的現金存款。該集團的負責人 A 人士每天早上要花幾個小時存錢，下午賣大麻，晚上則準備第二天的活動。

370 為掩飾資金來源，集團負責人 A 人士將資金混入多個帳戶，A 人士分別以自身名義、信託名義和家庭成員的名義，在多間銀行開立了多個銀行帳戶，接著將從大麻銷售中獲得的現金分裝到拋棄式塑膠袋，每一袋通常約 500 美元。A 人士會前往多家銀行，從投幣箱將現金存入各個帳戶，這樣一來就無須與銀行出納員的互動，此舉很可能是為了盡可能降低被查獲的風險。最後 A 人士將這些資金與合法來源的資金混合在

一起購買資產，整個集團成員購買了十個不動產，其中多個物業由該集團設立的信託持有，其他現金也會存入該信託的銀行帳戶。

371 根據《2009年犯罪所得追討法》，約有225萬美元的資產受到限制，這些資產包括物業、車輛和現金。隨後，A人士遭控販賣大麻以及為供應大麻和洗錢而持有大麻。

5.23 使用假造的身分證件

斐濟

案例研究 1

372 斐濟金融情報中心收到一起來自外匯交易商對Z人士提出的STR，其中指出Z人士在接收匯款時提供偽造身分證，由於該身分證沒有有效期和居住地址等詳細資訊，因此懷疑是偽造的。據發現，Z人士已收到兩筆名稱不同的匯款，自2017年4月至10月所收到國際匯款共計12,930。

373 經過進一步分析，斐濟金融情報中心發現Z人士有兩個稅務編號和以兩個名字持有的銀行帳戶。

374 關於詐欺和偽造的報告已分發給斐濟警察情報局。指標包括：

- 假身分證。
- 同一人有兩個稅務編號。

案例研究 2

375 斐濟金融情報中心接獲多起 STR，表示某人涉嫌利用竊取而來的信用卡資訊在多家零售店和珠寶店購買珠寶和生活用品的個人的交易記錄。經與零售商進一步確認後顯示，該人使用兩張疑似為偽造的外國駕照。斐濟金融情報中心發布警報通知，要求金融機構將其目前使用的方法告知 EFTPOS 商家，另向斐濟警察部隊轉發一份報告。

376 發出警報通知後，零售商識別涉嫌個人，並將該個人的錄影帶提供給金融情報中心和斐濟警察部隊。錄影片段可詳細看到該人目前使用的車輛詳細資料，這讓斐濟警察部隊得以掌握明確的線索進行搜查。此案仍在調查中，可能犯罪包括詐欺和偽造。指標包括：

- 偽造外國身分證。
- 在不同位置的同一零售商購買大型物品。

中國香港

377 肅貪調查顯示，被告是家庭主婦，向其友人提供個人詳細資訊、身分證件，地址和銀行帳戶詳細資訊，以便將被告註冊為清潔服務承包商的員工。被告從未在該公司工作，但 2014 年 4 月至 2014 年 12 月間卻領取了總額為 83,408.66 港幣的薪資，被告從薪資將大部分款項退還給友人。

378 2017 年 8 月裁定洗錢罪名成立後，被告被判處三個月

兩個星期的監禁。

日本

379 犯罪者使用偽造的國民健保卡、非法獲得的銀行帳戶、居留證件和郵政服務，作為接收犯罪所得以及用於洗錢的工具。

巴基斯坦

380 A 先生在巴基斯坦經營鞋業，他在 AB 銀行開了一個帳戶，但 3 個月後立即關閉該帳戶，這 3 個月內，該帳戶轉出高價值資金。嫌犯在 AB 銀行關閉帳戶後立即在 CD 銀行開立另一個帳戶。

381 此外，發現嫌犯在 AB 銀行和 CD 銀行開戶表格的簽名筆跡相異，因此懷疑這是貝納米（Benami）帳戶。審查帳戶對帳單時，發現平均每月營業額以及借方和貸方營業總額較高。嫌犯透過內部轉帳、線上轉帳、多次現金存提款以及清算支票等，進行大量分散交易，藉此規避避免申報門檻。此外還發現，大多數交易都涉及不相關的交易對象。

382 與執法機關共享資訊。

新加坡

383 新加坡最古老的其中一家合作社的兩名前員工，因涉嫌詐欺超過 500 萬星幣而被判詐騙、偽造、背信和洗錢等罪名，分別被判處 144 個月徒刑和 116 個月徒刑。

