洗錢防制工作年報

中華民國一〇九年

ANTI-MONEY LAUNDERING
ANNUAL REPORT, 2020

法務部調查局編印
Investigation Bureau, Ministry of Justice,
Republic of China (Taiwan)

法務部調查局一〇九年洗錢防制工作年報

Investigation Bureau, Ministry of Justice

Anti-Money Laundering Annual Report, 2020

序 言 PREFACE

109 年 COVID-19 疫情嚴重衝擊全球各地的生活及工作型態，直至撰寫本序言的今日，全球仍籠罩在疫情風暴中，世界各地正面臨一波又一波變種病毒的肆虐及挑戰，各國政府雖傾全力防疫、設法提高疫苗施打覆蓋率、祭出諸如邊境管制、城市封鎖、保持社交距離、居家隔離及振興經濟等措施，然如此迥異於過往熟悉日常的新生活模式，除了影響一般民眾外，也對各國金融體系、洗錢防制及打擊資恐機制造成重大改變。

特別感謝國內各相關公私部門、申報機構、受通報機關及國外對等機關，值此疫情嚴峻的時刻，仍堅守崗位，為追查犯罪、打擊不法，積極在防制洗錢及打擊資恐工作貢獻己力；109 年間，本局受理可疑交易報告、一定金額以上通貨交易資料及海關通報旅客（含隨交通工具服務之人員）攜帶或以貨運運送、快遞、郵寄等方法運送用於洗錢物品數量分別達 24,406 件、3,052,856 件及 269,841 件；另外在國際合作方面，本局洗錢防制處透過艾格蒙聯盟（Egmont Group）安全網絡與其他超過 160 個會員國交換防制洗錢或打擊資恐情資，其品質、數量及成效均獲會員國好評，109 年共進行 168 案、723 件情資交換。

在疫情的衝擊下，許多洗錢防制國際會議被迫取消或改為線上舉辦，例如原先預計在 109 年年中舉辦的亞太防制洗錢組織（Asia/Pacific Group on Money Laundering，APG）年會及艾格蒙聯盟年會，均因 COVID-19 疫情及邊境管制措施而停辦；防制洗錢金融行動工作組織（Financial Action Task Force on Money Laundering，FATF）第 31 屆第 3 次全體會議及各工作組會議亦因疫情關係改為線上方式辦理。本局洗錢防制處仍把握以非實體方式汲取國際寶貴資訊，積極參與 APG 等國際組織的多場線上會議及研討會，掌握國際洗錢防制規範趨勢及深化國際合作。

此外，公私協力夥伴關係（Public-Private Partnership）是促進洗錢防制機制發展及效能的關鍵動力之一，本局洗錢防制處在 109 年除了協助申報機構辦理 42 場等防制洗錢及打擊資恐教育訓練外，也陸續與金管會、警政署、廉政署、海巡署、關務署、稅務機關等權責及執法機關進行多次業務聯繫座談，溝通金融情資運用之實務需求，並舉辦「犯罪金流分析與異常交易態樣研討會」，邀請公私部門單位參與，分享國際最新資

訊、規範及趨勢，聚焦國內近期發生之案例與犯罪風險，提供執法機關、監理機關與申報機構直接交流與互動，全面提升洗錢防制工作綜效。

為回應讀者欲深入瞭解洗錢與資恐犯罪態樣及趨勢的需求，109 年度洗錢防制工作年報收錄比以往更廣泛的案例，這些案例皆係本局偵辦並以洗錢防制法或資恐防制法移送，其中不斷翻新的洗錢手法甚具參考價值；另外，本局洗錢防制處自 108 年 11 月起，陸續接獲來自不同金融機構申報具有相同或類似特徵之可疑交易報告後，察覺網路銀行人頭帳戶有風險提升趨勢，遂將相關態樣蒐整進行分析，製作「網銀人頭帳戶」策略分析報告，提供政策建議及趨勢分析，亦收錄於本年報。

隨著虛擬貨幣及虛擬資產的蓬勃發展及廣泛使用，近年來 FATF 在多份文件中，不斷更新虛擬資產防制洗錢及打擊資恐機制相關建議及規範，國內也於 107 年 11 月公告修正洗錢防制法，將「虛擬通貨平台及交易業務之事業」納入洗錢防制規範對象，110 年 7 月虛擬通貨業者正式納入洗錢防制申報機制。有鑑於針對虛擬資產業的規範與機制，是近期國內外洗錢防制工作一大重點項目，本局徵得 FATF 同意後，由洗錢防制處同仁將 109 年 9 月出版的「虛擬資產洗錢及資恐紅旗指標（Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets）」翻譯成中文收錄於本年報；另一份 FATF 文件「貿易型洗錢：趨勢與發展（Trade-based Money Laundering: Trends and Developments）」則針對傳統及新興的貿易型洗錢犯罪活動做了詳盡描述，提出相關行業風險評估及打擊此類型犯罪的建議。兩份國外洗錢防制資料謹供相關權責機關及私部門，作為未來申報可疑交易報告、制定相關政策或修正相關機制參考。

法務部調查局　局長

謹識

中華民國 110 年 8 月

編輯說明

一、編輯目的

FATF 於 101 年 2 月修正之 40 項建議中第 33 項建議：「各國應維護有關防制洗錢與打擊資助恐怖分子系統之效能與效率的綜合性統計數據，包括可疑交易報告之受理及分送，洗錢及資助恐怖分子案件之偵查、起訴、判決，財產之凍結、扣押、沒收及司法互助或其他國際請求合作案件之受理。」因此，本年報彙整一年來國內申報機構執行防制洗錢及打擊資恐工作之資料加以統計分析。

二、編輯內容

本年報分下列六個部分：

（一）組織簡介。

（二）工作概況（含統計圖表資料）。

（三）重要案例。

（四）策略分析報告。

（五）國外洗錢防制資料。

（六）洗錢防制處重要紀事。

三、凡例

（一）本年報所用各項單位，年度未特別表示者皆為以國曆紀年，提及國際性活動、策略分析報告部分參考文獻出版年度及國外洗錢防制資料則以西元紀年表示。可疑交易與一定金額以上通貨交易（以下簡稱：大額通貨交易）報告，以件為單位；海關之通報資料，

以筆為單位。金額以新臺幣元表示。情形特殊者分別於各該表（圖）中說明。

（二）本年報所稱「本局」指法務部調查局，稱「本處」指法務部調查局洗錢防制處。

（三）各項數字之百分比，採四捨五入方式計算，總數與小數點間或略有差異。

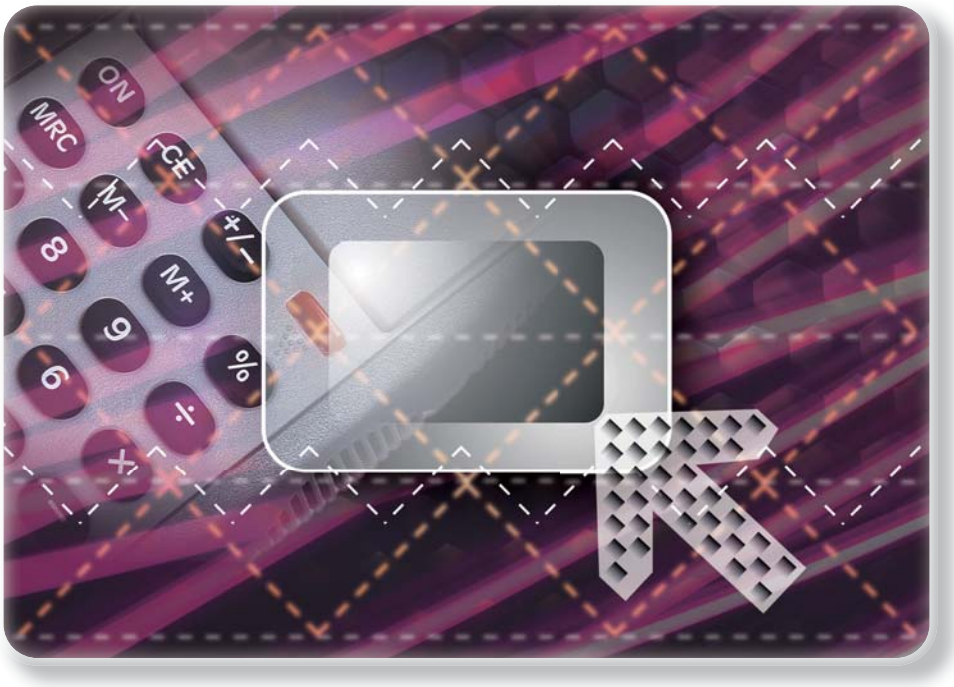
（四）本年報第二部分工作概況之相關統計數據係以 110 年 7 月 13 日為基準日。

表目錄

圖目錄

第一部分

組織簡介



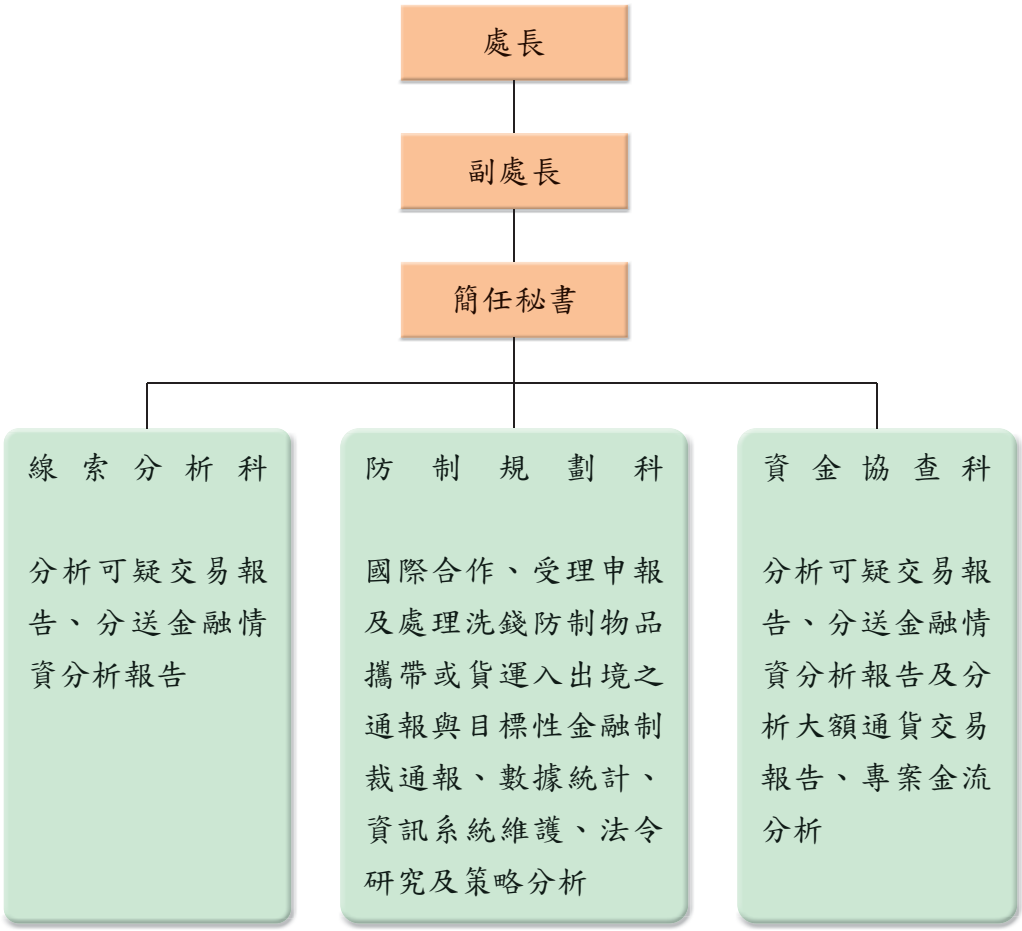
國際間鑑於毒品犯罪所獲得巨額利潤和財富，使得犯罪集團能夠滲透、腐蝕各級政府機關、合法商業或金融企業，以及社會各階層，因此西元 1988 年聯合國於維也納會議時，訂定《聯合國禁止非法販運麻醉藥品及精神藥物公約》（簡稱維也納公約）即要求締約國立法處罰毒品犯罪的洗錢行為。七大工業國體認到毒品犯罪所涉洗錢行為，對於銀行體系與金融機構產生嚴重威脅，於 1989 年之高峰會議中決議設置防制洗錢金融行動工作組織（Financial Action Task Force on Money Laundering，以下簡稱：FATF），發展並提升國際對於打擊洗錢之回應。FATF 於 1990 年制訂 40 項防制洗錢建議，作為國際間防制洗錢之標準規範，1996 年 FATF 修正 40 項建議，更進一步將洗錢的前置犯罪擴大至毒品犯罪以外其他重大犯罪行為，2001 年以後，FATF 又陸續將任務擴大到打擊資助恐怖主義及打擊資助大規模毀滅性武器擴散。

我國政府洞察洗錢犯罪之危害性，順應世界潮流，制定《洗錢防制法》草案，於民國 85 年 10 月 23 日經立法院通過，並奉總統明令公布，自 86 年 4 月 23 日施行。歷經 20 餘年的實務運作，執行成果已獲國際防制洗錢組織高度肯定，更針對實際所遭遇之問題，先後於 92 年、95 年、96 年、97 年、98 年、105 年及 107 年修法，以符合防制洗錢及打擊資恐的國際標準規範並兼顧實務運作之需要。

為防杜犯罪者利用金融機構等管道洗錢，並於交易之際發現可疑跡象，各國防制洗錢法律多課以金融機構申報大額通貨交易及可疑交易之義務，而負責受理、分析大額通貨交易報告及可疑交易報告之機構，即為金融情報中心（Financial Intelligence Unit，FIU）。我國洗錢防制法於 85 年間制定時，即借鏡各國法制，規定金融機構須向行政院指定機構申報可疑交易報告，本局於 86 年 4 月 23 日奉行政院核定〈法務部調查局洗錢防制中心設置要點〉成立「洗錢防制中心」執行金融情報中心及防制洗錢所涉相關業務。後於 96 年間立法院通過《法務部調查局組織法》，其中第 2 條第 7 款明定本局掌理「洗錢防制事項」，第 3 條明定本局設「洗錢防制處」。又 105 年 7 月公布施行之資恐防制法第 7 條規定由本局受理目標性金融制裁對象之財物或財產上利益通報。目前洗錢防制處下設線索分析科、防制規劃科與資金協查科，109 年間編制配賦人員 26 位。組織、分工及作業流程，如圖 A 與 B。依法務部調查局處務規程第 9 條，洗錢防制處掌理下列事項：

1. 洗錢防制相關策略之研究及法規之協商訂定。
2. 金融機構申報疑似洗錢交易資料之受理、分析、處理及運用。
3. 金融機構申報大額通貨交易資料與海關通報攜帶或運送洗錢防制物品資料之受理、分析、處理及運用。
4. 國內其他機關洗錢案件之協查及有關洗錢防制業務之協調、聯繫。
5. 與國外洗錢防制有關機構之資訊交換、跨國洗錢案件合作調查之聯繫、規劃及執行。
6. 洗錢防制工作年報、工作手冊之編修與資料之建檔及管理。
7. 其他有關洗錢防制事項。

圖 A：洗錢防制處組織圖



◎防制洗錢金融行動工作組織（Financial Action Task Force，FATF）

七大工業國於西元 1989 年在巴黎舉行之高峰會議，體認到洗錢行為對於銀行體系與金融機構之威脅，遂決議設置 FATF。而 FATF 負有了解洗錢技術與趨勢的責任，並審視各國對於洗錢行為是否業已採取國際標準及制定措施加以防制。為建立一般性適用之防制洗錢基本架構並致力於防止犯罪行為人利用金融體系，FATF 乃於 1990 年制定 40 項建議，並於 1996 年及 2003 年修正，以掌握洗錢威脅的發展，為因應 2001 年美國恐怖攻擊事件，於 2001 年、2004 年陸續增訂打擊資助恐怖活動的特別建議共 9 項，2012 年 2 月 FATF 會員大會通過「打擊洗錢及資助恐怖分子與武器擴散之國際標準」，將原 40 項防制洗錢建議及 9 項打擊資助恐怖活動特別建議予以整併及修正，同時新增反資助大規模毀滅性武器擴散建議。

FATF 會員國及區域性防制洗錢組織（FATF-Style Regional Bodies, FSRBs）會員間均利用自我評鑑（Self-assessment）或相互評鑑（Mutual Evaluation）等方式，以確保上開建議得以有效遂行。

目前 FATF 計有 39 個會員（37 個司法管轄體會員、海灣合作組織及歐洲議會等 2 個組織性會員）、9 個區域性防制洗錢組織為準會員（Associate Member）及 1 個觀察員（Observers），可全程參與會員大會及工作組會議。

◎金融情報中心（Financial Intelligence Unit, FIU）

依 FATF 第 20 項建議：「金融機構有合理依據懷疑資金係犯罪收益或與提供恐怖活動有關時，應儘速直接依法令所定之義務向金融情報中心提出申報」。第 29 項建議：「各國應設立金融情報中心作為全國性統一受理、分析可疑交易報告及其他有關洗錢、相關前置犯罪及資助恐怖活動之資訊，並分送分析結果」。而依據各國金融情報中心所組成的國際組織「艾格蒙聯盟」（Egmont Group），將金融情報中心定義為：「負責受理（或經同意可提出請求）、分析下列揭露之金融資訊，並送交權責機關之全國性中央單位：

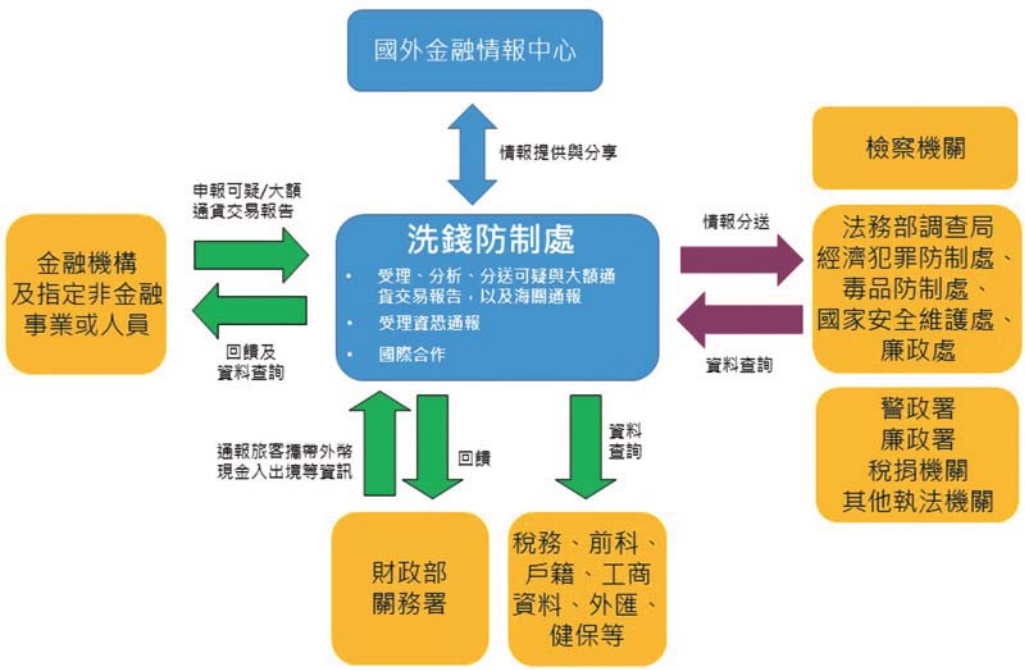
（i）可疑的犯罪財產，或

（ii）國家法令所定之防制洗錢資訊。」

我國洗錢防制法第 10 條第 1 項規定：「金融機構及指定之非金融事業或人員對疑似犯第 14 條、第 15 條之罪之交易，應向法務部調查局申報；其交易未完成者，亦同。」同法第 9 條與第 12 條並規定金融機構對於達一定金額（目前為 50 萬元）以上之通貨交易、旅客或隨交通工具服務之人員出入國境攜帶一定金額以上之外幣現鈔、有價證券、黃金及洗錢防制物品均應向法務部調查局申報或通報，以貨物運送、快遞、郵寄或其他相類之方法運送前述物品出入境者，亦同。

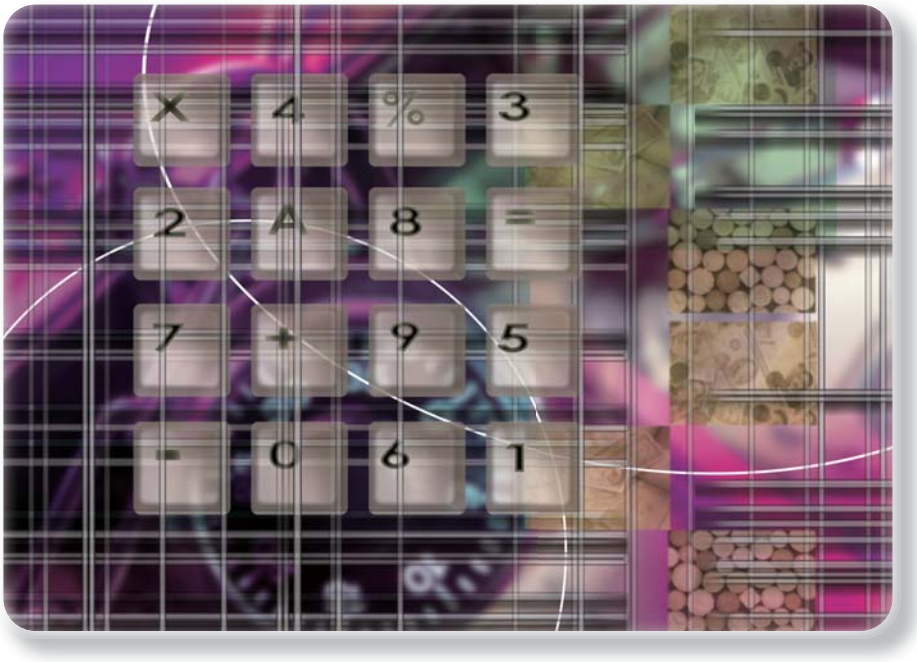
依《法務部調查局組織法》第 2 條及〈法務部調查局處務規程〉第 9 條，本局掌理洗錢防制事項，並由洗錢防制處實際執行金融情報中心業務。

圖 B：洗錢防制處作業流程圖



第二部分

工作概況



壹、受理可疑交易報告之申報

貳、受理大額通貨交易之申報

參、受理財政部關務署通報資料

肆、教育訓練與宣導

伍、公私協力與策略研究

陸、國際合作與交流

壹、受理可疑交易報告之申報

依 FATF 第 20 項建議：「若金融機構懷疑或合理懷疑交易資金是犯罪收益，或涉及資恐，應立即向金融情報中心申報該可疑交易。」並應以法律訂定相關規定。

《洗錢防制法》第 10 條第 1 項規定，金融機構及指定之非金融事業或人員對疑似犯第 14 條、第 15 條之罪之交易，應向法務部調查局申報；其交易未完成者，亦同。本局於受理後由洗錢防制處進行建檔、過濾及分析，研認疑似有犯罪嫌疑，或為穩定金融秩序、維護國家安全必要者，即彙編為實務性或策略性金融情報，並依其性質分送予本局辦案單位或其他權責機關參考。109 年度本局計受理 24,406 件可疑交易報告，較前一（108）年度受理之 26,481 件，減少 7.84%。依申報機構、處理情形、發生地區、申報月份、交易對象年齡及申報之交易金額進行統計及分析，109 年本國銀行申報件數約占 79.56%、辦理儲金匯兌之郵政機構約占 7.44% 及保險公司約占 5% 為前 3 大宗；109 年可疑交易發生地前 3 名為發生於臺北市者占 28.15%、新北市占 15.62% 及臺中市占 12.65%；109 年可疑交易對象之年齡層有 16.56% 分布於 21 歲至 30 歲間，53.53% 分布於 31 歲至 60 歲間，相較於 108 年有 12.58% 分布於 21 歲至 30 歲間，52.66% 分布於 31 歲至 60 歲間，可疑交易對象年齡有年輕化趨勢；交易金額則有 14.46% 為 50 萬元以下之交易，18.27% 為 3,000 萬元以上之交易，相較於 108 年有 18.29% 為 50 萬元以下之交易，17.53% 為 3,000 萬元以上之交易，可疑交易金額略為提高趨勢（以上詳細統計及分析情形詳表 01 至表 07 及圖 C 至圖 F）。另本局所受理的可疑交易報告，已提供法務部、內政部警政署等權責機關以專線方式線上投單查詢。

一、可疑交易報告申報情形

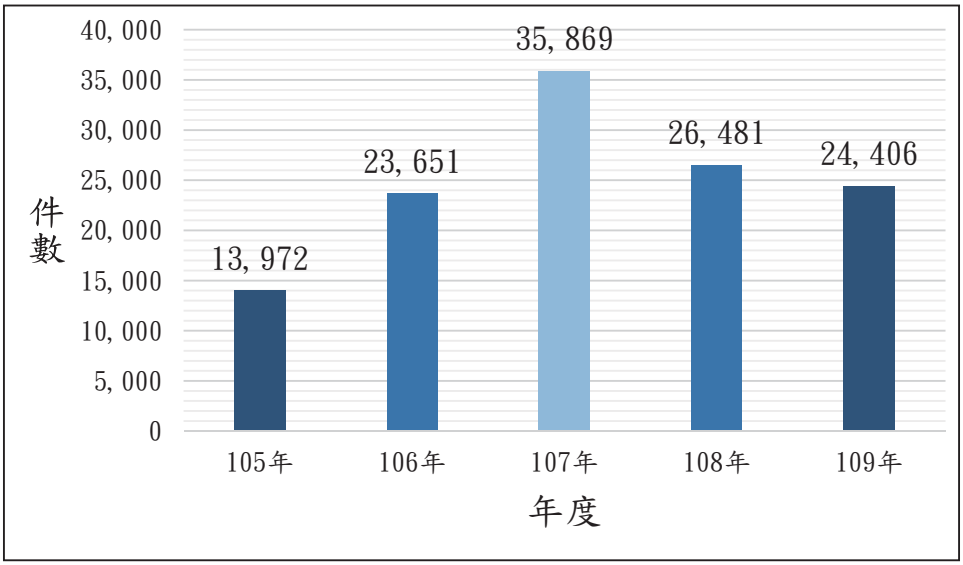
表 01：109 年受理可疑交易報告件數統計表

申　報　機　構	申報件數
本國銀行	19,417
外國銀行	20
信託投資公司	0
信用合作社	558
農、漁會信用部	679
辦理儲金匯兌之郵政機構	1,816
票券金融公司	2
信用卡公司	39
保險公司	1,221
證券商	271
證券投資信託事業	40
證券金融事業	8
證券投資顧問事業	1
證券集中保管事業	10
期貨商	85
指定非金融事業或人員	94
大陸銀行	19
電子支付及電子票證機構	106
外幣收兌處	0
創新實驗業	3
融資性租賃業	15
合計：24,406	

表 02：近 5 年可疑交易報告申報件數統計表

年　度	105 年	106 年	107 年	108 年	109 年
件數統計	13,972	23,651	35,869	26,481	24,406

圖 C：近 5 年可疑交易報告申報件數統計圖



二、本處處理情形

表 03：109 年可疑交易報告處理情形統計表

處　理　情　形	件數
分送本局辦案單位	1,398
分送警政、檢察署及其他權責機關	1,440
國際合作	47
併入資料庫	21,429
分析中	92
合計：24,406	

三、可疑交易發生地區分布

表 04：109 年可疑交易發生地區統計表

交易地區	件　數	交易地區	件　數
臺北市	8,585	嘉義市	438
新北市	4,765	嘉義縣	260
基隆市	351	臺南市	1,680
宜蘭縣	277	高雄市	2,951
桃園市	2,470	屏東縣	659
新竹市	673	花蓮縣	210
新竹縣	468	臺東縣	109
苗栗縣	399	澎湖縣	20
臺中市	3,858	金門縣	42
彰化縣	1,050	連江縣	3
南投縣	327	其他[1]	542
雲林縣	361		
			合計：30,498

註：一件可疑交易報告涵蓋發生地區可能包含一個以上。

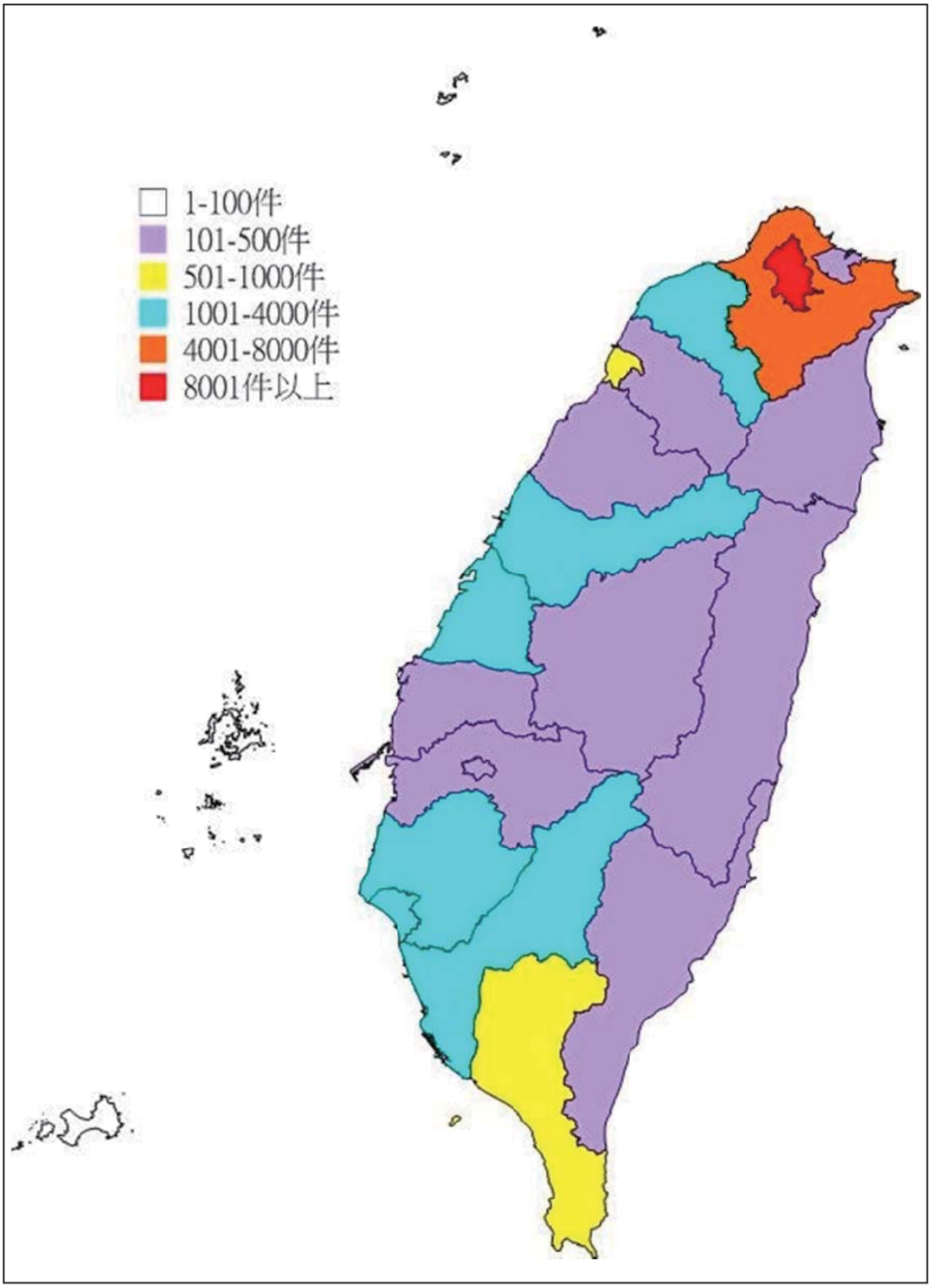
四、可疑交易申報月份分布

表 05：109 年各月份申報可疑交易報告統計表

月份	1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
件數	1,861	1,953	2,097	1,823	1,783	2,121	2,096	2,034	2,417	1,858	2,091	2,272

[1] 指境外。

圖 D：109 年可疑交易發生地區分布圖

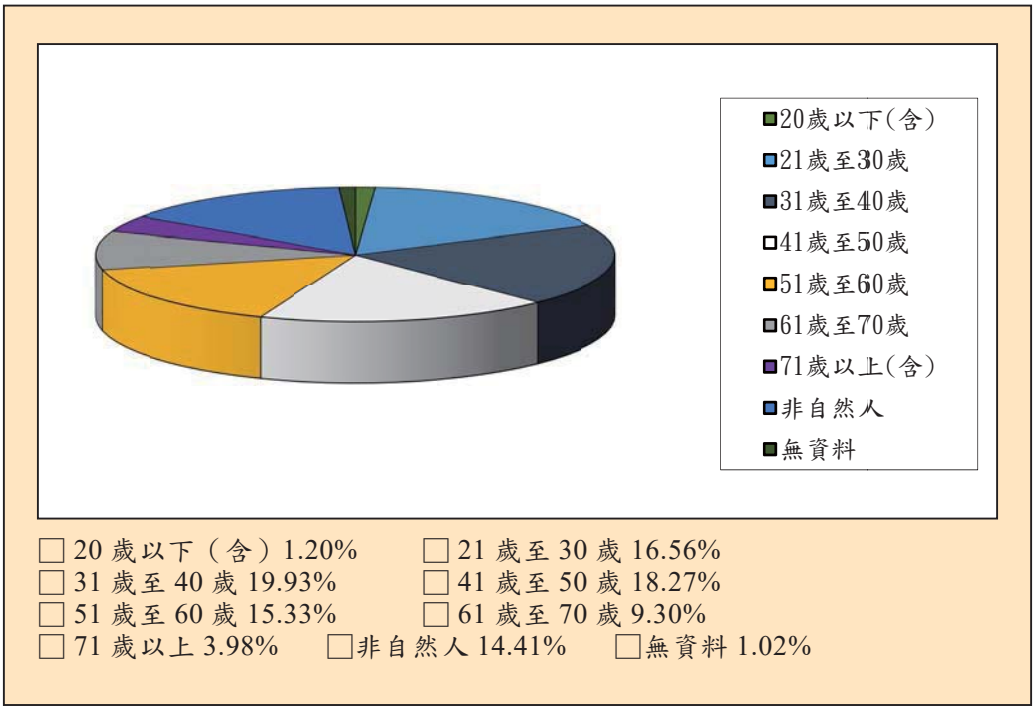


五、可疑交易對象年齡層分布

表 06：109 年可疑交易申報對象年齡層統計表

年齡分類	人數
20 歲以下（含）	295
21 歲至 30 歲	4,042
31 歲至 40 歲	4,864
41 歲至 50 歲	4,458
51 歲至 60 歲	3,743
61 歲至 70 歲	2,268
71 歲以上	972
非自然人	3,516
無資料	248
合計：24,406	

圖 E：109 年可疑交易申報對象年齡層分析圖

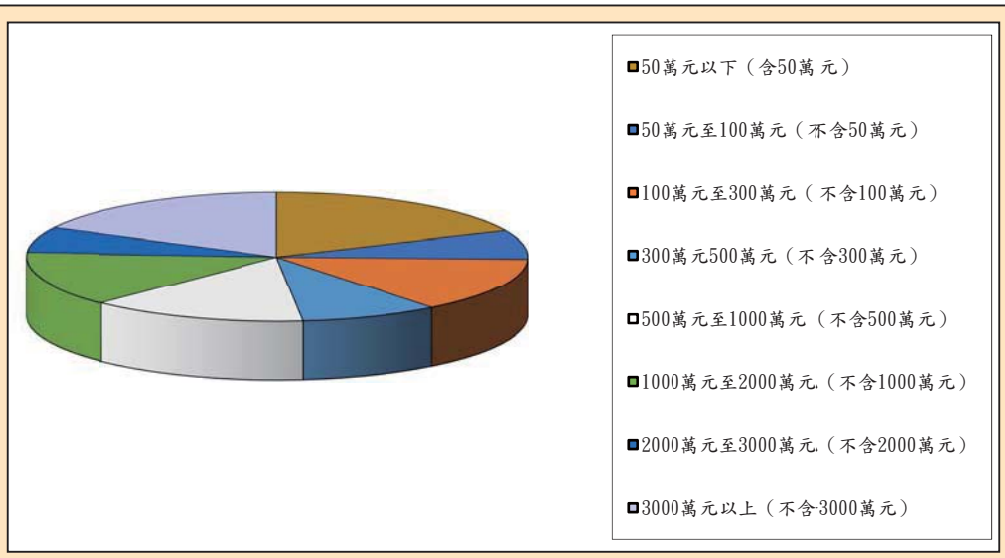


六、可疑交易金額分布

表 07：109 年可疑交易申報金額統計表

金　　額	件　　數
50 萬元以下（含 50 萬元）	3,528
50 萬元至 100 萬元（不含 50 萬元）	1,392
100 萬元至 300 萬元（不含 100 萬元）	3,450
300 萬元 500 萬元（不含 300 萬元）	2,363
500 萬元至 1000 萬元（不含 500 萬元）	3,887
1000 萬元至 2000 萬元（不含 1000 萬元）	3,715
2000 萬元至 3000 萬元（不含 2000 萬元）	1,613
3000 萬元以上（不含 3000 萬元）	4,458
	合計：24,406

圖 F：109 年可疑交易申報金額分析圖



- 50 萬元以下（含 50 萬元）14.46%
- 50 萬元至 100 萬元（不含 50 萬元）5.70%
- 100 萬元至 300 萬元（不含 100 萬元）14.14%
- 300 萬元至 500 萬元（不含 300 萬元）9.68%
- 500 萬元至 1,000 萬元（不含 500 萬元）15.93%
- 1,000 萬元至 2,000 萬元（不含 1,000 萬元）15.22%
- 2,000 萬元至 3,000 萬元（不含 2,000 萬元）6.61%
- 3,000 萬元以上（不含 3,000 萬元）18.27%

貳、受理大額通貨交易之申報

依據《洗錢防制法》第 9 條，本局受理國內金融機構申報大額通貨交易資料，依〈金融機構防制洗錢辦法〉第 2 條及〈農業金融機構防制洗錢辦法〉第 2 條之規定，所謂一定金額係指 50 萬元（含等值外幣）。本局於受理大額通貨交易申報資料後，由洗錢防制處建置資料庫並保管運用，並依〈法務部調查局辦理防制洗錢及打擊資恐業務作業要點〉規定，亦受理本局各處站、法院、檢察署及警察機關等查詢大額通貨交易。109 年度共受理申報 3,052,856 件，依申報機構、申報金額等進行統計及分析，其中，本國銀行申報件數占 78.74%，交易金額為 50 萬元至 100 萬元間之交易則占 73.13%；109 年度受理查詢大額通貨交易之件數為 38,704 件（詳細統計及分析情形詳表 8 至表 11 及圖 G 至 H）。

一、大額通貨交易申報情形

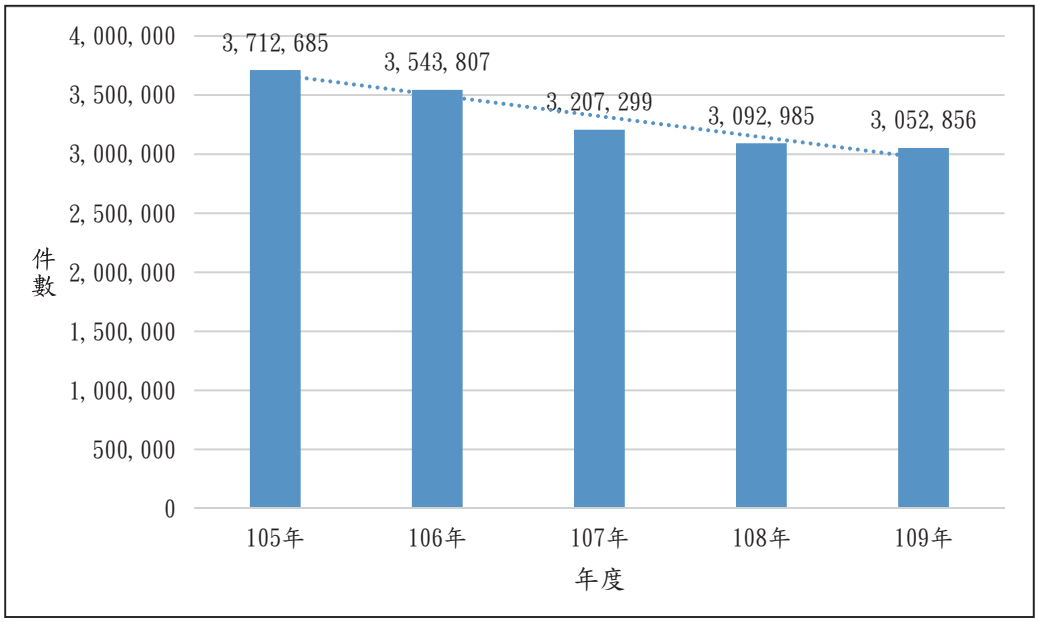
表 08：109 年申報大額通貨交易件數統計表

申　報　機　構	件　數
本國銀行	2,403,839
外國銀行	8,471
大陸銀行	0
信託投資公司	0
信用合作社	116,983
農、漁會信用部	252,256
辦理儲金匯兌之郵政機構	265,466
保險公司	5,560
書面申報（投信投顧公司）	8
書面申報（電子票證發行機構）	1
書面申報（金融機構 - 其他）	9
書面申報（銀樓）	272
其他金融機構	0
合計：3,052,856	

