APG年度態樣報告

亞太防制洗錢組織

2019

洗錢和資恐的方法和趨勢

亞太防制洗錢組織
2019 年 8 月

目　錄

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）機構。APG 編製有關洗錢（ML）和資恐（TF）方法的區域態樣報告，協助政府和其他防制洗錢 / 打擊資恐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以因應威脅。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 協同防制洗錢金融行動工作組織（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。這些報告旨在協助 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、不動產仲介商等）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。蒐集到的資訊不僅奠定了案例研究的基礎，也為選擇和設計深入研究特定態樣主題提供了依據，亦為參與 APG 態樣工作的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蒐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布。

2018-2019 年的態樣

6 APG 委由 APG 營運委員會進行態樣工作，該委員會目前由印度和紐西蘭擔任聯合主席。

1. APG 在 2018 年至 2019 年進行的研討會和專案

1 本節簡述了 APG 在 2018 年 7 月至 2019 年 6 月之間進行的態樣相關工作。

1.1 APG 的態樣研究專案

人口販運和人員偷渡專案（第二階段）

2 此專案的第一階段是聚焦於人口販運（HT）的 FATF/APG 專案，已於 2018 年 7 月完成（見本報告以下章節：*FATF 和區域性防制洗錢組織態樣專案 /FATF 態樣專案*）。

3 第 2 階段是 APG 區域專案，其以第 1 階段為基礎，包括有關 HT 和人員偷渡（PS）的須知事項。此專案著重於如何支援 HT 及 PS 控管工作的執行，包括公民社群等各種公 - 私合作夥伴關係。

4 HT 和 PS 區域研討會於 2019 年 4 月 8 日至 10 日在印尼萬隆舉行，聚焦於如何落實公共 / 私營 / 公民社群夥伴關係，以防制 HT 和 PS 問題。該研討會由 APG、PPATK 和 AUSTRAC 共同主辦，共有來自 12 個司法轄區、國際組織、私營部門、非政府組織和公民社群的 64 位代表與會。該專案預定於 2020 年結束。

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，（包括來自組織犯罪所得），不論資恐活動是由個別恐怖分子或由恐怖組織所為（請見本報告以下章節：*EAG– 打擊洗錢和資恐歐亞小組*）。

1.2 2018 APG/EAG 聯合態樣與能力建構研討會

6 每年，APG 態樣研討會都會召集來自調查和起訴機構、金融情報中心（FIUs）、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。

7 APG 與 EAG 於 2018 年 12 月 3 日至 5 日在俄羅斯新西伯利亞合辦 2018 年態樣學研討會，與會者包括 41 個 APG/EAG 轄區的約 250 名代表（其中約 130 名來自 APG 成員）、8 個國際組織和 21 名來自 APG/EAG 的代表私營部門、非政府組織和公民社群。

8 研討會包括一次全體會議（第一天和最後一天）和三場為期兩天的同步會議，主題涵蓋：（i）資恐和犯罪所得（包括組織犯罪）；（ii）與虛擬資產相關的風險和調查技術；（iii）HT 和 PS。

2. FATF 和區域性防制洗錢組織態樣專案

9 報告的本節簡述了 FATF 和其他區域性防制洗錢組織（FSRBs）在 2018 年 7 月至 2019 年 6 月之間發布的態樣報告。

2.1 FATF 態樣專案

人口販運產生的資金流（第一階段）

10 近年來，HT 和移民偷渡的受害者人數繼續大幅增長。2018 年 8 月，FATF 和 APG 發布一份報告，宣導如何辨別疑似人口販運（目的為性剝削或強迫勞動）的財務活動資訊，並加深認識器官販運的利潤潛力。該報告也重點介紹了 HT 和資恐之間的潛在聯繫。

11 報告強調在建立互助合作的重要性，尤其著重在公共部門、私營部門、公民社群和非營利社區之間合作發揮專業、能力和夥伴關係，當中的私營部門和金融機構尤其扮演著第一線的角色。

12 國家或區域的創新舉措已經證明防制洗錢 / 打擊資恐措施及其執行如何有助於制止這種犯罪。但是在全球，各界仍不夠關注如何運用財務資訊來偵查、阻斷和瓦解人口販運網路。該報告提供了良好實務，有助於司法轄區針對人口販運的洗錢和資恐問題制定因應措施，

其中包括警訊指標，以利識別負責處理相關犯罪所得的洗錢份子。

透明度和實質受益權

13 雖然企業體（例如公司、基金會、合夥企業和其他類型的法人和安排）對於支持商業和創業活動很重要，但也可能被濫用以掩蓋對不法所得資產的所有權和控制權。2018 年 7 月，FATF 和艾格蒙聯盟發布聯合報告，針對隱瞞實質受益權的相關漏洞進行評估，支援公私部門進一步分析風險。

14 該報告採用 FATF 全球網路中 34 個不同司法轄區提供的 100 多份案例研究、執法和其他專家的經驗、私營部門意見及公開研究和情資報告，以識別犯罪分子用於隱瞞實質受益權的方法，並且分析了有關實質受益權的漏洞，尤其關注專業中介機構的參與。

15 該報告強調，法人（主要是有限責任公司或類似機構）的成立程序過於簡單，使其特別容易成為漏洞，用於建立複雜的法人所有權結構，這種手法經常涉及空殼公司。此外，在這類結構的安排中，信託和公司服務業者經常扮演要角。使用代名董事和股東（不論是否正式）都會使所有權人或個人無法察知洗錢犯罪所得，進而加劇風險。專業中介機構經常發揮的角色之一，是協助建立或操作某種結構來掩飾實質受益權（不論是共謀或無意之間）。

專業洗錢

16 專業洗錢者（PML）專門為不法份子和組織犯罪集團的非法活動提供洗錢服務。FATF 在 2018 年 7 月發布一份報告，研究專業洗錢使用的技術和工具，幫助司法轄區予以識別和瓦解。根據 FATF 全球網路提供的案例研究，該報告指出了各種不同的洗錢機構和網路，包括資金運輸、現金控管業者網路、代理機構網路等。

17 該報告發現專業洗錢者使用了多種洗錢工具和技術，貿易洗錢、帳戶管理機制、地下銀行和替代銀行平台。為了使其活動具有合法性，專業洗錢者可以與貪污人士合作，除了犯法的洗錢活動外，也提供其他合法專業服務（例如銀行家、律師、會計師）。專業洗錢者通常為多名不法份子或犯罪組織工作。因此，成功起訴專業洗錢者可能會影響多個不法客戶的活動。

18 專案團隊也編製該報告的非公開版本，探討獨特的調查工具和技術，其已證實能夠有效偵測和阻斷專業洗錢者。

資恐阻斷策略（非公開）

19 2018 年 10 月，FATF 通過一份關於資恐金流阻斷的非公開報告。瞭解這些資金的流向不只對調查而言很重要，也攸關確保主管機關能否在恐怖襲擊發生前果斷採取決預防性措施、阻斷恐怖活動。

20 該內部報告以 FATF 全球網路的 33 名成員和觀察員的

資料為基礎，為主管機關提供了一系列阻斷工具和全面性策略的綜合方案，有助於改善國內打擊資恐行動，並找出權責機關可以有效合作的新方法，進而達到阻斷資恐活動的目的。

伊斯蘭國和「基地」組織及其附屬機構融資最新動態（2017年10月）– 非公開

21 2015年2月，FATF發表了關於伊拉克和黎凡特伊斯蘭國（ISIL）融資活動的綜合報告。自那時以來，FATF每年根據全球網路提供的資訊進行三次非公開的定期更新，這些更新也涵蓋蓋達組織、伊斯蘭國和蓋達組織的附屬組織。在2018年10月和2019年6月，FATF公開說明伊斯蘭國喪失領土後籌資方式的改變。

識別並評估資恐風險

22 識別、評估和瞭解資恐風險是瓦解和破壞恐怖分子網路的重要環節。2019年7月，FATF發布根據FATF全球網路的經驗發布一份指引，為司法轄區提供識別和評估資恐風險的最佳實務和考量。

非法利用虛擬資產的洗錢和資恐用途 - 透過調查和沒收來因應挑戰（非公開）

23 虛擬資產（VA）是具有獨特性質的資產類別，會阻礙財務調查和相關的沒收程序，進而阻礙主管機關利用這些技術偵查、調查和起訴洗錢/資恐犯罪的能力。2019年6月，FATF通過一項非公開指引，為從業人員

提供最佳實務，支援其針對疑似涉及 VA 的洗錢 / 資恐活動進行有效的調查。該報告也提供案例研究，以及主管機關可用來沒收非法 VA 的技術。

2.2 CFATF– 加勒比防制洗錢金融行動工作組織

24 CFATF 進行了多項態樣報告，包括：使用信託和公司服務業者的洗錢活動（2010 年）；人口販運和移民偷渡（2014 年）；非法彩票（2016）；現金和流通票據的變動（2016 年）；以及小型武器和彈藥的擴散（2016 年）。

CFATF 去風險態樣專案（2019）

25 CFATF 在 2018 年 6 月至 2019 年 4 月進行一場去風險（de-risking）演習，旨在突顯此情況對於該區域的負面影響。這項工作分兩個階段進行，包括對中央銀行和民間金融機構進行資料蒐集。

26 對於藉由資料蒐集所接收的資料分析顯示下列資訊：

27 根據 71% 的區域中央銀行表示，去風險是一種日益增加的威脅。此外，上述央行中有 90% 認為「去風險」是一種威脅，會造成營運成本增加、支付鏈延長等不利因素，已經且不斷在影響其營運能力。

28 根據總共 227 家金融機構的回饋意見，有 158 家（相當於 70%）表示其業務受到去風險化的負面影響（通匯銀行業務關係終止 / 限制），主要原因是通匯銀行難

以向客戶提供服務 / 產品，並且提高了他們的風險評級。其他原因包括：難以找到替代往來銀行；並且提高了行政費用。

29 對於終止 / 限制金融往來關係，金融機構提出的兩項主要理由是：利潤微薄和法遵成本過高。但是在許多案例並未提供任何理由。其他原因包括：防制洗錢 / 打擊資恐程序出現問題；往來銀行停止提供產品 / 服務；認為司法轄區存在風險；通匯銀行的風險緩解策略；風險胃納較低；業務類別與通匯銀行的策略不一致，並且擔心在本國司法轄區受到法規制裁。

30 在所屬轄區已知的通匯銀行當中，有一半位於北美，三分之一在歐洲。其他國家位於亞洲、加勒比海地區、非洲和南美。

31 受影響的產品和服務包括電匯、貸款 / 信用狀、支票清算和結算、電子遊戲 / 線上博弈、現金管理服務、信用卡處理、匯款業務和行動銀行。

32 在過去三年中，一些銀行（55 家銀行）終止了通匯銀行業務關係。這些銀行中的大多數（80%）失去 1 至 3 個通匯銀行業務關係，而 11% 失去 7 至 10 個通匯銀行業務關係。

33 去風險化報告在 CFATF 在 2019 年 5 月的全體會議中以內部文件的形式通過審查。

2.3 EAG– 打擊洗錢和資恐歐亞小組

資助恐怖主義和犯罪所得（包括組織犯罪）

34 資恐相關問題多年來一直是 EAG 議程中的常設主題，且是 EAG 及其成員國公認的首要之務。迄今為止，EAG 已經完成了許多有關打擊資恐的態樣學專案。最新一項是與 APG 的聯合專案（目前正在進行中），涉及資恐與組織犯罪之間的聯繫。主導這項專案的三個司法轄區是孟加拉、印度和俄羅斯。UNSCR2195 和 2322 構成此專案的基礎。

35 這項專案的目標是：

- 更加瞭解個別恐怖分子和恐怖組織將犯罪（包括組織犯罪）所得用於資恐的程度和方式。
- 確認組織犯罪等非法活動如何蒐集、轉移資金並將其用於恐怖活動。
- 確認最能有效偵測、調查和防止恐怖分子和恐怖組織使用犯罪所得的實務做法。

36 資訊蒐集分為兩個階段，第一階段是發送調查問卷。第二階段是 2018 年 12 月在俄羅斯新西伯利亞舉行的 EAG/APG 聯合態樣研討會，期間舉行分組會議，專門探討資恐與組織犯罪之間的聯繫。

37 聯合態樣學研討會的交流結果以及問卷答案是專案報告初步結論的基礎，並交由 APG 和 EAG 的 2019 年會進行討論和審核。

2.4 GIABA– 西非政府間防制洗錢行動小組

西非地區的認識客戶政策 / 客戶審查措施及金融普惠

38 本報告是直接由政府間防制洗錢行動小組（GIABA）在 2016 年 9 月開始進行的研究成果，延續先前在 2013 年的一項金融普惠性的相關研究。該研究旨在瞭解並因應認識客戶（KYC）/ 客戶審查（CDD）的洗錢和資恐防範措施在執行上的挑戰，同時適當考量金融普惠的要求。已根據研究結果提出建議，協助 GIABA 成員國的有關主管機關遵循 FATF 建議和評估方法（修訂版）的宗旨和精神，據以規劃有效的 KYC/ 客戶審查架構，以促進金融普惠目標。此報告可至 GIABA 網站取得：https://www.giaba.org/reports/typologies/reports.html。

西非藥品仿冒所衍生的洗錢活動

39 這項研究旨在瞭解西非藥品仿冒所衍生的洗錢活動性質和程度。所採用的方法包括：選擇 4 個司法轄區（象牙海岸、奈及利亞、塞內加爾和多哥）進行深入的全國研究，而其餘司法轄區則進行問卷調查。從司法轄區報告、成員國對問卷的答覆以及執法機關提供的案例研究中分析了洗錢與藥品仿冒之間的聯繫。此報告可至 GIABA 網站取得：https://www.giaba.org/reports/typologies/reports.html。

2.5 艾格蒙聯盟

新興金融技術、洗錢和資恐：虛擬通貨態樣

40 在過去的12個月中，艾格蒙聯盟完成了許多重要專案，其中包括一個名為「*新興金融技術，洗錢和資恐*」的態樣專案*：虛擬通貨的態樣學*。金融情報中心負責人於2018年5月核准此報告，並允許分發給所有金融情報中心、相關申報實體、權責執法機關和艾格蒙聯盟觀察員。

隱瞞實質受益權報告（與FATF聯合發表的文件）

41 FATF/艾格蒙聯盟的這份聯合報告從全球角度評估法人、法律協議和專業中介機構如何幫助罪犯隱瞞財富和非法資產。該報告旨在幫助金融情報中心、金融機構和其他專業服務提供者的國家主管機關瞭解其所面臨的風險及其性質。

貪污案件系列指標的專題文件

42 艾格蒙聯盟在文件中彙編一系列指標，有助於識別交易或與客戶互動中的貪污和及相關犯罪所得的洗淨活動。本文的最終目標是提升金融情報中心可用的情報品質，此願景有待情報部門應與執法機關、金融機構和其他前線申報實體進行協調，以增進對可疑交易和貪污嫌疑活動的識別能力。

43 就此主題而言，艾格蒙聯盟體認到其他國際組織所展開任務的重要性，包括FATF、世界銀行、聯合國毒品

和犯罪問題辦公室以及國際刑警組織，而在識別可疑交易、貪汙或其他前置犯罪之所得時，也必須將這些工作成果納入考量。

44 本文件於 2018 年 9 月 24 日至 27 日在雪梨的艾格蒙聯盟全體會議上獲得金融情報中心首長核准，但仍非詳盡的完整版本，將根據艾格蒙聯盟成員、觀察員、國際合作夥伴組織、不同權責機關及申報實體的反饋意見進行修訂和補充。

探討金融情報中心營運獨立性和自治性的 ECOFEL 文件

45 本文件旨在幫助政府（決策者）、金融情報中心和其他主要利害關係人識別和理解金融情報中心營運獨立性和自治性的決定性特徵。

46 本文旨在回應金融情報中心（EG）的艾格蒙聯盟成員，該團體要求編製一份最佳實務指引，說明金融情報中心應具備哪些特徵，方可最有效促進獨立性和自主性。本文著重說明有助於促進金融情報中心的運作獨立性和自治性特徵，既無意設定新標準，也無意討論實現這些特徵的策略。

3. 洗錢和資恐趨勢

47 報告的這一部分概述洗錢和資恐的趨勢，包括 APG 成員和觀察員所執行研究的公開資訊。

3.1 APG 成員和觀察員對洗錢 / 資恐方法和趨勢進行的研究

澳洲

非營利組織與資恐警訊指標 2018 年報告

48 2018 年，來自澳洲的 8 家金融情報機構（澳洲交易報告和分析中心）、汶萊（汶萊金融管理局金融情報中心）、印尼（金融交易報告和分析中心）、馬來西亞（馬來西亞國家銀行）、紐西蘭（紐西蘭警政署金融情報中心）、菲律賓（防制洗錢理事會）、新加坡（可疑交易報告辦公室）和泰國（防制洗錢辦公室）合作制定和編製區域危險訊號指標報告，力求達成年度打擊資恐峰會的任務目標。

49 該報告提供一系列警訊指標，涉及東南亞、澳洲和紐西蘭境內資恐濫用風險較高的非營利組織（NPO），旨在協助申報機構、國家機關和 NPO 更有效識別和緩解可能與當地資恐活動掛勾的可疑活動。

50 這些指標的參考資訊包括案例研究、區域金融情報中心、執法機關及 NPO 監管機構提供的情報。另有若干

資訊來自負責處理 NPO 財務事宜、且有義務通報可疑活動的金融機構。

51 詳細資訊請見 https://www.austrac.gov.au/sites/default/files/2019-06/npo-red-flag-indicators.pdf。

現場博彩業者風險評估

52 在 2018 年末，AUSTRAC 針對澳洲現場博彩業的整體洗錢 / 資恐風險發布一項風險評估。

53 經確認，由現場博彩業者提供的服務可能會助長輕度的洗錢和逃稅，但未觀察到任何資恐記錄。成長衰退性質和其他一系列因素，使該產業較少遭濫用於洗錢和其他犯罪的漏洞，因此得到了低風險的評等。可以確定的是，營業額相對較高的現場莊家（包括提供線上投注帳戶的莊家）較其他實體更容易遭濫用於犯罪活動。

54 風險評估提供了詳細資訊，以幫助該產業理解和因應現場博彩業者服務衍生的風險。請循以下連結存取風險評估資料：https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/course-bookmakers-money-laundering-and-terrorism-financing-risk-assessment

退休金部門指引

55 2018 年 12 月，AUSTRAC 發布了關於退休金部門的指引，內容涉及如何將 2006 年*《防制洗錢和打擊資恐法*

*案》*的要點應用於其業務中。

56 本指引舉出若干僅供參考的工作範例，突顯如何運用防制洗錢 / 打擊資恐綜合方案來識別、減輕和管理退休金部門的特定洗錢 / 資恐風險。這些工作範例可為業者提供洞見，使其瞭解如何搭配自身業務和風險概況，靈活地運用防制洗錢 / 打擊資恐綜合方案。

57 請循以下連結存取該指引：https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/industry-specific-guidance-superannuation-sector

加拿大

58 FINTRAC 資恐評估：2018 年 -http://www.fintrac-canafe.gc.ca/intel/assess/tfa-2018-eng.asp

59 FINTRAC 針對貿易及貨幣服務業 PML 的警戒任－http://www.fintrac-canafe.gc.ca/intel/operation/oai-ml-eng.asp

斐濟

60 斐濟金融情報中心針對洗錢 / 資恐的方法和趨勢進行了非正式研究。斐濟金融情報中心繼續發布年度報告以提供相關資訊。

61 斐濟金融情報中心年度報告收錄了有關可疑交易通報的案例研究，以及在斐濟成功起訴的洗錢案例研究。這些報告也介紹新興、持續和衰退的洗錢趨勢。年度報

告可至斐濟金融情報中心官方網站取得：www.fijifiu.gov.fj

中國香港

62 香港聯合財富情報組（JFIU）發布了有關電子郵件詐騙的策略分析報告，針對帳戶資訊、帳戶活動以及公司董事變更、帳戶簽署人和測試支付等主題進行了縝密分析。該報告可透過以下連結存取 -https://www.jfiu.gov.hk/info/doc/Strategic_Analysis_Report_on_Email_Scams.pdf

印尼

63 印尼政府對洗錢 / 資恐方法和趨勢進行定期研究，每種研究主題各不相同。該研究每年進行一次。印尼政府也可能進行非正式研究，來因應洗錢 / 資恐方法和趨勢相關的最新或特殊問題。但是，這些研究僅在內部發表，而且僅分發給限定的外部實體。

64 過去，印尼曾經針對洗錢 / 資恐方法進行研究，內容涉及前置犯罪、所用交易方法，以及所通報當事方的背景特徵。

65 關於洗錢 / 資恐方法和趨勢的最新研究包括 2017 年洗錢案件的法院判例態樣。研究顯示，在 2017 年判決的案件中，主要的前置犯罪與毒品有關。主要的交易模式是透過 ATM 轉帳、經由櫃員存入現金以及超額下單。

日本

66 日本犯罪收益移轉防止對策室（JAFIC）網站上發布了該機構年度報告，詳細介紹防制洗錢 / 打擊資恐統計數據、案例研究和趨勢。

馬來西亞

國家風險評估（NRA）

67 馬來西亞第三次 NRA 已於 2018 年 7 月完成並獲得國家反洗錢國家協調委員會（NCC）的背書認可。NRA 方法已進行改良，方法包括擴大範圍和修改資料點。在威脅風險評估和產業風險評估（FI 和 DNFBPs）之外，NCC 也審查通過了 NRA 中的國家 NPO 資恐風險評估。

68 2018 年 NRA 指出的高風險犯罪與 2013 年的發現相似，亦即詐欺、走私、貪污和毒品販運，不同之處在於組織犯罪取代了避稅，進入風險最高的前 5 種犯罪之列。所有高風險犯罪紀錄皆載明大量調查資料、涉嫌犯罪所得金額，以及從中得出的金融情報數量。

69 NCC 已在 NRA 流程中確認需要改進的領域，以減輕已知的新風險。有鑑於此，現行的《2016-2020 年國家防制洗錢 / 打擊資恐 / 中央公積金策略計畫》（NSP）將進行審查和重新校訂，納入現有行動計畫的進展，新的緩解策略（包括發現的新差距）以及國際標準。

70 另一方面，計畫審核通過之後展開了交流和宣導活動，特別是向申報機構進行簡報。

警訊和態樣簡介

71 在 2018 年和 2019 年，金融情報中心就以下犯罪發布了 5 項警告和態樣簡介，分別是資恐（2018 年 4 月）、資助武擴（2018 年 5 月）、貪污（2018 年 6 月）、詐欺（2018 年 10 月）和毒品販運（2019 年 1 月））。這些犯罪是經過 NRA 根據私營部門需求確認的高風險犯罪。文件限量已分發給申報機構（RI），其目的為：

- 提供洞見並提高對犯罪的認識 - 趨勢、技術、方法和渠道；
- 增強和促進申報機構對態樣的認識和理解；
- 協助申報機構識別客戶顯現的警訊 / 指標和所涉及的金融交易，從中識別違法行為；
- 使申報能夠及早發現，以阻斷與犯罪相關的特定活動，並進一步提高可疑交易報告（STR）的品質。

紐西蘭

通過專業把關者和匯款者洗錢

72 NZFIU 展開一項聯合專案，以查明其服務被罪犯濫用於洗錢的匯款者和專業把關者（律師 / 會計師 / 不動產經紀人）。相關方法包括審查自 2017 年 1 月起的 18 個月內紐西蘭警察（NZP）逮捕組織犯罪的案例，查明這些案件中協助犯罪所得轉移的實體，並將其輸入分析圖表以進行進一步分析。然後將每個實體的 NZFIU

資料轉換為分析圖表，並分析其資金流量和鄰近度，以識別有利於最大交易量和最大金額的實體，藉此判斷實體參與轉移犯罪所得的情形。

73 專案提出的關鍵主題總結如下：

74 關鍵節點：幾乎可以肯定有大約 65 個紐西蘭公司、個人和金融服務提供者組成的核心網路已被用於洗淨組織犯罪活動所得。自 2016 年以來，此「關鍵節點」網絡得到了數間位於奧克蘭匯款業者（MR）支持，並協助進行價值超過 2 億美元的可疑交易。這些資金中很大一部分可能來自毒品犯罪、詐欺和其他嚴重罪行。

75 匯款業者網絡違反防制洗錢 / 打擊資恐規定的文化：大多數列為對象的匯款業者都曾經持續違反防制洗錢 / 打擊資恐義務而引起了警察和內政部的注意；包括未能執行客戶審查、進行交易監控或提交可疑交易報告。這些漏洞幾乎肯定會被犯罪分子用來將非法資金投入合法經濟之中。

76 匯款業者的相互依賴性：匯款業者彼此密切合作，使用普通的銀行帳戶集中資金，並雇用普通的現金運送者來為其客戶進行一系列非法和合法交易。他們使用非正規的價值移轉和交易抵償的複雜業務模式，這使得非法資金很容易混入合法資金。這通常會妨礙執法部門有效追蹤資金流向的能力，因為非法資金通常在委託方客戶不知情的狀況下用來完成完全合法的交易。

77 雇用現金運送者：現金運送者依匯款業者委託收取現金，並透過紐西蘭銀行發放資金。他們是洗錢的高風險群，原因在於交易大量現金，而且未定期對所持有資金的來源或實質受益人進行盡職調查。幾乎可以肯定的是，一些現金運送者直接向組織犯罪集團收取現金，可能成為可行的調查目標。

78 資金移轉方式：組織犯罪集團雇用專業協助者擔任合法經濟的把關者。非法資金一旦經由協助者置入金融系統後，就會與合法資金混雜，並透過信託、財產購買或單純以現金支付。調解人廣泛使用交易抵償和現金池掩蓋資金流向，並阻礙執法機關反向追蹤資金流的來源。

菲律賓

加強防制洗錢監督，伴隨金融技術的進展

79 2018 年 8 月 21 日，防制洗錢理事會（AMLC）核准進行有關菲律賓境內虛擬通貨（VC）洗錢防制法規環境的研究。該研究旨在初步評估授信虛擬通貨交易所的交易概況，尤其關注可疑交易、涉嫌非法活動的客戶以及大額交易。風險投資交易須遵守菲律賓央行（BSP）2017 年 2 月 6 日發布之第 944 號通令（《虛擬通貨交易所準則》，涉及 BSP 第 942 號通令《非銀行金融機構規章》）提供金融服務，尤其是支付和匯款業務。該研究結果已發布在 AMLC 網站：http://www.amlc.