384 經調查後確定，兩名員工向合作社提交偽造的貸款申

請表、存款提領表和幽靈成員（其家人和朋友）的成員資格終止函。6年多內，該合作社遭騙支付超過500萬星幣的款項，隨後兩名員工藉由家人和朋友組成的車手網絡進行洗錢，最終以支票兌現、現金提領和電子資金轉帳等方式，取得犯罪所得。

泰國

385 警方要求 AMLO 查察一個跨國犯罪組織成員的金融交易紀錄，因為他們假借設立龐氏騙局公司涉犯公共詐欺罪。該組織在中國也犯行，100,000 多人受騙，總價值為 130 萬元人民幣。中共政府對 S 先生、G 先生和 W 女士發出逮捕令，後發現同一批人在馬來西亞也犯同樣罪行，詐騙金額總價值為 3 億馬幣。此外，這些人亦使用緬甸護照和偽造的泰國公民身分證進入泰國，以在泰國設立 Y 公司。

5.22 寶石和貴金屬

日本

386 洗錢人士以竊取而來的現金購買貴金屬，其選擇匿名交易，並就客戶身分提供不實資訊（簽訂銷售合約時冒充他人或提供偽造的身分證明文件）。

5.23 購買貴重資產（藝術品、古董、賽馬等）

馬來西亞

案例 1- 販毒集團

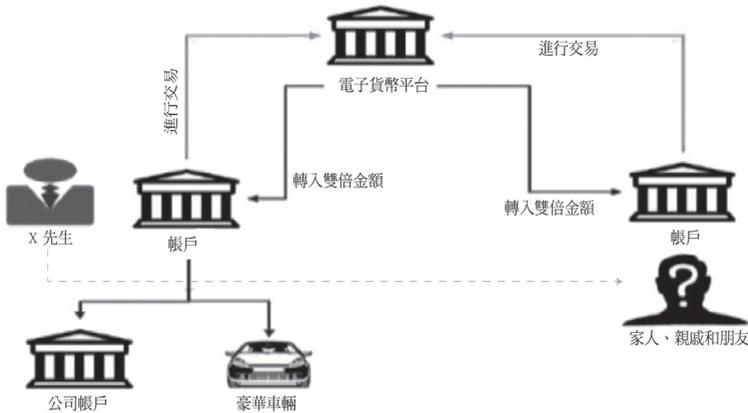
- 387 馬來西亞皇家警察最近對轄區北部經營的一個販毒集團提起訴訟，指控該集團與鄰近轄區的一個毒品集團有關聯。該集團還涉嫌生產毒品，透過一家空殼公司設立毒品實驗室。販毒收益由主要嫌犯的代理人（亦為嫌犯女友）管理，犯罪所得主要用於購買豪華車輛、珠寶、不動產和股票。
- 388 財務分析顯示，部分收益還用於資助其他非法活動，包括非法賭博。使用的洗錢方法包括使用代名人、信託、家庭成員或第三方；購買有價值的資產（藝術品、古董、賽馬、車輛等）以及使用空殼公司 / 企業。

案例 2- 詐欺

- 389 X 先生認購一家國際電子貨幣公司的股份，該公司與其在商業銀行中的儲蓄帳戶相關聯。電子貨幣公司定期進行系統維護作業，作業期間會發生系統故障而導致付款錯誤的問題，使得原本應從該帳戶扣除的資金，誤被加倍轉入 X 先生的儲蓄帳戶。X 先生利用每天特定時間發生的系統錯誤，反覆進行交易以詐取資金。X 先生也慫恿家人和親朋好友效法，5 個月內，該詐欺計畫涉及的帳戶超過 100 個，金額超過 1,000 萬美元。
- 390 非法所得除分層用於購買豪華車輛和放入公司帳戶

外，還存入嫌犯的個人帳戶作個人支出，迄今，已有 24 名嫌犯遭控犯有詐欺和洗錢罪。

- 391 使用的洗錢方法包括使用代名人、信託、家庭成員或第三方等；購買有價值的資產（藝術品、古董、賽馬、車輛等）。



5.24 資本市場投資，使用經紀人

斐濟

- 392 Y 人士是居住在美國的斐濟國民，是一家當地投資公司的客戶，據稱，Y 人士是被竊取身分的被害人，Z 人士入侵 Y 人士的電子郵件並竊取其個人身分證明文件，Z 人士以電子郵件指示投資公司出售 Y 人士擁有的投資，並將資金匯入嫌犯在愛爾蘭的銀行帳戶，共約 9,981 美元被轉入愛爾蘭的銀行帳戶。

