防制洗錢金融行動工作組織報告
專業洗錢

2018年7月

防制洗錢金融行動工作組織 (下稱「FATF」) 係一獨立的跨政府組織，旨在發展與推廣政策，以保護全球金融體系，對抗洗錢、資恐以及資助大規模毀滅性武器擴散。 FATF 建議已被認定為是全球性防制洗錢 (下稱「AML」) 與打擊資恐 (下稱「CFT」) 的標準。

關於 FATF 更多資訊，請參閱其網站：www.fatf-gafi.org

本文件及 / 或本文所包括的任何地圖不影響任何領土的地位或主權、國際邊界及邊界的劃界及領土、城市或地區的名稱。

引用文獻：

FATF(2018)，專業洗錢，FATF，巴黎，法國
www.fatf-gafi.org/publications/methodandtrends/documents/professional-money-laundering.html

行政院洗錢防制辦公室 2019 年 11 月印製

目 錄

專 欄

縮寫表

CFATF	Caribbean Financial Action Task Force 加勒比區防制洗錢金融行動工作組織
EAG	Eurasian Group 歐亞防制洗錢及打擊資恐組織
FIU	Financial Intelligence Unit 金融情報中心
LEA	Law Enforcement Agency 執法機構
MENAFATF	Middle East and North Afric Financial Action Task Force 中東及北非防制洗錢金融行動工作組織
ML	Money Laundering 洗錢
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism 歐洲理事會防制洗錢及打擊資恐評估專家委員會
MVTS	Money Value Transfer Service 金錢或價值移轉服務
PML	Professional Money Launderer 專業洗錢人士
PMLO	Professional Money Laundering Organization 專業洗錢組織

PMLN	Professional Money Laundering Network 專業洗錢網絡
OCG	Organised Crime Group 組織犯罪集團
STR	Suspicious Transaction Report 疑似洗錢或資恐交易報告
TCSP	Trust and Company Service Provider 信託及公司服務提供業

摘要

這是 FATF 首次特別關注於專業洗錢人士（下稱「專業洗錢人士」）協助罪犯，躲避防制洗錢、打擊資恐及制裁之計畫，這些專業人士藉此自非法活動中獲取利潤。本報告旨在說明「專業」洗錢人士之功能及特色，亦即這些參與第三人洗錢以收取費用或佣金之人士、組織及網絡。因此，本報告著重洗錢威脅而非其漏洞，並涉及犯罪者的介紹，包括專門提供專業洗錢服務的組織犯罪集團及洗錢過程中故意參與或有意疏忽的共犯。雖然專業洗錢者可以由專業人士（例如律師及會計師）從事並為一些合法客戶提供服務，但本報告主要針對那些為全職或兼職服務罪犯客戶之人。

專業洗錢為罪犯及組織犯罪集團自非法活動所獲得之犯罪所得，提供洗錢服務。由於專業洗錢人士的主要功用係協助洗錢，他們甚少涉及產生所得的犯罪活動，但專業洗錢人士提供專業知識，以掩護資金之性質、來源、位置、所有權、控制、來源及 / 或目的地，以避免被查緝。專業洗錢人士的客戶通常不區分毒販、詐欺者、人口走私集團或任何其他需要移轉或隱藏不法錢財的罪犯，這些都可以是潛在的專業洗錢客戶。專業洗錢可以在許多商業模式下運作，也可能是個人獨自行動 ; 或具有明確結構及層級的犯罪組織 ; 甚至鬆散附屬成員的網絡。專業洗錢人士是犯罪者，他們替犯罪者及犯罪組織提供服務，並從相關洗錢活動中獲利。

專業洗錢可為全套複雜的洗錢服務計畫奠定完整基礎，或根據想要漂白犯罪所得客戶的特定需求，量身訂做特別計畫。這些專業洗錢人士提供一系列可普遍適用的服務，使用相同的洗錢方法（及可能相同之

金融管道及路線），處理多個組織犯罪集團的犯罪所得。因此，專業之洗錢網絡可能透過跨國行動，利用各國特定企業、金融機構或指定之非金融事業或專業人士的漏洞。專業洗錢本身對金融制度構成威脅，由於其可以廣泛地協助洗錢及犯罪活動，並從這些非法活動中獲利。FATF 於第四次相互評鑑的結果顯示，許多國家未能充分調查並起訴一系列洗錢活動，包括第三人或複雜之洗錢活動，許多國家仍將調查侷限於自行洗錢人士：罪犯就販毒、詐欺、逃稅、人口走私或其他犯罪之犯罪所得洗錢。縱然這些行為可能涉及內部或自行洗錢，惟其不會影響專門為罪犯提供洗錢服務之人。專業洗錢人士、專業洗錢組織及專業洗錢網絡可躲避執法機關對其犯罪或組織犯罪集團客戶之查緝，同時仍隨時準備為下一個罪犯客戶提供服務。為有效打擊專業洗錢須仰賴情報蒐集及洗錢活動的調查，而非犯罪組織犯下相關的前置犯罪，打擊專業洗錢會影響其罪犯客戶的運作，且可成為干預眾多犯罪目標的有效策略。

本報告辨識專業洗錢為其客戶提供隱藏或移轉收益的專業技能，並詳細說明他們扮演的角色，讓權責機關可辨識並瞭解其運作方式，包括鎖定投資或購買資產 ; 設立公司或作出法律安排 ; 作為代理人 ; 招募並管理錢騾或其網絡 ; 提供帳戶管理服務，並開立及登記財務帳戶。本報告亦提供最新被犯罪事業收購或納入旗下，協助洗錢的金融事業的相關案例。分析顯示，專業洗錢者會使用完整的洗錢工具及技術 ; 然而，本報告特別關注常被用來洗錢的手法，例如以貿易洗錢、帳戶交割機制及地下匯兌等。

專案小組亦審查專業洗錢與資恐間之潛在連結，惟目前尚無足夠的材料單獨探討此主題，目前發現 Khanani 係一個最明顯的專業洗錢組織之例子，其為聯合國指定之恐怖組織提供服務。一個國家代表團指出，

關係鬆散之專業洗錢網絡與當地指定之恐怖主義組織之間存在潛在連結，惟提交之大多數案例係涉及洗錢，而非資恐案件。

本報告未公開版本亦探討已成功偵測並破獲專業洗錢的特殊調查工具及技術，以對尋求解決此問題的國家提供指引建議。未公開版本的報告包括強化專業洗錢辨識及調查的實用建議；確定阻撓並打擊這些團體的策略；並確定防範專業洗錢的步驟。打擊這些適應良好的專業洗錢人士，需要在國家層面，採取協調一致的執法及監督行動、適當之監理及有效的國際合作與資訊交流。本報告強調處理該問題需要在國家層面，強化業務間協調聯繫，及在國際層面有效分享資訊的重要性。本報告亦成功辨識、標記並調查專業洗錢所需之資訊及情報，目的係破獲並瓦解參與專業洗錢之相關人等暨其罪犯客戶。

本報告目的是協助權責機關於司法管轄權範圍內，鎖定專業洗錢及其用於洗錢之結構，阻撓並瓦解涉及從事非法活動並獲取利益的犯罪集團，讓犯罪者無利可圖。

專業洗錢

▪ 第 I 節：緒論

▪ *目的、範圍及目標*

FATF 已就洗錢 (「ML」) 風險進行多項研究，並在結果報告中檢視與特定犯罪所得造成的洗錢威脅或 FATF 標準所定義的實體相關之弱點。此報告評估與專業洗錢相關的威脅，但並未評估 FATF 於其他報告中涉及的洗錢弱點。具體而言，本報告旨在：

- 提高對專業洗錢特徵之認識；
- 瞭解參與專業洗錢之人員之角色及功能；
- 瞭解專業洗錢執行之業務模型及特定功能；
- 瞭解犯罪組織恐怖分子如何利用專業洗錢之服務轉移資金；
- 辨識相關洗錢類型及計畫；
- 為權責機關和私人部門制定專門適用於專業洗錢之風險指標；及
- 為偵測、調查、起訴並預防專業洗錢制定可行之建議。

▪ *報告架構*

第 II 節及第 III 節說明報告架構，包括專業洗錢之主要特點及涉及之個人、組織及網絡間之差異，並解釋他們所扮演之角色。此部分之目的係為確保在各國對於該議題有更進一步的理解並有一致的交流。

第 IV、V 及 VI 節強調洗錢網絡之主要類型，包括共犯、為犯罪者提供金融服務者的類型、一般參與專業洗錢之其他專業中間人，及用於洗錢的常見手段等。此部分所列的資訊類型，不應被視為固定之類型，原因在於專業洗錢者會利用其可用的所有洗錢工具及技術，持續調整其手段方法，試圖找出監理及執法漏洞。

▪ *方法*

本專案報告係由俄羅斯聯邦及美國共同主導，並納入 FATF 全球網絡各代表團的意見。專案小組包括阿根廷、澳洲、比利時、加拿大、中國、德國、以色列、義大利、馬來西亞、荷蘭、俄羅斯聯邦、新加坡、西班牙、英國、美國，歐亞防制洗錢及打擊資恐組織 (「EAG」) 成員國（白俄羅斯、哈薩克、吉爾吉斯、塔吉克及烏茲別克）、歐洲理事會防制洗錢及打擊資恐評估專家委員會 (「MONEYVAL」)（烏克蘭）、中東及北非防制洗錢金融行動工作組織 (「MENAFATF」)（黎巴嫩）、加勒比區防制洗錢金融行動工作組織 (「CFATF」)（貝里斯）及歐洲刑警組織等。

這些管轄區的權責機關提供詳細資訊，包括風險評估及專業洗錢安排的各種案例、策略分析結果、專業洗錢網絡的內部組織架構、行為資訊及調查技巧等。本報告亦選擇幾個範例國家作為必要的背景描述。

此外，2018 年 1 月 22 日至 25 日於摩洛哥拉巴特舉行的中東及非洲聯合類型及能力建構研討會上蒐集相關資訊，2018 年 5 月 1 日至 4 日於南韓釜山舉行之 FATF 聯合專家會議上亦蒐集資訊及回饋意見。本報告之調查結果亦仰賴金融情報中心及執法機構調查專業洗錢的經驗及回饋意見。

雖然關於該議題的研究屈指可數，但專案小組確實將 FATF 過去和目前與運作此問題有關的工作報告納入考量，包括 2012 年 FATF 財務調查指引、2013 年 FATF 洗錢及資恐法律專業人士之洗錢／資恐弱點報告及 2018 年 FATF/ 艾格蒙隱匿實質受益所有權有關的弱點聯合報告等。

▪ 第 II 節：專業洗錢之特徵

本節概述專業洗錢獨特之重要特徵，有助於建構本報告範圍。第 III 節

提供專業服務之清單，其中包括由不同個人執行的特定角色或功能。由於全球各地所使用的相關詞彙名稱不一，因此本報告在描述這些功能時，避免使用正式標題，以造成混淆情況（例如控制者、協辦者及協助者）。第 III 節說明專業洗錢一般如何進行金融計畫之商業模型。

▪ *主要特點*

專業洗錢係第三人洗錢之子類型。FATF 將第三人洗錢定義為未參與前置犯罪[1]行為之人的洗錢活動。專業洗錢獨特之主要特徵在於提供洗錢服務，以換取佣金、費用或其他類型之利益。縱使提供專業化的洗錢服務是專業洗錢人士一個主要特徵，但這並非意味著專業洗錢不參與其他業務活動（包括從事合法業務）。

同樣地也不代表這些人士僅單純從事非法收益洗錢。專業洗錢人士亦利用其專門知識及專業技能，鑽法律漏洞、為罪犯尋找機會、或幫助罪犯處理犯罪所得，使之合法化。

鑑於專業洗錢係第三人洗錢，專業洗錢人士通常不熟悉前置犯罪（例如毒品或人口販運），且通常不關心其所移轉之金錢之來源為何。專業洗錢人士知悉，他們移轉之金錢並不合法。專業洗錢人士主要關注所處理的金錢最後的目的地及其轉移之過程，客戶利用他們，創造犯罪者及其與犯罪所得之間的防線，或由於罪犯客戶未具備那些可避免被執法機構偵測到的洗錢知識及技能，而利用專業洗錢人士。