表 9：近 5 年大額通貨交易申報件數統計表

年　度	105 年	106 年	107 年	108 年	109 年
件數統計	3,712,685	3,543,807	3,207,299	3,092,985	3,052,856

圖 G：近 5 年大額通貨交易申報件數統計圖

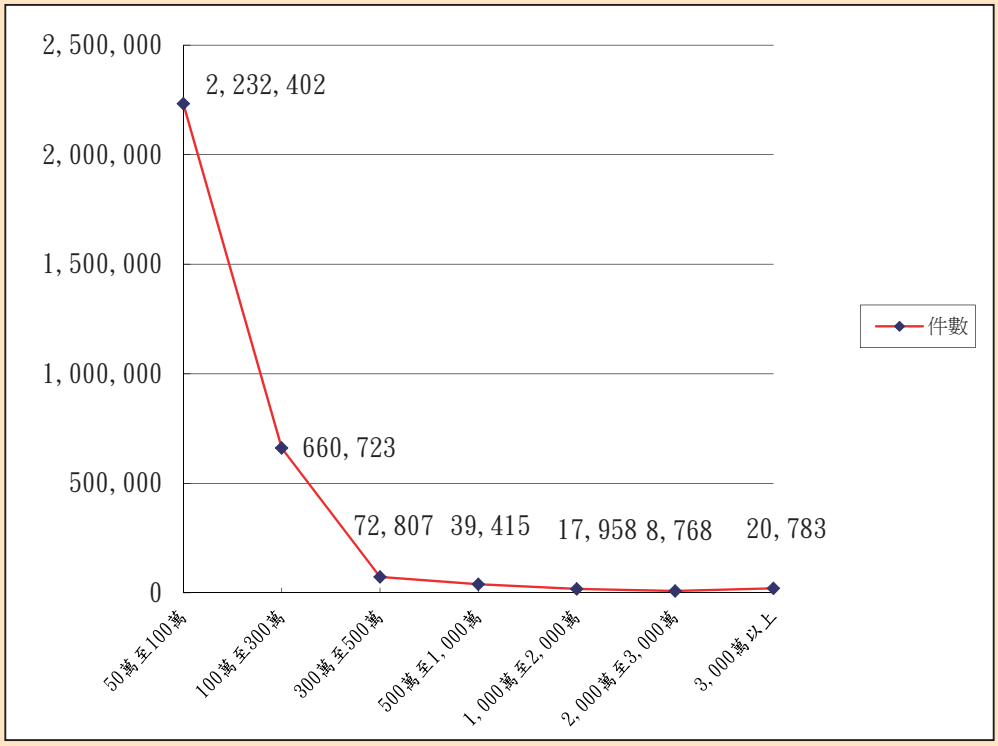


二、大額通貨交易申報金額分布

表 10：109 年申報大額通貨交易金額統計表

金　額	件　數
50 萬元至 100 萬元（含 50 萬元）	2,232,402
100 萬元至 300 萬元（不含 100 萬元）	660,723
300 萬元至 500 萬元（不含 300 萬元）	72,807
500 萬元至 1,000 萬元（不含 500 萬元）	39,415
1,000 萬元至 2,000 萬元（不含 1,000 萬元）	17,958
2,000 萬元至 3,000 萬元（不含 2,000 萬元）	8,768
3,000 萬元以上（不含 3,000 萬元）	20,783
合計：3,052,856	

圖 H：109 年申報大額通貨交易金額分析圖



- 50 萬元至 100 萬元（含 50 萬元）73.13%
- 100 萬元至 300 萬元（不含 100 萬元）21.64%
- 300 萬元至 500 萬元（不含 300 萬元）2.38%
- 500 萬元至 1,000 萬元（不含 500 萬元）1.29%
- 1,000 萬元至 2,000 萬元（不含 1,000 萬元）0.59%
- 2,000 萬元至 3,000 萬元（不含 2,000 萬元）0.29%
- 3,000 萬元以上（不含 3,000 萬元）0.68%

三、受理查詢情形

表 11：近 5 年受理大額通貨交易查詢筆數統計表

年　　度	105 年	106 年	107 年	108 年	109 年
法務部調查局	21,413	32,402	30,717	21,609	23,472
其他執法機關	13,012	17,929	29,153	19,236	13,047
檢察機關及法院	5,186	9,051	6,628	3,252	2,185
筆數統計	39,611	59,382	66,498	44,097	38,704

參、受理財政部關務署通報資料

依 FATF 第 32 項建議：「各國應對入境或出境之跨境運輸現金或無記名可轉讓金融商品建置申報系統或揭露系統。各國應確保該申報或揭露系統可用於所有實體跨境運輸不論是藉由旅客攜帶或透過郵件及貨運之方式，但針對不同的運輸模式可利用不同的系統。」

《洗錢防制法》第 12 條第 1 項規定：「旅客或隨交通工具服務之人員出入國境攜帶下列之物，應向海關申報；海關受理申報後，應向法務部調查局通報：一、總價值達一定金額以上之外幣、香港或澳門發行之貨幣及新臺幣現鈔。二、總面額達一定金額以上之有價證券。三、總價值達一定金額以上之黃金。四、其他總價值達一定金額以上，且有被利用進行洗錢之虞之物品。」及第 2 項規定：「以貨物運送、快遞、郵寄或其他相類之方法運送前項各款物品出入境者，亦同。」

另依〈洗錢防制物品出入境申報及通報辦法〉第 3 條第 1 項及第 2 項規定，旅客或隨交通工具服務之人員出入境，同一人於同日單一航（班）次攜帶下列物品，應依第 4 條規定向海關申報；海關受理申報後，應依第 5 條規定向法務部調查局通報：「一、總價值逾等值一萬美元之外幣、香港或澳門發行之貨幣現鈔。二、總價值逾新臺幣十萬元之新臺幣現鈔。三、總面額逾等值一萬美元之有價證券。四、總價值逾等值二萬美元之黃金。五、總價值逾等值新臺幣五十萬元，且有被利用進行洗錢之虞之物品」。因受 COVID-19 疫情影響，出入境旅客銳減， 109 年度海關受理旅客（含隨交通工具服務之人員）申報後再向本局通報共 7,364 筆，相較於 108 年通報 39,855 筆大幅下降許多，其中 109 年通報筆數中有 84.08% 為 100 萬元以下之外幣現鈔或有價證券（詳細統計及分析情形詳表 12 至表 15 及圖 I）。

此外，〈洗錢防制物品出入境申報及通報辦法〉第 3 條第 3 項亦規定，同一出進口人於同一航（班）次運輸工具以貨物運送、快遞、其他相類之方法，或同一寄收件人於同一郵寄日或到達日以郵寄運送前項各款所定物品出入境者，依前項規定辦理。109 年度海關受理之以貨物運送（含其他相類之方法）申報資料共 262,477 筆，金額近 2,558 億元，其中約 52.1%為出口申報（詳細統計及分析情形詳表 16 至表 19）。

一、旅客（含隨交通工具服務之人）通報數量

表 12：109 年旅客（含隨交通工具服務之人）通報筆數統計表

出、入境	筆　　數
入境	1,342
出境	6,022
合計	7,364

表 13：近 5 年旅客通報筆數統計表

年度	105 年	106 年	107 年	108 年	109 年
筆數	33,555	45,165	47,383	39,855	7,364

二、旅客（含隨交通工具服務之人）通報資料月份分布

表 14：109 年各月份旅客（含隨交通工具服務之人）通報統計表

月份	1 月	2 月	3 月	4 月	5 月	6 月
一般申報筆數	3,220	1,887	468	116	125	127
查獲違規[2]筆數	17	5	5	0	0	1
合計	3,237	1,892	473	116	125	128
月份	7 月	8 月	9 月	10 月	11 月	12 月
一般申報筆數	210	226	216	272	261	236
查獲違規筆數	0	1	2	2	0	4
合計	210	227	218	274	261	240

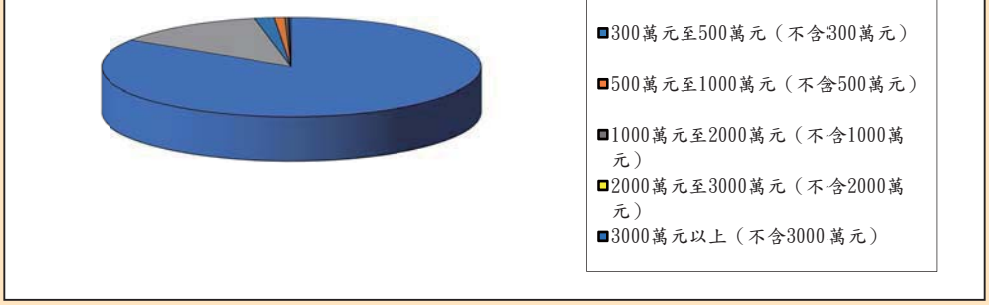
[2] 包括未申報或申報不實者。

三、旅客（含隨交通工具服務之人）通報資料金額分布

表 15：109 年旅客（含隨交通工具服務之人）通報金額統計表

金　　額	筆　數
100 萬元以下	6,192
100 萬元至 300 萬元（不含 100 萬元）	946
300 萬元至 500 萬元（不含 300 萬元）	122
500 萬元至 1000 萬元（不含 500 萬元）	66
1000 萬元至 2000 萬元（不含 1000 萬元）	19
2000 萬元至 3000 萬元（不含 2000 萬元）	6
3000 萬元以上（不含 3000 萬元）	13
合計：7,364	

圖 I：109 年通報金額分析圖



- ☐ 100 萬元以下 84.08%
- ☐ 100 萬元至 300 萬元（不含 100 萬元）12.85%
- ☐ 300 萬元至 500 萬元（不含 300 萬元）1.66%
- ☐ 500 萬元至 1,000 萬元（不含 500 萬元）0.90%
- ☐ 1,000 萬元至 2,000 萬元（不含 1,000 萬元）0.26%
- ☐ 2,000 萬元至 3,000 萬元（不含 2,000 萬元）0.08%
- ☐ 3,000 萬元以上（不含 3,000 萬元）0.18%

四、以貨物運送（含其他相類之方法）通報數量

表 16：109 年以貨物運送（含其他相類之方法）通報筆數統計表

進、出口	筆　　數
出口	51,538
進口	210,939
合計	262,477

表 17：近年以貨物運送（含其他相類之方法）通報筆數統計表

年度	107 年	108 年	109 年
筆數	290,084	320,481	262,477

五、以貨物運送（含其他相類之方法）通報金額

表 18：109 年以貨物運送（含其他相類之方法）通報金額統計表

進、出口	金額（單位：元）
出口	133,275,118,200
進口	122,518,919,465
合計	255,794,037,665

六、以貨物運送（含其他相類之方法）通報資料月份分布

表 19：109 年以貨物運送（含其他相類之方法）各月份通報統計表

月份	1 月	2 月	3 月	4 月	5 月	6 月
筆數	18,360	17,945	20,989	16,993	13,860	20,427
月份	7 月	8 月	9 月	10 月	11 月	12 月
筆數	24,675	21,324	28,417	26,000	26,773	26,714

肆、教育訓練與宣導

一、防制洗錢宣導

為提高一般民眾對於洗錢犯罪之警覺性，有效遏阻不法洗錢活動，本局外勤處站持續對外宣導洗錢防制工作，對象包含機關團體、學校、民間團體等單位，以輕鬆活潑之有獎徵答方式，介紹洗錢防制工作之範疇，讓民眾了解洗錢之危害性及洗錢防制工作之重要性。

本局臺中市調查處於「109 年就業嘉年華」辦理洗錢防制工作宣導

本局臺北市調查處於「109 年司法記者聯誼餐會暨形象宣導成果發表會」印製洗錢防制工作宣導品

二、協助辦理防制洗錢及打擊資恐教育訓練

根據 FATF 第 34 項建議「權責機關、監理機關及自律團體應建立準則及提供回饋，以協助金融機構及指定之非金融事業或人員遵循全國性防制洗錢 / 打擊資恐措施，特別是有關察覺及申報可疑交易。」為協助金融機構人員充分了解防制洗錢與打擊資恐所需資訊，提升金融機構人員申報可疑交易報告品質及加強金融機構從業人員了解可疑交易之表徵，本局洗錢防制處應金融機構之要求，派員前往各金融機構宣導防制洗錢工作，依金融機構申報資料及專業經驗與金融機構人員溝通討論，分享實際案例，介紹地下通匯、操縱股價、內線交易、企業掏空、詐欺及網路賭博等案件之犯罪手法，提升申報機構辨識異常交易能力及強化以風險為本之客戶盡職調查。

表 20：109 年協助申報機構等辦理防制洗錢及打擊資恐教育訓練統計表

申報機構名稱		小計	
		場次	人次
銀　行	本國銀行（含金控）	16	1,781
	外國銀行	1	23
農漁會信用部		4	297
證券投信投顧業		2	112
證券業		1	75
期貨業		3	205
保險業		10	602
信用卡業		2	47
電子支付業		1	8
虛擬資產服務提供商		1	30
指定之非金融事業或人員		1	52
合計		42	3,232

伍、公私協力與策略研究

一、與執法、監理及稅務機關業務聯繫會議

為強化國家金融情報中心支援執法、監理及稅務等權責機關實務需求、加強金融情資運用效能，同時也回應亞太防制洗錢組織（Asia/Pacific Group on Money Laundering，以下簡稱：APG）相互評鑑針對金融情報中心所提建議，本局洗錢防制處於 109 年積極與相關權責機關交流溝通，其中上半年與海洋委員會海巡署及財政部賦稅署（含財政資訊中心、臺北國稅局及北區國稅局等機關）進行業務聯繫會議，聚焦於各機關資訊分享機制，提升金融情資辨識不法活動的時效性及機關間協調合作；下半年更與財政部關務署、財政部北區國稅局、警政署刑事警察局、財政

本局於 109 年 2 月 18 日舉辦與財政部賦稅署等稅務機關之「強化金融情資分享及運用效能會議」

本局洗錢防制處同仁於 109 年 9 月 17 日與刑事警察局業務聯繫會議參加成員合影

部臺北國稅局、廉政署、財政部中區國稅局、金融監督管理委員會檢查局、財政部高雄國稅局及財政部南區國稅局進行業務聯繫會議，針對可疑交易報告類型、案例及風險趨勢等議題交換意見，面對面溝通金融情資運用之實務需求，強化各機關資訊提供及分享機制，並達成持續協力合作提供公私部門洗錢相關風險資訊之共識，冀能有效提升公、私部門辨識不法之成效及增進協調合作效能。

二、舉辦犯罪金流分析與異常交易態樣研討會

為深化我國公私部門協力夥伴關係，促進洗錢、資恐及資助武擴相關風險及案例分享，本局洗錢防制處與金融監督管理委員會銀行局於 109 年 12 月 10 日共同舉辦「犯罪金流分析與異常交易態樣研討會」，共計 140 名法令遵循及洗錢防制主管或專責人員代表 86 家金融機構參與研討。研討會首由本局呂局長文忠及銀行局黃副局長光熙致詞開幕，延請本局國家安全維護處陳調查專員希傑、廉政處陳調查官雅文、經濟犯罪防制處張科長傑程、毒品防制處李調查專員維鈞、洗錢防制處陳調查專員啟

109 年犯罪金流分析與異常交易態樣研討會現場畫面

明及警政署刑事警察局趙隊長尚臻，分就各單位執法工作重要案例、108年年報內容及未來執法重點提要說明。會後由本局洗錢防制處伍前處長榮春主持與談，與會人員踴躍發問並參與研討，對於犯罪暨洗錢手法都有更深入瞭解，希冀有助提升相關從業人員可疑交易態樣辨識能力並優化申報機制效能。

三、研編「網銀人頭帳戶」策略分析報告

為瞭解我國洗錢犯罪風險趨勢及態樣，適時協助監理機關及金融機構架構更佳的防制洗錢機制，本局洗錢防制處自 108 年 11 月起，陸續接獲來自不同金融機構申報具有相同或類似特徵之可疑交易報告後，察覺有針對風險提升的「網銀人頭帳戶」撰寫策略分析報告之必要，遂將相關態樣蒐整進行分析，亦抽查部分帳戶並發交外勤調查處站協助詢問開戶人。報告完成後，亦即時分送予相關機關和申報實體，以提供政策建議及趨勢分析，作為未來申報可疑交易報告、制定相關防制洗錢／打擊資恐政策或修正相關機制之參考。

四、發行洗錢防制處電子報

我國於 108 年完成 APG 第三輪相互評鑑並獲得一般追蹤之佳績，然評鑑團於建議中不斷強調金融情情報中心與執法機關、監理機關及私部門申報機構資訊共享及合作協調之重要性。本局洗錢防制處係國家金融情報中心，扮演傳遞資訊之樞紐角色，為持續強化金融情報中心之定位及功能，本處於 108 年 11 月創刊發行電子報後，109 年持續發行中英文版本電子報，宗旨在創建防制洗錢、打擊資恐及防制武擴相關知識及資訊合流的平臺，同時擴充 PPP（Public-Private Partnership）公、私部門跨域夥伴關係交流方式，彙整相關統計資料、犯罪趨勢、交易態樣及防制重點等專業意見，提供相關權責機關、夥伴機構及社會大眾參考，共同增進辨識風險能力，裨益採取與風險相稱之防制措施，適切分配有限資源，聚焦高風險活動，達於強化防制洗錢、打擊資恐及武擴機制之目標。

109 年犯罪金流分析與異常交易態樣研討會主持長官合影留念

◎亞太防制洗錢組織（Asia/ Pacific Group on Money Laundering，APG）

APG 於西元 1997 年設立，其目的在於協助其會員國接受並履行 FATF 所制訂有關防制洗錢、打擊資助恐怖活動及反資助武器擴散之國際標準。

我國曾於民國 90 年及 96 年兩度接受 APG 相互評鑑，評鑑報告經 APG 年會通過，對我國之防制洗錢機制均給予高度肯定。我國金融情報中心－本局洗錢防制處獲得最高評等，顯示功能運作良好。我國於 107 年接受 APG 第三輪相互評鑑期間，評鑑員對於本局洗錢防制處能具體發揮金融情報中心優勢效能，並在國際局勢的挑戰下，仍有效落實國際合作之表現，印象深刻。

目前APG計有41個會員國、觀察員8國及32個國際組織觀察員，並為FATF之準會員，我國係APG之創始會員國，名稱係「中華臺北」（Chinese Taipei），並得以APG會員之身分參與FATF之會務活動。

陸、國際合作與交流

一、國際情資交換

FATF 第 40 項建議「各國應確保權責機關能夠快速、有建設性且有效的提供有關洗錢、前置犯罪及資助恐怖分子最大範圍之國際合作，並應主動或經請求進行國際合作，且應有法律基礎提供此種合作。若有關機關需要雙邊或多邊協議或安排，如合作備忘錄，應適時與最大範圍的國外對等單位進行協商與簽署。」、「權責機關應有明確管道與機制，以有效傳送並執行資訊或其他類型協助之請求。有關機關應有明確與有效率的處理程序，優先且及時地執行請求，並保護所接收之資訊。」本局洗錢防制處運用艾格蒙聯盟管道，與全球 167 個[3]會員國交換洗錢及資恐、武擴情報，且相關情資並經分析後，分送予權責機關處置。洗錢防制處近 5 年與國外對等單位從事國際合作情資交換統計如表 21。

表 21：近 5 年從事國際合作之情資交換統計表

事項	年度	105 年	106 年	107 年	108 年	109 年
外國請求我國協查	案	50	55	47	71	58
	件	169	161	162	279	197
我國請求外國協查	案	34	26	23	38	32
	件	165	94	107	292	110
外國主動提供情資	案	25	53	99	81	66
	件	44	100	198	198	132
我國主動提供情資	案	26	45	20	17	12
	件	45	94	46	50	23
問卷及其他事項	案	0	0	0	0	0
	件	262	354	339	248	261
小計	案	135	179	189	207	168
	件	685	803	852	1,067	723

[3] 資料來源：艾格蒙聯盟官方網站 http://egmontgroup.org/，資料擷取日期：110 年 8 月 10 日。

二、與外國金融情報中心簽署瞭解備忘錄

洗錢犯罪常為跨越國境的犯罪，為有效打擊跨境洗錢犯罪、資助恐怖主義及資助大規模毀滅性武器擴散等，實有賴各國政府凝聚共識並攜手合作，秉持互信互惠原則交換金融情資，共同打擊洗錢犯罪及資恐活動。109 年間全球疫情肆虐，跨境往來成本提高且風險提升，在此期間，洗錢防制處仍於 109 年 6 月 1 日以異地換約的簽署方式，與科索沃共和國（Republic of Kosovo）金融情報中心完成「關於涉及洗錢、相關前置犯罪及資助恐怖主義金融情報交換合作瞭解備忘錄」簽署，透過合作瞭解備忘錄，對未來雙邊共同打擊跨國洗錢犯罪、重大犯罪及資恐活動等均有莫大助益。截至 109 年底，洗錢防制處已與 51 個國家簽署有關打擊洗錢及資恐合作備忘錄，未來還會持續爭取和更多國家簽署，以增進我國在國際上的能見度及打擊洗錢與資恐犯罪的國際合作。

三、參加「艾格蒙聯盟工作組與委員會會議」

我國為艾格蒙聯盟會員，洗錢防制處代表我國參加艾格蒙聯盟於 109 年 1 月 27 日至 1 月 31 日在模里西斯巴拉克拉瓦舉辦之「艾格蒙聯盟工作組與委員會會議」，並參與「會員、支援及遵循工作組」及「亞太區區域小組」會議。洗錢防制處自 87 年成為艾格蒙聯盟會員迄今，透過技術支援參與會務運作，亦曾擔任亞太區區域代表，參與決策核心業務，現與法國金融情報中心共同輔導越南金融情報中心入會申請案，積極創造與會員互動聯繫機會，深化我國參與國際組織面向。

艾格蒙工作組與委員會會議現場

◎艾格蒙聯盟 (Egmont Group)

西元 1995 年 6 月 9 日，各國金融情報中心在比利時布魯塞爾之艾格蒙宮（Egmont-Arenberg Palace）集會決議設立艾格蒙聯盟，為世界各國金融情報中心情資交換之重要平臺，藉以共同協商合作方式防制洗錢，特別是情報交換範圍、訓練與技術分享。

我國係於民國 87 年 6 月第六屆年會時加入，現行名稱為 AMLD（Anti-Money Laundering Division，即洗錢防制處）, Taiwan。目前該組織有 167 個會員國，會員間透過安全網路進行情資交換。本局洗錢防制處定期參加該組織所舉辦之年會、工作組會議，並進行情資交換且推動與各國金融情報中心簽署洗錢防制與打擊資助恐怖主義情資交換合作協定或備忘錄，以符合 FATF 建議與艾格蒙聯盟成立宗旨。

四、參加「亞太防制洗錢組織」會議

受到 COVID-19 疫情影響，原訂於 109 年 7 月舉行之 APG 年會被迫取消，其他相關工作組會議均改為線上方式舉行，包含治理委員會（Governance Committee，以下簡稱：GC）、相互評鑑委員會（Mutual Evaluation Committee，以下簡稱：MEC）、執行委員會（Operations Committee）及捐贈及技術提供小組（Donors and Providers Group）會議等，其中 MEC 會議通過會期外採認包括帛琉、薩摩亞、所羅門群島、孟加拉、斯里蘭卡、庫克群島、斐濟、萬那杜等多國追蹤報告（Follow-up Report），另 GC 會議討論並通過 109 年至 111 年 APG 優先事項（Priorities），包含強化技術協助與訓練活動、建構公私協力交流平臺、強化態樣分析工作及強化支援 APG 秘書處業務等 4 大主軸。此外，FATF 於 109 年 10 月間已正式採認四十項建議中第一、二項建議及其註釋中關於資助武擴之新增內容，要求各會員國辨識及評估資助武擴風險、採取風險抵減措施，並加強相關防制政策與合作機制。鑒於我國未來接受 APG 第四輪相互評鑑將採用前揭第一、二項修正建議內容，各權責機關、自律團體、金融機構及指定之非金融事業或人員應儘速制訂防制資助武擴之相關政策暨風險評估、抵減等因應措施。

第三部分

重要案例

壹、莊○文等涉嫌賭博及違反洗錢防制法等案

貳、黃○岡等涉嫌詐欺及違反洗錢防制法等案

參、童○維透過虛擬通貨交易平臺詐欺及違反洗錢防制法等案

肆、甲公司王○元等涉嫌賭博及違反洗錢防制法等案

伍、沈○存等涉嫌詐欺、違反銀行法及洗錢防制法等案

陸、黃○根涉嫌違反資恐防制法等案

壹、莊○文等涉嫌賭博及違反洗錢防制法等案

一、案情概述

（一）情資來源

本處於 109 年 8 月分析情資發現：新○旺公司及其子公司「群○公司」疑為博弈集團，該集團公司持有之金融帳戶經常以略低於 50 萬元現金存入，並透過境外公司、海外帳戶及地下通匯等方式移轉經營博弈平臺的不法所得，再用於投資不動產及併購其他企業，本處遂製作分析報告，分送予本局案件偵辦單位參考運用。

（二）涉案人

新○旺公司負責人莊○文、副總經理李○駿、群○公司負責人洪○琦及上○公司負責人溫○慧。

（三）涉案情形

莊○文等人共同基於意圖營利供給賭博場或聚眾賭博、掩飾及隱匿特定犯罪所得本質、來源及去向等犯意聯絡，於 103 年間共同發起、主持、操縱及指揮具有牟利性、持續性及結構性之博弈及洗錢犯罪組織，該集團以新○旺公司為首，其下設立群○公司等數十家子公司，共同組成新○旺博弈集團，該集團除經營「戰○博弈網站」外，另經營「GPK」博弈平臺，招攬遍及大陸與東南亞國家之站主，站主僅需招攬賭客，由新○旺集團子公司提供伺服器，並負責博弈網站、遊戲維護及設計，賭金出入金等服務（俗稱「包網」服務）。新○旺博弈集團按月向境外站主收取線路費，並依賭客賭金獲利抽成。集團子公司上○公司及群○公司負責「GPK」博弈平臺帳務管理、清洗境外不法所得並把資金移轉回臺灣，新○旺公司則統籌各公司資金調度及將不法所得轉為合法投資，該集團不法所得清洗手法如下：

以新○旺公司大股東及子公司負責人名義設立多家境外公司，

新○旺公司假借提供境外公司「資訊服務」，企圖以合法掩護非法的方式，將境外不法所得透過數家境外公司海外帳戶匯回臺灣，作為投資不動產及企業併購之用。

子公司或莊○文等人有資金需求時，均由群○公司負責人洪○琦及上○公司負責人溫○慧委託員工，以地下匯兌方式將境外不法所得兌換為新臺幣現金，新○旺公司會計人員嗣將現金存入子公司帳戶或莊○文等人私人帳戶，供子公司營運週轉或私人花費。

莊○文等人遭通緝逃亡期間，為隱匿賭博犯罪之不法所得，以遠低於市價價格移轉集團境外不法所得購入之國內土地、房產所有權予他人，更以每部 10 萬元之價格，移轉 10 部原價各約數百萬元至數千萬元之高級名車產權予他人。

新○旺博奕集團經營 GPK 線上博弈平臺獲取境外之不法所得，合計約 594 億 9,355 萬 1,920 元。本局於執行案件後查扣新○旺集團名下不動產及大量現金共計 7 億 5,007 萬 8,292 元，並於莊○文等人脫產後發動搜索追回脫產不法所得 10 億 460 萬元。

二、可疑洗錢表徵

新○旺公司會計人員頻繁以略低於大額通貨申報門檻之金額為現金存提，並設立境外公司帳戶，資金流動往來頻繁，符合洗錢表徵。

三、起訴情形

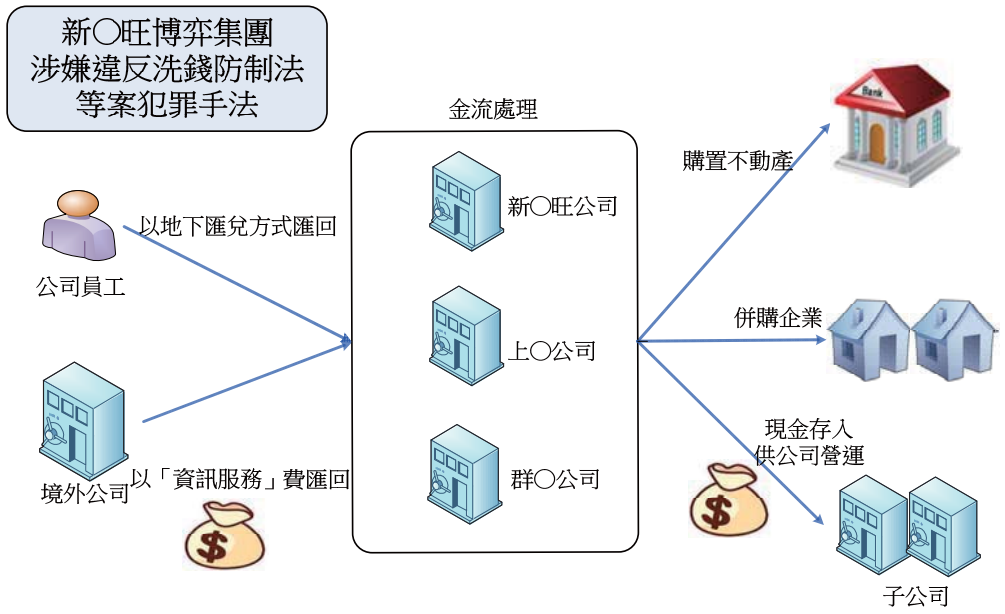
臺灣臺中地方檢察署於 110 年 3 月間，以違反刑法第 268 條、違反洗錢防制法第 2 條第 1 款、第 2 款之規定，觸犯同法第 3 條第 1 項第 2 款、第 14 條第 1 項、第 15 條第 1 項第 2 款及組織犯罪防制條例第 3 條第 1 項前段之罪嫌等起訴莊○文等人。

四、經驗參考

（一）案關數十家子公司名下所有金融帳戶，都由總公司多名會計統籌操作帳戶交易，且頻繁以略低於 50 萬元之現金存入及支出款項，

有企圖規避通報之虞，除了所宣稱的資金用途，支付公司營運所需薪資、水電及勞健保等之外，公司帳戶無任何銷項支出，與正常企業之帳戶交易模式有違。

（二）犯罪集團在薩摩亞及英屬維京群島開立有多個 OBU 帳戶，透過這些公司海外帳戶隱匿不法所得來源、本質及去向。金融機構若能適時發覺客戶與海外 OBU 帳戶有異常交易及可疑資金往來情形，向本局申報可疑交易，持續監控相關交易及往來對象，將有助偵辦單位掌握案關對象之金流，有效且及時啟動對犯罪的調查並追查不法資金。



貳、黃○岡等涉嫌詐欺及違反洗錢防制法等案

一、案情概述

（一）案件來源：

本處於 109 年 4 月間分析金融情資發現：國人蘇○民係列○公司登記負責人，帳戶經常有大額新臺幣及外幣現金存入後，旋以大額新臺幣現金提出或匯出，資金來源及去向不明，交易疑有異常。

（二）涉案人：

黃○岡、蘇○民及謝○哲。

（三）涉案情形

黃○岡佯裝為○集團千金及列○律師事務所主持律師，向 A 公司負責人 B 君誆稱可協助取得○集團銀行 VVIP 身分，獲取較優惠之存款利率及換匯匯率，另以共同投資房地產，並可協助處理 A 公司工程款訴訟糾紛，但需支付高額訴訟費用為幌，詐使 B 君陸續交付約 5,000 萬元及國外資產日幣 2 億 2,800 萬元，後續並存入黃○岡掌控之帳戶，黃○岡復使用蘇○民、謝○哲及列○公司名義開設 16 個金融帳戶及租用 4 個保管箱，以掩飾或隱匿犯罪所得來源及去向。

黃○岡向 B 君佯稱可取得○集團銀行較優惠匯率，協助 B 君將日幣攜回國內，於 108 年及 109 年間夥同蘇○民及謝○哲多次陪同 B 君赴日，自日本三○銀行提領日幣 2 億 2,800 萬元現金後，黃○岡等人再以「事務所受託待收款」、「法院裁定交保金」或「公司設立資金」等名義，向我國海關申報攜入現鈔，俟渠等將日幣攜回國內後，黃○岡再指示蘇○民將該等日幣以現金方式存入前揭黃○岡實際掌控之金融帳戶或置放於保險箱中。

黃○岡另向B君佯稱可代為處理A公司工程款訴訟糾紛，惟須預付3,000萬元予列○律師事務所，B君乃於109年4月8日使用A公司金融帳戶匯款3,000萬元至列○公司名下帳戶，同（8）日黃○岡隨即指示蘇○民前往銀行提領1,060萬元現金，並將該等款項交予黃○岡作其他不法用途。

本局於執行案件後，依法查扣黃○岡藏匿於住處及保管箱之新臺幣及日幣現鈔，另為免不法所得遭犯嫌提領，以緊急扣押方式發函協請銀行凍結前揭金融帳戶存款餘額，另扣押黃○岡使用犯罪所得購買之房地產3間，總計查扣不法所得達1億198萬5,366元。

二、可疑洗錢表徵

黃○岡以多人名義開戶後立即有達特定金額以上款項存、匯入又迅速移轉，經常接受國外匯款且立即提現達特定金額以上，又頻繁於數個不同客戶帳戶間移轉資金達特定金額以上，另有異常頻繁使用保管箱業務情形。

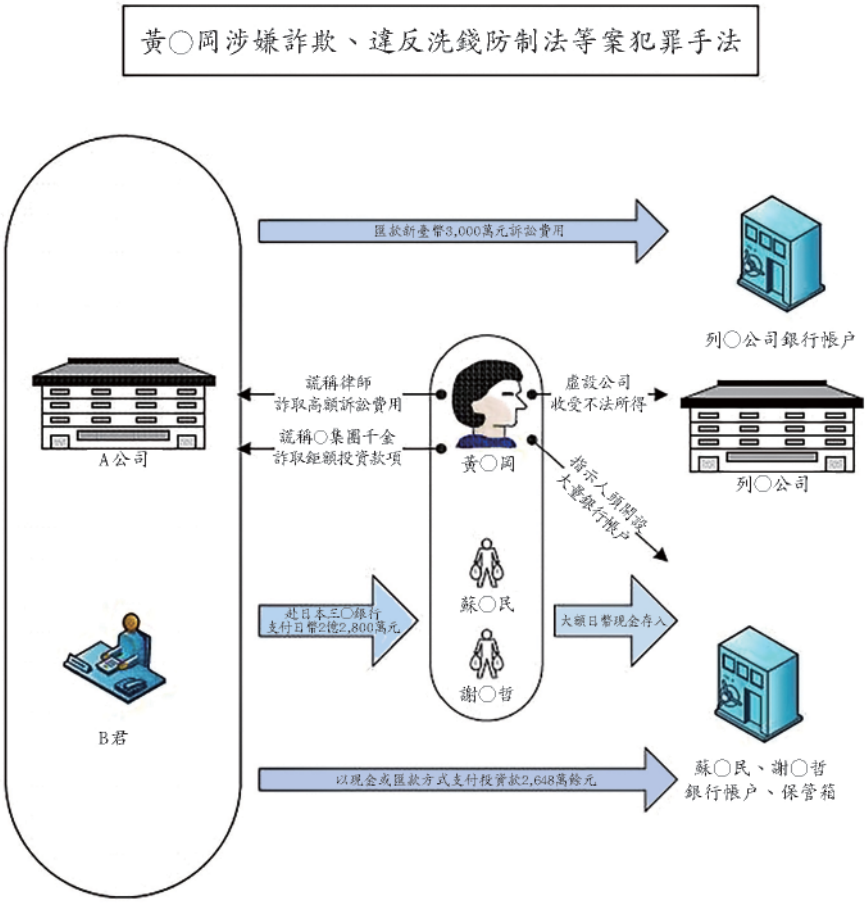
三、起訴情形

臺灣臺北地方檢察署於109年8月20日，以違反刑法詐欺、洗錢防制法、公司法及商業會計法等罪嫌，分別起訴黃○岡及蘇○民等人。

四、經驗參考

（一）黃○岡交付蘇○民不法所得後，經常由蘇○民以500萬元及1,000萬元等整數現金存入蘇○民等人金融帳戶，再由蘇○民以現金方式提領或匯款至其他黃○岡掌控之人頭帳戶，隱匿不法資金原始來源，符合洗錢表徵：客戶突有達特定金額以上存款；客戶經常於數個不同客戶帳戶間移轉資金達特定金額以上。

（二）黃○岡於 108 年間指示蘇○民及謝○哲等人開設 16 個金融帳戶，且該等帳戶於開戶後立隨即有大額新臺幣及日幣現金存入、其他金融帳戶匯入，或接受 B 君自國外匯入之大額美金及港幣等，惟該等款項均於入帳後即遭移轉，符合洗錢表徵：開戶後立即有達特定金額以上款項存、匯入又迅速移轉；客戶經常接受國外匯款且立即提現達特定金額以上。



參、童○維透過虛擬通貨交易平臺詐欺及違反洗錢防制法等案

一、案情概述

（一）情資來源

本局案件偵辦單位於 108 年 3 月間發掘童○維等人疑架設線上虛擬貨幣交易平臺吸引不特定民眾投資，並侵入他人虛擬貨幣帳戶移轉並詐取以太幣，初步查悉童○維等人以案關虛擬貨幣在冷、熱虛擬貨幣錢包進行多次交互移轉，甚至使用虛擬貨幣交易所「幣幣交易」功能增加查緝難度，並多次以現金存提製造金流斷點，顯有違法異常。

（二）涉案人

童○維及蔡○翰等人。

（三）涉案情形

童○維係虛擬貨幣網站 C 平臺負責人，蔡○翰係 C 平臺工程師。緣 107 年間，童○維及蔡○翰明知彼等實際上並未成功研發套利程式，亦無為他人代操管理虛擬貨幣以太幣之真意，竟意圖為自己不法之所有，向民眾宣稱已自行研發成功虛擬貨幣套利系統，可使用電腦自動偵測以太幣在各虛擬貨幣交易所之價差，藉買低賣高方式在各交易所間快速賺取價差獲利等話術，致徐○○等人陷於錯誤，移轉個人持有之以太幣共計 284.77 顆予童○維，童某再伺機侵占入己；童○維及蔡○翰復意圖為自己不法之所有，製作不具實際功能之套利程式吸引民眾投入以太幣參與套利投資，再利用 C 平臺之介面虛偽顯示投資人投入之以太幣及獎金顆數，製作不實之虛擬貨幣錢包增減等紀錄取信投資人，亦無故變更他人以太幣錢包

之電磁紀錄，使葉○○等二百餘位投資人陷於錯誤，遂將渠等所有之以太幣移轉至童○維及蔡○翰實際控制之虛擬貨幣錢包後，童、蔡 2 人再侵吞入己，總計詐取以太幣 1 萬 2,565.92 顆，不法所得約合 1 億 4,575 萬 8,037 元。本局案件偵辦單位執行搜索時，查扣童○維等人約 900 顆泰達幣（約合 2,507 萬 2,347 元）、房屋、車輛及案關金融帳戶餘額共計約 4,097 萬 7,445 元。

二、可疑洗錢表徵

經常利用自動化設備將小額款項存入及提出，每筆存、提金額相當且相距不久並達特定金額以上。

三、起訴情形

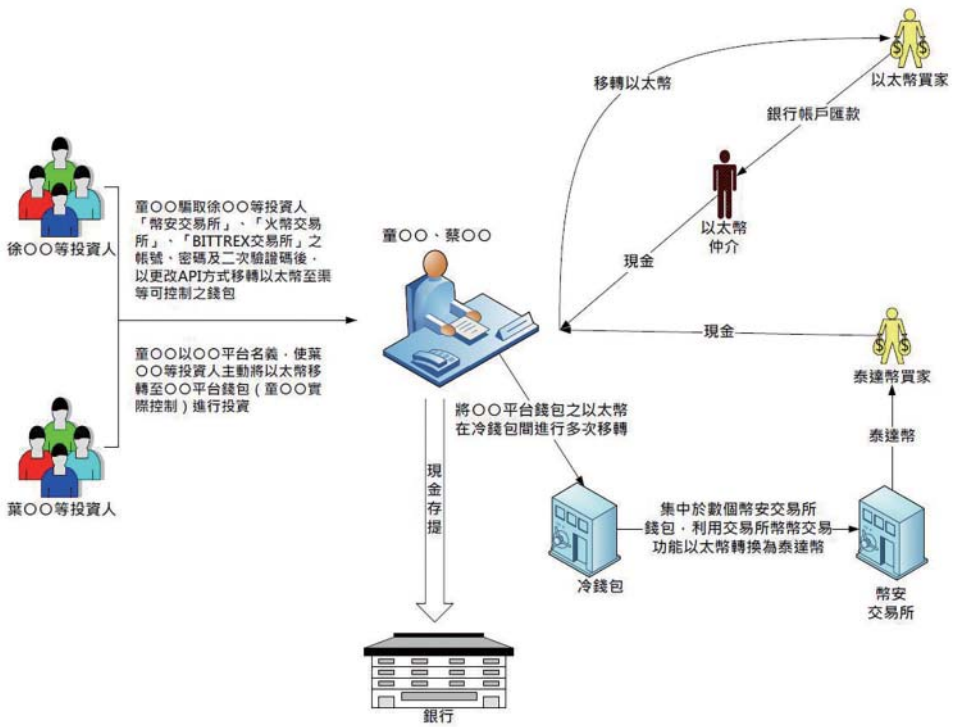
臺灣新北地方檢察署於 110 年 10 月間，以違反刑法詐欺、洗錢防制法、妨害電腦使用等罪嫌，起訴童○維及蔡○翰等人。