gov.ph/images/PDFs/Study%20on%20VC.pdf

80 該研究對 2017 年 3 月 6 日至 2018 年 4 月 10 日的 BSP 授信虛擬通貨交易的大額通貨交易報告（CTR）和可疑交易報告（STR）進行描述性分析，涉及 2014 年 4 月 28 日至 2018 年 4 月 6 日在其平台上執行的交易，總共產生 22,366 筆交易報告（包括 1,086 筆受轄交易報告和 21,280 筆可疑交易報告），總價值為 31 億比索（其中 24 億比索為受轄交易報告，7 億比索為可疑交易報告）。該研究發現，在 2017 年 2 月發布 BSP 第 944 號通令及後續於同年 9 月和 10 月核准虛擬通貨公司立案之後，虛擬通貨交易所 2017 年報告的交易量和金額均急遽增加。

81 BSP 制定虛擬通貨交易的監管架構，進而加強虛擬通貨相關風險的防範措施，例如對洗錢和資恐的控管、技術風險管理以及對消費者的保護。尤其是，將風險投資交易所納為受監管人（CP），可以更全面地監控可能涉及非法活動個人和實體的財務行為，並且在蒐集虛擬通貨交易所提交的陳詞以進行防制洗錢監控時，可以促成受監管人之間更緊密的協調和資訊共享。

非營利組織的風險評估

82 2018 年 11 月 28 日，AMLC 核准了 NPO 部門的風險評估，並授權將其分發給所有利益相關方。NPO 風險評估是根據 FATF 40 項建議中的第 8 項建議進行。AMLC

獲得 NPO 主管機關、證券交易委員會（SEC）和社會福利與發展部（DSWD）的支持。菲律賓非政府組織認證委員會（PCNC）和非政府組織網絡發展核心小組（CODE-NGO）在上述工作中也提供了寶貴的意見。

83 NPO 風險評估根據調查和實際案例、情資報告以及部門代表的意見，來介紹和分析 NPO 的洗錢 / 資恐風險。該產業的洗錢威脅經評估為中等；資恐威脅經評估為高 - 低。洗錢和資恐的漏洞評估等級為中等。雖然監管架構整體有效，但是法律和法規的執行仍然存在一些問題。

84 報告提出涉及公共部門和 NPO 部門的具體策略，旨在減輕 NPO 相關的洗錢和資恐風險。這些策略包括持續與主管機關和 NPO 進行接觸，採用風險導向法規、監督 NPO，以及加強政府與 NPO 之間的協調。

伊斯蘭國東南亞的自籌資金

85 東南亞打擊資恐工作小組（SEA CTF WG）成立於 2017 年第三次資恐峰會，曾調查伊斯蘭國和伊斯蘭國附屬團體在東南亞的融資情況。工作組分別編寫了四份報告：（a）伊斯蘭國在東南亞的資金籌措：區域環境、（b）東南亞伊斯蘭國的外部資金、（c）伊斯蘭國和東南亞其他高威脅恐怖組織的哈瓦拉交易商融資，以及（d）東南亞伊斯蘭國的自籌資金。上述報告是由各項主要專案團隊根據向 SEA CTF WG 成員蒐集的資

訊所進行之評估。

86 菲律賓的 AMLC 主導調查 ISIL-SEA 的自籌資金，以進一步瞭解並制定阻斷策略。自籌資金的報告指出，這些資金包括犯罪所得資金，例如綁架勒索贖金、勒索當地人口以及販毒或走私毒品。資恐自籌資金的另一種方法是通過合法來源，例如家庭援助、支持者的捐贈、商業利潤和合法收入。SEA CTF WG 成員和客座組織彼此分享伊斯蘭國同一陣線東南亞恐怖組織或威脅團體所使用自籌資金的相關資訊；分析可用的金融情報、機密和公開資訊；同意就最優先目標進行合作以制定阻斷策略（這可以透過分析師交流計畫進行）；並與執法機關或區域機構合作實施這些阻斷策略。

87 報告已提供給 CTF 峰會下的 SEA CTF 工作小組成員和金融情報顧問小組。

新加坡

ACIP 關於濫用法人和貿易洗錢的出版文獻

88 新加坡的公私合作夥伴關係組織「防制洗錢 / 打擊資恐產業合作夥伴（ACIP）」發表兩篇產業最佳實務文件，內容涵蓋法人濫用和貿易洗錢 / 貿易融資的態樣，包括該產業設立的預防措施，以及為減輕這些風險而採取的最佳實務。

89 請參閱以下報告：https://abs.org.sg/industry-guidelines/aml-cft-industry-partnership

3.2 洗錢或資恐類型與前置犯罪活動的關聯

斐濟

90 斐濟已於 2018 年 11 月開始對其 NRA 進行審查。審查的重點是更新對斐濟面臨的洗錢威脅和下列產業的洗錢活動威脅的評估：銀行、匯款服務提供者、會計師事務所、律師事務所和房地產經紀人。

91 販毒已成為洗錢的前置犯罪趨勢，而且金融情報中心正在與斐濟警察部隊調查員緊密合作，以協助分析毒品案相關財務概況並追查資產。

中國香港

案例研究 1

92 2015 年 10 月，香港海關調查香港銷售仿冒商品的集團。過程中發現多個小販攤位、展售間和倉庫涉及儲存和販賣仿冒商品。2016 年 1 月，海關拘捕 9 人，扣押總值 580 萬港元的仿冒商品。財務調查顯示，疑似因販售仿冒商品所得的大量現金已存入集團的個人銀行戶口，洗淨的黑錢總額為 575 萬港元。

93 2018 年 5 月，5 名集團成員被判偽造罪定讞。其中 3 人洗錢罪名成立，並被判處 11 至 26 個月徒刑。2018 年 12 月，法院下達一項沒收令，沒收三名主要成員持有的價值 156 萬港元的可變現財產。

案例研究 2

94 2017 年 3 月，香港海關展開一場禁毒行動，逮捕了一

對伴侶，並沒收了 4.6 公斤疑似大麻芽及 100 萬港元疑似毒品犯罪所得。財務調查顯示，這對伴侶洗淨涉嫌犯罪所得 540 萬港元。

95 於 2018 年 3 月，法院命令扣押價值 370 萬港元的可變現財產。2018 年 11 月，這對伴侶中的男性經審所有罪名成立，判處四年兩個月徒刑。

印尼

96 根據印尼最新的可疑交易報告統計，與洗錢相關的前置犯罪活動主要是詐欺、貪污和賭博，其中貪污最為嚴重。

日本

97 2018 年，與暴力團有關的洗錢案件（包括暴力團成員、員工及其他相關方）佔所有依《組織犯罪懲治法》判為洗錢案件的 12.3%。

98 暴力團常用的一種方法是以假名開一個銀行帳戶，以從詐欺和出售贓物中獲取犯罪所得。

99 一名涉嫌從事大麻走私活動的男子使用送貨到府服務，並安排客戶將總額約 160 萬日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。

馬來西亞

100 在驗證量化評估的初步結果期間，也對 NRA 的結果進行後續質性評估並提出結論如下：

- 貪污、詐欺和走私據信是與其他嚴重罪行關係最密切的三種犯罪活動。
- 經發現，非法毒品販運和人口販運是兩項嚴重罪行且據信與境外威脅有關。
- 詐欺據信是與受評估部門最相關的嚴重罪行，其次是貪污和逃稅。

紐西蘭

奧克蘭建築業的勞工剝削和移民詐欺

101 NZFIU 參與一場聯合機構調查，目標鎖定奧克蘭建築業中馬來西亞非法勞動力市場。該調查旨在查明可疑的移民犯罪，並阻斷奧克蘭建築業的非法市場。行動結束時，有 54 人被驅逐出境、36 人自願離開紐西蘭、有 15 人遭下達遞解令、190 人禁止在紐西蘭非法工作；起訴罪狀包括人員偷渡、身分詐欺、文件詐欺、協助和教唆、洗錢和逃稅。

102 NZFIU 對這項調查的貢獻著重於分析可疑活動報告（SAR）資訊和嫌犯銀行帳戶活動的財務狀況，以幫助識別犯罪網路及其他利害關係人。NZFIU 的分析顯示，資金在營建業者之間移轉，並從銀行提領現金支薪。也發現公司董事在違反簽證條件下經營業務，並查獲通過空殼公司匯入的資金。NZFIU 繼續以臨機的方式向調查小組提供資訊，以告知後續調查的可能線索。

巴基斯坦

案例研究 1- 搶劫 / 盜竊 / 贓物

案件背景：

103 SMARZ 先生是政府部門的一名員工，並在巴基斯坦 ABC 銀行開設了一個帳戶，透過線上存入和兌現支票獲得了高額資金。這項活動與他的個人資料不一致，銀行對他的帳戶活動感到懷疑。為了確認資金來源，該銀行嘗試撥打其所給予的手機號碼，並發信至其所提供居住地址，試圖聯絡 SMARZ 先生。電話聯繫不上，信件因無法投遞而退回銀行。由於驗證結果無效，ABC 銀行提出了可疑交易報告。在金融監察組（FMU）對可疑交易報告的分析中，發現嫌疑犯是政府部門的一名員工，薪水為 17,000 巴基斯坦盧比。但是另一方面，該員工正透過線上存入現金和 ABC 銀行各分支機構的兌現收受大量資金。自他開設銀行帳戶以來，透過該帳戶進行的活動總額約為 1700 萬巴基斯坦盧比。

104 在公開媒體資料中搜尋後，發現一位名叫 SMARZ 的人士因涉嫌參與銷售贓車及其他物品而遭維安部門逮捕。相關單位進行特別調查，試圖比對可疑交易報告所舉報的嫌犯資料，結果發現 SMARZ 先生在網路上提供個人手機號碼，從事緊急出售和交易二手車的業務。根據分析和金融活動概況，將金融情報提供給執

法機關以利調查盜竊、搶劫和可能的恐怖主義行動。

案例研究 2- 毒品走私 / 逃稅

案件背景：

105 匯兌公司針對三人頻繁且分散地購買外匯行為提出可疑交易報告。遭舉報的個人在不同的銀行中擁有多個帳戶。搜尋其中一名遭舉報個人的公開資料時，發現有負面新聞的紀錄。據報導，該人從巴基斯坦走私價值 700 萬英鎊的海洛因到英國，並被判入獄 20 年。他於 2005 年從監獄獲釋。從 2011 年起，此人在巴基斯坦開設了多個帳戶。這些帳戶位於各個城市，用於存放非法資金。此外，分析也顯示，雖然其他兩名嫌犯的帳戶營業額很高，但並未向聯邦稅收委員會申報所得稅。

作案手法：

106 嫌犯以尋常的手機號碼與他共犯聯繫，以分散方式購買了大量外幣，並將這筆資金運出了司法轄區。這些個人在不同的銀行有多個帳戶。據稱其中一名參與了海洛因走私活動。他在每家銀行揭露不同業務來分散營業額並逃避稅務機關稽查，進而巧妙地在不同城市的不同銀行開設了多個帳戶。他曾在不同的銀行提供過不同的業務資訊，並且在短時間內操作帳戶然後將其關閉。與他所陳述的業務概況相反，此人進行了多次高額交易。他在每個帳戶的整體交易模式啟人疑

竇，因為他持續在不同帳戶間移轉高額資金。雖然其帳戶營業額很高，但並未註冊國家稅號（NTN）。經判定，遭指控個人在不同帳戶之間存放並移轉毒品走私所得的非法資金。金融情報與執法機關關注所有方面的資訊，彼此共享金融情報，以調查可能的走私毒品和逃稅行為。

案例研究 3- 毒品走私

案件背景：

107 一則新聞報導反毒部隊（ANF）從一位搭乘廂型車的女士（「ABC」）身上繳獲其所持有的 2.4 公斤大麻，而「QRS」銀行依此資訊提出可疑交易報告。該銀行從消息來源蒐集了更多資訊，並在其分支機構中找到了一個匹配的帳戶。根據此資訊，QRS 銀行向 FMU 報告了可疑交易報告。

作案手法：

108 嫌犯 ABC 自 2003 年以來一直是 QRS 銀行 M 分行的附照片帳戶持有人。她自稱是一名家庭主婦。對帳單分析顯示帳戶僅有小額資金提出和存入。

案例四 - 貪污 / 逃稅

109 「Alpha」銀行和「Beta」匯兌公司針對 AX 先生和 JN 先生提出可疑交易報告，此 2 人分別是不同糖廠的所有者。嫌犯參與大量換匯交易，透過分散化的不同形式交易，蓄意違反巴基斯坦國家銀行的門檻。個

人在短時間內使用現金購買了高價值的美元，沒有任何明顯的經濟目的。同時，他們在 Alpha 銀行設置多個巴基斯坦盧比和外幣帳戶，傳出交易活動異常的報告。對可疑交易報告的分析顯示，嫌犯從其巴基斯坦盧比帳戶中提取資金，並從公開市場上購買美元，然後將金額存入外幣帳戶中。此外，資金已匯出他們在司法轄區境外的個人帳戶。

110 此外也發現，當事人的近親之中有重要政治性職務人士（AX 先生的兄弟）。在分析過程中，發現 AX 先生的兄弟和父母也在 Alpha Bank 的同一分支機構開設帳戶。在特定時期內，家族成員的帳戶中有大量的營業額，其中包括帳戶間交易以及高額現金提領和存款，與開戶時個人申報的收入狀況不符。這些帳戶中的交易以截斷資金流向和隱匿實質受益權的方式進行。該家庭成員的納稅歷史記錄顯示，所繳稅額與帳目中觀察到的交易活動不相稱。

111 基於上述情況，AX 先生和 JN 先生的帳戶疑似曾用於混合不同來源的資金，進而混淆了稽核線索並逃避了稅務部門的監管。此外，由於重要政治性職務人士的參與，人們懷疑匯兌公司和銀行進行的金融活動可能涉及濫用職權或貪污行為。因此，情報部門已與執法機關共享情報，以進一步調查問題並採取適當後續行動。

泰國

112 香菸走私犯罪所得用於資助南部邊境省份的事件。走私活動是由成員經營的一項事業。一家交易各種走私貨物的商店店主也與犯行集團有密切關係。此外發現一所宗教學校被用作進行招募、宣傳意識形態和進行培訓的場所，支援司法轄區境內的許多恐怖主義活動。該組織也獲得毒品走私者的金援，因為其恐怖行動阻礙了緝查走私的任務。

3.3 新興趨勢、減弱趨勢、持續趨勢

汶萊和平之國

113 在 2018 年收到的可疑交易報告中，金融情報中心觀察到的主要持續趨勢是大部分的通報案件帶有以下警訊指標：

- 帳戶持有者來自零或低收入背景；
- 多筆資金從同一銀行內的另一帳戶以線上方式存入特定帳戶；
- 多筆資金從特定帳戶轉出到同一銀行的另一帳戶；
- 同一天內多筆低於門檻的現金存款；
- 現金存款或線上轉帳存款之後立即提領現金；
- 將個人儲蓄帳戶用於商業活動（尤其是獨資企業和微型企業）；以及

- 可疑的客戶行為（帳戶持有人拒絕向銀行說明從事帳戶活動的理由，接著關閉自己的帳戶）。

114 上述趨勢似乎是犯罪活動的常見要素，包括非法存款、詐欺（投資詐騙）、未授權換匯以及偶發性的未授權匯款活動。此外，這些指標也暗示了潛在的非法活動，例如錢騾或線上交易，其中帳戶持有人可能受第三方委託投資資金。

中國

透過網路眾籌平台和直播平台洗錢

115 隨著技術的發展和金融創新，網際網路金融應運而生。網際網路金融、網路眾籌平台和直播平台在當今的金融市場中起著至關重要的作用，因為它們特別吸引新客戶，且能開闢新的業務渠道。但是，罪犯可能使用這兩類平台從事洗錢。

使用網路眾籌平台洗錢

116 通過「合法」網路眾籌掩蓋洗錢的非法目的：犯罪分子可能會在平台上建立虛假的眾籌專案，以向所謂的「投資人」籌集資金，而投資人將透過線上支付系統來收取資金。

117 使用跨境網路眾籌作為資恐的新渠道：恐怖分子或支持者可能使用假名或虛假註冊的 IP 來設立網路眾籌專案，並藉此方式吸引跨境資金。

118 利用網路眾籌平台作為投資媒介來籌集資金。

使用直播平台洗錢

119 犯罪分子可能使用虛假的身分資訊來建立直播平台，並安排虛假粉絲並佯裝給予大量獎金，或者透過期貨投資分析平台與所謂的投資專家一起收取金錢。所有獎金和收費透過線上支付系統匯入指定帳戶。在網路直播平台收取一定百分比的「平台費用」後，犯罪分子即可領取剩餘的資金。這種低成本的洗錢方法可以規避稅收責任和洗錢防制的監管措施。

網路眾籌平台和直播平台的防制洗錢措施

- 注重資訊誠信度，有效識別客戶身分。
- 注意異常交易，有效識別洗錢風險。
- 建立客戶評價機制和客戶洗錢評估指標系統。
- 加強對可疑交易報告的監測分析。
- 改善防制洗錢數據監測分析標準。

地下銀行的洗錢趨勢和新特徵

120 作為主要洗錢管道之一的地下銀行通常具有家族式經營、嚴格組織制度、隱藏經營模式和固定資本渠道等特點。近年來，隨著交易方式的不斷創新，地下銀行在工具使用和運作模式方面發展出一些新特性：

- 透過境外帳戶洗錢。境外帳戶可能隱匿實際的控制者和資金來源。同時，國內持有的境外帳戶資金易於控制，使其成為地下銀行吸收和轉移海外資金的新工具。

- 國內銀行為海外機構開設境外機構境內外匯帳戶（non-resident account, NRA）帳戶，但是銀行很難判斷此類帳戶客戶提交的原始開戶資訊真實性以及其資金的真實來源。
- 新的金融趨勢（以網際網路金融為主）使地下銀行洗錢更加便利。由於使用第三方支付系統作為交易平台，使電子商務具有高效率、非面對面交易、難以監控等特點，因此已經成為地下銀行的一種流行交易模式。

斐濟

持續趨勢：電子郵件洩露和電子郵件欺騙

121 斐濟金融情報中心持續建議商業銀行、金融機構、企業和公眾在處理進口貿易交易和大額個人匯出境外匯款交易的電子郵件支付指示時，務必謹慎行事。斐濟金融情報中心注意到，2018 年個人和企業成為電子郵件入侵和詐欺受害者的案件持續增加。

122 2018 年向斐濟金融情報中心通報的電子郵件外洩和電子郵件詐騙的最新案例包括：

- 2018 年 3 月，一家本地銀行客戶的電子郵件帳戶遭到入侵，並向該本地銀行發送了詐欺性的支付指示。大約有 575,000 斐濟元匯入一個網路犯罪集團的境外銀行帳戶。
- 2018 年 9 月，在一樁涉及網路洗錢的案件中，

556,000 斐濟元從當地商業銀行帳戶遭詐欺轉移到境外「錯誤」的銀行帳號。在此案例中，海外供應商的商業電子郵件遭到入侵。

- 2018 年 10 月，由於電子郵件外洩，一名居住境外的當地投資人出售股票所得收益約 27,000 斐濟元遭轉至另一個司法轄區的網路犯罪分子銀行帳戶中。
- 2018 年 10 月，清算房地產的收益總計約 845,000 斐濟元被匯入一名偽裝成房地產受益人的網路犯罪分子之境外銀行帳戶。調查顯示，受益人和當地相關方的電子郵件帳戶遭到入侵。

123 任何可疑的海外貿易交易或大量個人匯款，如果可能與電子郵件洩露和欺騙性詐欺行為有關，應立即視為可疑交易報告向斐濟金融情報中心通報。提醒商業銀行和匯款服務提供者針對可疑的之附指示執行更嚴格的盡職調查。

斐濟金融情報中心注意到以下趨勢的減退：

- 使用詐欺性文件進行金融交易；和
- 向金融情報中心通報的仿冒案件數量。

印尼

124 洗錢犯罪者仍透過銀行產業洗錢。根據法院判決；ATM 轉帳、臨櫃現金存款、使用電子資料擷取（EDC）進行交易以及透過行動銀行進行轉帳均呈上升趨勢。

根據印尼對 2017 年法院判例的研究顯示，現金交易（即直接給付和收取金錢）顯示下降的趨勢。

125 近年來，詐欺和毒品的前置犯罪越來越與洗錢相關，雖然貪污仍然是與洗錢相關的前置犯罪。

日本

126 2017 年隱匿犯罪所得的案例，主要是罪犯試圖以他人的名義將資金轉移到銀行帳戶的案件。這是在洗錢犯罪中看到的主要趨勢。

127 此外，犯罪分子使用各種方法使偵查主管機關失去追蹤線索，包括：使用假名出售贓物，並以他人名義簽約，將犯罪所得隱藏在倉庫中。

寮人民民主共和國

128 根據前置犯罪統計數據，在 2018 年 2 月至 2018 年 12 月期間，洗錢中的偽造支票或使用假支票的呈下降趨勢。但是，詐欺仍是持續發生的趨勢。

中國澳門

129 金融情報辦公室（GIF）自 2018 年 1 月至 6 月間共接獲 2187 起可疑交易報告，其中博彩業共計 1,074 起、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。

130 從收到的可疑交易報告中發現到常見的洗錢方法如下：

- 籌碼轉換完全沒有 / 或僅有最少賭博活動；
- 不定期領取大量現金；

- 購買可攜式商品和貴重物品；
- 可疑的地下銀行 / 替代匯款服務；
- 大量現金存款，但資金來源無法核實；
- 疑似使用信用卡 / 現金卡購買高額商品和現金折扣；
- 代表第三方進行籌碼轉換 / 籌碼贖回；
- 使用 ATM、電話銀行業務、現金存款機；
- 換匯 / 現金轉換；
- 嘗試交易但未成功；
- 資金來源不明的外匯交易；
- 使用支票 / 帳戶轉帳等方式移轉資金；
- 無法提供 ID/ 重要的個人資訊；以及
- 可疑電匯。

131 2017 年 1 月至 2017 年 6 月，公共檢察院共接獲 79 起可疑交易報告，這些案件主要與詐欺有關。

132 根據接獲可疑交易報告的觀察結果，銀行業過去數月特別關注日益增多的匯款詐欺和支票 / 帳戶轉帳行為。典型的情況是當地解款行收到匯出行的電報或受害者電子郵件聲稱相關匯款涉嫌詐欺，此外也有一些案件是根據收到的當地 / 海外情報向檢察署舉報。這顯示有效的國際合作和資訊共享，確實有助於在某些詐欺案件中進行有效、成功的調查、起訴和定罪。

133 2018 年上半年出現了一些案例，例如社群媒體欺騙、

網路戀愛騙局和電子購物詐欺。司法機構與海外執法機關保持緊密合作，並提醒民眾保持懷疑態度，不要向任何人揭露帳戶資料和交易驗證碼，以免造成金錢損失。

馬來西亞

可疑交易報告分析的持續趨勢

134 自 2008 年以來，可疑交易報告提交量呈上升趨勢，複合年增長率為 23%，這是因為民眾觀念改善，以及申報機構普遍加強了交易監控措施。此外，亦可歸因於公私部門的有效參與，包括共享高風險犯罪的風險資訊、資恐風險概況分析，以及頻繁運用公 - 私部門資訊共享平台。可疑交易報告主要由銀行、賭場和貨幣服務業部門提出。

135 申報機構通報的主要嫌疑罪行是詐欺 / 詐騙、逃漏稅、組織犯罪和貪污。

可疑交易報告分析新興趨勢

136 詐欺者逐漸從使用個人帳戶轉為開設企業帳戶，以避免遭到懷疑。

調查（洗錢、資恐和前置犯罪）的持續趨勢

137 現金交易仍然是轉移非法犯罪所得（收取、轉匯和支出）的首選方法。

138 使用第三方帳戶（包括騾子帳戶（mule account）持有人）接收和轉移非法犯罪所得。

139　透過高價商品（例如珠寶和品牌商品）洗錢。

紐西蘭

南太平洋地區的洗錢威脅

140　NZFIU 分析顯示，南太平洋諸島的銀行機構正成為洗錢、詐欺和潛在犯罪滲透的目標。在一個實例中，一名紐西蘭公民涉嫌參與組織犯罪，試圖在南太平洋許多司法轄區內建立洗錢架構。他是一名公司籌建代理人，對於國際金融、法律和防制洗錢體系有廣泛的瞭解。NZFIU 對該名個人試圖代表組織犯罪集團在南太平洋地區促進跨國洗錢表示擔憂。

141　最近在另一項不相關但類似嘗試建立銀行的計畫中，南太平洋的司法轄區政府接獲一項具商業規模的自然資源權利的提案，企圖藉此換取核發銀行牌照以供一家在第三地司法轄區註冊的公司使用。NZFIU 評估這項提案幾乎肯定具有詐欺性質，並且可能是企圖進入南太平洋金融業的惡意嘗試。

南太平洋地區的幫派成員人數持續增加

142　越來越多的幫派成員前往南太平洋司法轄區，這位一系列的組織犯罪活動提供了最佳環境，特別是運送非法藥物進出該地區並轉移到紐西蘭。紐西蘭的組織犯罪集團（OCG）與南太平洋地區有著密切的家族聯繫，這不但增加了招募機會，也加強了與紐西蘭的網絡聯繫。NZFIU 觀察到的洗錢技術包括現金走私、電

匯、分散式現金存入，以及將南太平洋司法轄區用作避稅天堂。

透過線上博弈平台洗錢

143 向 NZFIU 舉報的案例顯示，在線上博弈平台進行洗錢活動，是一項持續發生的趨勢。SAR 報告表明，涉及毒品網絡和組織犯罪集團的個人持續使用線上博弈網站，並以「退款」名義從紐西蘭銀行帳戶中取得大筆款項。由於這些場所在海外營運，因此幾乎可以肯定被濫用於規避紐西蘭的防制洗錢控制措施，並且讓犯罪者將非法資金移入或移出未發現的轄區。

巴基斯坦

144 在 2018 年，發現涉及逃漏稅的可疑交易收入呈增長趨勢。

145 在 2018 年持續接獲有關哈瓦拉 / 亨遞系統可疑交易報告的趨勢。

4. 洗錢和資恐的案例研究

4.1 資助恐怖主義

馬來西亞

146 自 2016 年以來，在敘利亞的馬來西亞恐怖分子透過封閉加密簡訊應用程式發出指示遭調查人員截獲，據此查出當地支持者籌集總計 7,000 多美元的資金。隨後，籌得資金的關鍵部分由網絡的金融服務商通過匯款公司匯至敘利亞和伊拉克附近的司法轄區或其他過渡司法轄區。