專業洗錢人士終究還是罪犯，其經常大規模運作並實施跨國性之計畫，有關「專業洗錢人士」定義並不包括被利用以協助洗錢計畫進行之不知情或被動之中間人。專業洗錢人士的其他特徵在於其有時會從事大規模運作且經常是跨國性的計畫。

---

1 2013 年 FATF 方法論，直接成果 7 之註釋。

▪ *佣金 / 費用*

許多不同且相互重疊的因素影響支付專業洗錢人士之費用或其為服務收取之佣金。這些費用通常取決於計畫之複雜程度、使用之方法及前置犯罪之知識。費用可能會根據專業洗錢承擔之風險水平而變化。例如，佣金的比例通常受到該計畫所涉及之國家或地區以及其他因素之影響，例如：

- 個人專業洗錢人士之聲譽；
- 洗錢之總金額；
- 鈔票之面額（即價值）（涉及現金之情況）；
- 客戶要求移轉或隱藏資金之時間（例如，如洗錢需要在較短之時間內完成者，佣金會更高）; 及
- 是否實施新法規或執法活動。

為獲得服務佣金，專業洗錢人士可以（i）提前以現金收取佣金，（ii）將一部分漂白的金錢轉移到其本身帳戶或（iii）將佣金整合至商業交易中。

▪ *廣告 / 行銷*

服務之廣告及行銷可以多種方式執行。一般而言，專業洗錢人士經由「口碑」（經由非正式之犯罪網絡）積極推銷服務。從以往的犯罪活動所形成之犯罪聯繫及信任，亦強化彼此的連結，並促使下一步之合作。權責機關亦曾發現在暗網上，有發布專業洗錢服務相關廣告。

▪ *紀錄保存（影子會計）*

據執法機關報告，專業洗錢人士通常會保留一個影子會計系統，其中包含帶有代碼名稱之詳細紀錄。這些獨特之會計系統可使用追蹤客戶

之詳細電子表格（使用代碼名稱）、洗錢、資金之來源及目的地、相關日期、及收到之佣金。專業洗錢人士可以使用電子方式，儲存其紀錄（例如，受密碼保護之 Excel 電子表格）或使用紙本紀錄。對於調查人員而言，這些紀錄相當重要。

▪ *個人、組織及網絡*

專業洗錢人士可屬於三個類別之一：

1. 專業洗錢人士，在配置、移轉及洗錢方面擁有專業技能或專業知識。這些人士專門提供洗錢服務，這些服務亦可於合法專業的業務中執行，內容包括但不限於下列業務：會計服務、財務或法律諮詢、成立公司及法律安排等（參閱下面之專業服務）。 專業洗錢個人經常將風險分散到各種產品中，並與多位金融專家及中間人發展不同業務活動（參見下面之例子）。

2. 專業洗錢組織（「**PMLO**」），由兩個或兩個以上之個人組成，作為一個自主、有組織之團體，專門為罪犯或其他犯罪組織提供洗錢的服務或建議。洗錢可能係該組織之核心活動，但不一定係唯一之活動。大多數專業洗錢組織具有嚴謹之層級結構，每個成員均在洗錢活動循環的環節，各司其職（參閱第 III 節）。

3. 專業洗錢網絡（「**PMLN**」）係相關人員或連絡人的集合，共同推展專業洗錢計畫及 / 或為特定洗錢任務，並分包其服務。這些網絡通常在全球運行，且可包括兩個或多個專業洗錢組織。專業洗錢組織亦可作為個人化的非正式網絡運作，為犯罪客戶提供一系列洗錢服務，此等網絡關係並非都是組織化，其通常相當彈性。

這類對外擴展的專業洗錢網絡能夠透過開設外國銀行帳戶、建立或購買外國公司並使用由其他專業洗錢控制之現有基礎設施，以滿足客戶之需求。不同專業洗錢組織間之合作亦使處理犯罪所得可利用的管道多樣化，進而降低受偵測及被查獲之風險。

專業洗錢組織通常在全球運作，與特定地區或國家的犯罪組織合作。同一個專業洗錢組織可代表數個犯罪組織或犯罪者，協助操作洗錢。此等人士技術嫻熟，能在不同的環境中運作，並且善於避開執法機關之注意。根據相關案例指出，專業洗錢人士向犯罪組織及恐怖組織提供服務（參閱下文專欄 1）。

專欄 1：Khanani 洗錢組織

Altaf Khanani 洗錢組織（「MLO」）為全球各地之犯罪組織、毒品組織及被指定的恐怖組織的非法所得洗錢。Khanani MLO 係許多個人及實體組成之犯罪組織，由 2015 年被美國緝毒署逮捕之巴基斯坦國民 Altaf Khanani 監督其運作。Khanani MLO 協助巴基斯坦、阿拉伯聯合大公國、美國、英國、加拿大及澳洲等國家間之非法資金流動，其每年負責為數十億美元之犯罪收益洗錢。

Khanani MLO 客戶來源相當多元，其曾為包括中國、哥倫比亞及墨西哥之犯罪組織及與美國當地被指定之恐怖組織有關之個人等，提供洗錢服務，Khanani MLO 亦為其他被指定之恐怖組織洗錢。具體而言，Khanani MLO 及 Al Zarooni 交易所之負責人 Altaf Khanani 曾參與處理塔利班之資金流動，據稱 Altaf Khanani 與 Lashkar-e-Tayyiba、Dawood Ibrahim 及 al-Qa'ida 與 Jaish-e-Mohammed 有關。此外，Khanani 負責自外國企業帳戶之銀行，以電匯方式，存入毒品收益，以隱瞞並掩護資金之性質、來源、所有權及控制權。Khanani 的執行方式係利用多家一般貿易公司，進行多次電匯交易。Khanani 洗錢之佣金為洗錢總額之 3%。

美國財政部海外資產控制辦公室 (下稱「OFAC」) 根據第 13581 號行政命令，於 2015 年將 KANani MLO 認定為「跨國犯罪組織」[1]。OFAC 於同一天，亦將 Al Zarooni Exchange 認定為 Khanani MLO 使用之交易所。美國 OFAC 於 2016 年認定 4 名人士及 9 個實體與 Khanani MLO 相關。Altaf Khanani 於 2016 年 10 月 26 日，承認聯邦洗錢罪名，Khanani 所有的約 46,000 美元之犯罪所得，經宣告沒收。2017 年，Altaf Khanani 因洗錢共謀罪被判 68 個月刑期。

澳洲、加拿大及美國等數個執法機構間，曾針對執法方式進行廣泛協調，這些執法機構處理不同範圍，例如指定 Al Zarooni 交易所為阿拉伯聯合大公國的中央銀行在杜拜警察總部的洗錢防制處協助下採取之行動，其於採取行動前與美國緝毒署密切協調。

註 1：跨國犯罪組織（下稱「TCO」）係美國認定過程中使用之特定術語，與 OCG 同義，本報告中使用後者。

來源：美國、澳洲、加拿大及阿拉伯大公國

犯罪組織使用外部人員及組織內的成員，以組織名義，執行洗錢服務。如犯罪組織之內部組成負責洗錢，這些成員會收到該集團之部分收益，而非薪資或佣金。專業洗錢人士參與洗錢計畫之程度，取決於犯罪集團之需求、其計畫洗錢操作之複雜性及與參與此活動相關之風險及成本。

當犯罪組織使用專業洗錢人士服務時，其通常會選擇熟悉犯罪組織網絡或組織內部人員之專業洗錢人士。這些專業洗錢人士可以是家庭成員或密切聯絡人。他們也可以是曾以合法身分從事業務之專業人士：

- 會計師、律師、公證人及 / 或其他服務提供者；
- 信託及公司服務提供業（下稱「TCSP」）；
- 銀行家；
- 金錢或價值移轉服務；
- 仲介；
- 財政專家或稅務顧問；
- 貴金屬或寶石商；
- 銀行業者或內部人員；
- 支付處理商所有人或內部人員；及
- 電子及加密貨幣交換所有人或內部人員。

犯罪組織會長期或臨時僱用外部專家，讓這類專家故意以企業家身分，且他們通常沒有犯罪紀錄，有助於躲避權責機關查獲，該些專業人士

的共犯出現在犯罪現場的頻率逐漸增加，於現場提供服務並支援特定的犯罪計畫或犯罪組織（參閱第 VI 節）。專業洗錢人士亦可同時為數個犯罪組織或犯罪份子提供服務，他們在各種環境中，都能嫻熟地操作洗錢活動，且善於躲避執法機關的注意。

專業洗錢人士亦存在區域化關係，專業洗錢網絡內部尤為如此，因為犯罪組織與負責洗錢的主要參與者之間，可能沒有直接聯繫，在此種情況下，資金被移交予專業洗錢人士洗錢前，籌措資金則透過許多人以分層化的方式進行（參閱第 III 節）。

▪ 第 III 節：專業服務和商業模式

專業洗錢人士可參與洗錢循環的單一或所有階段（即處置、多層化及整合），且可提供管理、蒐集或移動資金之專門服務。專業洗錢組織以更複雜之方式運行，且可為複雜之洗錢計畫，提供整個基礎架構，或依客戶之特定需求建構獨特的計畫。

專業洗錢人士可提供許多專門服務，包括但不限於：

- 諮詢及建議；
- 登記及維護公司或其他法律實體；
- 擔任公司及帳戶之代名人；
- 提供虛假文件；
- 混合合法及非法收益；
- 放置及移動非法現金；
- 購買資產；
- 取得融資；
- 辨識投資機會；
- 間接購買及持有資產；

- 策劃訴訟；及
- 招募及管理錢騾。

- *角色及功能*

本節介紹專業洗錢人士操作所需之眾多角色及功能。下面概述之特定功能並非詳盡清單。根據專業洗錢類型，個人可執行獨特之功能或同時執行多種角色。如能瞭解他們的角色，對於辨識所有相關參與者並確保可偵測、破壞且最終瓦解專業洗錢人士，至關重要。

- 領導及控制：可能有某特定人士負責組織之整體領導、指示並負責策略規劃及決策。通常由領導人行使控制集團洗錢活動，但亦可能由負責向客戶收取資金至交付階段，處理資金之個人獨自洗錢（例如，安排蒐集現金及規劃在選定之某跨國目的地交付現金）。這些人士亦負責確定佣金費用收取事宜，並且支付工資予專業洗錢組織 / 專業洗錢網絡內之其他成員。
- 介紹及推廣：通常有特定之個人負責將客戶引介專業洗錢人士並管理與犯罪客戶之通訊聯繫，包括負責與其他專業洗錢組織，或於當地 / 國外運作專業洗錢人士建立並保持聯繫之經理人，透過該聯絡人，專業洗錢組織可使用其他專業洗錢人士已建立的基礎措施。
- 維護基礎措施：這些人員負責建立一系列專業洗錢 基礎措施或工具。此可能包括設立公司、開立銀行帳戶並申辦信用卡。這些參與者亦可管理註冊者之網絡，註冊者則負責搜尋並招募代名人（例如掛名負責人）網絡，代表客戶登記成立空殼公司，接收線上銀行登錄及密碼或購買行動通訊之 SIM 卡。

  在管理基礎措施中的錢騾管理人（直譯為錢騾牧羊人 , money mule herder）的角色為例，其負責招募並管理錢騾（例如透過招聘廣告

及個人介紹），包括支付錢騾工資，該筆工資可作為其轉帳服務之費用或作為其服務總額（有關錢騾網絡及其角色之詳細描述，請參閱第 IV 節）。

- 管理文件：這些人士負責編製協助洗錢過程所需之文件。在某些情況下，這些人士負責製作或取得假文件，包括偽造身份證明、銀行對帳單及年度帳戶明細、商品或服務之發票、諮詢安排、票據及貸款、虛假簡歷及推薦信等。
- 管理運送：這些人士負責在跨國或當地接收並轉發貨物、提供海關文件並與運送或報關代理人聯絡，此角色與貿易洗錢計畫特別相關。
- 投資或購買資產：在需要時，會投資或購買不動產或其他資產（如寶石、藝術品、奢侈品或車輛），用於保存價值，以供日後銷售。罪犯會尋求協助，購買海外不動產，而專業洗錢人士則使用多層次空殼公司的複雜結構，來協助罪犯達成此目的。
- 收取資金：專業洗錢人士在洗錢過程之初期處置階段，負責收取非法資金。鑑於這些人處於洗錢流程之前端，極易被執法機關查獲。然而，會留下之文件紀錄卻寥寥可數，且經常透過將資金混入現金密集型企業的方式，成功地分散犯罪所得。這些人士均知悉其在洗錢刑事程序中之角色（與錢騾相比，這些人士可能係不知情之專業洗錢計畫參與者）。
- 運輸：這些特定人士負責在專業洗錢計畫中，將資金從一個地點轉移到另一個地點，而不受限於移動資金之機制，他們會使用傳統的銀行體系或貨幣移轉服務業（MVTS）供應商接收並處理資金，且通常亦負責提領現金及後續之匯兌交易。