四、經驗參考

（一）童○維及蔡○翰等人宣稱成功研發虛擬貨幣套利平臺，能自動偵測虛擬貨幣在不同交易所間的價格差異，提供投資民眾輕鬆賺取價差。近年來，套利平臺成為與虛擬資產相關常見的犯罪模式。犯罪者以自動套利和保證高額獲利等說詞，吸引民眾投資，卻在不久之後，關閉網站、負責人或管理人失聯，致使投資人血本無歸。

（二）本案犯罪集團大量使用金融機構存提現金，並利用多個虛擬資產服務業者，與大量虛擬貨幣買家交易，透過賣出虛擬貨幣取得現金，資金再回到犯罪集團控制的金融帳戶中。犯罪集團將虛擬貨幣透過不同交易所及冷、熱虛擬貨幣錢包進行多次交互移轉，亦使用虛擬貨幣交易所「幣幣交易」等功能，增加查緝難度，並多

次以現金存提製造金流斷點；金融機構及虛擬資產服務業者針對交易異常頻繁、移轉迅速，或不斷購買不同種類虛擬資產，且無合理說法之客戶，應加強警示以察覺不法活動，並在適當時機申報可疑交易報告。



肆、甲公司王○元等涉嫌賭博及違反洗錢防制法等案

一、案情概述

（一）情資來源

本處於 108 年 12 月間接獲金融情資並分析後發現：王○元為甲網路科技有限公司負責人，帳戶經常有大額現金提領交易，或將資金轉入名下同行庫另一個帳戶後，再行提現，且在一定期間內密集自特定帳戶轉入款項，資金來源不明，交易疑有異常，本處遂製作分析報告，分送予權責單位參考運用。

（二）涉案人

王○元及朱○儀等人。

（三）涉案情形

王○元及朱○儀等人自 106 年 6 月間起，以甲公司名義經營線上賭博網站，招攬中國大陸賭客使用網路加入會員及匯款後，登入益○娛樂等博奕網站進行賭博。王○元為掩飾或隱匿前述經營賭博網站之不法賭金，以甲公司名義收購中國大陸人頭帳戶，並將之分為多層資金帳戶，作為收受客戶網站儲值金額（俗稱入金）及支付客戶獲利後提現金額（俗稱出金）使用帳戶，並指示財務人員透過網路銀行使用銀行 U 盾執行轉帳，以入金為例，第一層資金帳戶係直接收取賭客「入金」，該層資金帳戶餘額達 2 萬元時，隨即轉帳存入「集水層」資金帳戶，「集水層」資金帳戶餘額超過 1 萬元時，再以快進快出方式依序轉帳存入「入 - 中轉第一層」、「入 - 中轉第二層」及「入 - 中轉第三層」資金帳戶，「入 - 中轉第三層」資金帳戶額度達 3 萬元時，即分別轉帳存入共計 8 個最終帳戶（稱為大倉或總大倉）；「出金」時，則以反向層層轉出至客戶綁定之金融帳戶，以避免銀行警覺或執法人員查緝、凍結帳戶。

王○元另指示朱○儀成立「金流部門」管理第四方支付業務，

負責媒合賭博網站與第三方支付公司，賭博網站接收賭客訂單後，即透過金流部門系統媒合第三方支付公司，金流部門依賭博網站需求支付管道（如支付寶），以人工選擇有提供支付寶服務且成功率較高之第三方支付公司平臺接收賭客「充值」（即儲值）；第三方支付公司收迄「充值」金額後，回報充值成功訊息至金流部門系統，並自動回報賭博網站，再更新賭客儲值金額；王○元藉此從中賺取媒合之手續費價差，並指示第三方支付公司將手續費價差轉帳至王○元指定之中國大陸人頭帳戶後，再透過地下匯兌業者將不法所得匯回臺灣帳戶。

王○元將賭金及透過第四方支付賺取手續費差額之犯罪所得，以上述使用人頭帳戶並多層化轉帳方式加以掩飾、隱匿來源及去向，自 106 年 6 月起迄 109 年 1 月止，甲公司總營業額合計約 53 億 5,665 萬 7,060 元。

二、可疑洗錢表徵

同一帳戶在一定期間內之現金存、提款交易，分別累計達特定金額以上；客戶突有達特定金額以上存款者；存款帳戶密集存入多筆款項達特定金額以上或筆數達一定數量以上，且又迅速移轉；客戶經常於數個不同客戶帳戶間移轉資金達特定金額以上。

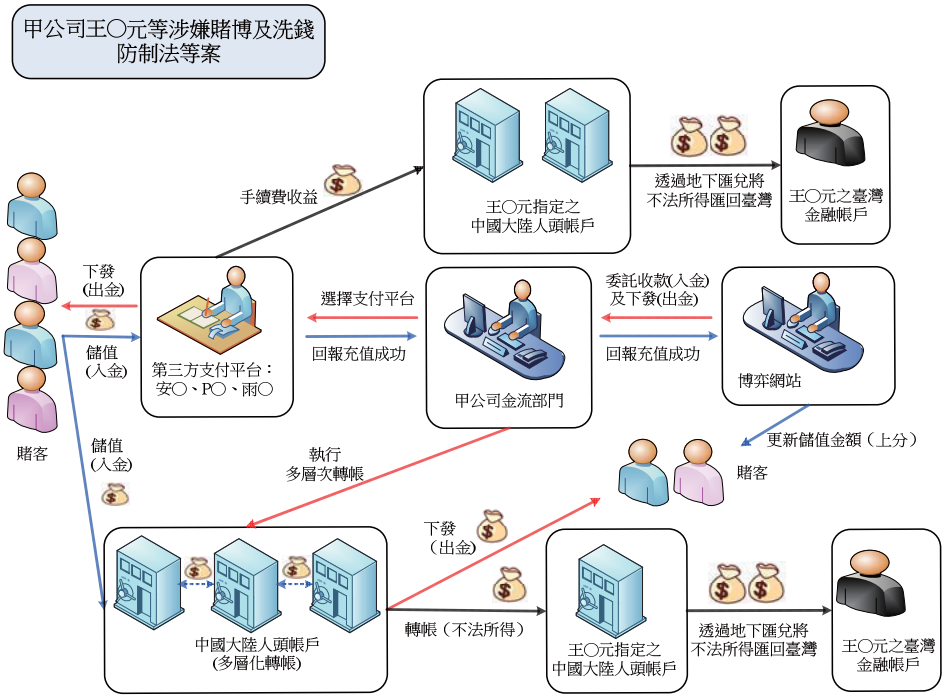
三、起訴情形

臺灣橋頭地方檢察署於 109 年 7 月間以違反刑法第 268 條及洗錢防制法第 14 條第 1 項等罪嫌起訴王○元等人。

四、經驗參考

（一）本案於分析王○元及其配偶金融帳戶發現，該等帳戶與特定數個帳戶間有密集存入、轉出金額及筆數達一定數量以上，符合洗錢表徵，金融機構發現異常，並持續申報相關往來對象及交易資料，有助於偵辦單位掌握案關對象金流，對後續追查金流或查扣犯罪所得等偵辦作為有相當助益。

（二）「第三方支付」方式洗錢已成為新趨勢，賭博網站可以透過超商、信用卡及虛擬帳戶收受、支付賭資，追查匿名身分、假帳號及追蹤第三方支付之金流不易。案關人頭公司金融帳戶，經常有小額整數款項存入，再以自動化設備提領現金，帳戶內僅留存象徵性餘額，符合「每筆存、提金額相當相距時間不久」表徵，且與正常企業之金融帳戶交易模式不符。



伍、沈○存等涉嫌詐欺、違反銀行法及洗錢防制法等案

一、案情概述

（一）情資來源

本局接獲民眾檢舉，沈○存夥同中國籍人士李○封等人，以投資石油期貨名義，向國人陳○○等人詐取財物，並透過銀樓業者以地下通匯方式將不法所得匯至大陸，藉此掩飾或隱匿詐欺犯罪所得。

（二）涉案人

沈○存、姜○偉、葉○雲、汪○、方○姍、谷○熙、連○麟、林○廷、鄭○木、陳○材、吳○賢、王○福及中國籍人士李○封等人。

（三）涉案情形

沈○存於 107 年間赴陸經商，在網路上結識中國籍廈門地區男子李○封。於 108 年 8 月起，沈員陸續提供設於臺灣行庫之方○姍等人頭帳戶予李○封作為隱匿及移轉詐欺不法所得使用，沈○存擔任在臺指揮提領帳戶犯罪所得之角色，並組成具有持續性及牟利性之結構性組織，在網路上詐騙國內不特定民眾陳○○等人，以投資香港石油期貨名義，將投資款項匯至指定之方○姍、谷○熙、連○麟及林○廷等臺灣人頭帳戶內，再由沈○存及李○封負責操縱及指揮上開犯罪組織，通知臺灣人頭帳戶方○姍等人提領現金，扣除領現的 1 至 3% 報酬後，剩餘資金交付給沈○存或其同夥姜○偉。

姜○偉復以自身運作多年之兩岸地下匯兌管道，透過位於中國出款人民幣之地下通匯業者劉○和及黎○陸，及臺灣銀樓業者許○熙（金○鑽銀樓）、莊○娜（金○珠寶銀樓）及聯○旅行社等地下通匯業者，參考匯款當日臺灣銀行人民幣與新臺幣匯率，加計自身利潤，將相關新臺幣犯罪不法所得，兌換算成等值人民幣後，由

該臺灣之地下匯兌銀樓業者，透過中國地區合作之地下匯兌業者，將人民幣款項匯款至李○封之指定中國地區金融帳戶內，總計沈○存等人以上開手法，詐欺取財金額約 1,511 萬 1,636 元，不法匯兌金額達 6,263 萬 2,189 元。

二、可疑洗錢表徵

金融帳戶密集存入多筆款項達特定金額以上，並與帳戶所有人之身分、收入顯不相當又迅速移轉；透過地下通匯銀樓業者私下換匯，且其用途及資金來源不清。

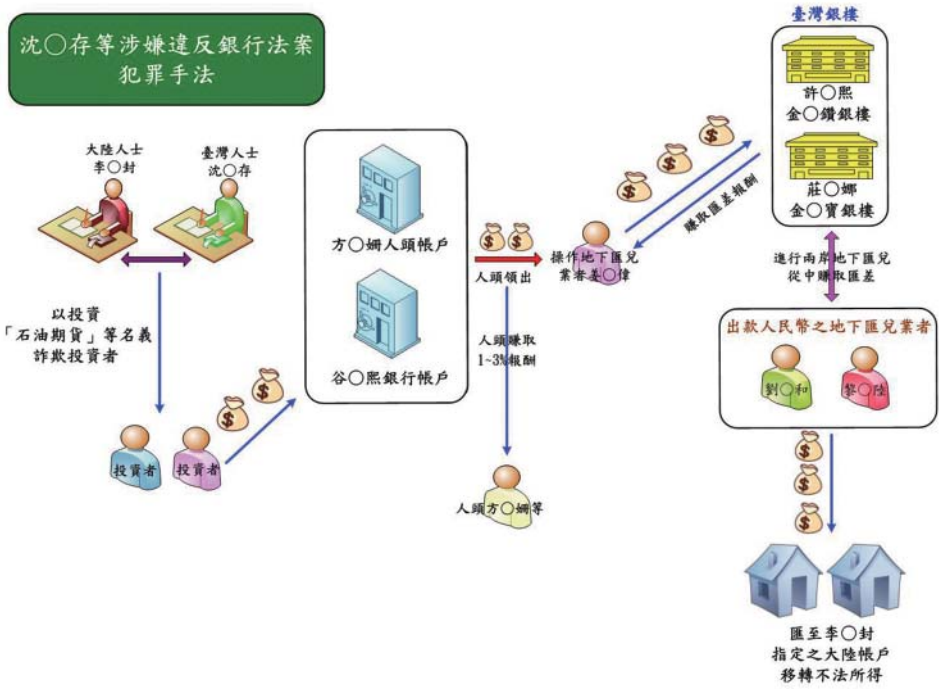
三、起訴情形

臺灣橋頭地方檢察署於 109 年 8 月間，以違反銀行法第 29 條第 1 項、洗錢防制法第 2 條及第 14 條、組織犯罪條例第 3 條第 1 項及刑法第 339 條之 4 第 1 項第 2 款 3 人以上共犯詐欺取財等罪嫌，起訴沈○存等人。

四、經驗參考

（一）民眾收到社群軟體或其他來源不明網路投資資訊，應特別注意是否涉及不法。本案經本局追查後，掌握案關對象之金流，清查出數十個供特定人指揮調度使用之人頭帳戶，查知係規模龐大之兩岸組織犯罪集團。該集團為將詐欺不法所得轉匯至大陸，透過臺灣銀樓業者（屬於指定之非金融事業或人員）及旅行社等，與中國業者合作，以地下通匯管道將臺新幣款項匯至大陸人民幣指定帳戶。

（二）偵查過程中發現，犯罪集團之詐欺手法日新月異，本案利用境外投資吸引不特定民眾上勾，提供特定帳號、密碼供其查詢投資情況，連結國際投資指數，讓人誤以為有真正投資及獲利，再利用各種話術要求被害人增加投資金額及標的，使民眾在不知不覺中受騙，並使遭詐騙金額逐漸增加，待時機成熟即關掉帳戶，民眾始驚覺受騙，待獲民眾檢舉報案或金融機構察覺，詐騙集團已將詐欺不法所得，透過地下匯兌管道匯至境外。


沈○存等涉嫌違反銀行法案
犯罪手法
大陸人士
李○封
臺灣人士
沈○存
以投資
「石油期貨」等名義
詐欺投資者
投資者
投資者
方○姍人頭帳戶
谷○熙銀行帳戶
人頭領出
人頭賺取
1~3%報酬
人頭方○姍等
操作地下匯兌
業者姜○煒
賺取匯差報酬
臺灣銀樓
許○熙
金○鑽銀樓
莊○娜
金○寶銀樓
進行兩岸地下匯兌
從中賺取匯差
出款人民幣之地下匯兌業者
劉○和
黎○陸
匯至李○封
指定之大陸帳戶
移轉不法所得

陸、黃○根涉嫌違反資恐防制法等案

一、案情概述

（一）情資來源

107 年間有國際情資顯示，巴拿馬籍上○堡油輪於 107 年 4 月 27 日離開高雄港後，分別於 107 年 5 月 18 日駁油予受制裁之北韓籍 A 油輪，及 107 年 6 月 2 日駁油予不明國籍 B 油輪。

（二）涉案人

黃○根、溫○榮、吳○彬及劉○法。

（三）涉案情形

黃○根、溫○榮、吳○彬及劉○法明知北韓因違反聯合國安理會 1718 號關於不擴散核武器之決議，遭聯合國安理會進行一連串制裁，渠等為提高海上駁油利潤，竟基於牟取暴利之意圖，協議允許「上○堡輪」與北韓船舶往來貿易，不顧違反聯合國制裁決議及我國資恐防制法，由溫○榮基於不實登載出口報單之犯意，向 S 公司購買油品後，於 107 年 5 月 6 日以油輪「金○泰」報運出口 1,350 公噸石油，並將出口報單之目的地國家登記為香港，將應於香港卸貨之油品在公海上轉運至黃○根為實際船東之「上○堡輪」，溫○榮旋於同年 5 月 8 日指示其聘僱之「上○堡輪」船東代表吳○彬全權處理「上○堡輪」駁油予受制裁之北韓籍 C 油輪事宜，吳○彬嗣指派「上○堡輪」中國籍管事「蘇仔」駁油 1,317.5 公噸予受制裁之北韓籍 C 油輪，駁油後再由溫○榮與黃○根進行駁油利潤分潤，不法獲利約達 2,600 萬元。

溫○榮等人依前揭相同犯罪手法，由溫○榮向 S 公司購買油品後，於 107 年 5 月 9 日以 D 油輪報運石油 6,400 公噸出口，出口報單之目的地國家登記為香港，惟同年 5 月 12 日 D 油輪即將其中 4,100 公噸油品輸送至「上○堡輪」；嗣劉○法仲介北韓籍 A 油輪予溫○榮，溫○榮旋於同年 5 月 17 日指示吳○彬處理「上○堡輪」駁油北韓籍 A 油輪事宜，吳○彬乃指派「蘇仔」駁油 1,479 公噸予

北韓籍 A 油輪，駁油後再由溫○榮與黃○根進行駁油利潤分潤，不法獲利約達 3,034 萬元。

二、可疑洗錢表徵

（一）電視、報章雜誌或網際網路等媒體即時報導之特殊重大案件，該涉案人在銀行從事之存款、提款或匯款等交易，且交易顯屬異常者。

（二）貨物運至或來自洗錢或資恐高風險國家或地區。

（三）客戶涉及疑似洗錢或資恐高風險之活動，包括輸出入受禁運或限制輸出入貨品者。

三、起訴情形

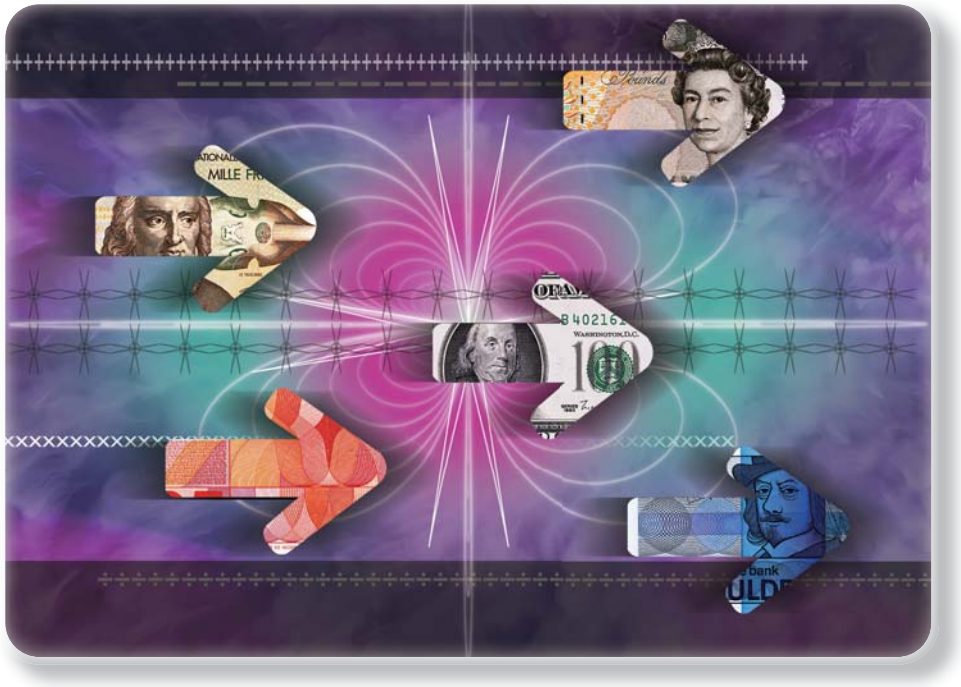
臺灣高雄地方檢察署於 109 年 10 月間，以犯刑法第 216 條、第 215 條行使業務登載不實文書及違反資恐防制法第 9 條第 1 項第 1 款直接為制裁名單提供財務之罪嫌，起訴黃○根等人。

四、經驗參考

黃○根名下香港○誠公司、○展公司及西○門得公司等 3 間境外公司，在多家金融機構開立不同 OBU 帳戶，金融機構於申報時，皆完整提供境外公司註冊證書、股東及董事名冊等，有助於釐清黃○根名下境外公司之設立情形與資金往來狀況。

第四部分

策略分析報告



網銀人頭帳戶策略分析報告

網銀人頭帳戶[1]策略分析報告[2]

壹、前言

一、研究動機與目的

緣法務部調查局洗錢防制處（下稱：本處）於108年11月起，陸續接獲來自不同金融機構申報具有相同或類似特徵之可疑交易報告（Suspicious Transaction Reports），其特徵略以：開戶人於開戶時觀看特定手機內容後，不約而同設定相同或類似之網路使用者代號，及設定數組重複之網轉約定帳號，於設定成功後，交易明細均出現自動櫃員機（Automatic Teller Machine, ATM）或網轉之小額測試交易，有疑似洗錢表徵。經本處初步分析相關帳戶之開戶人資金來源、流向及前科等背景資料等，發現已有部分帳戶與同時期執法機關偵辦網路賭博、詐騙及地下通匯等犯罪具高度關聯性，另本處抽查部分帳戶並發交外勤調查處站協助詢問開戶人，亦有部分開戶人坦承於網銀功能開通後，將帳戶出售予特定收購集團情事，大致上可認定係供他人使用之網銀人頭帳戶。而本處於清查資金流向的過程中，發現末端帳戶仍維持傳統使用自動櫃員機密集小額領現之方式製造資金斷點，而前端及中繼（過水）帳戶之金流，則有大量使用網銀交易（E-Banking，主要為手機或浮動IP）並與第三方支付（Third-Party Payment）業者對接的特殊現象及趨勢，顯示犯罪集團似已適應各銀行施行多年之自動櫃員機每日／每筆提領限額相關規定，金融機構是否有重新檢視或微調之必要，因涉及一般民眾使用提款機之方便性，將留待各銀行依據風險程度自行考量。至於網銀帳戶因具有非面對面交易（Non Face-to-Face Transaction）之特性，僅需要輸入使用者名稱及密碼即可操作，相較於傳統人頭帳戶，其取得成本更低、交

[1] 係指具有網路銀行功能之人頭帳戶，非指純網銀帳戶。

[2] 本報告作者為法務部調查局調查專員陳啟明。

易速度更快、操作無遠弗屆，因此危害性更大，由於網銀帳戶具有上開威脅（Threats）與弱點（Vulnerabilities），加上與具有類似新興風險之第三方支付對接，形成洗錢／資恐風險之「乘數效果」，但現行防制洗錢／打擊資恐機制對此等新興支付工具造成之洗錢／資恐風險，透由本次實務性分析顯示，似無法有效減緩或遏止，因此有必要重新檢視及調整相關防制洗錢／打擊資恐制度之規範強度。

鑒於以往反洗錢執行層面，多係藉由洗錢防制來反制或發現已完成或進行中之重大犯罪，並未臻於預防犯罪層次[3]。本處為發揮國家金融情報中心（Financial Intelligence Unit）之功能，並適時協助監理機關及金融機構機先防制洗錢犯罪，在發現前開疑似洗錢行為之趨勢後，於 108 年 12 月 11 日將上開洗錢趨勢函報金融監督管理委員會（下稱：金管會）銀行局參處[4]，該局隨即函轉銀行及信用合作社等同業公會[5]通報各會員[6]「注意上開趨勢，如發現疑似洗錢或資恐情形時，立即向本處申報可疑交易報告」等語，除使金融機構能及時採取相應之風險管控措施外，亦能適時申報相關可疑交易。截至本（109）年 4 月 30 日止（計半年），本處陸續接獲 15 家金融機構申報具相同或類似特徵之可疑交易報告[7]，計 238 件，開戶人計 1,435 人（自然人 1,429 人、法人 6 人），人頭帳戶總計 1,500 戶[8]。因以往並無專門執法或學術單位針對網銀人頭帳戶作大規模之系統性與實證性研究（Empirical Study），本處除陸續將相關犯罪

[3] 林志潔，「防制洗錢之新思維—論金融洗錢防制、金融監理與偵查權限」，檢察新論，第 3 期，2008 年 1 月，頁 271。

[4] 法務部調查局 108 年 12 月 11 日調錢貳字第 10835565590 號函。

[5] 金融監督管理委員會 108 年 12 月 31 日金管銀法字第 1080225400 號函。

[6] 中華民國銀行商業同業公會全國聯合會 109 年 1 月 13 日全一電字第 1080010756 號函。

[7] 截至本研究報告初稿完成日期 109 年 8 月 31 日止，本處累計接獲 408 件可疑交易報告、開戶人累計 1,683 人、疑似人頭帳戶計 1,790 戶。

[8] 本研究將金融機構申報之可疑帳戶歸類為人頭帳戶之方法如下：1 在 108 年 11 月至 109 年 4 月半年間開戶或設定網轉功能；2. 設定相同使用者名稱及密碼；3. 設定相同群組之網轉約定帳號；4. 設定完成後不久即出現 ATM 或網轉之小額測試進出金額；5. 同時期遭檢方起訴或司法警察機關調查之帳戶，並以該等帳戶作為「感染源」帳戶；6. 以「感染法」將與「感染源」具相同 2. 及 3. 特徵之帳號篩選出「被感染」帳戶，再依相同方法不斷「傳染」其他帳號，最後發現尚未遭檢方起訴或司法警察機關調查之帳戶，均悉數遭受「感染」，亦即與起訴或調查中之人頭帳戶具有密切之關聯性。上開歸類標準雖不若以起訴或判決結果作為歸類基礎準確，但對於整體趨勢觀察仍有相當之參考價值。

情資分送司法警察機關依法偵辦外[9]，亦嘗試以國家金融情報中心之高度及角度，針對前述 238 件可疑交易報告，及其所涵括之 1,435 個開戶人與 1,500 個網銀人頭帳戶作為研究母體，透由相關基礎資料進行大數據之加值分析，再將分析結果作成相關態樣蒐整及政策建議回饋相關金融機構及有關機關，作為未來制定相關防制洗錢／打擊資恐政策或修正相關機制之參考。

二、研究範圍、方法與限制

本報告之研究範圍，係以前述 238 件可疑交易報告所涵括的 1,500 個網銀人頭帳戶及 1,435 個開戶者作為研究母體，研究方法則係將上開母體與本處相關資料庫進行比對，分析開戶人之背景資料、人頭帳戶之金流型態、及同時期偵查（含輔助）機關經由本處情資分送或主動偵辦該等帳戶所涉罪名，以風險為本方法（Risk-Based Approach, RBA），歸納出網銀人頭帳戶可能涉及較高風險之前置犯罪種類、販售人頭帳戶者有那些較高風險之背景或特徵，及與人頭帳戶對接之新興金融機構或支付方式存在那些威脅、弱點及可能面臨之風險，作出相關整理與探討，俾有助於本報告之使用者（執法機關、金融機構、同業公會及監理／政策機關），能將有限之反洗錢資源，按照風險等級作出最有效的運用，使執法機關聚焦在偵辦高風險之前置犯罪、金融機構能鎖定在高風險之客戶及金流態樣，並針對該等客戶之風險等級作出相應之遏止或減緩風險措施，有關機關亦能針對新興支付方式可能存在之威脅及可能面對之風險，制定或修正能有效遏止或減緩風險之法規或政策。

本研究母體之篩選條件已如前述，係具備前述一定特徵之網銀帳戶，惟財產犯罪之不法所得（Proceeds of Crime）因具有變價性及移轉性，理論上均有使用人頭帳戶清洗之可能性，並不限於網銀帳戶，亦即不具網銀功能之一般帳戶亦經常成為犯罪者之洗錢工具，因此在從微觀角度進入本研究母體之量化分析前，本研究先回顧本處於 108 年分送可疑交易報告之犯罪類型，使讀者對於可能使用人頭帳戶之各種犯罪類型及其風

[9] 截至本研究報告初稿完成日期 109 年 8 月 31 日止，已知內政部刑事警察局（法務部調查局臺中市調查處及中部機動工作站協辦）已偵破新○集團涉嫌跨國網路賭博及地下通匯，其餘集團仍由法務部調查局桃園市調查處、臺中市調查處及中部機動工作站等外勤處站偵辦中。

險概況，先有宏觀性的初步認知。另由於本研究除受前述帳戶抽樣條件限制，亦受到母體之蒐集時間、範圍（例如未申報黑數或集中於某些特徵），及執法機關偵辦時程等限制，無法以法院之確定判決、甚至無法以檢方之起訴書作為統計分析依據，誠係本研究最大之限制與缺憾，導致統計數據之精確度確有影響，但對於讀者觀察網銀人頭帳戶之趨勢走向，及瞭解其衍生之弱點與威脅，仍具有相當程度之參考價值，是以本報告在此等限制下，暫且定性為先趨性之官方研究，相關之遺漏或缺失，留待後續之相關研究加以修正或補充。

此外，作為本研究母體之人頭帳戶，其主要來源係犯罪集團向不特定之社會中下階層大量收購，且共同特徵為集中於相同或類似之網銀使用者代號、密碼及網轉約定帳戶等，也較能解釋需要大量人頭網銀帳戶之前置犯罪，至於貪瀆或企業高層舞弊等特定類型前置犯罪，其作為犯罪工具之人頭帳戶，多係向少數親人（Family Members）或親信（Close Associates）借用，因此本研究對於該等前置犯罪較無法作出合理或充分之說明，亦係本研究之侷限，合先敘明。

貳、調查局洗錢防制處 108 年分送可疑交易報告之犯罪類型

表 1：調查局洗錢防制處 108 年分送情資類型統計

涉及犯罪類型	小計（件）	百分比
偽造文書＋	17	0.66%
仿冒、盜版＋	1	0.04%
違反證交法（內線交易、市場操縱、掏空、證券詐欺＋）	128	4.97%
期貨交易法	28	1.09%
侵害營業秘密＋	1	0.04%
非法吸金	178	6.92%
背信或特別背信	33	1.28%
組織犯罪＋	1	0.04%
侵占	39	1.52%

涉及犯罪類型	小計（件）	百分比
公司法、商業會計法	345	13.41%
地下通匯	90	3.50%
貪污賄賂＋	22	0.86%
環保犯罪＋	2	0.08%
政府採購法	3	0.12%
毒品販運＋	18	0.70%
搶奪＋	1	0.04%
詐欺、幫助詐欺或洗錢＋	260	10.10%
賭博	34	1.32%
重利	9	0.35%
竊盜＋	1	0.04%
其他（含逃漏稅等）	1,333	51.81%
武擴（含資助武擴）	29	1.13%
全年分送數（分母）	2,573	100.00%
全年受理申報數	26,481	n/a
備註	因本處分送之個案情資，係先過濾相關資料庫再分析與整併不同金融機構針對同一或相牽連案件申報之數件可疑交易報告，不宜以全年受理申報數 26,481 件作為分母，因此以（罪名分送數）/（總分送數）*100% 作為百分比統計之基準。	

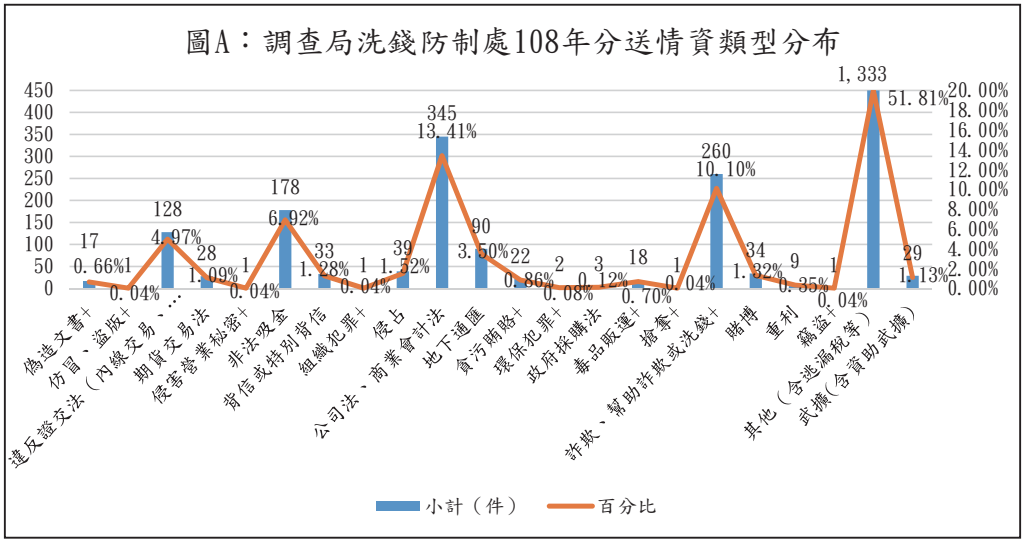
本處於 108 年總計接獲金融機構申報 2 萬 6,481 件可疑交易報告，經加值分析及整併後，分送予相關權責機關運用者計有 2,573 件。其中有 1,333 件、占 51.81% 係屬其他類型，極少部分係函轉金管會或中央銀行外匯局等行政機關職掌之案件，逃漏稅案件則占大宗，主要係因被申報對象為規避家族間之贈與稅、個人所得稅或公司營利事業所得稅等稅賦，而刻意以現金交易製造資金斷點，或以個人帳戶操作公司營運資金，抑或因公司實際營運處所在我國境內[10]，卻刻意以境外公司之 OBU 帳戶收取外國客戶貨款等交易異常情形而遭申報。論者有謂數位經濟下之稅務洗錢犯罪，尚有以架設境外網站逃避追緝、利用人頭取得與提供服

[10] 依所得稅法第 3 條規定，營利事務之總機構在中華民國境內者，應就其在中華民國境內外全部營利事務所得，合併課徵營利事業所得稅。

務，及利用非本國籍人頭帳戶掩飾及隱匿收入等態樣，並倡議建立外籍人士人頭氾濫之反制措施、加強對外籍人士之盡職審查（Customer Due Diligence），及強化跨機關之聯繫與情資分享，並鼓勵稅捐稽徵機關宜與本處、檢調機關、投資審議委員會及金管會建立橫向溝通平臺且定期分享查核案例，方能打擊數位經濟下層出不窮之洗錢逃稅犯罪行為[11]。

在偵查實務上常見使用人頭帳戶之犯罪類型，與分送之數量大致成正相關，依次為違反公司法（含商業會計法）案件計 345 件、占 13.41%；詐欺（含幫助詐欺或洗錢）計 260 件、占 10.10%；非法吸金計 178 件、占 6.92%；違反證交法（含內線交易、市場操縱、掏空及證券詐欺等）計 128 件、占 4.97%；地下通匯計 90 件、占 3.50%；侵占計 39 件、占 1.52%；賭博計 34 件、占 1.32%；背信或特別背信計 33 件、占 1.28%；武擴（含資助武擴）29 件、占 1.13%；違反期貨交易法案件計 28 件、占 1.09%；貪污賄賂計 22 件、占 0.86%；毒品販運計 18 件、占 0.70%（如表 1）。

若從所涉類型分布來看，主要的高峰落在逃漏稅、違反公司法（含商業會計法）、詐欺（含幫助詐欺或洗錢）、非法吸金及違反證交法（含內線交易、市場操縱、掏空及證券詐欺等）等 5 大類型，其次則為地下通匯、侵占、賭博、背信或特別背信等（如圖 A）。



[11] 梁建道，「數位經濟下逃漏稅洗錢態樣之分析與對策」，月旦財稅實務釋評，頁 17 至 18，2020 年 3 月。

參、網銀人頭帳戶開戶端之趨勢分析

一、自然人與法人帳戶分布

表 2：自然人與法人帳戶統計

類　　別	帳 戶 數	百 分 比
自　然　人	1,494	99.60%
本　國　人	1,494	99.60%
外　國　人	0	0%
法　　人	6	0.40%
本國公司	6	0.40%
外國公司	0	0%
合　　計	1,500	100.00%
附註	開戶人總數為 1,435 人（自然人 1,429 人、法人 6 人），其中 1,429 個自然人中，有部分開 2 個（含）以上帳戶，故其帳戶數為 1,494 戶，加上法人戶 6 戶，總數為 1,500 戶。	

在 1,500 個人頭帳戶的母體中，自然人計 1,494 戶、占 99.60%，均為本國人，尚未發現外國人；法人計 6 戶、占 0.4%，均為本國公司（如表 2），尚未發現外國公司之人頭帳戶，此種黑數可能係因人頭帳戶收購集團之語言及地緣關係、金融機構內部選案參數設定、前置犯罪特性或本研究抽樣限制所致。

在本研究中之母體中，雖僅發現 6 個本國公司人頭帳戶，代表性雖明顯不足，但該 6 個法人戶均呈現相同之特徵，諸如登記負責人均有毒品及／或詐欺前科、成立時間不久（半年內）、營業項目均為軟體服務及第三方支付業、資本額明顯過小[12]，與第三方支付業所承載之鉅額匯款顯不相稱等，大部分登記負責人亦提供其個人帳戶作為人頭帳戶等[13]，均係相當值得注意之表徵或趨勢。

[12] 資本額新臺幣 1 萬元計 2 家、80 萬元計 2 家、100 萬元及 500 萬元各 1 家。
[13] 6 家公司登記負責人中，僅 1 位負責人尚未被發現提供個人帳戶作為人頭帳戶。

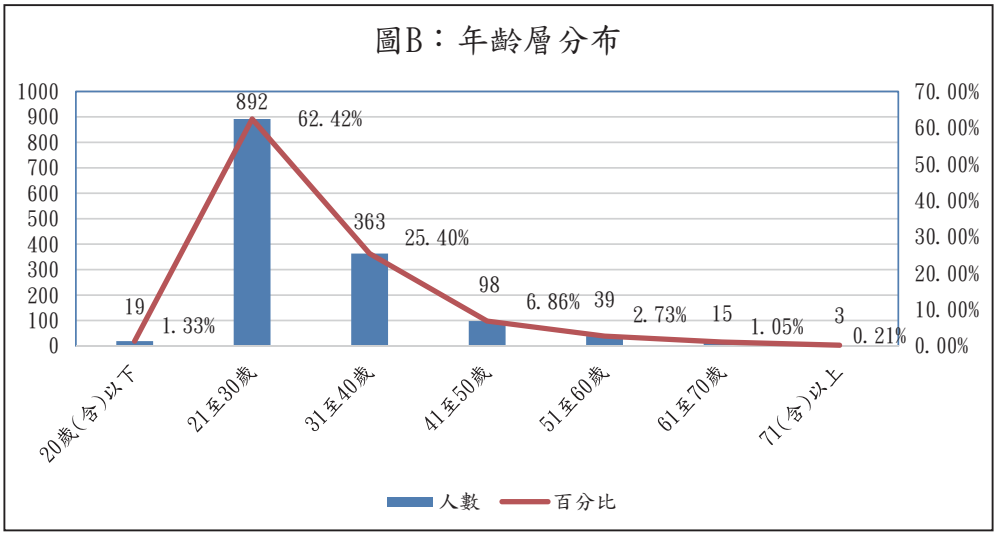
二、開戶人年齡層分布

表 3：年齡層統計

年齡層	人數	百分比
二十歲（含）以下	19	1.33%
二十一至三十歲	892	62.42%
三十一至四十歲	363	25.40%
四十一至五十歲	98	6.86%
五十一至六十歲	39	2.73%
六十一至七十歲	15	1.05%
七十一歲（含）以上	3	0.21%
合　　計	1,429	100.00%

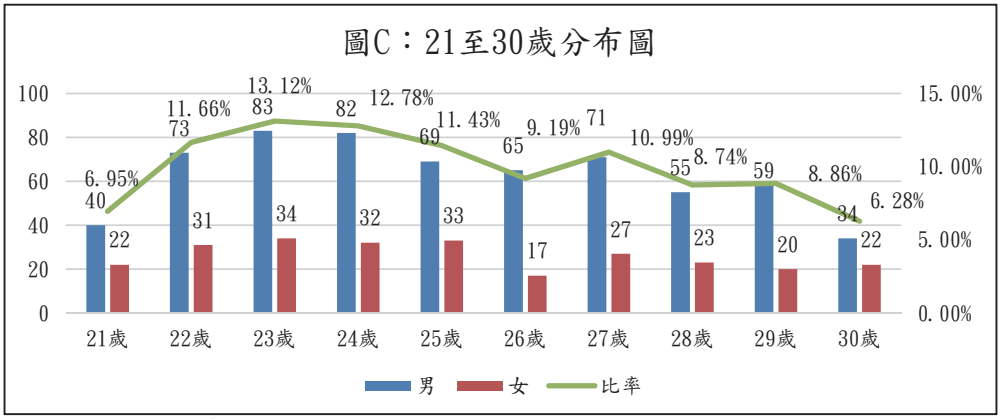
在 1,429 個自然人開戶人中，20 歲（含）以下計 19 名、占 1.33%；21 至 30 歲計 892 人、占 62.42%；31 至 40 歲計 363 人、占 25.40%；41 至 50 歲計 98 人、占 6.86%；51 至 60 歲計 39 人、占 2.73%；61 至 70 歲計 15 人、占 1.05%；71 歲（含）以上計 3 人、占 0.21%（如表 3）。販售人頭戶者之年齡層分布曲線，主要集中在 21 至 30 歲，其次為 31 至 40 歲（如圖 B）。

圖B：年齡層分布



若再針對 21 至 30 歲之族群細分，會發現大多數販售主體係甫從大學畢業或退伍不久之社會新鮮人（如圖 C），或因剛出社會暫時無法找到適合之工作、或薪資不如預期，甚至是失業，進而出售帳戶牟利[14]。

[14] 從部分個案中發現少數人頭戶或因欠缺社會經驗，於求職時遭不肖業主騙取帳戶，但因本研究無從逐一訪談母體，無法精準特定出售與遭詐之比例。



三、開戶人前科統計

表 4：前科統計

前科種類	罪 名	人 數	百 分 比
暴力犯罪	殺　　人	11	0.77%
	公共危險	66	4.60%
	妨害自由	34	2.37%
	傷　　害	51	3.55%
	槍　　砲	23	1.60%
	小　　計	185	12.89%
財產犯罪	重　　利	19	1.32%
	侵　　占	21	1.46%
	詐欺（含幫助詐欺及洗錢）	216	15.05%
	賭　　博	92	6.41%
	竊　　盜	63	4.39%
	強盜或恐嚇取財	32	2.23%
	小　　計	443	30.87%
毒品犯罪	毒　　品	228	15.89%
其　他	妨害風化	53	3.69%
	商標專利	23	1.60%
	小　　計	76	5.30%
無前科		707	49.27%
附　註	因部分母體有多項前科，因而個數加總將超過 1,435 人。 百分比之計算，仍以 1,435 人為分母。		