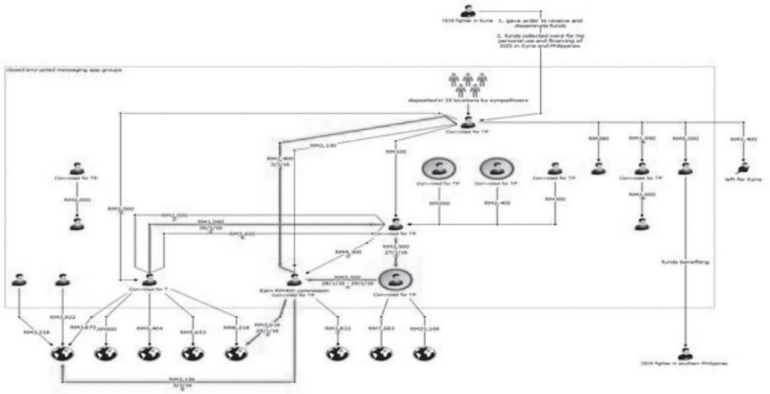
147 在這些資金流向國外之前，金融服務商試圖多次相互轉帳來掩蓋資金流向。據信，這筆資金的潛在用途包括購買一輛貨車來運輸貨物、炸藥包或支援前往或已在敘利亞境內的恐怖分子的旅行和生活費用。

148 在申報機構的交易監控系統發現協助者之間的財務往來線索之後，申報機構便查出其中一名嫌犯。

149 該網絡共有 9 名財務協助者因從事資恐活動，依第 130N（b）、130O（1）和 130Q（1）條法令判處共 65 年徒刑（從 4 年到 10 年不等）。

150 使用的資恐方法包括：

- 電匯 / 使用外國銀行帳戶。
- 地下銀行 / 替代匯款服務 / 哈瓦拉。



菲律賓

MG 和 M 市包圍戰

151 馬巫德集團（MG）是受到伊拉克和敘利亞的達伊沙 / 伊斯蘭國（ISIS）鼓舞的組織，總部位於菲律賓南部，該團體由當地的知名家族成員組成。

識別資金轉移網路

152 根據分析和調查結果，CJ（境外恐怖組織）團體成員於 2017 年 1 月至 2017 年 2 月使用跨境轉帳將資金匯入菲律賓。這些交易都是透過同一匯款代理機構和網路所採用的同一國際匯款平台接收的。

153 外國警方提供的資訊顯示，位於轄區 I 的敘利亞 ISIS 外籍戰士接受指示在轄區 I 出售資產來籌集資金。這些販售所得資金轉交給位於轄區 I 的 CJ，而這些販售所得資金也會透過 ISIS 提供給轄區 I 的戰士在敘利亞使用。透過此系統，敘利亞境內的外國戰鬥人員能夠

獲得資金，並且在轄區 I 內就可以使用資金，而無需仰賴跨境轉帳、匯款或運送實體通貨。其他資訊也顯示，轄區 I 的外籍 ISIS 戰士離開敘利亞時，會留下自己的銀行帳戶和金融卡供 CJ 成員使用。

與 MG 勾結的組織從轄區 T 轉帳到菲律賓

154 轄區 I 的資訊顯示，用於支持 M 市包圍戰的資金是從設在轄區 T 的個人網絡發送至菲律賓。其他資訊也顯示，轄區 T 的相一個成員網絡也從當地將大約 20,000 美元發送至菲律賓，上述成員透過兩家不同匯款機構在菲律賓取得這筆資金。

MG 相關組織路發送資金至轄區 I

155 經查發現一個成員網絡於 2016 年底將資金從 M 市轉移到轄區 I. 資金主要通過 CMAL 和 EMT 兩家匯款業者發送。在 2016 年 7 月至 2017 年 1 月之間，CMAL 的所有者與其可能的妻子以及另一人從菲律賓向司法轄區 I 發送了 12 筆交易。這些交易可能與合法的業務活動相關聯，因為轄區 I 中的收款者各自經營一家企業，但是這些交易似乎與業務內容無關。上述企業未註冊，也沒有任何相關進出口的記錄。

設在菲律賓的女性財務協助網絡

156 跡象顯示菲律賓南部可能有一個女性財務協助者網路，負責為 ISIS 和 ISIS 在東南亞的關係組織轉移資金。

157 女性融資者 ME 從司法轄區 M 和司法轄區 K 的成員

接收資金，該成員也向女性融資者 MM 發送了資金。在 2015 年至 2016 年之間，位於菲律賓的 ME 和 MM 女性融資者分別從司法轄區 M 的某人和 K 司法轄區的某人獲取資金。該網絡也向某未 MA 博士的第二任妻子匯款。女性融資者 ME 和另一名女性融資者 EI 均於 2016 年向司法轄區 M 的馬博士的第二任妻子匯款。

外國恐怖主義作戰人員

158 在 M 市包圍戰爆發之前，轄區 I 的 7 名外籍作戰人員已被查出身分並已前往菲律賓。經分析確認，這些人不太可能擁有資金或資源來安排旅行，包括自己的護照、簽證和機票的購買。資料顯示，特定轄區居民承認曾協助七名已知身分的轄區 I 境外戰鬥人員旅行前往菲律賓。轄區 I 的另一名公民協助當地其它三名外籍戰鬥人員旅行出境，轄區 I 的主管機關以資恐罪名逮捕了上述個人。

識別高風險匯款業務

159 CMAL 被認為是具有高資恐風險的匯款業者。CMAL 目前不再登記為 MSP，但似乎在包圍戰之前已經登記。CMAL 從未在 AMLC 上註冊為匯款業者，也未提交任何交易報告。CMAL 的所有者被記錄為高風險匯款業者，其並未為 CMAL 經營業務帳戶，但使用其個人銀行帳戶來進行匯款交易。司法轄區 A 的金融情

報中心也認定 CMAL 是一家匯款代理機構，負責接收轄區內某集團的資金，並在 2013 年 4 月透過分散式交易將資金轉至菲律賓。在轄區 A 中的團體涉嫌參與資恐活動。截至 2016 年，這些交易在 CMAL 收到的交易款項中佔有大部分。

160 2013 年 11 月至 2018 年 6 月之間，國際匯款平台提交了 22 份可疑活動報告，確認 CMAL 是 2013 年 7 月 11 日至 2017 年 3 月 20 日之間收發 49 筆可疑匯款的代理機構。提交的大多數可疑活動報告都以可疑的資恐活動為目標。

161 根據可疑匯款，CMAL 充當支付代理人的次數比充當傳送代理人多六倍。作為支付代理人，發送給 CMAL 的大部分可疑匯款都起源於菲律賓，其次是印尼；但印尼的匯款金額最高。

4.2 使用境外銀行、國際商業公司和境外信託

中國

162 2017 年 12 月，主管機關、稅務局和警方調查一名，其在交易中以作假方式使用外匯收據取得補貼折抵，並通過地下銀行和位於 H 市的多家立案公司隱匿稅收違法所得。

163 此案件已於 2018 年 2 月結案。嫌犯 X 設立一家空殼公司 Y，通過第三方購買了增值稅發票，然後假造發

票來申報 Y 公司的稅款。嫌犯 X 和嫌犯 Z 也透過偽造發票、購買海關報關單、虛假輸出和非法外匯等手段逃漏稅。據警方表示，增值稅發票和退稅總額已達數百萬元人民幣。目前，該案已移交給檢察官提起訴訟。

巴基斯坦

164 XYZ 夫婦（巴基斯坦著名的商業家族）與境外公司參與未經授權的資本外逃和逃稅。不同的換匯公司根據分散式換匯交易（美元計價）提出可疑交易報告，並透過分散式的方法利用不同的換匯公司，蓄意違反中央銀行的通貨購買門檻。涉及的金額（通過 CTR 確定）非常可觀，引發相關單位懷疑。FMU 查出嫌犯在不同的銀行擁有多個外幣帳戶。整體交易模式顯示，他們正在從其本幣帳戶中提取資金購買外幣，然後將其存入外幣帳戶，最終再匯出司法轄區。分析可疑交易報告時，也在外流文件中發現了嫌犯的姓名，他們的身分是境外公司的所有者，並且正在將公司出售給外國企業。另也發現，他們在向外國買家出售公司的過程中做出不實陳述。據研判，XYZ 夫婦涉嫌申報不實和詐欺性資訊、違反外匯規定、未經授權的資本外逃、逃漏稅和其他犯罪。FMU 總幹事下令凍結帳戶。相關金融情報根據《防制洗錢法》提供多間機構共享。

165 根據 FMU 的轉介，稅務機關追回了 62 億巴基斯坦盧

比的應納稅額。

菲律賓

166 2017 年 5 月，司法轄區的金融情報中心透過艾格蒙安全網（ESW）請求提供有關涉嫌參與洗錢、證券和電匯詐欺的各種個人和實體的資訊。

167 相關資訊涉及 GLADS，這是 GRALE 全資控股的菲律賓註冊實體。資訊顯示，GRAALE 的多數股權持有人 DT 先生於 2011 年 10 月贊助成立 G 收入基金（下稱「基金」）。DT 先生在 2012 年至 2014 年期間擔任基金的受託人、董事長、總裁和共同投資經理。該基金旨在主要投資於研究生、專科學生以及高收入就業領域的應屆畢業生簽署的個人本票，來為其投資人 / 股東創造收入。2012 年 1 月，GRALE 依據《貸款服務協議》成為該基金所有與貸款相關文件（包括原始本票）的保管人。

168 GRALE 疑似開始虧錢後，DT 先生設想一套詐欺手法，即捏造一筆由基金支付的虛假貸款，以維持公司生存和他的奢侈生活方式。根據 DT 先生的詐欺計畫，貸款犯罪所得匯入 TF-LLC（DT 先生也持股的有限責任公司），而不是發送給正式向借款人發放貸款的銀行。

169 詐欺行為之所以曝光，是由於 GRALE 的員工不慎向 DT 先生的前大學室友發送一份貸款明細，而該人列

為本金餘額為 342,000.00 美元的貸款人，2014 年 12 月，轄區 U 的調查局偵訊 DT 先生的前室友，他否認曾與 DT、GRALE 或該基金有業務往來、借錢或申請融資。這導致了轄區 U 的證券委員會發起調查，隨後逮捕 DT 先生，並向他提起刑事訴訟和多項民事訴訟。基金的一名獨立受託嫌犯 MS 先生簽署切結書，聲稱 DT 先生建議基金的獨立受託人間接投資菲律賓的一系列保理交易。此舉涉及向兩個潛在的有限責任公司之一放貸，而這些公司則充當了轄區 U–LCLLC 或 LC2LLC（「LC 實體」）的中介。這些 LC 實體將轉而向菲律賓的交易對手放貸，作為一系列保理交易的一環。保理交易對手方支付的本金利息和還款金額，隨後將透過 LC 實體返回到基金之中。據稱，該基金從 2013 年 4 月至 2014 年 10 月共向 LC 實體放貸 8,065,759.44 美元。但是，從基金轉移到 LC 實體的犯罪所得並未進行投資，而是轉移到 GRALE 的營運帳戶中。然後，部分犯罪所得保留用於 GRALE 的營運費用，部分則匯入 GRADS（由 GRALE 獨資擁有的菲律賓公司）。除了 DT 先生以外，GLADS 的創辦人中也有數名菲律賓律師，他們都與該司法轄區一所知名律師事務所有關聯。

170 據稱部分資金在菲律賓註冊實體 ELI 公司中遭到洗淨。DT 先生顯然偽造本票，這顯示了 BS 先生所代表

的 LC 實體放貸給由某 WD 先生代表的 ELI 公司。從 2015 年 4 月至 2015 年 11 月發行的偽造本票總額為 2.130 億菲律賓比索。據稱這些資金是由 ELI 公司通過《營運資本協議》（「WCA」）放貸給各個菲律賓商業實體。而這些 WCA 也是虛構的。

171 菲律賓金融情報中心根據請求採取行動並提供答覆，其中包括可能從 DT 先生控股實體（位於轄區 U）發出資金的最終實質受益人資訊。

172 2017 年 11 月，U 轄區認為金融情報中心提供的新資訊非常有用，因此再次提出要求，重點是將金融情報中心先前答覆所述的新涉案者納入他們對該案的調查。金融情報中心也對該案採取了行動，並在收到後續要求後的三個月內提供了所要求的資訊。

4.3 虛擬通貨之使用

澳洲

吊銷涉嫌參與組織犯罪的加密貨幣業者之營業登記證

173 在澳洲聯邦警察（AFP）逮捕一名男子之後，AUSTRAC 吊銷兩家數位換匯業者的營業登記證。

174 在 AFP 的逮捕行動之前，曾經對涉嫌透過國際郵件進口境管藥物的當事人進行調查。經過調查之後，AFP 員警於 2019 年初執行搜查令，扣押了類固醇、澳幣和加密貨幣相關物品。隨後起訴涉嫌進口、販運和持

有約 30 公斤非法藥物的個人，起獲藥物中包括搖頭丸、古柯鹼，安非他命和 K 他命。

175 犯罪集團涉嫌利用各種暗網、比特幣帳戶和合法事業進行非法藥物的採購、支付和配銷。

176 在另一項行動中，由 AFP 領導的犯罪資產沒收工作組（CACT）成功申請扣押與調查有關的資產。維多利亞州法院下令扣押價值超過 200 萬澳幣的財產。

177 其中包括多個銀行帳戶、房地產、數輛汽車、一台摩托車、現金和加密貨幣。扣押令是根據 2002 年《*犯罪所得法*》（Cth）發出

178 被捕後，AUSTRAC 吊銷兩家數位換匯業者的營業登記證，其中一名被捕者是關鍵成員，這使他們無法繼續營業。

中國

案例研究 1

179 公司 A 處理 U-bao，一種數位通貨流通系統。相關嫌犯利用 U-bao 非法收款，這些資金從多個帳戶流入系統。涉及數百個交易方，交易的備註 / 參考字樣是「U-bao」。有關公司 A 的公共負面新聞甚多，包括從事金字塔傳銷活動。一名嫌犯的帳戶涉及大量與甲公司有關的資金交易，總價值達數百萬元人民幣，有關案情已報警處理。

案例研究 2

180 WEIKA 是跨境網路平台發行的虛擬通貨。這種類型的貨幣可用於消費，並可通過購買與一定數量的 WEIKA 相關的股票來提高其價值。WEIKA 收取會員費。嫌犯 B 的帳戶經常有資金流入和流出，涵蓋不同部門和地區。嫌犯 B 和交易對手的交易備註 / 參考字樣是「Onecoin」、「WEIKA 啟用碼」、「購買動機方案」等。他們被懷疑使用 WEIKA 進行金字塔銷售和洗錢，本案總金額已達數百萬人民幣。

中華台北

181 IRS 是 2016 年成立於 S 轄區的法人，經營一項龐氏騙局的比特幣投資計畫來訛詐投資人。自 2016 年 10 月以來，A 先生一直是中華台北和中國的負責人，負責該集團的整體營運，招募投資、發放獎金等工作。A 先生和同謀成員舉行簡報會，向與會人員介紹了 IRS 的投資計畫、利潤和獎勵機制。他們確保所投資的產品每天都會進行估值，一年後投資人可以獲得的最大利潤為投資額的 255%。藉此方法，A 先生欺騙大約 3 萬名投資人，資金總價值約為 5100 萬美元。

182 A 先生等人將犯罪所得轉化為虛擬通貨和房地產的形式。在調查過程中，這些由 A 先生等人持有財產均遭扣押。2018 年 12 月，台中地檢署以違反《銀行法》和《多層次傳銷管理法》的罪名起訴 A 先生及其共犯。

中國香港

183 2017 年 7 月，駭客在位於轄區 A 的比特幣交易平台中竊取了 136.9 比特幣（價值約 1,364 萬港元）。遭竊的比特幣罪終於 2017 年 8 月轉移給了 A 先生。隨後，A 先生出售比特幣，並將犯罪所得轉入了中國香港的銀行帳戶。應轄區 A 的要求，在中國香港扣押其銀行帳戶中 460 萬港元和 73 萬美元的犯罪所得。相關調查正在進行中。

日本

184 一名男性上班族使用非法獲取的他人帳戶和信用卡資訊購買了 VA（即虛擬資產）。他通過一個海外交易所網站將虛擬資產變更為日元，然後以另一個人的名義將這筆錢轉移到了一個銀行帳戶中。他因違反《組織犯罪懲治法》（隱匿犯罪所得）而被捕。

紐西蘭

在暗網使用比特幣購買毒品

185 2018 年，某人因進口和供應大量 C 類管制藥物遭判罪定讞。此人使用比特幣從暗網網站購買了這些毒品。然後，他在暗網張貼廣告，將其販售給紐西蘭和全球客戶，接受比特幣、乙太幣和現金等支付方式。

186 在緝捕過程中，NZP 在犯罪者的錢包中起獲超過 40 萬紐幣的現金和價值約 18 萬紐幣的加密貨幣。總計超過 150 萬紐幣的資產依據紐西蘭的犯罪所得法規予

以扣押。

菲律賓

187 某人使用名下公司（登記不同目的之獨資公司）經營金字塔傳銷詐騙，並以比特幣作為掩飾來解釋公司的獲利來源，並透過虛擬通獲交易平台來輔助支付和投資流程。此詐騙手法向投資人承諾每隔幾週會有兩位數的利率。嫌犯利用金字塔制度並僱用中介人來招募新投資人，詐騙範圍擴大到了全國各地。肇事者最終被捕。在被捕前的幾個月，虛擬通貨交易所的系統會標記可疑的帳戶活動、交易和與涉嫌參與計畫的成員，進而針對團體及其同謀 / 共犯提交可疑交易報告。

新加坡

虛擬通貨的使用 – 跨國電子郵件詐欺犯罪所得的收入用於購買比特幣

188 在一項電子郵件詐欺案中，騙取自美國受害者的犯罪所得被轉移到新加坡一家公司所使用的銀行帳戶，而該公司提供線上交易平台和虛擬通貨網路支付閘道。犯案人使用偽造文件開通了一個線上交易帳戶，用於存入犯罪所得。然後，犯案人透過線上交易平台購買了比特幣，不論價格高低一律買入。由於交易方式異常，新加坡公司封鎖了線上交易帳戶。這家新加坡公司收到銀行的召回通知函後，清算了犯罪者購買的比特幣。資金則交由警方扣押。相關調查正著手進行中。

4.4 使用專業服務（律師、公證人、會計師）

斐濟

據稱使用把關者來協助進行異常的 EFTPOS 交易

189 金融情報中心接獲當地銀行的可疑交易報告，得知某台 EFTPOS 終端在一個週末進行了重大交易。由於 EFTPOS 終端是當地一家小型律師事務所新安裝的設施，因此引起懷疑。

190 金融情報中心確定，居住在轄區 B 中的一名斐濟公民 A 與當地律師事務所的負責人 X 聯繫，購買 EFTPOS 機器以其實體 A 公司的名義獲得投資資金。

191 雖然在經濟上無法負擔 EFTPOS 機器，這家當地的律師事務所仍購入了 EFTPOS 設施。一週之後，當地律師事務所的 EFTPOS 終端機上共有兩張境外信用卡在三週內依詐欺方式進行七筆交易，總計約 200 萬斐濟元。資金都轉入了律師事務所的信託帳戶。

192 可以確定的是，X 嫌犯、A 嫌犯和 A 公司一起參與了精心策劃的騙局，目的是使用 EFTPOS 機器詐取資金。X 嫌犯藉由詐騙所得的轉帳金額約為 221,000.00 斐濟元，而 A 公司在其當地銀行帳戶中收取約 650,000.00 斐濟元。其餘的 1,129,000.00 斐濟元保留在律師事務所的信託帳戶中。

193 然後，資金會從 A 公司的當地銀行帳戶中迅速提出，用來支付個人費用並購入資產。此外，也查出部分犯

罪所得用於購買昂貴的勞力士手錶。在本案中，地方邊境執法機關與金融情報中心之間進行了良好的協調和溝通。

194 金融情報中心向當地銀行發出了一份可強制執行的指示通知函，對此精心策劃計畫中涉及的所有銀行帳戶（包括資金受益人）發出禁制令，以確保徹底減少犯罪所得的損失。金融情報中心向斐濟警方提供分案報告，該案仍在調查中。

潛在罪行：

- 詐欺。
- 持有由犯罪所得的財產。
- 洗錢。

指標：

- 雇用律師擔任把關者協助詐欺行為。
- 使用與業務性質不相稱的罕見業務交易方法。
- 購買貴重資產和奢侈品。

假造的增值稅申報表

195 一家當地會計師事務所涉嫌向當地稅務機關提供假造的報稅單。該公司疑似誇大了其客戶的增值稅退稅申報金額。該公司也提交了假造的發票和收據副本，用作詐領退稅的證明文件。然後，會計師事務所的客戶從地方稅務機關收到增值稅退款，但後者表示他們無權獲得任何退款。這也導致斐濟地方稅務機關損失了

大量資金。可能的罪行包括洗錢、詐取財產和以背信行為牟利 / 造成損失。此事目前正在由當地執法機關進行調查。

紐西蘭

組織犯罪集團委託會計師在紐西蘭成立公司

196 一名紐西蘭會計師登記數間公司後，組織犯罪集團隨後利用這些公司將毒品進口到該司法轄區。會計師提交了公司登記文件，並註冊為公司的董事及 / 或股東。公司的銀行帳戶用於進口毒品及 / 或跨境償付毒品犯罪所得。會計師可能也會偽造這些公司的財務記錄（即「作假帳」）以隱匿非法活動，雖然這類行為尚無確切證據。

雇用律師來隱匿組織犯罪集團成員的置產活動

197 紐西蘭組織犯罪集團成員在簽訂置產契約時，聘請律師使用債權安排來混淆資金。組織犯罪集團成員的母親是一名律師，在取得現有房產的抵押債權後，以「房貸再融資」的名義透過另一名律師的信託帳戶提供這些資金，用來清算組織犯罪集團成員購置的不動產。組織犯罪集團成員定期向其母親名下新開設的交易帳戶付款，藉此償還抵押貸款。組織犯罪集團成員及其母親之間的債務關係確立後，成員的資金與財產交易區分開來，進而限制執法人員扣押資金及 / 或資產來阻斷購買行為的能力。

新加坡

使用專業服務 – 成立公司接收海外賄賂款項

198 提供公司秘書服務的律師事務所協助境外商人成立公司，由其律師擔任註冊公司的董事。然後，律師以董事身分為公司申請銀行帳戶，並將銀行帳戶的全部控制權交給境外商人，而後者依法向銀行申報其為公司的實質受益人。

199 然後，該境外商人利用該公司作為外國官員收賄的渠道。此人同時擔任公司員工，使其得以合法從公司銀行帳戶提款並轉入其個人帳戶或其他由其所控制的帳戶。將疑似貪污反罪所得轉入他的帳戶後，最終將支付給海外官員。

200 貪污行為調查局（CPIB）積極邀請外國主管機關對在新加坡受賄的貪污官員進行聯合調查。相關調查正在進行中。

泰國

201 南部邊境省的一所私立宗教學校委託一家會計師事務所對學校的帳目進行「財報窗飾」，以便從政府獲得*每位學生*的補助款，然後將其用於支持當地的恐怖主義活動。

4.5 交易基礎的洗錢和移轉訂價
Trade-based money laundering and transfer pricing

阿富汗

案例研究 1

202 經海關和稅務局核實，發現貿易公司 X 的海關文件是偽造的。這是一家「紙上公司」，沒有海關和稅務局的任何進出口記錄，但有系統地將款項記入公司的帳戶。然後，Y 先生將公司的帳戶記入借方，並利用這筆錢進行匯兌作業。Y 先生也通過國內機場將實體現金走私到司法轄區以外的其他省分。金融情報中心的情報促使執法機關進行公開調查。

案例研究 2

203 對公司進行的財務分析結果顯示，公司已將大量現金從國外轉移到轄區 A 和轄區 B，名義是用於支付進口貨物。但是，海關部門核實了進口貨物的價值，僅佔寄往國外總金額的一小部分。這些公司也向 C 轄區和 D 轄區轉移了大量資金，但沒有貨物進口到該轄區。

204 金融情報中心申報實體對發票的財務核實也顯示，這些公司透過進口相同商品的發票從不同銀行轉帳。

205 在金融情報中心將此案分派給執法機關後，重案組對這起案件進行了最高級別的調查。

206 這項調查不僅查出同一商品開立不同支付憑據，而且也顯示這些公司偽造了支付憑據。調查團隊核實公司

業主在法庭上出示的發票，並成立了一支專家小組來驗證發票是否真實。專家小組確認發票是偽造的。

207 在調查過程中，被告行賄警方試圖取消指控並撤銷該案，結果因企圖賄賂公職人員而被立即逮捕和羈押。

208 在拘留對象的同時，完成了對洗錢的調查，並展開洗錢的起訴程序。

209 根據有關執法機關的要求，金融情報中心彙編並向執法機關分發了 30 份文件，約 1500 頁的附加價值成果。

210 這些附加價值成果包括：

- 匯款交易佐證文件以及有關轉帳渠道、受益人和司法轄區的資訊。
- 這些企業行賄銀行員工以換取交易的贈禮資訊。
- 推介金融情報中心員工提供諮詢服務，並向執法機關提供專家意見。
- 有關被起訴公司的稅籍編號（TIN）資訊。
- 提供轉帳目的以及帳款轉入的轄區資訊。
- 根據執法機關要求凍結涉案銀行帳戶。
- 提供真實發票轉帳金額與偽造發票金額之間的差異資訊。
- 有關偽造發票內容、銀行轉帳程序以及定罪人員、轉帳總額資訊（檢附發票）。
- 成立一支由金融情報中心主持、並由三家銀行代表組成的技術檢查委員會，並將其技術檢查報告

發送給執法機關。

- 有關 2013 年至 2015 年期間受相關公司委託向國外匯款的個人特徵資訊。
- 有關這些公司的簽證機關及其在董事和代理董事缺席時的授權人資訊。

211 值得一提的是，上述附加價值成果是由金融情報中心依執法機關的 15 項要求而彙編並分發給後者參考。

212 這項起訴的結果是，被告人遭判洗錢罪定讞，處有期徒刑四年，立即生效。法院依依《防制洗錢法》做出該判決，並沒收了一定數量的資金。該案可以上訴（截至編寫本 2019 年度態樣報告）。