▪ *專業洗錢網絡之一般商業模式*

圖一 專業洗錢之 3 個階段

一般而言，專業洗錢人士執行之財務計畫包括 3 個階段：

第 1 階段：犯罪所得移轉至專業洗錢人士或由其收取

在第一階段，資金以實體或電子方式轉移予專業洗錢人士或代表其運作之實體。這些資金納入洗錢計畫之確切方式，取決於前置犯罪之類型及產生犯罪所得之形式（例如現金、銀行帳戶資金或虛擬貨幣等）：

現金：犯罪所得如果是現金，通常會交給現金收款人。該收款人最終可能將現金存入銀行帳戶。收款人透過現金密集型企業、金錢移轉服務業提供者或賭場，將現金導入金融體系，或將現金移轉到另一個地區或國家。

銀行帳戶：特定類型之犯罪活動會透過銀行帳戶接收犯罪所得，

例如詐欺、貪腐及稅務犯罪。此等犯罪所得與販毒所得不同，其少以現金進行，但最終在經過洗錢後，會以現金形式呈現。客戶通常會設立法律實體，並用其名稱開立銀行帳戶以進行洗錢，利用該帳戶將資金，轉移到由專業洗錢人士控制之第一層公司。

虛擬貨幣：以虛擬貨幣形式獲得犯罪所得之罪犯（例如線上非法商店之所有人，包括暗網市場），都必須在這些平台上具備電子錢包或地址，以便專業洗錢人士進行存取。

第 2 階段：個人及 / 或網絡執行之多層化階段

在多層化階段中，多數專業洗錢人士使用帳戶分散機制，使資金不易被追蹤。同一計畫中可能採用並結合不同之洗錢技術。在多層化階段，由負責協調相關金融交易之人士所管理。

現金：將犯罪所得現金多層化之洗錢機制包括：貿易洗錢、虛假貿易、帳戶結算及地下匯兌。

銀行帳戶:轉移到由專業洗錢人士所管理之銀行帳戶的犯罪所得，經常透過複雜之多層化方式或代理架構，進行資金轉移。代理架構由一系列複雜的空殼公司帳戶所組成，於當地及國外均設有帳戶，並在同一帳戶中混合不同客戶的資金，增加追蹤特定客戶的資金來源的困難度。

虛擬貨幣：從事網路犯罪、電腦詐欺或透過網路商店銷售非法商品的犯罪者，經常使用錢騾的網絡服務（參閱第 IV 節），犯罪所得通常以虛擬貨幣形式存在，並透過複雜之移轉程序，存放於電子錢包或虛擬貨幣錢包中。

第 3 階段：漂白後之資金返還予客戶進行投資或購置資產

資金在最後階段，移轉到由專業洗錢人士的客戶、代表人或與他們有關係的法律實體之親近相關人士或第三人所控制之帳戶。專

業洗錢人士可能代表這些客戶，將犯罪所得投資於不動產、奢侈品及海外業務運作（有些案例顯示也會投資資金來源國），此類資金亦可用於將貨物運送至資金來源國或第三國。

▪ 第 IV 節：專門洗錢組織及網絡之類型

如前幾節所述，專業洗錢人士可以透過專用網絡移轉資金，利用多種機制移轉資金。此等網絡通常在洗錢週期之處置和多層化階段使用，能夠快速調整和適應不斷變化之外部環境因素（如新法規施行）和應對執法活動。專業洗錢人士會提供詳細的指導，協助整個洗錢計畫，並且經常販售推動洗錢計畫所需之工具和服務的工具包。本節描述透過案例研究分析，辨識出專門洗錢組織和網絡的主要類型包括：（i）貨幣移轉和現金控制者網絡；（ii）錢騾網絡；（iii）數位貨幣和虛擬貨幣網絡；（iv）代理網絡。

▪ *金錢移轉及現金控制網絡*

具有大量現金的犯罪份子及犯罪組織經常利用能夠代表他們移轉大量現金的網絡服務，此類現金控制網絡具有接收、轉交並移轉犯罪所得之能力，提供服務的同時收取處理費。一般而言，此網絡結構包括控制、協調、收取及傳輸非法資金的個人[2]，及一起與犯罪組織進行研商交易的個人。

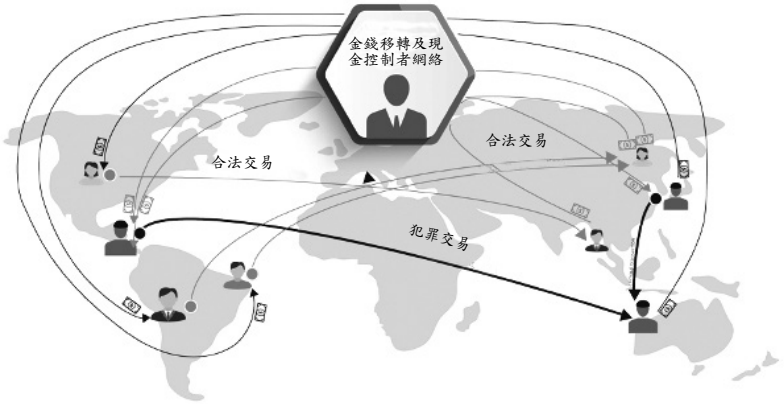
現金控制網絡經常利用帳戶交割系統，為全球多個犯罪組織統籌犯罪所得，進行洗錢，並以犯罪所得，代替合法資金，其採用的洗錢手法有時涉及透過不知情客戶之帳戶，從國外接收資金或付款，之後移轉

2 請參閱第 III 節所定義之角色與功能。

犯罪資金。在該計畫中，將款項移轉至不知情第三人銀行帳戶，與帳戶內的合法資金混合，再由洗錢人士以犯罪組織的犯罪所得取代。洗錢人士存入金額通常低於申報門檻以下的現金，以避免被偵測發現。

現金控制網絡存入的金額不會與犯罪所得的總金額相符，但長期來看，這些非法所得的金額最後還是會與存入金額一致。如非上述情況，專業洗錢人士可能會採用其他以貿易為基礎的手法，例如偽造或過度開票，以使兩個或多個管轄地間之資金流動合法化，進而平衡金額，此種手法讓專業洗錢人士可以監督在另一國家進行的支付行為，而不會有被偵測到利用自己名義持有的銀行帳戶進行交易的風險。

如國際現金控制網絡與在不同國家營運的犯罪份子及犯罪組織合作，如利用帳戶交割機制，即可不需跨境資金電匯，達成資金轉移之目的（參見第 V 節）。下圖顯示四種國際現金控制網絡運作的不同情況。



圖二：金錢移轉及現金控制網絡

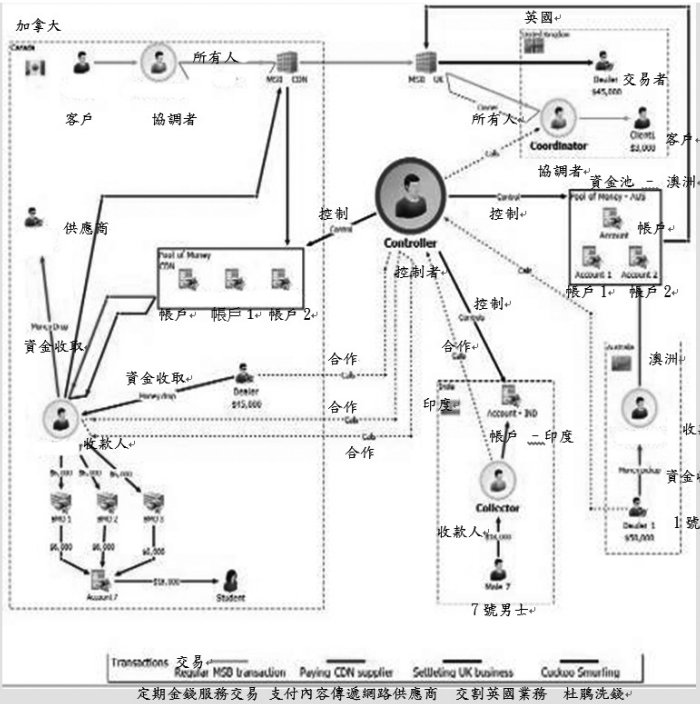
專欄 2 現金控制網絡及帳戶交割計畫

3,000 美元（綠色）：基本交易。加拿大客戶欲匯款予 1 位英國客戶，並經由金錢移轉供應商之中間人進行。

5 萬美元（紅色）：澳洲交易商欲向其加拿大供應商付款。交易商聯絡現金控制者，安排移轉資金，隨後控制者指示收款人取款。此筆款項此時屬於該國由控制者所控制的資金水庫的一部分。隨後控制者指示加拿大收款人自其加拿大資金池中取款，並將錢付給加拿大交易商。

45000 美元（藍色）：加拿大交易商欲在英國結清帳戶。交易商聯繫控制者並安排取款。取款人取款後，便依照指示，將款項交付予共犯，匯款人透過將錢存入銀行帳戶（拆分化）的方式，增加在加拿大的資金水庫金額。控制者接著自英國資金水庫取錢，並指示在英國收款人交付該筆資金。

18000 美元（紫紅色）：印度 1 位父親欲將錢寄給在加拿大的女兒。該筆資金透過哈瓦拉網絡[1]傳送，並由收款人確保控制者履行合約。其後，控制者指示加拿大收款人將資金分別存到個別銀行帳戶中，其前往 2 間不同銀行之分支機構，將存款拆分後存入帳戶中。



註 1：關於哈瓦拉更完整資訊請參閱 FATF 之哈瓦拉及其他類似服務提供者於 ML 及 TF 中之角色，日期 2013 年 10 月。

來源：澳洲

經洗錢後之犯罪所得如為現金，可能包括大量實體現金之運送。近期案例顯示，移轉現金之服務亦被外包予現金移轉專門網絡，其為負責收取現金，將現金運送到預定地點，並協助該現金存入在金融體系中。最近歐洲刑警組織發動的 Kandil 行動即為打擊協助歐洲境內販毒組織提供服務之現金移轉網絡，該網絡負責收取整個歐洲（西班牙、荷蘭、義大利及英國等國）的海洛因銷售所得，並將該筆現金移轉至德國，並透過購買二手車、零件及設備將錢納入金融體系。

專欄 3 Kandil 行動 - 現金攜帶者網絡

德國權責機關於 2016 年，在歐洲刑警組織 (下稱「EUROPOL」) 專家協助下，對涉嫌在國際間販售海洛因之毒販提供洗錢服務的伊拉克犯罪組織（總部設於德國）採取行動。德國於此次行動前，已對其進行廣泛且詳細的刑事調查，並取得歐洲刑警組織之支持，透過歐洲刑警組織與法國、西班牙、德國及荷蘭執法機關協調，此合作反映出歐洲司法部門之間協調的成果。

該犯罪集團主要由伊拉克國民所組成，負責收取整個歐洲（西班牙、荷蘭、義大利及英國等國）之海洛因販售所得，並透過德國向中東進行洗錢，洗錢後總金額估計約為 500 萬歐元。

犯罪份子之作案手法為唆使現金攜帶者（錢騾）駕車來往歐洲各地收取贓款，隨後採取貿易洗錢技術，將錢移轉至中東，前述移轉主要透過運送二手車；在德國購買並出口到伊拉克之重型機械及建築設備，這些貨物最終被轉售，以換取合法現金。

