APG 年度態樣報告

APG Yearly Typologies Report

Asia/Pacific Group
on Money Laundering

亞太防制洗錢組織

2021年

洗錢與資恐的方法與趨勢

Methods and Trends of Money Laundering and Terrorism Financing

亞太防制洗錢組織 2021年7月
Asia/Pacific Group on Money Laundering
July 2021

目 錄

引言

1. 亞太防制洗錢組織（APG）是防制洗錢金融行動工作組織（FATF）的亞太區域性組織。其任務之一是區域性的洗錢（ML）和資恐（TF）之態樣報告，以協助政府和其他利害關係人更瞭解現有及新興之 ML 及 TF 威脅之性質，並採取有效之策略以應對這些威脅。當一連串的 ML 或 TF 以類似的方式或使用相同方法進行時，通常被歸類為一個態樣。態樣研究有助於 APG 成員實施有效的策略，以調查和起訴 ML 及 TF，進而設計和實施有效的預防措施。
2. APG 成員國和其觀察員每年都會提供案例研究、趨勢觀察、研究、監管與執法行動之資訊以及國際合作的實例。所收集之資料用以作為進階研究特定及高優先主題之依據。
3. 本報告中介紹的案例研究只是亞太地區和其他地區的執法和情報機關在偵查和打擊 ML 及 TF 方面工作的一小部分成果。許多案件由於其敏感性質或正在進行偵查／司法程序而無法公開分享。
4. 本報告包括一個介紹 FATF 2020 年 10 月 23 日透過第 1 項建議及其注釋（INR.1）修正有關，對於資助武器擴散（PF）相關風險的了解的簡短章節。
5. APG 執行委員會負責監督態樣研究計畫，由薩摩亞和紐西蘭擔任共同主席（2020-2021）。

1. 資助武器擴散之風險

1.1 風險評估與資武擴

FATF 架構使用風險基礎法來對 ML 及 TF 進行評估，但這種要求直到近期才擴展到資武擴（PF）。2020 年 10 月 23 日，FATF 透過對第 1 項及第 2 項建議（R.1 及 R.2）的修正案，要求各司法管轄區、金融機構（FI）、指定之非金融事業或人員（DNFBPs）以及虛擬資產服務提供商（VASPs）識別和評估可能違反、不執行或規避與資武擴有關目標性金融制裁（TFS）之風險（如 FATF 第 7 項建議（R.7）所載），並採取行動抵減這些風險。在此情況下，與 PF 與 TFS 有關的態樣引起新的關注。

第 7 項建議旨在打擊資助大規模毀滅性武器（WMD）擴散的義務，側重于司法管轄區對於聯合國安理會決議（UNSCR）所建立的兩個特定司法管轄區，即朝鮮民主主義人民共和國（下稱北韓）[1] 和伊朗[2]）制度之執行。大體上，第 7 項建議要求各司法管轄區毫不遲延地凍結（a）聯合國安全理事會（UNSC）指定的任何個人或實體，（b）代表其或按其指示行事的個人和實體和／或（c）由其擁有或控制的個人或實體的資金或其他資產，並確保沒有資金或其他資產會直接或間接提供，或使其受益。

---

1 詳聯合國安全理事會第 1718 號決議（2006）

1 詳聯合國安全理事會第 2231 號決議（2015）

第 1 項建議中所列出之 PF 風險包括：

- 違反或不執行目標性金融制裁的潛在風險：當被指定的法人和個人獲得金融服務和／或資金或其他資產時，此類風險可能會實現，例如，由於在國家層級上對於指定制裁的溝通延遲，對金融機構和 DNFBPs 缺乏明確的義務，金融機構和 DNFBPs 未能採取適當的政策和程序來解決其資武擴風險（例如，薄弱的建立客戶關係程序和持續監控程序，缺乏員工培訓，無效的風險管理程序，缺乏適當的制裁檢核系統或不規則或不靈活的檢核程式，以及普遍缺乏合規文化）;
- 規避目標性金融制裁的風險：風險可能會因被指定的個人和實體協同齊心規避目標性金融制裁（例如，透過使用空殼或前台公司、合資企業、人頭帳戶、車手和其他詐欺中介）而發生。

本章簡要介紹新的義務，並概述亞太地區正在進行的或與其有關的態樣與風險評估工作。特別是，APG 與皇家聯合研究院（RUSI）合作，展示一些關於 PF 態樣和資武擴目標性金融制裁實踐的研究。

1.2 標準之修訂

第 1 項建議的新內容要求政府識別、評估並瞭解其司法管轄區的 PF 風險，以及第 7 項建議中關於目標性金融制裁架構的現行規範。修正案還要求司法管轄區內的金融機構、DNFBPs 與 VASPs 在與客戶打交道時，有義務識別和評估其可能違反、不執行或規避目標性金融制裁的風險，並根據所識別的風險程度採取適當的抵減措施[3]。重要的是，在第 1 項建議的背景下，" PF 風險 " 係嚴格地限指可能違反、不執行或規避建議第 7 項所提及之目標性金融制裁義務。

FATF 於 2021 年 6 月 29 日發布資助武器擴散風險評估及抵減指引[4]，以協助公部門和私部門執行第 1 項建議及注釋中定義的識別、評估和抵減 PF 的新要求[5]。值得注意的是，該 2021 年指引提供與識別 PF 有關的最新關鍵指標清單[6]。

對 FATF 建議的修改將在第四輪 APG 相互評鑑中生效[7]。

1.3 聯合國專家小組報告

如上所述，FATF 在第 7 項建議下的職責與聯合國安理會決議有關，這些決議側重於兩個特定的司法管轄區。北韓（聯合國安理會第 1718 號決議）和伊朗（聯合國安理會第 2231 號決議）。在批准《聯合全面行動計畫》時，安理會第 2231 號決議終止以前有關伊朗和大規模毀滅性武器擴散的決議條文，包括安理會第 1737（2006）號、第 1747（2007）號、第 1803（2008）號和第 1929（2010）號決議，但保留根據這些決議指定的一些個人和實體的目標性金融制裁，並建立新的具體限制，包括一些其他措施。然而，與北韓有關的義務仍然很廣泛。

聯合國安理會 1718 制裁委員會之任務為監督防止北韓獲得用於大規模毀滅性武器計畫之材料及物品之制裁措施。委員會下設一專家小組，負責自會員國及其他來源收集關於 1718 制裁措施執行情況的資訊以及不遵守決議之案例。

---

6 亦可參閱 FATF 2008 年資武擴態樣報告（提供於 https://www.fatf- gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html），以及 FATF 2018 年打擊資武擴指引 - 執行聯合國安全理事會決議的金融條款以打擊大規模毀滅性武器擴散（提供於 https://www.fatf-gafi.org/publications/financingofproliferation/documents/guidance-counter- proliferation-financing.html）。

7 作為分階段方法的一部分，FATF 將在下一輪（第五輪）相互評鑑中開始評估各司法管轄區對這些要求的執行情況，以便讓各國政府有時間採取必要的國內措施。

專家小組擬撰一份通常作為期中和期末發布之報告[8]，詳細說明北韓尋求獲得所需資源以推進其核武器、彈道飛彈和其他大規模毀滅性武器計畫的動向和方法。這些報告觀察北韓為獲得材料（包括軍民兩用物品）和技術（包括外國專家的智慧財產權）以支持和擴大大規模毀滅性武器擴散所採取的活動。重點為這些報告中標題為＂金融＂的一個章節，專門介紹北韓得以進入國際金融系統的方式。透過規避制裁活動籌集的資金和透過這些網路進行的洗錢活動支持北韓的核武器、彈道飛彈和其他大規模毀滅性武器計畫。

專家小組報告收集、審查並分析公開來源之資料，及聯合國會員國、相關聯合國機關和其他有關各方主動和被動提交的關於措施執行情況的資訊，特別是關於不遵守決議之情況，以確定北韓獲取這些材料的方法。如果專家小組的調查顯示某會員國的某個實體或個人涉嫌參與其中，它將向該會員國提出要求提供進一步的資訊或採取行動。專家小組還積極主動地從會員國獲得情報和資料，以協助其調查[9]。

近年來，這些報告已確定北韓促進其 PF 而使用的新的和不斷變化的趨勢和態樣，也包括一些值得 APG 成員注意的重要訊息。北韓持續利用複雜的公司工具，包括合資企業、離岸帳戶、空殼公司和海外銀行代表，以掩蓋其持續利用進入國際金融系統，以籌集資金並推進其 PF 活動。最後，北韓越來越常對有從事虛擬資產（VAs）和虛擬資產服務提供商（VASPs）業務的金融機構和交易所進行網路活動，包括盜竊和將虛擬貨幣洗成法幣已逐漸成為一個重要的 PF 態樣。

---

8 https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports
9 https://www.un.org/securitycouncil/sanctions/1718/panel_experts/work_mandate
10 https://rusi.org/publication/occasional-papers/closing-crypto-gap-guidance-countering-north-korean- cryptocurrency
11 https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive- wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d- 1ac0fd7f097e_story.html?utm_term=.cd703dfb03a2

皇家聯合研究院：虛擬貨幣及 PF

使用虛擬貨幣來規避制裁和提高收入是現代 PF 的一個特點。2019 年，皇家聯合研究院發表一份關於北韓在東南亞的虛擬貨幣活動的里程碑式的研究。

- 獲取：網路犯罪無疑是受制裁者取得虛擬貨幣的最普遍方法，特別是透過駭客攻擊東亞的虛擬貨幣交易所。北韓還參與勒索軟體，如 WannaCry [11] 的使用，並在過去幾年裡對網路釣魚和線上詐欺特別感興趣。
- 金流態樣：北韓等大規模虛擬貨幣洗錢者與傳統的洗錢一樣使用多層化技術 [13]。攻擊者透過使用一次性虛擬貨幣錢包即時創建數以千計的交易 [14]，然後他們能夠模糊自身的蹤跡並破壞金流的路徑。
- 交易所：越來越明顯的是，北韓嚴重依賴不受監管的 [15] 或不合規的 [16] 交易所以及點對點場外交易來清洗資金。許多司法管轄區缺乏監管，使得這種行為實行起來相對容易。
- 清算速度：北韓一般將其虛擬貨幣兌現為法定貨幣或另一種虛擬貨幣的速度相對較快，[17] 最近清算速度也在增加。他們似乎對儲存虛擬貨幣以供未來使用興趣不大。
- 規模：根據最新的分析 [18]，北韓駭客估計已經從虛擬貨幣交易所竊取至少 17.5 億美元。

---

12 https://www.justice.gov/usao-cdca/pr/3-north-korean-military-hackers-indicted-wide-ranging-scheme- commit-cyberattacks-and

13 https://www.swift.com/sites/default/files/files/swift_bae_report_Follow-The%20Money.pdf

14 https://www.justice.gov/opa/press-release/file/1253491/download

15 https://www.elliptic.co/blog/following-money-from-bithumb-hack

16 https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency- exchange-hack

17 https://go.chainalysis.com/2021-Crypto-Crime-Report.html

18 https://www.forbes.com/sites/thomasbrewster/2021/02/09/north-korean-hackers-accused-of-biggest- cryptocurrency-theft-of-2020-their-heists-are-now-worth-175-billion/?sh=691163865b0b

報告還指出，航運業持續被濫用，其方式包含船對船過駁、改變船舶標識、操縱旗幟和船舶標識，以及以技術方法欺騙自動識別系統追蹤。在澄清聯合國安理會決議所涵蓋的 " 資助 " 範圍時，聯合國安理會第 2270 號決議申明，" 經濟資源 [19] " 包括各種資產，它們可能被用來獲取資金、貨物或服務，並明確指出這包括海上船隻。

皇家聯合研究院：航運與 PF

皇家聯合研究院的專案 " Sandstone " 使用開源的資料探勘和資料融合等技術，來發覺北韓規避制裁，特別是在海洋領域的活動。該專案旨在為參與執法及研擬政策者提供開源情報和可操作的證據。Sandstone 調查包括研究北韓的石油採購網，資金透過國際金融體系流動的態樣，以及丹東市在與北韓 PF 有關的貿易公司中的重要性 [20]。

在亞太區域，中國大陸和新加坡的相互評鑑報告能夠借鑒專家小組報告所做的工作，以瞭解直接成果第 11 項的有效性的程度。例如，相互評鑑報告中提到專家小組的報告，其中包含被評估司法管轄區內指定實體持有的帳戶、資金或資產的案例，以及指定實體在該司法管轄區經營的（前台）公司 [21]。此外，專家小組要求提供與指定實體聯繫的相關訊息，以致主管機關在其國內採取法律遵循行動 [22]。

---

19 此一術語是專門為釐清安理會第 1718 號決議第 8（d）段的目的所定義的。聯合國安理會第 1718 號決議第 8（d）段，廣義來說該段規定要求成員國有義務凍結與朝鮮人民軍有關的資金、其他金融資產與經濟資源。

20 https://rusi.org/project/project-sandstone

21 中國相互評鑑第 274 段：http://apgml.org/includes/handlers/get-document.ashx?d=5b27e83d-c28b-4e87- 9549-20839d4bd92c

22 新加坡相互評鑑第 288 段：http://apgml.org/includes/handlers/get-document.ashx?d=1280e446-2110- 430c-b709-3a777b85a020

1.4 亞太地區之資武擴風險評估[23]

印尼

2020 年，印尼啟動資武擴風險之評估，並隨後更新現有的 ML / TF 風險評估。印尼的資武擴風險評估方法類似於印尼的 ML / TF 風險評估，經由定量與定性資訊，根據弱點程度、威脅程度和影響程度確定風險。這種方法也類似于 FATF 進行國家風險評估（NRAs）的方法。制定資武擴風險評估涉及以下利害關係人：印尼國家警察（印尼國家警察國家情報和安全局第 88 反恐怖特別支隊）、國家情報局（BIN）、外交部、海關總署（財政部）以及作為報告實體的金融服務提供商及 DNFBPs 的監理機關（印尼銀行／中央銀行、金融服務管理局、印尼金融情報中心等），以及金融機構與 DNFBP 的代表。

印尼確定 3 個級距的 PF 風險，包括 9 個象限，即低度（3-5 分）、中度（5-7 分）與高度（7-9 分）。根據第 7 項建議的要求，印尼的資武擴風險評估的範圍僅限於與資武擴相關的目標性金融制裁的有效性。資武擴風險評估不包括聯合國安理會第 1540 號決議及其後續決議中提到的廣泛的資武擴風險範圍。然而，印尼依據海關和消費稅資訊考量了軍民兩用貨物貿易的數量和重要性，特別是針對伊朗和北韓兩個指定司法管轄區。在進行資武擴風險評估時，印尼還利用跨境現金運送者的資訊，特別是與伊朗與北韓有關的個人或實體。

總體而言，考慮到與伊朗與北韓目前的外交和經濟關係，以及該司法管轄區在地理上靠近北韓，印尼已確定其資武擴之中度風險。印尼還辨識出一個潛在的威脅，即不再在印尼服務的前外國外交官之帳戶隨

---

23 本節包括 APG 成員提供的關於他們執行第 1 項建議與第 2 項建議中提及修正案之工作。APG 並無在此審查或評估其成員就 PF 風險進行之工作。

後被其他人濫用。然而，印尼已經進行一些 PF 風險抵減措施，如發布聯合條例（2017 年 5 月 31 日頒佈），根據聯合國的名單（針對伊朗和北韓，涉及 PF）指定個人或實體，並毫不遲延地凍結所列個人和實體的資金。聯合條例之實施範圍擴大要求金融機構識別和凍結個人或實體的資產，包括那些與聯合國指定的個人和實體有關聯的資產。此外，為減少資武擴風險，印尼的一些金融機構限制與伊朗和北韓有關之資金交易（含電匯），部分金融機構將不會與伊朗和北韓建立任何業務關係。印尼還在 2017 年成立一個大規模毀滅性武器專案組，由印尼金融情報中心、國家情報局、印尼國家警察、外交部及核能監理機關（NERA）組成。大規模毀滅性武器專案組的主要任務是透過整合自發的資訊交流，識別和監測個人或實體的活動和資金流動，包括那些與聯合國指定人員和實體有關聯的個人或法人實體。

馬來西亞

馬來西亞國家防制洗錢協調委員會（NCC）最近批准並認可 2019 年初與馬來西亞出口管制當局合作開展的防制資助武器擴散風險評估（PFRA）的工作。PFRA 企望實現以下目標：

- 提供基線評估，以加強對馬來西亞所面臨之 PF 風險的瞭解。
- 識別和解決金融和 DNFBP 部門的關鍵弱點，這些弱點可能被利用於資助大規模毀滅性武器擴散或逃避聯合國安理會制裁有關的金融活動；以及
- 支持制定適當的戰略及建議措施，抵減已查明的風險和弱點，以加強馬來西亞的整體防制資助武器擴散（CPF）之架構。

該評估的重要性不斷增加，並與最近通過修訂的 FATF 建議第 1 項和第 2 項相一致。完成 PFRA 將是一個關鍵步驟，以確保有效實施來自

以下四個不同組別的建議：

- 立法、政策和協調架構。
- 監管與監督舉措。
- 實施與指引；以及
- 執法行為。

在得到國家協調委員會的認可後，簡化版報告預計將在 2021 年第三或第四季度向公眾公布。

菲律賓

2021 年 3 月 4 日，菲律賓中央銀行（BSP）完成對銀行和其他 BSP 監管的金融機構（BSFI）的部門風險評估，該評估強調銀行和其他 BSFI 的 ML / TF / PF 威脅和弱點及犯罪活動的後果，以及與其他優先領域（如基於貿易的 ML / TF / PF 及目標性金融制度的實施）相關的整體 ML / TF / PF 風險。

皇家聯合研究院：私部門與 PF 的實施

2020 年，皇家聯合研究院與國際公認反洗錢師協會（ACAMS）合作，進行一項關於 PF 合規性的全球調查，重要結論包括：

- 國際銀行（在世界多個地區有業務）似乎最有可能擁有包含 PF 的合規職能（76%），相比之下，國家銀行（63%）和非銀行機構（46%）較少。這一發現與皇家聯合研究院自身在世界各地提供培訓和技術援助的經驗以及一些相互評鑑報告相吻合，這些報告證實銀行普遍更瞭解其 PF 義務，而 DNFBPs 則沒有將 PF 視為一種獨立的金融犯罪風險。

- 在國際銀行工作的受訪者也比起其他機關更有可能考慮紅旗、態樣和其他 PF 資源；一些資源，如聯合國專家小組關於北韓的報告，很少被參考。調查還發現，與國家銀行（3%）相比，國際銀行中查閱聯合國專家小組報告的受訪者人數更多（25%）。此外，國際銀行的受訪者大多參考美國政府發布的諮詢報告（39%），而其他類型的機構則相對較少（16-17%）。
- 在 PF 意識方面也存在重要地區差異，在亞洲有最高比例的受訪者表示，他們透過新聞報導瞭解最新的北韓制裁規避活動。
- 超過五分之三的受訪者同意，將軍民兩用物品清單納入交易監測計畫是具有挑戰性的，大多數受訪者也同意行業應該優先且嚴格的確認最終使用者，而不是在交易中識別具體的物品。
- 關於針對北韓的制裁問題，受訪者最關心的是有效履行聯合國對北韓合資企業的義務，以及察覺和阻止向北韓出售燃料。

泰國

泰國的金融情報中心，即洗錢防制辦公室（AMLO），目前正在更新其國家風險評估報告，以獲取資武擴及其他犯罪以及洗錢防制法（AMLA）尚未涵蓋的實體。PF 風險評估的範圍是可能違反、不執行或規避第 7 項建議之目標性金融制裁義務。更新後的國家風險評估報告預計在 2021 年底前定稿。

透過這次行動，AMLO 旨在瞭解泰國的 ML / TF / PF 威脅、弱點、風險和影響。該行動旨在作為制定政策、戰略和措施的指引，以抵減 ML / TF / PF 風險。

泰國對其 NRA 的 PF 更新包括公部門和私營合作夥伴、主管機關，如洗錢防制辦公室、安全和情報機關、監理機關和自律機關、商工登記處、稅務機關、財政機關、外交機關、執法機關（包括海關和邊境機關）、進出口控制機關和司法機關。關於私部門，將包括申報機構（金融機構與 DNFBPs）、非營利組織（NPOs）和其他法人。最後，風險評估將諮詢國際合作夥伴，如在泰國的相關警察聯絡官。

迄今為止的進展包括收集和分析機構風險評估資料，以及來自問卷調查和訪談／焦點小組的資料。洗錢防制辦公室將分析收集的資料，以評估威脅、弱點和其影響。

洗錢防制辦公室將向所有相關的公部門和私營夥伴傳播國家風險評估報告，以進一步加強他們的政策、計畫、措施和程序，確保有效地減少 ML / TF / PF 風險，並妥善保護泰國的金融系統免遭濫用於 ML / TF / PF。

有益的是，洗錢防制辦公室已經能夠深入瞭解進行 PF 風險評估所面臨的挑戰。缺乏對 PF 的瞭解，特別是在私部門，導致對 PF 風險的認知程度低落，抵減風險的程度也不恰當。泰國回應：已確定有必要就 PF 義務及規避制裁的相關風險進行宣導。

在國際金融體系中混合合法業務與非法交易，也造成識別及抵減 PF 風險之困難。因此，PF 風險，包括 PF 的量，可能是基於感知而不是統計資料來評估的。這一挑戰要求加強合作和協調，並在國家和國際層面分享資訊。

1.5 提供金融機構與指定之非金融事業或人員之指引與培訓

中華臺北提供之案例

2021 年 2 月 2 日，金融監督管理委員會向金融機構轉發聯合國對北韓制裁實施手冊，該手冊由國際合規和能力技能組織與全球民用研究及開發基金會合作，於 2019 年 3 月出版[24]。

新加坡提供之案例

新加坡金融管理局（MAS）於 2015 年 4 月發布金管局洗錢防制及打擊資恐 626 號指引[25]。該指引包括關於 PF 的潛在指標資訊，以及銀行和金融機構在 PF 與凍結資金、客戶盡職調查及內部控制方面的要件。

新加坡金融管理局也一直在與金融機構合作，協助他們應對資武擴風險。在對銀行進行一系列監督訪查後，新加坡金融管理局於 2018 年 8 月發表一份題為打擊資武擴的正確做法的文件，其中概述重要結論，並討論他們在專題監督訪查期間觀察到的正確做法。銀行和金融機構可以利用這份文件來加強其與資武擴有關的現有控制和做法[26]。

此外，新加坡金融管理局與新加坡銀行協會（ABS）合作，將 PF 作為新加坡銀行協會年度金融犯罪研討會的常設議程項目，該研討會是新加坡重要的 AML / CFT 行業外聯活動之一，有來自新加坡和該地區的 500 多名代表參加。

---

24 https://www.amlo.moj.gov.tw/media/15269/dprk-un-sanctions-implementation-handbook_english- version.pdf?mediaDL=true

25 https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and- Licensing/Commercial-Banks/Regulations-Guidance-and-Licensing/Guidelines/MAS-Notice-626- Amendments-Nov-15/Guidelines-to-MAS-Notice-626：November-2015.pdf

26 https://www.mas.gov.sg/regulation/guidance/sound-practices-to-counter-proliferation-financing

泰國提供之案例

洗錢防制辦公室與聯合國毒品和犯罪問題辦公室（UNODC）和皇家聯合研究院（RUSI）等外國單位合作，為主管當局和其他相關合作夥伴（如洗錢防制辦公室（金融情報中心）、安全和情報機構、監理機關、金融機構、外交機關、包括海關在內的執法機關、司法機關，以及最後的報告實體（金融機構和 DNFBPs）辦理有關理解資武擴風險和資武擴風險評估的培訓及研討會。

培訓和研討會的範圍包括：

- 識別由國家和非國家之行為者構成的風險，這些行為者試圖獲取或協助獲取大規模毀滅性武器。
- 採取措施抵減 PF 的風險，包括檢測、調查及阻斷 PF；以及
- 提高對確保國家執行聯合國安理會防制資武擴決議與 FATF 相關標準的意識。

2. COVID-19 對洗錢／資恐態樣影響之最新情況

2020 年度 APG 態樣報告的第 1 章側重於 COVID-19 對 ML / TF 態樣的影響，因為它不僅與 APG 成員有關，且與全球各國有關。該章概述全球 COVID-19 如何促使犯罪集團調整其 ML / TF 態樣，以應對邊境關閉、社交距離要求、對數位通訊／支付管道的更大依賴以及因挪用政府財政支援款項而產生的更多犯罪機會。

隨著 COVID-19 持續到 2021 年，APG 成員被要求提供與 COVID-19 相關的前置犯罪（如福利詐欺、騙局、偽藥、貪腐、毒品、走私等）有關的 ML 及 TF 態樣的最新資訊[27]。

成員們提供的一些案例研究顯示，COVID-19 如何繼續改變 ML / TF 的外觀，包括與個人防護設備（PPE）和醫藥產品銷售有關的網路詐騙和詐欺的增加。還發現利用假的慈善機關接受與 COVID-19 有關的捐款，以及個人假裝與政府之個人以徵求捐款之詐欺行為。持續有會員報告與 COVID-19 有關的政府補貼之詐欺性索賠。

鑒於與 COVID-19 有關的邊境關閉，據報告，與非法毒品、酒精和煙草有關的走私活動也有所增加。與線上賭博有關之可疑交易報告數量的增加被認為是 COVID-19 隔離措施的結果。

---

[27] See section 9

3. 2020-2021 亞太防制洗錢組織之研討會與專案

本報告的這一部分簡要介紹 2020 年 7 月至 2021 年 6 月期間 APG 開展的態樣相關工作。

3.1 態樣專案

數位化瞭解你的客戶（KYC）研討會

在 2019 年 APG 第 22 屆年會上，成員們批准一個關於在亞太地區實施數位 KYC 的兩階段專案。獲准之專案其目標是支援數位 KYC 與數位身分證的實施，包括應用 2020 年 3 月發布的 FATF 數位身分（ID）指引的宣導和能力建構。

- 該項目的第一階段是由設在中國香港的非營利組織資訊科技促進金融穩定聯盟（AFS-IT）與 APG 秘書處合作舉辦的關於數位 KYC 的區域研討會。第一階段的最初計畫是於 2020 年 3 月底在首爾舉行研討會，然而，由於 COVID-19 的影響，該研討會被推遲至 2021 年 2 月 2 日至 2 月 5 日第 22 屆 APG 態樣研討會時線上舉行。
- 目前正在進行的是專案的第二階段，將根據研討會的結果，由 AFS-IT 及 APG 合作制定接續活動的文件。關於這一問題之未來任何工作將取決於秘書處的可動用資源和成員的需求。

資助和協助東南亞的外國恐怖主義戰士

2020-2021 年期間，APG 秘書處與全球合作安全中心合作，最終完成關於資助和協助東南亞外國恐怖主義戰士和回歸者之態樣報告。該報告最終將由秘書處完成，預計於 2021 年 7 月在 APG 年會上通過。

在第 22 屆 APG 態樣研討會之前，報告草案已與 APG 成員分享，以供他們提供反饋和審閱，外國恐怖主義戰士財務概況（與全球合作安全

中心合作）在研討會中另成一個組別。

APG 主辦一次私部門圓桌會議，以收集私部門對外國恐怖主義戰士財務概況的看法和回饋。

FATF 與非法武器販運有關的 TF 風險專案

APG 參加 FATF 關於非法武器販運與資恐之專案。

人口販運和人口走私專案（第二階段）

由於 COVID-19 造成旅行限制，原定於 2020 年 6 月完成的人口販運與人口走私專案（第二階段）的最後一次研討會沒有舉辦，該方案將被視為已完成。

3.2 第 22 屆態樣與能力建構研討會

每年的 APG 態樣研討會都會將來自包括調查和起訴機關的政府機關、金融情報中心、監理機關和私部門的 AML / CFT 部門的從業人員聚集在一起，審議應優先考慮的 ML 與 TF 風險及弱點。

由於 COVID-19 流行期間的旅行限制，第 22 屆 APG 態樣研討會於 2021 年 2 月 2 日至 5 日以線上形式舉行。為期 4 天的研討會有來自 36 個 APG 成員、10 個 APG 觀察員與 29 個私部門或非政府組織的約 325 名代表參加。

研討會包括一次全體會議（第 1 天和最後 1 天）和兩個同時進行的分組會議。分為（i） 數位 KYC（與 AFS-IT 合作）和（ii）外國恐怖主義戰士的財務狀況（與全球合作安全中心合作）。APG 成員、觀察員和來自全球網絡的其他人士在這兩場會議上進行專家簡報、小組討論和其他貢獻。

4. 防制洗錢金融行動工作組織、區域性防制洗錢組織與其觀察員之專案

此節簡要介紹 FATF 與其他 FATF 的區域性組織（FSRB）在 2020 年 7 月至 2021 年 6 月期間發布的態樣報告。

4.1 防制洗錢金融行動工作組織態樣專案

虛擬資產洗錢及資恐紅旗指標（2020 年 9 月）

這份 FATF 報告是對 FATF 於 2019 年發表虛擬資產與虛擬資產服務提供商之風險基礎指引的補充[28]，包含與虛擬資產相關的 ML / TF 紅旗指標，以協助申報機構，包括金融機構、DNFBPs 及虛擬資產服務提供商。各紅旗指標是基於 2017-2020 年各司法管轄區提供的一百多個案例研究而來。

本報告的關鍵指標特別關注於以下方面：

- 增加匿名性的技術特點：如使用點對點交易網站、混幣服務或隱私幣。
- 地域風險：犯罪者可以利用對虛擬資產不具充分、甚至缺乏國家層級應對措施之司法管轄區。
- 交易模式：不合常規、不尋常或不常見的交易模式，這可能顯示存在犯罪活動。
- 交易規模：當交易量及頻率沒有合理的商業解釋。
- 發幣者或收幣者之情況：不尋常的行為可能顯示有犯罪活動；以及
- 資金或財富的來源：可與犯罪活動有關。

---

28 https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

該報告已可在 FATF 網站上查閱：
https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag- Indicators.pdf

貿易洗錢：趨勢和發展（2020 年 12 月）

這份報告[29]的出版標誌著 FATF 和艾格蒙聯盟完成貿易洗錢的聯合計畫。該報告利用 FATF 全球網絡的大量案例研究，審閱利用貿易交易轉移資金而非貨物的犯罪方法。

報告包含針對公、私部門應對貿易洗錢風險的建議，包括使用國家風險評估報告和其他注重風險的材料來提高參與國際貿易的實體的意識。報告還建議改善金融和貿易資料的資訊分享，以及公部門和私部門之間的合作，包括公私夥伴關係。

該報告已可在 FATF 網站上查閱：
https://www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and- Developments.pdf

貿易洗錢活動：風險指標（2021 年 3 月）

FATF 和艾格蒙聯盟於 2021 年 3 月公布這些風險指標，以協助公、私實體識別與貿易洗錢有關的可疑活動。

該報告包括以下方面的風險指標。

- 企業架構；
- 貿易活動；
- 貿易文件及商品；以及

---

29 https://www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

・帳戶和交易活動。

該報告已可在 FATF 網站上查閱：
https://www.fatf-gafi.org/media/fatf/content/images/Trade-Based-Money-Laundering-Risk- Indicators.pdf

更新：COVID-19 相關的洗錢及資恐風險（2020 年 12 月）

本文件更新 FATF 在 2020 年 5 月發布的成果，強調與 COVID-19 有關的洗錢和資恐風險和政策應對。利用 FATF 全球網絡以及 2020 年 7 月和 9 月的私部門和公部門網路研討會的投入，本文詳細介紹犯罪者如何持續利用危機。一些案例研究說明隨著 COVID-19 的發展，風險是如何演變的，以及當局是如何處理的。這些案例包括偽造醫療用品、網路犯罪、投資詐欺、慈善詐欺和濫用經濟刺激措施。

該文件證實 FATF 在 2020 年 5 月表達的擔憂，包括：

- 金融行為之改變：線上購物的數量大幅增加，特別是由於大多數實體銀行分行的廣泛封鎖和暫時關閉，服務轉向到網路上；以及
- 金融波動和經濟萎縮加劇：主要是由於數百萬個工作崗位的損失、數千家公司的倒閉和迫在眉睫的全球經濟危機造成的。

本文件建議當局和私部門採取風險基礎法（RBA）來應對這些不斷變化的風險，正如 FATF 標準所要求，在不擾亂合法的基礎金融服務和不將金融活動推向不受監管的服務提供商的情況下，抵減 ML 及 TF 風險。

該報告已可在 FATF 的網站上查閱：
https://www.fatf-gafi.org/media/fatf/documents/Update-COVID-19-Related-Money -Laundering and-Terrorist-Financing-Risks.pdf

TF 調查和起訴指引（2021）

該機密指引為國家當局提供提高其打擊資恐法律行動有效性的最佳做法，涵蓋偵查、常見資恐態樣調查策略、證明意圖及意識，以及沒收資產作為阻斷 TF 的工具。這份機密報告的最終版本已經分發給執行部門。當局如果想獲得報告的副本，應與其國內 FATF 聯絡人聯繫。

與非法武器販運有關的 TF 風險（2021 年）

這份機密報告旨在提高整個 FATF 全球網絡對於非法武器販運和 TF 之間聯繫的意識，特別是在國家風險評估內容的呈現上，並幫助各司法管轄區制定有效的對策。

這份機密報告的最終版本已分發給各負責主管部門。當局如果想獲得報告的副本，應與其國內之 FATF 聯絡人聯繫。

資助伊拉克和黎凡特伊斯蘭國和基地組織及其附屬組織之更新（2020 年 10 月）－非公開

這份針對 FATF 關於伊拉克和黎凡特伊斯蘭國（ISIL）資助問題的綜合報告[30] 之非公開更新，發布於 2015 年 2 月，基於 FATF 全球網絡提供的資訊，涵蓋基地組織、ISIL 和基地組織之附屬組織。如果當局想要一份最新的伊拉克和黎凡特伊斯蘭國更新資料，應與其國內之 FATF 聯絡人聯繫。

聯合專家會議（2020 年 11 月）

2020 年 11 月，FATF 首次以線上形式召開年度聯合專家會議（JEM）。有來自 FATF 全球網絡、FSRB 及國際組織的 95 個司法管轄區約 400 名代表參加會議。

---

30 https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf

會議從高層次會議開始，討論 FATF 全球網絡成員所面臨的不斷變化的 ML / TF 風險，並舉行一總結會議，討論在多邊背景下追查 ML 案件時加強合作的必要性。另外還舉行四次會議，以推進 FATF 德國主席任期內正在進行和即將進行的優先項目。這些會議涉及：（1）洗錢和環保犯罪；（2）資助具有民族或種族動機之恐怖主義；（3）非法武器販運和 TF；以及（4）業務機關的 AML / CFT 數位化轉型。聯席會議的討論還涉及高層次問題，包括新出現的洗錢和資恐風險，以及在多司法管轄區洗錢案件中的共同行動。這次會議為 FATF 正在進行的工作提供寶貴的意見。

有關這些成果的更多細節可在 FATF 網站上查閱：
https://www.fatf-gafi.org/publications/methodsandtrends/documents/jem-2020.html

環保犯罪的洗錢行為（2021 年 7 月）

本報告旨在加強對環保犯罪的犯罪收益和洗錢技術之規模和性質的意識。該報告彙集 FATF 全球網絡的專業知識，以確定政府和私部門可以採取的較佳做法，以阻斷環保犯罪的盈利能力。本報告的結論是基於 40 多個司法管轄區提供的案例研究和較佳做法，併同民間社會和私部門的專業知識。

該報告的重要結論包括：

- 預估環保犯罪資金流動之規模存在很大差異，但有證據顯示，每年有數千億美元的收益影響到所有地區。除廢棄物販運外，環保犯罪通常發生在資源豐富的發展中國家和中等收入地區，收益來自較大的發達經濟體。
- 犯罪者通常依靠現金密集型企業（通常與出口部門有關）和利用貿易詐欺來清洗環保犯罪的收益。

- 利用貿易詐欺和濫用空殼公司與前台公司來清洗盜伐林木、非法採礦和廢棄物販運的收益，發揮重要作用。
- 犯罪者經常利用資源供應鏈將合法和非法貨物混在一起，以掩蓋其非法來源。
- 在貪腐的驅使下，犯罪者依靠公司架構、轉讓第三方和離岸司法管轄區來混淆實質受益人的身分。
- 在識別和打擊環保犯罪方面，各司法管轄區面臨一系列挑戰。這些挑戰包括：對與環保犯罪相關資金流動的有效理解和意識存在差距；內部協調與機構間的協調存在差距；在資金流動方面的國際合作水準較低；對風險指標的意識不足，無法制定有效的紅旗警示；私部門的能力不足，無法成功實施預防措施。
- 各司法管轄區強調一些好的做法，包括協調涉及環境保護和防制洗錢機構的風險評估、明確和一致的法律架構（包括對發生在國外的環保犯罪進行刑事追訴）、國內外合作指引、聯合工作小組和資訊交流，追蹤和返還來自海外的環保犯罪資金，以及與私部門協商制定紅旗警告。