在 1,429 個自然人開戶人中，無前科者計 707 名、占 49.27%，約占

母體之半數；有暴力犯罪前科者計 185 名、占 12.89%；有財產犯罪者計 443 名、占 30.87%；有毒品犯罪者計 228 名、占 15.89%；其他犯罪者計 76 名、占 5.30%（如表 4），若僅以暴力、財產、毒品及其他四種犯罪類型區分，前科主要集中在財產犯罪之類型、其次依序為毒品犯罪及暴力犯罪。

若以前科罪名再細分，可發現前科主要集中在詐欺（含幫助詐欺及洗錢，以下同）及毒品兩個罪名，分別為詐欺前科 216 名、占 15.05%；毒品前科 228 名、占 15.89%，係風險最高的 2 個前科（如圖 D）。至於賭博前科 92 名、占 6.41%，雖不若詐欺及毒品前科顯著，但仍值加以關注。

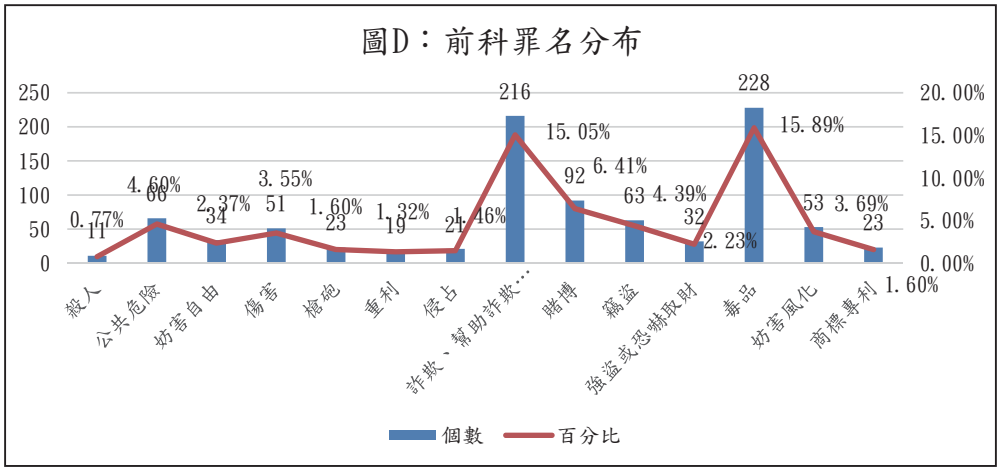


表 5：詐欺與毒品前科交叉分析表

交叉分析（人數）	詐欺	毒品	小計	重複比例
詐欺	86	130	216	60.19%
毒品	130	98	228	57.02%

另從前科罪名交叉分析中發現，一人同時具有詐欺與毒品前科之情形，相較於其他前科罪名之重複比例，具有高度之顯著性[15]，在 216 名詐欺前科者中，同時具毒品前科者，有 130 名、重複比例占 60.19%；

[15] 前科罪名之交叉分析，除詐欺與毒品外，各種排列組合均不具顯著性且限於篇幅，爰不再逐一表列及說明，但仍可看出毒品犯罪係萬惡之母，幾乎各種犯罪前科都有與毒品前科重複之狀況。

而 228 名毒品前科者中，同時具詐欺前科者，有 130 名、重複比例占 57.02%（如表 5）。詐欺前科是否係毒品前科者為賺取購買毒品費用，進而行騙或出售其帳戶作為詐欺或洗錢工具所致，尚無法直接證明，但應係可能性較高之合理推測。姑且不論詐欺與毒品前科兩者間之因果關係，至少從交叉分析結果可看出，詐欺與毒品前科同時存在之比例，大致上互為 60%（如表 5），同時具有詐欺與毒品前科者，係販售人頭帳戶風險最高之族群。

四、開戶人學歷分布

表 6：學歷統計

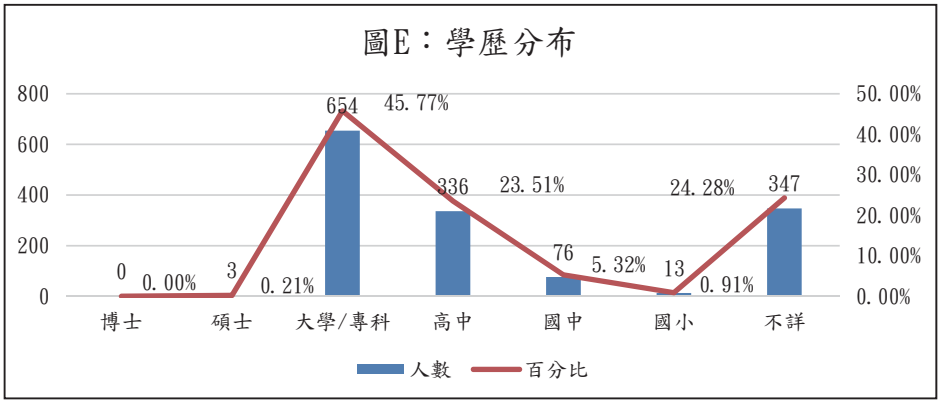
學歷分布	人數	百分比
博　士	0	0.00%
碩　士	3	0.21%
大學 / 專科	654	45.77%
高　中	336	23.51%
國　中	76	5.32%
國小（含以下）	13	0.91%
不　詳	347	24.28%
合　計	1,429	100.00%

在 1,429 個自然人開戶人中，並無具有博士學歷者；碩士計 3 名、占 0.21%；大學（含專科）計 654 名、占 45.77%；高中計 336 名、占 23.51%；國中計 76 名、占 5.32%；國小（含以下）計 13 名、占 0.91%；學歷不詳者計 347 名、占 24.28%（如表 6）[16]。

理論上，或至少從一般人的直觀，教育程度愈高，出售人頭帳戶之風險應較低，而教育程度愈低，則出售人頭帳戶之風險應較高，亦即兩者之關聯性應呈現負相關；惟從本研究之學歷分布圖來看（如圖 E），教育程度高低與販售人頭帳戶風險，卻狀似正相關，此現象當然不能解讀

[16] 係指開戶當時填寫之最高學歷資訊，與實際狀況容有誤差；另並非所有銀行均提供學歷資訊，併予說明。本研究母體之人頭帳戶，逾 7 成以上係於 108 年下半年開戶，因此仍有相當程度之參考價值。

為教育程度愈高、販售人頭帳戶之風險愈高，而係因學歷分布曲線與年齡分布曲線相當一致（如圖 B 及圖 E），毋寧解讀為教育程度與販售人頭之風險無關，至於販售人頭帳戶之風險，並沒有因為學歷愈高而相對降低，顯示我校園法制教育仍有加強之空間。



五、開戶人職業別統計[17]

表 7：職業別統計

職　業　別	人　　數	百分比
無業 / 臨時人員	255	17.84%
服務員	217	15.19%
店員 / 銷售員	140	9.80%
網拍 / 直播主	127	8.89%
工程員	126	8.82%
作業員	83	5.81%
保全員	72	5.04%
司機 / 物流 / 外送員	66	4.62%
攤　販	63	4.41%

[17] 以開戶人在銀行開戶資料中填寫之職業別作為統計標的。

職　業　別	人　　數	百分比
八大行業	54	3.78%
學生	52	3.64%
加油員	45	3.15%
娃娃機台主	42	2.94%
行政	23	1.61%
廚師	18	1.26%
美容 / 美髮	14	0.98%
軍人	12	0.84%
保姆	7	0.49%
主管 / 負責人	6	0.42%
船員	5	0.35%
自耕農	2	0.14%
合　　計	1,429	100.00%

有關人頭戶職業別之統計，並非要作出何種職業與洗錢或販售人頭帳戶風險高低有關之推論，且此種推論亦涉及職業歧視，因此本研究僅將職業別統計數據加以列表（如表 7）。事實上，出售人頭帳戶係來自於對金錢的需求，以職業別作區分，應不若以年收入區分有鑑別度（詳後述）。但其中仍有部分值得注意的行業別，如無業／臨時人員計 255 名、占 17.84%，可能係風險較高的族群，畢竟無業者不需使用薪資帳戶，而臨時人員之勞務收入，大多係收取現金，此種族群突然至銀行開戶，行員受理開戶時自然會提高警覺，在關懷客戶詢問（Know Your Customer）時，給予較高度之關切。另自稱網拍／直播主、八大行業及娃娃機台主，也是進行本研究發現較特殊之職業別。而職業別為軍人者，均係義務役者在退伍前或甫退伍，於開戶時所填寫，並非一般有正常收入之職業軍人。

六、開戶人年收入分布[18]

表 8：年收入級距

年收入（新臺幣）	人　數	百分比
無所得資料	972	68.02%
50 萬元（含）以下	457	31.98%
51 萬元至 99 萬元	0	0.00%
100 萬元（含）以上	0	0.00%
合　　計	1,429	100.00%

在 1,429 個自然人開戶人中，查無所得申報紀錄者（包含前述 6 個公司法人之登記負責人），計 972 名、占 68.02%；其餘 457 名、占 31.98% 者，年收入均低於 50 萬元（如表 8）。雖不乏論者提出諸多「貧窮並非犯罪根源」之說法[19]，但仍不否認貧窮與犯罪兩者間，仍存在一定程度之關聯性，例如相對剝奪感、飢寒起盜心及社會排除（Social Exclusion）等[20]。從本研究母體之經濟狀況顯示，大多為無所得資料或年收入 50 萬元以下者[21]，出售人頭帳戶可立即獲得數千元或數萬元之代價，甚至亦有僅提供犯罪集團「帳戶過水」服務，每月收取租金之狀況[22]，本研究依據上述統計資料，認所得愈高者，出售人頭帳戶之風險愈低，亦即所得與出售帳戶之風險大致呈正相關之推論，應與相關研究結論不相衝突。

[18] 以開戶人向稅捐機關申報之年所得作為統計標的。

[19] 中央研究院社會學研究所張硯評「階級不平等的心理學」，網址 http://twstreetcorner.org/2019/12/31changyenping。

[20] 卓雅芊，「從貧窮、犯罪與社會排除論少年犯罪問題之研究」，國立中正大學犯罪防治研究所碩士論文，2015 年 10 月，頁 1 至 2。

[21] 因部分金融機構未提供開戶問卷或問卷內並無更精細之年收入級距，可能母體中絕大部分之年收入遠低於 50 萬元。

[22] 甚至本處在初步分析時，發現有數人於開戶後，旋即於當日或次日掛失身分證，以規避金融機構之開戶審查並取得報案證明，而檢方加以採信，並以「被告既已提出身分證掛失證明・・・不排除其身分遭他人偽冒開戶」為由處分不起訴，是開戶後掛失身分證件，可能已係犯罪集團指導出售帳戶者脫罪之手法。

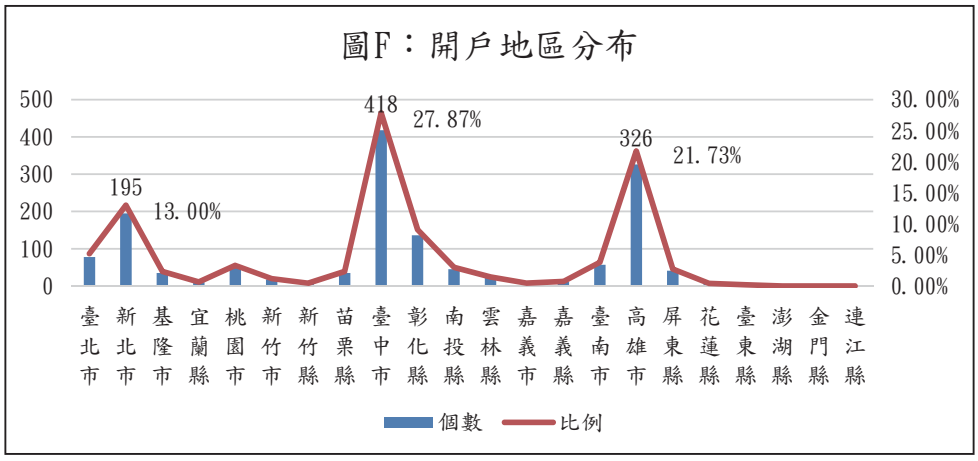
七、開戶地區分布

表 9：開戶地區統計

縣市	個　數	比　例	縣市	個　數	比　例
臺北市	78	5.20%	雲林縣	22	1.47%
新北市	195	13.00%	嘉義市	7	0.47%
基隆市	35	2.33%	嘉義縣	11	0.73%
宜蘭縣	10	0.67%	臺南市	57	3.80%
桃園市	50	3.33%	高雄市	326	21.73%
新竹市	18	1.20%	屏東縣	41	2.73%
新竹縣	7	0.47%	花蓮縣	6	0.40%
苗栗縣	35	2.33%	臺東縣	3	0.20%
臺中市	418	27.87%	澎湖縣	0	0.00%
彰化縣	136	9.07%	金門縣	0	0.00%
南投縣	45	3.00%	連江縣	0	0.00%
合　計	1,500				100.00%

本研究母體的 1,500 個人頭帳戶中[23]，開戶地集中度由高至低分別為：臺中市 418 戶、占 27.87%；高雄市 326 戶、占 21.73%；新北市 195 戶、占 13.00%；彰化縣 136 戶、占 9.07%；臺北市 78 戶、占 5.20%；臺南市 57 戶、占 3.80%；桃園市 50 戶、占 3.33%；南投縣 45 戶、占 3.00%；屏東縣 41 戶、占 2.73%；基隆市 35 戶、占 2.33%；苗栗縣 35 戶、占 2.33%；雲林縣 22 戶、占 1.47%；新竹市 18 戶、占 1.20%；嘉義縣 11 戶、占 0.73%；宜蘭縣 10 戶、占 0.67%；新竹縣 7 戶、占 0.47%；嘉義市 7 戶、占 0.47%；花蓮縣 6 戶、占 0.40%；臺東縣 3 戶、占 0.20%；澎湖縣、金門縣及連江縣均為 0 戶、占 0.00%（如表 9）。

[23] 開戶地與開戶人戶籍地之重疊性逾 8 成，因此不再重複作戶籍地之比較，可能與無業在家，或在戶籍地謀生有關。



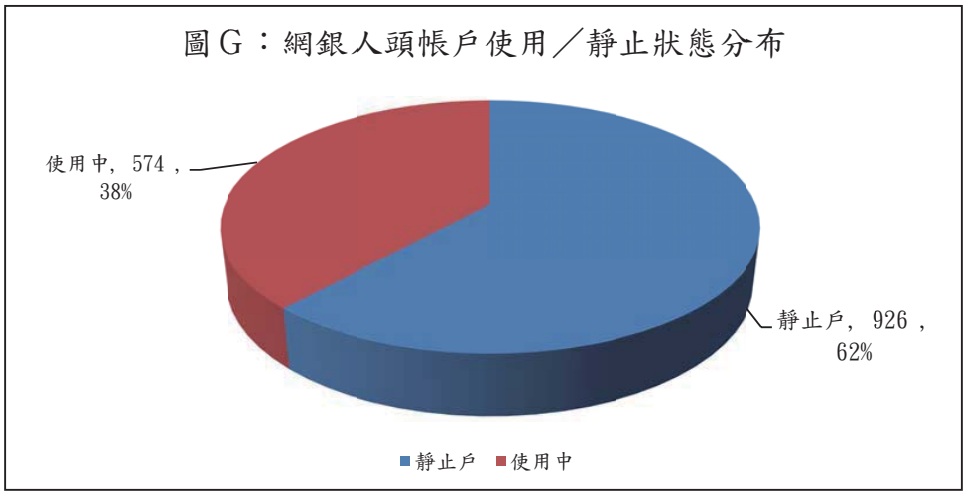
若開戶地由北到南排列，會發現人頭帳戶之開戶熱點，有集中於北（雙北市）、中（臺中市及彰化縣）及南（高雄市）三個都會區之趨勢（如圖 F），亦即與都市化之程度大致上呈現正相關之關聯性，而非本研究一開始所假定的負相關，亦即愈鄉下愈容易發現販售人頭帳戶之情形，可能與此種網銀人頭帳戶所涉及之前置犯罪多係都會型犯罪有關（詳後述），因此距離都會區愈遠，發現之個案愈少，而離島地區甚至未發現任何個案。

肆、網銀人頭帳戶使用端之趨勢分析

一、網銀人頭帳戶使用／靜止狀態統計

表 10：網銀人頭帳戶使用／靜止狀態統計

帳戶狀態	個　數	百分比
靜止戶	926	61.73%
使用中	574	38.27%
小　計	1,500	100.00%



在 1,500 個網銀人頭帳戶中，有 926 戶、占 61.73% 於設定網轉功能後、或僅出現 1 元、100 元或 1,000 元不等之小額測試匯款後，迄無任何資金流動；有 574 戶、占 38.27% 有密集的資金流動（如表 10 及圖 G），顯示犯罪集團像收集人頭電話卡般地收集網銀人頭帳戶，若與金融機構後續申報之可疑交易報告一併觀察，網銀人頭帳戶一般的使用期限約為 1 個月至半年不等[24]，與人頭電話卡使用期限大致雷同，人頭帳戶使用期限不長之原因，應與人頭電話卡大致相同，亦即係為了增加執法機關查緝之困難。

二、網銀人頭帳戶之活動國家／地區分布

因並非所有的金融機構在申報可疑交易時，均會提供申報對象之網銀帳戶 IP 登入資料或活動報表，而礙於技術及現實等限制，亦僅能提供特定時段之登入活動紀錄，因此無法針對前述已有資金活動之 574 戶進行全面性之統計分析。但從部分可疑交易報告所檢附之報表的片段資料中，仍可大致歸納出網銀人頭帳戶活動之國家或地區，主要出現在臺灣、大陸、香港、菲律賓、馬來西亞、越南、柬埔寨、美國及加拿大等，至於 IP 出現之國家或地區，究僅係跳版、或機房／水房之實際所在地，現階段尚無法完全確認，但若係位於東南亞國家，應可大致認定係機房／

[24] 因並非所有的金融機構均會針對同一個帳戶進行後續之動態申報，因此無法針對每個帳戶之使用期間進行有效之統計分析。

水房之實際所在，而美、加等國，則僅係跳版之可能性相對較高。

另從網銀人頭帳戶之 IP 及登入活動報表顯示，每個已有活動之網銀人頭帳戶，幾乎都會於每天、在不同的國家或地區進行密集的網路轉帳及查看餘額等相關活動，為節省匯款手續費，亦會約定數組相同之約轉帳戶，為了方便管理，會請開戶人設定相同之使用者名稱及密碼，此係網銀人頭帳戶的一種相當違常卻又普遍的特殊現象，但此種網銀支付工具之特性，並未被列入現行疑似洗錢表徵之常見態樣。傳統疑似洗錢表徵之發展，主要係聚焦於資金之數額、進出頻率，及交易人資歷與能力是否相稱等指標，為順應網銀及新型支付工具時代之來臨，在發展新表徵時，宜考量網銀及其他相關新型支付工具之特性。

三、網銀人頭帳戶之功能分布

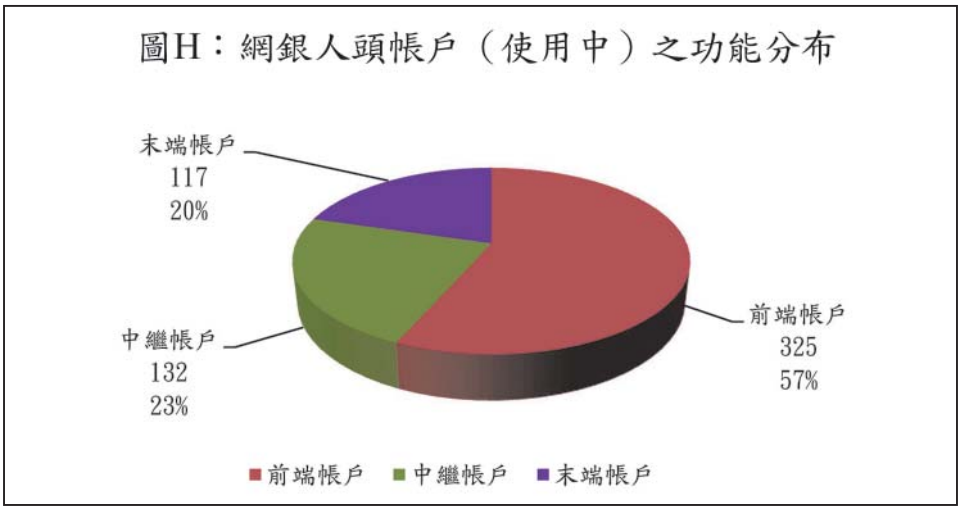
表 11：網銀人頭帳戶（使用中）之功能統計

帳戶功能	個　數	百分比
前端帳戶	325	56.62%
中繼帳戶	132	23.00%
末端帳戶	117	20.38%
小　　計	574	100.00%

在 1,500 個網銀人頭帳戶中，約轉帳戶之聯集計有 538 戶[25]、占 25.33%，但因母體中之靜止戶高達 926 戶，無從直接判斷各個帳戶及約轉帳戶究係前端、中繼或末端帳戶，僅能從有資金活動的 574 戶中，依據金流所呈現之交易型態或特徵加以研判。一般而言，若有密集且小額之資金轉入（數百元至數萬元居多），多係不特定人購買遊戲點數或匯入賭資等不法所得之最前端帳戶，金額較大者則可能為詐騙帳戶；金額稍大且密集度稍低者，可能為中繼帳戶，若每筆金額達數十萬元、甚至上百萬元或千萬元者，則大多為地下通匯帳戶；而匯入後密集以自動櫃

[25] 本研究母體中，發現有不同集團間之約轉帳戶，有部份帳戶重疊之交集現象，爰予剔除；另此種現象顯示，該約轉帳戶係地下通匯或水房洗錢帳戶之可能性甚高。

員機（ATM）密集提領現金者，則大多係末端帳戶，車手會將提領之現金攜至水房或特定場所暫時存放，之後再透過地下通匯帳戶，以貨款、投資、借貸或任何合法名義進行跨國洗錢。



依據前述之初級判斷標準，在有資金活動之 574 戶中[26]，狀似前端帳戶者計 325 戶、占 56.62%；狀似中繼帳戶者計 132 戶、占 23%；狀似末端帳戶者計 117 戶、占 20.38%（如表 11 及圖 H），但偶有交替變換功能之狀況。由於執法機關對於不同功能之人頭帳戶，後續之查證方向及重點會有所不同，因此有關人頭帳戶功能之區分，對於執法機關之後續偵查有相當之重要性，惟以上統計數據僅代表本研究母體各功能帳戶之分布狀況，且該母體分屬數個不同犯罪集團[27]，並不代表將等比例出現於其他個案中，不可不察。

[26] 本統計僅係針對相關網銀人頭帳戶進行初級研判，各該帳戶之實際用途，仍應以起訴或判決之認定為準，自不待言。

[27] 本處初步分析結果，作為母體之 1,500 個網銀人頭帳戶中，從相同之使用者代號及約定帳戶加以區分，至少分屬於 8 個以上犯罪集團，但實際集團數量仍須以偵辦結果為準。

四、網銀人頭帳戶與第三方支付業之對接情形

表 12：網銀人頭帳戶（使用中）與第三方支付對接統計

帳戶功能	個　數	對接第三方支付	百分比
前端帳戶	325	287	88.31%
中繼帳戶	132	98	74.24%
末端帳戶	117	79	67.52%
小　　計	574	464	80.84%

在前述有資金活動之前端帳戶 325 戶中，有 287 戶與第三方支付業[28]對接、占 88.31%，比例最高；中繼帳戶 132 戶中，有 98 戶與第三方支付業對接、占 74.24%；末端帳戶 117 戶中，有 79 戶與第三方支付業對接、占 67.52%；總計有資金活動之帳戶 574 戶中，有高達 464 戶與第三方支付業對接、占 80.84%（如表 12）。從以上數據發現，不論是前端、中繼及末端帳戶，與第三方支付業對接之狀況均相當高。

五、網銀人頭帳戶可能涉及之前置犯罪[29]

表 13：網銀人頭帳戶（使用）可能涉及前置犯罪統計

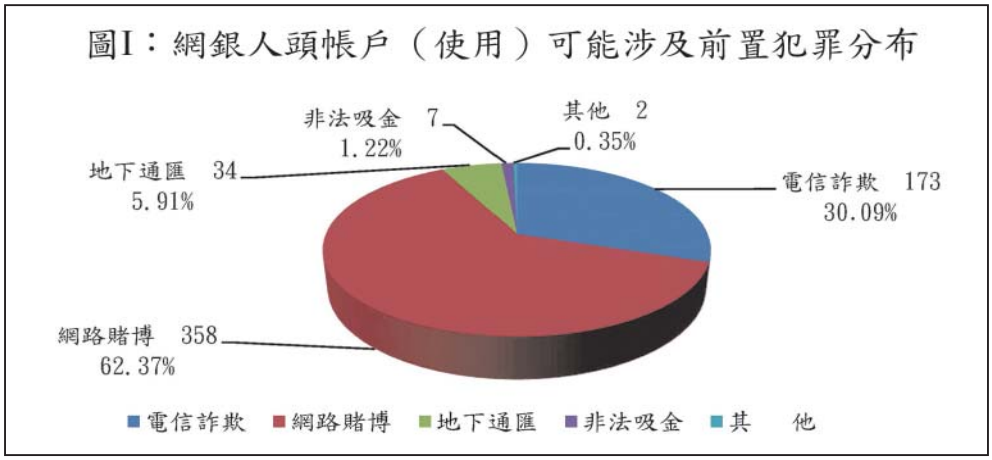
前置犯罪	個　數	百分比
電信詐欺	173	30.09%
網路賭博	358	62.37%
地下通匯	34	5.91%
非法吸金	7	1.22%
其　　他[30]	2	0.35%
小　　計	574	100.00%

[28] 在中國大陸及部分歐美國家，只要係透過非銀行體系之支付系統，即統稱為第三方支付，有關第三方支付的分類，但在臺灣則因相關政策考量，區分為：一、電子支付業；二、電子票證業；三、第三方支付業。相關內涵及區別詳後述，本研究所稱之第三方支付業係指上述第三種。

[29] 有關可能涉及前置犯罪之統計，主要係以本處之初步分析結果、部分可疑交易報告記載之警方或本局外勤處站調卷資訊、地檢署起訴書及少數法院判決個案作概括性之統計，與實際狀況必然有一定程度之落差，但與趨勢應大致相符。

[30] 司法詐欺及違反廢棄物清理法各 1 案。

因本研究母體 1,500 個網銀人頭帳戶中，有 926 戶係靜止戶，在統計期間內尚未被啟用，因此無從得知係被作為何種前置犯罪之匯款或洗錢工具。至於已有資金活動之 574 戶中，可能涉及電信詐欺有 173 戶、占 30.09%；可能涉及網路賭博有 359 戶、占 62.43%；可能涉及地下通匯有 34 戶、占 5.91%；可能涉及非法吸金有 7 戶、占 0.35%（如表 14 及圖 I）。並未發現違反證交法、公司法及稅務犯罪等使用人頭帳戶之高風險犯罪，主要係因該等前置犯罪之人頭帳戶蒐集主體（股市炒手、代書或記帳業者、公司經營階層）及被蒐集對象（親友），與本研究母體之蒐集主體（犯罪集團）及被蒐集對象（親友不特定之社會中下階層），有族群及特性上之差異所致。



伍、研究發現與相關建議

前述各該統計數據所對應之風險項目，例如開戶人之年齡、前科、學歷、職業／年收入、帳戶開戶及活動國家／地區、上下游功能帳戶分布及前置犯罪等，請參閱各該統計資料及相關說明，本節不再贅述。以下僅針對網銀人頭帳戶之威脅、弱點及所造成之洗錢風險[31]，提出研究發現與相關建議如下：

[31] 威脅係指可能造成危害之個人、團體、目標或活動；弱點係指由威脅所利用、支持或有助於其活動之事物。馮素華及陳啟明譯，「FATF 新修正通過國家洗錢／資助恐怖分子風險評估指引」，收錄於本局洗錢防制處 101 年洗錢防制工作年報，102 年 6 月，頁 80。

一、網路交易及相關金融科技係今後之必然趨勢，宜強化客戶審查流程及動態防制作為，以兼顧洗錢防制與金融普及性

網路交易有其便利、隱密、低成本、普遍與快捷等特性，亦伴隨技術面、交易面之不確定性與風險，甚而引發新型態犯罪手法[32]。網路交易及其嫁接之相關金融科技（FinTech）不論在現今及未來，均已呈現沛然莫之能禦的必然發展趨勢，僅能加以導正而無法全然禁止[33]，否則將嚴重戕害國家之全球競爭力與市場機會，但也因其便利、隱密及快捷等特性，使犯罪集團有可乘之機，造成金融監理及執法機關查核之困難；甚且，因網銀帳戶與相關金融科技均係高度非面對面交易之支付工具，兩種以上之高風險支付工具透過交易對接後，將會加劇洗錢／資恐風險之「乘數效果」。因此，洗錢防制與金融普及性 (Financial Inclusion) 如何兼顧，係值得吾人深思的首要課題。本研究發現網銀人頭帳戶在現階段與第三方支付業對接之狀況相當普遍而密集，有必要對此現象進行相關探討，尤其是化整為零、化零為整僅需數以「秒」計[34]的時間，即可完成多層化的資金移轉，造成金融監理及犯罪調查之困難。隨著網路及科技之快速發展，網銀帳戶在未來勢必與更多元之金融科技支付工具對接，因此本研究於下段針對網銀帳戶與第三方支付業對接現象所發現之問題與所提建議，亦可作為有關機關或金融機構在未來研擬其他金融科技業相關防制對策或措施之參考。

在中國大陸及部分歐美國家，只要透過非銀行體系之支付系統，即統稱為第三方支付[35]。但在臺灣則因相關政策考量，區分為電子支付業、電子票證業及第三方支付業。目前由金管會主管的電子支付業計有 28 家

[32] 蓋華英、谷湘儀、黃文昌、曾逸凡、陳美如合著，「如何防制人頭戶之研究」，臺灣證券交易所委託研究案，2001 年 12 月，頁 4~9。

[33] 例如比特幣等虛擬通貨，各國政府亦已從初期的完全禁止，走向有限度之開放，完全無法阻檔此種網路支付工具之發展趨勢。

[34] 比喻在極短的時間內，即可完成數筆網路交易。

[35] 歐盟支付服務指引（Payment Services Directive, PSD）定義為：經由付款人同意，藉由何電信、數位或資訊設備將交易款項交付予電信業者、、數位、資訊或網絡營運商，並以其作為付款人與受款人之中間交易人者；美國統一資金服務法（Uniform Money Services Act, UMSA）則以資金服稱之，凡資金傳輸、支票兌現或匯兌業務均屬之；日本資金結算法則分為預付式票證及資金移動兩種。蔡宗霖，網路交易支付大躍進：簡介中國非金融機構支付服務管理辦法，科技法律透析，2010 年 11 月，頁 9。

（含 5 家專營及 23 家兼營機構）、電子票證業計有 5 家（含 4 家專營及 1 家兼營機構）[36]；而由經濟部主管的第三方支付業登記家數則高達 1 萬 1,115 家，扣除已解散或廢止等 1,961 家，目前存續家數仍高達 9,154 家[37]（相關比較資訊整理如表 14）。前述金管會主管之電子支付業及電子票證業，因家數較少，金融監理亦較為落實，且已有相當完整的防制洗錢／打擊資恐規範，客戶審查及資料保存亦相對完備，因此在落實防制洗錢／打擊資恐國際標準的技術遵循面（Technical Compliance）及金融監理之執行效能（Effectiveness）上，目前尚未有重大窒礙之處。但對金融情報中心及執法機關而言，目前最大的難處在於情報分析與執法之執行效能，亦即該等支付工具（第三方支付亦有相同之問題）交易速度及頻率過於龐大，已非傳統分析或偵查人力所能負荷[38]，此難題有賴業者願意配合及協助建置完整 Log 檔等資料庫及執法機關發展大數據偵查技術加以克服。

表 14：廣義第三方支付比較表

行業別	電子支付業	電子票證業	第三方支付業
家數	28（專營 5+ 兼營 23）	5(專營 4+ 兼營 1)	9,154
主管機關	金管會	金管會	經濟部
適用法規	1. 電子支付機構管理條例 2. 電子支付機構業務管理規則 3. 電子支付機構使用者身分確認機制及交易限額管理辦法 4. 電子支付機構防制洗錢及打擊資恐注意事項範本 5. 銀行業及其他經金管會指定之金融機構防制洗錢及打擊資恐內部控制與稽核制度實施辦法 6. 金融機構對經指定制裁對象之財物或財產上利益所在地通報辦法 7. 電子支付機構評估洗錢及資恐風險及訂定相關防制計畫指引等…	1. 電子票證發行管理條例 2. 電子票證發行機構業務管理規則 3. 電子票證應用安全強度準則 4. 電子票證發行機構防制洗錢及打擊資恐注意事項範本 5. 銀行業及其他經金管會指定之金融機構防制洗錢及打擊資恐內部控制與稽核制度實施辦法 6. 金融機構對經指定制裁對象之財物或財產上利益所在地通報辦法 7. 電子票證機構評估洗錢及資恐風險及訂定相關防制計畫指引等…	1. 信用卡機構簽定提供網路交易代收代付服務平臺業者為約商店自律規範 2. 第三方支付服務定型化契約應記載及不得記載事項

[36] 金管會 109 年 8 月 4 日「109 年 6 月份信用卡、現金卡、電子票證及電子支付機構業務資訊」，網址 http//:fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2。

[37] 資料來源：政府資料開放平臺，網址 http:// data.gov.tw/dataset/22184，查詢日期：109 年 8 月 27 日。

[38] 實則，相關電子化支付工具均會造成相同的問題，相關分類及說明，請參閱沈中華、王儷容及蘇哲緯，臺灣行動支付發展與歸類探討，存款保險資訊季刊，第 33 卷第 1 期，2020 年 3 月。

最低實收資本額限制	5億元		3億元		無限制
最高儲值金額限制	5萬元		1萬元		不得儲值
交易限額	第1類:限個人，付款及儲值	每月收付累計上限3萬元、儲值餘額上限1萬元	第1類：繳交政府規費稅損等	不受限	無限制
	第2類：個人及非個人，收款、付款及儲值	每月收付金額上限30萬元	第2類	單筆上限1千元、單日累積上限3千元	
	第3類：個人及非個人；收款、付款及儲值且限臨櫃辦理	個人每月收付金額上限100萬元、非個人上限為1千萬元且應臨櫃辦理			

為防止第三方支付成為防制洗錢／打擊資恐的漏洞，法務部已於103年2月間會銜經濟部正式公告第三方支付業亦適用洗錢防制法有關金融機構之規定[39]，因此第三方支付業仍有依據洗錢防制法規定，進行客戶審查、留存交易紀錄及申報大額與可疑交易報告之義務。但第三方支付業因本質上係代收代付業務，因此在政策上劃歸經濟部管轄，該部既有之主管業務本身即相當龐雜，其防制洗錢／打擊資恐專業、經驗及監理能量自難期與金管會同步，而從上列表格所列資訊顯示，第三方支付業目前家數高達9,154家、業者素質良莠不齊，亦缺乏完整之防制洗錢／打擊資恐相關技術規範，以經濟部現有能量，欲落實防制洗錢／打擊資恐之監理，確有事實上之困難。另第三方支付業之代收代付業務，在性質上雖非銀行匯款業務，但透過業者內部虛擬帳號之設計，實質上仍可達成資金移轉之目的及效果，加上其快速、便捷，且無交易額度限制等特性，自然淪為犯罪集團欲加以利用之弱點。

本研究發現網銀人頭帳戶與第三方支付業對接之狀況相當密集，且若干第三方支付公司之登記負責人本身即前科累累、甚至亦係人頭帳戶之提供者，另由於第三方支付業並非特許行業，其設立人資格、資本額

[39] 法務部及經濟部103年2月19日法令字第10204554850號暨經商字第10202146100號會銜令：指定第三方支付自即日起適用洗錢防制法有關金融機構之規定。

及交易限額均毫無限制，防制洗錢／打擊資恐之技術遵循僅有少數自律規範及行政指導關於反洗錢之隻字片語，且登記家數已近萬計，規範強度及監理密度均有所不足。經濟部已於本年 9 月初開始舉辦「研商第三方支付服業防制洗錢及打擊資恐辦法草案」專案會議[40]，並邀集有關機關、專業單位、主要業者及同業工會共同參與討論，係朝上述第三種途徑發展，本研究對於經濟部及與會單位對於填補第三方支付業防制洗錢／打擊資恐規範缺漏所作之努力與貢獻表達高度之認同與肯定，相關法規之技術遵循缺漏，在未來應可獲致大幅度之改善。至於未來如何提昇第三方支付業之監理密度，本研究建議或可依據行政程序法第 16 條以委託行使公權力之方式，將監理權限委託資策會等民間團體、會計師或律師等專業人士查核，並科予受查核對象繳納全部或一定比例規費之義務，或依據同法第 19 條請求金管會進行職務協助等，拒繳規費、不接受查核或違反相關規定者，再依據公司法相關規定科處罰鍰、廢止公司登記或部分登記事項，或依據洗錢防制法第 7 條科處罰鍰，均不失為可行之方法，本研究尊重各權責機關之協調結果，僅在此提出以上之思考方向供參酌。

另代收代付之資金移轉係伴隨實際交易而產生，如何以數位技術檢驗該交易是否實際存在，亦係未來發展防制作為之重點，至於第三方支付業者本身應如何防制網路交易及金融科技弱點所造成的洗錢風險，不妨從強化數位資訊之客戶審查流程，及動態防制作為開始著手，例如從載具、APP、IP 位置、使用者資訊及密集的網路交易 Log 檔，以完整的大數據資料（Big Data）配合電腦運算等輔助工具，建立高風險指標俾及時發現異常交易狀況，使金融機構犯罪預警之功能得以發揮，並適時提供金融情報中心與司法警察機關有價值之犯罪情資及查證路線，有效防制洗錢及相關重大犯罪。

二、網銀人頭帳戶有突然活動、暫時休眠、交易密集、快速及無遠弗屆等特性，現行疑似洗錢表徵無法涵蓋網銀人頭帳戶之異常狀況

[40] 經濟部已分別於 109 年 9 月 9 日及 10 月 5 日召開兩次會議，目前仍持續進行中，與會單位包括：行政院洗錢防制辦公室、法務部、調查局洗錢防制處、金管會、內政部刑事警察局、第三方支付紅藍綠三大業者等、無店面零售商業同業公會、台灣品牌暨跨境電子商務協會，及資訊工業策進會科法所等。

表 15：金融機構申報之疑似洗錢表徵統計

疑似洗錢表徵及其代碼	個數	百分比
A11: 同一帳戶在一定期間內之現金存、提款交易，分別累計達特定金額以上者	9	2.72%
A12: 同一客戶在一定期間內，於其帳戶辦理多筆現金存、提款交易，分別累計達特定金額以上者	8	2.42%
A14: 客戶突有達特定金額以上存款者（如將多張本票、支票存入同一帳戶）	2	0.60%
A15: 不活躍帳戶突有達特定金額以上資金出入，且又迅速移轉者	15	4.53%
A16: 客戶開戶後立即有達特定金額以上款項存、匯入，且又迅速移轉者	12	3.63%
A17: 存款帳戶密集存入多筆款項達特定金額以上或筆數達一定數量以上，且又迅速移轉者	84	25.38%
A18: 客戶經常於數個不同客戶帳戶間移轉資金達特定金額以上者	30	9.06%
A1A: 客戶每筆存、提金額相當且相距時間不久，並達特定金額以上者	22	6.65%
A1B: 客戶經常代理他人存、提，或特定帳戶經常由第三人存、提現金達特定金額以上者	1	0.30%
A1C: 客戶一次性以現金分多筆匯出、或要求開立票據（如本行支票、存放同業支票、匯票）、申請可轉讓定期存單、旅行支票、受益憑證及其他有價證券，其合計金額達特定金額以上者	1	0.30%
A83: 數人夥同至銀行辦理存款、提款或匯款等交易者	2	0.60%
A91: 客戶具「存款帳戶及其疑似不法或顯屬異常交易管理辦法」、「銀行防制洗錢及打擊資恐注意事項範本」、或其他無法完成確認身分相關規定程序之情形者	4	1.21%
A92: 同一地址有大量客戶註冊、居住者經常變更，或地址並非真實居住地址	1	0.30%
AB1: 客戶經常匯款至國外達特定金額以上者	1	0.30%
AZZ: 其他有疑似洗錢交易情形者	139	41.99%
小　　計	331	100.00%

本研究母體 1,500 個網銀人頭帳戶係來自金融機構所申報之 238 件可疑交易報告，但因每個報告可勾選兩個以上之疑似洗錢表徵，故表徵數 331 個大於報告數 238 件，先予說明。其中，網銀人頭帳戶被申報最多之表徵為「AZZ: 其他有疑似洗錢交易情形者」，計 139 次、占 41.99%，主