- 393 斐濟金融情報中心進行財務檢查，並與其國外友軍單位建立聯繫，確定該銀行帳戶為 Z 人士所有，而該人又與愛爾蘭的某些犯罪活動有關。
- 394 報告被傳送至投資公司和當地銀行以供參考，投資公司依建議應就 Z 人士竊取資金的補償事宜與當地銀行聯繫。在此之前也向斐濟警察部隊發送一份報告，以進一步調查詐欺和識別竊賊身分。指標包括：
- 詐欺性電子郵件
 - 被害人並非資金匯入目的地帳戶的持有人

5.25 環境犯罪

泰國

- 395 K 先生是位在泰國的外籍人士，主要在從事野生動植物交易，曾涉嫌將保育泰國紅木（Thai Rosewood）走私到外國轄區。K 的網絡使用多達 28 個獨立帳戶，利用其在泰國和許多鄰近司法管轄區的聯繫管道來轉移非法資金。運輸紅木相關的付款源自外國轄區，透過 K 在泰國南部的同夥發送到另一個外國轄區的帳戶。
- K 的網絡使用其帳戶、聯繫管道和商業利益漂白高達 11.8 億泰銖（約 3,500 萬美元）的資金。
 - 珠寶首飾 – 警方在 K 妻子的家中查獲 14 枚奢華女錶。
 - 車輛 – 從 K 和其妻共同擁有的汽車經銷店中扣押 29 輛汽車。

- 現金 – 警方從該網絡成員身上查扣 600 萬泰銖（約合 185,000 美元）的現金。
- 土地 – K 集團的成員擁有多達 24 塊土地。

5.26 毒品相關

泰國

396 AMLO 接獲一起 STR，詳細指出 S 女士（P 先生的情婦）進行的交易涉及大量現金存提款，金額為 100-190 萬泰銖（約 30,000 美元至 47,000 美元）。S 女士只提領小面額的紙幣，藉此規避向 AMLO 的申報義務。根據 AMLO 的調查，發現這對男女在多家銀行擁有 70 個帳戶，P 先生有吸毒記錄，而 S 女士沒有此類記錄。AMLO 將財務分析報告分發給泰國皇家警察總署肅毒局（NSB），以採取進一步行動。

397 NSB 進行調查，發現這對夫婦涉嫌販毒並與 WA（泰國的少數族群）直接接觸，NSB 佯裝欲購買 74 公斤的海洛因，實際是為了逮捕這對男女和其他共犯。NSB 沒收了 74 公斤的海洛因，價值約 455,590 美元的泰銖現金、總計 114,251 美元的現金和價值約 360,175 美元的銀行帳戶。AMLO 人員、NSB 人員和 ONCB 人員一一搜查 13 戶據信為這對男女處置毒品收益的人家，共查獲約 215,835 美元的現金和 9 張價值高達 115 萬美元的銀行存摺以及許多車輛。

5.27 直接根據可疑報告或門檻交易報告發展出的案例 阿富汗

案件標題：幽靈公職人員

- 398 X 人士開設了 13 個銀行帳戶；其中 11 個帳戶的開設目的為薪資帳戶，根據該當事人的「瞭解您的客戶」（KYC）表格，所有帳戶均以不同電話號碼、地址和薪資收入開立。
- 399 調閱該人的 KYC 表格和銀行對帳單後，發現當事人透過不同銀行帳戶收到大量公共資金為月薪。當事人的月薪為 300 美元，但 4 年內以薪資騙局共計詐領了 482,746 美元。STR 分析報告已分發給檢察總署進行調查和起訴。

孟加拉

- 400 ‘A’ 銀行對兩個合作社和一個宗教機構的帳戶提交 3 起 STR，指控其挪用公共資金。經初步分析後發現，這些帳戶分別在同一天以支票兌現的方式轉入相同的金額（90,500 孟加拉幣），這些支票多由當地政府機構（簡稱「‘G’ 政府」）從其在 ‘H’ 銀行持有的 ‘F’ 帳戶所開立的。除了支票存款和現金提領之外，這些帳戶中沒有任何交易，在 BFIU 資料庫中亦未找到有關這些實體的 CTR、投訴或不利資訊。
- 401 上述情況無法解釋實際發生的情況以及資金遭挪用的方式，因此，BFIU 分析師決定在孟加拉銀行的