該報告為 FATF 全球網絡的成員確定以下關鍵的優先事項：

- FATF 全球網絡內所有成員應考慮犯罪者是否可能濫用其金融和非金融部門來掩蓋和清洗環保犯罪的收益，包括沒有國內自然資源的司法管轄區。
- 各成員還必須加強其發現及追查環境犯罪之金融調查執行能力。這包括與外國友軍合作，分享資訊，促進起訴及有效追回被轉移和持有的海外資產。
- 各司法管轄區應充分執行 FATF 的標準，作為打擊環保犯罪洗錢的有效工具。這包括確保向 FATF 標準所涵蓋的相關中介機構（如貴

金屬與寶石交易商以及信託和公司服務提供商）宣導洗錢防制。

- 各司法管轄區應考慮建立和加強公部門和私部門的對話，以分享風險資訊，並組織由行業帶領之倡議，以加強針對供應鏈及其資金流動的盡職調查。這些舉措可以在提高對可疑金融活動的認識，並透過尋找證明貨物合法來源等方法來解決混入不法資金等方面發揮重要作用。

該報告已可在 FATF 網站上查閱：
https://www.fatf-gafi.org/publications/environmentalcrime/documents/money-laundering- from-environmental-crime.html?hf=10&b=0&s=desc（fatf_releasedate）

民族或種族動機之恐怖主義融資（2021 年 6 月）

本報告彙集在處理牽扯民族或種族動機之恐怖主義（EoRMT）方面具有經驗的司法管轄區和機關的專業知識，目的是提高主管當局、非政府機關、私部門和廣大公眾對與極右翼勢力有關的更廣泛 TF 風險的理解。報告中的發現是基於 FATF 全球網絡中約 30 個司法管轄區的意見，以及來自私部門和與 FATF 合作的國際機關的專業知識。報告概述極右翼勢力籌資、轉移和使用資金的主要方式，並提供這方面的實際案例。

報告的重要結論包括：

- 雖然極右翼恐怖襲擊主要是由自籌資金的單獨行動者實施的，但極右翼團體採用一系列的籌資方式。其中包括捐款（透過眾籌和個人捐款）、會員費、商業活動（包括舉辦音樂會、銷售商品和房地產投資）以及犯罪活動。值得注意的是，極右翼勢力的大部分資金似乎都來自合法來源。

- 與其他形式的 TF 相比，極右翼勢力似乎不特意隱藏其交易。許多司法管轄區還報告說，極右翼勢力行為者在轉移資金方面的操作越來越複雜。
- 資金似乎被用於不同的活動，從資助攻擊到購買設備、培訓、設計及散布文宣、招募、人脈網絡、法律費用，甚至購買和維護房地產資產。
- 報告強調在面對資助極右翼勢力動機團體及攻擊所面臨之挑戰，包括在不同的司法管轄區有不同的打擊極右翼勢力恐怖主義的法律制度；很少有國家對此團體做出指定；團體（及在某些情況，實施恐怖襲擊之個人）之間的跨國聯繫越來越多；大多數極右翼勢力所執行的攻擊是由自籌資金的孤狼所為；以及在交換金融訊息方面有限的公部門和私部門夥伴關係。

報告中的建議包括：

- 鼓勵各司法管轄區繼續深化對資助民族或種族動機之恐怖主義的瞭解，特別是透過將此威脅納入其國家風險評估，與相關公部門和私營夥伴合作偵查威脅，並與相關國際夥伴交流最佳做法，以應對資助民族或種族動機之恐怖主義日益增長的跨國特徵。
- 各司法管轄區應在 COVID-19 危機提供招募資助民族或種族動機之恐怖主義團體之機會的背景下，繼續關注其所帶來的不斷變化的威脅。

該報告已可在 FATF 的網站上查閱，網址是：
https://www.fatf-gafi.org/publications/methodsandtrends/documents/ethnically-racially- motivated-terrorism-financing.html

4.2 中東與北非防制洗錢金融行動工作組織

關於新冠病毒流行（COVID-19）及其對中東和北非地區 AML / CFT 系統的影響研究。（2020 年 8 月）

本報告紀錄由中東及北非防制洗錢金融行動工作組織向其成員分發的問卷調查回覆，該問卷要求提供關於 COVID-19 對該地區 AML / CFT 系統的影響以及在實施相關犯罪時使用的最重要方法和趨勢的資訊和案例研究。

本報告探討該地區各司法管轄區為應對 COVID-19 帶來的發展而採取的 AML / CFT 系統措施。一些司法管轄區表示，由於經濟衰退和隔離條件的影響，可疑交易報告的數量大幅減少。報告探討該地區 AML / CFT 系統所面臨的最重要的挑戰，包括遠距工作方面的技術困難、國內當局各機關之間的合作減少以及國際合作減少、將資源轉用於防治 COVID-19 以及對監理機關執行實地檢查的影響。

該報告還紀錄該地區各司法管轄區為抵減 COVID-19 的影響而採取的最佳做法，包括利用科技進行線上實地檢查及履行 " 瞭解你的客戶 " 要求。

報告還概述該地區在 COVID-19 期間發現的主要態樣有：網路犯罪、貪汙、跨境現金走私和詐欺，包括在捐贈和偽造醫療物品方面。

報告建議主管當局採取幾項關鍵行動，包括：

- 不僅要試圖將合規水準恢復到 COVID-19 疫情流行之前的水準，而且要持續不斷地加強 AML / CFT 體制，即使在危機時期也應如此。
- 制定統一的與 COVID-19 相關的 ML 及 TF 的風險示意圖，並努力尋找措施來緩解它和類似的危機。
- 審查 AML / CFT 法規的適當性及其應對關鍵和危機情況之能力。

・啟動國際合作管道以便及時準確地回應資訊之請求。

該報告已可在 MENAFATF 網站上查閱：

http://www.menafatf.org/information-center/menafatf-publications/coronavirus-pandemic- covid-19 and-its-impact-amlcft-systems。

4.3 歐亞防制洗錢及打擊資恐小組

金融機構使用預防措施進行犯罪偵查和風險評估的態樣（2021 年）

本報告總結各司法管轄區與運用可疑交易報告有關的方法和最佳做法，並包括金融機構為識別犯罪和評估風險而採取的預防措施。報告包括歐亞防制洗錢及打擊資恐組織（EAG）成員關於運用可疑交易報告及預防措施的最佳做法的案例研究，還概述報告機構在 COVID-19 疫情流行中監督和實施預防措施的具體情況。

本報告的重要結論包括：

- 在實踐中證明對抵減 ML / TF 風險有效之主要預防措施是拒絕為客戶進行交易與拒絕為客戶提供存款銀行帳戶服務，也被稱為拒絕服務。
- 在一些 EAG 成員中，可疑交易報告格式包含客戶之實質受益人以及客戶用於存取網上銀行服務之裝置之 IP 與 MAC 位址的資訊。這些資訊使金融情報中心能夠識別更多的關聯並集合同一主題的可疑交易報告。
- 在 COVID-19 疫情流行期間，由於線上服務的快速增長和電子商務的發展，金融行為已發生改變。
- 在疫情流行期間，網路犯罪、網路詐欺和濫用公部門資金的情況有所增加。
- 與個人防疫設備、藥物和慈善機構有關的詐欺行為也在增加。

- 跨境網路博弈之情況有所增加。
- 在疫情流行期間，一些司法管轄區的可疑交易報告數量增加，原因在於數位交易激增和網路犯罪增加，而其他司法管轄區的可疑交易報告數量減少，原因是經濟活動衰退；以及
- 在 2020 年上半年，一些 EAG 會員國取消對金融機構一些部門的預定檢查，並將實地檢查改為遠距檢查。

報告中對 EAG 成員的建議包括：

- 分析金融機構在運用拒絕交易及拒絕開立帳戶（存款）的權力為風險緩解措施之做法，及如有必要，採取措施加以優化。
- 考慮在關於可疑交易的電子表格中加入客戶之實質受益人資訊，以及客戶在遠距銀行業務中所使用之裝置之 IP 與 Mac 位址，以及一個特殊記號去標記需要緊急回應的重要可疑交易報告。
- 建請 EAG 成員的主管當局與私部門合作，審查當前的疫情流行趨勢和風險，在必要情況，更新關於識別高風險交易的相關建議和指導文件；以及
- 請 EAG 成員的主管當局考慮擴大使用資訊技術工具與申報機構進行遠端互動的形式，以實施非接觸性監督，並在廣泛的回覆者中迅速收集有關風險和弱點的資訊。

該報告已可在 EAG 網站上查閱：
https://eurasiangroup.org/files/uploads/files/Preventive_measures_final_report_eng.pdf

4.4 洗錢防制措施與資恐評估專家委員會

在 COVID-19 危機期間洗錢防制措施與資恐評估專家委員會司法管轄區之洗錢及資恐趨勢（2020 年 9 月）

本報告使用向所有洗錢防制措施與資恐評估專家委員會管轄區發出之問卷調查之答覆，以確定疫情流行期間出現的新的洗錢案件、實際挑戰、態樣及趨勢。

該報告的重要結論包括：

- 總體犯罪之程度仍然穩定或略有下降，可疑交易報告保持穩定。
- 各司法管轄區申報某些犯罪，特別是跨國犯罪陡然上升，如詐欺（透過電子方式）和網路犯罪，為洗錢目的創造新的收益來源。
- 與販毒、TF、濫用非營利組織和內線交易有關的犯罪並未增加。然一些司法管轄區報告醫療犯罪、網路犯罪和貪汙方面的增長。
- 發現有可能濫用政府用來支援企業和民眾的緊急經濟抒困措施（如財政援助和稅制獎勵）。
- 一些司法管轄區暫停原本公部門採購醫療設備和用品之複雜程序，因而造成詐欺和貪腐。
- 金融情報中心之間的合作則沒有受到影響，事實證明，在交流與詐欺性提供醫療和衛生設備、仿冒品、未交貨騙局及非法超額定價相關的跨境案件的資訊方面，合作尤為重要。

確認與 COVID-19 有關的三種主要詐欺態樣：
醫療設備詐欺、經濟抒困措施詐欺，以及與公部門採購合約相關的詐欺／貪汙。

報告中的建議包括

- 執法部門應充分重視調查 COVID-19 疫情危機期間的詐欺和網路犯罪。
- 邊境警察及海關當局應特別關注可能與不法資金轉移有關的 " 逾期需求 " 的現金跨境流動。跨境現金流動被犯罪者用來資助他們的行

動，據說現在由於 COVID-19 導致國家邊境暫時關閉，犯罪組織面臨著現金跨境運輸的 " 逾期需求 "。

- 當局應密切監測公部門採購的情況，以發現並避免可能的濫用和貪腐案件，特別是在已放鬆管制的地方。

該報告已可在特設專家委員會網站上查閱：
https://rm.coe.int/moneyval-2020-18rev-covid19/16809f66c3

4.5 艾格蒙聯盟

關於重大稅務犯罪的洗錢問題的公告（2020 年 7 月）

本公告旨在介紹重要經驗、最佳做法和有代表性的案例，幫助在國家和國際層面加強打擊重大稅務犯罪的洗錢行為。該公告依據向艾格蒙聯盟的金融情報中心分發的問卷調查及相關案例之調查所取得之資訊。

公告中的主要經驗教訓包括：各國當局有效接收、獲取、分析和分享相關涉稅資訊，包括相關洗錢的資訊，為各司法管轄區有效處理嚴重涉稅犯罪的關鍵。此外，給予高度稅收保密的國家法律架構使資訊交流的對等性變得複雜。此外，低稅率／零稅率政策不僅增加有關司法管轄區對投資者的吸引力，而且也增加對犯罪者的吸引力，這可能在其他司法管轄區造成弱點，因為缺乏受益所有權透明度阻礙跨國調查。

公告就打擊重大稅務犯罪之洗錢行為的最佳做法提出建議，包括促進金融情報中心和稅務機關在國家層級的有效合作以及金融情報中心之間的國際合作。公告提供一系列案例來說明最佳做法，包括金融情報中心之間如何進行有效合作。

該公告可在艾格蒙聯盟網站上查閱：
https://egmontgroup.org/en/filedepot_download/1661/117

COVID-19 金融情報中心的最佳實踐（2021 年 3 月）

本報告參考艾格蒙聯盟 FIU 卓越及領導訓練中心（ECOFEL）為加強金融情報中心在 COVID-19 疫情期間的能力而舉行的一系列虛擬圓桌會議，以及對艾格蒙聯盟成員、觀察員和其他國際組織發表的公開資料進行的評估工作。該報告紀錄因 COVID-19 疫情流行而出現的各種態樣。

報告發現，在疫情流行期間，可疑活動報告的數量並沒有明顯減少，金融情報中心只注意到在經濟衰退或申報機構能力受限的情況下出現減少。

重要的是報告還指出，大多數金融情報中心都發現一些新出現的風險，特別是與詐欺（涉及醫療設備和個人防護設備）、放寬公部門採購規則有關的貪腐以及包括網路釣魚在內的網路犯罪。金融情報中心已經注意到詐欺、網路釣魚、其他網路詐騙以及濫用公部門資金的情況有所增加。其他新出現的風險包括兒童色情製品和兒童剝削、偽造貨幣和野生動物犯罪的出現。金融情報中心也意識到新出現的風險，如與 COVID-19 疫苗的開發有關的風險。

報告提供金融情報中心針對 COVID-19 相關犯罪所採取行動的案例，並羅列金融情報中心應對 COVID-19 風險形勢變化之建議。

該報告已可在艾格蒙聯盟的網站上查閱：
https://egmontgroup.org/en/filedepot_download/1661/123

艾格蒙 FIU 卓越及領導訓練中心 - 對野生動物犯罪的金融調查（2021 年 1 月）

本報告旨在為金融情報中心提供對於野生動物犯罪能進一步瞭解，並介紹與野生動物犯罪資金流動相關的趨勢和模式。報告還探討野生動物犯罪與其他形式的犯罪活動，如毒品犯罪、貪汙、TF 和非法武器貿易之間的聯繫。報告指出，從歷史上看，全球範圍內對野生動物犯罪的財務調查非常少，導致缺乏金融調查及低處罰，使野生動物犯罪成為犯罪者的高利潤、低風險企業。

報告強調調查非法野生動物買賣資金流的好處，並解釋金融情報中心如何參與支持對野生動物犯罪的金融調查。報告列出提高金融情報中心工作有效性的建議做法，包括正確評估司法管轄區內非農產業的野生動物犯罪風險，根據司法管轄區內野生動物犯罪的戰略評估過濾和分析可疑交易報告，以及加強機關間合作和資訊交流，並建議將積極參與打擊野生動物犯罪的國際組織和非政府組織作為金融情報中心的良好合作夥伴。

該報告已可在艾格蒙聯盟網站上查閱：
https://egmontgroup.org/en/filedpot_download/1661/122

關於運用金融情報打擊網路兒童性虐及和剝削行為的公告（2020 年 7 月）

本公告重點介紹與網路直播兒童性虐待和剝削（CSAE）有關的支付款項的戰略情報。公告指出，專門為網路串流所創造的犯罪商業模式為該活動帶來的金融問題在其他形式的 CSAE 犯罪並不普遍。公告隨後解釋網路串流的 CSAE 的金融問題，包括網路串流內容的支付模式和相關的商業模式。它還強調私部門實體提交的報告（包括可疑活動報

告和可疑交易報告的分析）讓金融情報中心能夠向執法機關提供與資金流動及查明犯罪者與協助者有關的可操作情報。

該公告可在艾格蒙聯盟網站上查閱：
https://egmontgroup.org/en/filedepot_download/1661/119

4.6 西非政府間防制洗錢行動組織

西非之非法野生動物貿易和金融調查（2021 年 4 月）

本報告由 RUSI 在西非政府間防制洗錢行動組織（GIABA）的支持下出版。本文依據對西非和中非主要利益相關者的 89 次訪談，以及對 GIABA 17 個成員中的 12 個 FIU 的調查，評估該地區非法野生動物貿易（IWT）在金融層面的調查程度。

本文分析西非的非法交易野生動物趨勢，重點是高收益的象牙、穿山甲鱗片和紅木販運，並指出目前阻礙運用金融調查於非法野生動物貿易案件的主要挑戰。

該文件的主要發現包括：

- 86% 的受訪者認為非法野生動物貿易是一個嚴重問題，但只有 58% 的受訪者在其國家 ML / TF 風險評估中提到環保犯罪或非法野生動物貿易。
- 只有一個金融情報中心認為自己經常參與調查非法野生動物貿易案件。
- 只有 25%（3 個）的金融情報中心報告說曾經進行過非法野生動物貿易金融調查，沒有一個司法管轄區完成過一次以上的調查，而且沒有一個司法管轄區因為非法野生動物貿易對 ML 或其他金融犯罪進行起訴。

- 金融情報中心對西非用於產生、轉移和清洗非法野生動物貿易收益的方法瞭解甚少。
- 大多數西非政府間防制洗錢行動組織會員國將環保犯罪作為 ML 的前置犯罪，但大多數金融情報中心認為：缺乏將非法野生動物貿易作為前置犯罪的意識，是目前在野生動物案件中未進行金融調查的最重要原因。
- 大多數金融情報中心認為，需要更多的培訓、知識和財政資源，以追查國際野生動植物資源案件，這是能力建設的一個優先事項；以及
- 該文件確認，全球執法行動仍然不成比例地集中在低度的、容易被取代的偷獵者身上，而幾乎沒有觸及非法野生動物貿易的控制者和最終受益者。

該文件的主要建議包括：

- 在西非打擊野生動物犯罪網絡中設立一個金融犯罪工作組，負責協調在區域層級實施西非打擊野生動物犯罪。
- 將金融情報中心和反貪汙機關納入所有為解決野生動物犯罪而設立的國家級國內工作組。
- 負責制定國家打擊野生動植物犯罪策略和行動計畫的政策制定者應納入在所有合適的非法野生動物貿易案件中啟動平行金融調查的要求。
- 改進國內和國際合作及資訊分享的建議。

該報告已可在 GIABA 網站上查閱：
https://www.giaba.org/media/f/1131_IWT_west_africa_Report_2021.pdf

5. 洗錢及資恐方法

5.1 利用國際金融業務分行、國際商業公司及境外信託，包含信託或公司服務提供商

斐濟

境外利潤轉移和逃稅

B 君為斐濟與 X 司法管轄區的雙重國籍人士，被舉報以合法的商業支出為藉口向當地稅務局申請偽造增值稅退稅。斐濟金融情報中心的檢查顯示，B 君在斐濟開辦一家獨資企業，從事不動產貿易活動，同時是斐濟另外兩家公司的董事，這兩家公司從事建築業。然而，由於他的一家公司沒有明顯的貿易活動，而另一家公司在同一時期出現虧損，因此確定沒有與增值稅申報相匹配的貿易活動。斐濟金融情報中心確定，B 君以個人名義向稅務機關申報並退還超過 110,000 斐濟元（53,981 美元）的增值稅。且在 5 年內，以公司名義申請退稅 75 萬斐濟元（368,893 美元）。這些款項用於在斐濟購買三處房產，總價值超過 180 萬斐濟元（885,359 美元），其中部分資金來自貸款。向斐濟的稅務部門及 X 司法管轄區的相關金融情報中心提供本案件情資分送報告。

紐西蘭

濫用紐西蘭信託或公司服務提供商和相關架構進行境外貪汙收益的洗錢活動

在一境外個人的指示下，一家紐西蘭（NZ）信託或公司服務提供商（TCSP）建立兩個境外信託架構，使用紐西蘭有限責任公司作為受託人，並作為多個紐西蘭有限合夥公司的合夥人（有限合夥和普通合夥），這些公司也被納入該架構並用於開設紐西蘭銀行帳戶。該信託

或公司服務提供商是所有法人實體的董事，並有權操作銀行帳戶。該境外人士和他的妻子是上述信託協議的受益人，但在紐西蘭公開之資料庫中，他們與上述架構沒有任何可識別的聯繫。

該境外人士隨後被起訴，罪名是利用一家位於 B 司法管轄區的公司，共謀進行電信詐欺，並且違反 A 司法管轄區的反回扣法。當局指控該境外人士參與一個更廣泛的共謀，涉及一份偽造的行銷協議，用於掩蓋與提供醫療用品有關的回扣和賄賂付款。人們懷疑這一計畫的收益是透過一個國際信託和公司架構網絡進行洗錢的：包括以其名義購買海外資產的紐西蘭境外信託架構，且據信其所擁有之紐西蘭銀行帳戶已協助挪移了 150 多萬美元的資金。

透過紐西蘭清洗的海外政治貪汙和賄賂所得款項

境外司法管轄區 A 的一名政務人員和一家國有能源公司的負責人在司法管轄區 B 被起訴，罪名是賄賂、貪汙和合謀洗錢，因為他從司法管轄區 B 的公司高階人員那裡收受賄賂，以貪汙方式獲得能源合約和未付款發票的優先付款。在過去的七年裡，該官員與他的妻子一直居住在 C 司法管轄區。

該官員向當局承認，在 2011 年至 2014 年期間，他與 A 及 B 司法管轄區的官員合謀，向一系列關係人索賄和直接行賄，並透過一系列金融交易清洗賄賂，包括向該官員或關係人在 D 及 E 司法管轄區擁有或控制的銀行帳戶洗錢。

一筆 1,740 萬紐西蘭幣（12,564,408 美元）的資金從一位被起訴官員的妻子在 E 司法管轄區註冊的銀行帳戶轉入一個紐西蘭帳戶。這些資金被匯入一家紐西蘭會計師事務所的紐西蘭帳戶，該事務所專門代表國際 " 高淨值 " 客戶創建和管理離岸架構。在巴拿馬文件的報導中，該

會計師事務所的雇員被列為許多紐西蘭和海外公司的主管和／或代名人，這些公司構成莫薩克　馮塞卡律師事務所的一部分。

這些資金轉移是根據被起訴官員的妻子的指示進行的。作為加強盡職調查的一部分，紐西蘭的銀行要求會計師事務所提供進一步的資訊，這些資訊顯示，基於一部分政治人物因素的考量，司法管轄區 E 的銀行關閉了在司法管轄區 E 具有營業活動的司法管轄區 A 國民的帳戶，並清算投資組合，資金後續轉移到紐西蘭用於投資。會計師事務所表示，該官員妻子預計在不久的將來前往紐西蘭。於此同時，會計師事務所已代表她建立 " 所需架構 "。

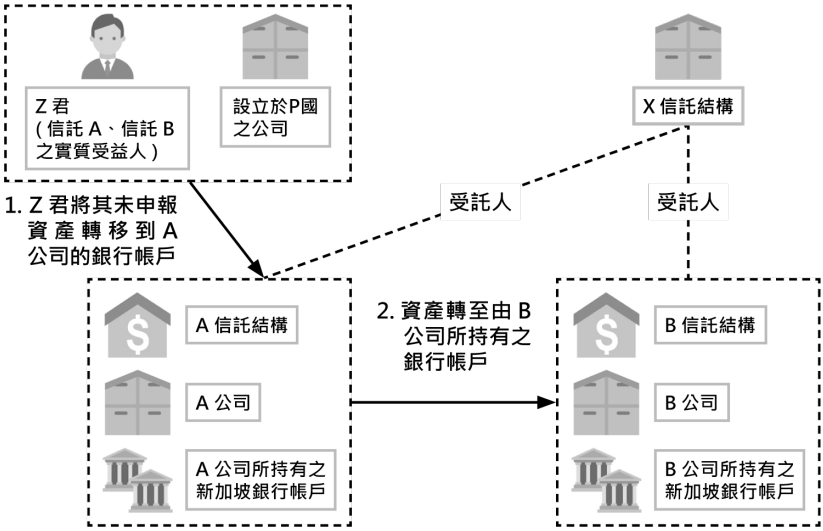
新加坡

新加坡警察部隊商務事務局針對一持有執照的專業中介機關遭指控利用信託架構隱匿實際所有權案件進行調查。

一家在新加坡註冊的信託公司（" 信託公司 X"）據稱與位於 S 司法管轄區的資產管理公司合謀在新加坡建立複雜的信託架構，目的是隱匿屬於 A 司法管轄區 Z 君的金融資產之實質受益人。這項調查源於 A 司法管轄區的司法互助請求，A 司法管轄區啟動了對 Z 君個人的民事沒收程序。根據 A 司法管轄區的法律，Z 君面臨逃稅指控，因為他沒有申報在 A 司法管轄區以外其未揭露且未納稅的離岸銀行帳戶的資產。

信託公司 X 協助兩個信託架構的建立和管理，並被註冊為資產的受託人。信託架構的實質受益人是 Z 君。信託架構包括在 B 司法管轄區註冊的公司（A 及 B 公司），這些公司又另在新加坡設有銀行帳戶。從 2012 年到 2017 年，Z 君將其未申報的金融資產從 P 司法管轄區的一個基金會轉移到在 B 司法管轄區註冊的上述公司在新加坡開設之銀行帳戶。

在調查過程中，新加坡與 A 司法管轄區當局密切合作，查封銀行帳戶中的資金，金額約為 350 萬新加坡幣（260 萬美元）。根據 A 司法管轄區當局與被告 Z 之間的和解協議，A 司法管轄區逃稅犯罪的收益被追回，並最終歸還 A 司法管轄區政府。目前，正針對信託公司 X 涉犯之洗錢罪進行調查。



5.2 利用虛擬資產（加密貨幣）[31]

澳洲

2020 年 6 月，澳洲聯邦警察局（AFP）開始調查一個身分不明的人利用身分盜竊受害者的資訊在數位貨幣交易所（DCE）註冊多個帳戶，隨後利用這些帳戶清洗犯罪所得。澳洲聯邦調查局與數位貨幣交易所

[31] 根據 FATF 的定義，虛擬資產是一種以電子方式來定義其資產價值交換、交易，並可用於支付或投資目的。虛擬資產不包括法幣、證券和其他金融資產之數位型態，這些在 FATF 建議中已經涵蓋（https://www.fatf-gafi.org/glossary/u-z/）。

合作，發現有超過 40,000 澳幣（31,100 美元）被存入虛擬貨幣自動提款機，並透過在數位貨幣交易所註冊的九個獨立帳戶進行轉移。隨著進一步的調查並確定未知的責任人，他隨後被逮捕並被指控犯有以下罪行：

- 使用偽造客戶姓名接受指定服務，此舉違反 2006 年防制洗錢和反恐怖主義資助法（Cth）第 140（1）條；以及
- 盜取身分資訊，違反刑法（聯邦）第 372.2（1）條。

紐西蘭

比特幣交易商助長詐欺

一名在 localbitcoins.com 上營業的點對點比特幣幣商，協助在海外的國際詐騙犯將騙來的法幣兌換成比特幣。這些海外詐騙者會聯繫紐西蘭的受害者，並採取欺騙手段（主要是感情詐騙和預付費詐騙）來說服受害者向他們提供資金。騙子指示受害者與他們在當地的 " 合夥人 "（比特幣幣商）會面，進行現金交易，並向受害者提供與合夥人會面的時間和地點。與此同時，騙子還會聯繫比特幣幣商，告知他們希望用紐西蘭幣購買比特幣，指示幣商在一個特定的時間和地點與他們的 " 合夥人 "（實際上是詐騙受害者）見面，進行交易。騙子向幣商提供他們的比特幣錢包地址，接收與受害者交給他的現金價值等值的比特幣。比特幣幣商在協助進行這些交易、接受受害者的現金及在”不過問任何問題”的情況下將等值比特幣存入騙子的帳戶時，都沒有進行任何形式的盡職調查。

巴基斯坦

販運毒品和未經授權的虛擬資產交易

XYZ 銀行懷疑 AM 先生參與未經授權的虛擬資產交易，因此對其帳戶申報可疑交易報告。在一個虛擬資產交易平臺上的活動顯示，AM 先生參與比特幣買賣，根據中央銀行的指令，此行為在巴基斯坦是非法的。

據申報內容來看，由於該帳戶有不尋常之高周轉率與許多不相干的交易對象，交易活動相當不尋常，故銀行對 AM 先生的帳戶進行調查。在對交易活動的分析中，很明顯該人參與虛擬資產的交易。

此外，AM 先生正在與許多無關的交易對象進行高額交易，其中大多數人被懷疑參與哈瓦拉或其他犯罪活動。根據巴基斯坦金融情報中心的資料庫，在緝毒警隊的調查中，發現 AM 先生的一個交易方（即 M / s AA 的業主 BA 先生）其收益來自銷售毒品。BA 先生的帳戶被存入來自 AM 先生帳戶的大量資金，但卻沒有明確的用途。

由於銀行懷疑 AM 先生參與虛擬資產交易，並可能為其他人利用虛擬資產進行犯罪所得轉匯，因此與執法機關和中央銀行分享該金融情報。

龐氏騙局與虛擬貨幣

XYZ 銀行將一個法人實體（即 ABC 公司）申報可疑交易報告，因為銀行透過巴基斯坦首相執行管理辦公室（PMDU）和工商登記（SECP）之投訴專用網站收到投訴，稱法人實體 ABC 貿易公司涉及從公開募資活動中非法吸收存款，承諾不切實際的高額投資回報。根據 ABC 貿易公司的網站，它從事虛擬貨幣買賣與投資，還在不同的司法管轄區提供虛擬貨幣的錢包裝置及 ATM 設備。

ABC 貿易公司沒有在巴基斯坦證券交易委員會（SECP）註冊。被投訴後發現，該法人實體大概是透過多個不同的公司在其司法管轄區內

運作，而他們的事務由三個人負責，包括 SR 先生、他的妻子 ZK 女士及他的兒子 AW 先生。

此外，其他銀行也申報關於 SR 先生及其家庭成員的多份可疑交易報告，原因是他們大規模地參與龐氏騙局和虛擬貨幣。

SR 先生在 2011 年至 2020 年期間開設 70 個銀行帳戶，資金主要透過來自其司法管轄區內不同城市的網路交易存入，並透過清算交易方式轉出。70 個帳戶中的 59 個是在 2018 年至 2020 年期間開設的。在這些帳戶中觀察到龐大營業收入。大部分資金透過網路交易存入，並透過清算交易、支票或提現方式轉出。

在這些人以不同的公司名稱經營各種營業項目，這些公司開戶表格中卻使用相同的公司地址。在內地稅務局的納稅人資料庫中搜索時，發現這些企業只繳納微不足道的稅金。該金融情報已與執法機關和中央銀行分享，以調查此事。

菲律賓

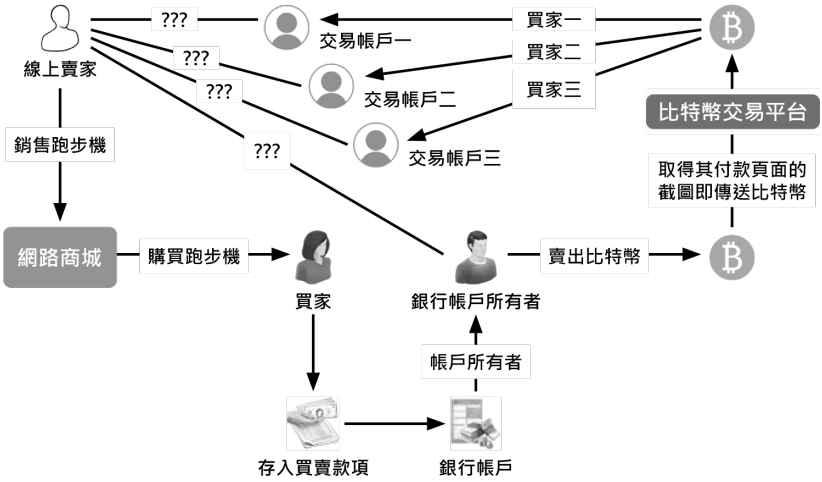
涉及比特幣而非基於合法交易之存款或資金轉移

犯罪嫌疑人於 2020 年 1 月在菲律賓南他加祿地區的一家銀行開設一個可用自動櫃員機且提供存摺之帳戶。根據填寫的客戶資訊表，當事人為一家雜貨店的老闆，月收入為 70,000 菲律賓披索（1,461 美元）。然而，由於 2020 年 3 月有一筆來自單一匯款人的匯款，金額為 55,400 菲律賓披索（1,156 美元），引起銀行監控系統警報的觸發。銀行試圖與當事人聯繫，要求其提供該警示交易的證明文件。銀行於 2020 年 5 月 13 日與當事人取得聯繫，他透露這筆交易的款項是來自一位訂購 5,000 個口罩的客戶。然而，銀行確定該筆匯入匯款是來自一家經核實

的比特幣公司。該客戶被通知到分行提供證明文件，但由於呂宋島實施加強社區檢疫（ECQ），該客戶無法照做。該分行遂要求當事人透過電子郵件發送一份憑證和送貨單的副本或任何交易證明。當事人提交一份送貨單和憑證，但經查，所提交文件均無法被接受。因當事人聲稱該交易是網上銷售，銀行又另外要求當事人提供一份送貨／快遞收據的影本和有關該交易的對話截圖。在 2020 年 5 月 13 日至 27 日期間，銀行幾乎每天都打電話給當事人，以尋求進一步的文件，但沒有結果。當事人現在拒絕接聽銀行的電話，而且當事人帳戶內的資金已經低於維持帳戶之要求。

比特幣網路購物騙局

一個買家從一個網路商城購買一台跑步機，線上賣家指示買家將款項存入某個銀行帳戶。2020 年 6 月 1 日，買方進行五次資金轉帳，總額為 22,000 菲律賓披索（459 美元），但買家從來就沒有收到跑步機。受款人銀行帳戶所有人（BBAC 先生）否認與網上所謂騙子／賣家有任何關係，強調他從未出售過任何配件／設備。BBAC 先生提到，在 COVID-19 疫情開始時，他開始在一個合法的線上點對點金融平臺從事比特幣交易，在該平臺上之人係以用戶名稱或化名註冊。2020 年 5 月 31 日，BBAC 先生與三個用戶進行比特幣交易。在收到向其銀行帳戶成功轉帳的截圖後，BBAC 先生將比特幣發給交易者，但不知轉帳的資金是來自何人。BBAC 先生提交所有的證明文件，包括交易的截圖。本案最終受益人／嫌疑人的細節仍然未知。



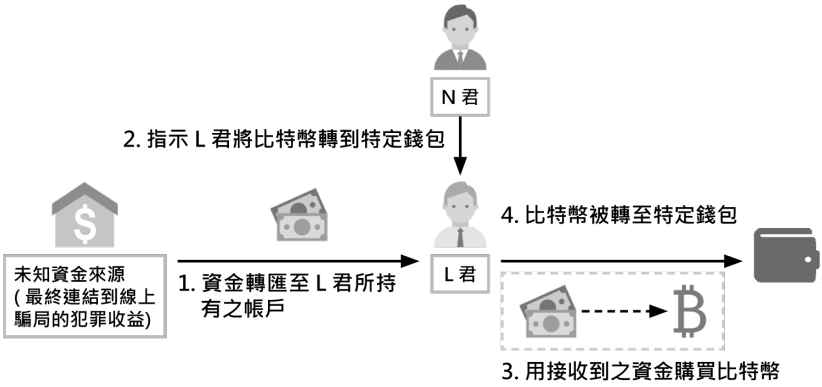
新加坡

L 君於 2021 年 1 月 28 日因未經許可提供數位付款代幣服務被判處 4 週有期徒刑。這是新加坡根據 2020 年 1 月生效的支付服務法（PS Act）首次定罪之人。支付服務法規定，在沒有上述法案規定之必要許可證的情況下從事提供支付服務業務的個人行為屬於犯罪行為。

在 2020 年 2 月底時，L 君看到一個名為 "N 君 " 的網路人物在社交媒體平臺上發布的招聘廣告。這份工作要求 L 君在自己的銀行帳戶中接收資金，並使用這些資金購買比特幣，酬勞定為交易額的 10%。

L 君接受這份工作，期間收到轉入她銀行帳戶的 13 筆匯款，並提取接近 2,800 新幣（約 2,110 美元），多次在一台比特幣自動櫃員機上購買比特幣。在 N 君的指示下，L 君將比特幣轉入指定的比特幣錢包，並在每次購買比特幣後從手機上刪除他們之間的 WhatsApp 對話紀錄。