要係因大部分帳戶仍係靜止戶，主要篩選依據係相同之使用者名稱、密碼，或 IP 位置在短時間內出現在不同國家或地區等異常等警訊；次高者（10 次以上）依次為「A17: 存款帳戶密集存入多筆款項達特定金額以上或筆數達一定數量以上，且又迅速移轉者」，計 84 次、占 25.38%；「A18: 客戶經常於數個不同客戶帳戶間移轉資金達特定金額以上者」，計 30 次、占 9.06%；「A1A: 客戶每筆存、提金額相當且相距時間不久，並達特定金額以上者」，計 22 次、占 6.65%；「A15: 不活躍帳戶突有達特定金額以上資金出入，且又迅速移轉者」，計 15 次、占 4.53%；「A16: 客戶開戶後立即有達特定金額以上款項存、匯入，且又迅速移轉者」，計 12 次、占 3.63%（如表 13）。從以上統計顯示，現行之疑似洗錢已無法涵蓋網銀人頭帳戶之交易特性，此乃因傳統疑似洗錢表徵之發展，主要係聚焦於資金之數額、進出頻率，及交易人資歷與能力是否相稱等指標，而犯罪集團如同蒐集電話卡一般地蒐集網銀人頭帳戶，為方便管理，會設定相同之使用者代號及密碼，並有輪流使用或一定期間即加以替換之情形，雖有部分金融機構已有所警覺並於內部自行研發相關警訊指標，但為順應網銀及新型支付工具時代之來臨，呼籲相關金融機構在未來發展新表徵時，宜考量網銀及其他相關新型支付工具之特性。

三、落實異常與人頭帳戶之通知及風險控管與善後機制

曾有研究報告針對證券人頭戶議題，提出證券商得於相關帳戶交易異常之際，主動寄發異常交易通知書（Warning Letter），告知該帳戶異常交易情形及出借人可能面臨之法律責任，以收警惕及嚇阻之效果，並以該通知制度促使人頭戶本人知悉其帳戶正遭利用，使其難再以主觀上並無故意作為抗辯之政策建議[41]。現行制度已大致符合該建議之精神，於「防杜人頭帳戶範本」第 1 條第 4 項規定：「符合『存款帳戶及其疑似不法或顯屬異常交易管理辦法[42]』（下稱：『帳戶顯屬異常管理辦法』）

[41] 蓋英華、谷湘儀、黃文昌、曾逸凡、陳美如合著，「如何防制人頭戶之研究」，臺灣證券交易所委託研究案，2001 年 12 月，頁 6~7。

[42] 該辦法第 4 條所稱疑似不法或顯屬異常交易存款帳戶之認定標準及分類如下：一、第一類：（一）屬偽冒開戶者。（二）屬警示帳戶者。（三）屬衍生管制帳戶者。二、第二類：（一）短期間內頻繁申請開立存款帳戶，且無法提出合理說明者。（二）客戶申請之交易功能與其年齡或背景顯不相當者。（三）客戶提供之聯絡資料均無法以合理之方式查證者。（四）存款帳戶經金融機構或民眾通知，疑為犯罪行為人

第 13 條第 2 項所列情形者[43]，應拒絕客戶開戶之申請；對於疑似人頭申請開戶者，得委婉拒絕或暫時不受理金融卡、電話語音銀行、網路銀行等自動化服務業務。」而「金融機構開戶作業審核程序暨異常帳戶風險控管之作業範本」（下稱：「異常帳戶風險控管作業範本」）第 2 第 1 項第 3 款亦規定：「受理開戶時應向客戶宣導，如提供帳戶供非法使用應負法律責任。」係針對疑似人頭帳戶開戶時之防制措施。至於事後發現疑似人頭帳戶之情形，則規範於同範本第 5 條：「金融機構辦理存款帳戶應建立事後追蹤管理機制……開戶後發現可疑之客戶，應以電話、書面或實地查訪等方式再確認，並作『適當處理』。」亦即現行機制已有相關之風險控管與善後機制。

惟本處在受理大量疑似網銀人頭帳戶可疑交易報告之過程中，發現申報之金融機構對於應如何「適當處理」有不同之作法，有逕對疑似人頭開戶人拒絕開戶／逕為關戶、停止網銀功能、拒發金融卡、亦有為數不少之金融機構逕致電要求本處具體指示或同意金融機構建議之處置措施等不同狀況；實則，本處僅係依法受理可疑交易報告之金融情報中心，並無權指示或同意金融機構對開戶人做出任何處置。金融機構於發現疑似人頭帳戶時，應如何處置始符合前述「異常帳戶風險控管作業範本」第 5 條所稱之「適當處理」，本研究建議金融機構採取「帳戶顯屬異常管理辦法」第 5 條列舉之具體措施[44]（按：本研究母體大部分屬第二類之

使用者。（五）存款帳戶內常有多筆小額轉出入交易，近似測試行為者。（六）短期間內密集使用銀行之電子服務或設備，與客戶日常交易習慣明顯不符者。（七）存款帳戶久未往來，突有異常交易者。（八）符合銀行防制洗錢注意事項範本所列疑似洗錢表徵之交易者。（九）其他經主管機關或銀行認定為疑似不法或顯屬異常交易之存款帳戶。

43 該辦法第 13 條第 2 項全文：銀行應確認客戶身分，始得受理客戶開立存款帳戶，如有下列情形之一者，應拒絕客戶之開戶申請：一、疑似使用假名、人頭、虛設行號或虛設法人團體開立存款帳戶。二、持用偽、變造身分證明文件或出示之身分證明文件均為影本。三、提供之文件資料可疑、模糊不清、不願提供其他佐證資料、或提供之文件資料無法進行查證。四、客戶不尋常拖延應提供之身分證明文件。五、客戶開立之其他存款帳戶經通報為警示帳戶尚未解除。但有下列情形之一者，不在此限：（一）為就業薪資轉帳開立帳戶需要，經當事人提出在職證明或任職公司之證明文件。（二）為向銀行申辦貸款並經審核同意撥款。（三）其他法律另有得開立帳戶之規定。六、受理開戶時有其他異常情形，且客戶無法提出合理說明。

44 該辦法第 5 條規定：存款帳戶依前條之分類標準認定為疑似不法或顯屬異常交易者，銀行應採取下列處理措施：一、第一類：（一）存款帳戶如屬偽冒開戶者，應即通知司法警察機關、法務部調查局洗錢防制處及財團法人金融聯合徵信中心，銀行並應即結清該帳戶，其剩餘款項則俟依法可領取者申請給付時處理。（二）存款帳戶

非「偽冒開戶、警示帳戶及其衍生帳戶」)，並參酌防制洗錢／打擊資恐國際標準第 1 項建議之精神，以風險為本方法[45]，依據相關帳戶之風險等級及前述相關作業規定，實施與風險等級相對應之反制措施，俾有效減緩或遏止洗錢／資恐風險。

本研究重申上開作業規範並呼籲相關金融機構落實上開規定，於開戶時或嗣後發現帳戶有明顯疑遭他人利用為犯罪工具之可疑表徵時（例如在同一時段 IP 位置出現於不同國家／地區等），通知開戶人臨櫃或提出書面說明，並於書面通知加註具警語，若開戶人說明之理由顯不足採信者，金融機構得經內部核決程序，將帳戶內餘額以現金返還法定領取權人或匯至其指定之親友帳戶並均加以登記，俾日後循線清查，若無正當理由不到場或提出說明者，得將帳戶餘額予以提存。除能維持警惕與嚇阻之效果外，亦能兼顧預防犯罪及人民財產權之保障，並增加犯罪集團收購人頭帳戶之成本。

四、金融機構宜在不違反相關法規及影響執法機關偵查之前提下進行同業照會

在銀行實務上，金融機構在同業間已有行之多年的「照會」慣例，亦即同業間會針對特定事件或帳戶進行某種程度之資訊交換，但資訊交換的範圍及深度則不一，照會慣例有助於擴大可疑交易報告視角，並有利於提昇可疑交易報告之申報品質與金融情報中心之後續分析研判，被照會之金融機構亦能因此對被照會之帳戶有所警惕，進而提高該帳戶之風險等級並適時申報可疑交易，因此本研究鼓勵金融機構同業間，在不違反相關法規及影響執法機關偵查之前提下，進行相關正式或非正式之資訊交換。但對於第三方支付業者，本研究則持保留、甚至傾向否定之

經通報為警示帳戶者，應即通知財團法人金融聯合徵信中心，並暫停該帳戶全部交易功能，匯入款項逕以退匯方式退回匯款行。（三）存款帳戶屬衍生管制帳戶者，應即暫停該帳戶使用提款卡、語音轉帳、網路轉帳及其他電子支付功能，匯入款項逕以退匯方式退回匯款行。（四）依其他法令規定之處理措施。二、第二類：（一）對該等帳戶進行查證及持續進行監控，如經查證有不法情事者，除通知司法警察機關外，並得採行前款之部分或全部措施。（二）依洗錢防制法等相關法令規定之處理措施。

[45] 應用以風險為本之方法（Risk-Based Approach）在體例上規範於防制洗錢／打擊資恐國際標準的第一項建議，依體系解釋之法學方法，後續各項建議均有其適用，亦係解釋防制洗錢／打擊資恐相關技術規範之指導原則。

態度，或至少先對該第三方支付業者進行一定程度之研究或瞭解後，再決定是否進行照會事宜，否則可能因該第三方支付業者本身即為犯罪集團之一員而造成曝光或產生不良後遺。

五、金融機構申報可疑交易時，除提供客戶審查及交易資料外，亦宜提供其他任何有助於後續分析及犯罪偵查之相關資訊

本處在受理大量疑似網銀人頭帳戶可疑交易報告之過程中，絕大部分之金融機構僅提供開戶資料及一定期間之交易明細，並敘述相關可疑之理由，但卻未同步提供可佐證該等可疑理由之相關資訊，例如部分金融機構在可疑報告中描述有不明人士在銀行門口或車子內以電話遙控開戶人填寫相關開戶資料，如能進一步提供車號或相關錄影畫面，或除描述該帳戶之 IP 在短時間內密集出現在不同的國家／地區顯有異常外，同時檢附相關 IP 登入資料，而非僅單純提供一組或數組沒有登入時間及活動紀錄的 IP，將可加快金融情報中心之分析腳步，縮短目前執法機關追查金流與犯罪集團移轉犯罪所得速度上的差距，避免喪失蒐證最佳契機或證據遭滅失，曾有極少數金融機構人員不解的表示「並不曉得這些資訊亦能申報」等語，但多數行員會相當機警的提供開戶時取得之相關資訊，例如請人頭開戶者電話照會「公司老闆」的電話號碼或提供臨櫃錄影或手機翻拍畫面等，更有申報單位提供相當完整的 IP 登入資訊，此等案關資訊極有助於執法機關循線追查。因此，本研究報告亦鼓勵金融機構在申報可疑交易報告時，一併提供任何有助於後續分析與追查之額外資訊。

參考文獻

一、政府機關及同業公會相關函示：

（一）金融監督管理委員會 108 年 12 月 31 日金管銀法字第 1080225400 號函。

（二）法務部調查局 108 年 12 月 11 日調錢貳字第 10835565590 號函。

（三）中華民國銀行商業同業公會全國聯合會 109 年 1 月 13 日全一電字第 1080010756 號函。
（四）法務部及經濟部 103 年 2 月 19 日法令字第 10204554850 號暨經商字第 10202146100 號會銜令。

二、期刊論文：

（一）林志潔，「防制洗錢之新思維—論金融洗錢防制、金融監理與偵查權限」，檢察新論，第 3 期，2008 年 1 月。
（二）沈中華、王儷容及蘇哲緯，「臺灣行動支付發展與歸類探討」，存款保險資訊季刊，第 33 卷第 1 期，2020 年 3 月。
（三）卓雅芊，「從貧窮、犯罪與社會排除論少年犯罪問題之研究」，國立中正大學犯罪防治研究所碩士論文，2015 年 10 月。
（四）馮素華及陳啟明譯，「FATF 新修正通過國家洗錢／資助恐怖分子風險評估指引」，收錄於本局洗錢防制處 101 年洗錢防制工作年報，102 年 6 月。
（五）蓋華英、谷湘儀、黃文昌、曾逸凡、陳美如合著，「如何防制人頭戶之研究」，臺灣證券交易所委託研究案，2001 年 12 月。
（六）蔡宗霖，「網路交易支付大躍進：簡介中國非金融機構支付服務管理辦法」，科技法律透析，2010 年 11 月。
（七）梁建道，「數位經濟下逃漏稅洗錢態樣之分析與對策」，月旦財稅實務釋評，2020 年 3 月。

三、網路資料：

（一）中央研究院社會學研究所張硯評「階級不平等的心理學」，網址 http://twstreetcorner.org/2019/12/31changy enping。
（二）金管會 109 年 8 月 4 日「109 年 6 月份信用卡、現金卡、電子票證及電子支付機構業務資訊」，網址 http//:fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2。
（三）政府資料開放平臺，網址 http://data.gov.tw/dataset/22184，查詢日期：109 年 8 月 27 日。

第五部分

國外洗錢防制資料

FATF 報告

虛擬資產
洗錢及資恐紅旗指標

2020 年 9 月

防制洗錢金融行動工作組織（The Financial Action Task Force, FATF）是一個獨立的政府間組織，其目的在發展與推廣各項政策，以保護全球金融系統免於遭受洗錢、資助恐怖分子與資助大規模殺傷性武器擴散等活動的傷害。FATF 建議（FATF Recommendations）被視為全球防制洗錢（AML）與反資助恐怖分子（CFT）的標準。

有關 FATF 的詳細資訊，請參閱 www.fatf-gafi.org

本文件及／或內文所包含的任何地圖，皆未對任何區域之狀態或主權、國境與國界的界定以及任何區域、城市或地區之名稱有任何偏見。

文獻引用格式：

防制洗錢金融行動工作組織（2020 年），虛擬資產洗錢及資恐紅旗指標（Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets），FATF，法國巴黎，
www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

本出版品業經 FATF 秘書處授權，由法務部調查局洗錢防制處譯為中文（譯者：調查官林可凡），如內容有出入以公布於 FATF 官網 http://www.fatf-gafi.org 之英文版為準。

註：本文業經 FATF 秘書處授權法務部調查局譯為中文並載於本年報，原文請參考 http://www.fatf-gafi.org. The FATF Report “Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing” (September 2020) has been translated into Chinese under the responsibility of the Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice, Taiwan (R.O.C.) with the authorization of the FATF Secretariat. The official English version of the report is available on http://www.fatf-gafi.org.

目　錄

名詞縮寫

AEC	Anonymity enhanced cryptocurrency 高度匿名加密貨幣
CDD	Customer due diligence 客戶盡職調查
DNFBPs	Designated non-financial businesses and professions 指定之非金融事業或人員
DNS	Domain name registrars 域名註冊商
FATF	Financial Action Task Force 防制洗錢金融行動工作組織
FIs	Financial Institutions 金融機構
FIUs	Financial Intelligence Units 金融情報中心
ICO	Initial Coin Offering 首次代幣發行
KYC	Know-your-customer 瞭解你的客戶
LEAs	Law enforcement authorities 執法機構
ML	Money Laundering 洗錢
STRs	Suspicious Transaction Reports 可疑交易報告
TF	Terrorist Financing 資恐
VA/Vas	Virtual Assets 虛擬資產
VASPs	Virtual Asset Service Providers 虛擬資產服務業者

前言

1. 虛擬資產及相關服務具有刺激金融創新及效率的潛力，然而他們的特殊性質亦為洗錢犯罪者、資恐者及其他犯罪者清洗不法所得或資助犯罪活動創造了機會。快速跨境交易的特性不僅讓犯罪者得以獲取、移動和儲存數位化資產，通常是置外於受規範的金融體系，而且，易使資金的來源及去向模糊化，並增加申報實體及時辨識可疑交易的難度。這些因素使得國家機關在偵查及調查犯罪活動時形勢更險。
2. 2018 年 10 月間，FATF 更新先前的標準，釐清 FATF 標準對虛擬資產活動及虛擬服務業者的適用，以便協助司法管轄區降低與虛擬資產活動有關的洗錢及資恐風險，並保護全球金融體系的健全度。2019 年 6 月間，FATF 採用第 15 項建議的解釋性註解，進一步釐清 FATF 在虛擬資產活動及虛擬服務業者適用的規範，包含涉及有關可疑交易的申報。
3. FATF 出版此份虛擬資產洗錢及資恐紅旗指標的簡要報告，目的是協助包含金融機構、指定之非金融事業及人員與虛擬服務業者等申報實體；然而，指標是依照辨識及申報潛在涉及虛擬資產的洗錢及資恐活動來分類。本報告亦應可助於申報實體採用以風險為本的方式達成他們客戶盡職調查的要求，這包含瞭解誰是他們的客戶及最終受益人，知悉交易關係的本質及目的，及明白資金的來源。
4. 金融情報中心、執法機關及檢察官等單位會發現，本報告對涉及虛擬資產濫用的可疑交易報告分析、偵查、調查及沒收，是有用的參考文件。
5. 金融機構、指定之非金融事業及人員與虛擬服務業者的監理機關，則會發現本報告的指標在準備申報可疑交易報告及監控申報實體是否遵循防制洗錢及打擊資恐控制規範時有所幫助。檢視申報實體是否在擁有包含一項或多項指標，又無法作出合理交易解釋的已知訊息情況下，儘管客戶有前後不一致的解釋，而未能完成可疑交易的申報，或無法尋求對交易的清楚說明，權責單位會考慮將如此情況註記在申報實體的營業紀錄上。

制訂紅旗指標之方法論及資料來源

6. 本報告包含的紅旗指標是以 2017 年至 2020 年間在多個司法管轄區，超過 100 個案例研究為基礎，及「FATF 涉及虛擬資產金融調查機密報告（2019 年 6 月）」與「FATF 虛擬貨幣關鍵定義及潛在防制洗錢 / 打擊資恐風險報告（2014 年 6 月）」的發現，還有在公開領域可得的濫用虛擬資產資訊。

利用虛擬資產洗錢 / 資恐目的之趨勢

大多數有關虛擬資產的犯罪都與洗錢或其前置犯罪有關。儘管如此，犯罪者確實會利用虛擬資產躲避金融制裁及為支持恐怖主義募集資金。司法管轄區通報的犯罪態樣包含洗錢、販賣管制物品及其他非法品項（包含軍火）、詐欺、逃漏稅、電腦犯罪（例如網路攻擊導致竊取）、兒童剝削、人口販運、逃避制裁及資恐。在這些犯罪當中，最常見的濫用態樣是管制物品的非法販運。第二常見的濫用種類是有關詐欺、詐騙、勒索軟體和財務勒索。最近，專業洗錢業者已經開始開發利用虛擬資產作為他們移轉、整合和多層化不法所得的一個管道。

來源：2017 年至 2020 年間多個司法管轄區之案例研究

閱讀本報告應注意事項

7. 指標是針對虛擬資產的特性及與其有關的金融活動，並非詳盡臚列。利用虛擬資產相關的洗錢 / 資恐可疑活動，與利用法定貨幣或其他種類資產有雷同的特點。申報實體應考量來自於客戶、產品、營運及其他常規風險指標。紅旗指標在任何情境下都應予以考量。
8. 各別獨立的紅旗指標例如以下所述，可能因機關增加資訊而發展或整併，亦藉由公私協力進一步發展，在如此循環之下，演進成特定司法管轄區、客戶群體、申報實體獨特的風險及脈絡。僅憑紅旗指標的出現不必然足以作為洗錢或資恐可疑的判斷基礎，但可以促發進一步的監控及檢驗。最終而言，一個客戶可能有辦法提供對紅旗指標的合理解釋，包含在商業或經濟上的交易目的。

9. 當評估潛在可疑活動時，權責單位、金融機構、指定之非金融事業及人員與虛擬資產服務業者應該要留心某些紅旗指標在一般性交易監控中容易被看見，而其他的指標可能要在特殊交易中才易被發覺。一個或更多指標的發覺，取決於一個機構或虛擬資產服務業者提供的經營範圍、產品或服務，及業者如何與客戶互動。當一個或更多的紅旗指標出現，伴隨著鮮少或沒有合理經濟或商業目的跡象，申報實體更應展開對洗錢或資恐發生的懷疑[1]。這些指標不應成為決定是否申報可疑交易報告的唯一因素。申報實體應當在知悉、懷疑或擁有合理基礎認為洗錢 / 資恐發生時，考慮申報可疑交易報告。

紅旗指標

10. 接下來的章節透過 2017 年起 FATF 網絡來自超過 100 個案例研究、文獻回顧及公開資訊研究，建立可疑虛擬資產活動，或規避執法偵查可能企圖的一系列紅旗指標。如前所述，單一紅旗指標的存在不必然意味著犯罪活動。通常存在多項指標又無法進行合理解釋的交易，會引起存有潛在犯罪活動的懷疑。存在多項指標時，應進一步開啟適當的監控、檢視及申報。

有關交易之紅旗指標

11. 當虛擬資產仍未為大眾普遍使用時，早已經在犯罪者之間廣為流行。於數十年前，使用虛擬資產作為洗錢目的就已出現，但虛擬資產逐漸在犯罪活動中成為主流並廣泛被利用。這個章節的指標描述與常見的支付方式交易有關之傳統型紅旗指標，是如何去察覺與潛在使用虛擬資產的不法活動。

交易的規模及密度

- 分散虛擬資產交易（例如換匯或轉帳）成較小金額，或低於須作成交易紀錄或申報門檻的金額，與現金的分散交易雷同。
- 進行多項高單價交易—

[1] 許多紅旗指標同時適用於洗錢及資恐的案例，例如使用虛擬資產舉行募資活動、資助外國恐怖戰士、購買武器（例如從黑暗網路中），讀者可以閱讀 FATF 資恐偵查機密報告：相關風險指標（2016 年 6 月）（限 FATF 會員取得）。

○ 在短時間內連續交易，例如在 24 小時內；
○ 持續規律的模式，在此後卻長時間無交易紀錄，這常見於勒索軟體有關的案件；或
○ 存入一個新開立帳戶或久未交易帳戶。

● 在多個虛擬資產服務業者間快速移轉虛擬資產，尤其是透過註冊於或營運地位於其他司法管轄區的虛擬資產服務業者，而該司法管轄區—
○ 與客戶居住或商業活動沒有任何關聯；或
○ 不存在或僅有薄弱的洗錢防制 / 打擊資恐規範。

● 存入虛擬資產至交易所且通常立即—
○ 在沒有其他虛擬資產交易活動的情形下提領虛擬資產，顯為不必要的交易步驟且會引發交易手續費。
○ 變換虛擬資產為多種態樣的虛擬資產，再度引發額外的交易手續費，卻無法提供合理的交易解釋（例如：投資組合多元化）；或
○ 立即從一個虛擬資產服務業者中提領虛擬資產至私人錢包。這有效地使該交易所 / 虛擬資產服務業者成為一個洗錢攪拌器（ML Mixer）。

● 收取疑似為盜取或騙取的資金—
○ 從被辨識為持有盜取資金的虛擬資產位址，或自持有盜取資金的竊盜者相關的虛擬資產位址存入資金。

案例 1. 大量的虛擬貨幣複雜而快速地移轉至海外虛擬資產服務業者

一個當地的虛擬資產服務業者申報可疑交易報告，有關多個個人購買大量虛擬資產，隨即移轉至位於國外司法管轄區的虛擬資產服務業者。在不同的案例中，這些個人有共同的居住地址，且多數虛擬資產位址使用相同 IP 位址登入—顯示可能有職業型的洗錢者利用「錢騾」（money mules）清洗不法所得。

進一步來說，在錢騾購買虛擬資產之前，會先有一系列針對法幣資金的多層化安排。為了掩飾資金來源，首先把現金存入位於該司法管轄區不同金融機構的不同帳戶。這些資金進而移轉至註冊於該司法管轄區

實體的不同帳戶。更小額的電子支付交易會將資金轉至這些帳戶。隨後，資金移轉至另一組帳戶群後，才會轉至錢騾於當地虛擬資產服務業者持有的帳戶。在購買虛擬資產後，立即移轉至國外的虛擬資產服務業者。本案共涉及超過 150 個個人，移轉了價值約 1 億 835 萬 2,900 元美元（或 1 萬 1,960 個比特幣）的虛擬資產至兩個海外虛擬資產服務業者的多個虛擬資產帳戶。

來源：南非

案例 2. 多樣虛擬資產及複雜的移轉交易至海外虛擬資產服務業者

一個當地虛擬資產交易所申報約 4 億韓元（30 萬 1,170 歐元）的網路釣魚受害款項被盜取，最終並轉換為虛擬資產作為多層化手段。觸發申報的是多次的高價交易，移轉至位於海外虛擬資產服務業者的單一錢包。被盜取的法幣首先被轉換成三種型態的虛擬資產，然後存入嫌犯在當地虛擬資產服務業者持有的虛擬錢包。隨後嫌犯企圖隱匿資金來源，而透過 48 個位於當地不同虛擬資產服務業者的不同帳戶，進行了另外 55 次的資金移轉，最終移轉至位於海外的另一個虛擬資產錢包。

來源：南韓

有關交易態樣之紅旗指標

12. 如上，下列的紅旗指標描述虛擬貨幣被濫用作為洗錢 / 資恐目的，可以如何透過非常規、異常或極端的交易態樣來進行識別。

與新使用者相關的交易

- 以初次大額存入開啟與虛擬資產服務業者的新關係，然而資金金額與客戶身分顯不相當。
- 以初次大額存入開啟與虛擬資產服務業者的新關係，並在開戶首日存入所有資金，此後客戶在同日或隔日開始將全數或大部分的資金進行交易，或客戶在隔日提領所有的款項。大多數虛擬資產有存入的交易限制，大額洗錢亦可透過「場外交易」[2] 進行。
- 新使用者企圖交易所有虛擬資產的結餘，或提領虛擬資產並企圖轉出平臺中所有結餘。

[2] 場外交易指證券在非正式交易所名單上的公司，並透過仲介業者網絡進行的交易。

案例 3. 與客戶身分不相符之初次存入

以下可疑指標的出現促使金融機構（銀行）申報可疑交易報告給權責機關，並引發有關洗錢的調查：

- 交易內容與帳戶持有者身分不相符—在一個年輕人帳戶開戶首兩日，帳戶以商業名義收受多個合法個人的大額存入。
- 交易態樣—存入之款項立即（在同一天）移轉至不同的虛擬資產服務業者，用以購買虛擬資產（比特幣）。
- 客戶身分資料—銀行發現其中一個訂購方是詐欺案件的嫌犯。銀行也提供使用網路銀行的 IP 位址給權責機關。

在調查中發現，帳戶持有人是由犯罪者在社群平臺招募的錢騾，用來協助收受聲稱為販售網路商品所得的款項。然而，這些款項被發現是由其他受害公司存入，並非販售商品的所得。存入的款項立即從個人銀行帳戶，以拆分交易方式，被移轉至另一個由捷克某股份公司持有之帳戶，然後轉換為虛擬資產（比特幣）存於當地多個虛擬資產服務業者。這些虛擬資產隨後立即自帳戶中被提領。除了申報可疑交易報告，銀行也暫停該可疑交易，有助於接下來對資金的查扣。

當地的虛擬資產服務業者也發現收受資金的非常規性，並提供有用的資訊以協助調查。這些資訊包含：虛擬資產購買的情況、交易及其他客戶盡職調查資訊如錢包位址、遭濫用來進行購買的身分文件影本、宣稱購買的買家名字。這使得權責機關可以向銀行請求進一步的資訊（例如交易明細）。

來源：捷克

與所有使用者相關的交易

- 涵蓋多樣虛擬資產或多個帳戶的交易，且未有合理交易說明。
- 在特定時間區間頻繁（例如一天、一周、一個月）與同一虛擬資產帳戶交易—
  - 由多人交易；
  - 由一個或多個人從同一個 IP 位址；或
  - 涉及龐大金額。

- 從大量不相關錢包存入相對小額（資金積累）之交易，隨即移轉至其他錢包或全數換為法幣。這些相關帳戶交易在最初可能使用虛擬資產而非法幣。
- 即使有虛擬資產及法幣間轉換的潛在損失（例如虛擬資產價值的波動，或無視與同業相比異常高額的委託費用，尤其當交易沒有合理的說明）。
- 轉換大量的法幣為虛擬資產，或轉換單一虛擬資產為多種虛擬資產，且沒有合理的交易說明。

案例 4. 交易期間具有週期性

一間當地金融機構（證券商）申報可疑交易報告，有關仲介及外國人士間虛擬資產帳戶的未授權支付交易。證券商決定要申報交易活動，因該外國人意圖進行總額 480 萬美元的交易（於同日拆為相差 6 分鐘的兩筆交易），隔日並向仲介申請一個交易帳戶。該錢包並非位於開曼群島。這份可疑交易報告成功地與國外多個金融情報中心情資交換，並讓位於國外的線上平臺能在犯罪完成前將嫌犯的帳戶凍結，使大部分受害資金得以返還。

來源：開曼群島

有關匿名之紅旗指標

13. 本節的指標描繪有關虛擬資產技術面固有的特性及缺點，下列不同的技術特點提升了匿名性及增加執法機關偵查犯罪活動的困難。這些因素使虛擬資產吸引犯罪者用來隱匿或藏匿他們的資金。然而，僅憑這些特點的出現，不能自動認定是一個非法交易。舉例而言，使用硬碟或紙錢包可能是為了防止遭竊的合法方式。再次強調，出現這些指標應該要併同考量其他有關客戶、關係或合理交易解釋等內涵。
    - 一名客戶交易超過一種型態的虛擬資產，忽視額外的交易手續費，尤其是那些提供高度匿名性的虛擬資產，例如高匿名加密貨幣或私人貨幣。
    - 將公開運作、具透明性區塊鏈的虛擬資產，例如比特幣，移轉至中

心化交換所，隨即換購為高度匿名加密貨幣或私人貨幣。

- 客戶在點對點（P2P）交易網站，以未註冊 / 沒有執照的方式經營虛擬資產服務業，尤其當客戶以自己客戶的名義，掌握大量虛擬資產的轉移，並向自己的客戶收取較其他交易所更高的傳輸服務費用。使用銀行帳戶協助這些點對點的交易。
- 在交易所透過與平臺相關的點對點錢包，將虛擬資產轉換為現金的異常交易活動（程度及數量），且沒有合理的交易解釋。
- 將虛擬資產從錢包轉入或轉出，而這些錢包與經營混和服務、加密貨幣混幣器或點對點平臺的虛擬資產服務業者曾有模式化的交易活動。
- 使用混和服務及加密貨幣混幣器的交易，顯示出企圖在已知錢包地址及暗網市場之 間，隱匿不法資金流向。
- 資金從虛擬資產地址或錢包中存入或取出，直接或間接暴露與已知可疑來源的連結，包含暗網市場、混和服務 / 加密貨幣混幣器、有疑慮的賭博網站、非法活動（例如勒索軟體）及 / 或竊盜通報。
- 利用去中心化 / 非託管的硬錢包或紙錢包進行跨境虛擬資產交易。
- 使用者透過代理伺服器註冊網域名稱，或使用隱藏或編造域名的域名註冊商，進入虛擬資產服務業者平臺。
- 使用者利用與暗網或其他同樣允許匿名通訊，包含加密郵件或虛擬個人網路的軟體有關之 IP 位址，進入虛擬資產服務業者平臺。
- 大量看似不相關的虛擬資產錢包，由同一 IP 位址（或 MAC 位址，即媒體存取控制位址）控制，可能涉及利用不同使用者註冊空殼錢包，以掩蓋彼此之間的關聯性。
- 所使用的虛擬貨幣，其設計未含適當地把交易做成紀錄，或與可能的詐欺犯罪及其他意在施行如龐式騙局的詐欺計畫相關。
- 從那些客戶盡職調查或瞭解你的客戶程序有明顯缺陷或沒有這些程序的虛擬貨幣服務業者收取或存入資金。
- 使用虛擬貨幣 ATMs/kiosks—
  - ○ 即使有較高的交易手續費用，仍經常被錢騾或詐騙被害者使用；或
  - ○ 位於高風險地點，即犯罪活動發生率高的地方。

單獨使用 ATMs/kiosks 並不構成紅旗指標，但若伴隨機檯位於高風險地區，或使用重複的小額交易（或其他額外的因素）則可能構成。

案例 5. 使用與暗網市場有關的 IP 位址— Alpha Bay

AlphaBay 是當局在 2017 年瓦解的最大暗網犯罪市場，該市場被數十萬人用來購買及販賣毒品、贓物及詐欺身分文件、存取裝置、假冒商品、惡意軟體及其他電腦駭客工具、軍火和有毒化學物，持續兩年之久。該網站營運於洋蔥路由器（TOR）中的隱藏伺服器，以掩蓋其原本的伺服器地點，以及管理者、版主和使用者身分。AlphaBay 賣家使用許多不同型態的虛擬資產，擁有約 20 萬個用戶、4 萬名賣家、25 萬筆商品目錄及在 2015 至 2017 年間超過 10 億美元的虛擬資產交易。

2017 年 7 月間，美國政府在外國對應機構的協助下，將 AlphaBay 市場的伺服器瓦解，逮捕了管理者，並根據加州東區法院核發的扣押許可，查扣了市場本身及 AlphaBay 犯罪集團不法所得的實體及虛擬資產。聯邦幹員在追查了來自 AlphaBay 虛擬資產移轉至涉嫌的管理者控制的其他虛擬資產帳戶、可識別的銀行帳戶和其他實體資產後，獲得扣押許可查扣這些不法所得。

來源：美國

案例 6. 使用混和及加密貨幣混幣器— Helix

Helix 是一個暗網的虛擬資產服務業者，提供混和服務及加密貨幣混幣器，收取費用協助客戶隱匿虛擬資產的來源和持有者，營運超過三年期間。Helix 涉嫌移轉超過 35 萬枚比特幣，時價超過 3 億美元。營運者特別宣傳暗網交易可以躲避執法查緝的服務。在 2020 年 2 月，針對營運 Helix 的個人刑事起訴罪名包含洗錢共謀和經營非法資金通匯業務。

Helix 與暗網市場 AlphaBay 共同合作，直到 AlphaBay 在 2017 年遭執法單位查扣。

來源：美國

案例 7. 使用去中心化錢包

此案例展示犯罪者如何使用去中心化錢包，使自非法販毒活動所得的不法資金來源模糊化。此案例中，犯罪者透過網路經營大量的毒品販賣，除利用法幣之外，亦利用虛擬資產（比特幣、EX-codes 及 EXMO-cheques）型態支付費用。

以法幣型態所收取的不法資金被轉換成虛擬資產，交易係由位於線上區塊鏈交易平臺的匿名帳戶協助進行。以虛擬資產形態存在的這些資金，透過交易商再被轉換回法幣後，轉回犯罪者銀行簽帳卡帳戶。而那些以虛擬資產型態所收取的不法資金，首先被移轉到與犯罪者有關的去中心化比特幣錢包，隨後進一步移轉到其他的比特幣錢包及不同的交易所。這增加了追蹤資金的困難度。同樣的，清洗過的資金（虛擬資產型態）接著被轉換為法幣，然後再存入犯罪者的銀行簽帳卡帳戶。犯罪者在審判後遭判決 7 年有期徒刑及罰金。

來源：俄羅斯聯邦

有關匯款者與收款者之紅旗指標

14. 本節指標與從事非法交易的匯款者和收款者身分背景及不尋常行為有關。

帳戶開戶期間察覺不法

- 利用不同的名字分別開立帳戶，來規避虛擬資產服務業者對交易或提領的限制。
- 源自不可信任的 IP 位址、被制裁的司法管轄區 IP 位址、或先前被警示為可疑的 IP 位址之交易。
- 頻繁企圖在同一個虛擬資產服務業者以相同的 IP 位址開立帳戶。
- 有關商業 / 公司用戶，他們的網域註冊在與他們設立地點不同的司法管轄區，或在網域註冊程序較不嚴謹的司法管轄區。

客戶盡職審查期間察覺不法

- 客戶提供不完整或無效的「瞭解你的客戶（KYC）」資訊，或拒絕回答「瞭解你的客戶（KYC）」相關問題或對資金來源的詢問。
- 匯款人 / 收款人對於交易、資金來源或與交易對象的關係缺乏瞭解或提供錯誤的資訊。
- 客戶在開戶引導程序中，提供偽造文件或編輯過的照片及 / 或身分文件。

案例 8. 客戶拒絕提供資金來源資訊

一間金融機構（銀行）申報一份可疑交易報告，有關一家以販賣商品（在此例中為生物塑料）優惠券營利的當地公司之銀行帳戶。資金由自然人及法人存入，有些來源為虛擬資產。即使銀行進一步詢問，帳戶代表人並未提供有關資金來源的資訊。權責機關接續的分析指出，由該公司轉出的資金與組織犯罪和詐騙計畫取得的款項有關聯性。

來源：義大利

身分背景

- 客戶提供的身分證明或帳戶憑證（例如：一個非標準 IP 位址或 flash cookies）與另一個帳戶相同。
- 與客戶身分資料相關的 IP 位址和操作交易的 IP 位址有不相符現象。
- 客戶的虛擬資產位址出現在公開平臺顯示與非法活動相關。
- 客戶在執法機關可公開取得的資訊中顯示與先前犯罪活動相關。

案例 9. 客戶身分背景與常態性高價虛擬資產交易不相符

一個虛擬資產服務業者（交易者）和一個金融機構（付款機構）申報可疑交易報告予金融情報中心，有關在交易所甫開戶即有高價虛擬資產交易。精確來說，帳戶持有者進行了超過 18 萬歐元，針對不同虛擬資產的購買及販售交易，與帳戶持有者的身分背景不相符（包含職業與薪資）。

分析後發現虛擬資產後續被使用在（1）暗網市場中的交易；（2）線上博弈；（3）透過沒有適當防制洗錢 / 打擊資恐控制，或曾涉及數百萬元洗錢調查案的虛擬資產服務業者交易；（4）透過提供點對點交易的平臺操作虛擬資產；及（5）「混幣」。帳戶持有者也利用多種不同的管道（例如：匯款、網路銀行、預付卡）在相同的時段將固定金額的資金轉出其帳戶。帳戶持有者收受的資金似乎來自一個個人組成的網絡，這些人透過匯款或銀行體系，以現金購買虛擬資產（比特幣），且位於亞洲及歐洲（包含義大利）多個不同的司法管轄區。他也透過預付卡收到來自非洲及中東人士的資金，這些人輪流向住在義大利和海外的同籍公民收集資金。這些資金接著用於跨境移轉及線上博弈，及從義大利的 ATM 提領現金。

來源：義大利

潛在的錢騾及詐騙受害者身分背景

- 匯款者顯然對虛擬資產技術和線上錢包保管方式不熟悉。這樣的個人可能是專業洗錢者所招募的錢騾，或是詐騙受害者，因受騙而在不瞭解資金來源情況下，成為移轉不法資金的錢騾。
- 年紀明顯大於平臺使用者平均年齡的客戶，開立帳戶並進行大量的交易，可能是潛在的虛擬資產錢騾或剝削長者財務的受害人。
- 財務弱勢的客戶經常被販毒者利用來協助販毒生意。
- 客戶購買大量的虛擬資產，而無法證明有充餘的財富或與他 / 她過去的財務背景相符，可能顯示其為洗錢行為、錢騾或詐騙受害者。

案例 10. 詐騙受害者成為錢騾

在這些投資詐欺案中，外籍人士以電話、電子郵件或透過社交平臺，直接聯繫通常為退休人士或長者，並提供他們投資比特幣或其他虛擬資產的機會，同時保證因為虛擬資產越來越普遍流行及價格上漲，能從中獲得龐大利益。首次投資為小額投資（多數案例不超過250歐元），從受害者的銀行帳戶、信用卡或透過其他方式，轉至多種支付服務，最終到犯罪者手中。或者，受害者被指示將法幣透過虛擬資產 ATM 兌換為比特幣，並將資金轉到犯罪者指定的地址。

受害者在技術上並不熟悉，且通常對虛擬資產科技或他們實際上投資的標的不瞭解。犯罪者也要求受害者在他們的裝置上安裝一個遠端桌面應用程式，以便犯罪者可以協助正確地轉出資金至特定帳戶。如此洩露了受害者的裝置，讓犯罪者可以在受害者未察覺的情況下，進行未經授權的資金移轉，直到受害者發現帳戶裡的資金不見了。在一些案例中，犯罪者甚至偽造文宣宣稱名人或富豪或新聞播報員在推銷虛擬資產投資，據此取得受害者的信任及型塑「投資」的正當性。

來源：芬蘭

其他不尋常行為

- 客戶經常更改身分資訊，包含電子郵件地址、IP 位址或金融資訊，這也可能是帳戶被其他人接管的表徵。
- 客戶在一天內密集嘗試從不同的 IP 位址，進入一個或多個虛擬資產

服務業者。

- 在虛擬資產訊息欄位使用的語言，顯示交易被用於支持非法活動或用於購買非法商品，例如毒品或竊取的信用卡資訊。
- 客戶重複地和同一群體進行有顯著獲利或虧損的交易。這顯示帳戶可能被接管，及試圖透過交易從受害者帳戶騙取款項，或透過虛擬資產服務業者進行洗錢行為以模糊金流。

有關資金或財產來源之紅旗指標

15. 從多個司法管轄區提供的案例顯示，虛擬資產的濫用通常與犯罪活動相關，例如非法麻醉藥物及治療精神疾病藥物的販運、詐欺、偷竊及勒索（包含網路犯罪）。以下是與這些犯罪活動資金或財產來源有關常見的紅旗指標：
    - 使用已知與詐欺、勒索或勒索軟體、制裁位址、暗網市場或其他非法網站有關聯的虛擬資產位址或銀行金融卡交易。
    - 源自或用於線上博奕服務的虛擬資產交易。
    - 使用一張或多張信用卡或金融卡，並可連結至一個虛擬資產錢包領取大額法幣（網路貨幣到塑膠貨幣），或用來購買虛擬資產的款項源自現金存款至信用卡。
    - 存入明顯高於平常的金額到一個帳戶或虛擬資產位址，且資金來源不明，接著轉換成法幣，可能暗示資金為竊取而來。
    - 對於資金來源和持有者缺乏透明度或資訊不足，例如資金涉及使用空殼公司或將資金放在首次代幣發行（ICO），因而無法取得投資者的個人資料，或轉入交易是透過信用 / 預付卡網路付款系統，隨即提領資金。
    - 客戶的資金直接源自第三方混幣服務或錢包混幣器。
    - 整批客戶的財產來源為投資虛擬資產、首次代幣發行或首次代幣發行詐騙等。
    - 客戶的財產來源不成比例地源自虛擬資產，而這些虛擬資產來自其他缺乏防制洗錢 / 打擊資恐控制的虛擬資產服務業者。