BACH 資料庫中進行搜尋，篩選由 ‘G’ 政府簽發的支票。結果顯示， ‘G’ 政府已簽發數千張支票（每張的金額為 42,000-49,500 孟加拉幣或 90,500-98,500 孟加拉幣不等），而且都是從 ‘F’ 帳戶開立給不同帳戶。BFIU 的分析師於是將時間縮短至過去 6 個月，發現大約 600 張支票的簽發對象包括宗教機構、孤兒院、教育機構、社會文化組織、合作社等 252 個組織，這些組織共在 29 家銀行分別開設帳戶。BFIU 指示這些銀行提交相關開戶表格、帳戶對帳單和其他相關文件，以及有關組織位置和活動等的查核報告；同一時間，BFIU 接獲有關 69 個實體帳戶的 69 起雷同的 STR，呼應了 BFIU 先前試圖尋求的資訊。

402 從銀行提供的文件和資訊可看出，將近 60% 的組織非實際存在或沒有實際組織活動，或與不存在的組織有直接或間接關聯。BFIU 下一個兩人小組另藉著銀行分行的現場查核作業對 10 個組織進行抽樣訪視，結果發現其中 3 個組織根本不存在，另外 3 個則沒有任何活動。最後 BFIU 分析師判定這 180 個組織共計收到 ‘G’ 政府藉基礎設施開發所開立的 479 張支票，價值 3,875 孟加拉幣萬。大多數情況下，款項存入後都會立即提領一空，除此之外並無其他交易行為。

403 BFIU 在資金支付和開戶程序中均發現異常。同一人士曾在多個以偽造註冊證書登記的組織下擔任委員會

成員，少數幾個在‘G’政府管轄範圍外的組織也獲得資金，但這些組織中大多數無法出示接收資金的證明文件。此外，銀行沒有按 BFIU 通知書遵守 KYC 程序，各銀行分行的人員看似都在協助開設假帳戶。其中確定有 26 個組織以不實文件註冊為合作社、34 個組織以不實文件註冊為自願性協會、18 個組織則提交假的成員證明。

404 地方政府機構（‘G’政府）承接地方機構的基礎設施開發專案，但一群不誠實者組成幽靈組織，假意出示必要文件、開設銀行帳戶後，向‘G’政府申請分配基礎設施開發資金。

405 由於此案涉及公共資金，因此 BFIU 將全案移交執法機關進行深入調查和後續法律程序。BFIU 針對使用偽造註冊證書一事，與合作社部門和社會服務部門交換資訊，還針對其中部分註冊實體向不存在組織核發成員資格證書等事宜，與合股公司暨農場註冊處（RJSC&F）交換資訊。執法機關已成立一調查小組，積極調查此案，合作社部門也對這些遭控訴的合作社採取懲戒措施。

中華台北

406 2016 年 9 月，金融情報中心接獲 H 銀行提交的 STR，指出 F 公司在貝里斯（Belize）設立的 OBU 帳戶經常從 L 先生在香港的帳戶收到匯款，L 先生表示

這些資金是 H 銀行「瞭解您的客戶」(KYC) 流程中的商品採購佣金，但每筆匯款的金額從 50,000 美元到超過 200,000 美元不等。H 銀行認為 F 公司 OBU 帳戶中的交易比往常更可疑，因此向金融情報中心提交 STR。金融情報中心發現，分析期間，L 先生涉嫌犯罪活動，於是將案件轉交調查。

407 L 先生和 Y 先生是成功上市公司 -I 公司的業務經理，負責產品銷售業務，兩人憑藉售價最終決定權，要求 T 公司的董事長 U 先生支付回扣。U 先生同意後，L 先生和 Y 先生就以較低的價格將產品從 I 公司出售給 T 公司，這使 I 公司失去獲利良機，也導致 I 公司無法賺取更多利潤。U 先生向 L 先生和 Y 先生提供 40% 到 50% 的利潤作為回扣，2014 年至 2015 年間，U 先生支付的回扣總額超過新台幣 3,000 萬元。