犯罪組織可利用金錢移轉服務及不受監理之金融管道（哈瓦拉系統）整合並進一步將資金轉入受監理之金融體系，此舉幾乎不會留下任何書面紀錄讓執法機關發現。

專業服務提供者如律師、會計師及公司設立之代理人，提供運作洗錢計畫所需的財務程序相關技能及知識，縱使目前已知很少團體提供這類服務，但這些人士會把大量資金漂白，並偽裝犯罪組織的身分及犯罪所得的來源，對於洗錢計畫是否成功產生重大影響，然而這些集團是執法機關在追查犯罪所得的重大障礙。

來源： 歐洲刑警組織 (德國)

▪ *錢騾網絡*

眾多專業洗錢計畫的重要組成分子為錢騾。錢騾係指透過洗錢或實體運送有價值之物，可能是贓款、貨物或其他商品之人。錢騾可能是自願參與者，或受到「交易經理」的招聘廣告吸引，或透過網路社群媒體互動而被犯罪份子招募。錢騾招募者亦被稱為錢騾「牧羊人」。錢騾可能在知情的情況下共謀洗錢，或在不知情的情況下為專業洗錢網絡或犯罪組織效力。網路犯罪份子根據潛在錢騾之動機，推出招募技巧，例如，提供檯面下的現金及免費旅行作為誘因，藉由輕鬆賺錢及免費旅行之名，激勵並招募那些還在觀望的錢騾。

專欄 4 利用錢騾漂白犯罪收益

A 人士係由奈及利亞集團所招募，以便自其銀行帳戶中收款，其可自每筆交易收取最高 5000 新幣（3160 歐元）之佣金，A 人士將在美國及巴哈馬從事詐欺犯罪行為收受的犯罪所得，存入其銀行帳戶，並根據奈及利亞犯罪組織之指示，在收到大部分之資金後之數日內轉出或提領。

A 人士不僅為收受犯罪所得之人頭，亦招募兩位錢騾，並控制錢騾的銀行帳戶，使其能夠透過多層化方式，以掩護犯罪所得的地點，並逃避偵測，會如此大費周章的原因在於資金分散於多個帳戶。A 人士及其錢騾網絡透過該方式，於 6 週內共收到 12 筆詐欺所得之電匯，金額高達 500 萬新元（3,160 萬歐元），這些電匯源自國外受害者並匯入新加坡之銀行帳戶。

A 人士因收受贓物及洗錢罪行而遭定罪，並被判處 72 個月之刑期。

來源：新加坡

專業洗錢計畫經常從僑民人際網絡及社區招募錢騾，較大規模的錢騾交易經常涉及非法網路商店及與網路犯罪相關，例如網路釣魚、惡意軟體攻擊、信用卡詐欺、商業電子郵件洩密及各種其他詐騙（包括愛情、樂透及就業詐騙）。

某些錢騾不知道自己遭利用從事犯罪活動，犯罪組織利用不知情的錢騾，兌現偽造支票及匯票，或利用被盜之信用卡號碼或盜用其他個人身分資料購買商品。在某些情況下，錢騾可能懷疑其移轉的金錢來源並不合法，但囿於經濟困難或自身貪念，他們故意裝作不知情，並經常使用擔任錢騾犯罪賺取的收入，填補其日常支出。

錢騾在過去被視為低階犯罪份子，僅負責移轉少量現金。然而，具有組織且複雜之錢騾網絡已演變為具備專業洗錢的機制，這些錢騾網絡由多層化結構控制，資源充足，在洗錢方面非常有效率，且通常與跨境運作的犯罪組織有所關聯，與網路犯罪及透過網路商店銷售非法商品的犯罪組織尤為相關。犯罪份子在一般情況下會設立看似合法企業之外在包裝，僱用毫無戒心的個人開設銀行帳戶，收受並傳遞所謂合法之付款。這些毫無戒心之人實際上就是錢騾，幫忙處理犯罪份子的犯罪所得，並建立犯罪份子間的聯繫網絡。

錢騾網絡在當地及全球金融中心，開設眾多個人銀行帳戶，協助犯罪所得流動。由錢騾開設銀行帳戶是洗錢過程多層化之初期階段，此一趨勢顯示犯罪份子仍認為錢騾帳戶、現金提領及電匯之結合是犯罪所得多層化的有效方式。

專欄 5 雪崩網路

雪崩 (下稱「Avalanche」) 為專門協助建造全球侵犯隱私及金融犯罪之犯罪基礎設施。雪崩為全球伺服器網路所組成的網路主機平台，由高度組織化的中央系統控制，該網路主機管理超過 24 種全球最有害的惡意軟體及數個大規模的洗錢活動。

Avalanche 網路最早自 2010 年起即開始運作，每日操作全球多達 50 萬台受感染電腦，為其客戶提供服務，因雪崩網路進行之惡意軟體攻擊所造成的金錢損失，全球估計高達數億美元。

Avalanche 網路提供網路犯罪份子一個安全的基礎設施，可以避免執法機關及網路安全專家之偵測。 Avalanche 網路從惡意軟體感染之電腦中，竊取網路銀行密碼及其他機密資訊，再重新導向至 Avalanche 伺服器的複雜網路當中，最終導向到由網路犯罪份子所控制之終端伺服器。Avalanche 網路於專門之暗網犯罪論壇上發布資訊，提供網路犯罪份子使用權限。

於 Avalanche 網路上運行之惡意軟體及錢騾計畫類型各不相同。例如，Nymain 等勒索軟體會將被害人的電腦文件進行加密，直到被害人向網路犯罪份子支付贖金（通常以加密貨幣之形式），其他惡意軟體如 GozNym，可以竊取被害人具機敏性的網路銀行憑證，以便使用這些憑證，對被害人的銀行帳戶進行詐欺性匯款。

在 Avalanche 上運行的洗錢計畫涉及高度組織化，犯罪網路之運作關鍵為此等人士控制伺服器網絡及錢騾網路。在某些情況下，領導者利用個人網絡在全球主要金融中心，開設銀行帳戶，協助電匯交易。錢騾通常係接受特定國家網絡的領導者所贊助，並帶往美國，或為不知情之受聘人士。錢騾將竊取的資金用來購買商品，使網路犯罪份子可漂白其透過惡意軟體攻擊或其他非法手段所獲取的犯罪所得。

來源：美國

▪ *數位貨幣及虛擬貨幣網絡*

專業洗錢人士安排犯罪份子透過非法網路商店（例如暗網的販毒商店），將虛擬貨幣的所得兌現，在網路購買非法藥物的付款會移轉到以法定貨幣或虛擬貨幣（例如比特幣）持有的電子錢包。虛擬貨幣隨後會透過複雜的電子錢包鏈移轉，其中可能包括使用攪拌器 (mixer) 及滾筒 (tumbler) 等措施，進一步增強虛擬貨幣交易的匿名性。資金隨後傳輸回犯罪組織的電子錢包，接著轉入不同銀行帳戶並以現金提領。

這些人使用的金融工具是以錢騾之名義申請（通常是透過學生申辦金融卡，將金融卡出售給犯罪份子並收取費用，但該學生對於後續使用及相關之犯罪活動一無所知）。專業洗錢人士僱用之錢騾配合前往 ATM 提款，並將款項交付犯罪組織之成員。

同一套洗錢計畫及個人網絡可同時為數個於暗網上運作的犯罪組織服務謀利，這些人隨後將資金重新分配給各自的犯罪組織。

專欄 6 漂白暗網毒品商店之犯罪所得

俄羅斯內政部及金融情報中心調查透過暗網銷售毒品的犯罪組織發現，客戶可透過指定之電子錢包，選擇以法定貨幣或比特幣支付訂單款項並移轉資金。多數客戶更傾向使用以法定貨幣持有的電子錢包，而非比特幣。

販毒商店的財務計畫由金融人員及其網絡所安排並管理，洗錢網絡僅負責籌募資金，不涉及販毒。此案件中涉及的許多電子錢包及金融卡均以代名人之名義申請，經常發生學生申請電子錢包及信用卡，再將其出售予洗錢網絡的成員，而學生不知道其後續使用的犯罪目的。某些電子錢包會在洗錢過程的處置階段使用，其限額為 30

萬美元，而其他電子錢包則有更高的限額。

為簡化洗錢流程，網路資訊科技專家開發「傳輸面板」，使用便捷的使用者介面，透過洋蔥 (TOR) 瀏覽器運作，此傳輸面板可自動切換為支付毒品用之電子錢包，其中的數位貨幣則透過不同電子錢包的複雜鏈自動移轉。

洗錢網絡將電子錢包的款項轉入銀行帳戶，由同夥持金融卡至 ATM 提領現金。ATM 提款由錢騾（車手）進行，車手身上具有多張金融卡（所有卡片均以人頭[1]的名義發行），提領出的現金隨後交付予相關人士。為增加洗錢流程複雜性，犯罪所得會被重新存入一套新的金融帳戶中，並移轉給犯罪組織（通常位於國外）。

在類似的洗錢計畫中，電子錢包的資金透過虛擬貨幣兌換成比特幣，並用比特幣支付販毒組織成員的工資，包括支付低階成員薪資等，如協助毒品銷售的小盤商及馬伕。由同一金融人員與暗網商店的所有人合作，將漂白後的資金分配給不同的犯罪組織。

註 1: 代名人 (人頭) 一詞係指由公司之實際所有人或控制人所控制之非正式代名人之股東及董事。

來源：俄羅斯聯邦

▪ *代理網絡*

代理網絡係由專業洗錢人士向犯罪組織提供銀行服務，通常透過銀行帳戶進行多層化傳輸，此專業服務具有透過合法的金融業，於全球移轉資金所帶來的所有優勢，此種代理網絡的主要任務係將客戶資金移轉至最終目的地，並模糊資金流的軌跡，經常利用於貿易洗錢方式。使用銀行帳戶的專業洗錢計畫，通常涉及來自不同管轄地的多層空殼公司，這些公司建立的目的純粹是為重新分配及混合各種來源之資金，這些空殼公司可能位於前置犯罪的發生地國家、轉帳國家或最終收取

贓款的國家，此種專業洗錢計畫讓客戶的部分資金無法追蹤。這些洗錢的資金會移轉到客戶的個人銀行帳戶、關係企業或其所控制之基金會，或以現金交付之。

一般而言，由代理網絡安排之跨境洗錢計畫具有以下結構：

- 步驟 1：客戶的資金轉移至以專業洗錢人士控制的空殼公司名義所開立之帳戶，通常係使用控制法人公司或代表其營運之實體，如犯罪所得係以現金方式取得，控制者會安排收取現金並將之存入專業洗錢人士所控制之空殼公司帳戶。
- 步驟2:資金透過國內空殼公司根據偽造合約，建立複雜的帳戶鏈，進行資金移轉，來自不同客戶的多種資金混合於同一帳戶中，致使調查人員難以追蹤何為來自特定客戶之資金。
- 步驟 3：根據偽造的貿易合約、貸款協議、證券購買協議等，將資金移轉到國外。在大多數情況下，第一層之外國公司帳戶係由完成第 1 步驟的同一洗錢人士所控制，或由與國內洗錢人士合作之外國專業洗錢人士控制這些帳戶。
- 步驟 4：透過複雜之國際移轉鏈移轉資金，他們使用的洗錢基礎措施（即由空殼公司建立之帳戶）通常用來移轉全球各地之資金，此種國際匯款通常具有類似的地理模式。
- 步驟 5：資金返還予來源客戶、與其關係密切之人或附屬法人及法律安排所控制之帳戶。專業洗錢人士取得資金後，代表犯罪組織購買商品及服務。安排該洗錢計畫的專業洗錢人士會提供不同的匯款事由，試圖證明其執行電匯是合理且合法，其中包括各種商品及服務之貿易、進出口服務、貸款、諮詢服務或投資，專業洗錢人士從中尋找漏洞及其他可能的付款目的，讓這些交易貌似具合法性，而透過銀行帳戶進行交易，亦可讓活動看似具合法性，

並避免疑似洗錢或資恐交易報告及 / 或金融機構偵測而阻止交易之情況，例如專業洗錢人士利用各種帳戶（即交易活動量小、中或大之帳戶）進行交易。

專欄 7 協助漂白詐欺銀行之收益

俄羅斯執法機關與金融情報中心及中央銀行於 2015 年合作，破獲一起大規模以侵占資金並隨後進行非法跨境犯罪所得移轉之案件。

此案件經調查確定犯罪組織成員協助竊取俄羅斯某些銀行之資產，其中銀行管理團隊故意核發不可贖回的貸款並進行虛偽之不動產交易，導致該銀行提前破產，犯罪所得隨後經由空殼公司之帳戶移轉到國外。