例 11. 利用空殼公司— 深點網（Deep Dot Web）

在 2019 年 5 月，美國執法單位根據法院命令查封了一個網站：深點網（DeepDotWeb, DDW）。涉嫌的 DDW 負責人和營運者被指控涉及數百萬美元向 DDW 暗網市場使用者收取佣金的共謀洗錢罪。透過提供指定的連結，涉嫌的 DDW 負責人和營運者從使用 DDW 網站暗網市場買賣不法商品（例如芬太尼和海洛因）的個人，收取手續費或代理佣金。這些佣金支付是透過虛擬資產，並存入 DDW 掌控的比特幣錢包。為了隱匿和掩飾總額超過 1,500 萬美元的非法所得來源及本質，負責人及營運者從他們 DDW 比特幣錢包，移轉非法佣金至其他比特幣錢包，同時也轉至由他們控制的空殼公司名下銀行帳戶。這些被告利用這些空殼公司移轉他們非法取得的獲利並進行其他有關 DDW 的活動。在 5 年的期間，該網站約收取了 8,155 個比特幣作為暗網市場的佣金支付，推算當時交易的比特幣價格，價值約 800 萬美元。在一系列超過 4 萬次的存入交易，比特幣被移轉至被告掌控的 DDW 比特幣錢包，隨即以超過 2,700 次的提領交易至不同的目的地。以 DDW 比特幣錢包提領交易當時的比特幣價格計算，比特幣價值約相當於 1,500 萬美元。

來源：美國

案例 12. 利用多個虛擬資產交易所，偽造的身份文件應付客戶盡職審查及預付卡

此案的被告涉及一宗洗錢犯罪，有關於網路犯罪者駭進一間虛擬資產交易所並偷走價值 2 億 5,000 萬美元的虛擬資產。兩名被告涉嫌清洗所偷取價值 9,100 萬美元的虛擬資產，及清洗另一網路竊賊偷取的 950 萬美元。遭偷取的虛擬資產經過了多個虛擬資產交易所的上百次虛擬資產自動交易。在某些案例，洗錢者使用竄改過的照片及偽造的身份文件，來規避虛擬資產交易所的瞭解你的客戶程序。約 3,500 萬美元的非法資金最終被移轉到國外銀行帳戶，也被用來購買預付卡，這些預付卡可以被轉換成虛擬資產。被告們操作獨立的或連結的帳戶，並為客戶提供虛擬資產轉換服務以收取費用，例如轉換虛擬資產為法幣。被告們也在美國境內經營事業體，但均未在金融犯罪執法局（FinCEN）註冊。

來源：美國

有關地緣風險之紅旗指標

16. 此節的指標強調犯罪者如何利用司法管轄區在施行 FATF 針對虛擬資產及虛擬資產服務業者建議的不同階段，移轉他們的不法資金[3]。根據司法管轄區所提供的案例，犯罪者利用不同地區針對虛擬資產及虛擬資產服務業者的防制洗錢 / 打擊資恐制度落差，將不法資金移轉到位於或營運於某些司法管轄區的虛擬資產服務業者，而這些司法管轄區對虛擬資產及虛擬資產服務業者不存在或僅有低程度防制洗錢 / 打擊資恐規範。這些司法管轄區可能缺乏註冊 / 執照制度，或沒有將虛擬資產及虛擬資產服務業者納入申報可疑交易報告義務實體，或尚未引進 FATF 建議要求的全套預防措施。這篇報告並非企圖列出「高風險」司法管轄區，但鼓勵申報實體在考量地緣風險時將下列指標納入參考。這些風險是關於資金來源、去向及交易轉運的司法管轄區。這些指標亦是關於交易發起者及資金受益人可能連結至某個高風險司法管轄區的風險。進一步來說，指標可以適用於客戶的國籍、居住地或交易活動地點。

- 客戶的資金來源或去向是一個未於司法管轄區註冊的交易所，不管這個司法管轄區是客戶所在地或交易所所在地。
- 客戶利用一個虛擬資產交易所或位於國外的金錢或價值移轉服務，而且位於針對虛擬資產業者缺乏或已知不充足的防制洗錢 / 打擊資恐規範，包含客戶盡職調查或瞭解你的客戶措施不足的高風險司法管轄區。
- 客戶轉出資金至虛擬資產服務業者，而業者營運於沒有虛擬資產規範或沒有實施防制洗錢 / 打擊資恐控制的司法管轄區。
- 客戶設立辦公室或將辦公室移至針對虛擬資產未有規範或尚未實施規範的司法管轄區，或於未有清楚商業關係的司法管轄區設立新的辦公室。

[3] 在 2020 年 7 月，FATF 出 版 12-Month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers.，該報告第二章涵蓋自 2019 年 6 月起修正建議的施行進展。

案例 13. 比特幣商經營未有執照的資金匯兌事業（跨境性質）

2019 年 4 月，被告因經營未有執照的資金匯兌事業，並販售數十萬美元價值的虛擬資產（比特幣）給超過一千名在美國的客戶，遭判 2 年有期徒刑。被告也被沒收 82 萬 3,357 美元的獲利。

被告在其網站上向虛擬資產使用者廣告他的服務，與一些客戶見面收取現金換為虛擬資產。其他客戶透過全國的 ATM 或資金交易服務支付給他。被告對所提供的服務收取現行交易利率百分之 5 的佣金。他首先透過一個美國交易所獲得比特幣，假如他的行為引發懷疑導致其帳戶關閉，則被告會移轉到一個位於亞洲的交易所。被告在 2015 年 3 月至 2017 年 4 月間，透過上百個分別的交易，利用這個交易所購買了 329 萬美元的比特幣。這個被告也承認其在美國境外，與貴金屬交易商兌換美元現金，而在 2016 年底到 2018 年初之間，他和其他人每次以略低於 1 萬美元的申報金額，總共攜帶超過 100 萬美元入境美國。

來源：美國

虛擬資產服務業者遷移其營運地點至防制洗錢 / 打擊資恐規範較不完善的司法管轄區

在位於亞洲的司法管轄區 A 於 2017 年施行禁止虛擬資產服務業者政策前夕，一個設立於司法管轄區 A 的虛擬資產服務業者（交易所），移轉其營運地點至在同一地區的司法管轄區 B。在 2018 年，司法管轄區 B 在幾個主要虛擬資產服務業者（交易所）的重大駭客事件後，提升了針對虛擬資產的防制洗錢 / 打擊資恐法律規範。在 2018 年 3 月，該虛擬資產服務業者宣布轉移總部至位於歐洲的司法管轄區 C 的企圖（一個當時尚未引入完整有關虛擬資產及虛擬資產服務業者防制洗錢 / 打擊資恐法規的司法管轄區）。稍後於 2018 年 11 月，司法管轄區 C 引入某些對虛擬資產服務業者的規範，在 2020 年 2 月，該虛擬資產服務業者確認沒有被授權營運。2020 年的近期報告指出，該虛擬資產服務業者已經轉移其註冊及設籍狀態至位於非洲的司法管轄區 D。

來源：公開領域

結論

17. 此報告來自 FATF 全球會員網絡的大量資料，尋求為公部門及私部門提供一個實務性的工具，用以識別、察覺及最終防範涉及虛擬資產的犯罪、洗錢及資恐活動。

18. 此報告包含的指標特別針對虛擬資產固有的特徵及脆弱性。指標並非在任何情況下都詳盡及適用。這些指標通常只是對更全面性潛在洗錢或資恐風險描繪的眾多元素之一，重要的是這些指標 (或任一指標) 不應被獨立看待，而應該放在相關權責機關獲得資訊的整體脈絡中考慮。

19. 透過公私部門常態性及動態發展的雙向對話，實施以風險為本途徑，無疑會增加此報告的有效性。權責機關因此被鼓勵將此報告分送給申報實體，並與他們進行交流及舉辦研討提高意識，促進對此報告的瞭解。

20. 雖然這些可辨的指標仍在持續演進，他們在國內執法單位及公部門資訊整體脈絡下能獲得最好使用。權責機關可能亦會提供私部門在該司法管轄區最相關的指標及資訊。例如，用此報告中的資訊來準備自己對相關申報實體的建議。然而，此報告不應該被刻意利用於遵循及檢查目的之管理工具，或作為監理私部門機構時的清單，因為並非所有的指標都適用於所有的司法管轄區或機構。

參考文獻

FATF (June 2014), FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks

FATF (June 2019), FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

FATF (June 2020), 12-month Review of Revised FATF Standards – Virtual Assets and VASPs

限 FATF 會員取得之報告

FATF (June 2016), Confidential FATF Report on Detecting Terrorist Financing: Relevant Risk Indicators

FATF (June 2019), Confidential FATF Report on Financial Investigations Involving Virtual Assets

FATF

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

貿易型洗錢

趨勢與發展

2020 年 12 月

防制洗錢金融行動工作組織（The Financial Action Task Force，FATF）是一個獨立的政府間組織，其目的在發展與推廣各項政策，以保護全球金融系統免於遭受洗錢、資助恐怖分子與資助大規模殺傷性武器擴散等活動的傷害。FATF 建議（FATF Recommendations）被視為全球防制洗錢（AML）與反資助恐怖分子（CFT）的標準。

有關 FATF 的詳細資訊，請參閱 **www.fatf-gafi.org**

本文件及／或內文所包含的任何地圖，皆未對任何區域之狀態或主權、國境與國界的界定以及任何區域、城市或地區之名稱有任何偏見。

艾格蒙聯盟（Egmont Group）成立宗旨在為全球各地金融情報中心（FIU）提供一個平台，藉以改善各方在打擊洗錢與資助恐怖主義等方面的合作狀況，並促進此領域在各國國內計畫之實施。

有關艾格蒙聯盟的詳細資訊，請參閱下列網站：**www.egmontgroup.org**

文獻引用格式：

防制洗錢金融行動工作組織－艾格蒙聯盟（2020 年），貿易型洗錢：趨勢與發展（Trade-based Money Laundering: Trends and Developments），FATF，法國巴　黎，www.fatf-gafi.org/publications/methodandtrends/documents/trade-based-money-laundering-trends-anddevelopments.html

本出版品業經 FATF 秘書處授權，由法務部調查局洗錢防制處譯為中文，如內容有出入以公布於 FATF 官網 http://www.fatf-gafi.org 之英文版為準。

註：本文業經 FATF 秘書處授權法務部調查局譯為中文並載於本年報，原文請參考 http://www.fatf-gafi.org. The FATF Report “Trade-based Money Laundering: Trends and Developments” (December 2020) has been translated into Chinese under the responsibility of the Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice, Taiwan (R.O.C.) with the authorization of the FATF Secretariat. The official English version of the report is available on http://www.fatf-gafi.org.

目　錄

名詞縮寫

ACIP	防制洗錢暨打擊資助恐怖主義產業合作夥伴（Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership）
AML/CFT	防制洗錢／打擊資助恐怖主義
APG	亞太防制洗錢組織（Asia Pacific Group on Money Laundering）
BMPE	披索黑市交易（Black Market Peso Exchange）
DNFBP	指定之非金融事業與人員（Designated Non-financial Businesses and Professions）
FATF	防制洗錢金融行動工作組織（Financial Action Taskforce）
FI	金融機構（Financial Institution）
FIU	金融情報中心（Financial Intelligence Unit）
FSRB	區域性防制洗錢組織（FATF-Style Regional Body）
LEA	執法機關（Law Enforcement Authorities）
ML	洗錢（Money Laundering）
MVTS	金錢或價值移轉服務（Money Value Transfer Service）
NRA	國家風險評估（National Risk Assessment）
OCG	組織性犯罪集團（Organised Criminal Groups）
PPP	公私協力夥伴關係（Public Private Partnership）
PML	專業洗錢人員（Professional Money Launderers）
SBML	服務型洗錢（Services-based Money Laundering）
STR	可疑交易報告（Suspicious Transaction Reports）
TBML	貿易型洗錢（Trade-based Money Laundering）
TBML/TF	貿易型洗錢與資助恐怖分子（Trade-based Money Laundering and Terrorist Financing）
TBTF	貿易型資助恐怖分子（Trade-based Terrorist Financing）
TF	資助恐怖分子（Terrorist Financing）

報告摘要

本報告為「防制洗錢金融行動工作組織（FATF）」與「區域性防制洗錢組織（FSRB）」先前就貿易型洗錢（TBML）所發布文件的系列報告，例如「亞太防制洗錢組織（APG）」所發布的「2006 年度指標研究」、「2008 年度最佳實務報告」以及「2012 年度報告」。

本報告補足了前述原始出版刊物所提供的深入見解，且另外加入艾格蒙聯盟、全國性暨國際性私人機構以及各個多邊機構所提供的寶貴見解。本報告以公部門與私人部門的深入見解為基礎，進行了一項完整的研究，其中概述了 TBML 依然存在重大洗錢（ML）風險的程度，並觀察到既有、已成熟的 TBML 技術之整合趨勢，以及非法現金整合（illicit cash integration）方面的各項新發展[1]。本報告亦說明了貿易資助恐怖分子（TBTF）的風險，以讓讀者認識並瞭解恐怖分子資助者運用貿易流程的方式。

報告中也反映了自 APG 報告發布日之後的進展，包括宣傳有關其風險分析、評估與降低風險等實務執行措施的重要發現。雖然報告認為，要對 TBML 成功提起刑事控告仍面臨許多重大挑戰，但同時也指出各項行動、工具與能力的發展狀況，有助於改善對 TBML 犯罪的調查與瓦解。其中包括先進的 IT 與風險評估系統，以及公私部門之間更深入且更系統化的合作。

本報告係以供廣泛讀者閱讀之目的而撰寫，對象包括負責辨識、調查或起訴 TBML ／ TF 的各權責機關；金融機構（FIs）；可能面臨 TBML ／ TF 濫用或發現相關議題卻不瞭解其真正代表意義等風險的指定非金融事業與人員（DNFBPs）；以及涉及區域或全球供應鏈的其他各方，例如持有相關且具意義的貿易或融資資料之貨運承攬商與報關業者。

若能提升各界對貿易流程各個面向的認知，將可能提高發現及成功瓦解貿易型洗錢與貿易型資助恐怖分子等行為的機會。

[1] 若以最簡單的方式來說明，貿易涉及了將商品或服務從一人或實體移轉至另一人或另一實體。貿易的條款，例如商品或服務的數量與價值、運輸方法、帳單結算方式、帳單結算人與時間，會隨實體的不同而有差異。本報告所示例子僅為非常基本的複雜交易釋例。

重要發現

無論是其本質或涉及的事務，貿易活動可以是相當複雜的，其反映了全球各地供應鏈互相連結的性質。組織性犯罪集團（Organised Criminal Group，OCG）、專業洗錢人員（Professional Money Launderer，PML）以及資助恐怖分子（TF）的網絡會運用貿易的複雜本質，建構無數種金融流程，包括犯罪所得的洗錢，例如販毒所得、資助恐怖主義，以及規避制裁。

本報告的各資料提供方都指出，2006 年 FATF 研究中所提到的 TBML 技巧[2] 洗錢情況仍持續存在。儘管全球貿易型態改變、新市場有所成長，這些技巧因具有高度彈性與調整空間，仍持續被運用在洗錢目的上。若進口商與出口商間存在共謀關係，這些技巧尤其有效，他們會積極的對貿易或相關帳單結算流程進行虛偽陳述。

因此，權責機關若能夠瓦解這些共謀行為，就能帶來更大的影響，包括透過刑事起訴或其他形式的瓦解，例如撤銷其貿易許可。

此外，運用貿易融資流程，是提供資料的私部門方最常注意到的洗錢型態。APG **報告提倡公部門機構深化對這些流程之瞭解的重要性，以補足其對於** TBML **相關前置犯罪**（predicate offence）**行為的既有瞭解。這點仍是本報告的重要發現，因為若能提升各界對貿易流程各個面向的認知，包括各種不同融資流程的管理方式，將可能提高發現與成功瓦解** TBML ／ TF **等行為的機會。**

本報告盤點了現有的 TBML 風險，包括運用全新或既有的方法，將非法現金納入金融系統。儘管以科技輔助的付款方式有所成長，多項案例研究都顯示犯罪者運用了「披索黑市交易（BMPE）」。報告中亦指出其他非法現金整合形式，例如運用代購[3] 或滲透至合法的供應鏈[4]。

TBML 或 TBTF 犯罪與空殼公司或掛名公司之間可能會有許多往來，

[2] 這類技巧最先是在 2006 年度 FATF 初步報告中被提到，其中包括低報或高報商品價格、低估或高估商品價值，以及／或虛擬交貨，亦即無任何商品移動。

[3] 富裕人士可能因為嚴格的匯率管制措施，而遭受購買較高價值商品的限制，此時就可由代購者代表富裕人士進行購買。其中有一個例子稱為 Daigou（即代購的中文發音），意指由位於亞洲國家以外的個人或出口商聯合組織，替該亞洲國家的顧客購買商品（主要為奢侈品）。

[4] 此滲透行為不必然會導致後續常見 TBML 技巧的成長。在某些情況下，除了非法現金納入進口公司現金流外，該貿易關係並無任何改變。這點及代購的運用，將於本報告「TBML 風險與趨勢」章節詳細說明。

不過，該等公司不必然會出現在所有 TBML ／ TF 犯罪之中。運用這些公司，不但能夠協助整合資金，還具有隱匿實質受益人的優點。

報告中提到了持續運用第三方中介機構的情況，且通常是在金融結算流程中發現。這些與組織性犯罪集團、專業洗錢人員或恐怖分子資助者有所關聯的第三方中介機構能夠快速的整合至交易鏈，因而能進一步在其活動與 TBML 或 TBTF 犯罪之間創造斷點。

金融機構雖已知道與第三方中介機構有關的風險，報告也認知，供應鏈中的其他方（例如合法進口商或出口商）或負擔監督責任的他方（例如稽核人員或會計師），可能不會質疑完全無關的第三方為何會涉及款項結算流程。

所有資料提供方都指出，在識別與打擊 TBML ／ TF 的例行性作業當中，仍須面臨許多挑戰。2006 年研究所發現的議題以及在 2012 年進一步追蹤的各項問題，目前依然存在。舉例來說，在進行國內與跨國系統性與一致性合作方面所面臨的挑戰，就可能對 TBML 與 TBTF 犯罪的發現與瓦解行動帶來不利影響。

相關貿易資料會由多個利害關係人持有，該等資料的分析範圍必須遵守相關限制規定，包括作業面與大量提供的方面。報告所指出的各項全新挑戰，包括網路業務的成長、主動遵循活動的範圍限制，以及新技術與貿易流程的數位化，都加快了貿易作業的速度。

同時，報告也指出，幾項新行動以及其他行動持續邁入成熟階段，其目的在於因應這些挑戰，以及提高各貿易體系辨識並因應 TBML 與 TBTF 的能力。舉例來說，有許多國家都制定了公私協力夥伴關係（PPP）的方案，由公部門與私部門利害關係人合作，互相分享重要金融犯罪風險的知識與專業，包括 TBML。部分國際組織也採用此方法與私部門實體合作。

過去這段期間以來，貿易相關活動的全面性研究呈現出成長趨勢[5]，且各權責機關也採用了全新型態的雙邊與多邊情報分享及調查行動[6]，希望能夠藉此瓦解 TBML ／ TF。報告反映了這些行動的趨勢，以及其他打

[5] 例如，沃爾夫斯堡集團（Wolfsberg Group）、國際商會（International Chamber of Commerce）以及金融與貿易銀行家協會（Bankers Association for Finance and Trade，BAFT），已各自及透過合作，針對貿易型洗錢編製了多份深入研究指南，例如 2019 年度貿易融資原則（2019 Trade Finance Principles）報告與各附錄。

[6] 例如，美國、加拿大、荷蘭、澳洲及英國等五國的稅捐主管機關在 2018 年成立了「全球稅務執法聯合組織（Joint Chiefs of Global Tax Investigation，J5）」，以調查從事跨國稅務犯罪與洗錢活動的人員。逃稅被視為是與 TBML 有關的前置犯罪。

擊 TBML／TF 最佳實務的釋例。

從策略面來看，FATF 在 2012 年對[7]**AML／CFT 導入風險基礎方法，可視為是 FATF 準則近幾年來最主要的改變。該方法鼓勵各司法管轄區針對其承擔的洗錢／資助恐怖分子風險進行系統化分析，包括 TBML。此分析的主要產出資料，通常為國家風險評估（National Risk Assessment，NRA），可用來縮短公部門與私部門對各項威脅與弱點之瞭解的差距，它有助於確保風險理解之一致性，以及告知各項風險基礎政策、程序及／或法規的發展。**

報告提供了載明 TBML 風險的幾個 NRA 釋例，並輔以私部門機構如何修改其風險評估流程以提升 TBML 察覺能力的案例研究。有鑒於相關風險的跨國性質，此流程被視為鼓勵各司法管轄區與各機構考量其所承擔 TBML／TF 風險的重要流程，尤其是來自新觀點的風險，無論是因為貿易活動成長、公司設立流程增加，或因其金融服務市場擴張而導致。

結論

本報告目的係以方便且容易瞭解的方式，說明各項複雜的議題。本報告適用於已擁有可察覺與瓦解 TBML 或 TBTF 之完善體制與流程的國家，以及因為注意到貿易交易相關可疑活動成長而開始朝此方向前進的國家。本報告提供了可有效打擊 TBML 與 TBTF 犯罪之各項概念與方案的參考，各司法管轄區可依據其國內情況予以調整。舉例來說，若公部門與私部門之間所能分享且可用於起訴洗錢或資助恐怖分子之情報範圍有所限制，採用 PPP 則可更加著眼於公私部門之間針對策略性威脅與風險理解議題建立有意義的對話。

本報告的重點主題在於風險警覺性

本報告的重點主題在於風險警覺性，我們鼓勵各權責機關、各私部門機構以及全球各供應鏈的其他參與方都能將本報告視為採取各項行動時的參考指南。

[7] FATF 網站提供了幾個可解釋修訂內容的有用資源，而採用風險基礎方法也意味著各司法管轄區、各主管機關及受規範的實體會評估與瞭解其承擔的洗錢與資助恐怖分子風險，並依據風險水準採取適當降低風險措施。

前言

背景

FATF 在 2006 年發布的貿易型洗錢研究，針對 TBML 現象提供了完整且詳細的評估，並列示了在 TBML 犯罪中運用的各種類貿易活動。該報告將 TBML 視為組織性犯罪集團（OCG）為隱匿資金與資產來源而用於移動資金與資產的三個主要方法之一。FATF 後續並於 2008 年發布了「貿易型洗錢最佳實務報告（Best Practices paper on TBML）」，協助各權責機關評估所發現的風險。

亞太防制洗錢組織（APG）依據前述原始研究，在 2012 年發布了一份更新報告，並提出影響有效辨識 TBML 及其後續調查的幾項關鍵議題。除前述具體報告外，TBML 也在其他幾份 FATF 文件中被提及，包括因與自由貿易區有關而被普遍採用者（2010 年）以及專業洗錢網絡（Professional Money Laundering Networks）對其運用的狀況（2018 年）。

有鑒於國際貿易的動態性質，包括可買賣商品與服務的多元性、涉及多個交易方，以及貿易交易的速度，TBML 仍然是貿易活動中影響深遠且重大的一項風險。在這裡簡單介紹一下其背景。「世界貿易組織 2019 年統計回顧（WTO Statistical Review of 2019）」[8] 指出，2018 年全球貨品（亦即商品）貿易量成長了 3%，而貿易總值成長了 10% 至 19.67 兆美元，部分原因來自於原油與採礦產品顯著成長 23% 所致。此成長可從幾份問卷回覆中提到的 TBML 犯罪利用了原油與採礦產品此事看出端倪。該份報告也指出，2018 年全球商品貿易出口總值成長了 20%。

有鑒於可買賣商品與服務的多元性、涉及多個交易方，以及貿易交易的速度，貿易型洗錢活動仍然是貿易活動中影響深遠且重大的一項風險。

該報告也指出，過去十年期間，開發中經濟體在世界貿易中的表現，大部分超越或等同於已開發經濟體的表現。此情況可能代表貿易活動已經擴張到先前未開發的市場，包括商品與服務，並因此創造了組織性犯罪集團、專業洗錢人員與恐怖分子資助者操縱貿易活動的全新機會。

[8] 世界貿易組織 2019 年統計回顧（WTO Statistical Review of 2019）：www.wto.org/english/res_e/statis_e/wts2019_e/wts2019chapter02_e.pdf

本報告採用先前所發布評估報告為基礎，但進一步納入了 FATF 全球網絡、艾格蒙聯盟、各私部門機構以及其他多邊機構的深入見解與專業。本報告對 TBML 方法與降低風險措施提出了一個完整且全新的觀點，包括各項新措施的影響，例如建立公私協力夥伴關係（PPP）架構。報告也提供 TBTF 的全新深入見解，建立對於恐怖分子資助者如何且確實運用貿易流程的認知與理解。

目的與報告架構

本報告係以供廣泛讀者閱讀之目的而撰寫，對象包括負責辨識、調查或起訴 ML 或 TF 的各權責機關，可能面臨 TBML ／ TF 濫用或發現相關議題卻不瞭解其真正代表意義等風險的金融機構（FIs）及指定非金融事業與人員（DNFBPs），以及涉及區域或全球供應鏈的其他各方。

其目的在以易於瞭解的方式描述國際貿易與相關金融體系的複雜狀況，讓負責降低TBML／TF風險的關鍵利害關係人能夠清楚瞭解。然而，考量此主題的複雜性質，報告也提供了其他人就此部分所進行的深入且具參考價值的研究，以供進一步瞭解 TBML ／ TF 時參考。

與艾格蒙聯盟之間的合作，除了能夠增進對 TBML ／ TF 犯罪與相關風險指標的瞭解外，也代表可取得各金融情報中心（FIU）在察覺 TBML 方面所採用資源與技巧的絕佳機會。另外，這部分也提供了擔任 TBML ／ TF 網絡察覺、調查與起訴先鋒之執法機構的見解，以及海關的豐富經驗，包括多份案例研究，有助於進一步成功阻擋犯罪行為的發生。

第三個重要資料來源為多個全國性與國際性金融機構，其不僅協助提供風險方面的額外深入見解，也帶來了多個採用犯罪調查與起訴行動以外替代措施成功瓦解 TBML 犯罪的案例。

有鑒於上述背景，本報告以達成以下目標為架構：

第 1 節：定義與貿易融資活動

本節：

- 整合先前各項貿易型洗錢（TBML）的定義，並釐清貿易型資助恐怖分子（TBTF）的活動，讓讀者能夠改善對 TBML 與資助恐怖分子（TF）的瞭解。本節尤其適用於新接觸此議題或可能尚未確定如何評估其所

承擔風險的讀者[9]。本節亦有助於釐清 TBML 與貿易相關前置犯罪之間差異，例如走私。

- 簡要說明貿易流程與融資，以協助公部門機構深化對這些活動如何運用於 TBML／TF 犯罪的瞭解。對這部分的需求是 2012 年報告的主要建議，也是各報告資料提供者反映仍有不足之處。

第 2 節：貿易型洗錢風險與趨勢

本節：

- 說明 FATF 全球網絡各成員如何提升其對 TBML／TF 議題的認知、評估與辨識能力，並提供各公私部門所執行風險分析與評估作業的案例。這些案例意為各司法管轄區、各權責機關及／或其他各私部門機構提供建議，以協助分享對 TBML／TF 風險的理解。
- 提供承擔 TBML／TF 風險之各經濟體與產品的摘要。此摘要並非涵蓋所有情況的清單，其目的是希望協助對 TBML／TF 察覺過程較不成熟的各權責機關，作為其未來分析風險與威脅的起點。
- 2006 報告將 TBML 的評估作業定義為「基礎（basic）」TBML 技巧，但更精確的說，應該將其視為「通則（common）」技巧。這些活動廣泛歸類為涉及不實的商品及／或價值，亦反映持續使用披索黑市交易的情況。
- 匯總關鍵 TBML／TF 風險，反映各項新現金整合方法，例如運用代購方網絡，及滲透至未使用任何不實貿易流程的合法供應鏈。
- 分享 TBTF 相關深入見解，瞭解其相對於 TBML 之額外偵查複雜度。另外也提供各項提醒，讓各司法管轄區、各權責機關或各私部門機構能夠從已發現且成功瓦解 TBTF 的其他方學習到寶貴經驗。

第 3 節：打擊貿易型洗錢所需面臨的挑戰

本節：

- 檢視當前影響成功辨識、分類、調查或起訴 TBML 或 TBTF 犯罪的各項作業面挑戰，並將這些挑戰與 2012 年評估時完成之類似分析資料，

[9] 此包括尚不需執行防制洗錢（AML）／打擊資助恐怖主義（CFT）活動但涉及貿易交易且可能須承擔 TBML／TF 風險的公司。例如，貨運承攬商或報關代理人。

並重申先前各項重要發現，以鼓勵 FATF 全球網絡進一步採取正向行動。

第 4 節：打擊貿易型洗錢之各項措施與最佳實務

本節：

- 反映了為改善各司法管轄區內部與管轄區之間合作狀況而採行之各項新行動，包括建立 PPP 制度及其他形式的跨機關工作小組。
- 提供採用 IT 與進階系統面分析之各項全新且創新的風險辨識方法。運用從這些活動整理與學習到的經驗，協助採行各項整合式瓦解與調查作為。

因此，本報告旨在促進有關 TBMLL／TF 方法及各行業或商品開發既有靈活性的風險，相關的思量、討論與進一步的群體交流。

研究方法

本報告受益於由 FATF 全球網絡與艾格蒙聯盟成員所組成專案團隊的支持與指導。為提供本報告所需的深入見解與發現，專案團隊除召開會議外，亦採用下列流程：

- 編製與發送問卷。第一份問卷是向 FATF 全球網絡各權責機關發出，請求其提供 TBML 的深入見解，包括辨識所運用行業、進一步調查及／或起訴所面臨的挑戰，以及各項成功瓦解 TBML 的案例。第二份問卷鎖定私部門，請求其提供對 TBML 的看法，包括為改善對風險的理解及／或辨識而設計的各項活動。第三份問卷是由艾格蒙聯盟「資訊交換工作小組（Information Exchange Working Group，IEWG）」所設計，目的是向各參與金融情報中心（FIU）蒐集各項案例研究、經驗、挑戰、最佳實務以及有用的風險指標。
- 重申先前針對 TBML 所發布 FATF 報告的各項學習重點與重要發現，主要為 APG 所發布的 2012 年度報告。包括對 2012 年「貿易融資流程」說明的更新，以反映全球貿易的成長與變動。
- 檢視與更新先前發布的紅旗指標，併同考量從問卷及與公私部門間互動而獲得的額外深入見解。

- 針對提倡打擊 TBML 最佳實務公開文件之文獻回顧，包括世界海關組織（World Customs Organisation，WCO）與艾格蒙聯盟合作發布的「海關與金融情報中心合作手冊（Customs-FIU Cooperation Handbook）」，及由沃爾夫斯堡集團（Wolfsberg Group）、國際商會（International Chamber of Commerce）與金融與貿易銀行家協會（Bankers Association for Finance and Trade，BAFT）共同發布的「2019 年貿易金融原則（2019 Trade Finance Principles）」報告[10]。

本報告各節皆反映了來自問卷的回饋意見，並提供多個案例研究，以強調應予注意的各項 TBML ／ TF 犯罪要件。於編寫與各項風險及趨勢有關的章節時，本報告也列出了問卷受訪者（包括公部門與私部門）在 TBML 調查期間所觀察到的幾個行業與商品。然而，正如一名問卷受訪者提到的，**組織性犯罪集團、專業洗錢人員以及恐怖分子資助者，會在找到機會時，運用任何一種行業、商品或服務**。

[10] www.wolfsberg-principles.com/sites/default/files/wb/Trade%20Finance%20Principles%202019.pdf

第 1 節　定義與貿易融資流程

定義貿易型洗錢與貿易型資助恐怖分子

貿易方面的運用，為組織性犯罪集團、專業洗錢人員與恐怖分子資助者，提供了阻撓權責機關與金融機構辨識與干擾犯罪活動的機會， 亦有助於支援各種其他非法資金流動，包括資金外逃、規避制裁逃稅。為協助簡化議題，本節：

- 重申 FATF 先前就 TBML 所作的定義，並提出一個 TBTF 的實務性定義；
- 描述 TBML 與貿易相關前置犯罪的差異，主要著重於意圖；
- 描述 TBML ／ TF 犯罪運用該等貿易融資技巧的基本狀況；

貿易型洗錢 vs 貿易相關前置犯罪

根據 2006 年 FATF 報告的定義，TBML 係指「透過採行貿易交易的方式，掩飾犯罪所得並移動價值的過程，以將其非法所得合法化或資助其活動的進行」。

貿易型洗錢的目標不是移動商品，而是移動資金，這可透過貿易交易來達成。

綜而言之，任何 TBML 犯罪的主要目標，都在於透過運用貿易交易的方式來蓄意移動非法所得。犯罪者可透過這類方式從事各種其他潛在非法活動，例如製作偽造帳單、錯誤描述的商品特性以規避管控，以及其他違反關務與稅務規定之行為。**不過，與貿易相關前置犯罪不同的一**

點在於，TBML 的目標不是移動商品，而是移動資金，這可透過貿易交易來達成。

TBML 犯罪的另一項主要差異，在於涉及專業洗錢人員（PML）。從事貿易相關前置犯罪的犯罪者通常為該等非法所得的最終受益人，而 PML 則擁有可採用各種洗錢技巧（例如 TBML）分散其風險的專業。這些 PML 負責代表組織性犯罪集團（OCG）收取犯罪所得，並在透過（包括）TBML 犯罪移轉與轉換該等所得給 OCG 之前，扣除其服務費或佣金。

定義貿易型資助恐怖分子

TBTF 運用與 TBML 相同的貿易流程，但存在重大且基本面上的差異，即所移動的所得或價值可能來自合法與非法來源，這增加了察覺與瓦解 TBTF 的複雜度。

因此，本報告將 TBTF 定義為「透過運用貿易交易的方式掩飾來自合法或非法來源的價值移動，以資助恐怖主義」。

本報告雖然提及了察覺 TBTF 複雜度的其他層面問題，但所引用的案例研究及對所提供其他資料進行的分析[11]，對 TBTF 某些面相作出定義，都可能有助於權責機關強化對 TBTF 犯罪的理解。

貿易流程與融資

本節匯總了先前發布的 FATF 報告中所列常見的貿易融資種類。此清單絕非無所不包的清單，僅是為確保擁有基本的理解而提供。

國際貿易的交易各方須承擔各種類的風險，導致出口商與進口商之間對付款時點存在不確定性。此情況造成供應鏈間的緊張情勢，並可能對進口商與出口商帶來不利影響。

貿易流程與融資都為因應此緊張情勢而有所調整，同時繼續支持全球的成長。對此，國際交易共有五種主要付款方法，匯總如表 1.1。這些方法依據進口商或出口商的偏好而排序，因此進口商最不偏好的方法通常是預付現金，因為他們必須在收取商品之前就付款給出口商，不過，此方法卻是出口商最偏好的方法。

[11] 例如，在建議採用的次分類法當中，包括採購供恐怖分子團體使用的品項。此部分不僅包括典型商品（例如槍枝），也包括後勤設備以及可武器化的技術，例如將二手車或無人機銷售至衝突區。

表 1.1　付款流程與風險管理層級

	最不偏好	較不偏好	沒意見	較偏好	最偏好
出口商	託售	專戶記帳	跟單託收	信用狀	預付現金
進口商	預付現金	信用狀	跟單託收	專戶記帳	託售

資料來源：修改自國際貿易付款方法（Methods of Payment in International Trade）(Export.gov), https://2016.export.gov/tradefinanceguide/eg_main_043221.asp]

資料提供方指出，專戶記帳（open account）與跟單託收（documentary collection）在他們的 TBML 分析與調查活動中是最常見的方法。事實上，根據沃爾夫斯堡集團（Wolfsberg Group）資料，在各金融機構所處理的國際貿易交易當中，約有 80% 屬於專戶記帳交易。然而，就如同此觀察並未提及其他種類貿易融資，這不代表該等融資種類未被運用在 TBML 犯罪當中。儘管如此，若以定期預付現金作為有系統掩飾犯罪所得的方法，進口商可能會引起權責機關或金融機構的懷疑。

專戶記帳

聯合國「貿易便捷化執行指南（Trade Facilitation Implementation Guide）」提到，「專戶記帳交易是指商品在款項到期之前就已經出貨與交貨的交易」。此方法的款項通常按特定期間支付，大概是介於收到商品或服務日起算 30 日～ 90 日期間。TBML 犯罪經常採用此方法，因為金融機構在此方法中扮演的角色較少，亦即其監督程度會比跟單託收流程還低。無論是透過自動化或人工交易監控，金融機構可能在客戶營運合法性評估的精確度和持續性有所掙扎。

APG 報告也指出此問題，並將其描述為「在標的貿易及其融資資金之間創造斷點」[12]。組織性犯罪集團、專業洗錢人員或恐怖分子資助者因而運用了此斷點，以隔絕的方式運用特定漏洞或差異，降低其被察覺的風險。另外也可以透過在多個司法管轄區採用第三方中介機構的方式來增加複雜度，以阻礙執法單位或金融機構的察覺與瓦解行動。

[12] 2012 年度報告包含了針對各種專戶記帳機制進行的完整分析，包括（出口與進口）應收帳款收購、買賣斷（forfeiting）、交貨前與交貨後融資，以及買方與賣方之間的信用安排。

然而，其特別強調的是專戶記帳交易是全球貿易流程中非常重要的一部分，因此若要針對加強專戶記帳交易規範提供一個簡要答案，那麼在後勤或經濟面都不具可行性。本報告後續章節重點說明了可提高找到洗錢或資助恐怖分子運用手法的既有與較新措施，並提供可線上取得的額外參考資料，載明專戶記帳貿易的遵循程序，以提高察覺 TBML 的機會。

跟單託收

在跟單託收流程中，出口商會提示買賣商品的運送與收取文件給其金融機構，並要求付款。出口商的金融機構會將這些文件交給進口商的金融機構，進口商的金融機構則會將資金轉帳給出口商的金融機構，由後者將資金計入出口商帳戶。

然而，儘管我們認為金融機構在此方法下所扮演的角色將會加重，但金融機構並不必然需要驗證文件的真實性，因此其功能也甚為有限。此外，各項文件不見得經過標準化，從而提高了透過虛假或偽造帳單運用 TBML 的風險。然而，若確實檢查與查證這些文件，則可運用特定資料點來找出 TBML 行為，包括：

- 運用個人電子郵件信箱取代合法商業電子郵件。
- 依據金融機構資料儲存能力之不同，明顯回收先前編輯較少或無任何編輯的文件，包括如日期等基本資料。
- 金融機構研究後，發現出口商完全沒有任何交易據點，包括使用住宅而非出口商的營運據點來提供大量商品。

第 2 節　貿易型洗錢風險與趨勢

本章節進一步探索各項 TBML 風險與趨勢，內容涵蓋：

- 確認既有 FATF 建議之要求，給予各司法管轄區信心使用或強化其既有 AML／CFT 法律架構、政策與程序，以提升其辨識與瓦解 TBML／TF 的能力。

全球所有國家皆與貿易活動有關。貿易型洗錢與運作活動（例如濫用企業架構）可能發生在各司法管轄區。

- 說明各司法管轄區與公司如何完善對 TBML 與 TBTF 風險的瞭解，包括透過任何國家風險評估（NRA）流程或風險別威脅評估來達成，諸如一司法管轄區的企業架構可能被利用為協助進行 TBML 活動的情形。
- 列出以 TBML 活動為偏好或顯著採用洗錢機制的常見前置犯罪種類。本報告並未詳細說明這些前置犯罪，但鼓勵各權責機關重新檢視過去進行或正在進行的前置犯罪調查，確定其是否涉及 TBML 活動。
- 彙總容易遭受 TBML／TF 活動影響的經濟行業或產品，如同彙整前置犯罪活動一樣，係為引導各權責機關或受規範企業檢視該等行業或產品，以確定其是否被運用在 TBML／TF 活動。此活動清單並非確定，但可用來說明組織性犯罪集團（OCGs）、專業洗錢人員（PMLs）與恐怖分子資助者利用的各種行業與產品。
- 深入瞭解犯罪者常用的 TBML 技巧，並列出幾項最近出現的較新種類 TBML 風險。
- 提出服務型洗錢（SBML）的各個面向，但強調即使其與 TBML 具類似性質，仍為完全不同的洗錢形式。

儘管本節重點在於風險，本報告也發現各司法管轄區在試圖量化其 TBML ／ TF 風險方面所遭遇的困難。其主要挑戰包括國際貿易的複雜性與成長、海關權責機關在檢查多批國際貿易貨物時遭遇到的挑戰[13]、TBML 跨司法管轄區的性質，以及某些情況下金融機構及其顧客對 TBML ／ TF 風險的瞭解有限。