斐濟

213 斐濟金融情報中心接獲一份可疑交易報告指出嫌犯 M 從 D 公司收取大筆資金。

214 事實證明，M 嫌犯也是 D 公司的董事兼股東。D 公司已從位於轄區 B 的 E 公司收取約 510,138 斐濟元的匯款，據稱是用於支付帳單、購買商品和支付貿易款項。斐濟金融情報中心發現，嫌犯 M 同時也是轄區 B 境內 E 公司的董事兼股東，並且 D 公司沒有向 E 公司出口任何符合匯款項目的商品。這些資金隨後轉入嫌犯 M 的本地銀行帳戶，並用於購買房產。

215 金融情報中心進一步確定，嫌犯 M 已從轄區 B 境內的嫌犯 N 處收取大約 897,913.00 斐濟元。嫌犯 M 隨

後將這些資金用於購買另一處房產。

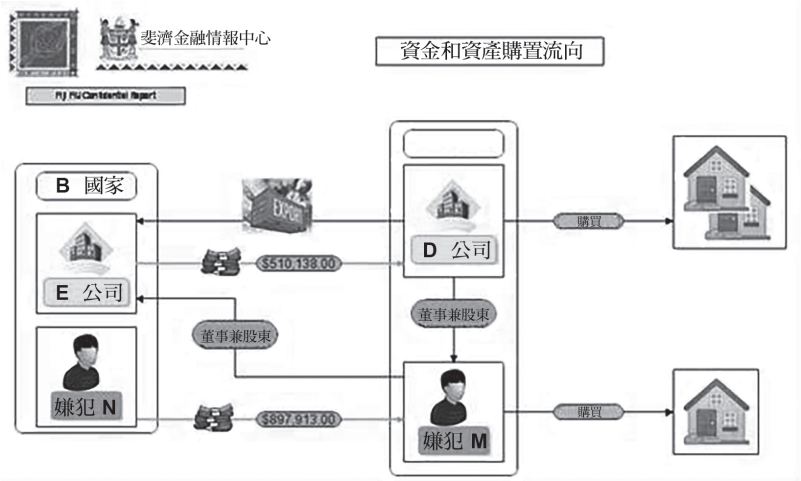
216 向 B 轄區的金融情報中心和斐濟稅收與海關總署（FRCS）提供了分案報告，以進行後續分析和調查。

潛在罪行：

- 貿易洗錢
- 稅務犯罪。

指標：

- 大量的匯入款項。
- 資金從企業迅速轉移到個人帳戶。
- 許多相關實體用於轉移資金。
- 物業投資。



印尼

217 JT 將大量資金匯出海外，如 5419 份《國際資金轉移指令》（IFTI）報告所記錄，將總計 3.6 萬億印尼盾（2.54 億美元）轉移給 2365 名當事方（個人和公司）。JT 是一家進口貿易公司、換匯商和貨運代理公司的所有者之一。根據對 JT 帳目的檢查，發現任何海外資金轉移皆附有境外供應商公司進口商品的購買憑據文件。中國、中國香港和日本是 JT 轉入最多資金的司法轄區。匯到中國的金額為 1,085,182,450,627 印尼盾（74,840,169 美元），收款人包括 710 名當事方。

218 將 JT 進口的貨物資料與海關總署（DGCE）海關數據進行比對，發現 JT 檢附於銀行的發票與 DGCE 現有的資料之間似乎有差異。資料經過比對處理後，可以看出銀行的發票從未記錄在 DGCE 數據中（即假造或虛構）。

219 海外有 2,365 名資金接受者。其中大多數（1,246 名當事方）是不從事進口活動的公司，其中 494 名是個人。其餘為進出口貿易公司。

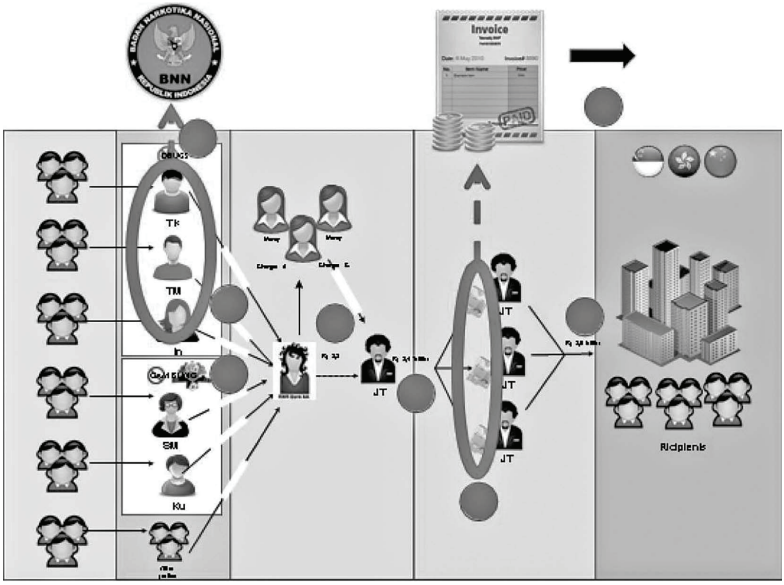
220 RWR 是 JT 在 A 銀行帳戶的資金來源之一。RWR 將 7,720 億印尼盾（53,241,379 美元）轉入了 JT 在 A 銀行的帳戶。資金隨後發送至 B 銀行，金額為 3,458 億印尼盾；匯入 C 銀行的金額為 1,34 兆印尼盾（92,413,793 美元）；D 銀行為 796,170 億印尼盾

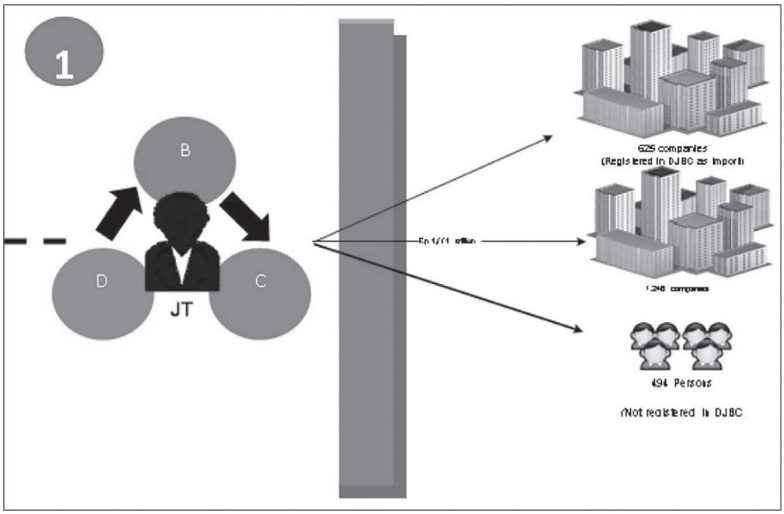
（54,908,275 美元）。

221 PPATK 分析了 RWR 在 2014 年至 2015 年期間在 A 銀行帳戶活動，發現該帳戶的多方收款資金總額為 9,62 兆印尼盾（合 663,448,275 美元）。調查發現若干與毒品有關的犯罪活動，包括 965 項交易涉及麻醉品 TK，金額達 313,2 兆印尼盾（21,600,000 美元），328 項交易涉及 TM，金額為 1,145.3 億印尼盾（1,002,068 美元），以及 AAS，金額達到 98.6 億印尼盾（680,000 美元）和 45,000 美元。調查單位向國家禁毒委員會（BNN）通報相關方參與麻醉品犯罪的情況。

222 據稱，RWR 帳戶也用於向參與線上博弈的各方收取資金，並進一步通過 JT 的帳戶將資金發送到海外。JT 的帳戶疑似用於處理 RWR 的收益。JT 帳戶上的交易模式（過渡交易）突顯了這一點。

223 JT 和 RWR 個人帳戶之間的過渡交易模式金額從數百萬盧比到數十億盧比不等，並且主要通過網際網路銀行進行。根據銀行資訊，JT 和 RWR 開設的帳戶旨在進行商業交易。

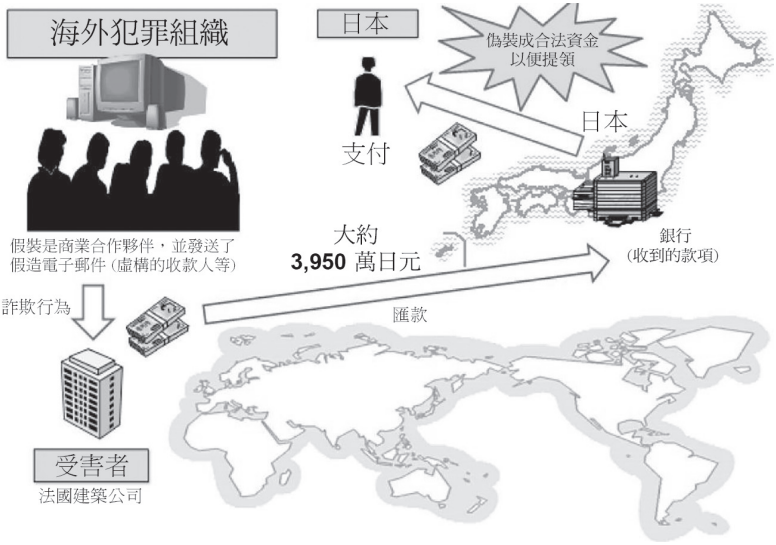

BNN
Invoice
PAID
TK
TM
SM
Ku
JT
JT
JT
Recipients


1
B
D
C
JT
625 companies
(Registered in DJBC as Importi
494 Persons
(Not registered in DJBC

日本

224 一名無業男子出售贓車時，將另一輛汽車的車牌裝在贓車上，並透過一家不知情的出口管理公司將其外銷到境外司法轄區。他因違反《組織犯罪懲治法》（隱匿犯罪所得）而被捕。

225 一名日本男子向法國的一家建築公司發送了偽造的交易電子郵件，並要求他們將資金匯入以他人名義開立的日本銀行帳戶。在提領資金時，他向銀行員工佯稱這些資金是正常商業交易匯款，藉此將這些錢偽裝成合法的商業利潤。結果，他因違反《懲治組織犯罪法》（隱匿犯罪所得）和詐欺罪被捕。



紐西蘭

非法漁撈業使用以物易物的支付方式

226 一家紐西蘭漁撈公司被控進行複雜和大規模的詐欺行為，其中涉及其漁獲量的漏報。這涉及兩種類型的違法行為 – 向初級產業部謊報漁獲收益，以及出售未申報的魚類。一些非法漁獲隨後出口到一家澳洲公司，該公司向紐西蘭出口商提供了一艘新船以支付非法漁獲物的費用。這種方法通過國際貿易來交換價值（用新船支付非法捕撈的魚）而不是交換現金。

巴基斯坦

227 FMU 收到了有關貿易洗錢嫌犯的可疑交易報告。嫌犯 A 先生正在喀拉蚩執行業務並開設了一個銀行帳戶。開戶一段時間之後，嫌犯向銀行提交了 EIF（電子進口表格）以進行認證。經詢問，銀行確認進口商參與貿易洗錢活動。嫌犯經由其他轄區的公司進口來自特定轄區的坯布，但謊稱是從中國進口。海關情報局也扣押了布料和總共 106 個貨櫃的走私物品。

228 嫌犯在喀拉蚩擁有一個銀行帳戶，海關情報局正在調查此案，然後將財務情報轉發給執法機關，以進行深入調查並根據《2010 年防制洗錢法》的規定採取必要行動。

菲律賓

229 菲律賓禁毒局在一次臥底緝毒行動中逮捕了轄區 C 的

公民 ZTC。ZTC 涉嫌向臥底探員出售當地稱為 shabu 的冰毒而以*現行犯*身分逮捕。除毒品外，也查獲了他持有的各種財務文件，特別是將可疑毒品犯罪所得存入的多個自然人 / 實體銀行帳戶，分別是 QH、XQ、WL、CG、WH、RDS、MAD、BJC、JE 和 YSMW 企業。

230 ZTC 的毒品前科要追溯到 2009 年之前，當時他因出售大量非法毒品而被政府特工逮捕。

進行財務調查的若干要求

231 菲律賓金融情報中心接獲政府機構要求，調查涉嫌非法毒品活動的 QH、WH 和 YSMW 企業的財務狀況。因此，菲律賓探員在菲律賓中部逮捕毒販時，扣押了一些其所持有與 QH、WH 和 YSMW 企業有關的財務文件。此外，從不同監獄設施中的囚犯扣押的行動電話中查獲專門暗示 YSMW Enterprises 和 QH 銀行帳戶的簡訊，這些簡訊被用於轉移非法毒品活動的犯罪所得。

232 金融情報中心對已知相關方的銀行和投資帳戶進行了調查，同時與以下各方進行了協調：（1）不同的政府財產登記處核實當事人的財產所有權和在企業中的持股；（2）執法機關確定貶損記錄並協助執行監控任務。

財務調查結果

233 ZTC 沒有已知的財務交易記錄，僅發現他持有其他人的銀行對帳單。

234 YSMW 企業的銀行帳戶用於移轉毒品犯罪所得，從受刑人手機中擷取的簡訊可以證明這一點。該公司已登記為手提包的批發 / 零售商。其銀行帳戶中的金融交易記錄了許多大筆的金額，這在這種業務的日常活動中並不常見。此外，發現該公司的銀行帳戶不受其登記所有者 LTE 的實質控制，而是由 C 轄區的國民 DS 和 TS 所控制。

235 另一方面，QH、XQ 和 WH 具有血緣關係，且皆為 C 轄區的公民。在他們申報得收入來源中，有（a）一間證實不存在的電腦行，以及（b）申報業務為電腦墨水和配件銷售的公司 HK 公司。對他們帳戶的財務調查顯示，有數十億比索流入他們的帳戶，這與他們所申報得業務性質不符。

236 CG 是 C 轄區的國民，擁有幾家企業，但最近都停止了營運。但他卻在身分證明文件中聲明薪資為主要收入來源。2018 年，他成立了旅遊和房地產業務。從企業的交易情況可以看出，即使在起步階段，就有數十億比索流入了公司銀行帳戶。另一方面，WL（也是 C 轄區的國民）自稱是 GPT Company 的財務經理，該公司以從事線上博弈而聞名。金融調查顯示有數億比索流入了她的帳戶。她也向 CG 的妻子 WFG 的銀

行帳戶進行了幾筆轉帳。

237 從當事人的帳戶向外匯出資金中發現許多可能涉及非法毒品活動的利害關係人。這些交易的適當性尚未確立，也沒有理由在日常業務過程中進行。

238 追回 ZTC 的對帳單後發現了 QH、XQ、WL、CG、WH、YSMW 企業、RDS、MAD、BJC 和 JE 與非法毒品活動之間的聯繫。銀行之間轉帳的資金交換和使用貨幣服務業的記錄確立了他們之間的關聯。此外，根據他們通過銀行系統進行的電匯交易，發現他們的金融交易與其他個人和實體皆有關聯，而這些對象都是金融情報中心依菲律賓藥物法規而發起的民事沒收案件被告。

239 在沒有合法收入來源支持的情況下，卻有數億比索的龐大資金轉入他們的帳戶索，據此可判定他們也有其他收入來源。依據業務類型，匯入他們帳戶的交易規模並不尋常。帳戶及其收入來源特徵不一致的性質顯示，上述金融交易沒有任何基本的合理根據。

240 凍結在 13 個金融機構、六百多（650）家銀行的帳戶，涉及金額達 773,003,483.06 菲律賓幣和 142,407.25 美元，目前已予以沒收。

新加坡

供應指定的奢侈品 - 公司及其董事因向朝鮮民主主義人民共和國（DPRK）提供指定的奢侈品、舞弊和洗錢而被起訴

241 N 嫌犯是 T 公司的董事之一，2010 年至 2017 年，T 公司向北韓的一家百貨商店提供 80 次總值 600 萬新加坡幣的指定奢侈品，包括葡萄酒、香水和化妝品。

242 當朝鮮百貨商店延遲訂購的商品付款並導致 T 公司的現金流出現問題時，N 嫌犯設想出詐欺手法，並利用 T 公司向五家銀行提交了虛假的商業發票，以詐欺方式獲得融資 81 次，總計超過 9500 萬美元。

243 2018 年 7 月，N 嫌犯和 T 公司被指控根據聯合國 - 北韓條例向北韓供應指定的奢侈品。N 嫌犯也因涉嫌票據融資舞弊而遭起訴。T 公司也遭起訴從事票據融資詐欺犯罪所得的洗錢活動。

244 對 N 嫌犯和 T 公司進行起訴的程序正在進行中。

4.6 地下銀行 / 替代匯款服務 / 哈瓦拉

中國

案例研究 1

245 2014 年 7 月和 2014 年 11 月，主管機關向警方提供了可疑交易記錄。警方於 2015 年 5 月提起訴訟，並對嫌犯 Y 及其同夥進行了調查。

246 該案涉及三個地下銀行組織：通過 POS 機刷卡、非法交易外匯和通過 ATM 跨境提領現金。他們形成了一個完整的地下銀行犯罪鏈。截至 2018 年 6 月，涉嫌非法經營的 41 名涉案人員全部被判刑。

案例研究 2

247 2018 年 9 月，主管機關與當地警察共同發現了一樁地下銀行案。嫌犯 C 及其同夥在兩個城市非法交易外匯。他們使用了一個位於 J 市的嫌犯帳戶，從海外帳戶收取外匯，從國內帳戶收取資金。涉案總金額已超過十億人民幣。

中華台北

248 2017 年 5 月，B 先生在馬來西亞公民的協助下，將由 Y 集團研發的龐氏騙局引入中華台北。B 先生等人舉行了幾次簡報會，聲稱 Y 集團發明了可用於從體育彩票中獲利的軟體。根據投資額，投資人可獲得的年利率在 84% 至 180% 之間。為了欺騙更多的投資人並獲得更多的資金，B 先生等人開發了反饋計畫，以提供高額誘因或其他獎勵，使投資人願意介紹新的投資人加入或投入資金。截至 2018 年 9 月，B 先生等人欺騙了大約 3,000 名投資人，受害金額約為 1.98 億美元。

249 為了規避調查，B 先生及同夥隱匿他們向投資人騙取的現金，總計約新台幣 2 億元。在此過程中，透過地下銀行營運商向海外轉移了約新台幣 2.32 億元。其中一些資金以其名義用於其他投資，或轉換為外幣或虛擬通貨。在調查過程中查獲了與案件有關的資產，例如現金、虛擬通貨、汽車、房地產和銀行帳戶。2018 年 11 月，檢察署起訴 B 先生及其同夥違反《銀行法》、

《洗錢防制法》和《多層次傳銷管理法》。

250 CIB 在調查無關的綁架案時發現，以 Wu 為首的電子交易的 H 公司實際上經營地下銀行業務，包括在中華台北、香港和東南亞地區非法兌換人民幣、美元和新台幣等外幣。嫌犯開立 OBU 帳戶並濫用無關的紙品公司的企業形象犯下洗錢罪。匯款額高達新台幣 200 億元，非法收益達 1.8 億新台幣。CIB 根據《洗錢防制法》（擴大沒收）和《刑事訴訟法》於 2018 年 9 月 25 日成功向法院提出動議。在相關銀行帳戶中查獲了相當於 4.3 億元新台幣的款項。透過中華台北和中國的合作，在大陸逮捕了 5 名嫌犯，在中華台北逮捕了 7 名嫌犯。

印尼

案例研究 1

251 2014 年 7 月，HF 宣告效忠 ISIS。然後，他透過電報與 BS（印尼裔的 ISIS 東南亞指揮官）進行通訊。HF 從 BS 獲得指示，支援 MIT 集團（隸屬於 ISIS 的印尼恐怖組織）的需要並發動襲擊。根據對 IFTI 數據的搜索結果，PPATK 發現 2015 年 7 月中東資金流入額達 3,789.77 美元。

252 此外，調查發現 HF 控制其他人的帳戶，用於收取國內恐怖組織的資金。據主管機關稱，這筆資金已於 2015 年 7 月發送給菲律賓的多個涉案方，特別是通過

MSP 發送 10,500 美元，用於購買恐怖組織使用的武器。2016 年 1 月，警方以雅加達塔林大街的槍擊和爆炸事件等罪名逮捕了 HF。此後，HF 因恐怖主義和資恐罪被判入獄六年。

案例研究 2

253 2015 年 5 月，AS 在監獄裡探訪 AA 時遇見了 AJ，他們都是 ISIS 的成員。在會面時，AJ 要求協助動員印尼各方前往敘利亞加入 ISIS。以 AJ 名義進入銀行帳戶的資金來源主要是國內涉案方，金額為 3 億印尼盾（約合 21,428 美元）。這些資金被用於購買前往敘利亞的機票。在 2016 年 4 月，AJ 指示美國透過 MSB 匯款，使用相當於 2 億印尼盾（約合 14,285 美元）的菲律賓比索向 SM 匯款，以購買在印尼進行軍事訓練所需使用的武器。

日本

254 越南裔嫌犯的客戶想要從日本匯款到越南。他們讓客戶將錢匯到他們在日本銀行以其他人名義開設的帳戶。他們用這筆錢購買了便利商品和食品，並以合法交易的名義將其出口到越南。然後，出口的貨物在越南出售，進而轉為現金。此手法實際上相當於國際匯款。嫌犯因違反《懲治組織犯罪法》（隱匿犯罪所得）和《銀行法》（從事地下金融）而被捕。

255 在一項案例中，客戶匯入他人名下帳戶的資金被用於

購買重型機械和農用設備，並將所購買的機械和設備以偽裝合法交易的方式出口到外國司法轄區，並轉換為現金。這種安排實際上相當於國際匯款。

巴基斯坦

256 一名申訴人通報，他接到來自阿富汗和當地的電話號碼，對方敲詐勒索 100 萬盧比。來電者被告知是巴基斯坦塔利班運動的成員，並警告如果不付款，將炸毀他們的房屋。申訴人及其侄子前往白沙瓦某處，並將贖金移交給不明人士。

257 調查顯示，這筆錢是透過哈瓦拉系統轉移到阿富汗。相關單位為此組成聯合調查小組。現金流向報告（CDR）分析揭示了雙方之間的聯繫，進一步的調查發現這兩名被告均與 JuA 有關聯。被捕後，兩人都承認參與移轉贖金。調查顯示，其他涉案人員仍在逃，並被宣佈為通緝犯。後續調查正在進行中。

4.7 網際網路的使用（加密、ID 的存取、國際金融等）

斐濟

商業電子郵件遭駭導致重大損失

258 金融情報中心從 D 銀行收到了可疑交易報告，證明 C 公司是企業電子郵件入侵的受害者。金融情報中心發現，C 公司與其外國供應商往來的商業電子郵件受到轄區 F 的一名駭客入侵。駭客攔截了該電子郵件通信，

並指示 C 公司向國外銀行帳號轉入約 266,000.00 美元。駭客給 C 公司發送的電子郵件地址類似於 C 公司的外國供應商。

259 金融情報中心分別向相關的外國金融情報中心提供了分案報告以供其調查。目前已確定資金隨後在同一天分配給了不同的實體。但是，無法確定資金的最終去向。

潛在罪行：

- 詐欺牟利。
- 一般背信罪。

指標：

- 粗制濫造的電子郵件，使收件人忽略錯誤。
- 在最後一刻變更付款明細和收款人明細。

共謀透過未經授權的網路銀行以利處理非法收益

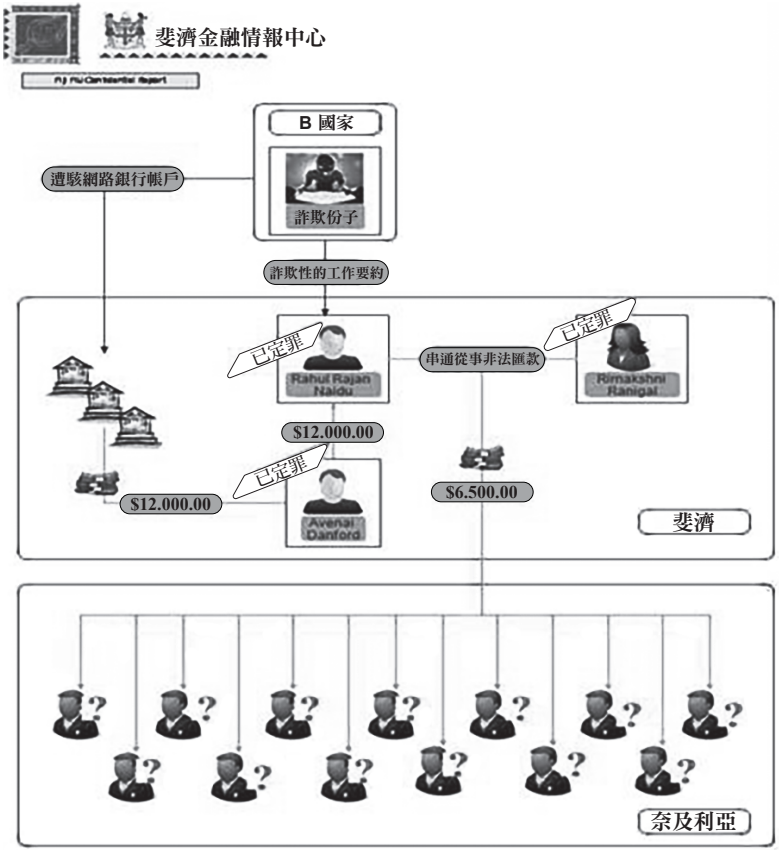
260 Rahul Rajan Naidu 先生收到了「Global Link Money Services 的 Jasmin Olich」的工作要約，工作內容是透過西聯匯款收發金錢，藉此對西聯匯款的服務進行秘密評估。Rahul Rajan Naidu 先生被告知資金只會轉移到西太平洋銀行的一個銀行帳戶，然後他將從該帳戶提款，扣除其佣金並將剩餘的款項匯給奈及利亞特定地區的不同人士。

261 由於 Rahul Rajan Naidu 先生沒有在 Westpac 開戶，因此他與友人，亦即斐濟肉品有限公司的工資主管 Shoeb Nur Ali 先生聯繫，以幫助他找尋 Westpac 帳戶

的人頭身分。Shoeb Nur Ali 先生問他的朋友 Avenai Danford 先生是否願意讓 Rahul Rajan Naidu 先生使用他的帳戶來收取資金。Avenai Danford 先生表示同意，並從網路銀行以未經授權方式將三名受害者的 12,000.00 美元轉入他的 Westpac 銀行帳戶。Avenai Danford 先生提出這些資金，並將其交給了 Rahul Rajan Naidu 先生。

262 Rahul Rajan Naidu 先生隨後要求 Shoeb Nur Ali 先生提供自己以及三位同事的身分證副本。一家外匯交易商的第一線人員 Rimakshni Ranigal 女士使用這些文件以及 Rahul Rajan Naidu 先生獲得的其他身分證件副本用於向奈及利亞發送 12 筆匯款。