雖然這些錢被追蹤到是來自網上詐騙的犯罪所得，但調查並沒有發現 L 君故意清洗犯罪所得。然而，L 君在沒有許可證的情況下提供數位付款代幣服務，其行為構成犯罪。



5.3 利用專業服務（律師、公證人、會計師）

馬來西亞

律師事務所參與抽走公司資金

嫌疑人受某政府機關委託，負責監督購買土地備以種植橡膠樹的工作。購買土地的存款被存入一家律師事務所的客戶帳戶，該帳戶內資金隨後被轉移到一家公司，然後被嫌疑人及其同夥在律師的配合下施以詐騙。購買土地之計畫從未實現，最終被政府機關中止。該律師事務所允許使用其客戶帳戶接收非法活動的收益，然後再轉到公司，最終透過現金支票提取資金。

菲律賓

利用 DNFBPs 設立被指控自非法活動中獲得資金之法人實體

2018 年，一外國政府請求菲律賓提供協助調查一起有關其國民涉嫌販毒和洗錢之案件。這些外國國民向幾個司法管轄區轉移大量資金，涉及從菲律賓偽造貨物進口。據稱，上述對象將價值 15.3 億菲律賓披索（3,060 萬美元）的販毒收益轉移給 21 個菲律賓法人實體與 2 名個人。

4 家國內註冊的服務提供商獲得價值約 1.893 億菲律賓披索（379 萬美元）的收益。然而，財務紀錄顯示，3.8642 億菲律賓披索（773 萬美元）被存入上述 4 個服務供應商的帳戶。

該請求中的 21 個法人實體註冊登記為服務提供商、貿易公司、軟體解決方案、顧問公司等。某位律師和律師事務提供協助幫忙成立這些公司（包括 4 家服務提供商）。

根據態樣，明確可知提供服務的律師和律師事務所屬於 DNFBPs 準則的範圍，例如作為組建代理人，提供通訊地址，以及代表 DNFBPs 準則中定義的法人或安排行事。他們是 2001 年洗錢防制法（AMLA，經修訂）規定的人員，因此應在菲律賓反洗錢理事會註冊。

態樣的存在和可疑交易報告數量的增加可能顯示出更高的威脅等級，因為這兩者暴露可能出現的威脅，涉及管轄範圍內的法人。

5.4 貿易洗錢及移轉訂價

澳洲

在貿易洗錢中使用高端電子產品

2017 年，澳洲邊防署（ABF）開始審查自另一個司法管轄區移交的，與利用小型可攜式電子產品貿易有關的貿易洗錢。透過一系列詳細的技術分析檢查，並輔以金融和犯罪情報，邊防署專家能夠對相關法人實體準備一個詳細的犯罪網絡進行評估。透過拼湊一個廣泛的洗錢協助者網絡，澳洲邊防署發現自 2014 年以來有超過 5 億澳幣 [3.198 億歐元／ 388,806,522 美元] 透過澳洲銀行帳戶進行匯款。

收益是透過在北美銷售毒品產生的。犯罪所得被轉移到東南亞的銀行帳戶，然後透過澳洲金融機構的眾多澳洲銀行帳戶進行分層。這些販

毒收益被匯入海外銀行帳戶，或用於購買小型高端電子設備，出口到東南亞和中東的公司。出口設備價值的低報，擴張了轉移到境外的非法價值。

在這種情況下，澳洲邊防署能夠使用自動與人工貿易資料差異分析技術，以更好地識別和評估可疑的貿易洗錢實例。從 A 司法管轄區出口的貨物申報應與相應的進口到 B 司法管轄區的申報相匹配（因為從理論上講，這批貨物是相同的）。在這種情況下，當它們無法匹配時，澳洲邊防署官員有理由相信，這些差異是開立錯誤發票貿易的一個指標，因此，可能是貿易洗錢。進一步的調查和與夥伴機關的合作得以將組織犯罪集團與交易聯繫起來。

協助貿易洗錢的代購業務

調查顯示，在代購業務中使用四個步驟方法來促進貿易洗錢。代購業務是指一個司法管轄區的人為另一個司法管轄區的消費者進行購買，而且通常是大規模的購買。

第一步：在澳洲以銷售非法商品（包括比特幣鑽石（BCDs））獲取資金。

第二步：非法獲取的資金由洗錢組織（MLO）" 匯集 "，並提供給多個代購協調人。洗錢組織用會利用加密通訊平臺向代購協調人提供指示。

第三步：代購協調人負責將資金分配給澳洲的代購消費者，以資助他們購買消費品。代購協調人還與相關法人實體合作，利用集中的資金資助其商業運營。

第四步：消費品被包裝並運往海外的相關代購協調人，然後在接收的司法管轄區銷售這些物品套利。

利用代購網路從事貿易洗錢的出口指標。

- 表現出的非法或不合規行為的主要指標包括：
- 代購者的購買資金來自協調人提供的現金池。
- 匯集的資金停留在正規銀行系統之外。
- 購物者以現金形式獲得活動報酬。
- 沒有法律文件來證明協調人和購物者之間的商業關係的性質。
- 設在澳洲的代購協調人和他們的海外同行之間做互相抵消安排被以代碼的形式記錄和／或沒有向政府官員申報。

孟加拉

兩家服裝公司 X 服裝有限公司和 Y 針織有限公司向商業法人實體 Z 有限公司出口價值 509 萬美元的貨物。共計 509 萬美元，透過四家銀行即 M、N、O 和 P 向商業法人實體 Z 有限公司開出 33 張出口匯票。四家銀行根據銷售合約內容以預付款方式簽發 33 張出口匯票（EXP）。然而，在 509 萬美元的出口收益中，有 468 萬美元沒有從商業法人實體 Z 有限公司匯出。

M 銀行針對 X 服裝有限公司提交的一份偽造合約發出一份轉開信用狀（BTB LC）。M 銀行簽發 2 份出口匯票，P 銀行針對合約簽發 19 份出口匯票，並將票據貼現。N 銀行開出 6 張出口匯票，O 銀行也以預付匯票的方式開出 6 張出口匯票。

透過 M、N 與 P 銀行簽發的信用狀出口的貨物（離岸價值 429,000 美元）被發現在進口商管轄的 L 港口公開拍賣。即便發現原始運輸文件係由 O 銀行保管，進口商公司 Z 有限公司仍以影印的文件放行 O 銀行 6 張出口匯票的貨物。

X 和 Y 公司都與商業法人實體 Z 有直接聯繫，因為 X 公司的總經理也是位於中東地區的商業法人實體 Z 的所有者。因此，發現 S 先生將貨物從他的孟加拉公司出口到他自己位於外國司法管轄區的公司，最終沒有將出口收益匯出，從而透過貿易從孟加拉將資金進行清洗。根據分析，一份帶有證明文件的情報報告被分送給海關情報和調查局、國家稅務局和孟加拉警方的刑事調查局（CID），以便根據 2012 年洗錢防制法（MLPA）的規定進行更進一步調查和採取必要的法律行動。

侵吞銀行資金

X 先生是進出口和供應商公司、名為 ABC 貿易公司的經營者，他違反 1947 年外匯管理法的規定，在國外建立業務。一項公開的調查顯示，ABC 貿易還有 20 家姐妹公司，其中 4 家公司（1.AB 有限公司，2.BC 有限公司，3.CD 有限公司和 4.DC 有限公司）正在境外開展貿易業務。

一份可疑交易報告以及媒體報導引起對 ABC 貿易公司所為出口的調查，並確定一份價值約為 5,000 萬美元的出口訂單，該訂單由四家外國銀行開出，並被送到一家名為 PQR 銀行（信用狀承兌行）的孟加拉銀行。這些信用狀是由四家銀行為三家進口公司 L 有限公司、M 有限公司和 N 有限公司開具，用於從孟加拉 ABC 貿易公司進口瓷磚。儘管包括信用狀承兌銀行 PQR 銀行分行經理在內的一個小組訪查 ABC 貿易公司的工廠，但他們沒有提供任何照會報告。這一空白讓人懷疑該出口公司是否有任何出口瓷磚的生產設施。

另一方面，對瓷磚進口公司的信用報告進行分析後發現，這三家進口公司的業務性質是皮革和羊毛製品。與他們各自的實收資本相比，大量進口不同種類的產品似乎很可疑。此外，還發現這三家進口公司的所有者是孟加拉公民 Y。

由於不相信其出口情形，金融情報中心進行進一步分析，發現所有四家信用狀開狀行都是空殼銀行。X 先生和 Y 先生與 PQR 銀行的高階管理人員合作，透過詐欺、偽造和高估出口匯票，成功地走私約 2,500 萬孟加拉塔卡（295,115 美元）。後來，銀行又允許出口商以出口押匯的名義再拿走 1,800 萬塔卡（212,486 美元）。如此一來，220 張出口匯票中只有 80 張被送回孟加拉，用以掩蓋非法業務。孟加拉金融情報中心分析認為，出口商和進口商與銀行高階官員合作，在國際貿易的偽裝下，將錢移轉到國外。

調查結果出來後，根據 2012 年洗錢防制法，將一份情報報告送交各執法機關，以便進一步調查和採取法律行動。

斐濟

規避和隱匿

F 公司在一份可疑交易報告中被舉報，因為它從斐濟向海外供應商支付預付款，並且沒有及時向其銀行出示進口報關紀錄。斐濟金融情報中心的分析顯示，資金從公司貸款銀行帳戶轉移到 F 公司的日常管理銀行帳戶。分析顯示，F 公司在 2016 年停止進口活動，並從 2015 年開始作為另一個法人實體 B 公司進行交易。斐濟金融情報中心進一步確認，B 公司被歸類為飯店經營者，服務營業稅（STT）和環境與氣候變遷稅（ECAL）也適用於 B 公司。一份案件分送報告被傳送給當地稅務部門，以供進一步調查。

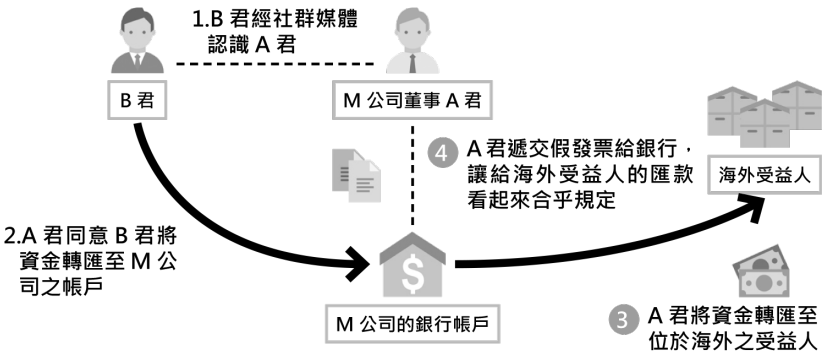
新加坡

M 公司的唯一董事 A 因偽造發票和洗錢罪被起訴。

根據新加坡金融情報中心—可疑交易報告辦公室（STRO）提供的情報，新加坡警察部隊（SPF）商業事務局（CAD）開始調查此事。2019 年初的某個時候，A 君透過社交媒體認識一位 B 君，後者自稱是一名投資者，熱衷於投資 A 君的公司。隨後在 2019 年 7 月，B 君尋求 A 君協助接收和轉移資金給海外受益人，A 君將因此獲得與存入金額相等的酬勞。A 君同意並允許為此目的使用 M 公司的銀行帳戶。

M 公司的銀行帳戶最終被發現收到約 225,000 新加坡幣（約 169,546 美元）的犯罪收益，這些收益來自位於 N 司法管轄區的一個所謂的商業電子郵件入侵詐欺受害者。根據銀行收到的與這筆錢的資金回收請求有關的通知，A 君向銀行提交一張假發票，以證明交易的合法性，並稱 M 公司已向一個客戶提供所述的服務，但其實其並未提供服務。他還向 B 君提供一份假發票的影本，為在進一步檢查時讓欺騙行為更為可信。

新加坡通知 N 司法管轄區當局，他們的公民是詐欺的受害者，這促成最終的資訊交換。N 司法管轄區和新加坡當局之間的成功合作對起訴由外國前置犯罪引起的洗錢罪很有價值。



5.5 地下通匯／替代性匯款服務／哈瓦拉

中國大陸

地下通匯案

D、W 和其他嫌疑人開發一網站和一智慧手機應用程序，為中國大陸和外國客戶銷售遊戲卡並提供充值服務。他們在第三方平臺上提供非法跨境貨幣兌換、支付和結算服務以獲取傭金。

公安機關和中國大陸人民銀行防制洗錢部門成立一個聯合專案小組進行調查。2020 年，公安機關對該犯罪網絡進行打擊，逮捕 50 多名嫌疑人。

中華臺北

J 先生是 S 集團公司（S Group）及其旗下子公司的負責人。2016 年 1 月至 2020 年 8 月間，J 先生以提供賭博場所或聚眾賭博為目的，網羅各成員成立 W 網路賭博集團公司（W 集團）並設立其分公司，以支援集團的硬體維護、客戶服務、資料庫管理、財務管理等基本功能。2016 年起，W 集團吸引到其他線上賭博網站所有者的興趣，他們希望使用 W 集團設計的平臺及其後臺管理服務。W 集團根據月收入與這些網站所有者分配利潤。據估計，截至 2019 年底，有超過 500 個網站所有者加入，而 W 集團獲得約新臺幣 595 億元（2,121,308,344 美元）的利潤。

後來發現大多數賭徒都來自 X 司法管轄區。這些賭徒將資金轉入 W 集團提供的人頭帳戶，然後 W 集團利用地下匯兌將這些資金轉移回中華臺北。當 J 先生和他的同夥收到上述以新臺幣計價賭博收益後，他們將這些收益藏在 S 集團旗下子公司的保險箱中，並將部分收益用於支付 S 集團的人員和設備費用。此外，為透過投資來清洗犯罪所得，J 先生和他的同夥成立一家投資公司 D，然後以 J 先生及其同夥的名義

購買上市公司的股票。此外，在集團成員的協助下，J 先生購買地塊，用以實現在 P、Q 和 R 司法管轄區的進一步投資專案，並在 S 司法管轄區收購一家上市公司 T。

地方檢察署於 2020 年 10 月以違反刑法和洗錢防制法的罪名起訴 J 先生及其同夥。

中國香港

案例一

在中國香港一家被指控的科技公司的銀行帳戶中發現頻繁的港幣和美元換匯交易，交易金額高達 16 億港幣（206,023,727 美元），並有臨時資金存放。這種交易模式讓人懷疑是未經許可的貨幣服務運營商的活動。警方的調查顯示，該公司確實是一家空殼公司，已採取行動將其從商工登記處註銷。警方的調查仍在進行中。

案例二

有超過 300,000 港幣（38,628 美元），主要來自於便利店的現金充值或透過電子錢包點對點資金轉移，被存入中國香港的一名家庭雇工及其雇主的儲值支付工具（SVF）帳戶內。這些資金隨後被存入該外籍家庭雇工名下的另一個儲值支付工具帳戶。調查顯示，該家庭雇工在未經同意的情況下使用其雇主的身分證註冊三個儲值支付工具帳戶，用於將資金匯往其母國。該家庭雇工被逮捕，並承認為其朋友匯錢並向他們收取匯款費用。該家庭雇工被指控犯有 " 詐騙 " 和 " 無證經營貨幣服務 "。

紐西蘭

紐西蘭境內替代性匯款網絡清洗非法毒品犯罪的收益

一個位於奧克蘭的外匯和匯款業務網絡被懷疑在知情的情況下為價值數百萬美元的非法毒品、詐欺和其他犯罪所得的流動提供服務。該網絡利用現金收款人從希望在國際上匯出資金的客戶那裡提取現金，並將資金存入年輕的第三人（主要是在紐西蘭持學生簽證的外國人）所持有的銀行帳戶，這些資金會被整合並用於完成那些想將資金從紐西蘭境外移入轉成紐西蘭幣的境外人士的匯款（為非正式價值轉移系統）。據信，該網絡收集者收集的現金中有很大一部分來自於嚴重的非法毒品犯罪，以及詐欺和其他侵犯財產罪。負責人和收款人都沒有對其客戶進行充分的（如果有的話）盡職調查。

巴基斯坦

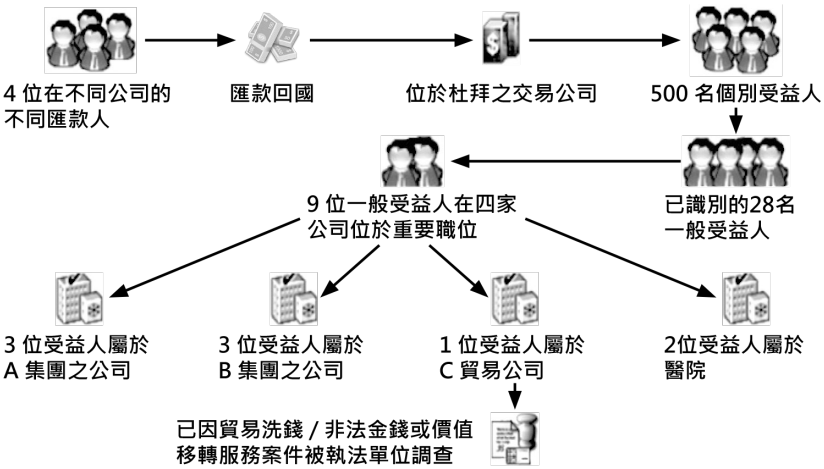
逃稅／非法貨幣價值轉移

報告指出一法人實體對四個不同的人提出可疑交易報告，因為他們從 D 司法管轄區向巴基斯坦的多人匯出大量資金。這些匯款人是居住在 D 司法管轄區的巴基斯坦國民，他們從事不同的職業／業務。資金是透過 D 司法管轄區的一家兌換公司匯出的，目的是匯款回國。如此大量的匯款僅以匯款回國為目的，引起人們的懷疑。

這四個人透過 1,300 筆交易向巴基斯坦的 500 多名個人匯出相當數量的資金。經過詳細分析，發現有超過 28 名共同受益人從一個以上的匯款人那裡收到資金。28 名受益人中，有 9 位屬於四個不同的事業團體，他們擔任著關鍵管理職位，並從一位以上的匯款人處收到匯款。這 9 名受益人在過去 3 個財政年度中繳納的個人和企業所得稅非常少。在分析過程中，還發現其中一名受益人經營的法人實體，即 XYZ 貿易公司，已經因貿易洗錢案件被執法機關調查。由於犯罪嫌疑人明顯參與利用非法金錢或價值移轉服務和國內匯款管道逃稅，因此將金融情報分享給各相關執法機關。

國際合作請求：

向 D 司法管轄區發出提供所有四個匯款人資訊的國際合作請求。D 司法管轄區的金融情報中心及時回應關於目標匯款人的寶貴金融資訊，金融情報中心向相關執法機關分享這些資訊，以便在其正在進行的調查中進行分析。



新加坡

W 君已因從事未經許可匯款業務，涉嫌接收犯罪所得並試圖將其匯往海外，而被依支付服務法起訴。

W 君是新加坡人，受雇於一家貨幣兌換公司，負責向公司介紹客戶。然而，儘管沒有執照，W 君也以自己的身分提供貨幣兌換和匯款服務。

W 君協助其客戶透過與海外聯繫人的淨結算來兌換或匯出資金。他從客戶處收取現金，並與海外聯繫人接洽，將等額的外幣從賭場帳戶轉移到客戶指定的目的地帳戶。在一個案例中，W 君依據其客戶 T 君指示，從第三方廠商收取現金，並協助 T 君將錢從新加坡匯到另一個司

法管轄區。最終發現 W 君的這些錢是透過假冒公署詐騙 3 個人的詐欺手段獲得的。

5.6 利用網路（進行加密、取得個人身分、國際銀行業務等）

中國香港

一名來自 X 司法管轄區的居民發現她的網上銀行帳戶被駭客攻擊，導致她損失約 1,600 萬港幣（2,060,186 美元），其中超過 500 萬港幣（643,808 美元）被匯入中國香港的三個銀行帳戶中，這 23 筆未經授權的轉帳被轉到全球其他銀行帳戶。這些資金被進一步轉移到五間香港空殼公司的銀行帳戶中，這些空殼公司由五個來自 Y 司法管轄區的當地人擔任董事。目前一名香港人被逮捕，銀行帳戶中的 350 萬港幣（450,660 美元）被凍結。調查還在進行中。

5.7 利用新支付方式／系統

中國香港

案例一

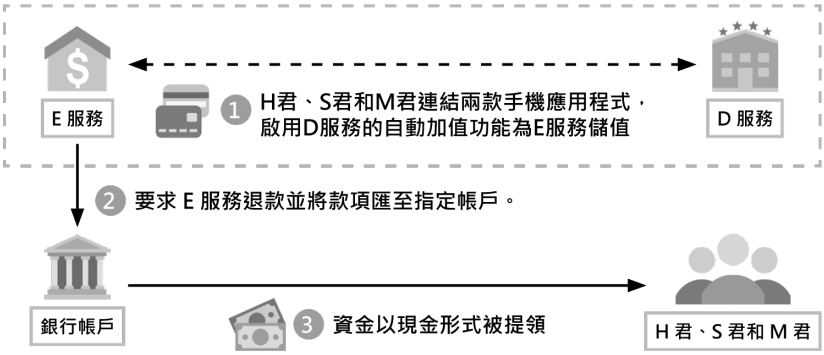
一博彩集團為接收和清洗非法賭博的收益，以其仲介和下屬的名義在中國香港設立一些儲值支付工具（SVF）帳戶。賭徒將錢轉給經紀人，以換取線上網站上的賭博遊戲積分，並透過仲介以儲值支付工具交易將積分兌換成法幣。該集團進一步將犯罪所得轉入下屬的儲值支付工具帳戶，並在貨幣兌換商處兌現。調查顯示，在兩年的時間裡，有超過 10,000 次交易，金額達 400 萬港幣（515,681 美元）。17 名儲值支付工具帳戶持有人因犯有賭博和洗錢罪而被捕。調查正在進行中。

案例二

透過對一系列線上投資詐騙和線上勒索案件的分析，發現受害者將錢財轉移到中國香港的虛擬銀行帳戶，這些帳戶是由一個博彩集團所雇用之下屬所開設的。該集團還被發現在一家貨幣服務運營商負責人的協助下清洗總額為 9,000 萬港幣（11,588,125 美元）的犯罪收益。38 人被逮捕。調查正在進行中。

新加坡

這是一起組織案件，警方調查洗錢罪和違反電腦不正使用法等罪行。2020 年，主謀 H 因洗錢罪和違反電腦不正使用法被判處 27 個月有期徒刑。S 君和 M 君被判處 24 個月的監督緩刑，並分別被罰款 5,000 新加坡幣（約 3,767 美元）。2019 年 1 月至 2 月期間，H 君、S 君和 M 君在手機應用程序 "E " 和 "D " 上創建帳戶，以方便進行支付服務詐欺。E 服務是一種儲值卡，可用於支付商品，並提供現金退款服務作為其功能之一。D 服務提供虛擬預付卡服務。在連接這兩個應用程序的帳戶後，犯罪者利用 D 服務向 E 服務自動充值的功能，當後者達到最低餘額時，犯罪者就會自動充值。在這種安排下，E 服務允許使用者用 " 充值 " 的餘額進行交易，而在稍後階段才與 D 服務結清債務。E 服務的使用者也能夠將其帳戶中的剩餘餘額 " 退還 " 到指定的銀行帳戶。因此，透過故意保持 D 服務的帳戶餘額不足，犯罪者能夠在 D 服務中產生越來越多的債務，而他們並不打算償還這些債務，同時收到退款到他們的個人帳戶，他們從自動取款機中提取現金。由於以上述方式使用 E 服務，H 君涉犯電腦不正使用法。在這個計畫中，H 君成功地在他的銀行帳戶中獲得總計約 36,000 新加坡幣（約 27,127 美元）的退款，直接使用他自己的銀行帳戶或在參與該計畫的其他各方，如 S 君和 M 君的協助下，H 君隨後將非法資金挪為己用。



5.8 稅務犯罪所得之洗錢行為

澳洲

2020 年 7 月，澳洲聯邦調查局決定進行博爾德隆行動，該行動逮捕一些澳洲國民，他們被指控參與一個大規模的稅務詐欺陰謀，涉及透過勞務雇傭行業內的法人實體架構挪用聯邦的實支實付預扣稅額（PAYGW）。這一罪行的收益隨後透過澳洲境內和境外的獨立法人實體進行洗錢。

被指控的詐欺行為涉及以下三個層次的架構。

第一層由兩家廣為人知的勞務公司組成，由值得信賴的專業人士指導。這些公司將服務外包給跨國建築法人實體（客戶），提供勞務雇傭和薪資服務。客戶透過發票資助安排，向第一層公司支付勞務雇傭服務費。收到這些款項後，第一層公司將薪資總額加上養老金轉入薪資服務公司（二級）。

第二層由一個或多個人事薪資委外服務公司組成，這些法人實體由犯罪集團指定的專業人頭董事組成。這些公司處理薪資單，將薪資和養老金轉移到指定雇員帳戶。財務分析顯示，集團利用其專業從這個層

級收到部分實支實付預扣稅額，作為他們服務的回報。剩餘的實支實付預扣稅額被澳洲稅務局扣留並直接轉給第三層公司。

第三層包括多個公司，由該集團經營和控制。假發票被用來掩蓋向這些法人實體轉移資金的實際性質（例如，將其定性為諮詢工作的付款或貸款）。然後，犯罪所得被轉移到更廣泛的犯罪集團成員的個人和法人帳戶中，為他們帶來財務效益。

斐濟

逃稅和財產來源不明

斐濟金融情報中心收到一份關於 A 君的可疑交易報告，稱其濫用個人帳戶進行商業相關交易，進行大額存款並可能存在逃稅行為。斐濟金融情報中心的檢查顯示，A 君是一家公司的董事，還擁有一個獨資企業。該公司和獨資企業的業務性質是提供貨運服務，據稱這兩個商業法人實體在過去四年中都出現累積虧損。然而，斐濟金融情報中心確定，儘管兩個法人實體都宣佈虧損，但 A 君在四年內從公司領取大筆 " 薪資 "，數額超過 450,000 美元（221,904 美元）。進一步分析還顯示，A 君在申報虧損後開立一筆 13 萬美元（64,105 美元）的定期存款。斐濟金融情報中心向當地稅務部門了提供一份案件分送報告。

中國香港

兩名 X 司法管轄區的居民在 X 司法管轄區被逮捕，原因是他們未經申報從中國香港向 X 司法管轄區偷運現金和奢侈品。他們還被發現出示偽造發票，聲稱增值稅已在 X 和 Y 司法管轄區結算，以達到逃稅之目的。香港警方的調查顯示，逃漏稅額後匯入中國香港的銀行帳戶，並扣留 1,100 萬港幣（1,416,315 美元）。調查正在進行中。

印尼

正如印尼金融交易報告和分析中心（PPATK）在 2020 年發表的關於 AML / CFT 的有效性指數的學術論文中所述，RAS 先生透過開具並非基於實際交易的稅務發票以及濫用或未經授權使用納稅人識別號或應稅企業家登記號，進行稅務相關前置犯罪的洗錢行為。這一犯罪行為造成的國家損失達 577 億印尼盾（39,903,910 美元）。RAS 先生在進行洗錢犯罪所得的態樣如下：

a. 處置：透過指示代理商或虛構發票的賣家及用戶，將至少 25,761,908,836 印尼盾（1,781,455 美元）的稅務犯罪收益存入 RAS 先生的帳戶和／或嫌疑人的代表公司。
b. 轉帳：透過犯罪嫌疑人在同一銀行或向另一銀行轉帳，以及從犯罪嫌疑人的公司在同一銀行或不同銀行轉帳，以及從犯罪嫌疑人／公司轉移屬於犯罪嫌疑人的第三方帳戶的資金，轉移稅務犯罪的收益。其中匯入匯款至少有 51,881,427,007 印尼盾（3,586,524 美元）和 1,465,648 美元的，匯出匯款至少有 14,002,394,683 印尼盾（968,290 美元）和 75,855 美元。
c. 花費：透過購買至少 15,200,000,000 印尼盾（1,050,728 美元）的地產和商辦等形式之資產來花費稅務犯罪的收益。

紐西蘭

清洗逃稅犯罪所得

一位餐館老闆在六年時間裡，透過他所擁有的 13 家連鎖餐館，隱匿超過主要為現金銷售的 650 萬紐西蘭幣（4,660,912 美元）。作為這一計畫的一部分，他的公司提交 115 份消費稅申報表，其中包含偽造或誤導性的銷售數字和超過 70 萬紐西蘭幣（501,953 美元）的消費稅稅收短報。

違法所得是透過不相干的活動進行洗錢的，這些活動的目的是為掩飾資金來源。這包括將一袋袋現金交給他的會計，然後匯到世界各地，並透過外匯交易和外匯買賣進行洗錢。

鑒於犯罪行為跨越數年，缺乏可靠的紀錄，以及犯罪者一直未能確保其餐館提交納稅申報，犯罪行為的確切規模和性質尚不清楚。該犯罪者承認 34 項逃稅指控和 9 項洗錢指控，並被判處三年半有期徒刑，罰款 50,000 紐西蘭幣（35,853 美元）。

新加坡

新加坡稅務局（IRAS）、新加坡警察部隊新加坡警察部隊商業事務局（CAD）和新加坡貪汙調查局（CPIB）對 A 君展開聯合調查。2020 年 6 月，外國公民 A 君因逃稅、貪汙和洗錢罪被定罪，並被判處 18 個月有期徒刑和 6 萬新加坡幣（約 45,212 美元）的稅務處罰。

A 君於 2013 年在負責批准退稅申請的新加坡海關官員 B 的協助下，利用電子旅遊退稅計畫（"eTRS"）進行至少六次詐欺性的旅遊退稅申請。調查顯示，A 君向 B 君行賄，以認可這些詐欺性索賠。隨後，A 君多次攜帶消費稅退稅款共計 27,895 新加坡幣（約 21,020 美元）的現金離開新加坡，這構成從新加坡轉移犯罪所得行為。

A 君在調查開始前就離開新加坡，但他在 2019 年 10 月再次進入新加坡時迅速被逮捕。B 君也因逃稅和貪汙罪被定罪和判刑，並不再受雇於新加坡海關。

5.9 不動產、包含不動產之經紀人所扮演之角色

中華臺北

2018 年 12 月，C 女士及其同夥偽造能夠借用 W 先生名義進行不動產登記的合約，還未經 W 先生同意，擅自刻製 W 先生的印章。合約記載，C 女士向 X 先生購買 A 地塊，並以 W 先生的名義進行登記。

根據這份合約，C 女士可以在任何時候要求 W 先生將土地歸還給她。本著詐騙其他出資人的目的，C 女士於是設計一個詐騙方案：她先是指責 W 先生在她正式提出法律要求後不歸還 A 地，然後又向法院提出民事訴訟調解申請。2019 年 1 月，C 女士的同夥偽造 W 先生的身分，委託律師與 C 女士達成協議，C 女士隨即取得 A 地的合法所有權。C 女士隨後與 L 女士達成協議，由 C 女士提供 A 地，並以最高額度抵押貸款的方式向出資方抵押。C 女士即雇傭 L 女士為仲介，招攬可以提供資金援助的人。

為隱匿和轉移犯罪所得，C 女士在 E 銀行和 F 銀行開設個人帳戶，並在 G 銀行開設銀行帳戶。在收到上述出資者的匯款後，C 女士多次到這些銀行提取小額現金。此外，她還要求上述銀行開出本票，隨後借用他人的銀行帳戶來兌現這些支票。

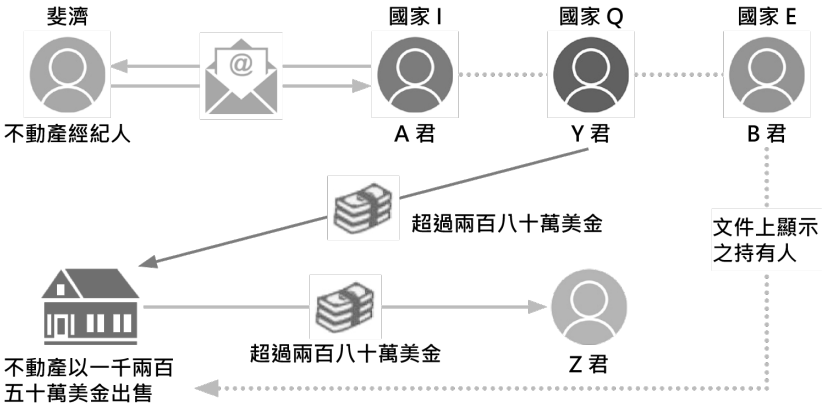
經過調查，該案於 2019 年 8 月依違反刑法和洗錢防制法移送地方檢察署。

斐濟

透過不動產交易洗錢者

A 君、B 君、Y 君和 Z 君是外國國民，在一件申報給斐濟金融情報中心可疑交易報告中被舉報，因為他們可能涉及一起超過 280 萬斐濟元（1,380,713 美元）的不動產交易洗錢案件。2019 年 12 月，A 君試圖

以 1,250 萬斐濟元（6,163,944 美元）的價格購買一處高端豪華房產。A 君和另一個身分不明的人就房產交易乙事與不動產仲介公司會面。2020 年 1 月，A 君透過 Q 司法管轄區的 Y 君安排資金，Y 君將 280 多萬斐濟元直接匯入不動產機關的信託帳戶作為押金。A 君表示，B 君是他在 E 司法管轄區的商業夥伴，他將在買賣協議中被列為房產所有人。當 A 君提出的 1,000 萬斐濟元（4,931,206 美元）的報價未被房產供應商接受時，他指示不動產仲介公司將訂金退給另一個人，即 Q 司法管轄區的 Z 君。 斐濟金融情報中心的分析顯示，A 君是唯一透過電子郵件和即時通訊應用程序與不動產仲介公司溝通的一方，其中不包括B君、Y君和Z君，看來A君是控制不動產交易的主要方。有趣的是，A 君、B 君和 Y 君從未到過斐濟，而且人們注意到 Y 君和 Z 君的出生日期相同。經向國內和國際執法機關進一步查證發現，A 君據稱與一個有組織的犯罪集團合作，參與 Y 司法管轄區的非法毒品進口，B 君和 Z 君是 Q 司法管轄區的國民，透過 E 司法管轄區的政府發展支持計畫獲得 E 司法管轄區的公民身分。此外，已確定 B 君是 Q 司法管轄區的紅色通緝令逃犯，他在斐濟使用假身分證件。B 君於 2020 年 1 月被驅逐到 Q 司法管轄區。



中國香港

一犯罪集團的成員在中國香港購買八個豪華不動產，並向銀行申請抵押貸款。調查顯示，申請抵押貸款中提出的收入被證明是虛構的，是該集團人為編造的。九名集團成員被逮捕，1,000 萬港幣（1,287,484 美元）的犯罪所得被暫時凍結。調查仍在進行中。

5.10 寶石與貴金屬交易

澳洲

2020 年 10 月，美國外國資產控制辦公室（OFAC）將一名位於澳洲的與基地組織有關的協助者 A 列入名單，因為他曾實質性地協助、贊助或為基地組織提供財務、物資或技術支援，或向其提供物品或服務。

A 君在多個司法管轄區進行金融交易，並參與寶石交易，這使他有能力為基地組織的利益在國際上轉移資金。A 君在世界各地開展業務。

中國香港

一人和兩個同夥在中國香港的一家銀樓用 6,000 萬港幣（7,724,993 美元）現金購買 3,000 兩[32] 的金條。這三人被逮捕，調查顯示後他們被雇來從貨幣服務運營商處收取現金用於購買黃金並交付他人。進一步調查顯示，這些錢是從 X 司法管轄區匯出的，黃金被交付給中國香港的一個集團。隨後，三名集團成員被逮捕，共緝獲 600 根五兩金條、現金及珠寶，總金額為 7,800 萬港幣（10,042,222 美元）。調查目前仍在進行。

---

32 中國大陸的一種計量單位。一兩被定義為 1+1 3 盎司，近似於 37.7994 克。

新加坡

2020 年 3 月，三個寶石和貴金屬經銷商（PSMDs）P 公司、G 公司及 T 君在法庭上被指控違反貪汙、販毒和其他重大犯罪（利益沒收）法（CDSA）第 65A 章的罪行。這與一個犯罪集團在 2019 年對一個公部門機關實施的一系列詐欺行為有關，這些詐欺行為導致總損失達 4,000 萬新加坡幣（約 3,000 萬美金）。特別是，該集團的兩名成員被發現使用犯罪所得，以現金形式從這三家經銷商購買價值 60 萬新加坡幣（約 452,123 美元）的珠寶和金條。這兩名集團成員已被指控犯有洗錢罪等罪行。在新加坡，從事現金交易超過 20,000 新加坡幣（約 15,070 美元）的寶石和貴金屬經銷商有義務在 15 個工作日內向可疑交易報告官提交大額交易報告（CTR）。本案中的三家經銷商沒有對上述購買行為進行申報。此外，T 君也沒有執行必要的客戶盡職調查，根據貪汙、販毒和其他重大犯罪（利益沒收）法，這是一項應受懲罰的罪行。在 2020 年 8 月至 10 月期間，P 公司和 G 公司以及 T 個人被判處 9,000 新加坡幣（約 6,781 美元）至 40,000 新加坡幣（約 30,141 美元）的罰金。