執法機關、金融情報中心與外國對等機關合作，破獲一起規模更大之非法跨境匯款計畫，該計畫目的移轉數個國外前置犯罪的犯罪所得，資金經由國內空殼公司及境外公司（登記於英國、紐西蘭、貝里斯及其他管轄地區）之帳戶移轉，依偽造合約及偽造的法院判決為據，其帳戶由摩爾多瓦及拉脫維亞之銀行所持有。

本計畫之主要洗錢人士之一從本計畫所利用之兩家境外公司所收到的犯罪所得收益，隨後存入個人銀行帳戶中。

此計畫所涉的犯罪組織由超過 500 名成員所組成，執法機關查獲超過 200 份網路銀行帳戶電子密鑰、超過 500 個法人公司印鑑、虛偽會計文件、偽造聯繫人資料及現金。該案已由俄羅斯政府逮捕銀行經理及其他共犯。

來源：俄羅斯聯邦

公共工程詐欺及其他類型之網路詐欺通常為犯罪所得來源，並可能透過代理網路進行漂白：

專欄 8 為洗錢建立基礎措施

該項調查由以色列專業洗錢特別調查工作小組進行，其中包括以色列警察、稅務機關、IMPA（金融情報中心）及檢調人員，調查活動包括執法機關在另一國家的合作。

該案件的嫌疑犯為從事大規模詐欺及勒索的犯罪份子以及專業洗錢人士，並協助前置犯罪者漂白犯罪所得，其利用歐洲及遠東地區所建立的空殼公司、「人頭」、馬伕及哈瓦拉貨幣服務漂白資金。這些公司會事先設立在詐欺被害人認為不易受非法活動影響之國家。

專業洗錢人士建構協助洗錢活動的基礎措施，作為全球洗錢網絡之一環。專業洗錢人士透過使用其他個人開設的外國銀行帳戶，建立外國公司，並利用外國移民匯款網絡，將資金移轉到部分洗錢網絡當中。

嫌疑人將詐欺所得移轉到以空殼公司及人頭之名義，所開設之銀行帳戶，這些資金隨後被移轉到遠東地區的其他銀行帳戶，嫌疑人立即透過以色列的馬伕、哈瓦拉網絡及貨幣服務提供者，提領現金後，將資金移轉到最終目的地。

第三國的執法機關在調查過程中，逮捕一名以色列嫌犯（其中一位專業洗錢人士），有助於調查瞭解專業洗錢網絡的運作方式，發現該網絡中的專業洗錢人士能提供各種不同的銀行帳戶（即根據洗錢總金額之活動量小、中或大之帳戶），透過使用銀行帳戶，以使活動看似合法，亦可避免異常活動通報及 / 或交易遭相關金融機構阻止之情況。

來源：以色列

協助資金跨境流動的代理網絡往往與數個不同國家的其他專業洗錢網絡有所聯繫，其在前置犯罪發生的國家中移轉資金及洗錢。協助從前置犯罪發生的國家轉出資金的專業洗錢人士是全球洗錢網絡的一環，此網絡專門於全球移轉犯罪所得，由相關國家辨識出的第三方洗錢者透過與在國外活動的其他專業洗錢人士合作，根據客戶的要求，提供洗錢服務。他們會利用位於不同國家的專業洗錢網絡，並使用不同方法，在各國之間移轉資金，確保金融交易的多樣化，此有助於降低被偵測的風險。對於代理網絡的調查發現，專業洗錢可根據需求，改變其運作方式，並居中使用不同的聯繫人遂行目的。

專欄 9 大型國際洗錢平台

俄羅斯政府對某公共財產侵占及貪污案件進行金融調查，發現一個大規模的國際洗錢平台，專門移轉不同來源的資金。

這個洗錢平台的運作方式是將犯罪所得移轉到於拉脫維亞、賽普勒斯及愛沙尼亞銀行持有的空殼公司帳戶，進一步再將這些犯罪所得移轉到受益人的親屬所控制的公司帳戶，最後移轉回俄羅斯，根據進一步調查顯示，涉及的公司都使用同一管道移轉資金。

此案依據「俄羅斯聯邦刑法」，對於涉嫌「詐欺」、「組織犯罪集團安排」及「洗錢」規定，進入刑事訴訟程序。俄羅斯聯邦之中央銀行亦因為該銀行違反防制洗錢法律當中，使用假合約協助頻繁跨境匯款，取消該銀行的許可證。歐洲中央銀行亦以協助犯罪所得再分配為由，撤回拉脫維亞銀行的許可證，拉脫維亞銀行帳戶內的大量資金遭凍結。

縱使此案件調查始於特定的前置犯罪，但其亦辨識出移轉各種犯罪所得的大規模國際專業洗錢計畫，亦有跡象顯示其他國家之客戶也使用

此洗錢計畫。有關此案件專業洗錢人士的交互關聯性而言，參與該計畫的公司與阿拉伯聯合大公國的公司具財務上聯繫，該阿拉伯聯合大公國之公司如專欄 1 所述遭美國認定與 Altaf Khanani 洗錢組織[1] 有關。

註：1。有關此洗錢組織的案例研究，請參閱第 III 節。
來源：俄羅斯聯邦

專業洗錢計畫及基礎設施亦可用於漂白資金並協助大規模逃稅，案例顯示進口商及位於國外的生產商會利用多層次的空殼公司，用來購買國外貨物的資金會經過複雜之交易，但最後僅有其中部分資金，實際用於進口交易，剩餘資金則流入受益人控制之帳戶。

代理網絡亦使用多層化計畫，將金融體系內產生的犯罪所得，轉換為現金，這個網絡主要服務那些需要將犯罪所得從銀行帳戶轉為現金的客戶，大部分的客戶涉及侵占公款、稅務詐欺及網路詐騙。這些犯罪所得在最後階段，會轉入公司金融卡，隨後即提領出現金，其中涉及的空殼公司及個人銀行帳戶的數量可能超過數千個，因此可減少被偵測的風險並分散潛在損失。

專業洗錢人士在某些情況下，可能在國外提領現金。在案例中曾發現，資金流至登記於中東公司的帳戶後，再透過交易所提領現金，隨後將現金運回資金流出國，並於邊境虛偽申報該筆現金為於中東合法商業活動的利潤，並利用為了購置不動產的虛偽名目。

▪ 第 V 節：專業洗錢網絡採用之輔助機制

專業洗錢網絡使用各種洗錢工具及手法，其中最關鍵的機制為貿易洗錢、帳戶交割機制及地下金融。

▪ *貿易洗錢 (TBML)*

貿易洗錢定義為「透過貿易方式，掩飾犯罪所得及移轉價值以合法其非法來源之過程。」[3] 專業洗錢人士可採用各種貿易洗錢形式，包括：

- 以犯罪所得購買高價值貨物後，於國外裝運並轉賣貨物；
- 移轉之資金為貿易相關或購買未發貨或收貨的貨物 (亦稱為「影子裝運」)；
- 偽造所運送貨物的數量及 / 或價值高於或低於相對應之款項，協助移轉或收受犯罪所得之價值（亦稱為高報貨價或低報貨價）;
- 利用犯罪所得購買商品後，進行合法轉售，即由合法企業主（例如黑市披索交易所、黑市比索交易）向毒販 / 經銷商支付貨款；及
- 使用貨幣（披索）仲介，他們在毒梟盛行的犯罪所得的地區 (例如哥倫比亞及墨西哥），以折扣價購買毒品，再轉賣獲取價差，作為犯罪所得。貨幣仲介會根據販毒組織或犯罪組織的指示，僱用許多人士，負責收取並處置毒品的犯罪所得。

[3] FATF，2006 年。

專欄 10 洗錢網絡為貿易洗錢的基礎計畫之一環[1]

加拿大的 OROAD 專案進行聯合財務調查，發現某可疑集團[2]涉嫌從事毒品相關的洗錢活動，並從金融交易和報告分析中心 (FINTRAC) 處收到的情報，認定某複雜的貿易洗錢計畫，其中兩名主嫌僱用 10 位代名人，並建立 25 家空殼公司，這些公司採用不同行業的名稱，包括園林綠化、室內設計、電子產品、金屬回收、塑膠回收、建築用品、美容用品等。

這個洗錢網絡包括在金融及不動產行業經營的合法企業，以及與洗錢有關的小型金融公司。洗錢人士提供大量現金給共犯某金融公司，隨後再存入空殼公司的商業帳戶中，直到金融機構發現該空殼公司帳戶因大量可疑交易，並關閉該帳戶為止。

調查人員認為洗錢集團係使用貿易洗錢騙局，其中的洗錢計畫及空殼公司都主要集中在某物流公司，根據目擊者指出，其中一名洗錢人士攜帶大量現金離開物流公司，該筆現金疑似為販售毒品的犯罪所得，洗錢人士藉由代名人將多筆現金存入他們的個人及企業帳戶。

洗錢人士指示代名人 i）將資金匯回物流公司 ; 或 ii）將資金移轉到其他企業帳戶，並由位於加拿大、中國、巴拿馬及美國之代名人持有。資金透過電匯、銀行匯票或支票轉移，部分資金返還物流公司。洗錢人士多使用偽造發票方式，計算販售毒品所得，以便更容易將其整合到金融體系中。

調查人員認為，部分資金已匯回墨西哥販毒組織及由該組織控制在中國、墨西哥及美國的其他公司，犯罪組織利用這些犯罪所得購買巴拿馬或墨西哥貨物。加拿大的犯罪首領在這些國家建立公司，讓

這些犯罪所得的轉移看似合法，隨後將購買的貨物運往其他國家銷售，這些犯罪組織購買的貨物到達目的地國家後，隨即被出售，銷售所得（以目的地國家之貨幣）隨後移轉至販毒或洗錢組織，以提供犯罪份子透過貿易洗錢漂白的「乾淨」資金。

註：

1 請參閱第 III 節中之案例研究「操作蛇 (Operation Snake)」，其中涉及使用貿易洗錢及貨幣服務提供計畫之另一個專業網絡。

2 調查亦顯示，洗錢網絡與仲介之間進行大量現金交易，但此處重點著重在洗錢網絡。

來源：加拿大

專業洗錢製作及利用偽造文件與多層化相關之金融交易，設立空殼或架上公司架構虛偽的貿易交易。專業洗錢人士透過使用貿易洗錢機制，切斷前置犯罪與洗錢活動之間的關聯，亦模糊犯罪份子與洗錢活動之間的聯繫。

專欄 11 委內瑞拉貨幣走私網絡

一位西班牙人於 2015 年，設立 10 家有限責任公司，透過行動支付「銷售時點情報系統（「POS」）」處理超過 11 萬筆交易，總計 2240 萬歐元，其中 9 家公司據稱為旅行社與 8 家公司共用相同的登記辦公處所，其中的 6 家公司則擁有相同之員工及董事。

前述公司的 POS 終端專門收受委內瑞拉政府 (下稱「(Comisiún de Administraciún de Divisas - CADIVI)」所發行的支付卡。鑑於委內瑞拉實施嚴格貨幣管制政策，居民僅得於旅外時兌換外幣，因此，以 1 美元兌 6.3 玻利瓦之匯率而言，最高可兌換 3000 美元。在一起「el raspao」之大規模貨幣兌換詐欺案件當中，該案件假藉委內瑞拉居民在國外旅行之藉口取得歐元或美元，並使用 CADIVI 發行的

支付卡，以官方匯率在國外進行扣款，在此同時，毒販則獲得相同價值的歐元或美元現金，這些現金隨後被走私回委內瑞拉並在黑市以大約為官方匯率十倍的價格出售。在盧森堡的權責機關懷疑，大量 CADIVI 發行的支付卡走私到西班牙，並利用西班牙人頭公司運作的交易商共犯所使用的 POS 終端系統，進行刷卡。