263 匯款時，列為匯款發送方的 12 個人都沒有在場，並且他們不知道資金是使用他們的姓名和身分證發送的。2018 年 9 月 4 日，Rahul Rajan Naidu 先生被裁定犯有四項洗錢罪，Avenai Danford 先生和 Rimakshni Ranigal 女士各被判犯有一項洗錢罪。2018 年 9 月 18 日，Rahul Rajan Naidu 先生，Avenai Danford 先生和 Rimakshni Ranigal 女士分別被判處六年九個月、三年和五年徒刑。



4.8 使用新的付款方式 / 系統

澳洲

264 2018 年 6 月，內政部長證實 AUSTRAC 已與澳洲聯邦銀行（CBA）達成協議，其中 CBA 承認違反澳洲 2006 年《防制洗錢和打擊資恐法》（AML/CTF 法）共計 53,750 次）。CBA 同意支付 7 億澳元的罰款，這是澳洲有史以來最大的民事罰款。

265 CBA 承認其智慧型存款機（IDM）導致失職，更具體地說是其 IDM 風險管理的失效以及未能及時提供門檻交易報告和可疑事件報告。CBA 也承認未能充分對客戶和帳戶進行適當監控。

266 CBA 未達到合規標準，導致情節重大的組織化犯罪分子有機可趁，利用金融部門洗淨其違法活動（包括社區販毒）的犯罪所得。

267 該案例提供了組織犯罪活動非常真實的範例，也例示了申報實體未能遵守其防制洗錢 / 打擊資恐義務時，犯罪分子可以利用金融部門的方式。

268 這項處罰是澳洲公司歷史上最大的民事處罰。2018 年 6 月，AUSTRAC 就此事發布了多篇媒體新聞稿：http://www.austrac.gov.au/media/mediareleases。

269 該案的結果向業界發出強烈警訊，即嚴重容忍不遵守澳洲的《2006 年防制洗錢和反資恐法》（AML/CTF 法），而民事處罰程序則例示了合規不彰的真實後果。

270 該案也重申金融機構、其董事會和高層主管員的責任，以確保企業認真履行防制洗錢 / 打擊資恐義務，並確保落實企業文化履行此義務。

中國

案例研究 1

271 2017 年 6 月，嫌犯 D 向其女友（已遭判刑）提供了帶有真實姓名認證的支付寶 QR 碼，以接收毒品犯罪

所得，並將款項轉入女友的遊戲 ID。嫌犯 D 用他的帳目隱瞞了犯罪所得的來源和性質，並參與了洗錢犯罪。2018 年 4 月，法院判處嫌犯 D 有期徒刑兩個月，並處以罰款。

案例研究 2

272 2017 年，嫌犯 E 涉嫌販毒，並使用微信或現金取得毒品費用。嫌犯 E 通過同樣的方式將錢轉移給了他的前妻（嫌犯 F）。法院裁定，嫌犯 F 將其微信帳戶提供給嫌犯 E，隱瞞了犯罪所得的來源和性質，並協助轉移犯罪所得。他們被裁定犯有洗錢罪。2018 年 3 月，法院將嫌犯 F 判處有期徒刑七個月，並處以罰款。

斐濟

操縱內部系統和流程

273 Vika Sadrau 女士受僱於 Post Fiji 有限公司，擔任客戶服務專員，負責處理電子匯票（EMO）。

274 從 2015 年 3 月到 5 月，Vika Sadrau 女士通過操縱 EMO 系統以背信方式獲取 55,779.32 美元。Vika Sadrau 女士為客戶處理了一筆 EMO 交易，並使用相同的 EMO 密鑰 ID 為同一筆交易建立了多筆付款。

275 然後，Vika Sadrau 女士變更了付款金額和收款人詳細資訊，並獲得了其上司的核准以向自己付款。Vika Sadrau 女士共向自己支付了 55,779.32 美元。然後，她將 $21,000.00 存入了她的銀行帳戶。

276 Vika Sadrau 女士承認犯下一項盜竊罪和一項洗錢罪名。2018 年 8 月 22 日，Vika Sadrau 女士因盜竊被判 18 個月徒刑，並因洗錢罪判處 4 年徒刑。此案例研究顯示出違反了內部控管程序的情況。

中國香港

277 在 2017 年 12 月至 2018 年 6 月期間，發現許多儲值工具（SVF）帳戶記錄頻繁的現金加值或來自其他帳戶的轉帳。存款資金不用於進行任何購買，而是主要從相關的個人銀行帳戶中提領，然後將少量資金退還給原始發送者。交易監控發現，某些傳遞消息的參考術語是足球投注和參加國際足球錦標賽的國家隊名稱。SVF 服務供應商懷疑該 SVF 帳戶可能被用於非法賭博，因此向 JFIU 進行揭露。

278 透過 JFIU 的分析，發現一些帳戶持有人申報了同一住宅區中的地址，並且某個帳戶持有人的手機號碼直接連結到非法足球投注網站。SVF 帳戶用於現金加值和轉移來接收賭博集團非法線上足球投注相關的賭注。賭注透過 SVF 帳戶合併，然後根據比賽結果轉移到由集團成員持有的個人銀行帳戶或原始 SVF 帳戶。該資訊已分發給當地執法機關以採取後續行動。

印尼

279 在對 Surakarta（中爪哇省的一個地區城市）發動襲擊之後，從與居住在敘利亞的印尼伊斯蘭國東南亞指

揮官 Y 先生通訊的個人銀行帳戶中查出用於資助這次襲擊的幾筆資金轉帳。金融情報中心和執法機關查明 Y 先生（敘利亞）將大約 1,000 美元的 H 先生（印尼）的帳戶轉入 PayPal。H 先生將 PayPal 餘額轉入到他的銀行帳戶中，並將其轉給 M 先生（印尼）。然後，M 先生將這筆錢轉至多個銀行帳戶，這些資金將兌現並轉交給恐怖分子。參與資助這次襲擊的 M 先生依《反恐公約》被定罪。此外，Y 先生已被列入 UNSCR1267 制裁名單和印尼的國內恐怖分子名單中。

日本

280 一名男性上班族收到詐欺集團成員的電子郵件提供有關電子貨幣的資訊，而他知道該資訊是非法獲取而來。他因違反《懲治組織犯罪法》（收受犯罪所得）而被捕。

4.9 透過稅務犯罪中洗錢

中國

案例研究 1

281 2017 年 12 月，主管機關從某些金融機構收到了四家公司的可疑交易報告。經過進一步調查，主管機關將資訊提交當地警方。警方發現 G 公司假造增值稅發票。2018 年 4 月和 2018 年 5 月，六名嫌疑犯被捕。在撰寫本文時，三名嫌犯仍被拘留，另外三名正在保

釋候審。

282 在 2017 年 1 月至 2018 年 4 月期間，涉案公司虛報了 1,000 多張增值稅專用發票，偷逃了數百萬人民幣的稅款。

案例研究 2

283 2018 年 2 月，主管機關向警方提供有關特製發票的可疑交易報告。2018 年 6 月，警察和地方稅務機關成立了一個聯合小組調查此案。2018 年 7 月，該團隊成功搗毀了四處犯罪巢穴、五個犯罪團夥並逮捕了 23 名嫌犯。該團隊也扣留了 1000 多個公司印章、數百張銀行卡和 USB 鑰匙、80 多個財務帳簿、90 個空殼公司的營業執照、50 個稅控磁碟、數千張偽造增值稅發票，並凍結了數百萬元。

斐濟

通過現金密集型業務洗淨商業犯罪所得

284 據報導，A 公司存入大量現金之後，再用現金購買銀行支票。

285 金融情報中心判定 A 公司在 2016 年和 2017 年未提交報稅單。但是，它的帳戶卻存入大約 640 萬斐濟元。進一步分析發現，股東 O 和他的妻子 P 的銀行帳戶收到了大約 740,000.00 美元的存款，同樣並未提交報稅單。

286 已向 A 公司，嫌犯 O 和嫌犯 P 的稅務機關提供了分案報告以進行調查。

潛在罪行：

- 稅務犯罪。

指標：

- 大量現金存款。
- 利用家庭成員協助逃稅。
- 利用現金密集型業務洗錢。

涉嫌通過業務多元化和利用家庭成員逃漏稅

287 金融情報中心收到了有關嫌犯 A 的交易記錄，據稱其正在將商業資金轉入個人銀行帳戶。嫌犯 A 是 X 公司的董事，並在同一場所經營加油站。

288 金融情報中心進行了財務檢查，確認嫌犯 A 已使用其個人銀行帳戶向 Y 公司付款，以供應加油站的燃料金融情報中心進行了深入檢查，並確定嫌犯 A 收取大量現金和支票，並存入他的個人銀行帳戶中。已經確定，大多數現金和支票都是從 X 公司名下的商業帳戶提領。

289 金融情報中心擁有嫌犯 A 兒子的過往情報，據稱他也可能涉嫌稅務相關犯罪。金融情報中心進行了後續檢查，並注意到了嫌犯 A 及其兒子的未繳清稅額。

290 因涉及稅務犯罪，因此向稅務機關提交了一份報告。

潛在罪行：

- 逃漏稅。

指標：

- 向稅務機關提交的零稅單。

- 將商業資金存入個人帳戶。
- 利用家庭成員逃漏稅。
- 經營多元化事業以逃稅。

利用第三方逃稅

291 Y 公司據報會以員工「償還貸款」的名義存入大量現金。金融情報中心曾經接獲關於 Y 公司類似活動的先前報告。

292 金融情報中心確定，Y 公司在 2016 年至 2018 年期間共收到約 1200 萬斐濟元的存款，並且未提交同期報稅單。進一步的分析顯示，Y 公司的董事是其他疑似涉嫌逃稅活動的公司董事。

293 已向稅務機關發送分案報告進行調查。

潛在罪行：

- 逃漏稅。

指標：

- 大量現金存款。
- 利用第三方。
- 關係企業。

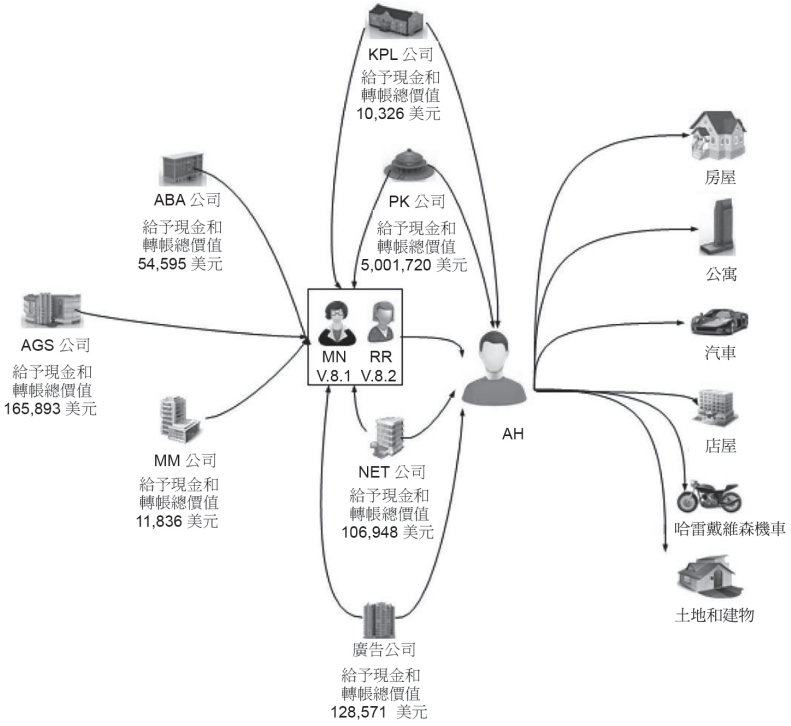
印尼

294 AH 是 LPS 公司的執行長。他根據虛構交易假造稅務憑單，並將其賣給了 7 家公司。他獲得的利潤總計約為 3,510,621 美元。他從出售假造稅務憑單中獲得的大部分所得是現金，其餘則存入他的個人銀行帳戶

中。他也要求員工收取現金並將其存入他的個人銀行帳戶。

295 在其個人銀行帳戶中收到資金後，AH 使用自己和他的家人 / 親戚的名字（例如妻子和孩子）購買資產。他一天之內用現金購買了約 71,428 美元的土地和物業。他也在購買的土地上建造了共住房屋或辦公室，以獲取更多資金並投資於其他公司。為了進一步掩蓋金錢的來源，他將非法資金與公司資金混雜在一起。

296 根據從稅務局獲得的資訊，他以印尼盾存款，但以美元提領。



巴基斯坦

案件背景：

297 嫌犯以其配偶、女兒和兒子的名義在不同的銀行開設了帳戶。為了逃稅，他將紡織業務所得大量資金以本幣和外幣轉入其家庭成員的帳戶。

作案手法：

298 X 先生的個人在不同銀行的不同分行中開設了個人和合夥帳戶。銀行向 FMU 舉報了多個帳戶的其中之一，因為發現在短時間內向該帳戶中存入現金的異常方式。

299 80 筆交易存入大約 6,200 萬巴基斯坦盧比的現金，其中 77 筆交易以分散方式存入。然後，在同一天以「Z」的個人名義使用四種工具領取累積資金，目的是購買房產。值得注意的是，所有分散式現金存款交易都是通過大量存款單在半小時內完成。此外，也發現存款單的簽署人是同一個人。發生在帳戶中的這些活動沒有任何邏輯或經濟意義。此外，客戶沒有提供有關通過現金存入帳戶的資金來源的任何詳細資訊，並且客戶也沒有向銀行提供有關購買物業的文件證據。

300 在分析過程中，發現上述犯罪所得來自嫌犯經營的事業。這些犯罪所得已透過分散式現金交易的方式，經由其配偶的獨資帳戶轉入，以規避向 FMU 報告的義務。

301 搜尋 FMU 的內部資料庫找出了嫌犯的家庭成員的帳戶，並在這些帳戶中發現存有高營業額。值得關注的

是，嫌犯及其家人已經註冊國家稅籍編號。雖然嫌犯本人在各個帳戶中進行高額交易，但只有嫌犯本人繳納了所得稅，而其家人均未繳納所得稅。

302 根據上述活動，遭舉報的個人涉嫌參與逃漏稅活動。因此，金融情報已分案給稅務機關。

4.10 房地產，包括房地產經紀人的角色

中國

303 嫌犯 V 是許多投資和技術公司的法定代表人、股東和主管。其中一間公司推廣一項專案，要求房主使用其房屋來擔保從銀行獲得的貸款。該公司將向房屋所有者支付固定收入，並支付貸款利息和本金。交易對手也包括投資公司、小額貸款公司和商業公司。調查發現，該專案具有非法集資的特點，如果資金鍊斷裂，將產生較高的風險。該案的資訊和情報已提供給警方。

巴基斯坦

304 被告 X 先生在 2004-2006 年期間在英國取得 6 筆房產，價值 6,885,625 英鎊。然後，這些財產在被告控制的公司之間轉售，其價格被抬高到原始價格的 5 到 16 倍之間。在哄抬的價格基礎上，被告人透過不實的房地產估價獲得了總計 49,276,250 英鎊的抵押貸款。在 2004 年至 2006 年期間進行了 20 筆交易，將詐欺取得的 28,883,098 英鎊轉入巴基斯坦銀行。X 先生於

2011 年被英國一家法院判處 13 年徒刑。而被告 Y 先生設法逃往巴基斯坦。據報導，Y 先生隨身攜帶了超過 2,500 萬英鎊的贓物到巴基斯坦。英國主管機關要求提供援助，以追回被告在巴基斯坦非法持有的犯罪資產。開始調查後，國家權責局（NAB）從各個機構和金融機構蒐集了相關的財務資訊，根據《巴基斯坦國家問責制條例》第 23 條，對 12 處住宅和農業用地發布警告（NAB 宣布財產轉移無效）。該案目前正在調查階段。

4.11 人口販運和人員偷渡關聯

阿富汗

305 貨幣服務提供者（MSP）X 充當擔保人角色，收取阿富汗公民的分期付款，用於在國外進行招募。MSP X 與外國組織（XYZ）協調招募事宜，但未遵守招募外籍員工的管理法規。被徵募的阿富汗人將分期付款存入 MSP X 的銀行帳戶中，而 MSP X 未能提供任何證明文件。然後，這些阿富汗人通過阿富汗邊境省份極高風險的路線被偷運到國外。

306 結果，該公司的執照被吊銷，上述案件送交相關執法機關進一步依法處置。

斐濟

307 GC 女士和她的雙胞胎姐妹 SR 女士各自經營旅行社，

並在報紙上刊登廣告，要求有興趣的人前往紐西蘭從事採摘水果和建築工作。該廣告吸引了 17 個人，他們獲得承諾支領高薪、住宿、食物、交通和從早上 7 點到下午 5 點的六天工作時間。這 17 個人獲發紐西蘭訪客簽證，並被告知將於抵達紐西蘭後獲得工作許可。他們也需要支付諮詢費、住宿費、管理費、發放護照和機票費用，每人總計約 3,768.00 斐濟元。

308 這 17 個人僅需在空白的簽證申請表上簽名，再由 GC 女士和 SR 女士填入虛構和誤導的資訊。

309 抵達紐西蘭後，這 17 個人大多是由 FA 先生從機場接走。然後，受害者被帶往住所，且被迫與異性陌生人同住一間臥室，睡在床墊上或地板上，然後在同一房間更衣。受害者有時也必須支付交通和膳食費用，而食物有時未經烹煮或不衛生。個人的薪酬也非常少。

310 某些受害者聯絡 NZP 並通報他們的處境。紐西蘭和斐濟兩地同時對此案進行調查。

紐西蘭

果園工人被控奴役和人口販運

311 霍克灣果園的一名工人最近因在薩摩亞和霍克灣地區犯下的罪行被指控奴役和人口販運。據稱，他以誘人的高薪工作誘使薩摩亞國民來到紐西蘭，但是當他們抵達後護照遭到沒收、控制並嚴密監控行動，並使他們遭受人身攻擊和威脅。他將受害人承包到霍克灣的各

個果園，並從其個人銀行帳戶中獲得外包勞務的款項。

菲律賓

312 菲律賓金融情報中心接獲菲律賓執法機關的轉介，此案為三名菲律賓公民和八名外籍人士涉嫌參與販運人口和兒童色情製品。受訪者在中維薩亞斯經營一個網路色情巢穴，並招募未成年人從事色情行為。2014年，U 轄區都會警察署扣押並沒收電腦、平板電腦、手機、攝影機、硬碟和 DVD，其中包含外籍人士 C 先生擁有的菲律賓兒童的不雅影像和視頻。視頻顯示 C 先生和成年菲律賓女性對菲律賓兒童施加性 / 身體方面的虐待。起獲的文件也揭露多筆匯給向三名菲律賓公民的款項。對這筆資金的追蹤顯示，它起源於 U 轄區和 C 轄區，通過兩名匯款代理人和一家本地銀行轉移到菲律賓，平均每筆匯款為 21.2 萬菲律賓比索。查獲總金額為 238 萬菲律賓比索，其中包括各種匯款和現金存款，以及 206 萬菲律賓比索的提款。調查結果 2016 年發布了凍結令、民事沒收申請並起訴被告從事洗錢。

4.12 使用代名人、信託、家庭成員或第三方

中國

案例研究 1

313 主管機關調查發現，嫌犯 U 利用職務之便挪用了數百

萬元人民幣。然後，嫌犯 U 要求嫌犯 B 將錢存入嫌犯 B 的帳戶。在嫌犯 U 的妻子（嫌犯 O）的安排下，嫌犯 D 提出這筆錢，然後將大部分錢匯給嫌犯 P，而後者是嫌犯 O 丈夫的兄弟。然後，嫌犯 P 以自營旅館的名義將錢轉給了嫌犯 O 的兒子。嫌犯 O 隨後要求嫌犯 D 將剩餘的錢轉給嫌犯 P 的妻子（由嫌犯 O 控制），然後嫌犯 O 將銀行卡交給她的兒子。

314 2018 年 11 月，嫌犯 O 被判處洗錢罪名成立，被判處有期徒刑兩年，緩刑兩年，並處以罰款。嫌犯 P 被裁定相同罪行，並被判處 10 個月監禁和 1 年緩刑，並處以罰款。

案例研究 2

315 嫌犯 Q 接受賄賂，並被判犯有賄賂罪。在調查過程中，嫌犯 Q 和他的妻子要求其兄弟嫌犯 K 轉移數百萬人民幣和數千港元。嫌犯 K 隨後向嫌犯 T 支付現金。2018 年 4 月，法院判處嫌犯 K 有期徒刑兩年零十個月，並判處罰款。嫌犯 T 被判處三年十個月徒刑，並處以罰款。

案例研究 3

316 在對嫌犯 R 的賄賂進行調查期間，發現嫌犯 R 的姊妹嫌犯 G 有洗錢嫌疑。在 2012 年至 2016 年期間，雖然清楚掌握嫌犯 R 的活動，但嫌犯 G 持續保有嫌犯 R 的賄賂犯罪所得存入她的銀行帳戶。然後，嫌犯 G 根據 R 的安排購買了房屋和車輛。2018 年 12 月，嫌犯

G 被判處一年徒刑，緩刑一年和罰款。

中華台北

317 2016 年，上市公司 T 公司的股價低迷了一段時間。C 決定操縱 T 公司的股價。C 先生與股市投機者 D 先生合作，使用他們控制的 42 個證券帳戶買賣大量 T 公司股票。他們利用這些證券帳戶對做，使 T 公司的股票交易活躍起來。他們也發布假消息，謊稱要向 T 公司投資。因此，不知情的散戶誤信 T 公司的股票值得投資，紛紛投資交易 T 公司的股票。T 公司的股價從 2016 年 8 月的每股新台幣 6 元左右漲至 2017 年 2 月的 20 元左右。

318 T 公司董事會於 2017 年 5 月再次當選。C 先生公開謊稱，他將參加選舉並尋求管理權，以使不知情的散戶參與該投資。但是，C 先生等人於 2018 年 2 月至 3 月間（即 T 公司股價升高且交易活躍時）先後以較低的價格先後將 T 公司的股票以較低價格出售給了散戶投資人，並獲得了可觀的利潤。他們實現的利潤總額約為新台幣 11 億元。C 先生等人因違反《證券交易法》於 2018 年 8 月被起訴。

斐濟

違反雇主信任和操縱內部系統和流程

319 Rosheen Praveena Raj 女士和 Rine Munivai Sorby 女士在太平洋神學院（PTC）擔任財務官。他們負責處理

薪資和帳單的檢查。從 2006 年到 2011 年，Rosheen Praveena Raj 女士和 Rine Munivai Sorby 女士操縱該系統，以詐欺方式獲得總計 582,244.42 斐濟元的收益。Rosheen Praveena Raj 女士負責處理所有應付帳款，包括薪資。她篡改了每週薪資單電子表格、付款憑單和支票，藉此分別向自己和 Rine Munivai Sorby 女士支付超額薪資 96,576.86 斐濟元和 73,099.93 斐濟元。

320 Nilesh Avinesh Sharma 先生於 2012 年獲任命為財務與行政總監時，發現了這項詐欺行為。他在財務記錄中發現了重大異常，並進行了內部調查和稽查，以查明這些異常的原因。Rosheen Praveena Raj 女士和 Rine Munivai Sorby 女士也篡改了帳單支付發票，向自己給付總計 412,567.61 斐濟元的款項。2018 年 9 月 18 日，Rosheen Praveena Raj 女士和 Rine Munivai Sorby 女士分別被判兩項洗錢罪。2018 年 9 月 19 日，Rosheen Praveena Raj 女士和 Rine Munivai Sorby 女士分別判處 11 年和 10 年徒刑。

不同轄區無關人員之間的重大資金流動

321 金融情報中心接獲有關嫌犯 Y 的可疑交易報告，因為他從某個不相關的個人（轄區 D 中的嫌犯 X）接收了總計約 167,000.00 斐濟元的匯款。

322 嫌犯 Y 聲稱這筆資金是用於建設嫌犯 Y 的房產。斐濟金融情報中心確認，嫌犯 Y 在 2018 年購買了價值

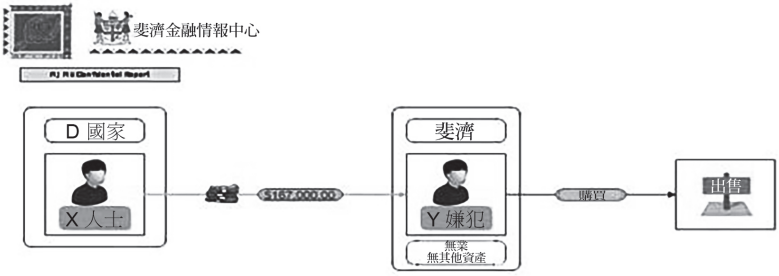
100,000.00 美元的土地。嫌犯 Y 在過去兩年中沒有申報任何收入，並且似乎沒有工作。