5.11 人口販運與人口走私相關之洗錢與資恐

中國香港

香港警方瓦解一人口走私集團，該集團安排非法移民從 X 司法管轄區透過中國香港進入其他司法管轄區，並逮捕主謀和三名活躍的集團成員。調查顯示，約 340 萬港幣（437,766 美元）的可疑犯罪所得是透過主謀在中國香港的兩個個人銀行帳戶進行清洗。該集團主謀被以洗錢定罪，並被判處 3 年有期徒刑，沒收金額總計為 270,000 港幣（34,764 美元）。

5.12 利用人頭、信託、家庭成員或第三方等

中國香港

案例一

對一名在中國香港被捕的毒販及其親屬所擁有個人銀行帳戶之調查顯示，該毒販一直在利用他自己和母親的銀行帳戶，用以清洗超過 700 萬港幣（901,293 美元）的犯罪收益。該毒販被指控犯有洗錢罪，法院審理程序正在進行中。

案例二

香港、X 司法管轄區和 Y 司法管轄區開展一次聯合行動，打擊跨司法管轄區的販毒活動，該集團的主謀安排漁船將危險毒品從 X 司法管轄區運往其他司法管轄區，並與 Y 司法管轄區的同夥勾結，採購船隻和招募船員進行運輸。調查顯示，主謀和他的兩名家庭成員利用在中國香港的 21 個銀行帳戶清洗 1.13 億港幣（14,548,025 美元）的毒品收益。其中一名家庭成員被以 11 項洗錢罪定罪，並被判處 3 年有期徒刑。其銀行帳戶中剩餘的 4200 萬港幣（5,407,255 美元）被沒收。

印尼

NL 先生是 XYZ 金融信貸機構（FCI）的總裁，該機構企圖在沒有監理機關的營業許可下向大眾招攬資金，然後以 10% 的利率將資金貸給大眾。在 5 年的運作中，該機構成功地從 16,155 名客戶那裡籌集到 4,130 億印尼盾（28,533,176 美元）的資金。然而，另一方面，XYZ 金融信貸機構實際上並沒有從印尼銀行的管理層獲得營業執照。

對於已經收取的每一筆資金，XYZ 金融信貸機構帳戶中約 70 億印尼盾（483,791 美元）至 100 億印尼盾（691,120 美元）的金額，將由 NL 先生轉入個人帳戶，然後再轉回許多帳戶，包括屬於 NL 先生、NL 先

生的妻子、NL 先生的孩子和雇員的帳戶。此外，NL 先生還用這筆錢支付土地款、建築、工程款、汽車和三份保險，每份價值 5 億印尼盾（34,555 美元）的資產。由於這一行為，NL 先生已被判處四年有期徒刑，並被罰款 10 億印尼盾（69,084 美元）。

中國澳門

犯罪嫌疑人 B 和犯罪嫌疑人 C 是一對夫婦，據稱挪用 N 司法管轄區的 80 多萬美元。為掩飾和隱匿資金的非法來源，犯罪嫌疑人 B 和犯罪嫌疑人 C 將其在 N 司法管轄區的存款匯至中國澳門，並通知犯罪嫌疑人 D 和犯罪嫌疑人 E（即犯罪嫌疑人 C 的父母）來收取這筆錢。犯罪嫌疑人 D 和犯罪嫌疑人 E 多次在銀行接收匯款後，申請定期存款、購買保險、投資股票，並在中國澳門從事不動產交易，透過將犯罪所得轉化為其他形式的資產，轉移和隱匿犯罪所得。

犯罪嫌疑人 B 和犯罪嫌疑人 C 被以公款罪定罪，並在之後被 N 司法管轄區法院判刑。2020 年，犯罪嫌疑人 B、犯罪嫌疑人 C、犯罪嫌疑人 D 和犯罪嫌疑人 E 被檢察院以洗錢罪起訴。N 司法管轄區在調查犯罪嫌疑人 B 和犯罪嫌疑人 C 的貪汙案時，向中國澳門發出刑事司法互助請求，要求協助調查以及取證。

巴基斯坦

洗錢／逃稅

2019 年至 2020 年期間，兩個不同的申報機構針對一個家庭的多個成員及其雇員申報許多可疑交易報告，理由是他們持有多個銀行帳戶，並將操作這些帳戶的任務交給兩個彼此為父子關係之家庭成員 A 先生和 B 先生。

在分析報告機構所提出關於該家族成員及其雇員的多份可疑交易報告後，發現他們都在該司法管轄區大城市之一的一個著名市場從事木材生意。此外，還發現在經營獨資企業的同時，他們還在一些私營有限公司擔任董事職務，並持有個人、獨資企業和公司帳戶。在所有銀行帳戶的開戶表格中都提供相同的企業地址和聯繫電話。對這些帳戶的報表進行分析後發現，大量資金是透過家庭成員及其雇員在不同銀行開設的各種帳戶流轉的。在帳戶中收到資金後，立即被轉移到 A 先生和 B 先生有效控制的其他家庭成員的帳戶中。位於該司法管轄區偏遠地區、似乎參與哈瓦拉／布隆迪活動的交易方也透過轉帳將資金存入。除可疑交易報告中報告的 72 個帳戶外，在關於同一家庭成員的交易報告中還發現 37 個帳戶，其中經營這些帳戶的任務又是由 A 先生和 B 先生兩人持有。根據該分析，將該金融情報分享給一個執法機關，以進一步調查洗錢和逃稅的問題。

菲律賓

X 司法管轄區的國民利用並吸引菲律賓人註冊獨資企業，並為上述企業開設銀行帳戶。菲律賓人只是文件上所稱之所有者，而 X 司法管轄區的國民則實際完全控制企業和帳戶。

Z 君（X 司法管轄區國民）將數百萬菲律賓披索存入 D 君（X 司法管轄區國民）和 F 君（菲律賓人）的帳戶。收款人申報 H 公司（在菲律賓註冊的企業）為資金來源。

防制洗錢委員會（AMLC）與上述執法機關合作，得以追蹤這些帳戶，並凍結估計價值為 7,800 萬菲律賓披索（1,624,174 美元）的資金。

5.13 博奕活動（賭馬、網路博奕等）

中華臺北

刑事警察局收到有關詐欺集團 T 的資訊，該集團專門在 X 司法管轄區設立人頭帳戶，並將這些帳戶提供給其他人用於非法用途。經過調查，發現該集團的主要嫌疑人 A 招募不特定的人在 X 司法管轄區的銀行開設金融帳戶，並利用這些帳戶透過非法線上遊戲運營商進行洗錢。

經確定，所有被吸收的帳戶都是由在同一棟樓裡工作的同一組人所收集及使用，亦即該處為一洗錢水房。據估計，每天的洗錢流量約為 X 司法管轄區法定貨幣 1,000 萬（1,544,823 美元）。2020 年 6 月 8 日，刑事警察局搜索該建築等多個地點，隨後查獲 19 台電腦、87 支手機、57 張 SIM 卡、23 份合約、323 個來自 X 司法管轄區銀行的 USB 帳戶登入鑰匙、140 張銀聯卡和其他洗錢物證，並逮捕 A 君和另外 8 名在上述洗錢中心工作的成員。

經過深入調查，刑事警察局進一步發現，在水房工作的成員都是 Y 公司的員工。2020 年 6 月 18 日，刑事警察局搜索 Y 公司總部，發現 Y 公司經營之另外三個網路博弈平臺。刑事警察局立即扣押 10 台電腦、16 支手機和 7 個銀聯帳戶，並逮捕該公司負責人 B 及其同夥。

中國香港

案例一

中國香港和 X 司法管轄區聯合瓦解一個跨境博彩集團，在中國香港有 23 人因博彩和洗錢被捕，在 X 司法管轄區有 33 人被同步逮捕。調查顯示，超過 2.16 億港幣（27,806,578 美元）的球賽賭博所得款項經由四個核心集團成員名下的 18 個帳戶進行洗錢。其中三人被以洗錢和賭博罪定罪，並被判處 24 至 57 個月監禁，200 萬港幣（257,467 美元）

被沒收。對最後一名主謀的訴訟正在進行中，他面臨洗錢之指控，在中國香港和 Y 司法管轄區價值 2,000 萬港幣（2,574,701 美元）的資產已被凍結。

案例二

一項財務調查顯示，A 先生利用他的個人銀行帳戶和他在中國香港的家庭成員及合夥人的帳戶，在五年內清洗約 1 億港幣（12,873,244 美元）的犯罪收益。A 先生的住所被搜索，還查獲投注單及語音投注紀錄等博彩用具。經過調查，A 先生、他的家庭成員和同夥被指控犯有參與賭博和洗錢罪並被定罪。沒收令要求其中三名被定罪的人向政府支付約 400 萬港幣（514,928 美元）。

蒙古

一家銀行提交一份可疑交易報告，懷疑客戶 B 帳戶的交易金額、數量和頻率與客戶的工作和業務不相符。他可能參與經營非法線上賭博。

蒙古金融情報中心對這個可疑交易報告進行分析，從申報機構那裡收集更多的資訊，發現 B 君利用他的兩個帳戶收取賭資，並將贏來的錢分發給玩家。在分析期間，B 君透過自動櫃員機和國內銀行轉帳，從大約 500 次交易中收到總額 10 億圖格里克（約 35 萬美元）轉入其第一個帳戶。此外，他還從五個不同的人那裡收到 57 億圖格里克（約 200 萬美元）進入同一個帳戶，這些交易的附言中含有相同的詞。據推測，這五個人是 B 君的同夥。收到資金後，他從第一個帳戶轉一大筆錢到第二個帳戶。然後，他透過 70,000 筆交易的附言中有隨機字母與數字，從第二個帳戶向 6,000 名不同的個人轉移和分配小額資金。此外，上述大部分交易是在淩晨 1 點至 5 點進行的，間隔時間為 1-2 分鐘。

基於此分析結果，蒙古金融情報局將此案轉交給執法機關作進一步調查。

在調查過程中，確定這些犯罪嫌疑人經營非法線上賭博，對賭博所得進行洗錢，並購買價值 40-50 億圖格里克（1,404,201 美元至 1,755,251 美元）的動產和不動產。此案的調查仍在進行中。

5.14 購置高價資產（藝術品、骨董、賽馬、豪車等）

紐西蘭

涉及數十億美元之國際詐騙，其收益被以紐西蘭境外信託的名義購買藝術品、財產和車輛

一個海外犯罪者網絡，從一家（非紐西蘭）政府擁有的投資公司挪用數十億美元，並透過一個複雜的信託及公司架構之網絡清洗資金。該網絡的負責人之一（個人 A）建立兩個紐西蘭境外信託基金，指定其本人及其親密家人為受益人，由紐西蘭信託或公司服務提供商建立的紐西蘭有限責任公司作為信託基金的受託人。這些信託基金在幾個境外司法管轄區擁有資產，包括一位國際知名藝術家的幾件藝術品、一艘豪華遊艇和數棟豪華房地產。所有權架構涉及創建擁有這些資產的特殊目的（非紐西蘭）公司；這些公司的股份由另一個（非紐西蘭）司法管轄區的控股公司擁有，這些公司的股份又由紐西蘭境外信託基金擁有，其受益人是個人 A 及其家庭成員。

5.15 利用經紀人投資資本市場

中華臺北

S 先生是 T 公司的負責人，而 Z 女士是 T 公司的會計及出納。在 2016 年至 2019 年期間，Z 女士為侵占公司財產供自己使用，拿著 S 先生在

A 銀行開設帳戶的存摺和他的印章（S 先生只提供給 T 公司使用），共提取新臺幣 7,615,420 元（272,306 美元）。

為隱匿這些犯罪所得，在 2018 年至 2019 年期間，Z 女士從 S 先生的上述帳戶中分三次提領合計新臺幣 108 萬元（38,621 美元），隨後將這筆錢轉入她兒子的交割帳戶，用於購買 C 公司的股票。

經法務部調查局的調查，該案件於 2020 年 10 月以違反刑法和洗錢防制法的罪名移送地方檢察署。

中國香港

在中國香港，兩個大麻植物種植園被搜索，導致包括主謀 X 先生及其家庭成員 Y 女士在內的四人被捕。根據 X 先生的 11 個銀行和證券帳戶的紀錄，在 3,500 次交易中，存款總額超過 700 萬港幣（901,142 美元），其中一半以上是由來源不明的現金存入，其餘部分則是由不同的交易方匯出。Y 女士被發現控制超過 15 個銀行和證券帳戶，在 7,500 次交易中存款總額達 1,500 萬港幣（1,931,008 美元），這與她的財務背景不相符。X 先生和另外兩人被定罪並被判處 5 年 10 個月的有期徒刑，超過 500 萬港幣（643,657 美元）被沒收。Y 女士被指控洗錢，價值超過 700 萬港幣（901,142 美元）的資產被凍結。法庭訴訟正在進行中。

印尼

操縱市場

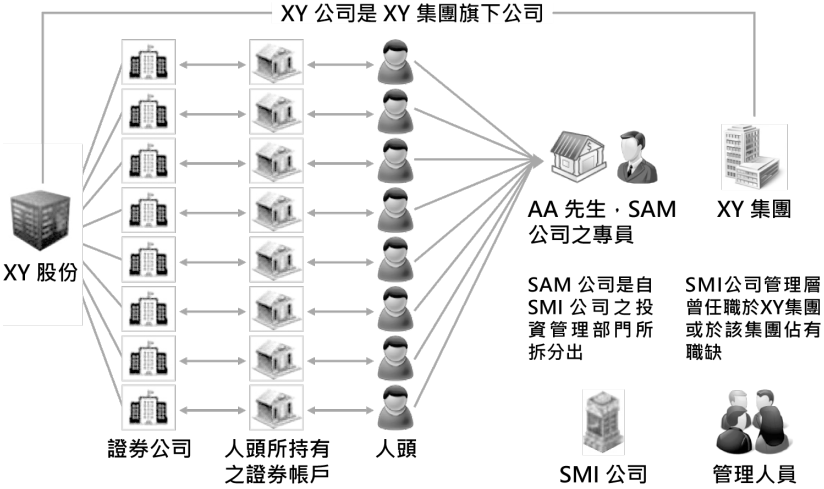
AA 先生是 A 公司的專員，該公司自 SMI 公司的投資經理公司部門拆分，因而進入投資管理部門。A 公司本身擁有監理機關核發的投資經理執照。

AA 先生利用當事人作為人頭，經由 13 家不同的證券公司進行股票交易。根據客戶的人頭證券帳戶資訊，帳戶是於同一時期在同一家銀行（即 XX 銀行）進行開戶或關戶。

這些被利用的人頭的工作類型差異很大，包括私企雇員和自營職業者，他們的收入和年齡概況各不相同，甚至有人每月收入低於 200 萬印尼盾（138 美元）。

其後，AA 先生轉帳到人頭帳戶，然後全部用來購買一種相同的股票，即 XY 股。2016 年間，AA 先生的帳戶總交易量為 7 兆印尼盾（484,940,661 美元）。

根據金融交易之分析，有從人頭帳戶流向 AA 先生帳戶的迴轉交易形式的金流。於是對 AA 先生透過人頭戶的交易進行比較分析。當 XY 股票價值達到最高值時，人頭的總交易量達到 XY 股票市場交易量的 40% 以上。這顯示 AA 先生透過人頭進行的 XY 股票買賣交易的重要性。此外，AA 先生送出給人頭戶的資金只用於 XY 股票的交易。據稱，AA 先生與 XY 集團之間存在關聯關係，因為 AA 先生在 XY 集團工作，而且 AA 先生的帳戶中存在來自 XY 集團幾個子公司的資金流動。



RDN：證券帳戶　　PT：公司

5.16 混合式洗錢（商業投資）

印尼

詐欺和非法銀行

B 合作社是一個在印尼從事運輸和其他業務的合作社。其管理層由 AND 先生擔任負責人，CEK 先生擔任秘書，JUL 先生和 YUL 先生擔任行政人員。同時，同樣由 AND 先生領導的 A 公司面臨著財務責任，阻礙 AND 先生將其公司上市。據稱，A 公司受到 Bapepam（印尼證券交易委員會）條例的限制，當公司對超過 50 個當事人負有債務，就不能上市。

A 公司與其投資人（稱為合夥人）之間有一個合夥協議。但在合夥人不知情的情況下，AND 先生與 CEK 先生達成協議，將合夥企業轉讓給 B 合作社。該合夥企業還將 A 公司的債務轉移給 B 合作社，以便為 A 公司在證券交易所上市鋪路。然而，B 合作社並沒有獲得向公眾募集資金的許可。

A 公司從 2007 年至 2014 年收取的合夥人資金達 4,779,976,704,333 印尼盾（333,823,791 美元），其中約有 3,264,688,621,100 印尼盾（227,924,779 美元）無法返還其合夥人。

被告將社區／合夥人的投資款存入 B 合作社名下的帳戶，然後透過支票和劃撥匯款形式提取現金。這些資金透過銀行工具，以支票、劃撥匯款和即時總額清算的方式被放回被告和被告擁有的公司的個人帳戶，金額約為 319,456,000,000 印尼盾（22,309,663 美元）。這些資金被用於支付員工薪資、支付汽車牌照稅、購買土地和建築資產以及借給 A 公司，金額為 200,000,000,000 印尼盾（13,967,582 美元）。

5.17 利用空殼公司／企業

中國香港

一名毒販在 X 司法管轄區被捕，調查顯示該毒販透過中國香港兩家空殼公司的四個公司帳戶洗錢 5.4 億港幣（69,524,478 美元），其中 1.38 億港幣（17,767,240 美元）透過 X 司法管轄區的匯款業務公司匯出。這兩家公司的董事被以共謀洗錢罪定罪，並被判處 38 個月有期徒刑。

紐西蘭

在紐西蘭註冊的空殼公司被用作國際洗錢網絡的一部分

在紐西蘭設立的一家有限責任公司（A 公司）被用於在境外司法管轄區（A 司法管轄區）開設銀行帳戶。資金從 B 公司在另一個境外司法管轄區（B 司法管轄區）的帳戶匯入 A 公司在 A 司法管轄區的帳戶。海外調查顯示，A 公司很可能被利用作一個更廣泛的公司網絡的一部分，將非法資金從 B 司法管轄區轉移到 A 司法管轄區。

A 公司被列為製造商或批發商，但實際上它在紐西蘭或境外司法管轄區都沒有實質性的業務活動。以 A 公司名義支付的款項伴隨著偽造發票，其中提到紡織產品，並在電子文件上添加偽造的標識、印花和簽名。境外機關的進一步調查顯示，實際上沒有貨物被運走，它們是幽靈貨物。A 公司是由一家紐西蘭信託或公司服務提供商註冊成立的，其網站宣傳說：離岸資產保護和稅收最小化 ..... 根據要求提供專業的董事服務。它在紐西蘭沒有實質營運痕跡，沒有紐西蘭銀行帳戶，董事和股東都是由紐西蘭信託或公司服務提供商指定的人頭。

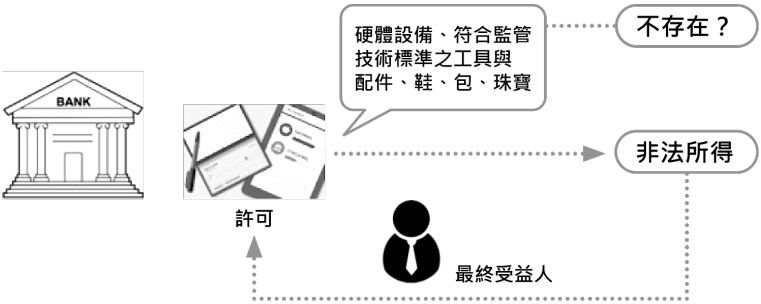
菲律賓

利用商業機構為毒品販運提供便利

2020 年 8 月，防制洗錢委員會公布一份關於外國國民利用菲律賓國民及其企業從事非法毒品活動的態樣。

已確定的操作方式涉及菲律賓國民（前台），他們代表某些外國國民向貿易與工業部（DTI）註冊獨資零售企業，而這些外國國民是上述企業的實質及最終受益人（UBO）。上述企業的經營也同樣沒有依據法律對於外國業主的資本額的規定。這些公司完全由這些外國公民控制和經營。

在貿易和工業部註冊後，前往銀行（主要是商業銀行和綜合銀行）持新獲得的貿易和工業部註冊許可證，以新註冊企業的名義開設帳戶。



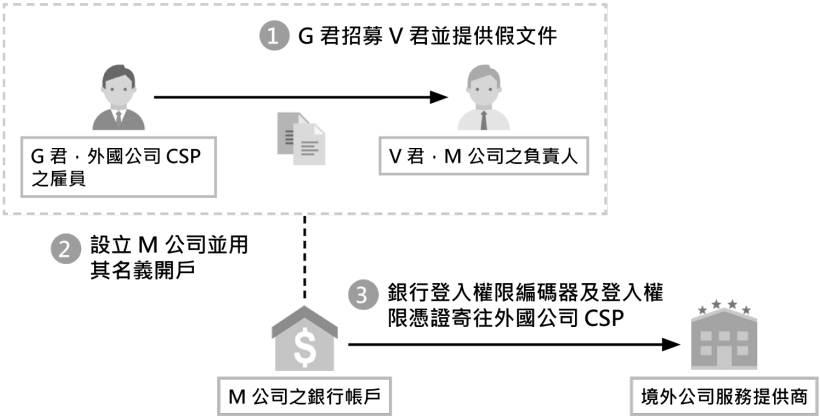
然後，上述銀行帳戶將由外國國民，即最終受益人來管理和控制，目的是接收犯罪所得的資金。此外，在這種作案手法中發現，大多數註冊的獨資企業都是空殼公司或不存在的公司。

新加坡

案例 1

G 君於 2020 年 1 月因洗錢罪被判處 10 個月有期徒刑。同案被告人 V 君因使用偽造文件誘使一家本地銀行批准其公司銀行帳戶申請而被判處 5 個月有期徒刑。G 君為一家海外企業服務提供商工作，他的職責之一包括招募個人成為公司的掛名人頭董事，並以公司的名義設立公司銀行帳戶。這些被提名的董事隨後將放棄對公司及其銀行帳戶的控制權，以獲取費用。G 君知道他的雇主從事銷售空殼公司及其公司銀行帳戶的業務，通常是為犯罪者洗錢。在這一特定案件中，G 君招募 V 君，兩人於 2018 年 12 月前往新加坡，成立 M 公司並開設公司銀行帳戶。據此，G 君交給 V 君一份假文件，將後者描繪成一個成功的商人，向銀行保證該公司是由財務狀況良好的人經營。銀行帳戶開立後，網路銀行登入權限編碼器和網路登錄憑證被快遞到海外公司服務提供商處。

2019 年 4 月，商業事務部接到舉報，M 公司的銀行帳戶收到 5 萬美元的犯罪所得。商業事務部迅速確定涉案人員的身分，並在 G 君和 V 君進入新加坡時將其逮捕。商業事務部在調查中追回約 7,600 美元的犯罪所得。



案例二

2020 年 8 月，B 君在法庭上被判犯有公司法第 157（1）條規定的罪行，因為他作為一名董事沒有盡到合理的注意義務。他被判處 5,000 新加坡幣（3,758 美元）的罰款，並被取消一年的董事資格。在判刑時還考慮到公司法所規定的另外兩項指控。2012 年至 2015 年期間，新加坡警方的商業事務部（CAD）對六家本地公司進行洗錢調查，這些公司涉嫌從三個不同洲的司法管轄區接收詐欺性資金，金額約為 225 萬美元。所犯的上游罪行包括鍋爐房投資詐騙伎倆和商務電子郵件和解詐欺。調查顯示，所有六家公司在新加坡都沒有合法的商業運作，實際上是空殼公司。所有這些公司都是在同一個公司服務提供商 B 君的協助下成立的，B 君還任命自己為每家公司的提名董事，以滿足公司法

第 145（1）條規定的當地居民董事的法律要求。然而，B 君幾乎沒有花時間去瞭解這些公司的事務，包括對這些公司的銀行帳戶幾乎沒有監督。商業事務部設法扣押約 45,000 新幣（約 33,909 美元），並將其返還給受害者，儘管大部分被指控的犯罪所得在調查前已迅速被隨意花用。

5.18 環保犯罪相關（盜伐林木、採礦、野生動物販運等）

澳洲

澳洲展開聯合金融調查，搗毀爬蟲類寵物走私網絡

2016 年，澳洲邊防署（ABF）截獲幾個含有本地野生動物的出境國際包裹。連同幾個被截獲的含有外來野生動物的入境包裹，它們與一個澳洲利害相關人（POI）有關。為進一步調查，環境和能源部（DoEE）與澳洲邊防署進行聯合調查，並與澳洲邊防署、金融情報中心（AUSTRAC）、農業和水資源部以及各州和地區的野生動物管理局進行大量協調合作。

澳洲聯邦調查局證實，該利害相關人協調一個出口澳洲本土爬蟲類寵物的非法野生動物貿易犯罪網絡。調查涉及與 X 司法管轄區的警察當局分享有關司法管轄區 X 國籍的利害相關人活動的情報。對利害相關人的住所進行搜索，最終將其逮捕。在搜索過程中，在該處發現兩條緬甸蟒，以及大約 30,000 美元的現金。

金融情報有助於識別更廣泛之犯罪網絡。從金融情報中心獲得的銀行交易資訊將主要的利害相關人與一些 X 司法管轄區野生動物販運者直接聯繫起來，同時支援刑事調查。同樣，金融情報中心的分析顯示，同樣的 X 司法管轄區法人實體一直在向另一個澳洲爬蟲類寵物交易商發送資金。

使用的付款方式有：現金、銀行轉帳、透過大型金錢或價值轉移服務（MVTS）供應商付款、實物交易（同等價值的野生動物交換），以及與野生動物販運者的同夥和家庭成員交易。資金流量難以量化；但是，估計顯示，主要的利害相關人從截獲的來自 Y 司法管轄區的魚類、魟魚、爬蟲類寵物和海龜進口中獲得 50 多萬澳幣（389,014 美元）。該利害相關人被判定犯有六項指控，包括：試圖出口受管制的本地標本（1999 年環境保護和生物多樣性保育法（EPBC 法）303DD）；進口受管制的活體標本（環境保護和生物多樣性保育法 303EK）；擁有非法進口的標本（EPBC 法 303GN）；以及洗錢（1995 年刑法）。此人被判處四年有期徒刑，兩年半不得假釋。在調查期間，當局沒收約 30,000 美元的現金作為犯罪所得，以及 340,000 美元（野生動物的估計價值）。

中國大陸

非法販運野生動物案件

2020 年，中國大陸海關查獲 110 萬條透過偽造申報單走私出口的日本鰻魚苗。由於日本鰻魚苗無法進行人工繁殖，是受中國大陸野生動物保護法律法規保護的野生動物。透過與中國大陸防制洗錢監測分析中心的合作，中國大陸海關迅速查明關聯至賣家、清關服務商和海外收貨人的資金鏈，並確定集團成員及其交易模式。執法機關打擊鰻魚苗走私者，並逮捕 16 名嫌疑人。涉案資金價值達 1.5 億元人民幣（23,213,713 美元），其中 3,000 多萬元人民幣（4,642,859 美元）被凍結。

中國香港

對一個於 X 司法管轄區從事跨境博彩和非法野生動物交易活動之犯罪集團的調查顯示，主謀利用其公司和同夥在中國香港的銀行帳戶洗錢超過 5.5 億港幣（70,814,566 美元）並將犯罪所得用於購買債券、證券和不動產。在中國香港的兩名同夥被逮捕，超過 2.6 億港幣（33,475,035 美元）被凍結。目前調查正在進行中。

根據環境和林業部、印尼海軍、印尼刑事警察局（刑事調查部門）、海關和稅務局組成的聯合小組開展之林產品流通行動的調查結果，港口負責人已經檢查並保護 199 個裝有涉嫌非法採伐的加工木材的集裝箱。

印尼

此案涉及到沒有合法林產品證書的林產品運輸。根據文件核對和檢查結果，只發現 12 份加工林產品木材合法性證書形式的運送單證，共計 57 個集裝箱為 A 公司所有。B 公司所有的 27 個集裝箱被沒收，因為這些集裝箱是使用該公司的木材運輸單據形式的文件運輸的，與該運輸產品並不相符。非法木材產品是在東爪哇泗水 Teluk Lamong 碼頭有限公司港口使用 C 公司擁有的船隻運輸的。D 公司也做同樣的事情，故意濫用由授權官員簽發的木材林產品運送單證。該犯罪行為的估計價值為數千億印尼盾。

據瞭解，根據資金流向，A 公司從國外收到的進賬資金達 50 億印尼盾（349,766 美元），以及幾筆數十億印尼盾的現金金融交易。此外，DG 先生作為 A 公司的董事收到的現金財務交易金額超過 130 億印尼盾（908,558 美元）。此外，作為 A 公司的董事，DT 先生的大部分現金流是以現金提取交易的形式，達到 20 億印尼盾（139,965 美元）。同時，TS 先生（D 公司的董事）將資金存入個人、子女和妻子的保險單，金額超過 30 億印尼盾（209,948 美元）。

5.19 外幣兌換／換鈔

中國澳門

一名電話詐騙受害者按冒充警察的犯罪者指示，多次將現金存入指定的中國澳門銀行帳戶，造成的損失總計約為 20 萬澳門元（25,000 美元）。為獲得部分詐騙所得，嫌疑人 A 按照犯罪集團的要求提供一個在中國澳門的銀行帳戶。然而，這個銀行帳戶由嫌疑人 K 持有，其業務是提供手機程序充值和匯款服務。在收到澳門的資金後，嫌疑人 K 將上述犯罪所得從澳門兌換成另一種外幣，預先扣除外匯服務費，然後將外幣資金轉入嫌疑人 A 的手機程序內或海外銀行帳戶。嫌疑人 A 隨後將錢匯入犯罪集團指定的另一個海外銀行帳戶。在上述案件中，儘管知道轉移的資金來自犯罪活動，但嫌疑人 A 仍然透過使用嫌疑人 K 持有的第三方銀行帳戶來掩蓋資金的非法來源，並掩蓋其參與騙局的事實。嫌疑人 A 於 2020 年被人民檢察院指控犯有詐欺和洗錢罪，嫌疑人 K 被指控接受贓物罪。

巴基斯坦

透過非法貨幣兌換和利用哈瓦拉／亨遞清洗收益的行為

針對 XX 先生個人提出的可疑交易報告顯示，他進行結構式高額貨幣兌換交易，這與他所申報的薪資收入情況不符。

經過分析發現，除可疑交易報告外，嫌疑人還在 2016 年至 2020 年期間與包括銀行和交易所在內的不同申報機構進行的大量現金交易報告（超過 200 萬巴基斯坦盧比約等於 13,078 美元門檻的現金交易）中被識別出來，而其中涉及大量資金。

在 2018 年至 2020 年期間，70% 的現金交易報告是由不同的外匯公司報告的，而其餘 30% 是由不同的銀行針對個人 XX 先生申報的。

對 XX 先生所擁有的銀行帳戶進行分析顯示，XX 先生在其他帳戶中進行交易的活動非常少。為確定交易的最終受益人，分析進一步延伸到 XX 先生進行交易的那些帳戶。結果發現，在 2020 年期間，XX 先生與一個名為 YY 先生其使用的個人帳戶頻繁進行交易。

在金融監測部門資料庫中搜索 YY 先生的電腦化國民身分證（CNIC）號碼，發現關於 YY 先生的金融情報早已與一個執法機關分享，並且正在接受執法機關的調查，因為他可能參與非法貨幣兌換和哈瓦拉／亨遞相關業務。

根據上述資訊，人們懷疑 XX 先生是 YY 先生的人頭，並在 YY 先生的帳戶中負責交易的傳聲筒。該金融情報被轉交給一個執法機關，以進一步擴大對 YY 先生的持續調查。

新加坡

L 君是一家銀行的雇員，他的職責是為客戶對沖外匯風險。在這方面，他只有在收到客戶的指示並向銀行的金融交易部查詢報價後，才被允許進行外匯交易。

L 君在 2011 年至 2013 年期間策劃一項方案，在其客戶的帳戶中進行未經授權的外匯交易，使用由他控制的兩個獨資企業的帳戶作為這些交易的對手方。L 君隨後在其他客戶的帳戶中進行額外的未經授權的交易，以關閉早期客戶的外匯頭寸。透過這一方案，L 個人積累約 120 萬新加坡幣（約 90 萬美元）的利益。L 君用這些犯罪所得來償還他未償還的信貸額度和貸款，並將其餘的錢兌換成外匯用於自己的投資。

2019 年，L 君因涉及未經授權修改電腦材料、盜用他人身分、清洗犯罪行為所得等罪行被判處 8 年 4 個月有期徒刑。

5.20 利用信用額度、信用卡、支票、本票等

印尼

案例一：

被告HT先生將KS先生和RH先生所有之X銀行發行信用卡進行修改，使用 X2 軟體將原信用卡晶片的資料轉移到智慧晶片上，如此一來信用卡就可以不透過 X 銀行的主機系統，直接在 X 銀行資料採集機上使用。在資料採集機器上使用信用卡會出具交易證明，這樣商戶就認為交易是合法的，並將交易在 X 銀行系統上註冊。

此外，被告 HT 先生在使用前會見被告 BS 先生和 MFN 先生，向他們解釋改裝後的信用卡的使用方法。其工作原理是，在選擇要購買的商品後，會要求購買者輸入密碼，這樣被告可以隨機輸入 6 位數字，交易就會成功。被告 HT 先生第一次邀請被告 BS 先生和 MFN 先生進行試用，使用該卡購買重約 8 克的黃金，價格為 3,200,000 印尼盾（224 美元）。此後，被告 BS 先生和 MFN 先生知道如何使用改裝卡後，他們接受被告 HT 先生要求，在蘇門答臘島和爪哇島各地區的不同商店裡使用卡片來購買黃金、手機和電子產品等商品。

所有購買商品的收入都交給被告人 HT 先生，讓他兌換成貨幣／或是出售，目的是掩蓋犯罪所得。X 銀行因使用信用卡而遭受的損失總額為 2,553,840,268 印尼盾（179,292 美元）。被告人 HT 先生將 32,000,000 印尼盾（2,251 美元）分給 BS 先生，將 31,000,000 印尼盾（2,177 美元）分給 MFN 先生。被告 HT 先生用這筆錢支付債務、妻子和孩子的生活費用、支付互助會（Arisan in Bahasa Indonesia）的費用、公寓租金，金額為 175,298,871 印尼盾（12,329 美元）的錢被存入 HT 先生的同事的帳戶。而被告 BS 先生將這筆錢用於服裝製造業務，被告 MFN 先生將這筆錢用於商業資本。

案例二：

身為 Z 銀行企金業務主管的 A 君利用其職務之便，為 A 公司 1,500 億印尼盾（10,494,664 美元）的信貸申請程序提供幫助。眾所周知，A 公司的實質受益人，即 HS 先生，操弄其他七家銀行。A 君利用他的權力修改為 A 公司提交信貸申請的方案，該方案之前被企業信用風險部拒絕。A 公司用來作為其對 B 公司基本抵押品或信用擔保之一，結果是 C 公司從未對 A 公司持有的債務，其實是虛構的。

與此相關，被告收到從 A 公司轉給 A 君的 15 億印尼盾（105,030 美元），作為辦公室行政總務之用。A 君隨後將資金轉入五個帳戶，其中一個帳戶在他名下，四個帳戶在其他人名下。這筆資金還被用於支付醫院醫療費用、購買汽車、海外旅遊的信用卡帳單、購買美元和新幣的外匯以及房屋租金。

紐西蘭

利用偷來的支票進行詐騙／洗錢計畫

一個犯罪網絡利用偷來的支票詐騙紐西蘭受害者 140 多萬紐西蘭幣（1,003,447 美元）。該網路使用偷來的支票本作為網上訂單的付款。一旦網上下單，犯罪者就要求提供銀行帳號，要以銀行存款匯款作為網上訂單的付款。然後，犯罪者透過自動櫃員機存款將假支票存入受害者的帳戶。當受害者查看他們的帳戶時，看起來他們已經得到付款，因此他們開始安排貨物的運輸。幾天後，這筆存款被確認為假的，然而，此時部分貨物已經被發往犯罪者手中。該網路將偷來的支票存入紐西蘭各地的眾多零售商，採購的物品包括金條、珠寶、相機、電腦商品、熱像儀、越野摩托車和空包彈槍。