408 為掩飾犯罪所得，L 先生要求 U 先生直接或由 U 先生的妻子交付現金，或使用 F 公司的 OBU 帳戶或其他外國法人帳戶，將資金轉入 L 先生在香港的帳戶。然後，L 先生將回扣的 60% 轉移到一家外國公司（其中 Y 先生為董事）在香港的帳戶中，或轉移到 U 先生妻子的帳戶，再由 U 妻提取現金後交付給 Y 先生。

409 新竹地檢署於 2017 年 4 月依背信罪起訴 L 先生和 Y 先生。

斐濟

- 410 2017 年，斐濟金融情報中心向斐濟警察部隊、斐濟稅務暨海關總署、外國金融情報中心和其他相關執法機關總共發布了 448 份案件分發報告（CDR），CDR 是經過分析 STR 後完成的報告。斐濟金融情報中心案件分發報的主要接收者是斐濟稅務暨海關總署（FRCS），內容大多有關涉嫌違反《所得稅法》和《增值稅法》。2017 年一共向 FRCS 發布了 317 份此類報告。此外，一共向斐濟警察發布 84 份 CDR，對象多包括洗錢防制小組和犯罪所得單位、跨國犯罪小組和警察情報局。
- 411 STR 分析程序中會在斐濟金融情報中心線上資料庫進行搜尋，該資料庫包括大額通貨交易報告（CTR）、電子資金轉帳報告（EFTR）和邊境貨幣報告（BCR）。
- 412 2017 年，金融情報中心收到：
- 共 623,213 份 CTR，平均每月約 51,934 份 CTR；
 - 共 1,220,602 EFTR，平均每月約 101,717 EFTR；
 - 共 792 份 BCR，平均每月約 66 共 BCR。
- 413 關鍵夥伴機構可經由直接資料存取安排，存取斐濟金融情報中心資料庫，2017 年，執法機關共 65 次存取資料庫以協助調查。

中國澳門

- 414 2017 年 6 月接獲的 STR 中，指出客戶 A 是一名 11 歲

學生，在當地一家銀行開設帳戶，其帳戶最終由其母 B 女士控制，母親 B 女士因未在兒子的帳戶中收到匯款而與銀行聯繫。由於銀行懷疑上述匯款交易的合理性，因此銀行回溯客戶 A 在 2017 年 3 月至 2017 年 5 月的帳戶記錄，發現其帳戶收到來自 20 多個不同第三方共 32 筆的轉帳交易，以及 11 筆以自動存款機的現金存款交易。收到上述資金後，立刻就會經網路銀行轉入 B 女士在另一家銀行的帳戶。該未成年人帳戶所收到的資金超過 100 萬澳門幣。

- 415 情報顯示，2012 年至 2017 年間幾起詐欺案件中，B 女士都是嫌犯，懷疑她利用兒子的帳戶向詐欺被害人收取資金。該案已提交公共檢察院深入調查。

馬來西亞

人口販運集團

- 416 金融情報中心最初分析有關 A 先生的 STR，其中指出 A 先生的銀行帳戶發現異常交易模式，涉及來自不同地點的現金存款和與不同個人之間的往來資金移轉。與主管機關核對後發現，其是三個犯罪集團的成員，曾涉入以飛機協助偷渡外國移民，當時甚至得到政府公職人員的協助。
- 417 隨後，金融情報中心的分析聚焦於另一集團成員 B 先生，其經常將資金移轉給 A 先生，前者在一年之內曾向當地一家航空公司進行數百筆付款，這顯示其可能

是在購買機票，以利集團走私外國移民進入馬來西亞。

418 與主管機關的進一步交涉後，發現該集團另外 11 個關聯人士。整體而言，金融情報中心分析並揭露涉嫌交易總金額為 150 萬美元的銀行資訊，這些交易中大部分為現金往來。

419 根據《2007 年防制人口販運暨反移民走私法》，該調查中有多人被捕，整體調查仍在進行中。

詐欺

420 根據外國執法機關對涉嫌詐欺活動的舉報，進而對某一實體和相關人士展開分析，經審查 STR 和查詢相關資料庫後發現：

- 獨資企業帳戶無正當理由，持續從海外收到大筆匯款。
- 發款人與受款人之間沒有關係。
- 交易與當事人的業務性質不一致，一般稱其涉及一般交易。
- 收到資金往往在當天或接下來幾天內，立即全額提出，或線上全額轉帳至個人或第三方帳戶。