323 金融情報中心也發現，嫌犯 X 可能是司法轄區 D 的執法部門關注對象，並可能利用嫌犯 Y 在斐濟洗錢。

324 一份報告已分發給斐濟警察情報局和轄區 D 的金融情報中心，以作進一步分析。

潛在罪行：

- 洗錢罪。
- 逃漏稅。



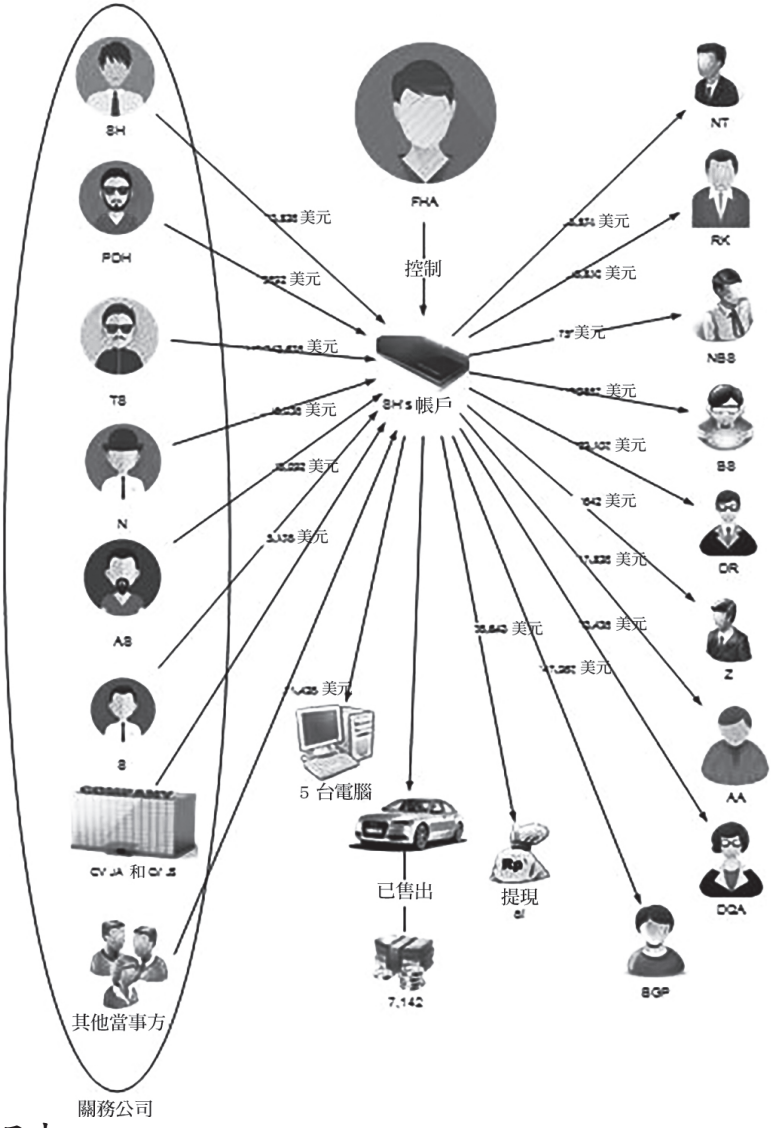
指標：

- 沒有明顯既定關係的本地和海外個人之間的大量匯款。

印尼

325 FHA 是印尼財政部海關總局的分析師。其經手分析的關務公司向他行賄，而 FHA 則借用 AMJ 公司所有者 SH 的帳戶存放這些賄款。AMJ Co. 也是被分析的公司之一。將 SH 帳戶中的資金轉移到不同的帳戶中洗錢

後，這些帳戶隨後用於購買資產，例如汽車和電腦。



日本

326　在一家貿易公司工作的男子以他人名義簽下合約，在

知情之下將一輛贓車藏匿在某個貨櫃堆場的倉庫中。他因隱匿贓物和違反《懲治組織犯罪法》（隱匿犯罪所得）而被捕。

327 該嫌犯在知情之下收取賣淫犯罪所得，作為保護費匯入以暴力團（日本組織犯罪集團）成員的女兒名義開立的銀行帳戶。

中國澳門

328 一名可疑交易報告揭露 2015 年 9 月至 10 月期間，A 先生曾在轄區 H 的一家運輸公司擔任會計部副經理，從其司法轄區 H 的銀行帳戶收到了多筆共約 600 萬的匯款。此後，A 先生用自己的現金卡在中國澳門的珠寶店購物，並將資金轉給了他的前女友 B 女士。B 女士的銀行帳戶經過審查，發現自 2015 年起使用存款機存入大筆現金，款項來源即為其男友。

329 在 2016 年 3 月，這家船務公司發現 A 先生涉嫌在 2010 年至 2016 年期間貪污約 3.8 億港元。船運公司在轄區 H 向執法機關舉報此事。獲悉部分非法資金被轉移到中國澳門後，船運公司派遣代表前往中國澳門向當地司法部門提起訴訟。2018 年 1 月，該新聞報導司法機構警察逮捕了 B 女士。她的家庭成員也因購買物業、汽車和貴重物品而被起訴洗錢罪名。扣押的資產總值約 4000 萬港元，其中包括現金。

330 為支援案件調查，金融情報中心發現 B 女士的銀行帳

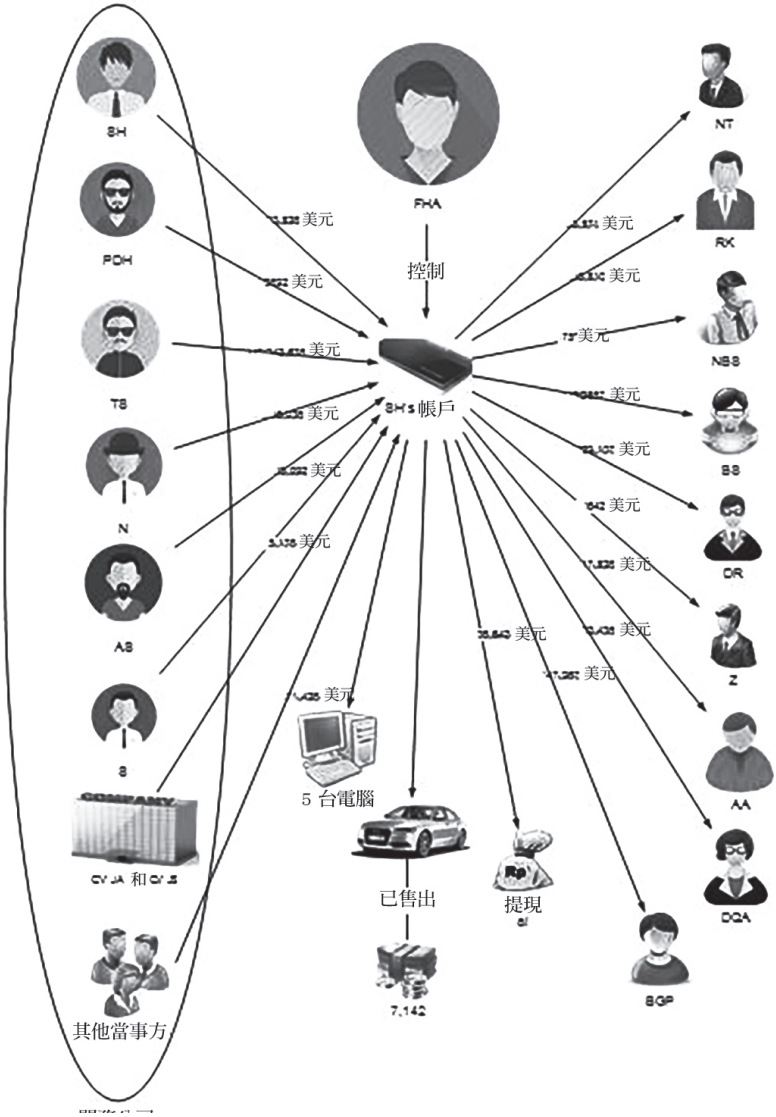
戶資金流入不規律，2015 年突然增至 2100 萬港元以上。然後，這些資金被用於購買財產和貴重物品，並加以轉售。B 女士將銷售後的犯罪所得匯回給 A 先生。在 A 先生的舞弊行為在轄區 H 曝光後，A 先生利用其前女友 B 女士及其家人將犯罪所得分層放置於中國澳門，引起當局高度懷疑。司法警察最終將此案移交給了公訴機關。

新加坡

使用代名人 – 成立空殼公司以收取境外賄款

331 CPIB 根據收到的線索採取行動，對金融情報分析後研判存在一個由新加坡企業組成的網絡，其可能由外國人控制，用於收取境外司法轄區的可疑來源資金或進行洗錢。其中兩家新加坡公司可能已經收到涉及行賄重要政治性職務人士的款項。

332 當局對這兩家新加坡公司以及涉及當地企業網絡的相關董事進行調查。初步調查發現董事是代名人，他們提供姓名來登記成立公司，並為公司開設銀行帳戶，藉此換取費用。然後，代名人再讓實質受益人完全控制公司銀行帳戶。這些新加坡公司貌似是空殼公司。他們的登記地址屬於註冊申報代理實體（「RFA」），這有助於公司的成立。CPIB 與 RFA 的主管機關合作，共同對該 RFA 進行檢查。此外，也向外國主管機關所取各種個人和實體的相關金融情報。相關調查正著手進行中。


SH
PDH
TS
N
AS
S
COMPANY
CV JA 和 CV JS
其他當事方
FHA
控制
SH's 帳戶
美元
5 台電腦
已售出
7,142
提現
NT
RK
NBS
BS
DR
Z
AA
DQA
BGP

4.13 賭博活動（賭場，賽馬，網路博弈等）

中國

案例研究 1

333 四名嫌犯開設了銀行帳戶，並網路銀行向許多客戶轉移資金，並在每次交易前測試轉帳功能。帳戶資金進出迅速，餘額極低，且 IP 位址在許多地方頻繁變更。上游交易對手包括曾因涉嫌參與線上賭博而遭主管機關調查的客戶。此案涉及金額高達數百萬人民幣，而相關情報已提供給警方。

案例研究 2

334 與此案相關的十四家公司同時在同一地點開戶。所有帳戶都使用相同的相同字元，並且所有聯繫電話均已重新註冊。交易備註 / 參考詞彙包括「加值」和「相似的 6 位會員編號」等。交易可以在一天中的任何時間進行，其中一些發生在午夜和凌晨。IP 位址集中在賭博的高風險區域。此案涉及金額高達數百萬人民幣，而相關資訊 / 情報已提供給警方。

中華台北

335 CIB 偵查第四大隊突擊檢查博彩網站。在 2018 年 9 月 5 日追蹤由嫌犯 Hsu 主持的「北京 PK10」在線博彩網站後，循消息來源查獲另一名嫌犯 Yao（幕後網管和莊家）。在檢查了監視影像並駕車追蹤嫌犯之後，偵查大隊發現他們住在同一社區。為了防止嫌犯

轉入另一個地區，偵查大隊立即向地方法院申請了搜查令。在 2018 年 9 月 17 日進行第二次搜查時，偵查隊在停車場逮捕了另一名嫌犯 Peng。嫌犯供認經營一個線上博彩網站。搜尋住所時，偵查隊發現 Peng 曾使用自己的「數鈔機」來檢查每週的下注金額。該集團旗下六個獨立投注代理人每週下注額各約為新台幣 1,000 萬元，該網站在六個月內的下注額超過了新台幣 10 億元。警方扣押包括現金新台幣 1,982,000 元、兩部手機、帳冊和數鈔機在內的證據。該案最後以賭博罪起訴嫌犯。

中國香港

336 2017 年 9 月，HKP 情報顯示 A 先生是一家博彩集團的策劃者，其在中國香港從事在線賭場、賽馬和足球博彩事業。A 先生可能也將其業務擴展到附近的其他司法轄區。當局對此展開平行財務調查。

337 警方在 2018 年 6 月採取執法行動，拘捕 45 名涉嫌賭博的相關罪行，並拘捕 5 名涉嫌賭博和洗錢的疑犯，扣押 200 萬港元現金，並扣押 168 萬港元的現金。相關調查正在進行中。

日本

338 暴力團（日本組織犯罪集團）的前成員在知情之下收取非法博弈商店以現金犯罪所得繳納的保護費（95 萬日元）。其因違反《組織犯罪懲治法》（收受犯罪所

得）而遭逮捕。

大韓民國

339 嫌犯 J 和其他 64 人是經營非法線上博弈網站的集團成員。在大約 2011 年至 2018 年 9 月之間，他們在中國、泰國和其他地區開設並營運了體育博彩網站，例如「Cola」、「Pasta」和「Y」，並且涉嫌將經營這些非法賭博網站的犯罪所得匯入借用或假名持有的帳戶，或以現金購買房地產後轉移所有權。

340 2017 年 5 月 24 日，相關單位接獲疑似犯罪活動的報告後展開初步調查。在調查過程中，總共執行了 82 份逮捕令和許可：25 份搜查和扣押令（針對財務帳戶）、27 份搜查和沒收令（針對住宅場所等）和 30 份通訊日誌存取權限。大約有 15,000 名賭徒和 1092 億韓元的賭資經查獲涉嫌參與其中。查獲的犯罪所得（現金提款）為 89 億韓元，並保留約 131 億韓元的犯罪所得。

詳細內容如下：

明細（房地產、現金等）	保留金額
4 間公寓（112m^2、188m^2 等）	54.75 億韓元
土地（1,150m^2）、室內高爾夫模擬器（租賃押金）、3 間網吧	18.50 億韓元
進口汽車 8 輛（奔馳、奧迪等），韓國國產汽車 3 輛、進口兩輪車 6 輛	10.547 億韓元
現金	334.586 億韓元
229 個隱匿犯罪所得帳戶	18.838 億韓元
室內高爾夫練習設施（高爾夫球組、電腦等）	1.87 億韓元
總計	131 億韓元（扣押：4,017.8 百萬韓元；在起訴前保留：90.83 億韓元）

341 如上所示，警方查獲 1092 億韓元的賭資，並扣押以下物品：i）4 間公寓、ii）包括土地在內的房地產、iii）進口豪華車輛以及 iv）現金和用來隱匿犯罪所得的帳戶。主管機關追回總計 131 億韓元的犯罪所得，並將其退還國庫，同時逮捕了 140 人（其中 11 人被羈押），並將其送交檢察署起訴。

紐西蘭

組織犯罪集團透過紐西蘭賭場清洗犯罪所得

342 在 18 個月內，NZP 至少策畫六起的刑事調查，其中涉及透過 NZ 賭場洗淨犯罪所得的行為。洗錢的基本方法包括使用犯罪所得進行賭博，非法現金裝入博弈機具後，再以賭場支票「退款」，以及將非法資金貸

記到賭場帳戶並將其轉入常規銀行帳戶。為疑似洗錢集團工作的現金運送者也會向賭場顧客「投放」現金。在賭場流失的現金中，疑似有一部分來自國內毒品交易。接受這些資金的賭場顧客是否主動參與洗錢計畫，或只是非正規價值移轉系統的不知情使用者，尚不得而知。

越南

343 2017 年，越南警方起訴一起涉嫌利用網路侵占財產的賭博案件，接受調查的當事人和參與者為數眾多且遍及越南各個省份和城市，甚至有執法人員涉案。在此案中，涉案者成立了一家 IT 企業，並濫用了 IT 領域的運作方式來組織線上博弈，例如投注或紙牌遊戲。這些涉案人利用許多犯罪手法，例如電信卡、遊戲卡、賭博遊戲加值、連接其他公司的支付閘道、成立代理投注站以牟取賭博利潤等。

344 這個賭博網路規模龐大，可以隱藏和合理化非法利潤。涉案人採用了不同做法，例如對專案投資、對業務注資、購置房地產、存款、兌換黃金、外幣並轉移到境外轄區。調查人員指出，用於洗錢的總金額約為 38,000 美元。

345 越南最高人民法院於 2018 年 11 月起訴並裁定 92 人犯有以下罪行：「組織賭博」、「賭博」、「洗錢」、「非法取得票據」、「濫用執法職務及 / 或權力」、「使

用網路、電信、電子設備侵占財產。」其中四人「洗錢」罪名成立。主管機關從被定為洗錢罪名的人中收回了大約 90% 的收益。

泰國

346 當地發生非法組織的網路賭博案件。罪犯使用銀行帳戶收取資金以購買遊戲點數，並且定期進行變更以避免觸發大量交易警示而導致帳戶凍結。組織者將所得款項用於購買資產。2019 年查獲 28 起案件，被扣押或凍結的總資產超過 2000 萬泰銖（66 萬美元）。

4.14 混合式（商業投資）和投資詐欺

馬來西亞

案例研究 1：非法和詐欺性投資計畫

347 馬來西亞主管機關阻止涉嫌非法和詐欺性投資計畫的集團活動。這項聯合調查涉及馬來西亞中央銀行（BNM）、馬來西亞皇家警察（RMP）、稅務局（IRB）、馬來西亞公司委員會（CCM）和馬來西亞合作社委員會。

348 這些組織通過在短時間內提供高報酬來吸引國內外公眾參與他們的金融騙局。

349 非法犯罪手法涉以下內容：

- 民眾受誘使簽訂短期合約，以購買由集團生產的加密貨幣，而集團聲稱這些貨幣有黃金的支持。

- 計畫聲稱這些黃金是由集團保留用於交易目的。
- 該計畫也聲稱可以提供高達每月 15% 的高報酬。

350 主管機關的聯合調查的在於是否違反有關非法和詐欺投資計畫的法令。目前調查仍在進行中。該集團也因涉入在 A 轄區的交易活動，使 A 轄區主管機關對其展開非法存款犯罪的調查。

351 在調查過程中，扣押超過 400 萬美元的銀行帳戶和豪華車輛等其他資產。

352 使用的洗錢方法包括：

- 購買有價資產；
- 電匯 / 使用外國銀行帳戶；
- 使用虛擬通貨使用；以及
- 混合資金（商業投資）。

4.15 使用空殼公司 / 企業

澳洲

利用勞動密集型企業網絡

353 據記錄，從 2015 年到 2018 年，利害關係人（POI）與七個從事清潔、安全和建築產業的法人實體進行超過 1500 萬澳元的現金提款交易。

354 疑犯的財務活動的特點為大量現金交易流入公司和個人帳戶，並展現出下列洗錢風險指標：

- 每間公司同時擁有多個銀行帳戶；

- 公司並未商品和服務稅（GST）稅籍；以及
- 並未為員工註冊隨賺隨付（PAYG）的扣繳稅籍

355 此外，疑犯可能試圖混淆公司事務：缺乏透明的預訂保留做法（即向倒閉公司清算人提供的基本記錄）；清算後不久建立與破產實體名稱相似的新公司；回溯職員任職日期，以及可能使用人頭董事。

356 該活動顯示，疑犯正在利用這些公司來協助洗錢、從事非法的詐騙活動和潛在的避稅行為。

中國

357 嫌犯 D 經常將轉帳許多公司和個人。在短時間內進行的單方面交易涉及金額總計達數百萬人民幣。資金被快速、分別地轉入和轉出帳戶，大部分交易是跨省進行，而且轉匯的資金涉及多層關係。交易總是在凌晨和通過網路銀行進行。IP 位址集中在毒品的高風險區域。所有金融對手都是當地銀行，其中大多數在 2018 年年中註冊，一些機構已遭撤銷。主管機關懷疑，在一家空殼公司的掩護下，嫌犯 D 及其同夥通過監管不善的金融機構轉移了毒品犯罪所得。

中華台北

358 一家造船業者 A 公司於 2014 年 10 月標得新台幣 349 億元共計六艘船的建造案，並於 2014 年 11 月簽訂合約。然而，A 公司的營運資金嚴重短缺，因為其資本僅為新台幣 5.3 億元，並且已在中國挹注大量投資。

A 公司總裁 E 先生認為，A 公司資金嚴重短缺可能無法通過銀行的聯合貸款信用調查。因此，E 先生和其他同夥偽造了相關文件，將 A 公司的資本從 5.3 億新台幣浮報到 40 億新台幣。提供這筆聯合貸款的 9 家銀行在 2016 年 2 月因誤信而核准信貸額度，總額為新台幣 205 億元。

359 為了申請過渡貸款、撥款等，E 先生及其同夥偽造了商業文件，包括採購合約、商業票據、採購請款單等，以假裝 A 公司根據造船專案的必要性而採購相關設備，船隻所有權則登記於境外空殼公司 AZ、OK、L3、HS 和 QY 的境外空殼公司皆由 E 先生的兒子擔任註冊董事長。2015 年，E 先生和其他同夥詐欺性地申請了五次過渡貸款，總金額約為 6,800 萬美元。2016 年，E 等人多次詐欺申請循環資金，總額約 1.34 億美元。

360 為了避免調查，E 先生將上述境外空殼公司存於外國銀行帳戶中的部分資金轉移到 E 先生控制的中華台北自然人或法人帳戶中。然後將資金轉入公司 A 的帳戶。境外空殼公司帳戶中的其餘資金用於投資或其他目的。

361 2018 年 2 月，檢察署起訴 E 先生及其同夥違反《公司法》、《商業會計法》、《刑法》和《洗錢防制法》。

日本

362 嫌犯欺騙了一家金融機構，使其以融資貸款名義將資金存入空殼公司的帳戶中。

紐西蘭

紐西蘭空殼公司被用來進行保加利亞、英國、馬紹爾群島和伯利茲的洗錢計畫

363 NZFIU 從合作夥伴金融情報中心接獲有關一家紐西蘭註冊公司的資訊，該公司由於涉嫌參與跨國洗錢而受到海外執法部門的關注。該紐西蘭公司是某家英國公司的唯一股東，後者的銀行帳戶則收取一家保加利亞公司的可疑犯罪所得。NZ Company 的董事和股東是一群 NZFIU 熟知的俄羅斯國民，他們併入了 NZ 公司架構，隨後又在海外司法轄區（主要是東歐）參與了洗錢計畫。幾乎可以肯定的是，該紐西蘭公司是一家空殼公司，形成了一系列複雜企業結構的一部分，旨在掩蓋海外司法轄區的資產和金融交易的實質受益權。

紐西蘭空殼公司被懷疑是朝鮮和伊朗武器販運網絡的一部分

364 合作夥伴金融情報中心報告掌握一家紐西蘭空殼公司，該公司第三方境外公司委託協助海外交易。紐西蘭空殼公司涉嫌參與北朝鮮和伊朗武器販運網絡。交易對手是位於避稅天堂轄區的其他空殼公司。該紐西蘭公司由一小群居住於紐西蘭的俄羅斯國民註冊成立，主要為境外的高財富客戶提供信託和公司註冊服

務。這些人設立的許多紐西蘭公司，後來都成為海外執法機關調查跨國洗錢 / 逃漏稅案件的關注對象。

菲律賓

365 A 委員會（AC）申請協助，以獲取轄區 A 境內正在面臨訴訟的某些個人和實體使用的銀行帳戶文件。AC 是依據根據菲律賓公司登記處簽署的《諮詢、合作與資訊交換的多邊諒解備忘錄》（MMoU）來請求協助。

366 據稱，申請檢查的帳戶被用於輔助從事非法活動，特別是未持有必要的金融服務執照、具有誤導性或欺騙性的行為，以及不合情理的金融服務業務。

367 經過調查，AC 發現一項計畫，旨在誘使包括當地居民在內的投資人將資金投入所提供的二元期權產品。投資人受到指示，以 AMPL 的名義將資金存入 A 轄區的銀行。在 48 小時內，這筆錢通過國際資金轉帳轉移到了世界各地。實際上，AMPL 負責協助將投資款項匯給各種國際實體。估計顯示，2016 年上半年大約有 280 萬美元存入 AMPL 的銀行帳戶，其中約 210 萬美元的資金分散到全球各地。審計委員會瞭解到，資金已經轉移到了由 EAS、SS、CDS 和 YI 控制的實體和銀行帳戶中。

368 AMLI 似乎已從 AMPL 接收匯款。因此，AC 研判 AMLI 可能是由 AMPL 擁有和經營的關係企業。因此，它要求 AMLI 和其他相關個人或實體提供 2014 年 7

月至今的銀行單據。

369 檢查 ST、AMLI 和 DTI 的銀行單據後發現，他們與 AC 提及涉嫌非法活動的個人和實體進行交易。這些交易的主要特點是從國內銀行帳戶匯出款項。

370 同樣重要的是，匯入轄區 A 國內銀行的款項可能來自個別的詐欺計畫受害者。這些將於後文詳細討論。AC 共享的資訊未提及外國實體 W 公司。但是，調查得到的資訊顯示，YI 向該公司轉移了大量款項。

371 AMLI 的公司章程顯示，ST（轄區 I 的居民）是 AMLI 的發起人之一。根據 AC 調查，AMLI 是接收 AMPL 資金的實體之一。此外，網際網路搜索顯示，ST 是 TGL 的營運長，TGL 是另一家疑似從 AMPL 獲得資金的公司。調查顯示，ST 是眾多公司匯款的受益人，其中一些是由 ST 本人控制的，也有個人與 AMPL 有關（如 AC 所述）。

372 ST 也是 TGPL 的匯款的受益人，TGPL 是 A 轄區法院的公司被告之一。而這些匯款是在檢查其與當地銀行的交易過程中所發現。IMC 同樣是聯邦轄區 A 法院的公司被告之一，該公司被發現使用當地銀行帳戶以 ST 名義匯款。

373 必須一提的是，ES 是 AMPL 旗下 WB 公司帳戶的資金接收人之一，也是 AC 起訴的個別被告之一。據確定，ES 向其本地銀行帳戶中的 ST 進行了兩次匯款。

374 ST 也是 ALALI 的總裁。ALALI 於 2014 年 12 月 18 日獲得了公司登記證。它的主要營業地點在 MCity 的 XX 公寓。法定股本異常少量，僅 190.00 美元，且分為五股，每股面值 38 美元。顯然，這筆款項不足以支持其營業目的，或以公司身分展開的任何相關業務。

375 AMLI 在 2014 年 9 月 30 日獲發公司登記證。其主要營業地點位於 M 市 XX 公寓應該強調的是；這與公司章程中規定的 ALALI 的主要辦公室地址相同。與 AMLI 相似，法定股本僅極少量的 190.00 美元，分為五股，每股面值 38 美元。雖然授權資本存量極低，但 AMLI 仍以其名義保留了許多銀行帳戶。

376 也應強調的是；根據審計委員會的說法，轄區 A 的客戶必須將資金存入菲律賓境內的某些本地銀行帳戶。檢查對帳單發現有六筆匯款，全部來自德國司法轄區 A，金額龐大且已記入上述當地銀行帳戶。值得注意的是，所有這些都是在 2015 年 6 月發生的。

377 調查進一步顯示，AMLI 正在與 AC 認定在 A 轄區從事地下金融服務業的數名個人和實體進行交易，而 AC 也針對這些個人和實體申請法院命令。AMLI 向 AMPL 進行了 9 筆匯出匯款。除了上述可疑活動外，在調查過程中也發現，AMLI 和 TGL 之間存在國際匯款活動。

378 設址於 A 轄區的 IMC 是 AC 獲得法院命令禁止其在

A 轄區從事地下金融服務業的實體之一。AMLI 的另一個本地銀行帳戶已被發現用來將款項匯入有受益人身分的 IMC。

379 US 是轄區 A 的聯邦法院禁止從事地下金融服務業的實體之一。對 AMLI 本地銀行帳戶的檢查顯示，其已向 US 匯入一筆行政費用。

380 菲律賓公司登記處於 2011 年 7 月 29 日向 DTI 頒發了公司營業登記證。值得關注的是，ST 在開設本地銀行帳戶時出示了聘雇證明，文件規定 DTI 是 IMC 的子公司之一。對 DTI 在當地銀行的帳戶進行的調查顯示，它已從 IMC 收到國際匯款。