巴基斯坦

詐欺／龐氏騙局

針對 AB 先生和 MA 先生申報的可疑交易報告，顯示這兩個人都參與非法汽車租賃業務。他們利用社交媒體平臺，以不切實際的高利潤率向公眾提供一些投資計畫。金融監測單位啟動對這兩個人的可疑交易報告的分析。

金融監測單位分析這兩個人的帳戶。在分析過程中發現，AB 先生和他的公司的所有被申報的 10 個帳戶都是在過去三年中開設。儘管他在銀行開戶文件中聲明自己是汽車租賃商，但在他銀行帳戶中沒有發現任何與汽車業務有關的交易。同樣，對 MA 先生的銀行帳戶的分析顯示，這些帳戶是在過去一年半的時間裡開設的。

二人透過提供低於市場行情的貸款利率來引誘公眾。他們分別以 4% 和 6% 的利率提供汽車和住房的資助服務。此外，這些人還在其網站上澄清，該放貸機制不向媒體和執法機關成員提供。

此外，上述人員經營的其中一家公司已經被巴基斯坦證券交易委員會（SECP）裁罰，原因是其參與非法經營與車輛、房屋、電子產品等有關的業務。然而，被舉報的個人最終還是想方設法繼續經營這些業務。上述金融情報被分享給執法機關，讓其對這些人採取行動。AB 先生的辦公室被搜索並封存，同時還對其進行逮捕。進一步的調查正在進行中。

5.21 電匯／利用外國銀行帳戶

中華臺北

H 先生是一個有數次犯罪紀錄的詐騙犯。L 女士是一家名為 YK 的外國公司（A 司法管轄區）的所有者。2019 年，為對 L 女士實施詐騙，

H 先生冒充中華臺北 G 銀行集團的成員和 B 司法管轄區的執業律師，聲稱可以幫助 L 女士獲得 G 銀行集團的 VVIP 會員資格，處理她家族合約官司，還能一起投資不動產。L 女士被該計畫騙走 400 多萬美元，並將其個人儲蓄的資金轉入 H 先生指定之人頭帳戶，包括一個在 B 司法管轄區註冊的公司帳戶。

地檢署於 2020 年 8 月以違反刑法和洗錢防制法的罪名起訴 H 先生及其同夥。

中國香港

司法管轄區 X 的一家銀行的銀行間資訊交換系統受到攻擊，有 11 筆未經授權的交易，總額為 1.08 億港幣（13,905,561 美元），被匯到全球各地的銀行。共計 5,200 萬港幣（6,695,234 美元）被匯入中國香港的銀行帳戶，其中一些資金在同一天透過電匯進而失去蹤跡。接到報告後，香港警方迅速扣留收款帳戶中的 2,700 萬港幣（3,476,411 美元）。共有 11 名帳戶持有人被逮捕。其中三人被定罪並被判處 26 至 30 個月的有期徒刑。兩名被告已經潛逃，尚未找到。

新加坡

2018 年，新加坡警察部隊商業事務部（CAD）收到來自 X 司法管轄區當局的資訊，稱來自 N 司法管轄區的 R 君在新加坡的幾個銀行帳戶被用於清洗犯罪所得。

R 君是位於 N 司法管轄區的一家公司的執行長，據稱該公司生產和銷售加密的手持裝置，旨在提供安全手段來公開交流犯罪活動而不必擔心被執法部門發現。根據 X 司法管轄區當局的調查，R 人最終承認涉及共謀敲詐勒索行為和分銷古柯鹼的罪行。作為認罪的一部分，R 君同意沒收他的一筆資產，包括存在新加坡銀行帳戶中的錢。

根據外國當局提供的資訊，加拿大稅務局開始在進行國內洗錢調查，並在此過程中扣押存放在 C 公司（一家在新加坡註冊的公司，R 君是該公司的董事和唯一股東）銀行帳戶中的 500 多萬新加坡幣（3,759,238 美元）的收益。在調查結束後，CAD 與總檢察長辦公室合作，援引我們的司法程序取消扣押，並在 2020 年成功地將被扣押的 3,971,468.40 美元資產返還給 X 司法管轄區當局。

此外，曾協助成立 C 公司的公司服務提供商可能犯公司法規定的罪行，包括作為 C 公司的董事沒有盡到合理盡職調查義務。目前訴訟正在進行中。

5.22 利用偽冒身分

汶萊和平之國

2020 年 3 月 9 日，一名受害者向警方報案，稱其與丈夫的聯合帳戶被轉出 67,800 汶萊元（50,943 美元），並懷疑第三方（他們的女兒）參與盜竊。汶萊皇家警察部隊（RBPF）啟動前置犯罪調查，並逮捕 A 君和 B 君。

調查顯示，受害人的女兒 A 君在其表弟 B 君的幫助下，使用欺騙手段將受害人帳戶中的資金轉入 A 君的帳戶。他們進入受害者的帳戶，並使用銀行的網上銀行應用程序，進行轉帳。

作為汶萊皇家警察部隊調查的一部分，警方查獲大量的物品，他們認為這些物品是用她的盜竊所得購買的。其中包括金額為 8,200 汶萊元（6,160 美元）和 1,600 萬印尼盾（1,118 美元）的款項。A 君和 B 君都將這些錢用於自己的個人開支和海外豪華旅遊。

在汶萊皇家警察部隊提交調查文件後，總檢察長辦公室（AGC）建議對 A 君進行進一步調查，以獲得可以支持洗錢指控的相關證據，如被

扣押物品的價值、購買地點、購買時間以及是否用贓款購買。

汶萊皇家警察部隊能夠獲得足夠的證據，2020 年 4 月 30 日，A 君被起訴並被判定犯有盜竊和洗錢罪。她被判處 32 個月的有期徒刑，然而，在公訴檢察官成功上訴後，這一刑度被增加到 40 個月。B 君被判處 8 個月的有期徒刑。

中國香港

在中國香港的一起房產詐騙案中，X 先生使用偽造的身分證，委託房產中介和法定代理人，代表房主出售房產。Y 先生將自己的名字正式改為房屋所有者的名字，並開設一個銀行帳戶。一位買家向 Y 先生支付約 3 百萬港幣（386,272 美元）的定金，Y 先生後來提取所有的現金，並改回自己的原名。當真正的業主收到一封來自律師事務所的信函，告知其所有權的變更時，此案浮出水面。Y 先生被判犯有偽造文件罪和洗錢罪，並被判處有期徒刑 48 個月，而 X 先生被判犯有詐欺和串謀詐欺罪，並被判處有期徒刑 42 個月。

印尼

有 52 名債務人與 CRR 作為 X 銀行的分行經理（BM）與分行主管（授信主管）犯下的詐欺跡象有關。CRR 透過借用債務人的身分資料來申請貸款，包括虛構債務人擁有的事業、偽造債務人的身分，製造用於貸款申請的抵押品的買賣紀錄，墊高事業的營收及抵押品價值，從而使貸款獲得批准。然後，CRR 給身分被借用的一方一筆錢，從 250 萬印尼盾（175 美元）到 500 萬印尼盾（351 美元）不等，作為使用該方身分向 X 銀行申請信用貸款的費用。

CRR 從銀行犯罪中獲得的資金達 931,300,000 印尼盾（65,511 美元）。洗錢是透過使用別人的身分購買土地形式的資產進行的。

由於這一行為，CRR 被判處 8 年有期徒刑和 2 億印尼盾（14,075 美元）的罰款。

紐西蘭

組織犯罪集團從事銀行貸款詐欺

一群紐西蘭公民透過辦理銀行貸款，透過單邊契據改變自己的名字以規避當局的監管，然後拖欠貸款償還，從而欺騙幾家紐西蘭銀行。該詐騙行為得到一家紐西蘭建築公司的幫助，該公司提供薪資單和假薪資以支援貸款申請。金融情報中心發現一些人從該紐西蘭公司收到附言為薪資的付款。這些人利用這些報表作為該公司更多文件（薪資證明、薪資單、勞動契約）的一部分，從幾家紐西蘭銀行獲得貸款。據估計，該集團從多家銀行獲得價值幾十萬美元的貸款。一旦獲得貸款，犯罪者就合法地改變他們的名字，使他們能夠更好地躲避銀行和執法部門的後續調查。騙取的資金大多以現金形式提取或透過第三方帳戶網路集中匯出。

5.23 與貪汙／賄賂相關之洗錢

孟加拉

政府官員向多個司法管轄區清洗犯罪所得

A 先生是一名政府官員，他的妻子 R 女士是一家名為 "A 公司 " 的商業法人實體的經營者，該公司是一向政府醫院和機關提供外科設備的承包公司。在 A 先生、其妻子 R 女士及其相關法人實體的銀行帳戶中，超過 52.02 億塔卡（61,286,951 美元）進行交易。大約 43 億塔卡

（50,657,108 美元）在 A 公司的銀行帳戶中交易，其中 10.2 億塔卡（12,016,424 美元）存入該帳戶，用於競標政府標案（根據存款單的聲明）。

錢從 A 公司的銀行帳戶轉到另一個法人實體、B 公司的帳戶，B 公司所有人的名字在巴拿馬文件中被公布。此外，大量資金從這個帳戶被頻繁地轉移到幾個帳戶。分析顯示，A 先生是其妻子的公司 A 的最終控制人和受益人。公開資料顯示，他曾準備偽造的貨物供應文件，並控制政府標案有利於其妻子公司招標，甚至設法在未提供最低資本／擔保金的情況下得標。

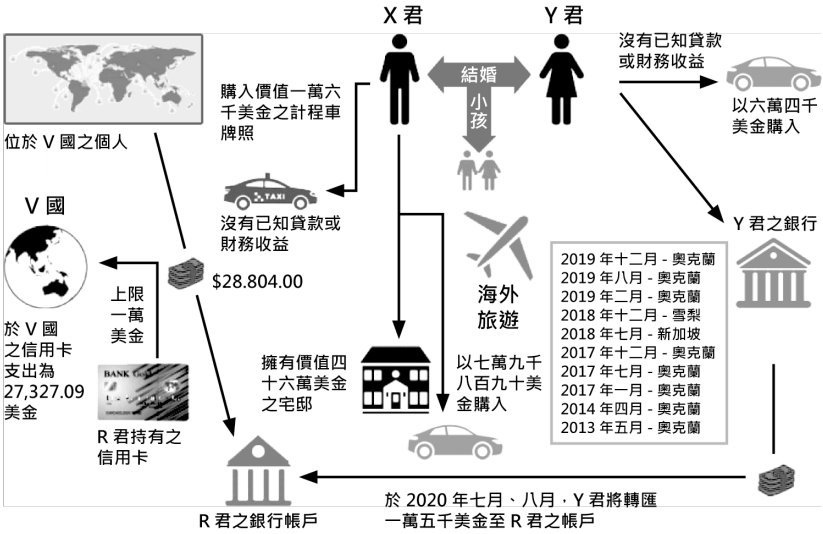
此外，孟加拉金融情報股獲得 A 先生及其妻子在四個外國司法管轄區，即位於 Wx 司法管轄區、Xy 司法管轄區、Yz 司法管轄區和 Zx 司法管轄區的帳戶資訊。有資料顯示，A 先生及其妻子在這些司法管轄區的帳戶被申報許多現金交易報告、大額交易報告和電子資金轉帳報告，總額達 1,345 萬美元。此外，在其中一個司法管轄區，申報 2014 年 12 月至 2020 年 6 月期間的可疑交易。此外，儘管孟加拉本國人在未經孟加拉當局批准的情況下不能在外國司法管轄區進行投資，但依然發現以 A 先生的名義在外國司法管轄區設立之商業法人實體。

經過分析，A 先生似乎在其妻子的協助下積累大量非法財富，並試圖透過以其妻子的名義成立一家承包公司來掩蓋其非法賺取的錢財，並最終透過非法管道將這些錢財匯集到境外司法機關。根據調查結果，聯邦調查局擬撰一份情報報告，並將其分發給反貪汙委員會，以便依 2012 年洗錢防制法（MLPA）進行更進一步調查與採取必要法律行動。

斐濟

貪汙、賄賂、回扣和不明真相的財富

受雇於當地一個立法機關的 R 君因可能的賄賂、貪汙和財產來源不明案件引起斐濟金融情報中心注意。分析顯示，R 君在 2018 年 7 月至 2020 年 9 月期間，從 V 司法管轄區和斐濟的不同人那裡收到總計約 28,804 斐濟元（14,107 美元）匯入其銀行帳戶。還注意到，R 君、他的失業配偶（Y 君）和他們的孩子經常前往 V 司法管轄區。2019 年 8 月，R 君獲得一個計程車許可證，但是，沒有相應的交易顯示 R 君購買該計程車許可證。R 君和 Y 君共擁有四輛高價轎車，這些車輛是在沒有任何資助的情況下購買的。進一步的分析顯示，R 君在中心區購置一套永久土地擁有權的房產，並在過去幾年對該房產進行重大改進。進多分析顯示，R 君的交易和財富積累模式與其申報的年收入不一致。還確定 R 君和他的家人經常出國旅行，然而，機票和旅行費用的資金無法從信用卡或銀行帳戶交易中追蹤到。向斐濟反貪汙獨立委員會（FICAC）提供案件情資交換報告，以審查該案件中可能因貪汙和賄賂而產生的不明財富。



印尼

案例一：

ZAI 先生是 2016 年至 2021 年期間南楠榜地區的統治者，從 2016 年到 2018 年，ZAI 先生透過 AGU 先生（2015 年至 2017 年 1 月在公共工程與不動產部辦公室財務分處負責人）和 ANJ 先生（2017 年 12 月至 2018 年 7 月在公共工程與不動產部南楠榜辦公室負責人）收到分配基礎設施工作的錢（稱為承諾費）。ZAI 先生與 AGU 先生、ANJ 先生、HER 先生和 SYA 先生從 2016 年至 2018 年分階段從被公共工程與不動產部辦公室授予專案的法人實體那裡收到現金，總額為 72,742,792,145 印尼盾（5,116,854 美元）。

根據承諾費安排，HER 先生組建一個由 SYA 先生協調的團隊。然後，HER 先生向 SYA 先生提供一份工作清單，並命令 SYA 先生根據專案規劃，向將要獲得工作（基礎設施工程）的法人實體收取承諾費。然後，承諾費被提交給 AGU 先生。由 SYA 先生協調的團隊的任務是為支付承諾費的公司準備投標文件，並將其上傳到電子採購服務（LPSE）系統。承諾費可能達到項目價值的 21% 左右。

案例二：

SLM 先生、BS 先生和 AN 先生是某政府機關的公務員。SLM 先生是負責供應基金（SF）和額外供給基金（ASF）方面支出的主管。然而我們發現，供應基金和額外供給基金並沒有完全用於按照該機關已決定之活動規劃為業務、非業務、供應、服務和維修支出提供資金，而是被用於 SLM 先生、BS 先生、AN 先生和其他各方的個人利益。違反正常支出準則使用之資金達 5,018,121,329 印尼盾（347,816 美元）。用於 SLM 先生、BS 先生和其他各方個人利益的資金為 4,685,971,329 印尼盾（327,794 美元），而剩餘的 332,150,000 印尼盾（23,022 美元）

由 AN 先生支配。這些當事人各方收到的資金隨後在被告的幾個同夥之間進行分配。

案例三：

a. 在兩個實例中，NZ 先生利用 PMI 集團及其旗下公司的帳戶和他人名下的帳戶留置或轉移自採購活動中貪汙之所得，金額為 700.18 億印尼盾（4 903 635 美元）和 1,034 新加坡幣（774 美元，約 930 萬印尼盾）。所有權以 PMI 集團控制旗下公司的股份形式轉移，即價值 504.25 億印尼盾（3,529,984 美元）的 ETU 公司和 PNH 公司股份。

b. 此外，NZ 先生轉讓價值 184.47 億印尼盾（1,291,476 美元）的土地和建築物之所有權；花費或支付購買土地和建築物的費用 1,111.17 億印尼盾（7,779,327 美元）；花費或支付購買機動車輛的費用 10.07 億印尼盾（70,500 美元），花費或支付 20.92 億印尼盾（146,525 美元）的保險費。

c. NZ 先生花費或支付購買股票，然後利用屬於 PMI 集團成員的公司或印尼證券交易所的其他人的名字轉售這些股票，包含 GRD 公司的股份、MDR 銀行的股份、ABC 銀行的股份、GG 公司的股份、KS 公司的股份、JAW 公司的股份、BCE 公司的股份（以 NZ 先生之妻的名字）、PRW 公司的股份、CA 公司的股份、DMK 公司的股份、ETU 公司的股份以及 PPM 公司的股份。除此之外，NZ 先生還購買總價值為 3,747 億印尼盾（26,211,738 美元）的債券。因此，NZ 先生在資本市場的總資產為 6,278.6 億印尼盾（43,915,767 美元）。

d. 為隱匿或掩蓋犯罪所得的來源，NZ 先生透過 PMI 集團財務總監將出售 GRD 公司股份所得的資金轉入 PPM 公司在 SCT 銀行[33] 的

[33] 一種專為在印尼開設證券戶之外國公司所擁有之證券帳戶

X 司法管轄區貨幣劃撥帳戶，金額約為 600 萬元 X 司法管轄區貨幣（4,494,743 美元）。此外，這也是透過 GL 先生作為一家名為 PT.TCL 的招聘機關總裁的指示，將約 600 萬元 X 司法管轄區貨幣（4,494,743 美元）轉入 LKS 先生的帳戶，似乎是用於支付在 X 司法管轄區購買拖船的款項。GL 先生作為一家名為 PT. GRD 公司在二級談判市場上賣出四家公司股份，即 PT. PRW 公司、PT. CA 公司、PT. MK 公司和 PT. ETU 公司給 PT. TCL 公司，金額為 1,630 億印尼盾（11,414,212 美元）。

e. 此外，還有這樣的交易：NZ 先生的妻子將出售 BCE co. 的股份轉移到 Jurisdiction X 的一家名為 WII, Pte Ltd. 的公司的帳戶，金額為 260 億印尼盾（1 820 517 美元）。

紐西蘭

海外貪汙計畫的收益透過紐西蘭不動產市場進行洗錢

紐西蘭金融情報中心收到三份關於一家在紐西蘭註冊的公司（A 公司）的可疑活動報告（SARs）。這些可疑活動報告涉及 A 公司以 2,300 萬紐西蘭幣（16,663,730 美元）的價格將其在奧克蘭的一處房產出售給一個未知人士。搜索報告指出，A 公司的實質受益人是一名境外司法管轄區的政府官員（A 君），他因涉嫌涉及另一司法管轄區自然資源的貪汙而受到另一司法管轄區反貪汙機關的調查，並且自 1980 年代以來一直受到 " 眾多 " 貪汙指控。作為 SARs 的一部分，申報機構提供 A 公司的實際所有權資訊，該資訊顯示 A 君是一個信託（位於歐盟司法管轄區）的委託人，該信託擁有 A 公司 60% 的股份，而 A 公司又是價值 2300 萬紐西蘭幣（16663,730 美元）的紐西蘭房產的唯一所有者。該資訊還顯示，A 君是第二個（設在境外的）信託的保護人，該信託擁有 A 公司 20% 的股份：實際上使他擁有該公司 80% 的所有權。

透過紐西蘭銀行帳戶清洗境外司法管轄區濫用公職的收益

紐西蘭金融情報中心收到一份關於居住在境外 A 司法管轄區之紐西蘭公民的可疑活動報告，該公民透過公開資訊引起申報機構的注意，指控他在司法管轄區 A 濫用其公職人員的身分以謀取私利。這些指控包括他無權申報的費用和休假，以及利用其影響力為主要工作人員爭取優惠待遇。此前，A 司法管轄區廉政署已對該嫌疑人進行訊問，調查正在進行中。

該嫌疑人的可疑活動報告顯示，他從 A 司法管轄區的銀行帳戶中收到超過 200,000 紐西蘭幣（144,823 美元）存入其紐西蘭帳戶的資金，這些資金隨後被轉入紐西蘭境內的第三方帳戶，還被用於資助個人開支。

通過紐西蘭境外信託架構洗海外賄賂所取得之收益

紐西蘭金融情報中心收到來自海外合作夥伴的自發傳播，涉及一名外國國民（標的 X），他受到關於 " 賄賂筆記本 " 的國際調查，位於 A 司法管轄區的一群海外商人被指控行賄以保持 A 司法管轄區的政府機關管理的公部門工程合約。夥伴金融情報中心指出，國民 X 是一個信託（信託 Z）的委託人和受益人，該信託於 2016 年轉讓給一家紐西蘭公司（Z 公司），該公司在一個離岸銀行帳戶中持有總計 860 萬美元的資產。

紐西蘭金融情報中心進行的調查發現，Z 信託被確認在 2016 年時被轉移至紐西蘭，被設立為以 Z 公司為受託人之紐西蘭境外信託。Z 公司與一個在紐西蘭和國際上提供信託和公司服務之集團有關聯，而這些公司以前曾因涉嫌參與複雜的國際洗錢計畫而引起紐西蘭金融情報中心的注意。Z 公司的股東是另一家境外公司。

紐西蘭金融情報中心調查顯示，Z 信託在紐西蘭沒有利用境內銀行設施，但多筆以 Z 信託名義支付的款項被存入 Z 公司的紐西蘭帳戶，據

紐西蘭金融情報中心評估，這些款項可能是紐西蘭信託或公司服務提供商代為管理架構的費用，其中一部分可能被指定轉入 X 擁有／控制的海外銀行帳戶。

巴基斯坦

貪汙與賄賂

AA 女士帳戶中的交易活動有可疑之處，因為該帳戶中的高額資金交易顯然與她家庭主婦的身分不符。此外，資金來源和其真正受益人也不清楚。

在分析過程中，發現 AA 女士在不同銀行開設數個巴基斯坦盧比和外幣帳戶，並發覺其中有大量的交易活動。此外，AA 女士從她父親的帳戶中收取大量當地貨幣資金，據稱是為贈與。贈與等值金額隨後被轉入她自己在另一家銀行的帳戶，但操作該帳戶的授權是由她的丈夫 AK 先生持有。之後，這些資金透過現金和支票被提取。根據實名認證文件，AK 先生是一名高階政府官員。

透過在金融監控中心資料庫中搜索國民身分證（CNIC），發現 AK 先生和 AA 夫人進行貨幣兌換交易，並向國外匯出大量資金。

由於懷疑 AK 先生是這些資金的最終受益者，該財務情報因涉嫌貪汙和賄賂而與執法機關分享。

新加坡

2019 年，新加坡貪汙調查局（CPIB）對某體育協會前高級管理執行官進行調查，罪名是詐欺，涉及因隱匿與相關供應商的利益而不正授予其合約。調查顯示，在 2016 年至 2018 年期間，該管理人員詐欺的總收益達到 647,180 新加坡幣（約 487,766 美元）。上述前副局長和其他

三名共同被告人于 2020 年 12 月 9 日根據刑法第 224 章起訴詐欺罪。新加坡貪汙調查局為追蹤犯罪所得，開始同時進行金融調查。調查顯示，這些資金被輸送到與前副局長有利益關聯的兩家公司，透過其與這兩家公司簽署的合約來實現。隨後，很大比例犯罪所得被從這些公司的帳戶中領出再存入前副局長妻子的個人銀行帳戶。這些犯罪所得與她的個人資金混在一起。2017 年 7 月，她提取約 573,000 新加坡幣（約 431,778 美元），用於一套私人房產的首付款。鑒於這些發現，新加坡貪汙調查局對該房產提出警示。新加坡貪汙調查局還查封前副局長和他的妻子所持有的約 15.6 萬新加坡幣（約合 11.7552 萬美元）現金。目前，調查仍在進行中。

5.24 濫用非營利組織（NPOs）

新加坡

根據阻絕恐怖主義金融流通法，三個人 A 君、B 君和 C 君於 2020 年 2 月和 3 月被定罪，罪名是收集和／或提供資金以幫助 J 司法管轄區內與伊黎伊斯蘭國有聯繫的恐怖組織法人實體 X，並被判處 18 個月至 45 個月的有期徒刑。

這三個人在新加坡擔任外籍家庭幫傭（"FDWs"）。在 2018 年 9 月至 2019 年 7 月期間，他們向兩個所謂的宗教慈善機關籌集和／或匯出 1,486 新加坡幣（約 1,118 美元）的資金，認為這些資金將用於支援法人實體 X 其激進事業及行動中被拘留或殺害的成員的家人。所有的錢都是透過自籌資金籌集的，並透過同一個有執照許可之匯款代理機關匯給 I 司法管轄區的人。因此，這三人有合理的理由相信，所籌集和匯出的資金將被用於協助海外的恐怖主義行為，從而導致對他們提出資助恐怖主義的指控。

6. 資助武器擴散之方法與趨勢

6.1 對違反、不執行或規避與資武擴相關之目標性金融制裁之個案研究

中華臺北

執法部門（法務部調查局）在 2018 年 10 月的調查後，搜索 W 先生的住所和公司，該案件被稱為 S 號船案，涉及對北韓之非法船對船轉移業務。法務部調查局分析 S 號船案案件證據，發現 W 先生成立一家境外公司，從一家名為 S 公司在 X 司法管轄區的公司購買石油，然後儲存在位於台中港的一個油槽。2018 年 5 月，W 先生著手租用一艘名為 G 號的船隻，將 1,350 公噸石油從台中港運到公海，在那裡與 S 號船隻進行船對船轉運。W 先生還利用 G 號船與北韓的 P 號船進行進一步的石油船對船轉移。W 先生隨後將 G 號船賣給北韓，這違反中華臺北的法律和聯合國安理會第 1718 號決議。法務部調查局的調查發現，W 先生向聯合國制裁名單上的指定目標提供財務資源，這違反 2018 年資恐防制法（CFTA）第 9 條第 1 款第 1 項之罪名。此案已於 2020 年 11 月移交給地方檢察署起訴。

馬來西亞

2012 年至 2017 年期間，兩家馬來西亞私人有限公司被確認為一家與北韓有聯繫的公司的幌子，該公司為軍事和準軍事組織提供無線電通訊設備。經審查這些公司在當地金融機構的銀行帳戶，這些前台公司似乎收到來自不同外國法人實體的 50 筆國際轉帳，金額達 750 萬馬幣（1,819,806 美元），其中包括聯合國安理會後來指定的法人實體、接受專家小組調查的法人實體以及其他看起來可疑或與發送方的商業活動不一致的公司。收到資金後，立即轉給其他幾個法人實體，專家小組後來指控這些法人實體是聯合國安理會制裁人員的前台公司。

據觀察，這些公司經常在其帳戶之間轉移資金以避免被發現，然後再轉移到外國前台公司，隨後轉移到平壤的最終收款人。

紐西蘭

一家為促進紐西蘭和北韓之間關係而成立的紐西蘭慈善協會因向北韓紅十字會捐贈 2,000 紐西蘭幣（1,440 美元）而被牽涉到可能違反聯合國制裁。由於聯合國的制裁，紐西蘭紅十字會不能直接向北韓匯款，因此它將資金寄給 X 司法管轄區的一個聯絡人，該聯絡人將資金以現金形式轉交給北韓大使館。當局發現，該活動可能違反聯合國對北韓的制裁。

菲律賓

案例一：

2020 年 5 月，洗錢防制辦公室透過內政部發函與專家小組取得聯繫，就專家小組對涉及 A 船和菲律賓公民 X 對象的調查尋求協助。

2019 年 4 月 24 日，法人實體 B 在 X 司法管轄區註冊，其國民 X 成為法人實體 B 的董事、股東和實質受益人。2019 年 6 月，A 號船被出售，其名稱改為 B 號船，該船的所有權變更為法人實體 C。 2019 年 8 月，B 號船從 Y 司法管轄區前往北韓，並於 2019 年 11 月返回 Y 司法管轄區，裝載源自北韓的煤炭。

對國民 X 的調查發現，專家小組提供的出生日期和位址與 X 物件在其實名認證文件中提供的資訊相符。調查還發現，國民 X 在 2005 年 7 月至 2020 年 2 月期間進行 103 筆大額交易，金額從 400,000 菲律賓披索（8,000 美元）到 4,000,000 菲律賓披索（80,000 美元）不等。同一時期還有 10 份機密報告，涉及國民 X 和她的丈夫國民 Y 的聯合帳戶，

其中指出，聯合帳戶中的交易似乎沒有基本的法律或貿易義務、目的或經濟理由。另外還注意到，在購買船隻 A 和註冊法人實體 B 的同一時期，有大量的現金存款和支票兌現交易。國民 X 被要求提供有關資金來源的資訊，但她給出不一致和矛盾的回答，如這些錢來自企業和／或她丈夫的津貼。進一步調查發現，沒有企業在貿易和工業部註冊，國民 X 無法提供有關企業的資訊，也無法提供他們如何取得帳戶中的資金。

對國民 X 配偶國民 Y 的調查發現，國民 Y 在馬尼拉擁有一家服裝企業：法人實體 D。2009 年 7 月至 2015 年 12 月期間，當事人 Y 還進行 49 筆大額交易，金額從 400,000 菲律賓披索（8,000 美元）到 4,000,000 菲律賓披索（80,000 美元）不等，其中大部分交易是在與當事人 X 的聯合銀行帳戶中進行的。針對國民 X 調查正在進行中。

案例二：

專家小組進行的調查涉及一艘懸掛 Z 司法管轄區旗幟的船隻 C 號船涉嫌違制裁規定，並在 2020 年 4 月向北韓交付精煉石油產品。國際海事組織的網站列出一家海外公司，即 YYY 公司，自 2019 年 11 月起作為 C 號船的註冊船東、船舶經理和運營商。從專家小組獲得的資訊和公開資料顯示，YYY 公司的董事是菲律賓人 G 先生。對 G 先生的調查發現，從 2005 年 11 月到 2019 年 4 月，他進行共 130 次交易。G 先生還有總額為 2.5436 億菲律賓披索（532 萬美元）的現金存款，這似乎與他的商業收入不相稱。此外，他還有一筆總額為 2.2377 億菲律賓披索（4,578,228 美元）的貸款，與現金存款總額相近。

向北韓交付精煉石油產品發生在 2020 年，然而，在此期間沒有代表 G 先生的交易報告。可能是交易沒有透過財務系統，或者是進行在申報

門檻以下的小額交易。證券交易委員會（SEC）還發現，YYY 公司不是一家註冊公司，沒有出現在 SEC 資料庫中，然而，SEC 確實發現 G 先生與其他幾家公司有關聯。貿易和工業部證明，G 先生的名字沒有出現現有的商業登記實體中，相關調查仍在進行。

新加坡

2020 年 9 月，C 君因協助在 C 君控制下註冊的 S 公司、C 公司和 D 公司在 2010 年 12 月至 2016 年 11 月期間 40 次向北韓提供價值超過 50 萬新加坡幣（676,769 美元）的指定奢侈品而被定罪。調查顯示，C 君自 20 世紀 80 年代以來註冊多家公司，以便與北韓進行貿易並從中牟利。S 公司、C 公司和 D 公司曾向北韓的四家不同公司提供貨物，其中一家公司已發展成為分銷商和批發商，向北韓的其他商店供應各種貨物。

2010 年，根據聯合國法頒佈禁止向北韓供應指定奢侈品的條例，然而，儘管 C 君意識到與北韓貿易的風險，並積極採取措施避免被當局發現，但他們並沒有停止與北韓的貿易活動。C 君向北韓提供奢侈品的方式是透過鄰近的司法管轄區進行空運和海運，或透過機場托運進行手工運輸。北韓對奢侈品的付款是透過在海外註冊的前台公司支付給 S 公司、C 公司和 D 公司的銀行帳戶。調查還顯示，C 君為避免被發現而低調行事，不在註冊地址大樓的樓層指引或租用單位外展示公司名稱，而這三家公司的註冊位址都是一樣的。

C 人被判處三周有期徒刑，S 公司、C 公司和 D 公司還被罰款共計 130,000 新加坡幣（97,966 美元）。這些判決正上訴至高等法院，包括檢察官提出上訴要求更嚴厲判決。

7. 洗錢與資恐之趨勢

報告的這一部分簡要介紹 ML 及 TF 的趨勢，包括 APG 成員和觀察員進行的研究的公開資訊。

7.1 洗錢與資恐相關之方法與趨勢之近期調查與研究

澳洲

ML / TF 風險評估：澳洲博弈旅遊團業務

澳洲交易報告和分析中心於 2020 年 12 月公布其對其博弈旅遊團業務的風險評估[34]。該評估是作為一項有針對性之工作方案的一部分，重點關注澳洲最大的金融服務部門：即銀行、匯款和賭博部門。

澳洲交易報告和分析中心評估認為，在澳洲，與旅行團業務相關的整體洗錢和防制洗錢風險很高。

金融科技聯盟之貿易洗錢工作小組

2020 年初，澳洲的公私合營企業：金融科技聯盟成立一個專門的貿易洗錢工作組，旨在構築系統韌性、分享知識，並制定連貫的戰略來打擊和阻斷澳洲的貿易洗錢。該工作組每月召開一次會議，由來自政府、執法部門和金融業合作夥伴在該議題專精之專家組成。工作組的目標之一是確定和記錄金融設施和產品是如何被用於貿易洗錢目標的。工作組還旨在考慮和審查緩解貿易洗錢的控制措施是否充分。該工作組將培養國內和國際夥伴關係，並制定態樣和指標，以確立最佳做法，從而能夠加強和協作應對打擊貿易洗錢危害。在成立後的短時間內，該工作組已經發起一些倡議，包括：

---

34 https://www.austrac.gov.au/sites/default/files/2020-12/JTO_2020_FINAL.pdf

- 制定貿易洗錢指標文件，包括公部門和私部門合作夥伴的回饋意見。
- 在澳洲邊境防衛部隊的指導下，建立一個公部門和私人合作的資訊分享架構，以確保及申報特定高風險行業部門的可疑活動。由一家金融機構建立並提供關於貿易資助的專門培訓方案。

汶萊和平之國

汶萊和平之國看到一種持續的活動趨勢，暗示可能在沒有許可情況下進行放貸，這是放債人法第 62 章第 8 節規定的罪行，也是 2012 年《刑事資產追回令》第 3 節規定的罪行。

2020 年 12 月 7 日，金融情報中心向所有金融機構和指定之非金融事業或人員發布一份態樣，描述如下。

做案手法：

a. X 君（放款人）利用社交媒體，特別是 Facebook，搜索和識別潛在客戶。X 君可能會盯上其他需要透過獲得貸款購買資產但因超過總債付比率（TDSR）上限而無法透過貸款之人。
b. Y 君（客戶）為解決他的債務而尋求 X 君的幫助，以便取得更大額的款項或貸款金額之個人用途無法說明之款項。
c. X 君為 Y 君提供解決其債務所需的資金，條件是 Y 君獲得一筆新的貸款，其金額足以償還 X 君的傭金（寫作為利息支付）。
d. X 君可以以現金或電子資金轉帳等形式把錢給 Y 君。
e. X 君還可能讓第三人幫他們進行電子資金轉移。
f. Y 君用這些錢全額償還他們的貸款。
g. 此後不久，Y 君又申請一筆新的貸款，其金額比之前的貸款要大。這筆差額包括支付給 X 君的傭金。

需要注意的紅旗指標：

a. 客戶申請貸款，但由於超過他們的總債付比率限額而被拒絕。這包括任何其他嘗試（即與任何銀行／金融公司工作人員的協商）。
b. 客戶試圖獲得貸款被拒絕，但突然能夠提前對其現有的貸款完成結算。
c. 客戶在提前結清前一筆貸款後不久又申請新貸款。
d. 以該客戶的收入水準，不可能提前結清貸款的金額。
e. 使用不明來源的資金或客戶無法證明的來源或提供不合理來源之資金提前結清貸款。
f. 客戶在其個人帳戶中收到似乎不相干人士提供的大量資金。
g. 客戶在其個人帳戶中收到大額資金，然後立即用於解決他們的貸款。

印尼

印尼 2020 年洗錢風險評估的初步報告文件，包括以下結論：

- 具有高洗錢風險的前置犯罪包括貪汙和毒品。此外，具有中等風險的前置犯罪是銀行服務、環境、林業、詐欺和稅務犯罪。
- 高度涉及洗錢風險的工業部門申報機構是汽車產業和不動產公司／不動產代理。
- 法人實體具有較高的洗錢風險，而具有較高洗錢風險的商業法人實體是有限責任公司（PT）和政府機關，如各部門。
- 具有較高洗錢風險的個人工作概況是立法和政府官員以及公營國有或地方政府公有企業的雇員（包括退休人員）。
- 根據具有高風險水準的態樣進行風險評估，包括使用偽造身分、轉移到財產資產和使用代名人或借名、化整為零、拆分交易、使用專業服務、使用新的支付方法／系統、使用公司（法人）和利用監管不力的部門。