貪污

421 分析貪污相關的疑似洗錢或資恐交易時，觀察到以下趨勢：

- 嫌犯通常為政府公職人員，多半有能力做出或影響核准開發專案的決定，因此會藉此濫用職權以牟取

個人利益和金錢利益。

- 對主嫌帳戶的分析顯示，經常出現大量現金存款、資金轉帳和支票付款，這與個人資料不符。隨後，資金會用於購買單位信託、豪華車輛和不動產，購買後也多半登記在配偶或子女的名下。
- 部分案例中，根據外國金融情報中心共享的資訊，嫌犯或其代理人也持有外國銀行帳戶；其他情況下，則懷疑資金存款人是該轄區內未經註冊的貨幣價值移轉體系營運商。
- 檢查其他資料庫後發現，常使用代理人註冊的企業和公司，競標由嫌犯主導的政府專案。

紐西蘭

422 紐西蘭金融情報中心根據對各 STR 的獨立評估結果，向相關政府機關分發送資訊。就執法單位而言，會根據報告中對 STR 所提之個人、交易和可疑原因的評級矩陣，視情況將個別人士或實體納入報告，這些報告會以專案小組的方式發送給情報單位或個別人員。大多數情況下，個別人士已面臨起訴或受到調查。但不論如何，在調查之前發布的 STR 目前都不會列入記錄。

423 過去 12 個月間，因 STR 而展開的案件中，共 5 起紐西蘭警察組織的嚴重犯罪以及 27 起潛在詐欺案件（社會發展部）；此外，還有更多案例中，執法機關查案時高度仰賴 STR 的資訊，例如，STR 資訊曾用於支

援組織犯罪的調查案，包括對前置犯罪和相關洗錢行為、獨立洗錢行為和資產追討調查。AML/CFT 監理機關還使用 STR 資訊來調查 AML/CFT 法案違規行為。

- 424 紐西蘭稅務局還在所謂的巴拿馬文件專案中善用 STR，重大詐欺辦公室也發現 STR 可用於識別涉嫌詐騙民眾以資助國外 419 詐騙集團的詐騙累犯。商業暨移民部接獲大量 STR，這有助於聚焦於大規模移民詐欺和建築工地移民勞工剝削相關的光譜行動（Operation Spectrum）。紐西蘭警方下轄的防範兒童剝削單位（OCEANZ）使用 STR 資訊確證從國外對等單位獲得的情報，相關資訊進一步協助其識別嫌犯的个人資料。紐西蘭海關根據紐西蘭金融情報中心提供的 STR 資訊採取行動，包括界定範圍、發布警報（旅客和貨運）、郵件收發和徵用。

新加坡

利用可疑交易報告直接扣押一樁行賄案中的 1,600 萬美元

- 425 2016 年，貪污行為調查局（CPIB）截獲一起轉介來的 STR，內容有關 A 公司在新加坡銀行帳戶，A 公司是外國機構的調查對象，媒體傳出其收受來自 B 公司資金的不利消息，而據稱 B 公司又涉嫌賄賂外國公職人員。同一時間，A 公司的實質受益人力求清算銀行帳戶。CPIB 因應 STR 尋求外國主管機關釐清資訊，確定有合理理由可相信 A 公司銀行帳戶中的資

金與犯罪所得有關。為此，調查過程中扣押 A 公司約 1,600 萬美元的銀行帳戶，撰寫本報告時，該案仍在調查中。

金融情報中心發現的逃漏稅案件成功追討 200 萬星幣

426 新加坡稅務局 (IRAS) 收到 STRO 的財務情報後對此案進行調查，早些時候，STRO 收到有關 L 先生的可疑交易報告 (STR)，其經常在個人銀行帳戶中存提大量款項，每次存入款項後，都會立即提領出類似金額。

427 STRO 發現 L 先生是 H 公司的董事，與多份大額通貨交易報告 (CTR) 和現金流動報告 (CMR) 相關聯。由於存在大量現金交易，STRO 懷疑 L 先生可能利用個人帳戶與多個實體進行業務交易，進而可能逃稅。

428 L 先生和其妻是 H 公司的董事，H 公司從公司銀行帳戶向海外實體支付款項，L 先生聲稱這筆款項是 H 公司營收的扣除額，如此一來即可減少稅金。H 公司無法就該筆扣除額提出充分佐證，也無法合理解釋這些付款是如何從公司所得營收中產生。未獲准且無證據的扣除總額為 \$1,170 萬，IRAS 追回超過 200 萬星幣的稅款。