381 YI 是 ASIC 在聯邦法院 A 提起的訴訟中的被告之一。據 ASIC 稱，存入 AMPL 銀行帳戶的錢已轉移到了 YI 控制的實體和銀行帳戶中。調查顯示，YI 向一家當地銀行匯了四筆匯款，金額都皆十分龐大。

382 在仔細檢查了上述人員的銀行單據和關聯交易之後，可以完全確認他們之間有密切關聯且參與明顯的洗錢計畫。轄區 A 的個人已向 AMLI 的本地銀行帳戶匯入鉅額款項。相對的，AMLI 的銀行交易顯示匯入 AMPL、TGL、IMC、US 和 ST 的款項。

383 ST 是 AMLI 和 ALALI 的發起人，是 AMLI、TGL、IMC 和 ES 的多筆匯款的受益人。另一方面，IMC 和 YI 分別向 DTI 和 W 公司進行了國際匯款。

384 調查進一步顯示，AMLI 和 ALALI 具有空殼公司的典型特徵。兩家公司的相似之處非常明顯。

舉例而言：

	AMLI	**ALAL**
成立日期	2014 年 9 月 30 日	2014 年 12 月 18 日
主要營業目的	為我們的客戶開發軟體應用程式；支持其商業流程（包括系統整合），但前提是（h）不得從事網際網路服務供應商的業務。	為我們的客戶開發軟體的應用程式，以支持他們的業務流程，包括所提供的系統整合，但是該客戶不應作為網際網路服務供應商
主要營業地點	M 市 XX 公寓	M 市 XX 公寓
股份有限公司	1. ADR 2. AH 3. AP 4. ST 5. DWR	1. ADR 2. AH 3. AP 4. ST 5. GC
授權股本	一百九十美元（USD190.00），分為五（5）股，每股面值三十八美元（USD38.00）	一百九十美元（USD190.00），分為五（5）股，每股面值三十八美元（USD38.00）

385 這些公司顯然從事高度可疑的行為，這一事實在檢查其金融交易時變得更加明顯。雖然這些公司的資本異常低廉，但它們已經進行了大量交易。值得注意的是，幾乎全部都是匯款。

386 雖然 ASIC 的申請確實只提到了與本地銀行帳戶有關的文件，但可能並未察覺在洗錢計畫中利用菲律賓金融機構的程度。因此，有必要即時流通調查過程中獲得的資訊和相關文件。這是為了符合我們聲明的政策，如《共和國法案》第 2 款所明訂。第 9160 號美國法修正案（也稱為 2001 年《洗錢防制法》）擴大了跨國合作偵查和起訴洗錢活動參與者的範圍。

387 此外，鑑於在明顯的犯罪活動中濫用菲律賓法人的身分，因此也強調必須根據其與金融情報中心的《備忘錄》向公司登記處分享本次調查的結果。

4.16 貨幣兌換 / 現金轉換

中國

案例研究 1

388 嫌犯 E 是四個相關帳戶的實際控制人，而這些帳戶分別由他自己和其他三人持有，用來存放澳幣、加幣、美元和其他外幣的現金然後，嫌犯 E 通過網路銀行將錢兌換成港幣，並在多個分行提領現金。每次提款金額少於五千港元，以免被發現。嫌犯 E 涉嫌非法外匯交易。該案涉案金額為數百萬港元。E 嫌犯於 2018 年 7 月被捕。

案例研究 2

389 2018 年 1 月，主管機關發現嫌犯 F 和 G 的銀行帳戶

參與外匯交易。在 2011 年 9 月至 2017 年 12 月期間發生了許多不尋常的交易，高達數百萬人民幣通過臨櫃和 ATM 進行轉帳。這與現有資訊不一致，該資訊顯示嫌犯 F 和 G 已失業。

390 在調查過程中，主管機關發現無論匯率損失多少，都有大量錢款轉入和轉出嫌犯 F 和 G 的帳戶，通常以外幣存入，然後以港幣現金提領。為了避免被發現，每天的存款額少於五千美元。嫌犯 F 和 G 被懷疑從事非法外匯交易。F 嫌犯於 2018 年 12 月被捕。

斐濟

未申報的貨幣兌換

391 金融情報中心接獲換匯商針對嫌犯 M 提出的可疑交易報告，該嫌犯 M 是歸化的斐濟公民，經常前往轄區 Z。嫌犯 M 受 X 和 Y 兩人委託進行了三筆外匯交易，總計約 30,000.00 斐濟元。

392 斐濟金融情報中心進行了財務分析，並確定 30,000.00 斐濟元並非來自嫌犯 M、X 和 Y 的銀行帳戶。有人懷疑這些人將現金留在家中，並在轄區以外洗錢。相關單位向 FRCS 發送分案報告，以進行概要分析和調查。

潛在罪行：

- 未申報邊境貨幣報告。
- 洗錢。
- 可能與稅收有關的罪行 / 逃漏稅。

指標：

- 當事人未填寫邊境貨幣報告單。
- 當事人以他人的名義（尤其是未成年人）交換資金。

中國香港

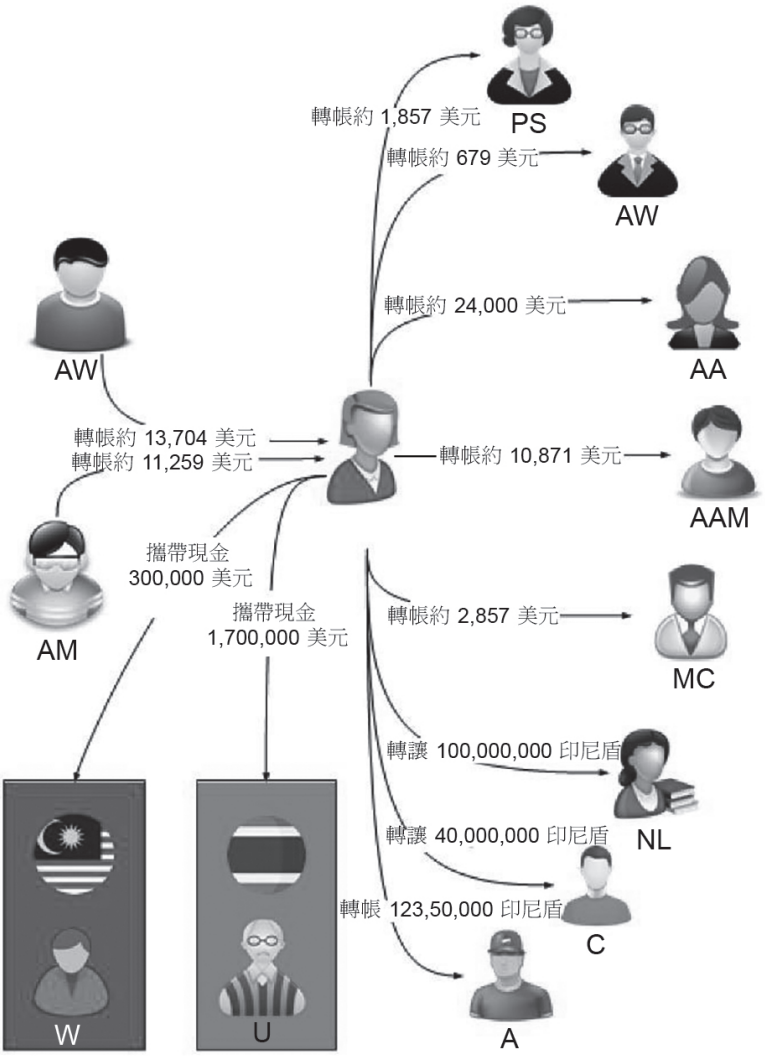
393 一家從事禮品貿易業務公司的銷售經理向其雇主謊稱，他已收到不同轄區客戶的 50 份銷售訂單。銷售經理向其雇主申請預付款 277 萬元人民幣（超過 340 萬港元），應付給中國的兩家供應商。他的雇主相信這項請求的真實性，所以將 277 萬元人民幣匯入了中國兩家供應商的指定帳戶，該帳戶由中國香港一家合法貨幣服務營運商的兩名代表持有。在 2012 年 11 月 23 日至 2014 年 11 月 26 日期間，MSO 的代表安排將 310 萬港元和 310,000 港元的相應款項從他們的銀行帳戶轉入中國香港的銷售經理的銀行帳戶。

394 2018 年 2 月，銷售經理因在知情之下處理有犯罪跡象的所得利益，而被裁定兩項罪名成立並判處四年徒刑。

印尼

395 HR 是 KM（又名 PR）的妻子。HR 一直在 PR 擁有的匯款公司中工作。HR 的帳戶用於存放毒品銷售所得。HR 也將這筆錢帶到國外兌換成其他貨幣。以現金或匯給 HR 的款項被轉換成美元，並在泰國和馬來西亞

收取。HR 每次旅行都攜帶 250,000 美元到 350,000 美元，總計約 2,000,000 美元。



4.17 貨幣走私

阿富汗

案例研究 1

396 在轄區內國際機場中，政府相關部門人員徹底搜查了 X 先生的提包。搜查結果顯示，嫌犯在手提袋中的嬰兒尿布中藏有 170 萬印度盧比。由於嫌犯無法提供起獲現金的任何文件，因此被捕。

案例研究 2

397 X 和 Y 先生在國際機場因被查獲手提包中走私貨幣而被捕後，聲稱是在某些機場職員的協助下將現金轉移到國外。相關單位根據嫌犯此一說法進一步調查，結果發現涉案者遊說了機場職員，以協助他們在轄區內走私一定數量的美元和沙烏地里亞爾。最終，四名機場職員與嫌犯一起被捕。

案例研究 3

398 來自轄區 A 的嫌犯 A 通過機場安檢，但是在嫌犯離開機場航站樓後不久隨即引起懷疑。邊防警察在懷疑之下對該人的行李進行了實體搜查，結果發現該人用化妝包暗藏一定數量的美元和沙烏地里亞爾。航站大廳的安全檢查（包括 X 光掃描）均未能檢測到偽裝成化妝品挾帶的外幣。該案已轉交執法機關進一步調查。

案例研究 4

399 在國際機場中，邊防警察懷疑嫌犯 X 和嫌犯 Y 的舉

動，當時 X 先生的行李在航空公司櫃檯的行李檢查站引起懷疑。基於這種懷疑，對 X 先生的行李進行實體搜查，結果發現行李中裝有重 11 公斤以上的金條。

400 X 先生聲稱將這些金條用鞋子穿入機場，然後在通過 X 光掃描後將它們放在行李箱中。但是監視錄影顯示，X 先生和 Y 先生同時進入洗手間，兩人各提著一個袋子。離開洗手間時，X 先生拿著兩個袋子出現在錄影中，而 Y 先生空著手離開洗手間。此外，錄影也顯示，X 先生將行李寄存在航空公司櫃檯後，Y 先生便離開了航站樓。在這種情況下，Y 先生可能在機場職員的協助下將金條帶入了機場。

401 在主管機關徹查此案後，X 先生依現行法律和法規遭罰款 490 萬阿富汗尼（相當於 72,558 美元）。

汶萊和平之國

案例研究 1

402 2018 年 2 月，三名外國人被發現以超過申報門檻的多種貨幣穿越汶萊國際機場且未作申報。涉及的貨幣包括馬來西亞林吉特、越南盾、泰銖和新加坡元，以現金形式藏在他們的行李裡。海關官員通過例行檢查和 X 光掃描發現了此違法活動。後來發現，這些人計畫將資金越過陸地邊界運到鄰國。當局根據 2012 年《犯罪資產追回令》第 37 條第（2）款（未申報）起訴當事人並處以罰款 5,000 巴西里爾，或每人監禁 5 個月。

案例研究 2

403 2018 年 3 月，發現一名外國人越過陸地邊界前往汶萊，攜帶高於申報限額的汶萊元和新加坡元且未申報。現金被藏在汽車前排乘客座椅的背包中。此不法活動是由海關人員隨機攔截並在管制站內搜查而發現的。當事人被起訴，然後因 2012 年《犯罪資產追回令》第 37 條第（2）款（未申報）而被罰款 5,000 迪拉姆或監禁 5 個月。

日本

404 2017 年 4 月 13 日，4 名韓國嫌犯從韓國仁川國際機場將六枚金錠攜入日本福岡機場（總計 6 公斤，價值 27,500,000 日元）。嫌犯也企圖未做申報或未經許可將現金（735,220,000 日元）帶到國外。福岡地方法院判處他們兩年零六個月徒刑，緩刑四年。

紐西蘭

中國男性試圖將約 65,000 美元現金從南太平洋轄區走私到紐西蘭

405 兩名中國男性在南太平洋島國的國際機場被攔下，他們試圖將約 65K 美元的現金走私到紐西蘭。資金包括大約 50K 美元和 15K 紐西蘭幣，並藏匿在自己的身上。此二人定期在紐西蘭和中國之間往返，其中一人經常去紐西蘭賭場，自 2015 年以來損失了超過 2 萬紐幣。懷疑這些人試圖將毒品進口犯罪所得帶回紐西

蘭和中國。

巴基斯坦

406 接獲消息指出，一個涉嫌外幣走私的組織團夥試圖在從伊斯蘭瑪巴德國際機場搭乘國際航班走私外幣。當局展開行動並收回了各種外幣，總計 3,869 萬巴基斯坦盧比（約合 276.168 美元）。AK 先生和 GD 先生這兩名被告也當場被捕。其中一名被告 AK 先生在被捕時已經攜帶外幣登機，準備起飛。

新加坡

通貨走私 – 現金運送者因走私數百萬元至新加坡而被監禁 36 個月

407 嫌犯 A 擔任鄰近轄區某換匯業者的現金運送者。在 2013 年至 2014 年期間，他並未提供完整、準確的跨境現金移動報告，將實體貨幣攜入新加坡達 100 次，金額為 1,200 萬新元。嫌犯 A 故意不實申報，聲稱他不知道實體現金的實際來源和收款人。這是非法帶入新加坡的最高現金數額。

408 2018 年 2 月，嫌犯 A 被定罪並被判處 36 個月監禁。

泰國

409 2019 年，一名寮國國民跨境攜帶未申報的泰國貨幣。此行為是出於洗錢目的而規避海關，屬於一種前置犯罪。在查緝過程中追查、扣押和凍結了大約 1 億泰銖（330 萬美元）的資產。

4.18 使用信用卡、支票、本票等

斐濟

支票漂白

410 金融情報中心接獲一家當地銀行提出可疑報告，指出一家公開上市實體 E 公司涉嫌企圖從是高級詐欺。金融情報中心確認嫌犯 F 變更 / 清洗了 E 公司向嫌犯 F 開立的 14 張支票。

411 當地銀行的驗證流程確定支票上的收款人已被變更且未兌現支票。

412 金融情報中心進一步確嫌犯 F 與 E 公司的一位資深職員有關聯。

413 相關單位向 FPF、網路犯罪偵查組發送分案報告，以進行概要分析和調查。此案現由蘇瓦地方法院審理。

潛在罪行：

- 詐欺牟利。
- 詐欺。

指標：

- 支票上的污漬或變色可能是由於擦除或改動造成。

日本

案例研究 1

414 一家也經營非法貸款的二手交易商計畫欺騙客戶的信用卡公司，並使用其客戶的信用卡來賺取非法利潤。

經銷商向信用卡公司提供了虛構銷售數據，其中詳細列出了用信用卡支付的銷售明細，但其實這些交易從未發生。然後，信用卡公司將資金存入以另一人名義開立但實際上由交易商控制的帳戶中。

案例研究 2

415 一名暴力團（日本組織犯罪集團）關係人士收到一張信用卡，這是由他的熟人以非法方式免費取得。他使用該卡提款，並用來支付生活和娛樂費用。

中國澳門

416 一家銀行的信用卡收單業務注意到，客戶 A 自 2018 年 1 月起使用 11 張在中國澳門以外地區發行的信用卡，在三家珠寶店進行了大量交易。三個月內共交易超過澳門幣 180 萬元。此現象引起了銀行的懷疑，即客戶 A 從卡中提領現金以在這些珠寶店中購買貴重物品。

417 在完成上述交易後不久，情報顯示客戶 A 涉嫌詐欺，隨後被司法警察逮捕。經過深入調查，客戶 A 疑似與珠寶店的工作人員串通進行了上述刷卡交易，並洗淨了其他司法轄區的詐欺犯罪所得。為了掩蓋資金來源，一些非法資金通過現金卡交易轉移到了中國澳門。此案也已提交公訴部門進一步調查。

4.19 拆分交易（洗錢）

澳洲

跨境大宗現金走私

418 澳洲邊防部隊（ABF）邊境金融犯罪防制組（BRFCU）發現各種洗錢方法的結構。尤其認定分散式分批現金走私是航空旅客 / 機組人員在旅行期間的重大邊境風險。

419 曾有機組人員受委託攜帶金額剛好低於 10,000 澳元申報門檻穿越內陸機場。這項活動由控制者進行協調，利用他們的網路在鋌而走險之前提供資金，並將在抵達時進行整合。

420 據觀察，這種態樣與市場的資本外逃有關，這類市場被認為比目的地司法轄區的市場更加不穩定，而且涉及到資助毒品販售的活動。

中國

案例研究 1

421 由一個境外黑幫主導的電信詐欺導致數以百萬計的損失。警方在金融情報中心的支持下進行調查，並從 20 多個城市蒐集了證據。包括外國人在內的多名嫌犯被捕，相關的銀行卡被凍結。境外黑幫通過分散交易洗錢。在短短幾天內，來自兩個銀行帳戶的資金就通過網路銀行轉移到了多個第一級帳戶、數百個第二級和第五級帳戶，以及數千個第三級和第四級帳戶。所有資金已轉移到國外並提出。

案例研究 2

422 A 和 B 是同居的伴侶。A 在知情之下協助 B 以下列方式轉移非法犯罪所得：

- 使用個人帳戶。開立兩個銀行帳戶以轉移非法收益，兩個帳戶的餘額一直很低。
- 購買不動產和車輛。
- 使用現金洗錢。
- 透過投資洗錢。

423 2018 年 9 月，法院裁定 A 洗錢罪名成立，並判處 A 徒刑 10 個月合併罰款。

馬來西亞

424 個案研究對象是一名 NPO 主席（嫌犯 B），他也是一位高階公職人員，濫用其身為 NPO 主席（即 ABC 基金會）的職務之便。嫌犯 B 的妻子在奢侈品上的信用卡支出由 ABC 基金會支付。NPO 支付的個人開銷強烈顯示當事人已觸犯刑事違反信託罪。

425 ABC 基金會在當地銀行開立一個活期帳戶，而嫌犯 B 是唯一的簽字人。

426 該帳戶從各個地點被發現進行頻繁的現金存款，且低於 CTR 要求的值，可能是為了避免客戶審查和報告要求。此外，也發現來自多個實體的大量高額支票，缺乏合理的理由就存入該帳戶。支票金額介於 16,000 至 1,000,000 令吉之間。

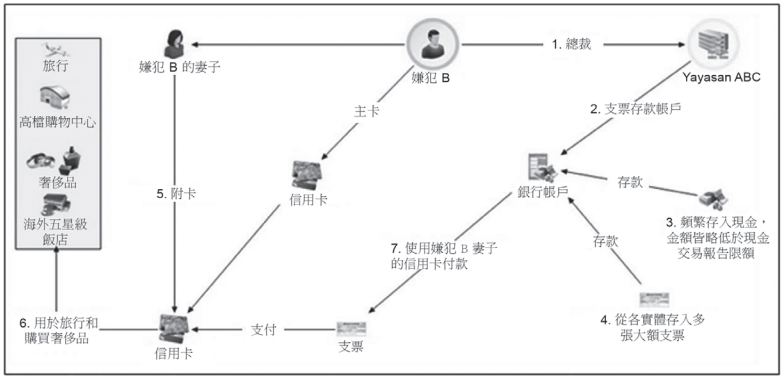
427 同時，嫌犯 B 的妻子與主卡持有人在合併限額之內擁有多張副卡。他們積極使用這些信用卡用於旅行、購買奢侈品以及在海外昂貴的酒店住宿。

428 信用卡費是使用 ABC 基金會發行的第三方支票來支付。當時曾以多筆大額支票付款，簽署人是嫌犯 B，而他也是 ABC 基金會主席。

429 嫌犯 B 被指控犯有多項背信、洗錢和濫用職權罪。此案目前正在審理當中。

使用的洗錢方法包括：

- 購買有價資產；
- 使用銀行帳戶 / 信用卡 / 支票；
- 使用現金；以及
- NPO 的涉入。



紐西蘭

毒品進口網絡使用分散式 / 藍芽和第三方銀行帳戶

430 一個毒品進口網絡採用分散式和第三方銀行帳戶來資助其進口活動。第三方在兩週內向個人的銀行帳戶存入了 2.75 萬美元的現金，單次的現金金額在 9,000 美元至 950 萬美元之間。存款是在奧克蘭地區的不同分行進行。然後，這些資金被轉移到另一個第三方銀行帳戶，在其中與價值 6,000 美元的電子信用額度合併，這些信用額度由其他多個第三方帳戶提供，然後作為一筆總金額，假借支付貸款的名義轉發到該第三方名下的另一個第三方銀行帳戶。

4.20 電匯 / 使用外國銀行帳戶

斐濟

律師事務所的企業電子郵件入侵受害者

431 金融情報中心收到了有關轄區 A 的 Z 銀行的帳戶可疑交易記錄，該帳戶被用詐領當地律師事務所的資金。

432 該律師事務所受委託協助為四人出售財產。其中一名個人 V 的電子郵件地址人被盜用，並且向當地律師事務所發送一封詐欺電子郵件，告知他們應將資金發送到 Z 銀行的帳戶。當地律師事務所在 2018 年 10 月經由兩筆交易將 845,000.00 斐濟元發送到該銀行帳戶。

433 一家當地律師事務所直到第五個人跟進付款時才意識到自己是「企業電子郵件入侵騙局」的受害者。匯出資金的斐濟金融機構試圖取回資金，但未成功。

434 據信在轄區 X 的 Z 銀行帳戶簽署人可能涉及與電腦有關的犯罪，並且涉及企業電子郵件入侵騙局。

435 金融情報中心與其海外同行聯絡以追回資金。此案仍在調查中。

潛在罪行：

- 商業電子郵件入侵 / 電子郵件帳戶入侵。

指標：

- 突然變更匯款支付的帳戶明細。
- 使用全名（而不是暱稱）和語言結構可能不符合預設發件人平常的通訊方式。

巴基斯坦

436 基於負面新聞的影響，ABC 換匯公司提交了與嫌犯 XYZ 相關的可疑交易報告；據稱該嫌犯製作和銷售的網路視頻涉及虐待兒童的行為。嫌犯 XYZ 被該國的聯邦調查局逮捕。外國司法轄區的警察逮捕了一名涉嫌虐待兒童活動有關的男子。在調查過程中，被告揭露巴基斯坦公民嫌犯 XYZ 也參與了非法活動。外國司法轄區的使館與巴基斯坦主管機關交流此資訊，並由執法機關據此逮捕嫌犯 XYZ。

437 嫌犯 XYZ 從六個轄區的不同個人收到少量匯款。嫌犯 XYZ 被懷疑藉由出售視頻牟取犯罪所得。被告也承認，他因出售一部影片而獲得少量收入。

438 FMU 與執法機關交流金融情報。該嫌犯在網路犯罪特別法庭遭判有罪，並處有期徒刑七年合併罰款盧比 120 萬。

4.21 商品交易（以物易物–例如對非法藥物的再投資）

紐西蘭

涉案的 TBML 洗錢易貨計畫藉由出口汽車零件來支付進口的安非他命

439 一家紐西蘭的汽車零件出口商因涉嫌參與貿易洗錢易貨計畫，而引起紐西蘭海關總署的注意，該計畫涉及將竊取的汽車零件運往海外，藉此支付從西非進口安非他命的款項。嫌犯與一個遍布紐西蘭、澳洲和西非的國際藥品進口集團有所關聯，並且涉嫌利用他在紐西蘭的車輛報廢業務來協助將付款（以汽車零件易物或以實體現金電匯）轉移至西非，用於交換經由郵件進口的安非他命。

4.22 使用假造的身分證件

阿富汗

案例研究 1

440 一名遭鎖定的 MSP 使用偽造的身分證明文件來獲取許可證，試圖在日後規避身分驗證等相關責任。發現 MSP 的不當行為後，有關主管機關無法找到該涉案人的真實身分。

441 結果，金融情報中心撤銷營業許可，並告知許可頒發機構應在簽發許可之前核實身分證件。

案例研究 2

442 X 工程公司向國家採購局提交的投標申請書經查發現該公司的銀行對帳單是偽造的。驗證顯示，該公司銀行對帳單的實際期末餘額為 155,486 阿富汗尼。但是，該公司偽造了銀行對帳單，顯示期末餘額為 200 萬 AFN。此據是為了滿足招標要求。結果，該公司被列入了國家採購局招標程序的黑名單。

日本

443 暴力團的一名資深男性成員非法從一間手機經銷商獲取手機等商品，並使用他人的身分證件將其出售。然後，他將非法犯罪所得轉入以他人名義開立並由他控制的銀行帳戶。此人因違反《組織犯罪懲治法》（隱匿犯罪所得）而被捕。

4.23 寶石和貴金屬

澳洲

貿易洗錢 – 貴金屬市場

444 由於其匿名性和內在價值，貴金屬市場已被認定是用來替代洗錢金融系統的理想方案。ABF 邊境金融犯罪防制組（BRFCU）最近與美國國土安全調查局（US HSI）合作，利用分析軟體「研究和貿易透明度系統

的資料分析」（DARTTS）聯合展開一項貿易透明度倡議計畫。

445 這項工作可以對進出口進行分析，以識別貿易數據差異。結果發現有澳洲實體涉嫌採用金條和假發票進行貿易洗錢（TBML）的方法，假借批發金條交易的名義，將非法資金轉移到海外。目前進行的調查工作包括貨物檢查和純度測試。

446 ABF BRFCU 針對黃金和金製產品的風險執行一項探索專案。在過程中發現，試圖隱匿價值轉移的實體日漸採用貴金屬和寶石來做交易。

447 該專案發現，貴金屬和鑽石尤其通常被用於轉移犯罪所得，以及分層和操縱金融交易的真實來源、去向和動機。在一項查明未申報或非法交易黃金的邊境攔截行動中發現，大量進出口商品都涉及這項原物料，並且由於假造票據；走私和其他非法貿易活動而造成大量收入流失的現象。

中國

案例研究 1

448 N 市海關和警方成立了一個聯合小組，調查了 14 起貴金屬走私案件。該小組已瓦解 5 支犯罪團夥。這些團夥的成員將黃金藏在人體中，反覆以此方式走私黃金。調查過程中起獲數公斤黃金，並逮捕了 22 名嫌犯。此案正在進一步調查中。

案例研究 2

449 2018 年 11 月，海關及其在 M 市的下屬機構調查了一起有關貴金屬走私的案件。某個犯罪團夥將黃金藏在人體中 40 多次，走私了數百公斤貴金屬。本案有五名嫌犯被捕，正在進一步調查中。