印尼關於 2020 年大規模殺傷性武器 TF 和 PF 風險評估的初步報告，包括以下內容：

a. 資助恐怖主義的方法

- 募資階段：個人贊助者（恐怖主義資助者／籌資者），透過群眾組織和合法的商業活動募集捐款。
- 資金轉移階段：透過金融服務提供商、攜帶現金跨越國界，以及使用新的支付方式。
- 資金使用階段：製造武器和爆炸物、外國恐怖主義戰士旅行費用，以及使用武器和爆炸物。

b. 跨國犯罪者的高風險特徵

TF 的高風險犯罪者的特徵是：企業家／中小型企業主、私人雇員和商人。

印尼金融交易報告和分析中心（PPATK）的 2020 年研究報告，彙編 2019 年的 ML 法庭裁決，確定。

- 50 項 ML 法庭判決及 50 項定罪。
- 5 項定罪與 DNFBPs（商品與服務供應商（GSPs））的報告有關，占定罪的 10%。
- 這些定罪與 8 個商品與服務供應商，被報出涉及到購買財產。

中國澳門

自收到之可疑交易報告中發現的常見 ML 方法如下：

- 不定期的大額現金提取。
- 大筆現金存款，其資金來源無法核實。
- 使用自動櫃員機、電話理財、現金存款機。
- 貨幣兌換／現金轉換。

- 兌換籌碼後沒有／僅有少量賭博行為。
- 資金來源不明的外匯交易。
- 涉嫌從事非法金融活動。
- 使用支票／帳戶轉帳等方式轉移資金。
- 可疑電匯。

馬來西亞

馬來西亞金融情報中心發布一份關於 2020 年逃稅之紅旗與態樣報告。這份報告只向申報機關（RI）發放，其目的是：

- 提供關於逃稅的見解和意識，包括其趨勢、技術、方法和管道。
- 加強和促進申報機關對逃稅態樣的意識和理解。
- 協助申報機關從其客戶和相關金融交易所顯示的紅旗／指標中識別逃稅罪行。
- 使申報機關能夠及早發現，以中斷與逃稅相關活動；以及
- 進一步提高可疑交易報告的品質。

菲律賓

摘自 2021 年貨幣服務企業 ML / TF 風險評估報告

貨幣服務業務（MSB）一直被犯罪者為及時轉移還有方便處理其犯罪所得所利用。在菲律賓的第二次國家風險評估中，貨幣服務行業在 ML / TF 的威脅方面被評為高風險，特別是舉 17 家匯款公司和外匯交易商參與毒品販運和非法性交易為例。2016 年最大的銀行搶劫案之一也影響該領域。在該案中，三家匯款公司和外匯交易商協助將 38 億菲律賓披索（75,721,308 美元）從虛設銀行帳戶轉移到賭場、博弈運營商和身分不明的個人。

採取的措施包括修正菲律賓中央銀行的法規手冊和廣泛的註冊程序，這導致該部門的重大重組和整合。雖然貨幣服務業對 ML / TF 風險和 AML / CTF 義務的理解程度在不斷提高，但新架構的貨幣服務業被認為為 AML / CTF 合規提供一個強有力的架構。

為監測及辨別與該領域有關的新風險，防制洗錢理事會在外國金融情報中心的協助和菲律賓中央銀行的支援下，利用交易報告的資料、菲律賓中央銀行的答覆以及相關行業和其他菲律賓政府機關的調查結果，進行一次風險評估。該風險評估應作為監管機關、金融情報中心和執法機關在政策發布和風險基礎戰略方面的指導。

在對交易的分析和對案件的調查中，貨幣服務業提供的某些服務或產品正被犯罪者用於其非法活動。匯款服務和現金交易，包括貨幣兌換處，是轉移犯罪所得的主要手段。

從 2017 年至 2020 年貨幣服務業提交的可疑交易報告來看，剝削兒童、兒童色情、販賣人口、詐騙／詐欺、違反證券交易法等都是報告數量最多的可疑交易。

關於 ML 案件，僅在 2020 年，防制洗錢理事會就促使 7 起案件提交凍結令申請，這些案件涉及非法毒品（4 起）、違反 2000 年電子商務法（1 起）、違反海關現代化和關稅法（1 起）以及違反證券監管法規（1 起）。在上述 10 起案件中，發現十六（16）個貨幣服務業。在這 16 間貨幣服務業中，有 12 個被列為上述案件的當事人。三（3）個貨幣服務業也參與至少兩個案件。來自洗錢案件的收益價值達 2.5869 億批索（520 萬美元）。

資助恐怖主義

傳聞情報和報告之前已經確定貨幣服務業的恐怖主義和 TF。自 2017 年到 2020 年，貨幣服務業共申報 2,007 件可疑交易報告，可疑交易報告估計申報價值為 2,000 萬菲律賓披索（40 萬美元）。貨幣服務業針對恐怖主義和 TF 的可疑交易報告也在增加，與 2019 年相比，2020 年增長超過 350%。

TF 相關資金的常見範圍是 500 至 5,000 菲律賓披索（低於 100 美元）。在防制洗錢理事會恐怖主義和 TF 風險評估研究中[35]，2018 年至 2020 年，獨立的貨幣服務業、電子貨幣發行商與當舖申報 6,000 多份可能與恐怖主義和 TF 有關的可疑交易報告。

涉及國際匯款的恐怖主義和 TF 相關可疑交易報告的受益人的國內地點包括巴西蘭、三寶顏、馬尼拉大都會區和蘇祿。

威脅、新興風險和固有風險的程度和緩解控制措施的可用性顯示，貨幣服務業被犯罪者廣泛用於轉移非法資金，並證明該領域的 ML / TF 威脅等級總體上為中高風險。

雖然有關於使用虛擬貨幣的指控和傳聞情報，但地方或國內恐怖組織仍然主要使用貨幣服務業，在某些情況下，共產主義恐怖組織利用銀行系統轉移和促進與 TF 有關的資金。

可能用虛擬貨幣資助的恐怖主義（TF）活動
來自防制洗錢理事會（AMLC）進行的 2021 年恐怖主義和恐怖主義資助風險評估報告（T / TF RA）。

35 http://www.amlc.gov.ph/images/PDFs/2021%20JAN%20TF%20RA%20EXECUTIVE%20SUMMARY%20（WEBSITE）.pdf

2020 年 5 月的一份報告[36]稱，菲律賓和平、暴力和恐怖主義研究所指出，與伊斯蘭國有關的恐怖組織在菲律賓首次使用虛擬貨幣進行交易，據稱這些貨幣隨後被用於資助在民答那峨島活動之恐怖組織，如印尼神權游擊隊和東印尼真主戰士[37]。

該報告進一步詳細說明瞭虛擬貨幣的使用包括兩個階段：

1）透過不明交易所轉移來源可疑的虛擬貨幣；以及

2）將虛擬貨幣兌換成法定貨幣，並將資金返回到合法貨幣體系中。

報告還稱，位於東南亞之恐怖組織可以在監管機關的監督之外交易虛擬貨幣。由於相對於虛擬貨幣的寬鬆法律架構被視為一種擔憂。該報告特別提到 2017 年的馬拉威恐攻事件，其中有未經證實的報告稱，私人匯款和現金攜帶用虛擬貨幣資助參與上述恐攻之組織。

雖然區塊鏈分析技術被用來解密和追蹤交易，但提昇隱密性的加密服務也被用來掩蓋交易雙方的痕跡。此外，區塊鏈分析無法確定參與交易的使用者，因為註冊電子錢包的個人可以使用假名或改變錢包的加密位址以保持匿名性。

然而，菲律賓已經允許虛擬貨幣作為法定貨幣使用。虛擬貨幣與法定貨幣之間的轉換可以很容易地透過自動櫃員機和其他註冊的匯款和轉帳公司完成。雖然虛擬貨幣轉換為法定貨幣受到菲律賓中央銀行（BSP）的監管，但由於菲律賓身分識別系統（PhilSys）尚未完全實施，監管機關可能發現很難確定參與交易的個人。綜合來看，這些因

---

36 https://thediplomat.com/2020/06/how-terrorists-use-cryptocurrency-in-southeast-asia/

37 https://cointelegraph.com/news/researchers-in-philippines-track-crypto-use-by-terrorists

素為恐怖分子提供足夠的空間，以利用虛擬貨幣達到 TF 的目的。截至 2020 年 11 月 30 日，共有 17 家提供虛擬貨幣兌換服務的匯款和轉帳公司在菲律賓中央銀行註冊[38]。

恐怖主義和恐怖主義資助風險評估報告確定涉及虛擬貨幣交易的個人，他們在 2019 年共被申報 8 起可疑交易，在 2020 年申報 106 起，估計價值為 177 萬菲律賓披索（37,027 美元）。報告的可疑交易顯示虛擬貨幣的使用正在興起。

新加坡

新加坡恐怖主義資助國家風險評估報告（TF NRA）

新加坡於 2020 年更新恐怖主義資助國家風險評估報告（TF NRA）：

恐怖主義資助國家風險評估是對過去幾年所有相關主管機關的經驗和意見的整理，並包括來自私部門和學術界的投入。其旨在進一步加深執法機關、監督者／管理者和私部門對新加坡面臨之恐怖主義主要的威脅和弱點的瞭解，以便採取適當的預防和抵減措施。

恐怖主義資助國家風險評估報告發現：

- 新加坡持續面臨恐怖組織在其區域內和國際範圍內構成的 TF 威脅，特別是新加坡的個人有可能激進化並被影響進而開始 TF 活動。
- 某些領域，特別是匯款（或提供跨境匯款服務的支付服務提供商）和銀行，由於相對容易獲得其服務，再加上新加坡作為金融和交通樞紐的地位，以及靠近有恐怖主義活動的司法管轄區，因此更容易受到 TF 威脅。

---

38 https://www.bsp.gov.ph/Lists/Directories/Attachments/16/MSB.pdf

7.2 洗錢與資恐之類型與前置犯罪（例如恐怖組織、恐怖分子訓練、貪汙、毒品、詐欺、走私等）

孟加拉

孟加拉網路賭博現況

本研究報告發表在孟加拉金融情報中心年度報告中。

孟加拉金融情報中心收到 20 份來自外國金融情報中心之自發情報報告。每份報告都描述孟加拉國民參與線上遠端賭博的情況。這 20 名孟加拉國民在馬爾他註冊的線上賭博公司註冊帳戶。他們透過 Neteller、Skrill、Moneybookers 等存入與出金賭博帳戶資金。這些金融情報中心還通知孟加拉金融情報中心，由於缺乏關於資金來源的資訊，以及這些人高流量現金存款，賭博公司已經關閉他們的帳戶。

分析中發現，一些賭徒在開戶時提供偽造的身分資訊，因此無法被追蹤。每個玩家的 IP 位址都被追蹤至世界上許多不同的司法管轄區。看來他們很可能使用虛擬專用網路，為他們的身分無法被追蹤。在帳戶被關閉之前，這些玩家的帳戶運作 1 至 4 年。這些玩家主要在體育博彩公司下注和玩賭場遊戲。這 20 名玩家存入資金總額為 39,77,141 美元，提款總額為 27,09,154 美元。在某些案例，發現賭徒在孟加拉有銀行帳戶。這些案件被轉交給孟加拉警方刑事調查部（CID）進行進一步調查。在一些案件中，刑事調查部回饋說沒有發現針對賭徒的具體證據。

賭博在孟加拉是一種被禁止的活動。1867 年的聚眾賭博法中也有對賭博的嚴格法律制裁。儘管禁止賭博，但大量的孟加拉人正在使用線上賭博網站。還有一些人參與付費遊戲的線上遊戲。這些遊戲透過身分盜竊和盜取帳號、詐欺，甚至作為 ML 及 TF 的幌子（因為它們依賴於

使用者在遊戲生態系統中的付費遊戲），引發網路犯罪。因此，洗錢和防制洗錢當局必須追蹤個人如何將資金用於線上遊戲和賭博。法律上來說，線上賭博帳戶不能透過銀行管道載入資金。此外，Neteller、Skrill、Moneybookers、Paysafe 或這類電子錢包（電子貨幣服務提供商）的使用在孟加拉是不合法的。另一方面，賭博者／玩家必須向其賭博帳戶存入資金才能進行遊戲。因此，他們使用另一種管道，即哈瓦拉／亨遞向他們的帳戶存款，大多數賭徒使用 Neteller、Skrill、Moneybookers、Paysafe 等服務對多種貨幣。

一個想在網上賭博的人在 Neteller、Skrill 或其他公司開帳戶，或找人代勞。然後，他們與手上擁有美元的人取得聯繫，比如說一個為外國客戶工作的自由職業者。他用當地貨幣支付給自由職業者，然後自由職業者要求他的客戶將部分服務費支付到屬於該賭徒的 Neteller 或 Skrill 帳戶中。這就是數位／電子貨幣錢包被載入並用於支付賭博的方式。有代理／中介機關從不同的准賭徒／賭徒那裡收集資金（通常透過 Bkash 等數位金融服務），並利用多個個人將資金注入這些電子錢包帳戶。此外，在 Facebook 上搜索發現，PaymentBD.com 等幾個網站宣傳 Neteller、Skrill 和其他類似電子錢包帳戶。按照 PaymentBD.com 的說法，他們可以經 Neteller 帳戶使用美元。

與線上賭博有關的情報報告是在相關帳戶被關閉後才收到的。不難推測，還有許多賭徒還在線上賭博。由於資金是透過哈瓦拉／亨遞從孟加拉抽走的，因此已採取舉措，與外國金融情報中心溝通，收集仍在賭博的賭徒其資訊，並與執法機關密切合作，確認嫌疑人身分。

中華臺北

案例一：

W 先生是 S 公司的董事長，從 2017 年 6 月開始，他雇傭不少員工來經營一系列網上賭博網站，其中包括 G1 網站、G2 網站和 G3 網站。為清洗賭博資金，W 先生使用大量錢騾的帳戶，這些帳戶是從一家暱稱為 KT 的未知公司在 X 司法管轄區開設的，並將資金分層存入三個不同的帳戶。第一層帳戶直接接收賭徒的賭博資金。當帳戶中的資金積累到一定程度時，W 先生再將這些錢轉入第二層帳戶，依次轉入第三層帳戶。為掩蓋犯罪所得，W 先生隨後借用一些朋友的個人帳戶，用以承接資金。據估計，2017 年至 2020 年期間，這些帳戶共收到 6 億外幣（93,190,941 美元）。

為從賭博業務中攫取更多的利潤，W 先生還聘請工程師開發一個第四方支付系統，將服務與第三方支付機關整合，並從收取服務費中獲益。例如，第三方支付供應商收取總賭金的 3.2% 的服務費，如果有某個賭場網站願意支付 3.5% 的費用，W 先生的系統將匹配雙方，並將 0.3% 的費用歸作淨利。

地方檢察署於 2020 年 8 月以違反刑法和洗錢防制法的罪名起訴 W 先生及其同夥。

案例二：

A 君自 2010 年起成立世紀王朝、贏世紀等短線公司，在 X 司法管轄區、Y 司法管轄區、Z 司法管轄區等地從事非法斂財活動。詐騙金額超過 1 億元人民幣（15,532,009 美元）。由於發生多起投資詐騙案件，國際刑警組織於 Z 司法管轄區於 2018 年 5 月 15 日發布紅色通緝令，國際刑警組織 X 司法管轄區中央局于同年 7 月 25 日發布藍色通緝令，有大量受害者來自 X 司法管轄區、Y 司法管轄區和 A 司法管轄區。A 君於 2019 年 12 月 31 日入境中華臺北。由於新冠病毒的爆發，他沒有離開該司法管轄區。在台中逗留期間，他於 2020 年 5 月 14 日被警方查獲。

在警方、國家情報局和 X 司法管轄區當局的共同合作下，A 君於 5 月 16 日被遣返到 X 司法管轄區。

根據 X 司法管轄區的資訊，A 君涉嫌自 2015 年起在 Z 司法管轄區參與商業犯罪，金額達 672,000 美元。此外，他還在 X 司法管轄區參與幾起投資詐騙案，初步估計金額為 135 萬多外幣（209,663 美元），總金額折算為 3,000 多萬新臺幣（1,068,154 美元）。A 君作案後滯留海外，往返於中華臺北、X 司法管轄區內等地。2019 年 6 月，A 君的配偶從 X 司法管轄區來到中華臺北與 A 君短暫會面。2020 年 2 月 24 日，X 司法管轄區當局為逮捕 A 君，取消他的護照，並請求周邊司法管轄區的協助。A 君因投資詐欺分別被 Z 司法管轄區和 X 司法管轄區通緝。他們擔心他在中華臺北拘留期間會從事新的詐欺，危及經濟秩序和損害人民的財產。在找到 A 君後，刑事警察局立即於 2020 年 5 月 14 日在台中市找到他。

印尼

在 2016 年至 2020 年印尼的 ML 犯罪方面，執法人員給出他們對各種態樣的洗錢犯罪風險看法。根據執法人員處理與 ML 有關的案件的經驗，對 ML 犯罪的全部態樣進行評估。

出現頻率最高的五種方法依次為：

- 使用偽造身分。
- 轉移到財產資產／不動產。
- 使用人頭或借名，如家庭成員、為犯罪者服務之人或其他受信任的人的名字。
- 化整為零；以及
- 拆分交易。

a. 使用假身分

在許多案例中，得以使用偽造身分是由於單一身分證號碼的機制失效，使同一人可在不同區域持有不同的身分證或偽造的身分證。然後，無效的身分證被用來開設帳戶，以清洗犯罪所得。下一個弱點是各區域或鄉鎮級官員作為記錄申請身分證的公民資料的官員誠信問題。如果各區域或鄉鎮級官員在製作身分證時在行政上出現錯誤，那麼可以認為作為製作身分證原材料輸入的資料也是無效的。

例如，被判犯有貪汙罪的 A 君逃到國外，並已經改變國籍，他想回到印尼，並與區域負責人勾結，偽造自己的身分證。這導致該區域負責人被免職。

b. 利用物業公司或物業代理

透過不動產進行洗錢的比例很高，這是因為銀行業的監管比較嚴格，相反，對不動產領域所進行之洗錢監管比較薄弱。銀行業更嚴格的監管使得犯罪者尋找其他地方來儲存他們的犯罪資金，其中之一就是不動產。出於這個原因，印尼加強其在不動產領域防止洗錢的法規，即 2010 年第 8 號關於防止和根除洗錢的相關法律（TPPU 法）和 2015 年第 43 號關於防制與根除洗錢犯罪的報告方的政府條例（第二條例）。TPPU 法要求不動產公司或不動產代理公司向印尼金融交易報告和分析中心（PPATK）提交以任何貨幣進行的價值相當於 500,000,000 印尼盾（35,020 美元）或以上的交易的可疑交易報告。第二條規定要求不動產交易公證人（PPAT）也要向印尼金融交易報告和分析中心報告與不動產買賣相關的可疑金融交易。

c. 使用人頭（借名）、信託、家庭成員或其他第三方

根據印尼金融交易報告和分析中心 2019 年研究，在目前正在進行

法律程序的 174 起 ML 案件中，有 50 起使用人頭之態樣，而在 2020 年，在 86 起 ML 案件中，這一數字為 58 起。這顯示，使用人頭進行 ML 的趨勢在增加。這種態樣傾向於頻繁發生，它不僅涉及家庭成員，還涉及犯罪者同夥。核心家庭成員很容易被執法人員追蹤到，因為他們被列在 KK（戶籍謄本）上，但如果此人在核心家庭之外，調查就比較困難。犯罪者通常透過使用為他們工作的人的身分，如司機、幫手和其他雇員。基本上，使用人頭是試圖透過使用被犯罪者信任的另一個人的名字來消除犯罪行為所得的痕跡。也有可能使用人頭來掩蓋合法商業法人實體的實際所有權。

d. 化整為零

化整為零是指透過使用不同名稱的多個帳戶將非法交易分解成多筆交易來進行掩飾。這種態樣仍然可以與使用人頭收取犯罪所得的行為有關。行為人在一定時期內使用許多不同名字的帳戶進行交易。通常情況下，這些化整為零所用帳戶的所有者會因為出借他們的個人帳戶而得到報酬，帳戶所有者不一定知道帳戶中的交易發生在哪裡以及出於什麼原因。

e. 拆分交易

拆分交易是指以相對較小的金額進行的交易，但其頻率很高，以掩蓋較大的交易。這種態樣的交易通常被用來規避設置在現金交易報告門檻或以下的可疑交易限額。通常情況下，犯罪者會將交易分割成低於該限額的名義價值，這樣就不會出現被認為是可疑交易。有時拆分交易是在購買奢侈品時進行的，在本案中是購買一輛豪華汽車。這種犯罪的行為人利用金融服務來購買汽車，然後行為人將每月存入資金作為購買豪華汽車的分期付款。

在各個領域，不僅在金融部門或金融服務供應商或貨物供應商內部，而且在專業領域，洗錢現象越來越普遍。通常採用的操作方式是將專業人員或機關作為洗錢的中間人。這裡的專業服務包括律師、公證員、不動產交易公證人（PPATs）、會計師、公部門會計師和財務規劃師。所提到的專業服務是洗錢犯罪者隱藏或掩飾犯罪行為所產生的資產來源的一種手段，他們以根據法律和法規的規定對與服務使用者的專業關係以保密規定為由進行掩護。

在許多情況下，專業服務提供商參與 ML 犯罪者的犯罪行為，如 A 君的案件中，律師也因違反反貪汙法和刑法而被警方逮捕。在一審和上訴法院階段，律師 B 被認定與犯罪嫌疑人、前人民代表大會（DPR）議長 A 一起妨礙 e-KTP（身分證）貪汙專案的調查，A 本人也違反反貪汙立法和刑法。甚至其他專業服務機關、像是醫生，也被指控與律師相同的罪名，因為他們被認為是阻礙調查。雖然在這個案件中，律師沒有被證明與洗錢犯罪有關，但至少可以看出，專業服務機關非常容易被捲入主要案件的背景。

g. 新興支付方式

技術的快速進步已經改變許多事情，包括金融服務的世界。市場不再是一個實體市場，已經轉變為一個線上市場。不僅是商品，各種服務也已經在網上銷售。因此，網上支付也是對網上市場支援。交易變得更加容易，人們不需要親自走到市場，也不需要親自付款。線上支付應用，無論是作為銀行服務產品的一部分，如手機銀行和網上銀行，還是透過許多金融科技公司（Fintech）提供的線上支付服務，如電子貨幣和電子錢包，在過去五年中變得越來越流行。它們的使用也成功地迅速推進到中小型企業去。銀行業是受到高度監管的行業之一，而這與金融科技行業形成鮮明對比，後者仍然是新

事物，自然監管也沒有那麼全面。事實上，許多金融科技公司提供開戶、支付、甚至投資的便利。

一般來說，銀行的行銷仍然是透過各銀行分行直接進行，而金融科技公司則是在網上作行銷，不需要和消費者面對面，這意味著監管較弱。開設電子錢包的程序只是用自己的照片、KTP（身分證）和電話號碼進行操作，沒有任何物理驗證或其他方式。一方面，它更容易服務消費者，但另一方面，人們擔心它可能被濫用於 ML。金融技術世界中的違規行為以及在其中進行交易的便利性，使得這種態樣被執法機關認為是一種高風險的 ML 手段。

h. 使用公司（法人實體）

" 官方 " 公司經常被用作幌子，成為洗錢的載具，即利用公司來掩蓋犯罪所得，作為公司的合法收入。說它是 " 官方 " 公司，是因為從法律的角度來看，這個公司是正式、符合法規的。犯罪者通常有許多公司從犯罪所得中收集資金，或準備作為洗錢的一種手段。這樣做是為掩蓋資金流動的痕跡，因為在董事會上正式列出的名字或公司股份的所有者並不是實質受益人（BO）。不符合標準的實質受益人資料也是這種態樣的主要弱點之一。在開設公司帳戶時，如果只使用合法的、正式的公司證書，而沒有任何其他資訊，甚至銀行部門也不能輕易發現實質受益人其真實姓名。

2020 年 1 月 17 日，雅加達貪汙犯罪法庭的審判中向公眾披露主要犯罪者 M，其貪汙模式之一是成立一家名為 P 的公司，該公司使用一個人的名字，而這個人實際上是為公司的一名董事擔任私人司機。這個司機 O 為一個與 M 君密切相關的人，即 P 個人工作，他只是借用自己的身分作為建立公司和簽署合約的條件。O 君對以他為董事的公司名義進行的拍賣過程一無所知。這一態樣也包含前面

討論的人頭態樣。這個司機的身分被借用，成為一個實際上不屬於他的公司的假董事，儘管該公司的活動他並不知道。O 君為某人工作的職位讓他別無選擇，只能聽從雇主的命令。

TF NRA 文件（2019 年更新）描繪國內的 TF 風險，包括：

a. 募資階段

- 向恐怖組織捐款案例。

  根據 MTR 的命令，HZ 君以其妻子的名義，即 RWI 在 A 銀行開設一個帳戶，提供後勤援助，該帳戶旨在接收由 Santoso（別名 Abu Wardah）領導的 MIT 組織成員的捐款，以食物和山上訓練所用工具的形式幫助 Santoso 在波索縣山區的逃亡鬥爭，總金額為 49,600,000 印尼盾（約 3,480 美元）。

- 合法來源的自籌資金

  案例：

  NNG 自費為包括他自己在內的七個人提供便利，以 590,000,000 印尼盾（約 41,000 美元）的價格出售他在東雅加達的房子，這筆錢從買方的 B 銀行帳戶轉帳到 NNG 的 C 銀行帳戶。然後將這筆錢與出售家居用品、汽機車和出售女裝所得的錢加在一起，共計 33,200,000 印尼盾（約 2,300 美元）。所有這些資金全用來以購買機票和電子簽證的形式，來資助包括 NNG 在內的七個人。

- 透過社交媒體捐款

  案例：

  2016 年 6 月初，BA 有來自於賣毒品的錢，想用來製造炸彈，這個想法透過他的 Facebook 郵件收件箱以 BA 的名義和 F 君的 Facebook 帳戶傳達給 HB 的 Facebook 帳戶。然後，BA 從

Facebook 上的朋友那裡籌集 32,800,000 印尼盾（約 2,300 美元）的資金，作為製造安非他命的資金，賣錢後用於資助製造用於恐怖行為的炸彈。

b. 資金轉移／移動階段

- 國內和跨境攜帶現金

案例：

AX 根據 BA 的命令從 AG 處收到 80 萬印尼盾（56 美元）的現金，BA 是恐怖組織東印尼真主戰士（MIT）的成員，目的是購買製作炸彈的材料，在中蘇拉威西省坡蘇縣的潘坦古垃巴村引爆炸彈。此外，AX 還以 WW 的名義用他們在 D 銀行的帳戶向錫江東印尼真主戰士的成員募集資金，存款金額分別為 10,000,000 印尼盾、5,000,000 印尼盾和 3,000,000 印尼盾（約 700 美元、350 美元和 200 美元）。

- 匯款

案例：

2016 年，AP 被 AJ 要求透過非銀行牌照機構匯款給 SM，使用一個 X 司法管轄區公民的名字，匯款總額為 150,000,000 印尼盾（10,536 美元），資金用於購買發生在雅加達市中心塔林大街恐攻事件所用之槍支彈藥。

- 銀行

案例：

根據 BN 先生的命令，2016 年 3 月左右，MK 先生收到轉到屬於 MK 妻子（PA）的 X 銀行帳戶的錢，金額為 6,000,000 印尼盾（約 400 美元），並被要求使用該帳戶將錢轉到 AH 的 Y 銀行帳戶，

金額為 800,000 印尼盾（約 53 美元），6 月底轉到 DA 的 Y 銀行帳戶，金額為 2,000,000 印尼盾（約 180 美元），7 月初為 2,000,000 印尼盾（約 140 美元）和。所有這些資金都用於蘇拉卡爾塔警察局的自殺式爆炸事件。

c. 資金使用階段

- 購買武器和爆炸物

  案例：

  根據 S 先生的要求，DN 先生透過使用非銀行牌照機構的匯款方式，將恐怖組織東印尼真主戰士支持者捐助的資金匯往 X 司法管轄區購買武器，即：2015 年 3 月 5 日，金額為 5,000,000 印尼盾（約 350 美元），2015 年 3 月 26 日，金額為 16,150,000 印尼盾（約 1,130 美元）。隨後，DN 先生前往 X 司法管轄區取回已購買的武器，費用為 2,000,000 印尼盾（約 140 美元）。

- 維持恐怖主義網絡

  案例：

  根據 BS 先生的命令，HD 先生建立一個小型小組來進行恐怖活動，所使用的資金是從支持者那裡得到的資金。這些資金被用來資助組建其他新小組。

- 恐怖組織成員移動和外國恐怖主義戰士旅行

  案例：

  AP 為促成 12 次外國恐怖主義戰士的旅行，使用屬於各集體代表的 Z 銀行白金自動提款卡，其自動提款卡被用來購買前往 Y 司法管轄區和 X 司法管轄區的機票，並透過轉帳支付電子簽證，總額為 468,376,080 印尼盾（約 32,910 美元）。

- 軍事訓練

  案例：

  根據 AT 先生的指示，SU 先生透過 WA 先生的 N 銀行帳戶向 O 銀行轉帳 2,000,000 印尼盾（約 140 美元），用於 MD 先生的軍事訓練，還多次向 AZ 先生的 P 銀行轉帳，每次 3,000,000 印尼盾（約 200 美元）。此外，在 AT 的指示下，SU 先生被要求向 MD 和位於塔曼吉卡的城鎮波索的成員發送資金，用於購買一台攝影機，費用為 2,500,000 印尼盾（約 175 美元）。

- 恐怖分子家庭補償

  案例：

  恐怖分子或恐怖組織籌集的資金被分配給恐怖組織成員的妻子，這些人有的是因被警察槍殺而死亡、有的是被有期徒刑、有的是因被警方列入通緝名單（DPO）而逃亡，有的是在波索為加入恐怖組織而搬離的個人。

中國澳門

來自中國澳門的夫婦因參與詐欺、偽造和洗錢被捕

金融情報辦公室收到的幾份可疑交易報告顯示，一家教育中心與一起詐欺案有關。該教育中心由一對來自中國澳門的夫婦經營。經檢查該公司的帳戶資料發現，該教育中心的銀行帳戶在 2016 年 8 月至 2017 年 8 月期間收到中國澳門持續進修發展計畫的政府補貼，金額近澳門幣 4,680,000 元（約 58.5 萬美元）。然而，這些資金主要是以現金形式提取的，還有一小部分是從中國澳門及一家婚禮策劃公司轉給這對夫婦的。資料顯示，該婚禮策劃公司也是由這對夫婦擁有，他們的資金來源主要是透過自動櫃員機或場外交易的現金存款，然後向其他第

三方發出出納單。

透過分析帳戶交易模式，金融情報辦公室發現，該公司的帳戶在 2016 年 8 月之前只進行少量的交易。大部分交易發生在 2016 年 8 月至 2017 年 8 月期間，資金主要以現金形式提取，不符合正常商業慣例。此外，金融情報中心發現，這對夫婦與過去的詐欺行為有關。因此，金融情報辦公室將這些案件移交給人民檢察院。

人民檢察院隨即要求司法警察對案件進行調查。經查，該案與 2017 年 2 月和 2019 年 6 月連續發生的婚宴押金和騙取持續進修發展計畫補貼的詐騙案有關。這對經營婚禮策劃公司的夫婦在兩年內騙取 40 多名客戶的婚宴訂金，總額達 500 萬澳門元（約 62.5 萬美元）。在同一時期，他們擁有一個教育中心，並獲得澳門幣 14 萬元（約 17,500 美元）的政府補貼，但實際上沒有舉辦任何形式的教育課程，並偽造學生的出勤紀錄。

在對這兩宗案件進行後續調查後，發現妻子多次透過婚禮策劃公司的帳戶，將總計 330 萬港幣（約 424,936 美元）的涉嫌詐騙收益匯入丈夫及其兄弟在附近地區的銀行帳戶。這些資金被進一步匯入其他銀行，並被用於簽發支票和償還信用卡貸款，以清洗犯罪所得。

此外，在對嫌疑人的銀行帳戶交易進行財務調查時，司法警察發現嫌疑人在 2017 年申請 223 萬港幣（287,160 美元）的房屋貸款時向銀行提交偽造的收入證明和偽造的存摺等文件。

2020 年 5 月，司法警察調集人員前往嫌疑人的住所，並將他們帶回調查。嫌疑人否認犯有該罪行。然而，他們未能對司法警察的調查結論作出合理解釋。因此，司法警察將他們移交給人民檢察院，罪名包括詐欺、偽造文件和洗錢等三項罪行。

馬來西亞

正如2017年國家風險評估（NRA）所確定的，詐欺、貪汙、非法販毒、組織犯罪和走私仍然是管轄範圍內的主要犯罪，這主要歸因於可疑交易報告和調查的進行方能確定。目前，馬來西亞正在最後確定其2020年的國家評估，涵蓋自上一輪國家評估以來的ML及TF的趨勢和模式。2020年國家風險評估旨在確定、評估和瞭解司法管轄區內的洗錢/TF風險，包括威脅和部門固有風險、控制措施、相關新趨勢以及部門和威脅評估之間的相互聯繫。

關於非法販毒，馬來西亞皇家警察（RMP），曾在2020年1月查獲價值3.66億令吉（88,812,328美元）的資產，這些資產與調查2019年9月查獲的用於走私12噸古柯鹼的公司帳戶有關，價值24億令吉（582,375,921美元）。這些古柯鹼與木炭混在一起，以避免被發現，據信是來自一個利用馬來西亞作為過境司法管轄區的國際毒品集團。隨後，包括6名外國公民在內的8人因販運危險毒品被指控。

調查顯示，主要由一個龐大的公司網絡和一名擔任上市公司董事長的商人參與。該商人是仍然在逃的主要嫌疑人的代理人，被確認為與他的同夥擁有幾個聯合帳戶。2012年至2020年期間，這些帳戶收到來自全國各地的大量現金存款，這些存款交易以低於申報門檻的方式每天都在進行，並且還有來自許多公司的資金轉移，包括那些與他的一家上市公司有關的資金。這些資金在聯合帳戶之間傳遞，隨後提取給各公司和個人之前形成多層化交易。此案例顯示，大量資金被用於購買犯罪嫌疑人、親屬和代理人所擁有的房產、股票和車輛。

巴基斯坦

恐怖主義資助：聯合國安理會第1373號決議的制裁對象

XYZ 先生的交易活動被視為可疑的，因為他與一被禁止制裁組織有關連，而在 2020 年 10 月被列入 1997 年反恐怖主義法（聯合國安理會第 1373 號決議）附表四的 A 類（恐怖主義）。

根據聯合國安理會第 1373 號決議的規定，不同銀行對 XYZ 先生的個人和商業帳戶提交可疑交易報告。根據實名認證文件，他是唯一的經營者，在鄰近司法管轄區邊界附近的恐怖主義重災區從事果乾和傭金代理業務。根據海外巴基斯坦人國民身分證（NICOP），此人是海外巴基斯坦人，且其戶籍地址在該司法管轄區內受恐怖主義影響的地區。在根據聯合國安理會第 1373 號決議對該人進行取締後，金融監控中心從不同銀行收到多份可疑交易報告。

經過分析，發現嫌疑人在司法管轄區的不同城市開設多個個人、企業和聯合帳戶。總的來說，在八個不同的銀行發現 14 個帳戶。此外，在過去三年裡，在取締前的帳戶中發現大量交易活動，資金流動迅速。交易活動顯示，資金透過現金和內部轉帳與無關的交易方進行交易，顯示 XYZ 先生參與哈瓦拉／亨遞業務。這些帳戶在該人被制裁後被銀行凍結。

在對 XYZ 先生交易對手的帳戶進行分析後發現，他的一個交易對手 A 先生是從事廢品、布匹和乾果業務的製造交易業務的經營者，因涉嫌參與哈瓦拉業務，已被金融監控中心移交給執法機關調查。從事糧食和果乾生意的 HAC 公司老闆 B 先生也已被執法機關調查，並因與聯合國安理會第 1267 號決議被指名之個人有聯繫而被列入通緝恐怖分子紅皮書。同樣，許多其他交易方也被懷疑參與哈瓦拉交易。