429 IRAS 還發現 L 先生未申報其獨資企業 \$877,000 的營收，因此追討約 \$133,000 的額外稅款。

根據可疑交易報告扣押外國前置犯罪所得

- 430 STRO 接獲一家銀行提交的 STR，通知 M 人士從海外一名被害人收到兩筆涉嫌詐欺資金轉帳，共計 112,000 美元；匯款後，M 人士在同一天提領出 48,000 星幣的現金。由於 M 人士是新加坡的外籍家庭幫傭，因此受款銀行認為交易方式相當可疑。
- 431 從 STRO 對車手犯罪趨勢的延伸到金融產業，以及在 STROLL 系統發布的詐欺性資金移轉的犯罪警示，促使受款銀行注意到交易模式似乎非常符合車手洗錢行為的操作方式，因而向 STRO 提交 STR。
- 432 憑藉該資訊揭示外國前置犯罪可能造成的洗錢行為，STRO 在一天之內將該資訊轉交給新加坡的相關執法機關，調查人員展開洗錢調查，並立即從 M 人士的銀行帳戶中扣押剩餘的 88,229 星幣。STRO 及時轉介，使得國內機構能夠找到證據以識別受款銀行帳戶的所有權人並追蹤犯罪所得，進而在其銀行帳戶中沒收 88,229 星幣。
- 433 M 人士因不當收受贓物和洗錢罪而遭定罪，並被判處 8 個月徒刑。

泰國

- 434 AMLO 接獲銀行的 STR，指出 P 先生的情婦 S 女士進行多筆現金存提款交易，金額涉及 1-190 萬泰銖，且大都取小額紙幣，藉此規避向 AMLO 申報。根據 AMLO 的調查，發現這對男女在多家銀行共有 70 個

帳戶，整體金額相當高，此外還發現，P 先生有吸毒記錄，而 S 女士沒有此類記錄。AMLO 將財務分析報告分發給泰國皇家警察總署肅毒局（NSB），以採取進一步行動。

NSB 而後展開調查，發現這對男女是大毒梟，與泰國的少數族群 WA 有直接接觸。後來 NSB 佯裝要購買 74 公斤的海洛因，最後成功逮捕這對男女和三名其他共犯，除沒收 74 公斤的海洛因外，還沒收價值約 15,463,520 泰銖的泰銖現金、總計 114,251 美元的美元現金和價值約 12,224,993 泰銖的銀行帳戶。之後，AMLO 人員、NSB 人員和 ONCB 人員一一搜查 13 戶據信為這對男女處置毒品收益的人家，共查獲約 7,325,810 泰銖的現金和 9 張價值高達 39,124,923 泰銖的銀行存摺以及許多車輛。

6. 公私部門合作計畫

澳洲

435 澳洲的金融科技聯盟（FA）是金融情報中心 / 私部門的聯合機構，旨在加深在開發金融情報和共享風險資訊方面的合作。FA 於 2017 年成立，旨在實現三個情報目標：

- 協助私部門合作夥伴更輕鬆識別和申報可疑交易
- 協助執法夥伴進行調查
- 協同學術界以建立知識並收集見解。

巴拿馬文件

436 利用 FA 識別：

- 國內各方如何在金融中心使用國際第三方中介機構（有哪些機構），而又無須直接與避稅天堂進行交易，
- 第三方支付服務如何為空殼公司提供中介和服務。

437 這種新的智慧型功能減少了分析「天堂文件」（Paradise Paper）資料所需的時間。

兒童剝削

438 執法單位的主題專家借調至行動小組，向小組成員介紹剝削兒童的財務特性；由產業和執法 / 情報單位共同設計的一份情報報告中指出，向易受兒童剝削的地點支付小額國際款項，是最明顯的犯罪跡象，有鑑於此，產業成員應致力加強交易監控和持續進行的客戶

盡職審查，藉此識別個人和活動，以便進一步及早發現這類指標。

439 透過這項行動，為執法和合作夥伴機構提供更可靠的資訊，能用於辨識轉介目標。AUSTRAC 還對可疑事務報告中的已識別指標進行自動分析，該過程可發現以前未知的目標，這些目標提出涉嫌購買兒童剝削資料。