案例研究 3

450 2018 年 7 月，L 市海關在私家車的工具箱中發現了數十條金條。該嫌犯已被捕，此案正在進一步調查中。

紐西蘭

詐欺累犯購買黃金 / 貴金屬

451 一名詐欺累犯使用遭竊支票在紐西蘭各地購買一系列高價商品，包括價值超過 10 萬澳元的黃金和珠寶。他將遭竊支票存入零售商的銀行帳戶，並在銀行確認支票無效之前向零售商訂購了商品。他利用這種*作案手法*「購買」了價值超過 10 萬美元的黃金和珠寶，並運往他和同事的住所。當警察進行搜查令時，他們無法找到任何黃金 / 珠寶，因此懷疑犯罪者將黃金 / 珠寶轉交給了當地組織犯罪集團，以償還毒品債務。

4.24 購買貴重資產（藝術品、古董、賽馬等）

澳洲

組織犯罪實體購買藝術品

452 ABF 邊境金融犯罪防制組（BRFCU）發現許多案例

藉由購買貴重物品來協助非法轉移資金。

453 在 2018 年，ABF 查獲一名澳洲國民與境內組織犯罪實體有重要聯繫，他們會四處旅行安排購買知名藝術家的作品。

454 在介入過程中，發現利害關係人擁有一些文件，包括銷售協議和估價申請單。高價商品的買賣可能成為重大價值流向合法化的機制。這些文件也可能是為此目的而製作。

中國

案例研究 1

455 嫌犯 A 是一家物流公司的員工。他的帳戶經常從高風險地區收到現金存款。然後將資金轉入多名個人帳戶。嫌犯 A 也在多個城市購買了低價值的二手車。嫌犯 A 被懷疑從事資恐活動，其職業也無法解釋交易異常的情況。涉案資金價值已達數百萬元。此資訊已提報相關主管機關處置。

案例研究 2

456 嫌犯 B 在 2010 年和 2011 年間多次製造和出售毒品，犯罪所得的下落尚不清楚。他的情婦嫌犯 C 和嫌犯 C 父母等人的帳戶有大筆資金進出。警方因洗錢嫌疑而對嫌犯 C 及其父母提起了訴訟。法院依證據判定嫌犯 C 沒有收入來源，用於購買金融產品、房屋和汽車的現金以及現金均來自嫌犯 B 的毒品犯罪所得。2018

年 9 月，嫌犯 C 經裁定洗錢罪名成立，判處五年有期徒刑和罰款。

斐濟

457 斐濟商人 Z 先生與海外投資人 Y 先生進行了商業合作。作為商業投資的一部分，Y 先生指示 Z 先生找到合適物業來進行超市投資。Z 先生建議房地產 B，並以 550 萬斐濟元（約合 275 萬美元）的價格發送買賣協議。Y 先生向兩個單獨的銀行帳戶匯款 530 萬斐濟元（約合 270 萬美元）用於購買該物業。不久之後，Y 先生對 Z 先生產生了懷疑，並要求其妻子 X 夫人前往斐濟並調查該房產的購買情況。X 夫人發現原始買賣協議指出，物業 B 是以 330 萬斐濟元（165 萬美元）購買。當 Y 先生針對這項價差詢問 Z 先生時，他堅信該物業是以 550 萬斐濟元（約合 275 萬美元）的價格出售，但買賣協議卻以 330 萬斐濟元（約合 165 萬美元）來進行逃漏稅。

458 事實證明，Z 先生誇大了 B 物業的價格，以詐欺方式獲取 Y 先生的 120 萬斐濟元（約合 60 萬美元），再以這些資金支付兩輛汽車、兩棟房屋的部分費用，再開設定存帳戶存放餘款。Z 先生已被起訴，正在等待審判。上述財產也已遭扣押。

4.25 使用經紀人投資資本市場

澳洲

小型交易所市場的有價證券場外轉讓

459 場外轉讓（OMT）是在交易所市場之外的各方之間雙向進行的證券所有權（包括託管投資方案權益）的轉讓行為。

460 2018 年，澳洲證券和投資委員會（ASIC）開始監控與小型交易所的 OMT 相關的洗錢 / 資恐風險。

461 在這項工作中，ASIC 識別出「澳洲公司 A」與交易所中的其他證券相較之下的交易活動不成比例。

462 「公司 A」的經營遍及多個境外零售市場，該公司的控股股東向澳洲一家賭場轉帳超過 100 萬澳元。

463 ASIC 指出，小型交易所可能容易發生透過 OMT 的洗錢活動，而 OMT 可能被認為是犯罪企業轉移財富的潛在誘人工具。風險因素包括下列事實：他們可以在澳洲銀行業之外運作、主要受到非監管股份登記機構的影響，且對於場外交易或盡職調查無強制性通報義務。

日本

464 嫌犯將詐欺產生的犯罪所得存入以假名開立的證券帳戶中，並將其兌換成股票。

4.26 直接根據可疑報告或門檻交易報告發展出的案例

阿富汗

465 根據金融情報中心從申報實體收到的可疑交易報告，某些貿易公司的活動引起了懷疑。調查單位根據風險矩陣分類，對申報實體提供的這些可疑交易進行優先排序，並對貿易公司 A 和貿易公司 B 的可疑交易報告進行了財務分析。

466 金融情報中心開始對這些公司進行財務分析，並將財務情報數據分發給執法機關。

467 在 2018 年期間，FinTRACA 向國內執法機關發送了（47）起主動和被動案件以進行調查或採取進一步行動。

澳洲

468 「砸」行動主要目標是新南威爾斯州從事販毒和菸草走私的犯罪集團。該集團涉嫌進口 5,000 萬支香菸，並密謀海運進口 200 公斤搖頭丸（MDMA）。

469 澳洲執法誠信委員會和新南威爾斯聯合組織犯罪防制小組（JOCG）對移民和邊境保護（現為內政部）官員進行了平行調查，據稱該官員利用職務之便協助該集團犯行。

470 2017 年 8 月，新南威爾斯 JOCG 對新南威爾斯境內涉及該集團的實體執行 13 份搜查令。在四個物業中查獲了約 80 公斤古柯鹼和總計 740,000 澳元的現金。在調查過程中，JOCG 也查獲了 200 萬澳元。JOCG 逮

捕 9 人，其中包括在雪梨的 8 人。據稱該集團負責人在杜拜被捕，並因涉嫌毒品進口罪被引渡至新南威爾斯州。

471 在整個調查過程中，AUSTRAC 提供了現場情報支持。金融情報確認了前所未知的國內外實體之間的關鍵聯繫，並發現了各種集團成員頻繁進行的大量現金存款。

中國

案例研究 1

472 金融機構發現，在短時間內有 100 多個客戶開設了帳戶。每個帳戶通過網路銀行購買了約 5 萬美元，然後將這些資金轉移到其他地方的個人帳戶。總金額已達數百萬美元，這些帳戶的控制者涉嫌非法經營地下銀行。

473 在可疑交易報告的推動下，該機構分析了超過一百萬筆大型交易和 10 個層級的參與方。主管機關對交易方式、人員特徵和犯罪類型進行了分類，並發現了數百個涉案方。

474 2018 年 7 月，執法部門成功逮捕了 26 名涉嫌此案的嫌犯，搗毀了 6 個大型地下銀行團夥和 21 個巢穴，並起獲了電腦和凍結的銀行卡等犯罪工具。

案例研究 2

475 2018 年 10 月，金融機構向主管機關報告，A 公司的法定代表人申請轉讓 8,000 萬元。主管機關立即向警

方提供了相關資訊。經調查，主管機關發現甲公司的交易具有以下特點：

a） A 公司有投資平台和私人籌款平台。

b） A 公司的財務經理也是四家關係企業的法定代表人。他擁有 27 個聯合銀行帳戶，客戶來自整個司法轄區。

c） 使用個人帳戶進行結算以逃避監管或稅收。

d） 交易對手主要是熟悉網際網路的年輕人和中年人，他們大多是朋友或熟人。

e） 少量定期回扣交易的特點是顯而易見的。

476 後來警方立案調查，凍結了數億人民幣，並逮捕了六名嫌犯。

中華台北

477 2015 年 7 月，洗錢防制處（AMLD）從一家銀行提交的金融情報中獲悉，S 先生的帳戶最近已收到幾筆大筆現金存款。財務活動與 S 先生的財務背景和交易歷史不一致，AMLD 決定進行進一步分析。在對金融機構提供的相關文件進行分析之後，AMLD 認為這些交易可能涉及非法活動。

478 2015 年 11 月，AMLD 將此案分給法務部調查局。法務部調查局展開了調查，發現以下事實：T 先生和 W 先生是中華台北上市公司 T 公司的前任和繼任董事長。L 先生是 T 公司的董事。2015 年 5 月，T 先生等

人成立境外紙業公司 F，並由不知情的 S 先生受任命擔任主席，並使用 F 公司購入 T 公司的應收帳款和 T 公司的子公司股權。但是估價和簽訂協議的過程並未遵循正常程序，相關文件未經董事會審議或核准。T 公司在 7 月份揭露的重大資訊顯示，F 公司購買了上述 T 公司資產總額約為新台幣 2.04 億元，且將分期支付。在支付了幾期之後，F 公司由於某種原因無法繼續付款。T 先生等人沒有積極要求 F 公司履行合約。因此，T 公司蒙受約新台幣 3,330 萬元的虧損。

479 在法務部調查局完成調查後，涉及違反《證券交易法》的案件於 2018 年 4 月移交給檢察署進行起訴。

斐濟

480 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構總共發佈了 321 份 CDR，CDR 是對可疑交易報告的分析而編製。斐濟金融情報中心 CDR 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》。2018 年，一共向 FRCS 發佈 207 份這類報告，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。

481 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，該資料庫包括現金交易報告（CTR）、電子資金轉帳報告（EFTR）和邊境貨幣報告（BCR）。

482 關鍵夥伴機構也可經由直接資料存取（DDA）安排，存取斐濟金融情報中心資料庫。

馬來西亞

資助恐怖主義

483 在區域打擊資恐計畫中，金融情報中心參加區域分析員交流計畫，試圖分析菲律賓南部的伊斯蘭國掛勾組織「馬巫德」武裝集團的可疑交易。該計畫於 2018 年 5 月至 8 月之間舉行，澳洲交易報告和分析中心（AUSTRAC）、金融交易報告與分析中心（PPATK）、BNM 和防制洗錢委員會（AMLC）的分析師參加了該計畫。交流計畫根據相關司法轄區的涉案交易，提出一份有關馬巫德集團的詳盡金融情資報告。該報告已分發給所有司法轄區的相應執法機關，以採取進一步的執法行動。

詐欺 – 商業電子郵件入侵

484 金融情報中心收到轄區執法機關的警報，在 2018 年 1 月到 3 月間將 150 萬美元（580 萬令吉）通過五筆交易從轄區 Y 的受害人 A 詐欺轉移到涉案人 X 在馬來西亞的銀行帳戶。據稱受害者 A 收到了貿易夥伴的一封信函，涉案人 Y 指示其工作人員將錢轉匯給馬來西亞的涉案人 X。從 2018 年 1 月至 3 月，冒名頂替者使用偽造的電子郵件地址誤導受害者 A 的員工，使其發起五筆交易將總計 150 萬美元匯入嫌犯 X 在馬來西

亞 C 銀行的帳戶中。

485 由於司法轄區 Y 的執法機關發出警報，金融情報中心立即聯繫 C 銀行以阻止該帳戶進行任何提款。但是當時，涉案人 X 經通過現金支票部分提領了資金，並轉移給三個當地交易對手，剩下的餘額約為 315 萬令吉。

486 對該案的初步分析顯示以下發現：

- 嫌犯 X 的名稱幾乎與受害者 A 的貿易夥伴的名稱相似；
- 涉案人 X 是在 2017 年末和 2018 年才與當地交易對手建立往來關係。在企業登記後，實體立即開立銀行帳戶以協助詐欺資金的接收和轉移；
- 從受害者 A 收到的大部分資金都在當日或次工作日立即透過現金支票、ATM 提款和線上資金轉入交易對手的方式提出，這類手法在詐欺案件中很常見；以及
- 從嫌犯 X 和交易對手的帳戶中可以看出，所有資金最終都是以現金提領，這使得追蹤最終受益人變得困難。

487 該案已轉交給相關的執法部門，嫌犯 X 的帳戶也因此被凍結，而相關涉案人正持續接受調查。

紐西蘭

案例研究 1

488 NZFIU 接獲有關 NZ OCG 成員在 NZ 賭場存入大量現

金的可疑活動報告。NZFIU 的一名分析師進行了財務分析，並確定了資產和資金，遠遠超出了他的預期。NZFIU 向當地的 NZP 刑事調查處發布了一份報告，對他的活動進行了調查。該人隨後涉嫌參與安非他命的生產和供應而被捕，並且根據紐西蘭的《刑事訴訟法》，約有 77 萬美元的資產受到扣押。

案例研究 2

489 NZFIU 收到了一個可疑活動報告，指出一名身分不名人士用大量現金支付了極高昂的家用電費。NZFIU 向電力公司進行了調查，以確認資金存入帳戶的持有者。NZFIU 向該人居住的 NZP 轄區發布一份報告，其中包括一項評估指出該人可能從事室內大麻種植業務。NZP 區開始對該人進行調查，判定他確實於家中經營室內大麻種植活動，此人隨後被捕並遭控犯有大麻相關罪行。

案例研究 3

490 NZFIU 收到了有關某電子商品進出口商的可疑活動報告通知，該公司的紐西蘭帳戶中發生可疑的金融活動，包括無法解釋的現金存款、信用卡超額付款以及與高風險轄區之間的交易。NZFIU 向合作夥伴機構進行了調查，並評估了該公司可能參與了貿易洗錢形式。NZFIU 發布了一份詳細報告此案的情報報告，並將其發布給專門的調查部門，該部門對該公司的活動

進行了正式的刑事調查。

新加坡

根據可疑交易報告，依背信罪追回 290 萬新元

491 STRO 收到了有關嫌犯 A 的可疑交易報告資訊，此人是在新加坡立案 B 公司的會計師。STRO 的分析顯示，境外公司存有多筆支票存款進入嫌犯 A 在新加坡的個人帳戶。這是不尋常的現象，因為境外公司是由公司 B 看守，而嫌犯 A 在這些公司中並無所有者權益。據指出，這些資金隨後通過現金和支票提領，沒有轉給其他公司實體。

492 STRO 將可疑交易報告的資訊及其分析結果發送給新加坡的相關執法機關。調查顯示，嫌犯 A 假造付款憑單並利用授權簽字人簽署的空白支票，從 B 公司及其境外公司挪用了相當於 4,620 萬新元的款項。犯罪所得主要用於資助嫌犯 A 的賭博活動。有關執法機關向嫌犯 A 追討 290 萬新元。

493 嫌犯 A 因背信和洗錢等罪名而判處 18 年有期徒刑。

5. 防制洗錢 / 打擊資恐措施效果

494 報告的本節簡要概述了立法、法規或執法對策的最新成果。

5.1 立法或法規發展對偵測及 / 或預防特定方法的影響

阿富汗

495 FinTRACA 已經建立了一個觀察列表，可供申報實體取用，以作為與客戶往來的參考。這份指名名單非常有助於警示申報實體注意不斷演變的威脅。

澳洲

AUSTRAC 數位通貨交易法規

496 在澳洲營運的數位匯換（DCE）供應商的新法律，已由澳洲金融情報中心 AUSTRAC 和防制洗錢與打擊資恐主管機關於 2018 年實施。

497 新的防制洗錢 / 打擊資恐法律涵蓋了加密貨幣服務供應商的監管（包括比特幣）、該機構的合規性和情報能力，以幫助 DCE 實施系統和控管措施，徹底減少犯罪份子使用 DCE 進行洗錢、資恐和網路犯罪的風險。

498 現在，在澳洲設點營運的 DCE 必須在 AUSTRAC 註冊並履行政府規定的防制洗錢 / 打擊資恐遵守和報告義務，以保護其業務免受洗錢和資恐的侵害，同時有助於增強公眾和消費者對該產業的信心。

499 這些變更也帶來更多契機，有利於產業和政府合作夥伴共享有關使用數位通貨（例如比特幣和其他加密貨幣）的金融情報和資訊。如此可為澳洲打擊重大犯罪和資恐活動帶來直接助益。

中國

500 根據*《國家外彙管理局關于規範銀行卡境外大額提取現金交易的通知》*規定（截至 2018 年），個人境外銀行卡現金提領每年不得超過等值 10 萬元人民幣。這項政策實施後，有效地遏止提領大量現金匯入境外的舉動。單人境外現金提領的最高限額已從一百萬減少到 2 或 3 萬元人民幣。與 2017 年相比，2018 年國內銀行卡的海外現金提領累計額減少了 44%。

中華台北

501 根據 2018 年 3 月 5 日指定的融資租賃事業範圍，金融監督管理委員會（FSC）於 2018 年 6 月 20 日發布了《辦理融資性租賃業務事業防制洗錢辦法》。11 月 9 日，FSC 頒布適用於融資租賃事業、銀行業、證券期貨業、保險業的防制洗錢和資恐內部稽核及內部控管法規。FSC 在同一天也發布了《會計師防制洗錢及打擊資恐辦法》的修正案。

502 為了加強中華台北的防制洗錢 / 打擊資恐機制，FSC 在 2018 年 11 月 14 日頒布《金融機構防制洗錢辦法》和《金融機構對經指定制裁對象之財物或財產上利益

及所在地通報辦法》的修正案。

503 FSC 將繼續監督金融產業遵守防制洗錢相關法規，並實施防制洗錢 / 打擊資恐措施，亦將持續審查相關法規以符合國際規範。

504 2018 年 11 月 7 日，中華台北通過了《洗錢防制法》（MLCA）和《打擊資恐法》（CTF 法）的修正案。MLCA 修正案主要範圍涵蓋在防制洗錢 / 打擊資恐制度下處理虛擬通貨平台或交易的企業。此外，根據新發布的修正案，金融機構和指定之非金融事業或人員（DNFBPs）應根據其洗錢 / 資恐風險和業務規模制訂內部防制洗錢 / 打擊資恐控管和稽核系統。《CTF 法案》的修正案規定，目標性金融制裁範圍適用於直接或間接全資或共同擁有或控制的資產，或適用於代表指定人和實體行事的個人和實體之資金或其他資產。

斐濟

505 斐濟目前正在審查其《公共秩序法》，進一步加強有關資恐（R.6）和資助武器擴散（R.7）的目標性金融制裁相關法律條款。這些規定的審查於 2018 年 2 月開始，目前處於諮商階段，並向 APG 和 CTED 徵求了有關條款草案的意見。

506 斐濟儲備銀行（RBF）加強對匯款服務提供者和換匯業者進行防制洗錢 / 打擊資恐的現場檢查，並修訂了相關部門的防制洗錢監管政策。

507 斐濟金融情報中心加強對指定之非金融事業或人員進行防制洗錢 / 打擊資恐的現場檢查。2018 年，金融情報中心對 5 家房地產企業和 8 家律師事務所進行了防制洗錢 / 打擊資恐的現場檢查。

508 目前正在對《公司法案條例》進行審查，旨在解決法律實體的實質受益人在透明度方面的重大法律空白地帶。

印尼

509 BAPPEBTI（期貨交易監督委員會）發布了關於加密資產和數位黃金的 4 項法規。印尼中央銀行（BI）禁止在支付活動和支付系統中使用任何虛擬通貨。但是在投資及 / 或交易用途中，仍然允許使用虛擬通貨 / 加密資產。這些法規要求期貨交易市場中的加密資產和數位黃金交易者必須遵守防制洗錢 - 打擊資恐法規。

馬來西亞

降低現金交易報告（以下各段簡稱「CTR」）門檻

510 從 2019 年 1 月 1 日起，馬來西亞國家銀行（BNM）作為 2001 年版《防制洗錢、打擊資恐及非法活動犯罪所得法案》（AMLA）的權責機關，將現金交易報告門檻從 50,000 令吉（約合 12,000 美元）降低至 25,000 馬幣（約合 6,000 美元）。

511 此決定源自 2017 年國家風險評估（NRA）的調查結果，其中指出貪污構成了該國第二高的淨犯罪風險。根據案例研究和可疑交易報告分析，存放在金融機構

和非銀行金融機構中的貪污犯罪所得金額有所不同，但通常低於現行的現金門檻限額。除非提出可疑交易報告，否則執法機關逐漸難以發現貪污犯罪所得的洗錢行為。此外，先前的 50,000 令吉門檻相較於其他司法轄區而言過高，並且無法準確反映馬來西亞經濟中現金使用的規模和普遍性。

512 降低門檻將使犯罪分子難以繼續透過申報機構洗錢。犯罪分子廣泛使用現金來儲存、轉移和支付違法犯罪所得，突顯 CTR 是預防洗錢和資恐風險的一項重要措施。降低門檻有助於加強監控，並更清楚發現可疑交易模式，以利查獲相關不法行為。

紐西蘭

513 規定交易報告（PTR）制度提高了 NZFIU 向國內外合作夥伴提供支援的品質。

514 根據最新的防制洗錢 / 打擊資恐法令，現在申報實體必須向 NZFIU 申報 10,000 美元以上的大額現金交易（LCT），以及 1,000 美元以上的國際資金轉帳（IFT）。以下範例說明 PTR 報告更有助於 NZFIU 建構情報視圖，全面掌握整個金融系統，支援重大組織犯罪的調查工作：

-- NZP 的一組專家調查小組向 NZFIU 提交申請，要求提供有關某些涉嫌安排進口安非他命至當地的個人相關資訊。NZP 先前並未掌握這些人的資

訊，而他們過往未曾涉入任何可疑交易。在後續數週內，NZFIU 接獲有關嫌犯的 PTR，其中詳細記錄將現金存入第三方銀行帳戶的情況。NZFIU 發布一份報告，旨在協助調查團隊開發線索，而相關調查目前尚在進行當中。由於申報實體在這些交易中並無嫌疑之舉，因此在舊制度下不會對這些交易發出通報。

-- 位於轄區 A 的合作夥伴金融情報中心向 NZFIU 提出申請，要求瞭解存入轄區 A 的紐西蘭匯款業者（即匯款人）銀行帳戶內的疑似犯罪所得。夥伴金融情報中心詢問資金進入轄區 A 匯款人銀行帳戶後的流向，以及交易的受益人身分。僅根據 PTR 資訊，NZFIU 就可以追蹤疑似犯罪所得並得知其已流入轄區 B 中的某個帳戶，同時確認交易的受益人身分。NZFIU 向合作夥伴金融情報中心發布一份報告以協助調查工作。

新加坡

加強對實質受益權資訊的存取管道

515 根據新的實質受益權制度，境外公司也必須遵守強制規定向註冊官提供控制人登記冊，來擷取其實益所有者的資訊。2017 年《公司法》第 386A 條修訂案規定，必須向負責管理或執行任何成文法（包括 CAD、CPIB 和 IRAS）的書記官和公共機構提供控制者登

記冊。實際上，這些變更改善了國內主管機關所持有基本資訊的普及性，可以從金融機構、公司服務業者（CSP）及其他指定之非金融事業或人員（例如律師和會計師）處取得這些資訊。

516 隨著上述發展，執法機關可以從註冊登記代理機構得知實質受益權資訊。因此，CPIB 與 ACRA 合作對 CSP 進行了聯合檢查，以全面的方式打擊洗錢犯罪。

6. 縮寫對照表

ABF– 澳洲邊防部隊

AFP– 澳洲聯邦警察

AML– 防制洗錢

AMLA– 防制洗錢法案

AMLC– 防制洗錢理事會

AMLD– 洗錢防制處

ANF– 反毒部隊（巴基斯坦）

APG– 亞太防制洗錢組織

ATM– 自動提款機

AUSTRAC– 澳洲交易報告暨分析中心

BCR– 邊境貨幣報告

C&ED– 香港海關（中國香港）

CDD– 客戶盡職審查

CDR– 現金散佈方式報告

CFT– 打擊資恐

CIB– 刑事警察局

CIPB– 貪污調查局

CTR– 現金 / 貨幣交易報告

DGCE– 海關總局（印尼）

DNFBP– 指定之非金融事業或人員

EAG– 歐亞小組

ECOFEL– 艾格蒙金融情報卓越和領導中心

EFT– 電子資金轉帳

ESW– 艾格蒙安全網路

FATF– 防制洗錢金融行動工作組織

FINTRAC– 金融交易報告分析中心（加拿大）

FIU- 金融情報中心

FMU– 金融監控中心（巴基斯坦）

FRCS– 斐濟稅務和海關管理局

FSRB– 區域性防制洗錢組織態樣專案

GIF– 金融情報辦公室（中國澳門）

HT– 人口販運

IDR– 印尼盾

ICRG– 國際合作審查小組

IFTI– 國際基金交易指示

INTERPOL– 國際刑事警察組織

JAFIC– 日本金融情報中心

KYC– 認識客戶政策

LEA– 執法機關

MIT– 東印尼聖戰士

MJIB– 法務部調查局

MG– 馬巫德集團（菲律賓）

ML– 洗錢

MR– 匯款業者

MSP– 貨幣服務提供者

NAB– 國家權責局（巴基斯坦）

NCC– 全國防制洗錢協調委員會（馬來西亞）

NGO– 非政府組織

NNB– 全國反毒委員會（印尼）

NPO– 非營利組織

NRA– 國家風險評估

NZP– 紐西蘭警察

NZFIU– 紐西蘭金融情報中心

OCG– 組織犯罪集團

PPATK– 金融交易報告與分析中心（印尼）

PS– 人員偷渡

PEP– 重要政治性職務人士

PKR– 巴基斯坦盧比

PML– 專業洗錢者

POI– 利害關係人

PTR– 規定交易報告

RI– 申報機構

RMP– 馬來西亞皇家警察

SAR– 可疑活動報告

SEACTFWG– 東南亞打擊資恐工作小組

SEC– 證券交易委員會（菲律賓）

STR– 可疑交易報告

SVF– 儲值工具

TF– 資恐

TRACFIN– 打擊非法金融管道情報處理和行動中心（法國金融情報中心）

TTP– 巴基斯坦塔利班運動

VAT– 增值稅

VC– 虛擬通貨

APG 2019 年度態樣報告

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

行政院洗錢防制辦公室 2021 年 12 月印製