針對貿易型洗錢採用風險基礎方法

自亞太防制洗錢組織（APG）發布 2012 年報告以來的一個重大改變，在於 FATF 建議及涵蓋各項 AML ／ CFT 措施之相關國家別評估程序的修訂。其修訂內容包括發展有效的評估方法，強調實際執行 AML ／ CFT 措施，而非僅將 FATF 建議轉換為國內法規。舉例來說，FATF 建議要求各國制定起訴洗錢犯罪行為的法律架構，而有效性評估則可依據各國風險屬性，決定這些犯罪行為（包括 TBML）的調查與起訴的範圍。

本節著眼於對洗錢／資助恐怖分子採用風險基礎方法，此方法是各國評估其所承擔風險的關鍵起點。

FATF 第 1 項建議[14]要求各國辨識、評估與瞭解其洗錢／資助恐怖分子風險，並依據所辨識的風險執行後續預防與降低風險措施。此風險可包括與 TBML ／ TF 有關的各項威脅與弱點。各國通常透過制定適用於洗錢與資助恐怖分子活動的國家風險評估（NRA）來符合此要求，該些文件的完整版及精簡版通常可以公開取得。這些評估作業主要由公部門機構所推動，但在評估發展流程的過程中會納入私部門的回饋意見。

雖然有多種方法可評估洗錢／資助恐怖分子風險以建立 NRA，國家通常還會評估多種不同資料，包括情報報告、可疑交易報告（Suspicious Transaction Reports，STRs）、威脅評估、調查結果與經濟及社會指標，以及威脅與既有弱點的程度[15]。

公部門提供的資料對本報告的主要貢獻，在於 TBML 與各種國內與

[13] 此活動可能包括各種不同資料或文件，包括但不限於 — 帳單、運送文件、相關海關文件以及實體現場檢查。然而，資料提供方也指出，即使能夠取得這些資料，也不保證能夠偵知 TBML，反映了與所有貿易鏈參與方合作的必要性。

[14] 有關具體 FATF 建議報告的詳細內容，請參閱 FATF 網站，網址為 www.fatf-gafi.org

[15] 有關流程的詳細內容，請參閱 FATF 所發布的「國家洗錢與資助恐怖分子風險評估指南（Guidance on National ML and TF Risk Assessment）」，網址為：www.fatfgafi.org/publications/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

外國前置犯罪之間的關係，包括因走私非法或受限制商品而導致之犯罪行為，例如毒品走私、武器買賣或煙草走私，而組織性犯罪集團（OCGs）與專業洗錢人員（PMLs）則會再次運用供應鏈走私商品，以達成犯罪所得洗錢目的。

其他人則提到，與前置犯罪相關但未採用商品走私方式的 TBML 犯罪，例如逃稅。這類犯罪（通常與 PML 有關）需要發展新的供應鏈與金融中介機構，因為並無既有的商品供應鏈可以運用。這些 TBML 犯罪通常跨多個司法管轄區，不只運用原始司法管轄區的貿易行業，也透過運用企業服務而影響了其他方。

少數問卷受訪者同時提到實際與潛在 TBTF 濫用情況，本節稍後將說明此見解。然而，大部分受訪者都沒有發現濫用貿易系統移動資金並協助恐怖分子的情況，或代表個別恐怖分子或團體的情況。

全球所有國家皆與貿易活動有關。TBML 或 TBTF 活動因此會發生在任何地方。資料提供者提到，協助 TBML ／ TF 的活動（例如濫用企業架構）可能發生在各個司法管轄區。組織性犯罪集團、專業洗錢人員及／或恐怖分子資助者，會運用任何潛在漏洞或差異，而 NRA 所帶來的助益，也讓各國不得不從威脅與弱點角度開始思考風險。

實例參考 2.1 德國國家風險評估與貿易型洗錢

2017 年 12 月，德國發表其首份 NRA，作為其打擊 ML 及 TF 努力的一部分。此評估計畫由德國聯邦財政部（Federal Ministry of Finance）主導，共有 35 個聯邦與地方機關參與。

德國的第一份 NRA 提及了 TBML 的重要性，主要係因德國的貿易量所致。該評估報告提及典型 TBML 方法，包括商品與服務帳單高報與低報、商品與服務多次發單收款、虛假交易、運用空殼公司以及將犯罪所得投資於高價值商品（例如車輛、手錶、珠寶、黃金、不動產、藝術品）。在這些情況下，與私部門行業合作及各負責方呈現報告的行為，扮演了瞭解 TBML 風險的決定性角色。

德國因為整合私部門（尤其是金融機構）知識與資訊而獲得的經驗，在於確保金融機構（除任何案例所需的文件外）對標的貿易交易與貿易夥伴擁有足夠的知識。金融機構（尤其是銀行業）因此更能夠察覺 TBML 活動的跡象，並將 STR 提交給金融情報中心。

資料來源：德國

幾乎所有公部門受訪者都表示已具體在其 NRA 提及 TBML，或已知悉透過其金融與貿易體系運用 TBML 的風險及／或濫用該國法律實體從事 TBML 活動的風險。有幾名代表將 TBML 列為高風險活動 [請參閱下列實例參考 2.2]。

實例參考 2.2 美國國家風險評估與貿易型洗錢

美國在進行國家風險評估時，將 TBML 同時歸類為威脅與弱點。墨西哥與歐洲跨國犯罪組織（TCO）及其相關毒品走私活動，都採用了 TBML 犯罪，其複雜程度使得權責機關難以察覺，並因此帶來了威脅。如美國金融與貿易業的多個弱點，皆被運用於 TBML 活動。

美國早在 2005 年就在其國家洗錢威脅評估中特別列出了 TBML。2015 年度國家洗錢風險評估（National Money Laundering Risk Assessment，NMLRA）提供了 TBML 犯罪的更新資訊，發現大部分案例都涉及美國的共謀商家或掛名公司，接受以非法所得交換商品。在發布該份 NMLRA 後，美國財政部也與美國境內金融機構聯繫，共同討論此等發現。

2018 年，美國發布了第一份「國家非法金融策略（National Illicit Finance Strategy）」[1] 及更新版的 NMLRA。2018 年報告指出，TBML 仍為毒品走私與販毒集團的主要洗錢方法，涉及使用非法所得購買商品並出口。這些報告也指出 PML 助長 TBML 活動的情況，以及其如何破壞前置犯罪與相關洗錢活動的連結，導致難以將毒品走私犯與洗錢活動建立關聯性。

最後，2020 年國家非法金融策略也提到，TCO 更仰賴亞洲 PML 擔任傳統 TBML 犯罪的洗錢中介。TBML 也被列為美國境內大量現金扣押案例減少的可能原因。扣押數量的減少，可能代表了 TCO 使用更隱密的方法移動非法資金的情況有所增加，例如 TBML。

註：
1. 請參閱 https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf

資料來源：美國

少部分受訪者指出其 NRA 完全未反映 TBML，主要係因未將該等活動視為重大風險。但儘管未於 NRA 提及 TBML，還是有一資料提供者分享了與 TBML 經驗有關的深入見解，另外兩個受訪者則在整體經濟犯罪風險中提及 TBML，包括法人實體的運用以及中介機構所扮演的角色，例如公司設立代理人或理財顧問。

許多私部門資料提供者也自行執行了內部風險評估，以估計其所承擔的 TBML 或 TBTF 風險。事實上，所有私部門受訪者都承認擔負 TBML 風險，包括金融產品或服務層面，以及其顧客可能主動或無意的協助 TBML。

實例參考 2.3 私人機構評估其貿易型洗錢風險的釋例

新加坡將 TBML 視為應優先處理之風險，且新加坡金融管理局（Monetary Authority of Singapore，MAS）在過去也持續努力提升業界對風險的認知。

舉例來說，新加坡一家擁有國際據點與全球貿易連結的金融機構，基於貿易在新加坡經濟的重要角色，將 TBML 列為重大風險。該機構基於地理區域、產品與交易風險，將其貿易融資業務評估為具有較高固有洗錢風險。

為強化其察覺 TBML 與其他風險的能力，該機構計畫推行自動化交易監控系統。其將採用資料與網路分析技術，找出較高風險的顧客並進行調查，去除人工審核個別貿易交易的需求。

資料來源：新加坡

FATF 建議要求各司法管轄區在辨識與瞭解所承擔的風險之後，須運用該資料採行降低風險行動，並推動其 AML／CFT 體系內的有效合作。舉例來說，各司法管轄區皆應採行風險基礎方法監督，就 TBML 方面，代表了設有大型貿易融資部門或處理大量跨國付款活動的金融機構都需要監管機構加以額外監督，以確保其任何威脅降低策略的有效性。

除會計服務提供方外，有專業公司設立行業的各司法管轄區也應考量這些公司遭受 TBML 或 TBTF 風險的可能性，並確保任何威脅降低策略的有效性。

實例參考 2.4 強化貴金屬與寶石交易商法規

依據德國 NRA 的結論以及 DNFBP 監督活動的意見，德國貴金屬與寶石交易商非常容易受到洗錢活動的影響，包括 TBML。德國權責機關注意到有大量的現金付款情況，且金額都剛好低於 10,000 歐元的盡職調查門檻。為因應此風險，德國在將「歐盟第四號洗錢指令（Fourth EU ML Directive）」轉換為國內法律的過程中，將要求貴金屬與寶石交易商進行盡職調查的現金門檻調降為 2,000 歐元。

資料來源：德國

容易受到 TBML 活動影響的經濟產業與產品

本節概要說明普遍經濟產業及商品可能承受的 TBML 風險，所列項目不應視為無所不包的清單，而係提供當前所面臨風險的簡述，同時強調所運用行業與產品的多元性。如同一個私部門受訪者提到的，犯罪者會運用各司法管轄區中可能存在客戶盡職調查與瞭解你的顧客流程差異或應用不一致之各種行業、產品或業務，且此情況可能會因為對 TBML 風險的瞭解不成熟或瞭解有限而更加惡化。

許多經濟產業很容易受到 TBML 影響，不管是高價值、低數量行業或產品（例如貴金屬），或低價值、高數量行業或產品（例如二手服飾），都可能被犯罪者用來進行犯罪所得洗錢。儘管存在行業多樣性，我們還是發現了少數幾個可能被用來進行 TBML 活動的常見情況：

- 訂價獲利區間較大的商品；
- 交易循環時間較長的商品（亦即，運送跨越多個司法管轄區）；
- 海關權責機關難以檢查的商品。

移動較低價值商品的供應鏈，最容易承受犯罪組織或 PML 網絡端對端（end-to end）所有權的風險。其設置成本可能遠低於移動較高價值商品的供應鏈，且可能無法吸引供應鏈中各權責機關給予相同的注意力。運用這些產品的另外一個優點，在於供應各司法管轄區多個市場的範圍[16]。這點亦有助於降低權責機關或受規範公司注意任何市場飽和可疑情

[16] 這些產品通常具有高需求（例如便宜的服飾），因此可為 TBML 網絡創造合法的交易形式。

況的風險，例如若特定較低價值產品（例如服飾）重複的運送到相同目的地，就不必然是可疑的情況。

這些因素為持續採用 TBML 技巧提供了合適的環境。舉例來說，犯罪組織可能合法運送化妝商品並創造足夠的有效文件，以於後續執行虛擬運貨及濫用該等文件。於部分情況下，交易可能維持完全合法（因此不需運用常見 TBML 技巧），但所運送的產品幾乎不存在可銷售的任何價值，且運抵目的地後即棄置（例如二手紡織品）。

當 OCG 或 PML 運用較高價值產品時，較可能透過滲透與後續濫用既有供應鏈的方式進行。OCG 或 PML 可能運用遭遇現金流問題的既有公司，以出錢擔任「隱名合夥人（silent partner）」的方式，運用該等事業及其供應鏈聯絡方進行犯罪所得洗錢。此滲透合法事業之情況，將於下文詳述。

黃金、貴金屬與礦物

TBML 犯罪經常運用黃金及其他貴金屬與礦物，包括以黃金作為洗錢流程內價值的替代形式，亦即不只是用來移動價值的商品，也是現金的替代品。

TBML 若與非法採礦活動有關衍生額外的問題，例如系統性的違反衛生與安全準則、其他形式的勞工剝削，及重大環保問題。

實例參考 2.5 在貿易型洗錢犯罪中運用黃金

在美國，四名秘魯人因遭控涉及一項數十億美元的國際黃金洗錢犯罪而遭到起訴。

這四個人在 2013 年至 2017 年期間，共謀購買來自拉丁美洲與加勒比海的價值數十億美元犯罪所得黃金，而且他們有可能知悉黃金是來自於犯罪活動所得，包括非法採礦、外國賄賂與非法走私。他們利用一家位於佛羅里達州且從事貴金屬交易的公司進行交易。

該等黃金後續出售給共謀的美國精煉廠，後者則透過以看起來像是大宗黃金採購之合法付款的形式，轉帳支付黃金款項並完成洗錢循環。

資料來源：美國

汽車零件與車輛

許多 TBML 犯罪都描述了運用汽車零件或車輛的情況，包括二手車輛或豪華車輛的買賣。其中一種犯罪包括自一個司法管轄區將受損的汽車運送到另一個司法管轄區，後者則在修復車輛之後在合法市場中繼續銷售。

組織性犯罪集團（OCG）在出口港適當申報了正確的價格，但在轉運點則申報了相當低的價值。儘管受損車輛的市場相對透明他們還是這麼做，而且車輛的銷售價格接近其未受損價格。為了進一步阻礙執法機關（LEA），OCG 透過位於多個其他司法管轄區的不同公司網絡進行付款。

以下案例說明了犯罪者如何為其 TBML 犯罪增加更多交易層與複雜度。OCG 運用了幾種不同的行業，包括高級車輛與較低價值的紡織品，以分散其所承擔的風險，並將其網絡延伸至多個司法管轄區。

實例參考 2.6 在貿易型洗錢犯罪中運用車輛

在一項由西班牙與義大利權責機關所共同進行的調查當中，發現多名居住於西班牙的義大利人設立了一個多公司網絡，用於針對清洗毒品走私與稅務詐欺不法所得進行洗錢。此犯罪與黑手黨活動有關。

該 OCG 使用犯罪現金所得在德國購買豪華汽車，另外還註冊並使用多個法人實體，並創造虛假的買賣交易紀錄軌跡，以創造增值稅連結。他們接著運用了貿易流程掩飾其原始犯罪所得，並因此創造額外犯罪所得。在此部分洗錢犯罪發展到一定程度後，OCG 說服一家義大利合法供應商每年交付大量車輛，以提高其洗錢活動的合法程度。

除了運用這些高級車輛外，OCG 也運用其控制的進口／出口公司購買其他奢侈品項（例如手錶），以及較低價值的品項（例如鞋子與織品）。該等手錶是在西班牙與瑞士所購買，然後供應給摩洛哥與荷蘭的毒品走私者，而服飾則是購自中國香港與中國大陸，然後出口至哥倫比亞與摩洛哥進行後續銷售。

2017 年的執法活動在歐洲多個國家發現總值 800 萬歐元的資產，而 2018 年的後續行動又另外發現了其他資產，包括扣押 11 處房地產、6 部車輛、32 個銀行帳戶，及兩家公司的股票。

資料來源：歐洲刑警組織（Europol）

農產品與食品

研究也發現 TBML 犯罪運用了農產品的情況，包括濫用涉及非常容易腐敗品項的食品供應鏈，例如新鮮水果與蔬菜。這些都是低價值高數量產品的良好案例，因其易於腐敗的特性，不必然會受到市場飽和度的影響。

OCG 與 PML 會滲透這些合法供應鏈，以其作為將非法現金納入金融系統的方法。他們並未運用任何常見 TBML 技巧，而是使用這些合法供應鏈將其犯罪所得移動到各個不同司法管轄區。下列案例突顯了鎖定運用低價值食品之 OCG 與 PML 網絡之聯合調查團隊的價值，同時也顯示 PML 如何藉由第三方帳單結算流程，來提升其 TBML 犯罪的複雜度。

實例參考 2.7 在貿易型洗錢犯罪中運用農產品

在例行性車輛檢查發現 300,000 歐元之後，法國、比利時與荷蘭等國在 2016 年發起了一項跨機構調查。該等國家成立了一個聯合調查團隊，重點稽查毒品走私所得的洗錢活動。

毒品走私者運用一個 PML 網絡的服務，而該等網絡則使用了多種不同的技巧，包括 TBML。此活動估計已活躍進行達四年期間，且疑似洗錢金額達到約 4 億歐元。該 PML 網絡採用了法國與比利時的地下金融網絡，協助收取與匯出犯罪所得。荷蘭地下匯兌業者任職於一家進口／出口公司，從事與北非各國買賣食品的業務。

該公司向荷蘭與德國採購馬鈴薯與洋蔥，接著出口給北非的數家公司。這些公司被指示將款項支付至由毒品走私者所控管的多個銀行帳戶。

在 2019 年調查結束時，決定了洗錢與毒品走私的判決，包括扣押價值 480 萬歐元的資產以及超過 700 萬歐元的現金。

資料來源：歐洲刑警組織（Europol）

服飾與二手織品

與食品相同，服飾與二手織品都是低價值高數量產品非常具說服力的範例，可延伸供應鏈，並使其非常適合被運用在 TBML 犯罪中。其具有極端價格波動的性質，也使其能夠透過錯誤描述價格的方式，用於洗錢活動。

多家金融機構都提到了運用此行業的情況，還有一個公私協力夥伴關係（PPP）機構製作了一份產業別警示機制，突顯與供應二手服飾與織品有關的重大風險議題。

攜帶式電子產品（行動電話、筆記型電腦等）

攜帶式或手持式電子產品，也經常被使用在 TBML 犯罪當中，因該等產品可蓄意的標示不當且錯誤的價值，提高了移動大量犯罪所得的機會。下列案例突顯了 OCG 運用攜帶式電子產品的情況。

實例參考 2.8 在貿易型洗錢犯罪中運用高價電子產品

澳洲邊防署（Australian Border Force，ABF）於 2017 年開始進行一項 TBML 的檢查作業，該等作業是由國際合作夥伴所建議，且與運用小型攜帶式電子產品的貿易活動有關。

ABF 的專家採用了各種分析式技巧進行詳細檢查，並輔以金融與犯罪情報，使其能夠針對相關實體編製一份詳細的犯罪者網絡評估報告。在彙整廣泛洗錢協助者網絡的資料後，ABF 發現自 2014 年起，共有超過 5 億澳幣（即 3 億 360 萬歐元）透過澳洲的銀行帳戶交換。

該等所得來自北美的毒品銷售。相關犯罪所得被轉到位於東南亞的銀行帳戶，之後則透過位於澳洲金融機構的多個銀行帳戶，增加交易層。該等所得後續被匯往境外銀行帳戶，或用於採購小型高價電子裝置，並出口至位於東南亞與中東的公司。裝置出口的價值被低估，移轉至境外時誇大了其非法價值。

在此案例中，ABF 結合了自動化與人工貿易資料差異分析技巧，以更加辨識與評估可疑的 TBML 案例。自 A 國出口商品的申報資料，必須與 B 國相關進口資料相符（因理論上寄銷交易是相同的物品）。於本案例中，若兩者的資料不相符，ABF 官員就有理由相信該等差異是交易價格不當標示的指標，且因此屬於潛在 TBML 活動。ABF 的進一步調查以及與夥伴機構的合作，使其能夠將 OCG 與各項交易連結在一起。

資料來源：澳洲

除上述行業與產品外，下列行業也存在 TBML 運用情況：建築材料（木材）、工廠機器、金屬廢料交易商、石油與能源產品以及酒精類與非酒精類飲料。

承擔貿易型洗錢風險的各類事業

各行業中，每種商業模式所承擔的 TBML 風險也各有不同。多數 TBML 犯罪都涉及中小型企業，但部分調查涉及大型跨國公司，通常是透過海外子公司進行，該等子公司擁有更活躍的貿易關係，可將產品經銷至較新的市場。

此處應注意的具體商業指標包括：

- 既有市場新成立公司的快速成長；
- 持續且大量現金付款的證據，包括支付給先前未知的第三方。這些事業亦可能收到未提供任何說明的第三方付款；
- 非必要而複雜的供應鏈，涉及多次轉運；
- 先前成立從事某特定行業的公司，非預期轉向完全不相關的行業。其中一個案例提到，一家 IT 公司在採購與經銷大宗藥品方面快速建立穩固基礎；
- 公司同時經營超過一項非相關行業。

應注意的一項重點是，即使公司符合上述一或多項風險指標，也不代表該等公司被用於 TBML 犯罪。我們建議進一步分析以減少誤判的風險，例如：從事多項商品貿易活動的一般貿易公司。

下列各節進一步分析涉及提供國際貿易且可能足以辨識出 TBML 的幾個私部門實體的類別（例如貨運承攬商與報關業者），或犯罪者經常作為 TBML 犯罪工具的類別（例如空殼與掛名公司），至於各金融機構與 DNFBPs 扮演的角色則在第 6 節說明。

空殼與掛名公司

運用空殼與掛名公司，已經成為許多不同種類洗錢活動，以及協助大量前置犯罪的關鍵特性。雖然 TBML／TF 犯罪與空殼或掛名公司之運用通常存在著大量的互動，但並非所有 TBML／TF 犯罪都涵蓋此等

公司，尤其是涉及運用合法供應鏈的情況。

然而，部分組織性犯罪集團、專業洗錢人員與恐怖分子資助者，確實會運用空殼公司建構其 TBML 犯罪，或在金融結算流程當中運用該等公司，並將最終實質受益人匿名處理以創造最大效果。另一方面，掛名公司則可提供將實體現金納入事業的便利機會，並可利用其與銀行往來關係，在各司法管轄區間移動現金。

貨運承攬商與報關業者

貨運承攬商在協助商品運送方面扮演了重要角色，其協助買方與賣方完成通常甚微複雜的海關與運送作業及流程。他們是決定商品移動最有效率運送方法的專家，且方法通常包括多種單一運送的模式。

對此，貨運承攬商可存取與檢視包括 TBML 指標的相關文件，包括：

- **商業發票（Commercial invoice）**－此文件雖然並無標準格式，但須包括例如交易各方、所運送商品以及商品名稱及編碼協調制度（Harmonised Commodity Description and Coding System）等資訊[17]。商業發票之內容，可能包括證明帳單係屬真實的陳述。
- **提貨單（The bill of lading）**，係由貨運承攬商或其代理人所開立的文件，用於確認收取所運送的貨物。此文件擁有三大主要功能：
  - ○ 此文件為具決定性的收據，確認商品已裝載。
  - ○ 此文件包括或證明載運契約的條款。
  - ○ 此文件可作為商品所有權的證明文件，且可將商品所有權移轉予指定寄銷方或合法持有人。

同樣的，報關業者無論與貨運承攬商具有關聯或互相獨立，會透過協助商品通過各項海關流程的方式，促使商品的進口與出口順暢運作。該等業者與進口商合作確認是否已備妥必要文件或許可，同時確保已支付正確的關稅及其他稅捐，以減少任何延遲狀況。其服務可能包括下列任何一項或全部：

[17] 前述協調制度是一種用於歸類貿易產品的國際標準化名稱與編號系統。此系統係以邏輯方式加以組織，亦即動物與動物產品屬於一個章節，而機器與機器用品則放在另一個章節。

- 確認商品的分類與價值，並確保使用了正確的商品編碼。
- 聯繫各政府機關及海關權責機關。
- 就進口限制或危險商品建議取得任何必要許可。
- 於必要時協助安排正確支付進口關稅與增值稅（VAT）。

雖然大部分司法管轄區並未要求貨運承攬商與報關業者負擔 AML／CFT 義務，但他們仍持有重要的貿易資料，可輔助各權責機關與金融機構持有的資訊，並用於察覺 TBML。這是非常重要的一個考量因素，因為打擊 TBML 時所需面對的關鍵挑戰，在於相關資料過於分散，亦即無任何單一利害關係人持有或可存取有助於辨識 TBML 的資訊。

各權責機關皆應考慮定期接觸這些關鍵國際貿易協助方，共同分享相關資訊與風險指標，以使其能夠更加瞭解 TBML／TF 犯罪。如此可以在現有聚焦於 TBML 公私協力夥伴關係中，加入貨運承攬商或報關業者，以建立全新或擴大涵蓋的成員。

常見貿易型洗錢技巧

FATF 於 2006 年報告中列出幾項建構 TBML 技巧：

- ***商品與服務帳單金額高報與低報***：此技巧的關鍵在於不實陳述商品或服務的價格以移轉價值。此類安排的關鍵運作層面，在於進口商與出口商共謀從事該等不實陳述。
- ***商品與服務多送與短送***：如上所述，此類安排涉及商品或服務數量的不實陳述，包括完全未移動任何產品的「虛假運送」交易。同樣的，此類安排仰賴進口商與出口商之間的共謀。
- ***商品與服務多次發單收款***：此類安排不需對價格作不實陳述，而集中在重複使用既有文件，用以證明同一批運送商品或提供服務的多次付款。犯罪者或恐怖分子資助者會在多個金融機構之間重複使用這些文件，使得單一機構難以辨識出此情況。
- ***虛假描述的商品與服務***：此類安排涉及商品或服務數量或種類的不實陳述，例如運送相對較不昂貴的商品，但會將其描述為較昂貴的品項或完全不同的品項，以證明價值的移動。

雖然這些技巧是獨立列示，但實務上犯罪者會在一次犯罪中混合多項方法，進一步使得交易鏈更為複雜。舉例來說，大部分複雜洗錢網絡可能合併使用虛擬運送與多筆帳單。單次運送可能涉及移動實際商品以創造合法的交易形式，或用於測試海關的遵循流程，使後續交易能夠針對虛擬運送交易使用多筆帳單，以掩飾資金的移動。

另一個傳統的 TBML 類型是***披索黑市交易***。中美與南美的販毒集團會使用這類交易對美國境內產生的販毒所得進行清洗。此犯罪活動背後的影響因素之一是貨幣管制，限制合法公司向外部供應商採購商品的能力。在這些限制之下，業者必須仰賴合作的貨幣交易商，將合法的當地貨幣兌換為美元。販毒集團使用此交易鏈，將非法美元自一個司法管轄區移到另一個管轄區。

通常在披索黑市交易犯罪中，貨幣中介會自販毒集團的現金控制方網絡取得美元，並使用該等美元付款給美國供應商。依據各犯罪的複雜度不同，貨幣中介可直接付款給供應商，或使用結構性存款將現金存入多個銀行帳戶，然後透過轉帳的方式將這些資金支付給供應商。美國供應商接著會將商品出口給位於中美或南美國家的公司，該等公司會將當地貨幣轉帳給當地貨幣中介。之後，貨幣中介會在扣除佣金之後，以當地貨幣支付給販毒集團。此犯罪活動確保在各司法管轄區之間並無任何現金的移動，因為跨境現金移動可能會被執法機會所發現與攔截。

下列案例說明了涉及披索黑市交易的犯罪，其突顯出這類犯罪涉及進口商與出口商對非法資金來源擁有一定程度瞭解的事實。

實例參考 2.9 披索黑市交易犯罪

2020 年 1 月，美國司法部（US Justice Department）起訴了六名哥倫比亞人，其等與一名印度人合作，從事涉及 TBML 的國際洗錢犯罪，及使用未獲許可的貨幣傳輸業者。

此犯罪的目的在於清洗毒品走私所得，且主要採用披索黑市交易類型的流程，使位於美國境內的現金不需要實際進行移轉。

此犯罪活動係以這些哥倫比亞人為中心而設計。該等人員被指控擔任貨幣中介，向位於美國各地的貨運承攬商收取犯罪所得，及收取匯入的國際匯款。這些實體現金會投入美國金融系統，避免引起懷疑，然後再移轉至由該名印度人所控管的公司銀行帳戶，該印度人遭控擔任共謀企業角色。此企業出口消費性電子產品給全球各地的買方，包括位於哥倫比亞的進口商。

該企業出口約略等同價值的消費性電子產品給哥倫比亞的進口商，後者則以支付披索給位於哥倫比亞之貨幣中介的方式支付產品價款，再由貨幣中介將款項轉交給毒品走私組織。這類安排使得毒品走私者不需要試圖跨國移動任何現金，因此降低了被察覺的風險。

此案例亦突顯了持續仰賴披索交易機制，以及濫用出口商與進口商間合法交易關係自美國移動等同價值至哥倫比亞的情況。

資料來源：美國

整體而言，由 FATF 全球網絡、各金融情報中心與私部門所提供深入見解獲得的一個關鍵發現，是上述這些技巧目前仍被普遍使用當中。然而，其他趨勢也持續在發展，包括運用未勾結進口商與出口商的合法供應鏈，或將犯罪現金納入貿易交易，包括代購交易的成長。

現有貿易型洗錢風險的評估

這些常見的 TBML 技巧，因先前幾種金融結算方法（例如第三方帳單結算）地強化，及支援整合現金至金融系統的各種較新技巧的發展，持續被搭配著使用。這些方法有些並未採用產品或交易文件不實陳述的技巧。

- **非法現金整合** — 考量 TBML 普遍存在於非法走私商品所得的洗錢流程，OCG 與 PML 需要一個能夠成功將非法現金整合到金融系統的方法，包括運用其他種類的金融機構。本報告已經說明了此類安排如何適用於傳統披索黑市交易犯罪，但此方法還有其他變化情況，亦即，希望處置非法現金的 OCG 或 PML 會試圖與其他有現金需求的 OCG 或 PML 合作。非法現金整合的另一個變種，在於運用代購網絡與滲透合法供應鏈。
- **第三方中介機構協助帳單結算** — 此種安排首先在 2006 年報告被提出，且持續存在於 TBML 犯罪當中，包括未涉及進口商與出口商間共謀關係的犯罪活動。有鑒於本報告係以廣泛讀者為標的，於此再次討論此風險，以協助那些發現自己被要求與完全不知悉及不相關的第三方結算帳單，能夠瞭解相關狀況。

非法現金整合

運用其他種類金融機構

雖然大部分 TBML 現金整合活動都涉及銀行，OCG 與 PML 也可運用其他種類金融機構，包括金錢或價值移轉服務（Money Value Transfer Service）或如哈瓦拉（Hawala）等非正式機制。舉例來說，虛假開立涉及 TBML 犯罪帳單者採用 MVTS 協助商品的付款，而非試圖透過銀行付款。OCG 或 PML 認為 MVTS 行業[18]對 TBML 的瞭解較不完整，因此 MVTS 不會質疑為何協助支付大額商業款項，而非由受款人採用適當方法進行。

此情況強化了 FATF 建議中列示的規範，即對顧客盡職調查與 MVTS 所分別須負擔之義務。監督人員與監管機關，應考量這些事業是否須制定具體 TBML／TF 風險降低政策，並控管其符合 AML／CFT 規定之情形。

互抵犯罪

披索黑市交易的一個變種，被稱為**互抵（offsetting）或補貼（compensation）**，由預計處分非法現金之 OCG 或 PML 與需求現金的 OCG 或 PML 合作。下列案例說明這些不同組織，如何互相合作以透過混合 TBML 與 SBML 犯罪的方式，來管理非法現金整合作業。

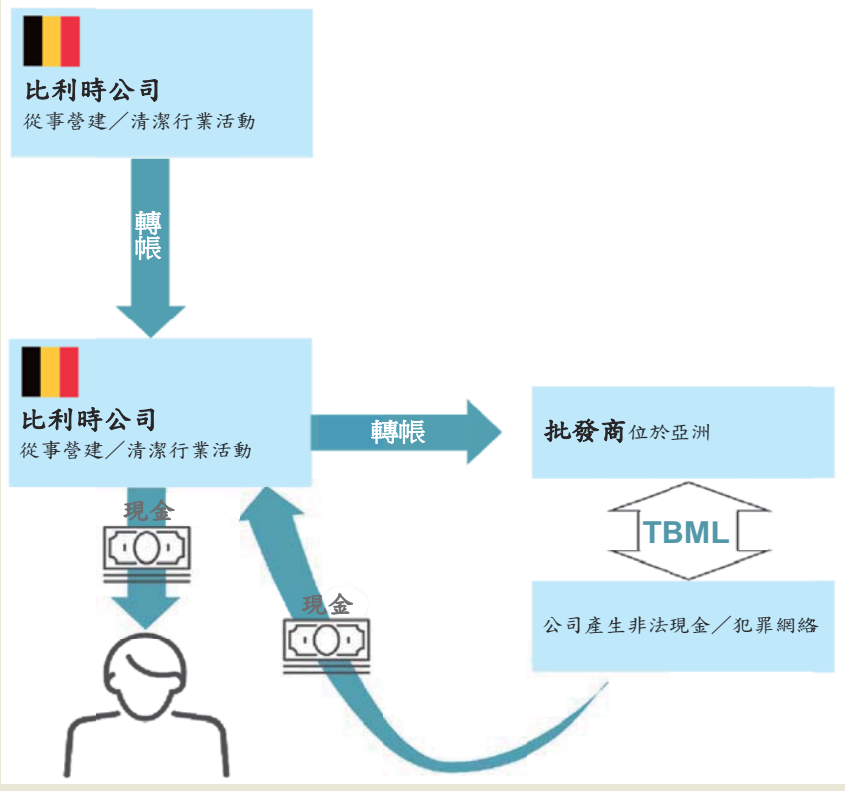
[18] 部分 PML 以操作 MSB 或與 MSB 具有密切關係而聞名，以確保維持對付款流程的掌控權力。

實例參考 2.10 補貼犯罪活動

多年以來，比利時權責機關已經注意到巴西或葡萄牙人設立或收購比利時營建或清潔公司的情形。

這些公司通常被用來掩護聘僱比利時境內未申報的勞工，且彼此串聯成網絡，通常具有設立與存在時間甚短的相同特性 — 主要是為執行特定交易而成立。

這些公司可快速且有效的由新公司取代，聘僱新的經理人，鑽體系漏洞並永久存在。這些公司會自其他犯罪者網絡收取犯罪現金，並以開立大樓維護服務帳單的方式，提供合法的交易形式；相關資金接著會被轉帳給位於亞洲的批發商。這些批發商會被指示代表比利時零售商採購商品，該等商品後續則透過相關 TBML 犯罪從事進口與銷售。



資料來源：比利時

代購網絡

代購網絡涉及代表富人購買需求商品的個人或網絡購物者，從形式上可規避海關控管或其他形式關稅限制。部分購物者也會代表 OCG 進行

採購，以在 OCG 與其資產之間建立斷點，代購者對於其是代表 OCG 的情形，具有一定程度的瞭解。此類活動一直被運用在 TBML 犯罪之中，且與披索黑市交易具有一定程度的類似性，由 OCG 或 PML 提供當地貨幣（犯罪所得）給這些代購者，後者則用於支付欲購買商品，並將該等商品運送至其他司法管轄區，然後轉交給 OCG 或 PML。

此種犯罪活動的變形，包含由代購者使用信用卡支付購買商品的價款，而 OCG 或 PML 則以其犯罪所得償還其信用卡款。舉例來說，學生多次購買攜帶式電子產品，如智慧型手機與平板電腦。其信用卡費用接著則由疑似從事毒品走私所得洗錢活動的公司，以電子轉帳的方式結算。如此不僅可以進行犯罪所得的清洗，相關電子產品也疑似被送到亞洲與中東的灰色市場（grey market）進行銷售。此流程可與傳統 TBML 技巧並用，包括不實陳述所購買之商品，以提高使用犯罪所得轉帳付款的獲利。

滲透合法供應鏈

於此情況下，OCG 或 PML 會購買合法事業的股份（該等事業可能存在、也可能不存在財務問題），並持續以該公司的供應鏈作為將非法現金整合至金融系統的手段。OCG 或 PML 並未試圖變更其所投資公司的實際營運，也不必然會採用前面提到的任何常見 TBML 技巧。其目標在緩慢且穩定的提高非法現金整合至事業的金額，同時維持既有的供應鏈關係。此方法對權責機關或金融機構察覺 TBML 犯罪帶來了挑戰，然而，從實例參考 2.6 所列案例可知，調查不法現金扣押及發現複雜的 TBML 仍存在其可能性。

第三方中介機構協助帳單結算

第三方中介機構自從在 2006 年度報告首次被提及後，一直存在於 TBML 犯罪中。該等機構通常存在於帳單結算流程之中，且通常與運用專戶記帳貿易有關，主要係因缺乏金融機構監督。依據其在相關 OCG 或 PML 交易鏈所處位置不同，該等機構可達到雙重目的。

舉例來說，若於滲透合法供應鏈並在無任何不實陳述之情況下採購商品，OCG 可能將先前未知的第三方（通常為負責整合犯罪現金的公司）納入交易，以支付該等商品的款項。如同空殼或掛名公司章節所述，這些第三方可能位於有實質受益人隱私條款的地點。

雖然金融機構顯然普遍知悉這些第三方結算帳單的風險，無可疑的收款公司，可能不會質疑為何其交易關係突然擴充並納入先前未知的第

三方，而該等第三方可能位於不同的司法管轄區。

即使這是與 TBML 犯罪有關且長期存在的風險，但 DNFBPs 並未進行系統化通報，例如：由可能接觸該款項的稽核人員或會計師通報。對此技術的更高程度認知，可提高其申報的頻率，及發展改善預防策略來，瓦解 TBML 犯罪。下列案例突顯第三方中介機構的角色，及於廣泛的 TBML 犯罪中濫用空殼公司的情況。

實例參考 2.11 第三方結算

紐西蘭金融情報中心（New Zealand Financial Intelligence Unit，NZFIU）收到了多份與付款給紐西蘭水果出口公司有關的可疑活動報告，該等款項來自於東歐的銀行帳戶，且帳戶之登記持有人為位於高風險司法管轄區的空殼公司。可疑活動報告顯示，該紐西蘭公司在 18 個月期間內，從這些海外帳戶收取了約 150 萬美元的款項。

NZFIU 調查發現轉帳給紐西蘭公司的款項，係合法出口紐西蘭水果至東南亞司法管轄區的款項。訊問時，該公司的代表人在遭到質疑時，無法解釋為何款項來自於空殼公司帳戶，且該等帳戶與實際收到出口商品的公司無任何已知關係。

處理該交易的各紐西蘭銀行，將所收到作為付款證明的付款通知，提供給金融情報中心。這些通知單明顯為偽造的，且載明交易為針對紐西蘭公司出口「陶瓷磁磚」向位於東歐的公司收取款項。相關通知單由聲稱為紐西蘭公司經理的人員所「簽署」，但經過調查發現該公司並未有此姓名的員工。

NZFIU 評估，這些款項（從其高帳戶活動判斷，約有數千萬美元）是根據地在東歐的複雜 TBML 犯罪的一部分，相關非法資金被轉換為貿易商品，並送到不同司法管轄區轉售，以產生乾淨的資金。

資料來源：紐西蘭

貿易型資助恐怖分子

只有少部分受訪者提到了貿易型資助恐怖分子（TBTF），尤其是在編製 NRA 時納入考量，並認為 TBTF 在建構 TBML 犯罪並移動價值時非常有幫助，為恐怖分子資助者提供了相同的機會。

實務上，TBTF 犯罪能夠、也確實採用常見的 TBML 技巧。該等犯罪活動也涉及了合法公司及透過供應鏈執行的交易，直至相關資金最終交付給恐怖分子組織為止。

在下列案例中，恐怖分子採用既有的供應鏈，將資金自一個國家移動到另一個國家，規避直接互相付款的必要性，並且以商品作為移動價值的方法。

實例參考 2.12 濫用既有貿易鏈為恐怖分子移動資金

案例 1：

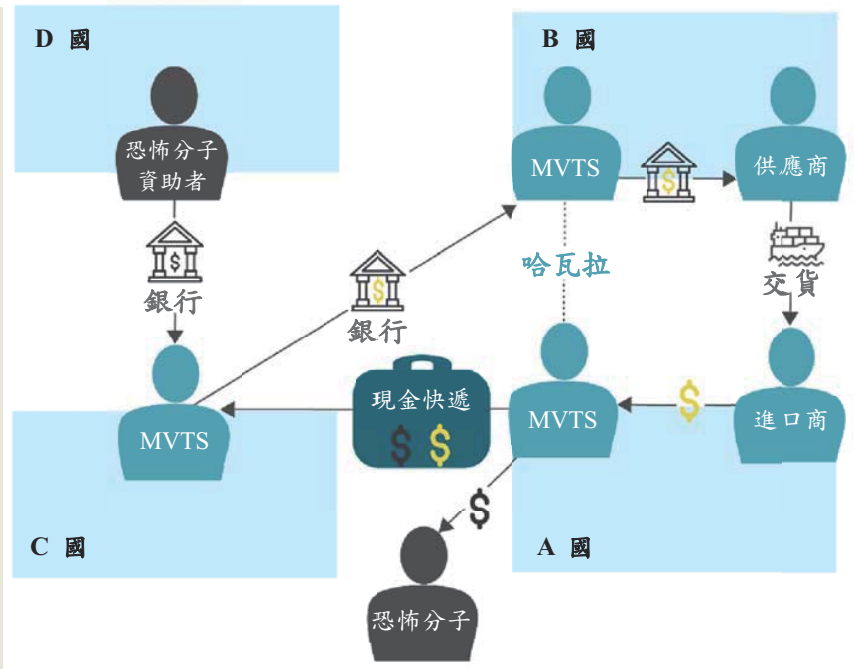
位於 A 國的進口商希望透過雙方之間的合法貿易，向位於 B 國的供應商採購商品。然而，商品的款項卻是由位於 C 國的恐怖分子組織成員所支付。供應商會在收到款項之後，將商品運送給進口商。進口商會在收到貨物之後，以現金將商品的價款支付給位於 A 國的同一恐怖分子組織成員。該恐怖分子組織只要採用此方式，就能夠以商品為貨幣，透過合法貿易體系將現金從 C 國移轉至 A 國。該等商品後來被以色列海關查獲並予以沒收。