440 此外，還編寫了一份未分類版本、標題為「金融科技聯盟 - 打擊兒童剝削背景說明資料」的報告，並已發布給國外讀者。

車手

441 這項行動的目的是發展偵測可能招募為車手之人的能力，並向其他私部門和政府夥伴近乎即時地傳遞相關資訊，以識別新的被害人。

442 與私部門即時共享資訊：

- 使資金能夠在流到境外前有效阻擋下來，且應設立自動警報流程，俾使申報實體可採取行動來阻止資金
- 使用支援服務（例如 iDcare）進行聯繫並提供建議，協助無意中被招募為錢車手的人。
- 識別車手網絡的高風險帳戶、司法管轄區、實體和參與者，
- 識別執法線索以及瞭解車手招募網絡的特性，同

時藉助國際金融情報中心的合作，識別國際車手網絡。

馬來西亞

資恐公私部門夥伴關係

- 443 自 2017 年 1 月以來，金融情報中心、風險管理計畫和高風險金融機構之間已建立起一個平台，旨在用於分享有關資恐行動情報的資訊。各方之間定期舉辦會議和活動，共享有關新興資恐風險和方法的資訊，並針對個人和團體進行聯合分析和監督。
- 444 該倡議取得積極成果，包括與資恐相關的 STR 數量增加（比 2016 年增加了 400%），隨後向 RMP 揭露的金融情報也有增加趨勢。
- 445 RMP 體認到該平台的重要性以及向其揭露的金融情報品質有所提升，這有助於增進對恐怖主義和資恐的調查以及防範恐怖主義行為。

7. 縮寫對照表

AML	防制洗錢 (Anti-MoneyLaundering)
AMLC	防制洗錢理事會 (菲律賓) (Anti-Money Laundering Council)
AMLO	洗錢防制辦公室 (泰國) (Anti-Money Laundering Office)
APG	亞太防制洗錢組織 (Asia/Pacific Groupon Money Laundering)
ATM	自動提款機 (Automated Teller Machine)
AUSTRAC	澳洲交易報告暨分析中心 (Australian Transaction Reportsand Analysis Centre)
BCR	邊境貨幣報告 (Border Currency Report)
CDD	客戶盡職審查 (Customer Due Diligence)
CFT	打擊資恐 (Counteringthe Financing of Terrorism)
CTR	可疑交易報告 (Cash/Currency Transaction Report)
DNFBP	指定之非金融事業及人員 (Designatednon-financial businesses and professions)
EAG	歐亞小組 (Eurasian Group)
EDD	加強客戶審查措施 (Enhanced Due Diligence)

EFT	電子資金轉帳 (Electronic Funds Transfer)
ESAAMLG	東非和南非洗錢防制小組 (Eastern and South African)
FATF	防制洗錢金融行動工作組織 (Financial Action Task Force)
FIU	金融情報中心 (Financial Intelligence Unit)
FSRB	區域性防制洗錢組織態樣專案
FTF	外國恐怖主義戰士 (Foreign Terrorist Fighter)
IFTI	國際基金交易指示 (International Funds Transaction Instruction)
JAFIC	日本金融情報中心 (Japan Financial Intelligence Center)
KYC	認識客戶政策 (Know Your Customer)
LEA	執法機構 (Law Enforcement Agency)
ML	洗錢 (Money laundering)
MLA	司法互助 (Mutual Legal Assistance)
MTO	資金移轉營運商 (Money Transfer Operators)
NBI	國家調查局 (菲律賓) (National Bureau of Investigation)

NRA	國家風險評估 (National Risk Assessment)
PEP	重要政治性職務人士 (Politically-exposed person)
STR	可疑交易報告 (Suspicious Transactions Report)
TF	資恐 (Terrorist Financing)
UNODC	聯合國毒品暨犯罪辦公室 (United Nations Office on Drugs and Crime)
VAT	增值稅 (Value Added Tax)

APG 2018 年度態樣報告

如欲再製本出版品之全部或部分內容，
應向下列單位提出許可申請：

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

電話：+61 2 9277 0600
電子郵件：mail@apgml.org
網頁：www.apgml.org

©2018 年 7 月 / 保留一切權利

本出版品業經 APG 秘書處授權，由中華臺北行政院洗錢防制辦公室譯為中文，如有出入以公布於 APG 官網 :www.apgml.org 之英文版為準。

行政院洗錢防制辦公室 2021 年 12 月印製