鑒於上述分析，人們懷疑此人可能參與哈瓦拉／亨遞的非法業務或利用這一管道轉移資金。此外，他被列入 1997 年反恐怖主義法附表四，

因此，不能排除他參與資助恐怖主義的可能性。該金融情報已與相關執法機關分享，以便對此事進行調查。此事正在調查中。

7.3 新興趨勢；遞減趨勢；持續趨勢

斐濟

新興趨勢

金融情報中心注意到，越來越多的個人使用替代技術和管道向其他個人轉移資金。這包括使用斐濟郵政電匯（TMO）和 Paypal。在某些情況下，人們注意到，使用這些替代技術和管道是為故意避免被發現。

2021 年，報告的非法層壓式推銷案件也有所增加。

持續趨勢

金融情報中心觀察到，直至 2020 年持續發生人們落入各種網上詐騙成為受害者。網路犯罪者利用當前的全球 Covid-19 局勢，向社會上的弱勢部門提供偽造貸款、包裹和關係，這些人向這些網路犯罪者匯出數十萬美元。

印尼

新出現的威脅是一種還沒有被相關部門所緩解的新洗錢模式。從最近發生的幾起募資案件中發現，有一些募資模式可能成為新的威脅，包括電子商務交易，特別是為買賣帳戶提供便利的初創公司。

a. 沒有嚴格的法規來懲罰代人銷售和購買以及使用帳戶的行為

   與網上銷售有關的詐欺行為越來越多。有一種方法涉及線上帳戶交易。透過某些電子商務／市場在網上進行的銷售和購買是以非法的帳戶進行，使實際擁有該帳戶的客戶受害。在帳戶買方成為受害者的情況下，通常賣方針對的是不瞭解購買該帳戶所涉及風險的

目標。大多數被出售的帳戶是屬於他人的封鎖帳戶或二手帳戶。在買方為犯罪者的情況下，更可能是為濫用或是為存留詐騙而得的資金。比較合理的情況是，如果客戶真的需要帳戶用於個人需要，而不是用於犯罪，他們會發現以自己的名義開立帳戶更容易。以上是與買賣和使用他人帳戶的普遍性有關的一些事實。

b. 針對電子商務和金融科技行為的監管法規有限

金融科技行業的快速增長和發展引起人們的關注。它所擁有的簡單性和實用性似乎是一把雙刃劍。這種擔憂源於監管機關缺乏與實施 AML 與 CFT 主義計畫有關的明確規定。

同時，技術發展的現狀，加上預防和消除 TF 支持的成果，導致恐怖組織繼續尋找新的替代路線，以往往難以發現和追蹤的方式尋求資助恐怖主義，包括：。

- 使用或濫用公司／企業

  透過合法的公司，恐怖組織可以利用金融設施和金融服務提供商來收取、轉移和使用資金，使其看起來像是普通的商業交易。執法機關成功揭露的 B 君犯下的資助恐怖主義的犯罪行為顯示，恐怖組織擁有油棕櫚種植園來資助他們的活動。

- 非法毒品

  根據聯合國毒品和犯罪問題辦公室（UNODC）的說法，在籌集資金以支援恐怖主義行為時，恐怖組織可以依靠，包括銷售非法毒品等傳統的犯罪活動，或通常被稱為毒品恐怖主義。聯合國毒品和犯罪問題辦公室關於阿富汗存在的毒品恐怖主義報告顯示，這與印尼透過犯罪管道資助恐怖主義的發展有關聯，而且在透過銷售非法毒品資助恐怖主義方面存在著潛在的新威脅。

- 虛擬貨幣

由金融科技公司領導的技術 4.0 的發展導致了虛擬貨幣籌資模式的出現，就像發生在 E 君在恐怖主義籌資中使用比特幣的情況一樣。虛擬貨幣的特點包括交易處理速度快，交易費用低，相對容易；然而，它們很容易被犯罪者利用，因為它們允許在不使用真實姓名的情況下進行交易，沒有報告義務，有些不需要第三方中介機關來完成交易。

- 線上貸款

以線上貸款形式出現的金融技術使人們很容易在很短的時間內獲得所需的資金，而且手續簡單。然而，技術的便利性也影響客戶線上貸款的便利性，因此可能被恐怖組織所利用。

- 透過社交媒體（眾籌）募資

透過社交媒體或眾籌募資，特別是在疫情流行期間，如為購買醫療設備籌集資金，可被恐怖組織用來資助恐怖主義。此外，社交媒體帳戶很容易利用匿名／假冒／他人的帳戶創建，這使得利用社交媒體傳播籌資資訊變得越來越頻繁。

在 2020 年 NRA ML 初步文件中，有一些技術和戰略問題被認為對決定未來消除和預防 ML 的有效性很重要，包括以下內容：

a. 國家和政府菁英們對所有洗錢前置犯罪的執法重要性的關注、意識和擁護仍然有限。對 ML 的優化可以導向“使犯罪行為成本上升”的作法，犯罪者在施行犯罪前會因更嚴重的後果而考慮再三。
b. 一些執法機關透過建立一個特別單位或 ML 工作小組，顯示他們對支持防制洗錢制度的承諾。

c. 防制洗錢調查員數量有限，各機關之間協調模式不足，特別是與林業和環境領域的案件有關，這些案件往往止于外地的行為者。
d. 有必要強化法律與人權部中負責司法互助的機關的品質，以提高協調和合作的有效性，並消除主管機關之間不願意分享資訊的現象。
e. 缺乏一綜合資料系統或某種大數據分析，以說明執法、監督和監管機關以及報告方優化其識別、監測和緩解與洗錢有關的實質受益人和重要政治性職務之人風險的能力。
f. 缺乏一個可以由防制洗錢制度權責相關者實施的綜合 ML 分析資料系統。
g. 要優化與企業和個人施行 ML 犯罪有關的舉報系統，該系統以企業對可能發生的 ML 的識別為基礎。

中國澳門

持續趨勢

網路詐騙

2020 年上半年，與網路有關的詐騙案件之趨勢仍然值得關注。詐騙案件主要透過網路發生，涉及投資詐騙、戀愛詐騙等。有時當地銀行會收到訂閱銀行的電話資訊或受害者的電子郵件，聲稱相關匯款與詐欺行為有關。透過執法機關的持續宣傳，一線銀行工作人員也會提醒疑似受害者在向第三方帳戶匯款前要三思而後行，並對欺騙行為保持警惕，以避免因詐騙而損失金錢。

馬來西亞

持續趨勢

在 2017 年至 2020 年期間，犯罪者利用錢騾帳戶進行金融詐騙，特別是電信詐騙，在馬來西亞仍然很普遍。最近還有跡象顯示，跨國詐欺／洗錢集團利用國內和離岸註冊的公司，透過各種詐欺計畫轉移或多層化資金，包括商業電子郵件詐騙（BEC）、個人防護設備（PPE）詐欺等。馬來西亞金融情報中心收到的與詐欺有關的可疑交易報告的增加以及去年的公眾投訴顯示，由於 COVID-19 的流行，犯罪集團利用民眾糟糕的財務現況，詐欺計畫變得更加突出。這些詐騙計畫的作案手法繼續演變，公司和個人利用非常規方法，如非銀行匯款服務提供商、電子貨幣發行商和虛擬資產來清洗這些詐欺計畫的收益。更為複雜的騙局涉及多個司法管轄區的網路，而且還出現使用先進技術的情況，如網路電話等欺騙技術和使用移動網路而不是 WiFi 來避免追蹤 IP 地址。

越南

目前，4.0 技術革命已經對經濟的各個部門產生巨大影響，尤其是在銀行和金融領域。相應地，出現許多態樣的支付中介，包括電子錢包和虛擬貨幣，為消費者的交易和商品買賣的支付創造有利條件。然而，這些支付形式也有被犯罪者用來進行洗錢和資助恐怖主義活動的潛在風險；其中，行動支付是具有許多潛在風險的服務之一，由於其匿名性、難以控制和快速執行等特點，會被犯罪者用來進行洗錢活動。

8. 防制洗錢／打擊資恐對策之影響

報告此一部分簡要介紹立法、監管或執法防制措施的最新成果。

8.1 立法或監管之發展對偵查和／或特定預防方法（例如追查犯罪所得、資產沒收等）

澳洲

在 2020 年 8 月紐西蘭基督城清真寺槍手 A 君被定罪後，紐西蘭政府對 A 君實施針對性的金融制裁，澳洲外交貿易部也在不久後對他實施類似的制裁。

中華臺北

2018 年 11 月 7 日，中華臺北透過資恐防制法（CTF 法）。該修正案確保目標性金融制裁的範圍適用於被指定之個人、法人或法人實體的代理人，或代表被指定之個人和法人實體或在其指示下行事的其他法人實體，以符合國際法規。2018 年 3 月 31 日，中華臺北對公民 A 實施目標性金融制裁，並在上述修訂後凍結 A 所控制的法人實體的資產。

此外，2019 年 2 月 1 日，中華臺北透過主管機關辦理特定財團法人洗錢及資恐防制辦法。該條例規定，對於從事慈善、文化、教育、社會、聯誼會等其他類似態樣的有益於公眾的目的而籌集或支付資金，並被主管機關透過風險評估程序列為高風險之財團法人基金會，主管機關應採取適當措施進行監督，避免這些基金會被濫用 ML / TF。此外，地方檢察署於 2020 年 9 月起訴 B 君及其同夥違反資恐防制法，涉及向北韓非法出售石油。這是中華臺北首次提出的此類起訴案件。

中華臺北

金融監督管理委員會已要求銀行公會於 2020 年 3 月 24 日將銀行辨識實質受益人實務參考作法發給金融機構參考。

關於加強執法機關和私部門之間的合作，金融監督管理委員會已要求相關金融業公會定期舉辦合規論壇。例如，銀行公會已邀請執法機關分享金融科技和新出現的犯罪態樣和案例，並邀請金融機構分享其識別實質受益人和金融集團的實務做法，以便在 2020 年分享防制洗錢／打擊恐怖主義資訊。

這些措施可以使金融機構更好地瞭解風險和威脅，有效協助執法機關調查犯罪所得。

2020 年，金融監督管理委員會修訂防制洗錢／打擊恐怖主義調查問卷，並在 2021 年初更新金融機構的風險評級和風險概況。

金融監督管理委員會將繼續實施其防制洗錢及打擊資恐策略藍圖，審查相關法規以符合國際標準，並監督金融機構遵守防制洗錢相關法規，實施防制洗錢／打擊資恐工作。

中華臺北目前正在起草一份草案，將第三方支付服務業在處理具體業務時納入洗錢防制法（MLCA）第 5 條第 3 款的 DNFBP，並將發布有關內部控制制度、稽核制度、身分驗證機制、特定服務的紀錄保存、可疑交易報告申報以及所有關於指定受制裁個人和法人實體的報告規定。

斐濟

2019 年 3 月，在斐濟警方搜索可能的非法藥物時，發現 B 君持有 28,000 斐濟元（13,718 美元）的現金。B 君是毒品犯罪嫌疑人的妻子，

她說這些現金是出售車輛所得，然而，沒有證據顯示她出售任何車輛，也沒有證據顯示她最初能夠以該剩餘價值購買車輛。警方懷疑這些現金來自於銷售毒品的收益。B 君繼續堅持說這些現金來自於出售給 X 君的車輛，但是 X 君否認從她那裡購買任何車輛，也沒有證據顯示她在這段時間內轉讓車輛。B 君未能對現金做出充分的解釋，最終導致這些資金在 2020 年被斐濟高等法院宣佈為不明財富，並被沒收給國家。這次成功的審判是斐濟引入財產來源不明法以來的第一個財產不明案件。

中國澳門

反洗錢五年策略計畫（2021-2025）

為應對洗錢／反恐／反貪污國際趨勢的複雜變化，進一步保障中國澳門經濟的持續健康增長和多元化發展，政府根據第一次整體風險評估專案的結果，制定 2016 年至 2020 年的第一個防制洗錢／反恐／反貪污戰略計畫。隨著第一個防制洗錢／反恐資助戰略計畫的到期，第二個戰略計畫被制定出來，以確定 2021 年至 2025 年期間的政策和目標。

中國澳門的反洗錢五年策略計畫（2021-2025）概述政府在相關制度方面的戰略方向。其中包括以下十個戰略目標。

目標 1：	繼續保持全面的防制洗錢／打擊恐怖主義／預防貪汙的法律和制度架構，以應對中國澳門不斷變化的經濟發展和國際標準。
目標 2：	加強對中國澳門的整體 ML / TF / PF 風險評估
目標 3：	促進與防制洗錢 / CFT / CPF 和相關前置犯罪有關的國際合作
目標 4：	進一步加強對所有主要前置犯罪的平行金融調查
目標 5：	繼續保持法人和法律協議的高透明度
目標 6：	加強沒收和資產追回工作，剝奪犯罪者的犯罪工具和收益
目標 7：	根據國際標準，將資助恐怖主義的調查作為更高的政策層面的目標進行優先處理
目標 8：	在對所有部門的監督和刑事調查中堅持一個健全的風險基礎法
目標 9：	按照國際標準，加強執行 CFT 和 CPF 的凍結機制
目標 10：	向所有受監管的法人實體推廣合規文化，提高對 ML / TF / PF 風險的意識和理解，以提高 AML / CFT / CPF 的合規水準。

在這十個戰略目標的架構下，進一步制定更詳細的次級目標和行動專案。與過去一樣，這個新五年策略計畫由中國澳門行政長官領導的行政委員會宣讀和討論，從而顯示對解決防制洗錢／打擊恐怖主義／預防貪汙問題的高級別政治承諾。

2020 年的其他 AML / CFT 的立法或監管動態

為讓申報機構更好地瞭解資產凍結執行制度相關法律的實施，監管機關：中國澳門金融管理局和博彩監察協調局分別於 2020 年 3 月和 6 月向金融機構和博彩特許經營者發出通知和實用指引。通知和實務指引

旨在更詳細地解釋資產凍結執行制度的法律要求，協助申報機構完善其標準作業程序，並與行業建立快速的協調和申報機制。

統計資料

（i）在 2020 年上半年，共收到 947 份可疑交易報告，57 份可疑交易報告已報告給人民檢察院。

（ii）在 2020 年上半年，AML / CFT 的調查、起訴和定罪的數量如下：

Activities	AML / CFT
司法警察的調查	25
反貪汙委員會的調查	2
檢察院的調查	20
起訴	6
定罪	2*

* 一宗案件還在上訴中

關於直接從可疑交易報告中發展出來的案件，請參考第 7.2 節中中國澳門的案例：" 來自中國澳門的夫婦因參與詐欺、偽造和洗錢被捕 "。

馬來西亞

為補充 2020 年 1 月 1 日生效的針對金融機構、DNFBPs 和非銀行金融機構的防制洗錢、打擊恐怖主義資助和目標性金融制裁政策文件（AML / CFT 政策文件）中基於原則的要求，馬來西亞中央銀行（BNM）發布兩份關於受益所有權和個人客戶核查的指導文件。這兩份文件旨在促進防制洗錢／打擊恐怖主義政策文件要求的實施，並為申報機關提供建議，以加強與風險水準相稱的適當控制。

為支持業界人士應對 COVID-19 疫情流行，馬來西亞國家銀行於 2020 年 4 月發布關於 COVID-19 疫情流行期間 AML / CFT 措施的監管預期的通知。它概述經修訂的 AML / CFT 政策文件中已經給予的監管靈活性，如實施 RBA 以確定與 ML / TF 風險水準相稱的適當客戶盡職調查措施。

為應對不斷上升的網路犯罪，馬來西亞皇家警察還主動開發一個移動應用程序 "Semak Mule"，除其現有的網站[39]，使公眾能夠切實檢查與犯罪活動相關之銀行帳戶和電話號碼。該手機應用程序還列出用於詐騙的十大銀行帳戶和電話號碼，讓公眾無論身在何處都能及早檢查，避免成為馬來西亞網路犯罪的受害者。由於公眾可以 24 小時使用該程序，這一舉措已經取得成果，截至 2020 年 10 月，共有 900 萬人造訪該入口網站，12 萬人下載該應用程序。

菲律賓

菲律賓有一個處理恐怖主義的現有法律架構。2007 年，菲律賓頒佈共和國法第 9372 號，題為保障國家安全和保護人民免受恐怖主義侵害的法案，又稱 2007 年人類安全法。2012 年，菲律賓國會參、眾兩院還頒佈共和國法第 10168 號，又稱 2012 年預防和制止恐怖主義資助法（TFPSA）。共和國法第 9732 號透過頒佈第 11479 號共和國法令，即 2020 年反恐怖主義法（ATA）而被廢除。

共和國法第 11479 號，題為預防、禁止和懲治恐怖主義，從而廢除共和國法第 9372 號（又稱 2007 年人類安全法），於 2020 年 7 月 3 日由總統簽署成為法律，並於 2020 年 7 月 18 日生效。

---

39 http://ccid.rmp.gov.my/semakmule/

第 25 條允許反恐怖主義委員會[40]（ATC）行以下行為：

a）自動採納聯合國安理會指定和／或確定為恐怖分子、恐怖主義資助者的個人、團體、組織或協會之綜合名單。

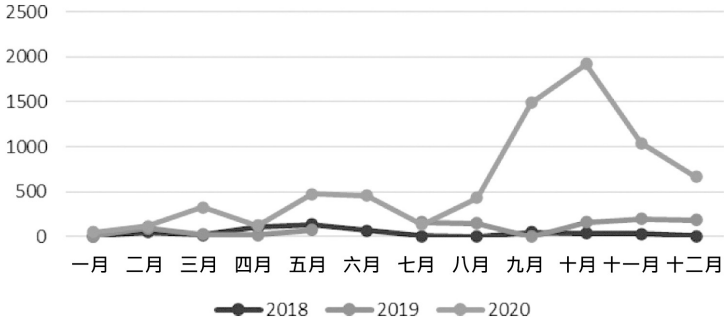
b）透過決議以採納外國對於聯合國安理會 1373 號決議之指定制裁請求；以及

c）基於潛在理由，透過決議指定國內恐怖分子。

反恐怖主義法的通過為相關人員識別潛在的恐怖分子以及與恐怖主義和 TF 有關的交易提供額外的意識。雖然反恐怖主義法是一個值得歡迎的補充法案，但菲律賓的執法機關仍然可以利用預防和制止恐怖主義資助法來起訴恐怖主義分子。

對可疑交易報告的評估顯示，與 2019 年的可疑交易報告申報數相比，2020 年增加 580%。月度趨勢顯示，2020 年 9 月至 12 月，在反恐怖主義法頒佈後的幾個月裡，可疑交易報告激增。在 COVID-19 疫情流行期間，特別是 3 月至 7 月實施社區隔離期間，可疑交易報告也激增 500% 以上。

2018 年至 2020 年間，恐怖主義與資恐相關之可疑交易報告



40 反恐怖主義法第 45 條規定設立反恐怖主義委員會（ATC）反恐怖主義委員會由九名內閣成員組成。內閣成員包括行政秘書、國家安全顧問、外交秘書、國防秘書、內政和地方政府秘書、財政秘書、司法秘書、資訊和通訊技術秘書以及反恐怖主義委員會執行主任。

透過防制洗錢委員會與舉報人之間的協調，申報可疑交易情況，以確定帳戶與恐怖主義和 TF 之間可能存在的聯繫。其他的助益是，透過防制洗錢委員會和其他執法機關與客戶和行業協會的定期接觸，定期更新對風險的理解；以及各機關在防制洗錢／打擊恐怖主義運動中的持續和協調努力。

新加坡

加強與金融情報中心情報分享的立法發展

自 2019 年 4 月 1 日起，新加坡修訂該國貪汙、販毒和其他重大犯罪所得利益沒收法（第 65A 章）（"CDSA"）第 41 條，使可疑交易報告辦公室（STRO）能夠在滿足以下條件的情況下與艾格蒙聯盟的金融情報中心交換金融情報，而無需簽訂合作備忘錄／合作意向書：

- 該金融情報可能與該外國司法管轄區的毒品交易犯罪或嚴重犯罪的調查有關。
- 該外國金融情報中心能夠應我們的要求向可疑交易報告辦公室提供金融情報；以及
- 該外國金融情報中心已作出適當的承諾，以保護金融情報的機密性並控制其使用。

這一立法修正案允許與更多的金融情報中心合作，以協助偵查洗錢活動、其前提條件以及 TF 活動。2020 年，與 2019 年相比，可疑交易報告辦公室發出和收到的外國金融情報中心援助請求的數量都分別增加約 10%。

支付服務法的立法發展

根據支付服務法（PS Act），購買、銷售或交換數位支付型代幣（DPTs）的虛擬通貨平台及交易業務事業（或支付服務法中提到的數位支付型

代幣服務提供商）需要獲得許可，並遵守防制洗錢／打擊恐怖主義的要求。為投資目的進行虛擬資產交易的服務提供商同樣需要根據證券和期貨法獲得許可，並遵守防制洗錢／打擊恐怖主義的要求。

為使新加坡的監管制度與 FATF 修訂的虛擬資產標準保持一致，議會於 2021 年 1 月透過公部門服務法的修正案，以擴大受監管之數位支付型代幣服務範圍，包括數位支付型代幣之轉移和為數位支付型代幣提供保管錢包服務。提供任何這些服務的數位支付型代幣服務提供商同樣需要根據公部門服務法獲得許可，並遵守新加坡金融管理局的防制洗錢／反恐要求。這將包括需要對客戶進行盡職調查、監測交易和申報可疑交易。新加坡金融管理局還在進行立法修訂，以將在新加坡註冊的法人實體納入其監管範圍，這些法人實體僅在新加坡以外提供虛擬通貨服務（即與支付和／或投資有關的服務）。

新加坡金融管理局採用風險基礎法來監督新加坡的虛擬通貨平台及交易業務事業。作為許可程序的一部分，對許可證申請人進行強有力的防制洗錢／打擊恐怖主義的重點檢查，以確保打算在新加坡經營的數位支付型代幣服務提供商具有相關的 ML / TF 風險意識和適當的防制洗錢／打擊恐怖主義控制。新加坡金融管理局還進行以風險為目標的檢查，以檢查持牌人的防制洗錢／打擊恐怖主義控制的有效性，包括其監測和監督活動，以發現不尋常的行為和可疑的交易。新加坡金融管理局還利用其監督能力，主動發現無證經營的數位支付型代幣活動，並利用公部門和其他資料來源，如公司註冊資訊和可疑交易報告，採取執法行動。

隨著增值服務行業的不斷發展，包括新加坡金融管理局和執法機關等單位，密切合作以確定和檢測 ML / TF / PF 的風險和態樣，並採取必要的措施來抵減這些風險。

在新加坡提高實質受益人的透明度

根據公司法和有限責任合夥人法，自 2017 年 3 月 31 日起，公司和有限責任合夥事業必須取得並保存實際控制者資訊，並應執法機關要求時提供這些資訊。

作為會計及企業管理局（ACRA）為維護新加坡作為一個值得信賴的金融中心的聲譽所做的持續努力的一部分，以及為進一步提高公司法人實體所有權和控制權的透明度，公司法和有限責任合夥人法已被修訂，自 2020 年 7 月 30 日起生效，要求所有公司和有限責任合夥事業向會計及企業管理局控制者登記冊中央檔案處提交他們在實際控制者登記冊（RORC）中保存的資訊。會計及企業管理局控制者登記冊中央檔案處中的實際控制者登記冊資訊將提供給執法機關，用於管理或執行其職權範圍內的法律。

8.2 自可疑或大額通貨報告直接查獲之案例

馬來西亞

商業電子郵件詐騙（BEC）和一名銀行分行經理參與協助開設錢騾帳戶

金融情報中心收到 X 銀行的可疑交易報告，報告稱法人實體 A 是一家新成立的獨資企業，儘管只經營兩個星期，卻從 S 司法管轄區收到大量的匯入資金。在匯款人銀行能夠提醒 X 銀行這些匯入資金與涉及商業電子郵件詐騙的詐欺性交易有關之前，一小部分資金立即在櫃檯上被領取。剩餘資金被轉出到法人實體 B 在不同金融機構的另一個帳戶。

經過進一步檢查，發現法人實體 B 的帳戶也曾被申報一份可疑交易報告，其懷疑的依據與上開情形類似，特別是收到來自一個外國法人實體的大量資金，並立即轉出到另一個法人實體。法人實體 B 的交易行為與法人實體 A 密切相關。

金融情報中心進一步分析顯示，這種商業電子郵件詐騙活動涉及一群獨資企業作為錢騾帳戶持有人，用在外國司法管轄區建立的類似合法企業的名稱來欺騙潛在的受害者。這些獨資企業的創建是為掩蓋這些外國企業，並採用與法人實體 A 和 B 相同的運作方式。

此外，在涉案的一家金融機構發起的內部調查後，發現該集團得到一名銀行分行經理的協助，為開戶和取款大開方便之門。

該案件被轉交給馬來西亞皇家警察（RMP），並進行調查，主要嫌疑人根據刑法第 420 條被起訴，而被扣押的資金則根據洗錢防制法第 60 條之規定返還給受害者。

專業人士提交不正確報表

一名醫生在一家私人醫院擔任外科顧問，他還擁有一家診所。馬來西亞稅務局（IRBM）對該醫生的資產、負債、收入和其他相關資訊進行的監督活動顯示，該醫生報告的收入被低估。他漏報他的私人診所和在私人醫院服務的部分收入。

馬來西亞稅務局調查顯示，該醫生帳戶中的巨額儲蓄總額與他申報的收入不相稱。對該醫生的營業場所和個人住所以及與他有關或有業務往來的配合廠商進行檢查。根據 1967 年所得稅法第 114（1）（a）條，該醫生被指控故意規避五年的所得稅，其未繳稅款約為 650 萬馬幣（1,577,096 美元）。在透過民事追繳解決應繳稅款和罰金後，該案件隨後被撤銷。

一家銀行申報之可疑交易報告顯示，在五個月的時間裡，有 820 萬馬幣（1,989,576 美元）被存入該醫生和他身為家庭主婦的妻子共同開設的個人帳戶。其中一些資金來自他已經關閉的定期存款帳戶，他還開出更多新的定期存款支票。根據銀行的說法，他總共有 12 個定期存款。

鑒於該帳戶的大量交易和他的職業，銀行懷疑該醫生將其個人帳戶用於商業目的，同時他可能涉及逃稅。

涉及非法收入／利潤之逃稅行為

馬來西亞稅務局與其他執法機關對東馬來西亞某州的 55 個法人實體進行聯合稽查，懷疑它們參與走私鄰近地區之香煙及酒類。這些走私的香煙和酒類被分發給該州的雜貨店和連鎖商店。

馬來西亞稅務局的調查顯示，這些法人實體的銀行帳戶周轉率高，交易量大。交易涉及的金額與向馬來西亞稅務局申報的收入不相稱。此案後來根據 1967 年所得稅法以民事追繳方式解決。總共支付逃稅總額 1,970 萬馬幣（4,779,828 美元）。

關於兩個主要對象、P 先生與 T 先生的多份可疑交易報告，他們參與食品和雜貨的批發和零售。以下是顯示 P 先生與 T 先生可能參與非法活動，即走私和逃稅的可疑交易摘要：

- P 先生的個人帳戶顯示有大量透過臨櫃現金、現金存款機和支票的存款交易。資金是透過現金支票兌現的方式提取的。
- P 先生告訴申報之機關，他帳戶中的交易是出於商業目的。然而，機關無法確定／核實 P 先生的資金來源和交易目的。
- 儘管 P 先生在一家賭場沒有進行賭博，但他卻聲稱從該賭場獲得一張非中獎支票，這顯示 P 先生可能使用銀行機關以外的管道（如賭場）來獲得商業收益。
- 根據他對申報機關的聲明，P 先生與 T 先生有關係，即公同共有企業或雇主相同。
- T 先生身兼數職，在涉及運輸和飯店等業務的多個商業法人實體中擔任董事／股東和／或授權簽字人。其中一些法人實體沒有明確的業務性質。

- T 先生以前曾被執法機關調查過（根據洗錢防制法第 48 條對他發出命令）。
- T 先生似乎正積極在透過一個賭場進行交易。據報導，他在一家賭場進行大量的現金交易，並兌換一些非中獎支票。與賭博無關的交易總額很高
- T 先生還將大量資金用於股票投資。

新加坡

由可疑交易報告直接形成的逃稅案件中被起訴之人

可疑交易報告辦公室收到一份關於 A 君的可疑交易報告。分析顯示，在四個月內有超過 100 萬新幣（約 75 萬美元）的大量現金存款存入 A 君的個人銀行帳戶。A 君曾提到，這些存款是她的酒吧生意收入。

根據可疑交易報告，新加坡稅務局（IRAS）開始對 A 君進行調查。新加坡稅務局利用資料分析和先進的統計工具，發現兩家酒吧的所得稅申報情況存在異常。新加坡稅務局還注意到，在向 A 君的個人銀行帳戶存款之前，以 A 君名義註冊的所有企業都已停止營業。

調查顯示，雖然 A 君沒有被列為這兩家酒吧的股東或董事，但 A 君實際上是這兩家公司所開展業務的決策者，並策劃一項安排，即省略現金銷售。這兩家公司在其所得稅申報表中做偽造紀錄，並在其消費稅申報表中短報銷項稅。

A 君因協助兩家酒吧規避所得稅與商品及服務稅而被定罪。A 君被判處 41 周有期徒刑，並被命令支付總額為 2,318,452 新加坡幣（約合 1,747,045 美元）的稅款、罰金和罰款。

可疑交易報告支援對可能的詐欺和貪污的海外調查

可疑交易報告辦公室收到的情報顯示，B 君參與可能的詐欺和貪污位於東南亞司法管轄區的儲蓄和合作貸款基金的資金，該基金從 2020 年 2 月起拖欠超過 10 億新幣（751,680,134 美元）的還款。

可疑交易報告辦公室對與 B 君在可能犯罪期間有關的金融情報進行進一步分析。分析發現，在此期間 B 君透過貨幣兌換商和銀行帳戶的電匯，讓超過 590 萬新幣（約 445 萬美元）的資金流向海外。隨著最近 B 君涉嫌貪污的事件被揭發，可疑交易報告辦公室有理由懷疑這些資金流動可能與上述基金有關。

可疑交易報告辦公室迅速將自己的分析與外國金融情報中心的同行分享，並從他們那裡得到回饋，分析和資訊為他們正在進行的針對 B 個人的調查提供見解。

9. COVID-19 相關之洗錢與資恐之趨勢

9.1 與 COVID-19 有關之特定前置活動（例如福利詐騙、詐騙、偽造藥品、貪汙、毒品、走私等）之洗錢或資恐之型態

汶萊和平之國

2020 年 3 月 16 日，汶萊和平之國政府實施關閉所有邊境的措施，並嚴格監測任何聲稱必要旅行的人抵達該司法管轄區。自那時起，發現的與毒品有關的犯罪行為急劇增加，涉及大量的非法毒品。

根據公開來源的報告，估計總共繳獲價值 590 萬汶萊元（4,432,815 美元）的毒品和 419,000 汶萊元（314,806 美元）涉嫌犯罪所得的現金（包括外匯），以及其他資產，如汽車、船隻、珠寶和手機。

在發覺這類情況的同時，煙酒等違禁品的走私也在增加。這一觀察結果顯示，關閉邊界與發現走私事件的增加以及走私到汶萊和平之國的產品數量之間存在著關聯。

走私毒品罪案件

a. 2020 年 9 月，汶萊毒品管制局（NCB）紀錄其有史以來最大的毒品、金錢和財產沒收案。在一次名為 Musang King 的行動中，國家邊境局搜索住宅，並逮捕幾個據信參與家庭毒品商業網絡的嫌犯，該網路被懷疑是汶萊最大的甲基安非他命供應商。

   這次行動繳獲 19 公斤甲基安非他命，估計市場價值超過 3,700,000 汶萊元（2,779,833 美元）。

   繳獲的其他重要物品包括金額超過 25 萬汶萊元（187,828 美元）的外幣、各種黃金珠寶、手提包和手錶、健身器材和電子設備、家庭傢俱、13 輛汽車、2 艘船和 1 輛摩托車。此外，還發現 202 箱各種品牌的香煙。此案目前仍在調查中。

b. 2020 年 5 月，國家邊境局查獲 100 粒據信是搖頭丸、155 克氯胺酮和現金，該嫌疑人試圖透過邊境管制站將其走私進司法管轄區。嫌疑人駕駛的車輛屬於當地註冊的貨運代理公司（包裹運送者）。被查獲的毒品的估計價值總計約為 25,000 汶萊元（18,782 美元）。

酒精和煙草走私案

a. 2020 年 12 月，一名印尼國民被認定犯有非法持有 12 箱、480 條和 10 包各種品牌香煙的罪行。他被處以 460,000 汶萊元（345,626 美元）的罰款，否則將被處以 35 個月的有期徒刑。這些香煙被發現藏在這個人的房子裡。
b. 2020 年 11 月，兩名男子因持有大量走私香煙而認罪，被勒令繳納遠遠超過 100,000 汶萊元（75,138 美元）的罰金。

一名 29 歲當地男子在認罪後被罰款 170,000 汶萊元（127,748 美元），如果不繳款，將不得不服 23 個月的有期徒刑。當局在 2020 年 3 月檢查他的房子時，發現他的車內有 537 盒和 107 包香煙。

一名外國公民因持有走私香煙和啤酒被勒令繳納 105,000 汶萊元（78,902 美元）的罰款。在他對指控認罪並承認他在淡布隆區邦阿縣駕駛車輛時被當局當場抓獲後，如果不支付罰款，他將不得不服刑 23 個月。他被發現車內有 125 箱香煙，而在他位於甘榜蘇博克的家中進一步檢查發現，他在沒有進口許可證的情況下保留 4 箱啤酒。

中華臺北

案例一

C 先生是個詐騙慣犯，有多次犯罪紀錄。在 COVID-19 疫情流行期間，他冒充外國富豪 Y 先生的秘書，打電話給中華臺北口罩製造公司 M 的

執行長，聲稱要訂購 5000 個成人口罩、5000 個兒童口罩和 100 盒酒精棉球作為禮物送給 U 醫院的醫務人員。除此之外，為說服 M 公司執行長，C 先生向 M 公司提供 U 醫院的地址作為發貨地址。但是，他把自己的電話號碼給 M 公司作為聯絡人。當這些口罩和酒精棉球到達後，C 先生便截留貨物供自己私用。地方檢察署於 2020 年 8 月以違反刑法的罪名起訴 C 先生。

案例二

刑事警察局的電信調查團收到關於網路上非法賣家在銷售醫療級口罩時欺騙消費者的資訊。消費者購買後發現品質有問題，於是向警方報案。為防止劣質醫用口罩在市場上銷售，工商局電信偵查總隊與彰化縣公安局鹿港分局聯合組織一次專項行動，並向地方檢察署報告。

專案組對上述情報和相關資訊進行分析後，在雲林縣將網上賣家某 A 抓獲。根據賣家 A 的供述，專案組繼續追蹤其上游發貨商 B，並對其在台中市的住所進行搜索，當場查獲 20 盒假冒偽劣口罩。專案組繼續追查假冒偽劣口罩的來源。經查，該批貨源是由犯罪嫌疑人 C 某提供。

本案證據收集完畢後，承辦檢察官指揮專案組對嫌疑人 C 某的工廠進行搜索。經查，C 某是一家口罩生產商。他利用從中國大陸進口口罩機設備的機會，謊稱自己是國家隊口罩機生產廠家，並以檢測口罩成品率為由，生產大量號稱醫用等級的口罩。然後，他將其批發給網上賣家牟利。專案組當場查獲 440 箱口罩成品和帳本。此案中，共查獲 115 萬個假冒偽劣口罩。整個案件因涉嫌違反嚴重特殊傳染性肺炎防治及紓困振興特別條例、刑法詐騙罪與藥事法而被移交給地方檢察署。

斐濟

2020 年 3 月，斐濟金融情報中心發布一份新聞稿，建議公眾注意與 Covid-19 有關的網上詐騙。斐濟金融情報中心收到一份與 COVID-19 有關的產品騙局報告，一家當地製藥公司為其從未收到的個人防護設備訂單付款。金融情報中心還收到一份報告，稱一個假冒的外國法人實體試圖與一家當地的會計師事務所合作，以促進個人防護設備的付款。當地會計師事務所被告知不要與該法人實體接觸，並停止所有接觸。