據調查毒販及哥倫比亞毒梟係利用該貨幣走私網絡，將在歐洲販售毒品所生之犯罪所得現金匯回南美洲，這些犯罪份子透過將現金交付予委內瑞拉的貨幣販子，漂白其所有的非法現金，於資金漂白後，扣款金額會貸記於相關之銀行帳戶，案經調查這些銀行帳戶中的國際銀行帳號（「IBAN」）係由盧森堡曾經認證的電匯公司所發行。監理機關及金融情報中心執行的反洗錢調查顯示，盧森堡電匯公司未依規範管理這些帳戶，而是將其移交予保加利亞認證之電匯公司，該電匯公司將這些帳戶提供客戶使用。前述 POS 由保加利亞之電匯公司出售予西班牙人頭公司。此外，這些西班牙人頭公司已申辦該保加利亞電匯公司發行的數百張提款卡 (大多數人頭公司至少各擁有 10 張提款卡)，讓這些公司可自其帳戶提領現金。調查發現，在哥倫比亞的 ATM 出現約 106,000 次提領紀錄，金額超過兩千萬歐元，這些提領金額並未符合保加利亞電匯公司一般條款規定的每日、每週及每月提領上限，而且盧森堡權責機關並未發現保加利亞金融情報中心曾經收到任何可疑交易通報，另外發現盧森堡及保加利亞的電匯公司均由同一實質受益人持有。保加利亞的電匯公司光就該次操作收取之佣金即高達 1,900 萬歐元或等同經 POS 處理金額 9% 的價值。

來源：盧森堡

▪ *帳戶交割機制*

專業洗錢網絡可以協助多個犯罪組織間進行帳戶交割，可為在不同國家運作的犯罪組織，從現金中獲得收益，並讓銀行帳戶中存有資金，例如，專業洗錢人士可同時向持有現金並欲匯款至其他國家銀行帳戶的犯罪份子提供洗錢服務，以及銀行帳戶中有存款但需要現金（例如為支付其網絡及工作人員之費用）的犯罪份子，如此的運作方式稱為帳戶交割機制。

下列案例說明專業洗錢組織如何收取並以車輛移轉現金至比利時，作為協助帳戶交割機制之一環。

專欄 12 洗錢活動作為各犯罪組織間「帳戶交割騙局」之一環

數家比利時企業客戶將資金轉入比利時建築或工業清潔公司及其經理人之帳戶，這些公司均具有下列類似情況：為同一產業；經理人多來自同一國家；公司章程僅經微調而內容大同小異；這些公司財務狀況不佳，其中某些公司已破產或已未符合法律規定。

以不同帳戶提供資金：提領部分存入帳戶的現金，用來給付工資，另一部分資金則移轉至位於海外、歐洲及亞洲之公司。

移轉到歐洲的資金記入同一行業其他公司的帳戶，這些縱使為大規模資金的移轉，但未附資金移轉說明，而有附理由者，內容亦多含糊不清，而且大部分資金隨後以現金方式提領。

移轉到亞洲（主要是中國及香港）的資金則記入有限責任公司的帳戶，但這些公司業務內容與建築或工業清潔行業間無任何關聯。

依據金融情報中心對等機關收到的資料顯示，該公司與涉及販毒犯罪組織往來，因該犯罪組織持有大量現金，並利用此機制洗錢，將現金以車輛運送到比利時，中間人隨後在比利時，將現金交給需要

現金的各種比利時公司。

權責機關根據調查的資訊發現，涉及此案的比利時建築及工業清潔公司是帳戶交割騙局的一環，並將那些販毒的現金犯罪所得，最後用來支付比利時公司的非法勞工。

來源：比利時

▪ *地下匯兌及替代性金融平台*

地下匯兌業務為專業洗錢人士經常使用的工具，使用此機制，可以避開受監理的金融產業，打造資金移轉，且可保留交易及會計紀錄的平行系統。

專欄 13 調查大規模地下匯兌體系

嫌疑犯 X 及其於加拿大英屬哥倫比亞省之共犯網絡組成專業洗錢組織，為跨國犯罪組織提供許多重要服務，包括墨西哥毒梟、亞洲犯罪組織及中東犯罪組織。據估計，這些組織每年透過地下匯兌洗錢的金額超過 10 億加幣，其中涉及合法及非法賭場、貨幣服務提供商及購買資產。這個洗錢網絡非法活動部分資金來源為販毒所得、非法賭博資金及敲詐勒索之資金，並提供給在加拿大的中國賭客現金。

嫌疑犯 X 據稱協助富有賭客，將賭注從有限制法定貨幣流出的中國移轉到加拿大，中國賭客將資金移轉到嫌疑犯 X 及其網絡控制的帳戶，以在加拿大換取現金，但這些資金實際從外移轉出中國到加拿大，這些資金價值則是透過非正式價值移轉系統移轉，嫌疑犯 X 可以從每筆交易，獲得 3 到 5%的佣金。

在這個機制當中，中國賭客在溫哥華當地或在抵達前獲得聯絡人資訊，中國賭客打電話給聯絡人安排現金交付，交付地點通常為賭場

停車場，並將現金用來購買賭場籌碼，其中某些賭客會將籌碼換成「英屬哥倫比亞省賭場支票」，如此可存入在加拿大的銀行帳戶，其中部分資金會用於購買不動產。

調查發現，這些賭客提供大筆賭注的現金都源自於 X 公司，X 公司是未認證的貨幣服務提供商並由嫌疑犯 X 所有。調查人員發現，黑幫成員及馬伕向 X 公司運送一箱又一箱的現金，每天平均約約 150 萬加幣，監控情報也證實 X 公司與 40 個不同組織聯繫，包括販售古柯鹼、海洛因及安非他命的亞洲犯罪組織。

X 公司收取現金後，資金由嫌疑犯 X 或其網絡在海外分送，大多數交易均採現現金方式，避免被傳統銀行業務偵測，嫌犯 X 從中收取洗錢及轉帳服務之 5%佣金。隨著洗錢業務的擴張，X 公司的資金移轉能力變得愈加複雜，以至其可將資金匯入墨西哥及秘魯，讓毒販在購買毒品時無需攜帶現金至加拿大境外，藉此掩護使用中國的假貿易發票在國際間移轉資金。調查人員已在中國發現超過 600 個銀行帳戶被 X 公司控制或使用的證據，中國警方已著手進行調查，並將其歸類為龐大的地下匯兌系統。

來源：加拿大

替代性金融平台（「ABP」）乃是於受監理金融體系外營運的替代性金融服務平台，但替代性金融服務平台可使用正規銀行系統的設施，同時建立平行會計及交割系統，可以說是一種影子銀行的形式，其利用量身訂製的網路軟體，提供與銀行相同的服務，而無需經過監理及稽核或客戶盡職調查。替代性金融服務平台可以有效地進行匿名移轉貨幣所有權，並對數個人所擁有的銀行帳戶提供銀行服務，而不會如同傳統的銀行交易留下相關紀錄。替代性金融平台在特殊軟體的輔助下，可加密網路流量；管理同一平台內帳戶之間的交易；收取費用並協助與外部金融體系的流通。

專欄 14 替代性金融平台

犯罪份子利用替代性金融平台，協助英國犯罪組織漂白增值稅詐欺的犯罪所得，這個平台在某管轄地設有登記事務所，又在第二個管轄地設立控股公司，並在第三個管轄地設立銀行帳戶，此替代性金融平台由位於英國以外的第四個管轄地的專業洗錢網絡操作。這個平台運作一年後，移轉之資金超過 4 億歐元，之後遭到關閉，在英國稅務及海關總署（「HMRC」）的協助下，這個財務軟體的開發者被國際執法合作夥伴逮捕，並且蒐集這個平台的伺服器資料，進一步發現在其他平台發生的案件。

來源：英國

替代性金融平台所使用的軟體，通常基於依隨機資料生成器原理所運作，在某些情況下，專業洗錢人士使用專門軟體建構洗錢騙局，利用眾多帳戶隨機移轉資金。

▪ 第 VI 節：由共犯 / 犯罪者提供金融服務及其他專業人士

如第 II 部分所述，這些專業洗錢人士可能在金融服務行業（例如銀行家及貨幣移轉服務代理商）及指定之非金融事業及人員 DNFBPs（例如律師、會計師及不動產專業人士等）中佔據一席之地，並利用其職業、商業基礎措施及知識，幫助犯罪者客戶洗錢。利用專門職業人士可以為犯罪份子及犯罪組織提供合法性，因此，犯罪組織會積極尋找內部人士作為協助漂白犯罪所得的共犯，在極少數案例中亦發現，協助專業洗錢騙局的共犯來自政府機構（即貪污的官員）。

專欄 15 貪污官員

烏克蘭的執法及檢察機關對一名濫用職權及官方職位的高級官員進行大約 3 年的調查。該官員參與建立某犯罪組織，並從事非法活動，以協助降低稅務責任，從而非法獲得稅收抵免，該公務人員從中收到提供不法服務的現金，其中包含其他公務人員及犯罪組織的其他成員共同參與。

公務人員濫用其職權，包裝犯罪所得成為看似合法型態的金錢，其非法活動還包括代表犯罪組織成員設立、註冊及擁有一些空殼公司，並代表他們購買財產。該名官員還在塞浦路斯及英屬維爾京群島建立境外公司，以其親屬為代名人，並透過從列支敦士登的銀行移轉資金，收購在烏克蘭註冊的某境外公司控制的實體。那些被轉入烏克蘭的資金用來購買房產，並且利用虛構實體網絡，為那些未曾提供過的服務建立虛偽聯繫或協議（例如諮詢服務）。

來源：烏克蘭

這些專業洗錢人士經常忽略或規避防制洗錢 / 打擊資恐的要求，或主動隱蔽特定機構或企業內的防制洗錢 / 打擊資恐疏失，亦無視其職業上應行的義務，例如與其執照或職業道德規範相關的限制。雖然這種共謀行為係屬國內法的議題，但普遍觀點認為這是故意行為，對於這些特定人士所處理的資金為犯罪所得知情，或故意對其視而不見。洗錢計畫是否成功的最終衡量標準是犯罪份子購買或獲得金融業務所有權或控制權的能力。

犯罪份子將積極尋求在現有政府機構或企業內招募內部共犯，因為這些人可以接觸到內部，能夠在其中偽造紀錄或啟動交易、迴避防制洗錢 / 打擊資恐規定或機構慣例。犯罪份子在極少數情況下可能會破壞

整個機構或企業，包括獲得機構的所有權或控制權，以及任命自己的犯罪者管理整個機構。上述共犯活動（內部人員妥協及機構妥協）不應與法遵能力低落、內部控制薄弱或公司治理結構不完善的情況相混淆，如此可能導致防制洗錢 / 打擊資恐要求的法遵缺陷。然而，該機構低弱的法遵聲譽對於尋求貪腐內部人士的犯罪組織而言，可能更具吸引力。

▪ *金錢或價值移轉服務（下稱「MVTS」）提供者*

各代表團提供的案例研究及意見顯示，MVTS 提供者在知情的情況下協助專業洗錢活動，包括貨幣兌換（即外匯）、基於現金之交易及 / 或電子轉帳。合作的 MVTS 提供者可在洗錢過程之處置階段發揮重要作用，其中由 MVTS 提供者推動且最常見的洗錢交易為：

- 以現金購買的資金在 MVTS 提供者的所在地移轉 ;
- 個人及企業帳戶中之高額現金存款，隨後轉帳到國內 MVTS 提供者帳戶，或購買用來付給 MVTS 提供者的銀行匯票（例如銀行本票）；及
- MVTS 提供者幫個人及企業購買銀行匯票，用來轉帳資金。

專欄 16 使用外匯經紀商及「快遞」工具

一名英國技師擔任某專業洗錢網絡的專業洗錢人士，該名技師在英國開設銀行帳戶，於 2013 年 10 月至 2014 年 12 月期間，存入 530 萬英鎊的現金，其使用銀行「快遞」設施，每天將數筆 25,000 英鎊存入帳戶，一旦存進銀行帳戶，這些資金即透過銀行及外匯中間人，轉帳至英國及其他 6 個管轄地之第三人銀行帳戶。該技師因為將現金移轉到國外，獲取 2 萬英鎊之報酬，他最後因違反 3 項洗錢罪，

於 2018 年 4 月被判處 6 年刑期，並遭褫奪擔任公司董事 9 年。

快遞為可直接在銀行或在第三人設施存入現金之存款工具，點鈔後再移轉到銀行存入[4]，快遞設施使現金更快地存放於更多地點，且一般不會與員工接觸。

來源：英國

權責機關的分析顯示，作為共犯的 MVTS 提供者可能故意持續提交疑似洗錢或資恐交易報告（「STR」）。例如，為了不引起懷疑並且營造 MVTS 提供者遵守法規的形象，從而頻繁提交 STR。在需要其他形式交易報告的管轄地，如具有現金交易申報門檻，MVTS 共犯則會操作 2 套帳戶紀錄（即影子會計），其中一套專門用於犯罪客戶且無提交報告的紀錄，這些 MVTS 提供者共犯最後會陳報虛偽的交易報告與細節資料。

專欄 17 協助第三人洗錢之共犯貨幣服務提供者代理

義大利金融情報中心辨識出三年內移轉至「A」國家之匯款大幅減少（從 2012 年 27 億歐元降至 2015 年 5.6 億歐元），這些資料顯示具有透過特定「管道」處理犯罪所得的風險。

針對 STR 進一步分析發現，專業洗錢網絡將大量資金移轉到 A 國的其他替代管道。匯往 A 國匯款減少的原因，大部分與許多義大利 MVTS 代理商遷移到外國有關，他們遷移至無要求必須製作統計報告的國家，也不必受到義大利反洗錢及財政要求的規範。

4 UK National Risk Assessment of Money Laundering and Terrorist Financing，日期：2015 年 10 月。

金融情報中心收到許多來自義大利匯款代理商之 STR，這些金流的主要特徵為大量現金存款及電匯，流入至國外 MVTS 的義大利銀行帳戶。據瞭解，這些資金流動是由 MVTS 代理人進行的匯款。然而，由於代理商有時將現金存入與其業務所在地距離較為遙遠的銀行分行之帳戶，因而引起懷疑。金融情報中心遂擴大研究範圍，以便更清楚瞭解由 MVTS 及代理商進行的資金移轉活動，依其研究顯示，在某些情況下：

- MVTS 法律代表參與其中 ;
- 最近剛成立的 MVTS;
- MVTS 與 A 國的嫌疑犯有關 ;
- MVTS 在義大利城市開設一處分支機構，此分支機構以其與 A 國的經濟及商業關聯而聞名 ;
- 同一個國外 MVTS 之許多代理商均來自 A 國，已向義大利金融情報中心通報或因異常交易及為客戶審查（CDD）目的，使用偽造身分證件，而被 A 國主管金融監理機關禁止從事代理活動 ;
- MVTS 代理商讓其客戶與數個共犯一起將匯款拆分成數次處理 ; 及
- 特定 MVTS 代理商透露與共同客戶群的實際聯繫。

依據分析發現，MVTS 提供者及代理商違反防制洗錢義務，並利用不同國家間監理架構的不一致，由代理人及國外 MVTS 所組成的技術熟練之共犯網絡，在義大利籌募資金，並將大量資金移轉到國外，並與數名共犯平分匯款。

來源：義大利

▪ *金融機構*

使用國際金融體系有助於協助大規模專業洗錢計畫，第 IV 節所述之複雜多層化計畫，均涉及透過開設空殼公司，利用不同管轄地的銀行帳戶移轉大量資金，即使在涉及內部人員的情況下，這些組織因為具有運作良好的計畫，通常不會被銀行察覺。

調查機關已能夠辨識專業洗錢人士如何利用銀行管道，及其選擇某些管轄地及轉移犯罪所得的模式。例如，某些犯罪份子試圖利用於寬鬆監理環境下營運的銀行，或因不遵守洗錢防制或打擊資恐法規而聞名的銀行。

由於權責機關難以蒐集證據，證明金融機構有積極涉及協助洗錢活動情事，銀行內部人員通常亦不會公開談論洗錢行為，因此不法份子可利用其內部人員身分，隱瞞違法行為，如此可讓其他金融服務專業人員難以發現，亦無法追訴這些蓄意違法的行為，此種結果反而是金融機構內的員工（從較基層櫃員到資深管理人員）成為洗錢者可利用的重大漏洞，如果資深的內部管理階層人員加入幫忙洗錢，將對金融機構造成更大的損失。

作為共犯的銀行員工可執行以下功能：

- 製作偽造支票；
- 監督（或不適當的監督）由共犯控制的帳戶間之資金流動；
- 協調金融交易以規避申報可疑交易報告；
- 接受客戶提供的偽造文件為交易基礎，不追問其他問題；及
- 在客戶帳戶內進行「虛擬交易」，意即實際上雖然進行大量交易，但帳戶淨值在該工作日開始至結束，未發生任何變更。

專欄 18. 外國銀行總經理及董事長

義大利調查機關揭露由外國銀行資深官員（總經理及董事長）及共犯會計師及律師進行的各種洗錢行動，犯罪所得源自某國際古柯鹼販運組織。

犯罪份子與外國銀行的總經理及董事長勾結，該銀行當時正經歷嚴重的流動性危機。犯罪份子及銀行高層主管同意，讓其中一名毒販以自己名義，在這個危機中，向銀行存入約 1500 萬歐元，該銀行承諾提供兩名專業人員（即上述律師及會計師，其為兄弟）一定數額的資金，並記入以其名義在該銀行特別開立的帳戶當中，作為他們居中工作的報酬。

會計師負責替毒販所有的數家公司執行會計業務，在居中活動之後，該銀行的總經理從毒販名下的存款中，分兩批領取 130 萬歐元，總經理隨後在銀行董事長核准下處理複雜的金融業務，以隱匿存款的非法來源。

權責機關在此案中確認律師作為其客戶（保管人）與銀行間中間人的功能，以及確認律師知悉案件中所涉金錢的實際不法來源。

來源：義大利

下面的案例示範不同要素及措施的組合，包括出售空殼公司、協助共犯銀行員工之交易及執行證券市場交易。

專欄 19 共犯銀行員工、證券市場交易及出售空殼公司

俄羅斯機關與金融情報中心共同合作，查獲銀行員工及中間人共謀安排的洗錢及逃稅計畫。

空殼公司銀行帳戶累積的資金依中間人 R 人士之指示，以購買證券

為藉口，移轉到國外。同時，在倫敦證券交易所經營的兩家經紀公司則以相同價格出售股份，進而協助透過影子交易移轉資金。
調查發現，此洗錢計畫中使用的有限責任公司，均由同一家法律服務公司建立，其專門銷售「既有」之公司。此案隨後進入刑事訴訟程序，其中一家協助跨境移轉的銀行及證券公司的證照，因違反防制洗錢法規而被撤銷。
來源：俄羅斯聯邦

從案例分析及收到資訊顯示，私人銀行顧問可充當專業洗錢人士，並透過採用各種手法，隱匿資金的性質、來源、所有權及控制權之服務，以規避審查，包括：

- 以帳戶實質受益人外的個人或境外實體名義開立及轉帳的銀行帳戶；
- 對銀行所要求識別客戶並揭露帳戶實質受益人之文件為虛偽陳述；
- 利用「諮詢服務」協議及其他類似之合約，為非法電匯創造合法性；
- 在同一銀行開立並使用多個帳戶，以便在內部管理這些帳戶間之資金移轉，而未使用資訊更透明的國際清算機制；及
- 以名稱類似的公司在相同或不同機構開設數個銀行帳戶，使電匯看似非來自第三人。

▪ *法律及專業服務*

為延長犯罪活動與資金流動的距離，有些犯罪組織使用第三人洗錢人士之服務，包括專業守門人如律師、會計師及信託及公司服務提供業（下稱「TCSP」）。某代表團指出，犯罪組織傾向使用專業服務，建立公司組織，且會計師因其可提供之各種專業技能及服務而受到青睞。

實際案例證明，這些專業人員已被招募成為代表規模大的犯罪企業（如販毒集團 DTO）的專業洗錢人士。2013 年 FATF 的洗錢及資恐法律專業人士在洗錢／資恐漏洞報告中提到，犯罪份子經常尋求法律專業人員，參與其洗錢及資恐活動，原因在於某些交易需要這些專業人員提供專業法律及公證技能及服務，協助漂白犯罪所得。

專欄 20 共犯律師及銀行職員

德州的一名律師因為協助犯罪組織洗錢並參與各種詐欺計畫而被定罪。該犯罪組織在美國、加拿大、非洲、亞洲及歐洲運作，其中一名共犯為銀行職員也因偽造支票且負責監控由犯罪組織控制的數個帳戶間之資金流動而被定罪。

多個詐欺計畫當中的所有被害人皆收到指示，將被害款項匯入由其他共謀（錢騾）持有的漏斗帳戶（funnel account），錢騾迅速在被害人發現被詐騙前，即將款項移轉到其他美國及全球其他帳戶，並利用此方式漂白數百萬美元。錢騾所開設之眾多銀行帳戶為洗錢過程中的第一層，因此讓共犯可遠離或隱瞞犯罪所得的來源及性質。例如，同一名錢騾在一年間開立 38 個詐欺性之銀行帳戶。

詐欺計畫有多種形式。許多被害人是經由網路招募的律師事務所，將犯罪組織提供的偽造銀行本票，存入事務所的信託帳戶。這些律師事務隨後依照指示，將金錢匯入由共犯所控制的第三人空殼公司，詐欺計畫當中亦包括僱傭駭客，破壞個人及事務所的電子郵件帳戶，要被害人從中間人及企業帳戶將錢匯入由共犯集體控制的空殼帳戶。這些空殼公司在佛羅里達州以虛構名稱註冊成立用於開設在佛羅里達州銀行的帳戶。

此案中的德州執業律師作為共犯，透過律師信託帳戶（「IOLTA」）的利息，漂白被害人被詐騙的款項，其亦與個人錢騾見面，自漏斗帳戶中取回現金，並招募律師助理及其他人士，開立洗錢計畫中使用的銀行帳戶。

來源：美國

其中一起案件涉及由某執業律師擔任犯罪組織的正式成員。如前述專欄所述，該名律師透過其律師信託帳戶之利息或 ILOTA[5] 以移轉毒品及詐欺的犯罪所得，以此方式協助洗錢。

專欄 21 CICERO 行動

本案例係由 Guardia di Finanza 內之特別貨幣警察小組在針對義大利巴勒摩（Palermo）境內主要的犯罪組織（La Cosa Nostra 或 LCN）領導人展開的司法授權搜索並在後續調查時所破獲。這個案件調查目的是欲確認作為犯罪組織代名人及代表 LCN 協助犯罪所得流動之主嫌。案經調查發現，一位知名律師為透過在巴勒摩的建築公司洗錢的公司實質受益人，該公司與犯罪組織領導人的家屬有關聯。

這個律師為 LCN 犯罪組織執行財富管理儲蓄箱（money box）的功能，包括管理犯罪集團的財務狀況，目的係為隱匿犯罪所得的來源，並避免權責機關發現。涉案律師利用這些犯罪所得所購置的任何資產，透過律師的職業專業人脈，開創社交網絡，隨後將這個社交網絡交給犯罪組織利用。

5 IOLTA 係由律師開設之帳戶，旨在為客戶持有資金，該帳戶係依律師與客戶關係及相關交易於具較高保密性之銀行所開立。

該名律師以專業洗錢人士身分提供多項服務，例如：（a）代表組織犯罪的家庭成員以犯罪所得購買 45 萬歐元的公寓並取得房貸；（b）使用假合約代表犯罪份子購買 11 萬歐元的公寓；（c）分層化及整合合法資金與以犯罪所得所購置土地上所進行的建築工程所生之犯罪所得。

這件案件調查最後對 9 名人士、涉案總金額為 55 萬歐元及該律師擁有的 7 處房產執行沒收。

來源：義大利

專業洗錢人士經常使用空殼公司，協助複雜的洗錢計畫，他們成立空殼公司時，可使用的專業服務如信託、公司服務提供者或律師的服務。這些專業人士可提供全方位服務，包括設立公司、提供代名董事及協助開立新銀行帳戶等。

專欄 22 使用空殼公司及會計師提供公司秘書服務

G 人士為一名特許會計師，提供中小企業公司的秘書服務，服務內容包括代表其客戶設立公司，並為非居住於新加坡之公司董事擔任常駐董事。

某國外集團成員之 N 人員及 S 人員聯絡 G 人員並同時成立 3 家公司：K 公司、W 公司及 M 公司，並在新加坡申請公司銀行帳戶。該帳戶成立後，N 及 S 人員隨即離開新加坡且不再返回，G 人員既非股東亦非這些公司之銀行授權簽署人，但卻被指派擔任 3 家公司之聯合董事。