中國香港

在香港金融管理局的支持下，香港銀行公會（HKAB）於 2020 年 9 月舉辦從防制洗錢和／或其他金融犯罪風險角度看 COVID-19 疫情流行影響的分享會，分享在 COVID-19 期間觀察到的金融犯罪趨勢和遇到的挑戰，以及銀行在管理和減少 ML / TF 風險方面的最佳做法。所分享的資訊是基於會員銀行對香港銀行公會分發的問卷回覆，該問卷旨在收集業界在疫情流行中的觀察和經驗。在分享會後，我們向業界分發一份答覆摘要，以幫助個別銀行識別可疑帳戶並採取適當的抵減措施。該摘要包括對金融犯罪趨勢的主要觀察，具體內容如下：

<u>犯罪活動趨勢</u>

詐欺態樣

- 與 COVID-19 有關：個人防護設備／藥品的銷售詐欺，特別是透過線上或社交媒體，為接受與 COVID-19 有關的籌資捐款而設立的假慈善機關，利用抗 COVID-19 基金的詐欺。
- 其他：愛情詐騙、電話欺騙（如冒充政府官員／銀行工作人員）、投資詐欺、商業電子郵件詐欺（BEC）。

做案手法／使用錢騾帳戶的開設與共同點

- 由於世界範圍內的旅行限制和隔離要求，非香港居民很難訪查中國香港，因此，疑似錢騾開立的帳戶情況發生變化，從在香港短期停留的特定國籍的個人轉變為在香港的家庭傭工和有弱點背景之香港居民。
- 休眠帳戶收到的存款激增，被標記為與 COVID-19 有關的籌資或捐款。
- 在 COVID-19 期間，交易量激增，臨時存款，透過現金／快速支付系統（FPS）和線上銀行平臺。交易的頻率和模式不符合客戶所述的帳戶目的和／或業務性質。
- 一些有一個受益人的錢騾帳戶是在一年內開設的，最初的交易與向其他司法管轄區銷售個人防護設備有關，這與客戶盡職調查簡介中提供的業務領域不一致。

案例一

政府為受 COVID-19 影響的企業實施補貼計畫。18 人透過提交偽造資訊和偽造文件，聲稱所稱的企業在指定日期前已實際運營，被以詐欺罪名逮捕，涉及金額超過 600 萬港幣（772,444 美元）。調查正在進行中。

案例二

針對網上銷售外科口罩和醫療設備的廣告，中國香港一家保健品貿易公司的老闆被詐騙將 45 萬港幣（57,936 美元）轉入香港和 X 司法管轄區的多個帳戶，並將相當於 400 萬港幣（514,963 美元）的比特幣轉入騙子持有的虛擬資產帳戶。所有的詐騙者在收到付款後都聯繫不上。一項調查正在進行中。

印尼

根據印尼金融交易報告和分析中心對與 COVID-19 相關的 ML / TF 風險研究，有印尼公民透過讓 X 司法管轄區的醫療設備管理和維護公司參與進來，實施商業電子郵件詐欺（BEC）。該公司與 Y 司法管轄區的公司簽訂合作合約，購買 1,500 台肺部呼吸機和 5,000 台多參數監測器，總價值為 17,011,980 歐元（20,643,657 美元）。犯罪者使用的方法是與印尼的法律法人實體建立幾個公司，這些公司從事實驗室、製藥和醫療設備的貿易，其名稱與司法管轄區 X 公司在司法管轄區 Y 的業務對應方的名稱相似。此外，透過使用與 Y 司法管轄區的公司電子郵件功能變數名稱相似的偽造電子郵件功能變數名稱，行為人以 COVID-19 的情況為由，發送關於支付銀行帳戶變更的資訊，導致義大利的公司向印尼的偽造公司帳戶發送資金，總額為 588 億印尼盾（4,000 萬美元）依靠 SWIFT 三次匯入交易。

就在差不多時間，總共 27 億印尼盾（189,105 美元）的匯入資金被轉移到幾個公司帳戶，這些資金在 72 次交易中被轉移到許多個人方，用於進一步的現金提款交易，帳戶中只剩下最低限度的餘額。同時，剩餘的 561 億印尼盾（3,928,718 美元）的資金被金融服務提供商成功阻擋。

中國澳門

對於金融部門（不包括保險部門），在 2020 年 7 月進行一項研究，為瞭解與 COVID-19 有關的新風險是從防制洗錢／打擊恐怖主義的角度來看對該部門的影響。結果顯示，由於中國澳門的疫情在早期階段得到充分控制，金融機構的防制洗錢系統沒有受到實質性影響，並迅速恢復正常運營。金融機構沒有發現任何與 COVID-19 具體相關的新出

現的 ML / TF 趨勢或態樣，但意識到網路詐欺案件數量的增加。中國澳門金融管理局提醒金融機構保持警惕，以發現其他司法管轄區的可疑交易以及相關的 ML / TF 風險趨勢和態樣。

就保險業而言，由於 COVID-19 疫情流行期間嚴格的邊境管制，保險公司推出保險轉介業務，其中非居民客戶由經紀人或第三方轉介到中國澳門以外的地方。由於銷售是由中國澳門的銷售人員進行的，與此類交易相關的風險將不可避免地增加。然而，只要規定的客戶或增強盡職調查得到良好的執行，這種 ML 風險是可以控制的。至於市場行為的潛在風險，已經建立與相關保險公司密切溝通和持續監督的機制，並採用新的聲明表格，以確保客戶清楚地瞭解潛在的相關風險。此外，保險公司被要求定期向中國澳門金融管理局提交轉介業務情況的報告，以審查任何可能違規行為。

馬來西亞

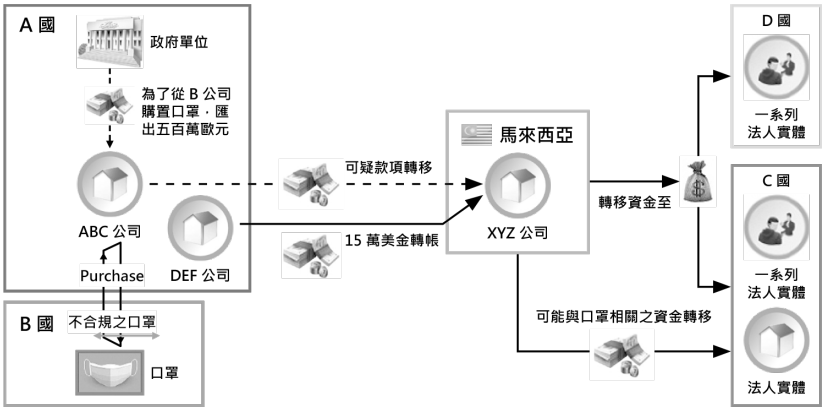
與 COVID-19 疫情流行導致的全球威脅外觀的變化相一致，馬來西亞也觀察到新出現的犯罪和／或詐欺活動的增加，特別是與偽劣假冒醫療商品（如個人防護設備和口罩）有關的犯罪，以及網路犯罪、非法線上賭博、香煙走私、非法投資計畫的線上促銷活動和毒品販運。網路犯罪數量的增長是由於司法管轄區內與網路有關的活動增加，犯罪者越來越多地利用 COVID-19 期間的不確定性，利用受害者的財務不安全感施行犯罪。

案例研究 1：偽劣假冒醫療商品

馬來西亞金融情報中心收到來自歐洲一個司法管轄區（A 司法管轄區）的資訊請求，內容涉及在 COVID-19 疫情流行期間發生的疑似口罩騙局。約 500 萬歐元（6,088,976 美元）由 A 司法管轄區的一個政府機關

轉給 A 司法管轄區的一個法人實體，即 ABC 公司，用於從 B 司法管轄區購買口罩。A 司法管轄區後來收集的金融情報顯示，ABC 公司可能隨後將用於購買口罩的大量資金轉移到另一個法人實體，即馬來西亞的 XYZ 公司。對該公司帳戶的進一步交易審查還顯示，XYZ 公司從位於 C 司法管轄區的一個法人實體那收到一筆匯入的匯款，其交易備註顯示可能與口罩有關的交易。在同一天，XYZ 公司收到來自 DEF 公司的另一筆鉅款，金額約為 15 萬美元，DEF 公司是 A 司法管轄區的另一個法人實體，據信從事保健產品的銷售，包括手套、護目鏡和聽力保護裝置。據觀察，XYZ 公司收到的資金已被支付給 C 司法管轄區和 D 司法管轄區的各個法人實體。

案例 1：口罩詐騙

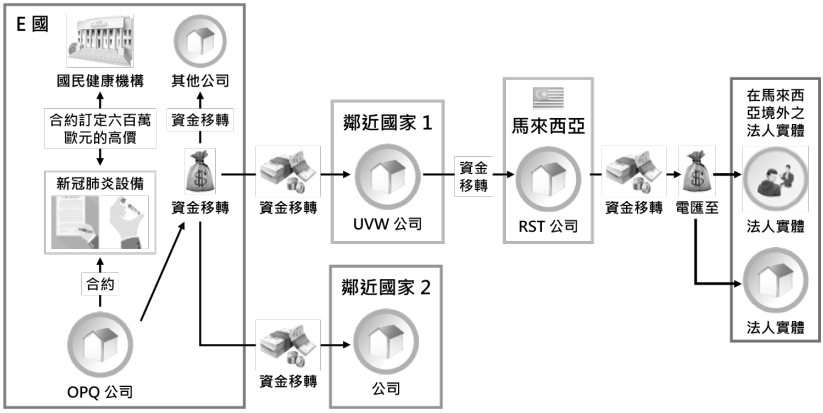


案例研究 2：偽劣假冒醫療商品

馬來西亞金融情報中心收到來自歐洲一個司法管轄區（E 司法管轄區）的資訊請求，涉及用於測試 COVID-19 的醫療設備之可疑詐欺行為。E 司法管轄區的一個國家衛生機關收到來自 E 司法管轄區 OPQ 公司的商業建議，購買用於測試 COVID-19 的醫療設備，價值數百萬歐元。

OPQ 公司透過提供偽造的產品資訊，欺騙 E 司法管轄區的國家衛生機關，使其簽署一份價格較高的設備合約。E 司法管轄區後來收集的金融情報顯示，OPQ 公司隨後可能透過涉及 E 司法管轄區和兩個鄰近司法管轄區的公司網絡，將用於購買測試 COVID-19 醫療設備的 605 萬歐元（7,367,814 美元）轉移給另一個法人實體，即馬來西亞的 RST 公司。對該公司帳戶的交易審查顯示，涉及多個交易方的快速和高頻率的進出交易模式，包括向內的 SWIFT 和國外電匯。對該帳戶的進一步審查顯示，RST 公司收到 UVW 公司的匯入匯款，該公司位於鄰近的司法管轄區之一。收到的資金後來透過電匯轉移到馬來西亞以外的法人實體。

案例 2：防護與測試設備詐騙



蒙古

根據觀察，並根據 2020 年蒙古國金融情報中心從申報機構收到的可疑交易報告的統計資料，與線上賭博有關的可疑交易的數量穩步上升。雖然 2019 年申報機構提交的與線上賭博有關的可疑交易報告總

數為 42 份，但這一數位在 2020 年增加到 362 份。據推測，由於受到 COVID-19 和隔離措施的影響，這類活動以前所未有的規模增加，因為一些人無法像以前那樣賺取收入，願意在家裡輕鬆賺錢，而不考慮其非法性質。根據蒙古國刑法第 20.17 條，組織賭博被認為是一種犯罪。

紐西蘭

濫用 Covid-19 政府刺激政策

在 2020 年 3 月至 12 月期間，金融情報中心收到 450 多份專門與涉嫌濫用政府 COVID-19 財政補貼有關的可疑活動報告，詳細列出價值數千萬紐西蘭幣的可疑交易。這些可疑活動報告中最主要的主題和趨勢包括：

- 沒有工作的人或領取失業救濟金的人將薪資補貼計入他們的帳戶。這些人中有很多人在警察系統中都有不良紀錄，因為他們之前參與詐欺犯罪、毒品，在某些情況下還參與組織犯罪。
- 企業為其雇員申請薪資補貼，但沒有將款項轉給雇員，而是將資金用於個人或雜項開支。
- 新成立的公司，幾乎沒有可識別的貿易活動，卻收到薪資補貼。
- 沒有已知的就業或商業關係之個人，收到似乎是為多個接受者提供的多項薪資補貼，然後將這些資金作為現金提取，轉移到第三方帳戶，或匯往海外。
- 沒有已知的商業關係之個人，收到稅務局（IR）的小企業貸款付款；然後將這些資金以現金提取，轉移到第三方帳戶，或匯往海外。
- 接受稅務局小型商業貸款的個人，其唯一的資金來源似乎是薪資（即他們似乎是雇員而不是雇主，因此沒有資格獲得貸款）。

菲律賓

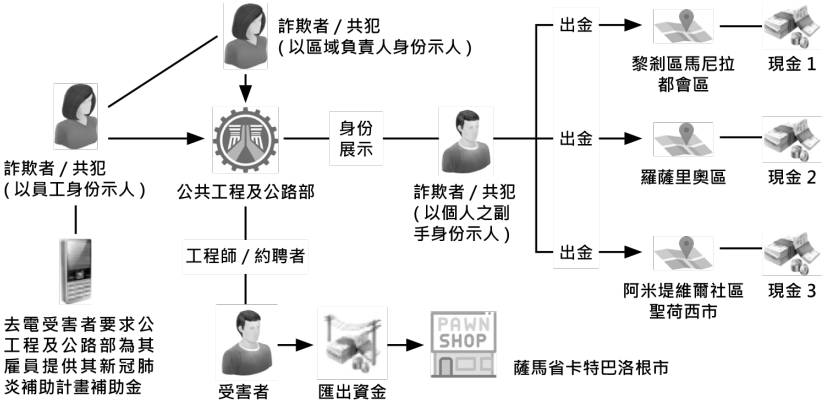
1. 詐騙者假裝與政府單位有聯繫，向受害者索取 Covid-19 捐款

地方政府單位

去年 2020 年 5 月 27 日以一名被指控的詐欺者名義開設的某個帳戶，據稱是用呂宋某省現任省長的名義為 COVID-19 募集捐款或資金。募集到的資金被存入該詐欺者的銀行帳戶。對交易的審查顯示，大筆現金存款共計 622,000 菲律賓披索（13,004 美元）被存入該帳戶，隨後在同一天被提取。還發現被指控的詐欺者在一天內頻繁查詢餘額。重要資訊的分類如下。（1）對收集到的文件的審查顯示，被指控的詐欺者是一名運輸網絡車輛服務[41]的司機，每月總收入在 20,000 菲律賓披索（418 美元）至 50,000 菲律賓披索（1,045 美元）之間，這是在入職過程中申報的唯一資金來源。透過公開來源的搜索，發現另一個政府機關在社交媒體上發布關於對一個類似名字的人（被指控的詐欺者）的警告，該人使用該機關執行主任的名字來募集據稱是為塔阿爾火山受害者提供的捐款，而且這些捐款正被存入該詐欺者的另一個銀行帳戶。

41 運輸網絡車輛服務或 TNVS 是用來描述經運輸網絡公司（TNC）認可的公部門事業車輛的術語，該公司被陸路運輸特許經營和監管委員會授予權力或特許經營權來經營公部門運輸服務。運輸網絡公司是利用基於網路的技術應用或數位平臺技術，將乘客與使用個人車輛的司機聯繫起來，提供預先安排的叫車服務，以獲得報酬。跨國公司的案例有菲律賓的 Grab 公司和 Angkas 公司。2020 年 10 月 8 日，詳 https://ltfrb.gov.ph/wp-content/uploads/2020/06/DO-2017-011-1.pdf

國內政府機關



據稱，犯罪者為兩女一男，冒充公共工程及公路部（DPWH）的雇員，而受害者是公共工程及公路部一個區域辦事處的工程師／承包商。2020 年 4 月 20 日，受害人接到一名女性的電話，她介紹自己是公共工程及公路部一個區域辦事處的工作人員。在告訴受害人公共工程及公路部區域主任（DRD）想要與受害人交談後，打電話的人將電話轉給另一名假裝是區域主任的女性。假冒的區域主任告訴受害人，公共工程及公路部副部長正計畫向其員工發放與 COVID-19 疫情流行有關的補貼或關懷包。為加強這一計畫，受害人被告知要籌集資金，金額為 15 萬菲律賓披索（3,136 美元），並將錢直接存入副部長在馬尼拉的銀行帳戶。由於時間有限，受害者被建議透過貨幣服務業者而不是銀行匯款。假冒的區域主任提供資金接收人的姓名和手機號碼：一名男性同夥，他被介紹為副部長的工作人員。受害人透過薩馬省卡特巴洛根市的貨幣服務業分行發送 15 萬菲律賓披索（3,136 美元），並給假冒的男性人員發短信說可以取錢。隨後，受害人收到短信通知，稱匯款被收款人在黎剎省的幾個分行領走。

2. 詐騙／信任詐騙（各種產品詐騙）

機密資訊顯示，醫療用品存在定價過高和未經授權銷售的情況，如酒精、醫用口罩和熱掃描器。此外，其他假冒或偽造的賣家以危機為契機，騙取受害者購買基本物品。大多數情況下，犯罪者會在其社交媒體帳戶中發布出售物品的資訊。在收到買家／受害者的預付款後，賣家／犯罪者會切斷通訊，並在社交媒體上封鎖買家／受害者。這些交易大多涉及當地買家和賣家。雖然違法者分佈在司法管轄區內的各個城市和省份，但觀察到犯罪者大量集中在國家首都地區（NCR）。

3. 捐款騙局（社交媒體影響者）

犯罪者在社交媒體平臺上設立一個假的捐款活動，向公眾募集資金。在加強型社區隔離（ECQ）期間，一個所謂的社交媒體影響者因其社交媒體挑戰而走紅，他在社交媒體上發布所謂的為 COVID-19 救援工作捐款，並鼓勵上層人士捐款。根據從不同來源收集到的資訊，此人使用虛構的身分來欺騙人們，據稱多年來被指控有各種 " 詐騙 " ／信任詐騙案件。

1. 與 COVID-19 有關的可能的恐怖主義資助活動

據稱，一個團體舉行抗議集會，要求在加強型社區隔離期間發放救濟品（營養補充），因為他們聲稱沒有得到當地政府單位的任何支援。據稱，上述抗議集會是由兩個左翼組織（LLO）和其他聯盟人士組織和預謀的，目的是疏遠政府與邊緣化社區的關係，煽動他們製造混亂，以描繪現政府在 COVID-19 危機中沒有能力治理國家。

由於人群變得失序，一些抗議者被逮捕，並被指控犯有刑事罪，包括違反加強型社區隔離規則，以及抵抗和不服從合法秩序。被告在交納保釋金後被暫時釋放。他們的法律顧問聲稱，用於支付保釋金的錢是透過網上募捐的法律援助服務獲得的。上述法律顧問稱，他們透過社交媒體募捐，並要求捐贈者將捐款存入兩個銀行帳戶，並透過網路捐贈／購物平臺。

地方行政部門否認沒有向這一群體發放營養補充的指控。此外，被捕的抗議者似乎不是有關地方政府的居民，並被確認為與一個共產主義團體（CG）及其武裝翼團體（AWG）有關的兩個地方組織的成員。用於募集資金的銀行帳戶也被確認為是共產主義團體和武裝翼團體的盟友和解放組織用於其籌資活動的共同存款銀行帳戶。

1. 可能利用游輪進行大宗現金走私

由於偏離客戶的常規活動，有一筆值得注意的嘗試性交易被申報。該客戶要求銀行透過存款提貨安排（DPA）從停靠在菲律賓港口的遊輪上提取大宗外幣現金。然後，該款項將被存入客戶在當地銀行開設的外幣帳戶。這種交易通常是透過國外銀行的電匯進行的，但由於 COVID-19 的考慮，客戶要求銀行根據存款提貨安排提取資金。然而，所涉及的金額超過該客戶的平均每日外匯量。此外，該客戶無法提供任何文件作為資金來源的證明。

2. 可能的詐欺：非營利組織從可疑的空殼公司接收 Covid-19 資金

一個非營利組織（NPO）於 2020 年 7 月 15 日開設帳戶，其目的是接受捐款。該非營利組織表示，該帳戶也將用於他們的運營費用，以及與慈善工作有關的資金。根據該非營利組織的網站，其主張是進行聖經研究。除開戶之外，該非營利組織還詢問如果它希望從海外公司獲得 1,000 萬歐元（12,143,443 美元）的捐款的文件要求。非

營利組織提交一份協議備忘錄，其中指出，該公司將與非營利組織合作開展一項關於預防 COVID-19 以及改善菲律賓生活品質和整體健康狀況等的全球企業社會責任計畫。雖然沒有實際的信貸，但有人指出，所提供的文件不足以支持預計將收到的大量資金。

3. 儘管業務受到封鎖的影響，但仍有持續的金融交易

魚類交易

一位女性客戶宣稱她的漁業生意是資金來源。據悉，從 2019 年 11 月 15 日至 2020 年 5 月 26 日，她的帳戶有 170 筆交易，從 50 菲律賓披索（1 美元）到 100 萬菲律賓披索（20,906 美元）不等，總價值為 4,100 萬菲律賓披索（857,210 美元）。客戶聲稱，這些交易與購買魚苗有關，因為她的業務是魚類貿易。然而，正如銀行所指出的，這些交易主要是在加強型社區隔離期間進行的，當時所有商業航班和海上旅行都被禁止。此外，客戶無法提供任何文件來支援她的主張。

美食廣場和餐館

某公司客戶從事美食廣場和餐廳業務，據觀察，在 2020 年 1 月 21 日至 2020 年 6 月 24 日期間，有 90 筆現金存入該客戶的帳戶，金額從 183,103 菲律賓披索（3,828 美元）到 5,411,042 菲律賓披索（113,124 美元）不等，總價值為 1.4 億菲律賓披索（2,926,923 美元）。銀行要求提供證明大量現金交易的文件。客戶提交現金轉帳單，但分行確認這些單據不足以支持現金存款。銀行還觀察到，這些交易大多是在加強型社區隔離期間進行的，當時大多數餐館都不允許營業。

4. 據稱從政府單位收到的大額交易，作為 Covid-19 相關產品和服務的付款

食品包裝

事主是一家建築和普通商品銷售企業的老闆。2020 年 7 月 30 日，當事人的個人帳戶收到來自第三方帳戶的資金轉帳，金額為 5,300 萬菲律賓披索（110,622 美元）。據當事人說，這筆錢包括 2,180 萬菲律賓披索（455,262 美元），第三方聲稱是大雅台市政府支付的與 COVID-19 加強型社區隔離第六波援助有關的食物關懷包。另據稱，全部 5,300 萬菲律賓披索（1,106,822 美元）將用於資助當事人和第三方的所謂合資企業收購不動產。

代表國內政府機關的飯店協調

該當事人在 2019 年 8 月至 2020 年 6 月期間在不同分行開設三個銀行帳戶，申報的資金來源為其不動產租賃業務收入。此外，其中一個帳戶是他與妻子的聯合帳戶。2020 年 6 月 11 日和 7 月 10 日，有三筆現金存入當事人的三個不同帳戶，總金額分別為 120 萬菲律賓披索（25,054 美元）和 105 萬菲律賓披索（21,922 美元）。根據銀行的調查，當事人說他們是海外工人福利管理局（OWWA）和合作夥伴飯店的協調人，海外菲律賓工人（OFW）在那裡被預訂用於隔離。該當事人進一步補充說，他們還與餐飲業者和消毒服務提供商進行協調。該當事人透露，他們沒有與海外工人福利管理局簽訂合約，存入的資金是對飯店的付款，然後用於支付服務提供商。危險信號包括 （1）無法為與海外工人福利管理局的交易提供可接受的證明文件，（2）交易的性質與開戶時申報的資金來源有偏差，（3）交易金額似乎是被拆分的。

5. 據稱是為棉蘭老島某省居民捐贈的 COVID-19 大額現金存款

事主於 2019 年 11 月 25 日在伊利根市開設儲蓄帳戶，作為其保險帳戶的結算帳戶。根據當事人的聲明，她擁有一家珠寶店，但系統中

沒有記錄她的月總收入。該當事人是另一名銀行客戶的兄弟姐妹，該客戶的帳戶也是在同一天開立的，由於試圖從未知來源存入大量現金，也被申報為可疑交易。2020 年 5 月 7 日，某位被列入黑名單的個人試圖將 450 萬菲律賓披索（93,000 美元）存入銀行。該黑名單人員是在當事人兄弟姐妹的帳戶中進行交易的同一個人。被列入黑名單的人聲稱，這些資金是由於加強型社區隔離而積累的捐款，這些資金是為馬拉維市的人民準備的。然而，該分行以缺乏證明文件為由拒絕這筆存款。對當事人 2019 年 11 月 25 日至 2020 年 5 月 22 日帳戶的財務審查顯示，有 14 筆現金存款，從 2,000 菲律賓披索（41 美元）到 246,000 菲律賓披索（5,137 美元）不等，總計 1,473,000 菲律賓披索（30,756 美元）。據該分行稱，這些存款是當事人的親戚提供的現金援助，用於她的生活開支。透過自動櫃員機提取的資金共計 471,000 菲律賓披索（9,833 美元），透過快捷支付系統（EPS）線上支付和購買的資金共計 195,665 批索（4,084 美元）。該當事人的帳戶餘額為 406,782 菲律賓披索（8,493 美元）。

6. 無法基於申報的業務性質和資金來源驗證的存款

從成衣生意到借貸

2019 年 1 月 18 日，當事人在邦板牙開設儲蓄帳戶。當事人申報的資金來源是來自成衣（RTW）業務。2020 年 4 月 29 日，一名代表在宿務市胡安 - 魯納分行向當事人的帳戶存入 499,000 菲律賓披索（10,419 美元），並於 2020 年 5 月 14 日再次存入 500,000 菲律賓披索（10,440 美元）。分行打電話給當事人核實資金來源，根據面談，當事人透露在加強型社區隔離期間，她從事小額貸款業務，主要涉及現金和無擔保交易，因為大多數商場都沒有營業。她告知分行，她將轉發她的貿易和工業部（DTI）更新證書的副本作為證明文件，

以及其他紀錄以支援大量存款。2020 年 5 月 29 日，由於她的業務性質和資金來源的變化，她的帳戶被標記為高風險。此後，分行無法與客戶聯繫，經過多次嘗試，客戶仍未提供足夠的證明文件來證明資金來源。

從海鮮交易到二手車交易

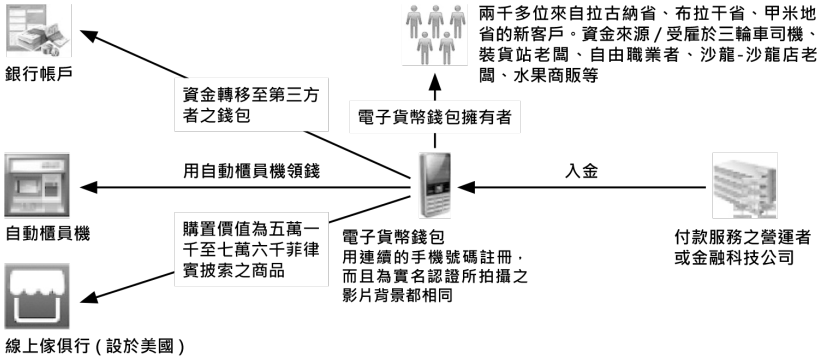
該當事人於 2020 年 6 月 30 日開設活期帳戶，初始存款為 25,000 菲律賓披索（521 美元），並申報資金來源為海鮮貿易業務收入。然而，由於 COVID-19 的影響，當事人轉而做起二手車代理。根據涵蓋 2020 年 7 月 1 日至 8 月 13 日的交易審查結果，該帳戶上值得注意的交易包括：（1）47 筆現金存款，從 500 菲律賓披索（10 美元）到 137 萬菲律賓披索（28,604 美元），共計 900 萬菲律賓披索（187,912 美元）；（2）130 筆 Instapay 匯款，共計 247 萬菲律賓披索（51,566 美元）；以及（3）11 筆當地支票存款，共計 190 萬菲律賓披索（39,641 美元）。按照當事人的說法，上述存款和匯款是出售二手車的款項。隨後，當事人開出總額為 1,100 萬菲律賓披索（229,572 美元）的支票，支付給某家聲稱擁有這些二手車的公司。銀行要求當事人提供買賣契約或其他交易證明，但當事人聲稱他只是上述交易的中間人／自由職業者，無法提供任何文件。根據公開資料，上述據稱擁有二手車的公司正在銷售／租賃消毒站。

重要政治性職務之人從事二手車交易

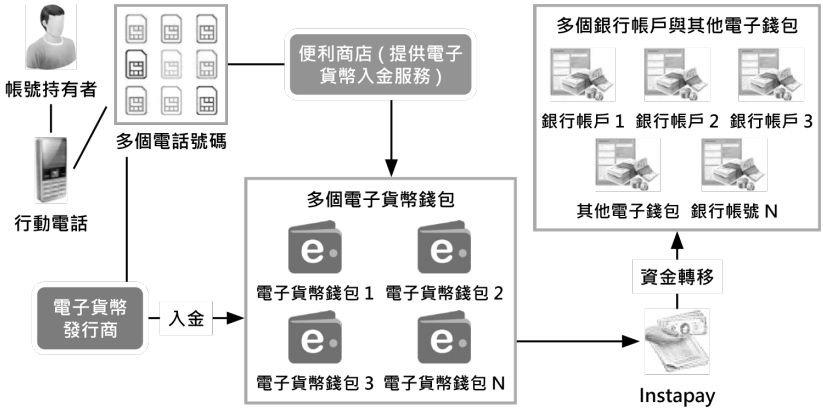
該當事人於 2010 年 2 月 15 日開設高級支票帳戶，初始存款為 40 萬菲律賓披索（8,345 美元），並申報作為北方某省市市長的薪資作為資金來源。據悉，在 2020 年 4 月至 6 月的交易審查期間，當事人的現金存款總額為 436 萬菲律賓披索（90,957 美元），支票存款為 340 萬菲律賓披索（70,930 美元）。隨後，這些款項被用來簽發應

付給某個第三方的支票。根據銀行與當事人的電話交談，這些存款是來自他的二手車買賣和建築業務。然而，該當事人表示，這兩項業務都沒有相對應商業文件。此外，據稱當事人將第三方稱為商業夥伴。當事人出示他最近購買的兩輛汽車的無條件銷售契約的影本。

7. 濫用數位 KYC / CDD 以創建可疑轉讓／錢騾／代理人帳戶



2,000 多名新加入的電子錢客戶向第三方銀行帳戶進行多次高額轉帳，總額達 1.8 億菲律賓披索（3,755,876 美元）。所有轉帳是在不到 6 個月的時間內完成的。大部分客戶是在 2019 年 7 月至 2020 年 2 月期間被邀請來的。大多數被確認為呂宋島各省的居民。這些帳戶持有人被描述為三輪車司機、裝貨站老闆、自由職業者、沙龍 - 沙龍店老闆、水果商販和私人雇員，他們將商業收入和薪資作為資金來源。涉及這些帳戶的可疑跡象如下。（a）透過某些金融技術（Fintech）或支付系統公司在一天內收到不明來源的高額存款；（b）考慮到客戶的情況，活動似乎過多；（c）透過隨後的現金提取和轉移到第三方帳戶的資金快速流動，證明分層問題；（d）大多數客戶的實名認證影片有類似的背景；以及（e） 連續的手機號碼被註冊。看到的其他值得注意的活動是在國外的一家線上傢俱店進行線上購買。



除上述案件外，在 2020 年 3 月 1 日至 5 月 30 日期間，一家電子貨幣發行商（EMI）報告2,933 份與疑似錢騾或走私者有關的可疑交易報告。這些交易的估計價值為 1,889 萬菲律賓披索（393,956 美元），在不到四個月的時間裡進行交易。個人，通常使用同一部手機，使用不同的手機號碼創建多個電子錢包帳戶。一旦創建電子錢包，個人就會在相隔幾天的不同日期透過便利店兌現。另一種套現方法是透過另一個電子貨幣發行商，這與發行電子錢包的電子貨幣發行商不同。在向電子錢包入帳的同一天，資金隨後透過 Instapay 轉到幾個銀行帳戶和／或其他電子錢包。交易的地域也集中在南達沃、北達沃、邦加西南、北伊洛科斯斯、塔拉克、西內格羅斯、錫基霍爾、拉古納、三寶顏、奎松市和馬尼拉市等地區。大多數帳戶持有人申報的職業是學生，而有一位是便利店的雇員。

新加坡

採購訂單詐騙案中的貿易洗錢

新加坡警方注意到，採購訂單詐騙再次出現，騙子冒充當地大學或政府機關的採購人員，誘使毫無戒心的公司交付貨物，並偽造承諾將稍後付款。這些非法貨物隨後被送往外國司法管轄區，然後可能構成對這些外國司法管轄區的貿易洗錢。

上述公司會收到據稱是由當地大學或政府機關（如衛生部）的採購人員發出的電子郵件，要求為電子產品、資訊技術相關專案或醫療設備進行報價。騙子會使用帶有 "precurement@ -sg.com " 或 "purchasing@ ,org " 尾綴的電子郵件，讓公司相信他們是真的。

一旦達成協議，採購訂單（PO）將透過電子郵件發送給該公司。公司相信他們收到一份真正的採購單，就會將貨物送到採購單上註明的交貨地址。這類騙局的採購單上註明的交貨地址通常屬於騙子雇用的貨運代理公司，用於將非法貨物運往海外，包括英國、岡比亞和尼日利亞。但最終沒有收到任何付款。

2020 年下半年，警方已收到至少 13 起此類詐騙報告，損失總額至少為 909,000 新加坡幣（約 684,970 美元）。在及時向警方提供資訊的情況下，警方成功地在一些貨物的預定運輸前將其攔截。

9.2 洗錢或資恐方法向既存態樣之轉移（例如現金使用之減少，結果利用網路洗錢與資恐的報告反而增加，邊境封鎖與關閉對走私與販運之影響等）

澳洲

硬性國際邊界關閉對澳洲執法部門的反恐能力產生重大影響，希望前往衝突地區和鄰近地區的利害關係人和潛在利害關係人已不再可能。雖然這對減少可能被用於資助恐怖主義的實物貨幣的流動有直接影響，但澳洲當局仍然對電匯和匯款到關注之司法管轄區保持警惕。

9.3 針對流行病、自然災害或經濟危機造成對洗錢／資恐之趨勢與態樣造成影響所進行之任何研究或報告

中國香港

中國香港聯合金融情報中心對選定的可疑交易報告進行深入的專題分析和整體審查，金融情報中心之間交換資訊和來自各種來源的關於中國香港普遍存在的犯罪趨勢的資訊，其中包括與 COVID-19 有關的 ML / TF 趨勢產生的犯罪。

此外，詐欺和洗錢情報工作組（FMLIT）在 2020 年發布與 COVID-19 有關的詐欺和欺騙案件的警示，並與本地機關和海外機關分享。在各種社交媒體平臺上也發布反詐騙資訊和宣傳活動，以提高公眾意識。

馬來西亞

2020 年，馬來西亞中央銀行就 COVID-19 相關犯罪、ML / TF 趨勢和紅旗問題向選定的行業製作一系列諮詢文件，以協助在疫情流行期間進行交易監測和發現可疑交易。

這包括馬來西亞證券委員會以影片／資訊圖表的形式向公眾發布的與 COVID-19 有關的騙局，以及納閩金融服務局向其申報機關發出的警示，如對 COVID-19 引起的新風險和威脅進行防制洗錢／打擊恐怖主義監測，就客戶盡職調查措施提出建議，以及提醒可疑交易報告的申報義務。

10. 縮寫與縮寫詞

ABF	澳洲邊防部隊
AFP	澳洲聯邦警察
AML	防制洗錢
AMLA	洗錢防制法案
AMLC	防制洗錢委員會
APG	亞太防制洗錢組織
ATM	自動櫃員機
AUSTRAC	澳洲交易報告暨分析中心
C&ED	海關總署（中國香港）
CDD	客戶盡職調查
CFT	打擊資恐
CTR	現金／貨幣交易報告
DNFBP	指定之非金融事業或人員
EAG	歐亞小組
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）
FPTBTS	虛構的稅務發票（印尼）

FSRB	區域型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	國際資金交易指令
INTERPOL	國際刑警組織
JAFIC	日本金融情報中心
KYC	認識你的客戶
LEA	執法機關
ML	洗錢
MR	匯款業者
MSP	貨幣服務提供商
NCC	國家防制洗錢協調委員會（馬來西亞）
NGO	非政府組織
NPO	非營利性組織
NRA	國家風險評估
PS	人口走私
PEP	重要政治性職務之人

PKR	巴基斯坦盧比
POI	利益相關人
RI	申報機構
SAR	可疑活動報告
SEC	證券和交易委員會（菲律賓）
STR	可疑交易報告
SVF	儲值工具
TF	資助恐怖主義
VAT	增值稅