這些公司的銀行帳戶收到的犯罪所得都是來自各種詐欺行為，金額超過 65 萬新幣，這些資金很快被 S 人員移轉到海外銀行帳戶。

犯罪者利用這些公司，犯下移轉犯罪所得的罪行，並把責任歸咎於

G 人員缺乏對公司事務監督的疏忽，使國外集團能夠順利控制公司，且不受阻礙地參與其洗錢活動。G 人員於 2016 年 1 月，因洗錢犯行，且未合理盡職地履行董事職責被判被判 12 個月有期徒刑，罰款 5 萬新幣，且在刑期結束後的 5 年內褫奪擔任公司董事的資格。

來源：新加坡

專業洗錢人士以空殼公司名義開設銀行帳戶後，可以從海外操作這些帳戶，從不同的個人及公司獲取犯罪所得，並將資金進行多層化漂白，這些空殼公司帳戶中收到的資金通常會在數天之內，移轉出管轄地。信託或公司服務提供者通常對其客戶實際使用公司的內容不知情，因此不認為自己是洗錢計畫中的共犯。然而，有些案例研究顯示，某些信託或公司服務提供者以「不詢問」或不受官方檢查為特色行銷自己的服務。此外，如信託或公司服務提供者亦擔任公司董事者，其必須履行董事的職責，並對公司所犯之違法行為負責，如上述案例所述。

全球執法機構均注意到，專業洗錢計畫通常採用公司型態，專業服務提供者則協助建立架構，執法機構目前已確定使用複雜的公司架構及境外工具，隱匿受益權並協助移轉犯罪所得，且專業洗錢網絡在建立架構時，亦利用信託或公司服務提供者服務。全球許多調查指出，無論是大型企業或較小型的信託或公司服務提供者，都有人擔任具有類似公司架構的代名董事，包括：

- 僅用「勾選」方式執行法遵活動；
- 遠離風險（即弱化其責任）;
- 在數個管轄地內使用一連串設立代理人 ;
- 故意疏忽之行為；及
- 偽造簽名及偽造的公證文件。

專欄 23 透過販毒相關之不動產投資、餐飲服務及節目製作服務洗錢

根據美國財政部的海外資產控制辦公室（OFAC）收到的資訊啟動調查，調查發現，一個非法網絡正在阿根廷進行商業活動，並與一名疑似犯罪組織成員 J.B.P.C. 有聯繫。

J.B.P.C. 及其家人與商業夥伴為全球許多公司的股東，其中 3 家阿根廷公司（2 家營運公司及 1 家管理公司）在阿根廷境內發展大規模的不動產專案，而這些公司的總裁及主要股東為 B 先生，他身為 J.B.P.C 的律師及朋友，B 亦提供有關如何發展業務的知識及經驗，另外調查發現 J.B.P.C. 亦為另外 2 家公司之股東，這些公司是進行重大不動產開發案的土地所有人。

調查機關蒐集的稅務資訊顯示，這些公司收到 C 人士的會計專業建議，C 人士為一名特許會計師，亦為相關公司之股東及董事會成員。J.B.P.C 進行的其他交易亦於同一時期被查獲。案經調查這些交易與另外 2 家提供酒吧服務、咖啡服務及節目製作服務的阿根廷公司有聯繫，其中 1 家還是 OFAC 名單上制裁的公司，經查發現該公司的股票係由 J.B.P.C. 之第一等親屬完全擁有，且管理職位係由其合夥人及近親所擔任；另一家與 J.B.P.C. 有聯繫的公司在另一位律師 D 人士之協助下在阿根廷開設辦公室。

本案調查由阿根廷金融情報中心 (FIU-Argentina) 與其他國內執法機關及哥倫比亞金融情報中心（FIU-Colombia）及美國（OFAC 及 DEA）的外國夥伴機關等協調合作，強化國際間合作對於該項案件調查的成功而言至關重要，並聯合對阿根廷及 J.B.P.C. 主要非法活動所在之其他國外管轄地同時進行大量搜查。最後，J.B.P.C、B 先生及其配偶 C 人士及 D 人士遭逮捕；這些人士之財產亦遭扣押。目前，渠等正面臨阿根廷之起訴。

來源：阿根廷

▪ *支付處理公司*

支付處理公司向商家及其他商業實體提供支付服務，例如信用卡處理或薪資處理服務，支付處理業持有的銀行帳戶通常用來協助代表客戶付款。支付處理公司在一些特定情況下，會充當「流通」帳戶（不需提供個人客戶身分予金融機構）。設立支付處理公司，在傳統上是為了處理傳統零售商的信用卡交易。然而，支付處理公司已逐漸發展為服務各種國內及國外商家，包括網路電商及傳統零售商、網路遊戲企業及電話行銷公司等。

犯罪組織可使用支付處理公司，掩飾交易並漂白犯罪所得，例如，已發現利用支付處理公司，將源自國外的犯罪所得直接存入金融機構[6]。某些國家發現洗錢網絡所使用的支付處理公司，另外也發現電話行銷公司亦疑似提供支付處理服務，包括結合犯罪所得及大規模行銷詐欺有關的詐騙款項。權責機關懷疑這類型的支付處理公司，可能已經遭到數個跨國犯罪組織成員及相關人士利用。

6 FINCEN，日期 2012 年；及 FFIEC(無日期)。

專欄 24 國際支付處理商提供洗錢服務

PacNet 是加拿大溫哥華的國際支付處理公司及貨幣移轉服務提供者，協助數十名詐欺犯獲得美國銀行之授權。PacNet 擁有 20 年洗錢及郵件詐欺之歷史，以故意發送予全球受害者之郵件詐欺騙局處理付款。於 PacNet 關閉時，發現這個網絡組織係由橫跨 18 個國家的 12 名人士及 24 個實體所組成，涉及詐騙全美數百萬弱勢被害人，詐騙總金額高達數億美元。

PacNet 在加拿大、愛爾蘭及英國及其他 15 個國家 / 地區之子公司或關係企業發展業務，提供各種郵件詐欺騙局，在美國的消費者每天幾乎會收到數千萬封有關樂透及其他主題的詐欺信件，這些詐欺信主要目的是詐騙老年人或其他弱勢群體。

PacNet 的處理業務有助於掩飾犯罪所得之性質，並防止詐欺計畫被查獲。在典型的情況下，詐騙人士寄詐騙信件給被害人，再安排將被害人的付款（包括支票及現金）直接或透過合作公司，發送到 PacNet 進行後續處理。這些被害人的被騙金錢 (扣除 PacNet 費用及佣金) 會透過 PacNet 所持有的帳戶，電匯給詐騙成員，並由 PacNet 代表詐騙成員支付相關款項，進而掩護其與詐騙者間之聯繫，所有的過程都是為了盡可能降低金融機構發現詐騙者並認定資金涉及可疑活動之可能性。

這個複雜的詐騙郵件計畫涉及遍布全球的參與者，各計畫均遵循類似模式運作，包括涉及一個實體組織，其中有直接郵寄者、名單中間人、印刷業者 / 分銷商、郵寄公司，「綁定」服務[7] 及支付處理商，由前述 6 個不同的團體共同運作：（i）每年郵寄數百萬招攬資訊包，（ii）收取並分配每年度被害人所支付之數千萬美元詐騙款項，以

及（iii）向全球受害者及執法機構掩飾其真實身分。

來源：美國

▪ *虛擬貨幣支付產品及服務（「VCPPS」）*

如第 **IV** 節所述，專業洗錢人士提供各種服務，包括使用虛擬貨幣隱匿犯罪份子身分及其非法交易，並利用複雜、以電腦操作的詐欺計畫，讓網路犯罪份子建立大規模之洗錢機制，移轉犯罪所得。更具體而言，虛擬貨幣兌換業者被視為未經認證或未登記之貨幣移轉服務提供者，將虛擬貨幣形式的犯罪所得轉換為法定貨幣。FATF 於 2015 年頒布指引，建議並說明在虛擬貨幣支付產品及服務背景下，虛擬貨幣兌換業者應遵守相關規定，並確定可能需要的防制洗錢及打擊資恐[8] 措施。然而案例研究顯示，這些共謀故意設立、組織並被公認為犯罪企業的虛擬貨幣兌換業者已然存在。

電子數位支付系統亦可幫助其他犯罪，包括電腦駭客及勒索軟體、詐欺、盜用身分竊盜、退稅詐欺計畫、貪腐及販毒，身為共犯的虛擬貨幣提供者亦利用空殼公司及關係實體，滿足全球網路客戶，並以電子數位方式，將法定貨幣先轉入再轉出這些交易所（可視為有效的電子貨幣錢騾），這些共謀服務的用戶利用服務提供者建置的聊天平臺功能，公開討論犯罪活動，客戶服務代表伺機就如何處理並使用在暗網市場販售毒品所得提供建議。

---

7 一般由僱用執行各服務之第三人處理郵件直接回應，可能包括這些服務之付款處理、編輯產品訂單、更正收件人地址、處理退回郵件、提供密碼服務及存入資金及相關資料之處理。 Caging 是綁定服務之簡易術語。

8 FATF，日期 2015 年。

專欄 25 虛擬貨幣兌換業者共犯

美國加州北區聯邦地方法院於 2017 年 7 月 26 日起訴 1 名俄羅斯人及其所經營的組織 BTC-e，該組織負責經營無照金錢服務業務，並犯下洗錢及相關犯罪。起訴書稱 BTC-e 為犯罪份子提供國際洗錢服務計畫，特別是網路犯罪份子，這種方式已經演變成全球犯罪份子將犯罪所得洗錢的主要手段。起訴書指出 BTC-e 的 1 名經營者指導並監督 BTC-e 之營運及財務活動，其他人故意設立、組織、營運及公開宣傳 BTC-e 是犯罪企業，並開發犯罪份子客戶群。BTC-e 是全球最大且被廣泛使用的虛擬貨幣兌換業者之一。調查顯示，BTC-e 在其營運過程中，獲取價值超過 40 億美元之虛擬貨幣，法院除起訴 BTC-e 及其中 1 名實際人士外，美國金融犯罪稽查局（FinCEN）另與司法部密切協調，對 BTC-e 故意違反美國反洗錢法律提出 1.1 億美元之民事罰款。

來源：美國

▪ 第 VII 節：結論

本份威脅報告談論包括專門提供專業洗錢服務的犯罪組織及在洗錢過程中故意參與或有意疏忽的共犯。報告基於大量案例研究，包括專業洗錢的作用及功能；使用之商業模式及相關類型及計畫，已經確認專業洗錢的許多特徵。如有需要可提供 FATF 成員及 FATF 全球網絡非公開版本的報告內容，在該非公開版本的報告中涵蓋更詳盡的資訊，例如偵測、調查、起訴及預防洗錢的實用建議。

參考文獻

FATF (2006), *Trade-Based Money Laundering*, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/tradebasedmoneylaundering.html

FATF (2012a), *FATF Recommendations*, FATF, Paris, France, www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfrecommendations.html

FATF (2012b), *FATF Guidance on Financial Investigations*, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/operationalissuesfinancialinvestigationsguidance.html

FATF (2013a), FATF Methodology for assessing compliance with the FATF

Recommendations and the effectiveness of AML/CFT systems – FATF Methodology,

FATF, Paris, France, www.fatf-gafi.org/publications/mutualevaluations/documents/fatfmethodology.html

FATF (2013b), *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/mltfvulnerabilities-legal-professionals.html

FATF (2015), *Guidance for a Risk Based Approach to Regulating Virtual Currency*, FATF, Paris, France www.fatf-gafi.org/publications/fatfgeneral/

documents/guidance-rba-virtualcurrencies.html

FATF Egmont Group (2018), *Concealment of Beneficial Ownership*, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/concealmentbeneficial-ownership.html

FFIEC (nd), Bank *Secrecy Act, Anti-Money Laundering Examination Manual, ThirdParty Payment Processors—Overview*, Bank Secrecy Act/Anti-Money Laundering InfoBase, Federal Financial Institutions Examination Council: www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_063.htm

FINCEN (2012), *Risk Associated with Third-Party Payment Processors*, FIN-2012-

A010. October 22, 2012, Department of the Treasury Financial Crimes Enforcement Network, Washington, United States, October 22, 2012, https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A010.pdf