案例 2：

另一個案例運用了 MVTS 與哈瓦拉（Hawala）網絡，以安排 A 國進口商與 B 國出口商之間商品貿易的結算。進口商透過 A 國的 MVTS 支付運送商品的款項，A 國的 MVTS 透過哈瓦拉網絡將資金移轉給位於 B 國的 MVTS。位於 B 國的 MVTS 接著透過銀行將款項轉帳給出口商。為了進行結算，位於 A 國的 MVTS 透過現金快遞將款項交付至位於 C 國的 MVTS，後者則透過銀行轉帳支付給位於 B 國的 MVTS。

接著，一名位於 D 國的恐怖分子資助者運用此貿易網絡，將資助恐怖分子的資金轉帳給位於 A 國的恐怖分子組織。該組織再將一筆款項轉帳給位於 C 國的 MVTS，後者則將該等款項轉帳給位於 B 國的 MVTS。該款項接著會從位於 A 國的 MVTS 為結算目的原須轉帳給位於 B 國的 MVTS 的款項中扣除。位於 A 國的 MVTS 則會將相同款項支付給當地恐怖分子組織。

在此案例中，恐怖分子資助者滲透了供應商與進口商的貿易鏈，運用共謀 MVTS 將預計用於資助恐怖分子的資金納入貿易交易，並因此避免直接付款給恐怖分子組織。



資料來源： 以色列

在下列案例中，可疑恐怖分子運用虛假付款通知技巧，協助將資金轉帳給恐怖分子。

實例參考 2.13 貿易型資助恐怖分子案例

義大利權責機關在與兩名兄弟有關的個人與企業銀行帳戶中，發現了可疑的金融活動。該等兄弟與從事汽車批發與零售貿易的公司有所往來。相關汽車的採購與移動表面上屬合法，然而引人懷疑之處在於汽車銷售背後的經濟活動存在重大差異。舉例來說，該公司的帳戶存在鉅額現金存入與提領的活動，而且個人銀行帳戶也存入來自其他商業實體的款項。義大利權責機關在初步分析時懷疑此屬洗錢網絡，且係利用虛偽的付款通知單犯罪。然而，在進一步調查後，發現了相關活動與資助恐怖分子有所連結，並取得了公開來源資料的佐證。其關鍵風險指標包含與出口汽車有關的司法管轄區打擊資助恐怖分子能力薄弱及交易的商業實體曾涉資助恐怖分子活動。

上述活動在後續可疑交易報告及義大利警方驗證的情報獲得了確認。跨國汽車交易的獲利，被移轉給中東的進口／出口公司，然後再轉給恐怖分子組織。

資料來源： 義大利

服務型洗錢

服務型洗錢（SBML）並非貿易型洗錢（TBML），但包括公開來源報告之內容[19]，顯示風險持續提升，在此談及僅供參考。然而，此兩類洗錢的根本差異，在於 SBML 犯罪係運用服務或其他無形資產的貿易，來掩飾與合理化非法所得的移動。

本報告雖未詳細探索 SBML 現象，此犯罪活動可能形成進一步的複雜度，使各權責機關或受規範實體更難以成功察覺與瓦解洗錢活動。舉例來說，針對像是顧問或諮詢服務這類服務來說，就很難評估服務購買方與服務提供方之間關係的合法性。此外，服務型洗錢也未交易任何實體商品，而實體商品通常會編製進口或出口資料。下列各項服務與行業被視為很容易受到 SBML 所影響：

- 博奕，尤其是線上博奕服務提供方；
- 軟體提供方，包括博奕與如電子銷售點服務的商業軟體；
- 金融服務，包括虛擬資產財富管理；
- 顧問與諮詢服務；
- 商標與類似的無形品項，例如智慧財產權。

[19] 保衛民主基金會政策簡報：服務型洗錢：下一個非法金融前線（Foundation for Defense of Democracies policy brief: Service-based money laundering: The Next Illicit Finance Frontier）

第 3 節　打擊貿易型洗錢所需面臨的挑戰

儘管 FATF 全球網絡與廣泛專家社群都非常重視 TBML，對各司法管轄區而言，打擊此型態洗錢依然存在著諸多挑戰。前述 2006 年、2008 年與 2012 年報告，及世界海關組織（WCO）與艾格蒙聯盟合作發布的「海關與金融情報中心合作手冊」（Customs-FIU Cooperation Handbook）[20]，都強調 TBML 是尤其複雜的洗錢形式，對察覺與調查流程的各個階段都帶來多種困境。這些困境，加上國際合作的各項挑戰與私部門在辨識 TBML 犯罪方面所遭遇的困難，都導致全球截至目前為止，只有相對較低的 TBML 調查成功案例數。本節彙整顯著影響各司法管轄區為有效打擊 TBML，執行各項措施時最關鍵挑戰。

缺乏瞭解與警覺

供應鏈中各個負法律合規義務的組織，只瞭解犯罪的其中一塊拼圖，而非全貌，因此也無法足夠察覺貿易型洗錢的各種跡象。

FATF 於 2006 年與 2008 年針對 TBML 發表的報告，讓全球各機構開始注意到 TBML，而執行 NRA 則使各司法管轄區更加瞭解 TBML 風險。其他國際機構、學術界與全國性權責機關就 TBML 主題發布的報告數量持續增加，也提供了對 TBML 的寶貴深入見解，並因此使各公部門與私部門行業更加瞭解此現象。然而，如同許多受訪者提到的，部分權責機關對於 TBML 仍然僅擁有基本的瞭解，且可能並未知悉此犯罪型態

[20] 請參閱該兩組織官方網站取得手冊的公開版本。

的更複雜內容。對已深入瞭解 TBML 的權責機關來說，持續跟上不斷演變的 TBML 風險步調，也是一項長期的挑戰。隨著權責機關提高對 TBML 的認知，採取行動調整相關措施來更有效的打擊這些犯罪，同時犯罪者也持續找尋各項新機會，透過濫用國際貿易體系的方式合法化其犯罪所得。

這些挑戰的重要關鍵因素之一在於 TBML 犯罪的相對複雜度。TBML 犯罪可能涉及運用多種行業與商品作為移動價值的方法，從二手車到花卉都有，換言之，沒有兩個犯罪活動是完全一樣的。此外，供應鏈中各個負法律合規義務的組織，只瞭解犯罪的其中一塊拼圖，而非全貌，因此也無法足夠察覺貿易型洗錢的各種跡象。。這些組織即使擁有察覺該犯罪所需的知識，也一樣可能會忽略該活動。因此，權責機關也難以辨識較高風險行業，並據以排定優先次序以及採取行動來降低風險。

線上商業機會的持續成長，為國際貿易開啟了全新的領域， 同時，這也對瞭解 TBML 方法增加了額外的挑戰，而且公部門權責機關為監督與分析貿易交易所採用的技術，也可能無法跟上犯罪的步調。各項新技術以及貿易的數位化已使貿易營運的速度加快，並因此導致權責機關須修改其策略，且不僅需要發展與犯罪者「犯罪手法（modi operandi）」有關的知識，也必須瞭解現代貿易體系的特性。為了即時在上千筆合法交易中辨識可疑貿易與金融交易，公部門權責機關亦須將其用於分析金融與貿易資料的工具與技巧加以數位化。

國內協調與合作

先前研究顯示，國內各權責機關間的協調困境，是打擊 TBML 行動的最重要議題。依據本報告取得資料，缺乏協調仍是各權責機關所面臨的最大疑慮，且影響了 TBML 的察覺與調查。

FATF 建議要求各司法管轄區應確保其前置犯罪調查人員，同時都具備自行調查相關洗錢活動能力，或能夠將相關案件轉交其他機構進行後續相應的金融調查。然而，與此項挑戰有關的因素之一，在於調查權責機關會強調前置犯罪，並將洗錢調查的順序往後排，包括 TBML，尤其當洗錢調查並非其主要功能時更是如此。舉例來說，警方主要強調前置犯罪的調查，稅捐機關則可能主要強調稅務舞弊，而海關單位則可能強調商業貿易詐騙與走私，洗錢案件的順序則較低。

有鑒於 TBML 是以利用貿易體系弱點為基礎，其某些關鍵要素可能與其他貿易犯罪類似。這樣的類似性可能導致權責機關將所發現的犯罪活動錯誤歸類為走私或詐騙，而非 TBML。例如，若權責機關發現貨物檢附的文件存在差異，他們可能會傾向停止運送，並控告貨運承攬商從事海關詐騙或違反智慧財產權，而未調查是否可能為 TBML 活動。

如同 FATF 建議所述，國內協調與合作是有效 AML／CFT 體系的基本要件，要求政策制定者、金融情報中心、執法機關、監督人員與其他各相關權責機關制定有效的機制，以互相合作與（若適當）協調及交換資訊。此準則確保各司法管轄區都能夠將負責蒐集、分析與儲存不同種類資料的權責機關，與負責調查前置犯罪及洗錢的權責機關整合在一起。

國內協調與合作，是有效 AML／CFT 體系的基本要件。

儘管如此，許多受訪者都提到了國家權責機關之間缺乏資訊分享或該分享機制的無效率，成為打擊 TBML 的關鍵挑戰。如同「FATF 與區域性防制洗錢組織相互評鑑報告（FATF and FATF-style Regional Body Mutual Evaluation Reports）」所述，截至目前為止受評鑑的許多司法管轄區，都已設置各權責機關間交換金融情報的必要法律架構，包括金融情報中心與執法機關。然而，在部分情況下，此合作有效性的不足可能導致權責機關沒辦法察覺並調查洗錢（包括 TBML），及提升沒收犯罪的所得。

調查人員、金融情報中心分析師與其他相關專家在分析與整合稅務、貿易與金融資料方面遭遇的困難，則是另一個常見的挑戰。為了適當辨識 TBML 活動，權責機關通常必須分析與比對來自多個來源的大量的資料，其中部分可能由不同的機構所持有，例如海關資料，可疑交易報告（STRs）資訊及犯罪紀錄。每個持有資料的機構，都可能將資料儲存在其內部 IT 系統，且可能未設置資訊分享機制，無法讓其他機構、執法機關或金融情報中心能夠即時存取該等資料。即使設置了前述機制，該等機構也可能不允許其他資料庫以自動化的方式交叉索引資料，因此相關權責機關必須投入額外時間與資源，進行人工比對與分析作業。舉例來說，通報金融情報中心的金融資料（尤其是 STRs）與進出口資料，可能以彼此無關連的方式儲存，或彼此存在資料品質與一致性問題。

國際合作

即時提供適當國際合作，對有效察覺與調查跨越多個司法管轄區的任何犯罪活動非常重要。對 TBML 而言，這類合作尤其重要，因為洗錢者通常會利用在某個司法管轄區登記的掛名公司，然後在多個司法管轄區之間進行資金轉帳與商品運送。所有這些拼圖合併構成完整犯罪狀況，且只有各相關司法管轄區互相提供必要協議才能夠解決。

洗錢者通常會利用於一個司法管轄區登記的掛名公司，然後在多個司法管轄區之間進行資金轉帳與商品運送。

TBML 可能跨國進行，例如前置犯罪通常是在 TBML 發生的司法管轄區以外的地區進行。因此，為了最終調查與起訴 TBML，各司法管轄區都須相當仰賴有效且運作順暢的國際合作管道，以確認前置犯罪是否已發生。

然而，各司法管轄區仍繼續遭遇缺乏有效資訊分享的困境，因此影響其辨識與調查 TBML 的能力。其中一個挑戰是在提供資訊並回應外國合作夥伴的要求時，沒有重大的延誤。有時延遲是因為提出要求之司法管轄區的國內合作問題所導致，因為所需資訊可能會由不同權責機關持有，且將其編製成一份報告可能會花費許多時間。此外，當一個司法管轄區的權責機關因應其他司法管轄區的要求而扣押商品時（例如當懷疑商品被用於 TBML 犯罪時），就會要求進口商依據扣押期間按比例支付持有與存放商品的額外成本，對進口商加諸額外的財務壓力。

調查與起訴

如同 FATF 的 2018 年專業洗錢報告（2018 Professional Money Laundering report）所提到的，TBML 是 P 專業洗錢人員最偏好的方法之一，且通常會與掛名公司[21]、掛名負責人（front men）及其他洗錢技巧合併使用。在專業洗錢網絡中，洗錢活動（包括 TBML）是由一個犯罪集團所執行，而前置犯罪則由其他犯罪者負責執行。這種洗錢活動與前置犯罪之間的斷點，代表了前置犯罪的調查人員（毒品走私打擊小組、反貪腐機構等）可能缺乏調查相關洗錢活動的足夠專業。遭遇國內合作困境的各司法管轄區，可能會導致僅起訴犯罪者的前置犯罪（例如毒品走私或人口販運）與其他貿易犯罪（例如增值稅詐騙）及走私。

至於任何其他種類洗錢活動，起訴 TBML 則須證明洗錢標的之資金

[21] 請參閱 FATF 與艾格蒙聯盟合作針對空殼與掛名公司其他特性發表的「隱匿實質受益人（Concealment of Beneficial Ownership）」報告。

或資產，係屬犯罪所得且被告已知。檢察官可能能夠蒐集足夠的證據，證明洗錢犯罪的客觀面，亦即犯罪所得如何轉換與移轉，但知情規定尤其難以證明，即使使用案例的事實面資料佐證也一樣。這點尤其適用於第三方洗錢或前置犯罪係於其他司法管轄區進行之情況。舉例來說，被告可能陳述其於收到資金時並不知悉資金的非法來源，且起訴將須取得可證明並非如此的足夠證據。若犯罪者另外也濫用合法貿易作業，則非法與合法資金通常會混合在一起，對權責機關在辨識洗錢資產時帶來了額外的挑戰。這些困境再加上整體缺乏對 TBML 的知識與瞭解，通常會導致僅起訴前置犯罪，TBML 活動則仍成為漏網之魚。

私部門角度的各項挑戰

依據 FATF 建議，特定私部門行業應擔負執行各種 AML／CFT 措施的義務，包括客戶盡職調查、紀錄保存及申報 STR。這些措施之目的在於限縮犯罪者洗錢及資助恐怖主義的能力，同時確保各金融機構與 DNFBPs 擁有足夠的工具，可自保以免於被濫用在洗錢與資助恐怖分子目的上。即使犯罪者試圖運用這些事業的服務，此等工具也應使相關實體能夠確認對該活動的懷疑，並即時通報金融情報中心。

金融機構與 DNFBPs 通常處於打擊洗錢的前線，因為他們可能涉及移動價值（例如代表客戶執行交易），或對其客戶的金融活動具有獨特的瞭解（例如會計師與律師）。在此同時，私部門行業也因身為打擊洗錢與資助恐怖分子的前線，而面臨了重大的挑戰，因為犯罪者會不斷的改善其洗錢方法，且私部門必須隨時跟上。另外也須注意的是，大部分貿易與生產鏈公司，都不需負擔與 FATF 建議規範類似的申報義務（除非落在建議中定義的商業活動範圍內，例如貴金屬或寶石交易商），且通常也不在許多司法管轄區的國內法律架構內，因此各金融機構與 DNFBPs 必須負責察覺這些活動的潛在情況，並以即時申報 STR 的方式，適當通報金融情報中心。

貿易型洗錢具有高度彈性，且能夠運用任何行業或商品。

大部分私部門受訪者（主要為金融機構）都將 TBML 視為最難察覺的洗錢活動類型。TBML 具有高度彈性，且能夠運用任何行業或商品，使得金融機構難以排定資源的優先順序，及將最新深入研究結果轉換為規則與遵循系統。實務上，TBML 犯罪可能包括大量掛名公司，並於多

家銀行之間進行資金轉帳，代表各個涉及的金融機構都只參與此網絡的一小部分。此 TBML 犯罪的片段特性，使得各金融機構無可避免的難以依據對整個交易鏈的分析來辨識潛在 TBML 犯罪，且在許多情況下甚至限縮其察覺證明文件與顧客基本資料間矛盾的能力。

金融機構所需面臨的另一項挑戰，在於驗證其顧客所提供資訊的正確性。此情況可能是所有洗錢類型的共通問題，因為缺乏公開登記資料，可能使金融機構難以驗證客戶的地址、所得或其他客戶相關資料。TBML 犯罪則會讓這些挑戰變得更加困難。舉例來說，在貿易交易的盡職調查流程中，一名客戶可能會將帳單、契約或其他增補文件的影本提供給銀行，以佐證資金從一個司法管轄區移轉到另一個司法管轄區。若銀行在存取海關資料時遭遇困難，其便無法即時驗證文件的真實性、商品是否已實際運送以及其數量和描述是否與契約相符。許多 TBML 技巧都需要買方與賣方共謀，且有時甚至是由同一個人或同一群人對交易各方擁有控制能力。於此情況下，取得顧客交易對手實質受益人相關資訊，將可協助金融機構察覺 TBML。然而，這些資訊有可能無法取得，例如，若交易對手過去皆非金融機構的顧客，或並無受益人資訊的公開登記資料。交易對手亦可能設立於金融機構執行付款所在管轄區以外的司法管轄區，使得金融機構在蒐集此資訊時遭遇更多困難。

金融機構在辨識 TBML 犯罪時經常會面對的另一項挑戰，在於估算貿易商品的「公平價格（fair price）」。此挑戰尤其與採用價值高報／低報技巧的 TBML 犯罪有關。犯罪者於這些犯罪中會將貿易商品標示比正常市場價格來得高或低，試圖以貿易交易掩飾額外價值的移動。金融機構通常僅能取得貿易商品的模糊描述，且確認「公平價格」可能需要動用大量資源，並可能僅依據公開來源資訊。此外，犯罪者所運用的部分商品並未於公開市場交易，因此無法取得可用於比較的價格。

此外，因為 TBML 涉及國際貿易，提供給金融機構的文件通常採用不同格式與語言編製，代表了驗證作業必須以人工進行。金融機構因此必須投入額外時間與資源，包括聘僱高知識水準員工，且因此對於法遵預算較為有限的小型金融機構可能造成更多困難。

在此脈絡下，以信用狀或跟單託收等付款方法，因顧客相較於專戶記帳貿易須提供更多文件給金融機構，而被私部門視為較不容易受到 TBML 所影響。因此，洗錢人士可能將專戶記帳貿易視為較適合採用的

方法，因為金融機構對交易的監督能力有限。於此同時，即使金融機構懷疑其顧客涉及 TBML 並終止與顧客的關係，顧客仍能夠在其他銀行開設新帳戶。

第 4 節　打擊貿易型洗錢之各項措施與最佳實務

FATF 建議提供 AML／CFT 措施的完整架構給司法管轄區，用於有效打擊洗錢與資助恐怖分子。於此同時，各司法管轄區對於如何將該等措施轉換為國內法律與監管架構及實務應用上，則具有一定程度的決定彈性。此彈性係依據各司法管轄區的治理環境、風險與其他結構性因素來決定。

本節旨在彙整一些用於打擊 TBML 的既有優良實務，以協助各司法管轄區強化其 AML／CFT 措施的有效性，同時也承認並無「一體適用（one-size-fits-all）」的方法。下列部分實務可能超過 FATF 建議所列措施的範圍，但可能仍有助於各權責機關，在考量國內 AML／CFT 架構與洗錢／資助恐怖分子風險之組成與特性的前提下，作成相關決定。

讀者亦應參考 2006 年、2008 年與 2012 年 TBML 研究報告的相關章節，以瞭解可能提高國內 TBML 打擊措施效果的其他實務。

提高對貿易型洗錢的瞭解

如前述章節提到的，建立對 TBML 犯罪足夠的瞭解，應當作打擊此形式洗錢之任何策略的基礎。從公部門角度來看，此情況通常代表需

辨識與評估司法管轄區內存在的各項 TBML 風險，包括所涉及的各經濟行業與金融工具。這有助於公部門與私部門相關人員依據其資源狀況，適當調整更廣泛的洗錢策略。然而，如同許多受訪者提到的，缺乏對 TBML 犯罪的知識與瞭解，不僅是私部門的常見挑戰（可能沒有足夠資源追蹤最新的 AML／CFT 發展），也是公部門所面臨的挑戰。

各司法管轄區可能使用不同來源的資訊，發展公部門與私部門對 TBML 犯罪的瞭解。其中一個資料來源是 NRA，因為該報告通常彙整了司法管轄區內所存在洗錢／資助恐怖分子風險的相關資訊，有時甚至會按具體行業細分。NRA 雖然應能反映司法管轄區內完整的 TBML 風險及其組成要件，但可能比較適合已經對 TBML 擁有一定程度瞭解與知識的專家採用。此外，部分國家並未公開 NRA 資料。因此可能需要投入額外的努力，讓更廣泛的大眾能夠取得與瞭解 NRA 的內容。

此報告的目的，並非為各司法管轄區或私部門機構提供如何辨識與評估其 TBML 風險與弱點的指南。事實上，多個區域所採取的各項行動，都將重點放在提升 TBML 的知識，及改善對 TBML 風險的瞭解。這包括許多全國性與區域性經驗，範圍涵蓋提供 TBML「基本」知識、聚焦於金融機構顧客，乃至為需要更多進階訓練的專家提供相關行動。該等行動可能由不同機構推動與規劃，例如：

＊私部門實體尋求提升其顧客的警覺性以降低顧客涉入 TBML 犯罪的可能性。

實例參考 4.1 荷蘭銀行的行動

荷蘭的一家金融機構為其所有商業顧客提供一份傳單，以提升顧客對 TBML 風險的認知。傳單內容包括一個 TBML 犯罪的案例，及顧客有任何與 TBML 及其業務相關問題時，能夠聯絡的電子郵件信箱。

資料來源：荷蘭

＊金融情報中心或其他權責機關，希望針對被視為可能受 TBML 影響的行業，提升其申報 STR 的水準與品質。

實例參考 4.2 金融情報中心與指定之非金融事業與人員的合作

2019 年，德國金融情報中心透過發布一系列定期演說，及透過工商會接觸的方式，為 DNFBPs 與其他受規範實體（例如汽車貿易商與藝術品／古董貿易商）提供指南。此行動預計會在 2020 年持續進行，並將新冠肺炎（COVID-19）疫情相關限制納入考量。

該指南使得登記申請數量大幅增加（向金融情報中心登記為申報實體），及於貿易展與演講會場向金融情報中心及其代表人所提出問題的品質有所改善，代表了對洗錢風險的瞭解亦有所改善。

DNFBPs 在網站登記之後，金融情報中心會將洗錢防制及 STR 申報的態樣與其他相關資訊提供給 DNFBPs。為了接觸尚未向金融情報中心登記的商品貿易商，金融情報中心也密集的與相關協會進行對話，以提升其成員對洗錢的警覺性。

資料來源：德國

實例參考 4.3 提升金融機構對 TBML 之瞭解

「防制洗錢與打擊資助恐怖主義產業合作夥伴」（The Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership，ACIP）匯集了特定產業從業人員、權責機關、執法機關與其他政府實體，合作辨識、評估與降低新加坡所面臨洗錢、資助恐怖分子與資助武器擴散的關鍵風險。ACIP 的一個工作小組著眼於 TBML 風險，整合了來自各銀行（尤其是專門經營貿易融資的銀行）、權責機關、執法機關與專業服務組織的深入見解。此工作小組針對 TBML／貿易融資風險的管理編製了一份業界最佳實務報告書，且亦載明金融機構預防措施與訓練及認知技巧等資訊[22]：

* 金融機構應為其員工提供與察覺及預防 TBML 風險有關的具體且目標性訓練，及提升該相關員工的風險認知及能力，以降低洗錢／資助恐怖分子／資助武器擴散風險，並且遵守監理機關規定。

[22] https://abs.org.sg/docs/library/best-practices-for-countering-trade-based-money-laundering.pdf

＊金融機構應為所有相關員工提供訓練及相關資訊，著重於重大監管變動與各項新風險，以及可用於管理 TBML 風險的各種方法。

＊前述訓練應依據金融機構之風險評估結果定期更新，且應符合金融機構的各項政策與程序，並應考量適用於該金融機構的情況，例如所提供產品、營運據點及顧客類型。

資料來源：新加坡

＊國際機構應在其國際計畫中提供 TBML 指南，或強化與私部門的合作。

實例參考 4.4 提升金融機構對 TBML 之瞭解

2020 年 7 月，艾格蒙聯盟資訊交換工作小組（Information Exchange Working Group of the Egmont Group，Egmont IEWG）核可了一本以「大規模跨國洗錢犯罪之結論（Conclusions from large scale cross-border money laundering schemes）」之專案結果撰擬的「案例彙編（Case Book）」。此專案之目的，在鼓勵透過整合金融情報中心過去自「洗錢事務所（Laundromats）」所取得深入資訊，討論與發展可用於辨識大規模跨國洗錢犯罪網絡、模式與指標的可能方法。

專案的一個工作小組，致力於依據金融情報中心過去察覺與分析大規模跨國洗錢犯罪的多元專業與經驗，蒐集相關案例研究。不同金融情報中心觀察到，犯罪者在這類犯罪中廣泛採用 TBML 技巧，以掩飾與移動犯罪所得。因此，該案例研究蒐集作業的目的是聚焦於 TBML 犯罪及不同 TBML 技巧的使用。合計共有超過 20 個金融情報中心為此工作小組作出貢獻，因此能夠整合多元 TBML 案例研究並編製成「案例彙編」，說明犯罪者如何能夠為洗錢目的而濫用國際貿易體系。

各金融情報中心可自艾格蒙聯盟的安全網站下載此「案例彙編」。其他國內各權責機關及特定報告實體，則可透過其相關金融情報中心存取相關內容。

資料來源：Egmont IEWG

實例參考 4.5 歐洲刑警組織金融情報公私協力夥伴關係（Europol Financial Intelligence Public Private Partnership，EFIPPP）

EFIPPP 是防制洗錢與反資助恐怖分子領域第一個成立的跨國資訊分享機制。該夥伴關係是在 2017 年 12 月啟動，作為「歐洲刑警組織 - 執法、監理及銀行業國際金融機構高級合作方案（Europol-Institute of International Finance High Level Project of Law Enforcement, Regulatory and Banking Sector）」的試行專案。其目標在創造一個平台，讓國家間與各行業間互相信賴的夥伴能夠互相交換資訊。此機制提供了實務的意見（例如態樣），致力於將可疑交易報告，從遵循導向轉為情報導向，以優化其成效。

EFIPPP 聚集了來自 11 個歐盟會員國及歐盟以外 4 個國家的執法機構、金融情報中心及／或監理機關，擁有國際營運據點的 25 家金融機構，歐盟各機構與組織，一個國際組織，及擔任觀察員的多個民間社團組織與研究機構。EFIPPP 提升了各界對此議題的興趣：從 2017 年的 15 家金融機構與 6 個參與國家，到今日的 25 家金融機構與 15 個參與國家。EFIPPP 近期也通過且目前正在採用一個全新的治理模型，以架構 EFIPPP 在未來幾年的成長基礎與優先要務。EFIPPP 的會員每季會以專責工作小組的模式開會一次，並透過專屬的專家平台持續交換意見。

EFIPPP 過去針對 TBML 態樣所進行的研究，都與毒品走私及增值稅詐騙有關。此態樣聚焦於在毒品相關犯罪（生產、種植、走私與配銷）、洗錢及稅務舞弊之間建立的關係。

資料來源：歐洲刑警組織（Europol）

實例參考 4.6 亞洲開發銀行（ADB）的 TBML 經驗

亞洲開發銀行（ADB）在 2019 年發表了一份簡要有效的實務報告，內容檢視了貿易融資營運的 AML ／ CFT 遵循活動。此報告提供了貿易融資的實務理解，及這些部門如何在商業銀行中運作。

此外，ADB 也與多個公部門與私部門利害關係人合作，採用亞太防制洗錢組織（APG）2012 年報告的提案，處理貿易資料品質與整合相關

的挑戰，以改善對 TBML 的察覺能力。2019 年 3 月在新加坡舉行的 AML／CFT 研討會，促進了貿易資料點的發展，且可供納入公部門與私部門既有或新興回饋意見圈之中加以考量。該等貿易資料將提供給權責機關與私部門實體使用，以改善 STR 的申報品質。其內容可能包括所發現 TBML 技巧的更多具體資料、貿易交易對手的重要資訊及交易與運送方法的詳細資料。

透過 PPP 採用此種方法，亦有助於整合相關資料持有人、擴大對風險的瞭解，及處理與資料片段化有關的阻礙。

資料來源：亞洲開發銀行

雖然各司法管轄區可自行決定提升對 TBML 風險瞭解的最佳方法，但各司法管轄區也應確保為擴大公部門與私部門對 TBML 的瞭解所採行的各項措施，能夠與其風險層級相符。

各金融情報中心蒐集的金融情報

各金融情報中心身為其所在國家的金融情報集散地，擁有許多有助於發現潛在 TBML 案例的寶貴資訊來源。各金融情報中心可透過整合不同來源的資料，擁有察覺與分析可能 TBML 犯罪的獨特地位，並可將適當的金融情報分送給其國內與國際夥伴。因為各金融情報中心的分析經常被當作進一步公開行動的基礎，所以金融情報中心對 TBML 擁有充分瞭解，並且擁有足夠的資源可編製相關金融情報是非常重要的。雖然金融情報中心在 TBML 案例中所使用資訊的來源，及所執行的分析，可能與其他洗錢／資助恐怖分子案例類似，還有某些專屬於 TBML 的層面，說明如下。

金融情報中心資料的基礎，為各金融機構與 DNFBPs 在察覺其客戶可疑活動時負有申報義務提交所提交的可疑交易報告。STRs 通常是金融情報中心整體分析洗錢／資助恐怖分子案例的起點，因此該等報告所包括資訊的品質與正確性，對金融情報中心分析的品質與及時性具有直接的影響。對同時擁有貿易與金融交易要件的 TBML 案例來說，這點也同樣相關。舉例來說，STR 不僅提供可疑金融交易的描述（包括交易各方及懷疑依據的詳細說明），也提供了相關貿易活動與相關資訊的深入見

解，因此有助於金融情報中心進行分析。

考量各金融機構涉入貿易融資的程度、對顧客行為的瞭解、擔任金融中介的角色及代表顧客執行付款等背景，金融機構擁有為金融情報中心提供寶貴資訊以察覺可能 TBML 犯罪活動的獨特地位。就貿易融資方面，金融機構可直接存取與貿易交易有關的文件。此外，各金融機構在為顧客提供融資或擔保客戶之財務狀況與穩定能力時，也可能因此針對顧客進行加強盡職調查。相較於直接記帳貿易與通匯銀行業務作業方面，金融機構所取得與客戶及其活動有關的資訊通常較少，但仍可透過察覺異常狀況的方式辨識可疑活動，例如相異於正常顧客行為之交易，及其他異常交易模式。

資訊圖表 4.1 金融機構提交予金融情報中心之報告種類

貿易融資相關報告

- 金融機構直接涉及貿易交易，並可存取與貿易交易相關的標的文件，並因此可察覺例如文件及／或顧客活動／交易對手活動或貿易融資流程所提供資訊所存在的舞弊狀況。

顧客貿易交易之專戶記帳結算報告

- 標的文件通常不會提供給金融機構；然而，金融機構會察覺例如顧客與貿易相關之金融活動、及／或其交易、及／或其交易對手相關的舞弊狀況。

往來銀行貿易交易報告

- 金融機構也無法取得標的文件或顧客資訊；然而，其可察覺例如跨國交易的舞弊（包括遭控與商品及貿易有關的舞弊），及／或辨識潛在與先前發現洗錢網絡或洗錢活動有關的可疑交易方。

資料來源： Egmont IEWG

DNFBPs 所提交的 STRs，尤其是公證人、稽核人員與會計師所提交的報告，可作為金融情報中心另一有關 TBML 犯罪的寶貴資訊來源。這些專業人員依據其專業經驗與 AML ／ CFT 知識，擁有很好的優勢，可

辨識與發現僅用於隱匿付款原始來源之公司，及為洗錢活動而設立之其他複雜法律架構。針對該等企業架構而編製的 STRs 對察覺 TBML 有重大價值，因為掛名公司與空殼公司已被發現廣泛用於各種 TBML 技巧之中。

除了 DNFBPs 與金融機構（如 FATF 建議要求）提交之 STRs 外，部分金融情報中心也會收取來自其他行業別的 STRs，例如從事國際貿易的商業實體。這樣的申報可作為察覺 TBML 的有用工具，尤其該申報來自於容易受 TBML 影響的行業更是如此。雖然這些實體提交的報告量增加，具有大幅度提高 TBML 察覺能力的潛能，此等措施並不能補足某些司法管轄區的金融情報中心指出 DNFBPs 申報不充足的情況。

實例參考 4.7 其他行業被指定為申報實體的案例

依據德國的國家法律架構，「商品交易方（traders of goods）」（包括工業生產廠商，例如汽車製造商等）被指定為德國的申報實體。德國金融情報中心因此會收到該等公司提交的 STRs，包括未知第三方支付可疑款項至其顧客帳戶的報告。這類報告讓德國金融情報中心能夠察覺部分 TBML 潛在案例。

在其中一個案例中，一家汽車製造商向金融情報中心通報，有來自不同國家的銀行的多個第三方帳戶，代表位於 X 國的銷售夥伴 A 支付數筆款項。該等第三方付款者登記於多個司法管轄區，且皆為汽車製造商所未知的對象。經分析過去數年匯入的付款狀況後，發現由多個第三方付款人代表 A 轉帳支付的款項，合計超過 5,000 萬歐元。

第二家汽車製造商則發現並通報，多筆第三方代表位於 X 國的銷售夥伴 B 付款的情況。分析顯示此二銷售夥伴 A 與 B 實際上擁有相同的最終實質受益人，亦即位於 X 國的個人。代表 B 支付的第三方款項，合計超過 3,000 萬歐元。其中一家第三方實體列名「洗錢事務所（laundromats）」中的「核心公司（core company）」。

資料來源：德國／ Egmont IEWG

有鑒於國際貿易的跨國性質，各金融情報中心之間所交換的即時資訊，也對察覺 TBML 具關鍵重要性。各金融情報中心可透過與超過 160

個國家的直接合作夥伴聯繫，取得與自然人及法人有關的額外行政、執法與金融資訊，及涉及具體案例的交易資訊。自外國金融情報中心取得的資料，有助於辨識既有的 TBML 案例要件，或促使金融情報中心發起全新分析並揭發新的 TBML 犯罪。

國際合作與資訊交換的重要性，可從幾個案例看得出來。多個金融情報中心指出，針對部分 TBML 犯罪所蒐集的資訊及後續分析，只有在位於其他司法管轄區的合作夥伴提供回饋意見時才有可能做到。此外，及時交換資訊與跨國支援，例如依據外國要求延遲交易之進行，及成立由來自各相關司法管轄區之專家所組成之專案小組，以研究常見案例，在幾個案例中都證明對調查與資產追回具有重要性。因此，各金融情報中心於國際層級進行雙邊與多邊的密切合作與資料交換，對打擊 TBML 來說是非常關鍵的部分。透過相關外國金融情報中心與該國國內執法機關、海關或其他權責機關直接合作，也被證明是一個情報蒐集以及確認初步懷疑的有效機制。

金融情報中心的貿易型洗錢分析方法

金融情報中心不只在處理 STRs 方面扮演了核心角色，在編製 TBML 犯罪的更複雜分析報告時亦是如此。金融情報中心在針對取自不同來源（包括各報告實體、行政與執法機關與國際合作對象）之資料與資訊進行分析時，會整合相關情報以架構較為完整的金融犯罪狀況，並因此有助於察覺、證明或甚至駁回 TBML 案例。金融情報中心針對 TBML 案例所執行的分析，可能包括例如商品流向與資金流向相關資訊的比較，以初步辨識異常狀況，或證實可疑的差異，以及報告可疑貿易相關交易。

此「典型（classic）」操作分析仰賴貿易與金融資料的比較來察覺可能異常狀況，雖然似乎是金融情報中心辨識 TBML 案例最常見的方法，但部分金融情報中心也曾有過從其他面向切入，並找出可能 TBML 犯罪的經驗。此方法涉及企業架構、登記資料、聲稱公司設立目的、企業銀行往來狀況以及企業網絡間關係等分析，例如共同代表人、重疊的所有權架構、相同的登記地址以及聯名銀行帳戶。透過在一定確信程度下認定某「國際貿易公司」只不過屬於複雜的空殼公司型態，金融情報中心或許可以假設這些「子公司」之間所進行的各種貿易交易係屬虛假交

易。權責機關可依據這些初步發現，啟動 TBML 犯罪的調查。此「反向（reverse）」方法突顯了蒐集與整合不同金融情報與其他可取得資料之重要性，並顯示了在分析與察覺 TBML 時，不必然一定需要取得佐證貿易文件。

在進一步跨入全新的分析與發現領域之後，各金融情報中心突顯了建立處理大型資料集合之能力的重要性，包括透過使用分析性與視覺工具達成目的。各金融情報中心也強調了在其分析性作業當中使用配對技術（matching technology，亦即主題式配對篩選工具）的重要性。有鑒於貿易相關交易通常非常複雜且涵蓋多個司法管轄區，創新 IT 解決方案，例如圖形分析與人工智慧（AI）及機器學習，尤其有助於金融情報中心進行 TBML 相關分析。這類解決方案不僅可用於分析大型資料集合，也可填補既有網絡不足之處（例如，依據已知犯罪網絡辨識未知犯罪網絡），及找出代表虛假貿易活動的交互關係。

策略分析是任何金融情報中心的核心功能之一。實務上，依據可用資源及國內 AML／CFT 架構之不同，金融情報中心會採用不同的方法執行此功能。不過，最終策略分析應該可提升金融情報中心、其他權責機關、金融機構及廣泛大眾對風險的瞭解。具體而言，金融情報中心可就 TBML 相關案例為這些單位提供與潛在規模、範圍及最常見方法的深入見解，以改善對風險的瞭解。

實例參考 4.8 義大利金融情報中心所執行的策略性分析

義大利金融情報中心與義大利銀行（Bank of Italy）的統計分析處（Statistical Analysis Directorate）合作針對義大利外國貿易的雙邊統計資料進行了一份實證分析。1 此分析是依據對義大利與夥伴國家在四年期間的貿易商品統計資料差異進行之評估。

在一個國家所記錄的進口或出口商品的價值，很少會與貿易夥伴國家所記錄的出口或進口商品的價值一致，該等一致情況亦稱為鏡相統計數據（mirror statistics）。有幾個客觀因素會導致此不一致情況，包括保險與運送成本、兩國之間文化與語言的差異、報告系統無效率、商品分類要件差異以及蓄意錯誤報告。

義大利權責機關採用的分析方法，參考了完整的國際非法資金流動相關文獻，能夠控制鏡相統計數據差異的主要「合法」來源，及在合理近似的範圍內，辨識蓄意錯誤申報非法跨國移轉資金之情況。其最終目的在於辨識異常貿易流量，並據以定義與國家及商品在行業層級的 TBML 風險量化指標。

依據義大利金融情報中心執行的操作分析，及與其他全國性權責機關交換資訊的結果，部分的發現與潛在非法交易有所關聯。

其他國家也可複製此方法，因為研究中使用的相關資料，是各國際組織 [聯合國貿易和發展會議（United Nations Conference on Trade and Development）、世界銀行（World Bank）以及經濟合作暨發展組織（Organisation for Economic Co-operation and Development）] 針對所有國家所編製。

註：

1. Gara, M., Giammatteo, M., and Tosti, E.（2019 年），「魔鏡啊魔鏡 ... 貿易鏡相統計數據如何能夠協助我們察覺非法金融流量（Magic mirror in my hand… How trade mirror statistics can help us to detect illegal financial flows）」，The World Economy，42: 3120--47。

資料來源：義大利

儘管存在此察覺洗錢活動之潛能，許多司法管轄區的金融機構與 DNFBPs 在辨識 TBML 時依然遭遇挑戰（請參閱私部門角度的各項挑戰章節），且經常導致低品質的 STRs 或漏申報之情況。就此方面，各司法管轄區應採取相關步驟，確保金融機構與 DNFBPs 擁有辨識可疑交易與即時通報金融情報中心之必要能力。前述步驟可能包括將 NRA 發現通報金融機構與 DNFBPs，包括犯罪者如何濫用或可能濫用特定行業遂行 TBML 犯罪。其他步驟則可能包括標的訓練、提供風險指標及金融情報中心之回饋意見，以支持金融機構與 DNFBPs 辨識 TBML 活動。一般而言，金融機構與 DNFBP s 向公部門取得的 TBML 資訊越具體與詳細（相較於對風險的一般性且模糊描述），這些步驟所能帶來的影響就越正面。此等措施也應與相關權責機關配合執行。

海關在打擊貿易型洗錢方面扮演的角色

海關通常為貿易領域的最主要執法機關，有責任阻截包括 TBML 等濫用國際貿易體系之犯罪行為。海關因此對國際貿易領域、商品的流動

及國際供應鏈擁有深入的瞭解，這些因素對辨識與調查 TBML 活動都非常重要。海關也經常擁有存取國際貿易文件與資料的唯一權限，而這點則是辨識 TBML 的關鍵。海關貨物分析尤其能夠協助察覺 TBML，因為此資料的異常狀況可能代表了 TBML 犯罪及其他貿易相關犯罪。

海關身處非法貿易活動哨口的獨特地位，使其得以察覺國際貨運被用於非法目的。同時，越來越多的國際貿易量（貿易資料因此增加），都對海關試圖辨識 TBML 犯罪與其他貿易犯罪帶來了重大挑戰。與 TBML 相關的貨運，僅佔整體合法貿易的一小部分，導致辨識 TBML 尤其困難。此外，海關也必須在分析與檢查貨運方面作出權衡取捨，因為必須確保貨物清關快速完成，以及確保貿易架構可行且有效率。其他典型的海關優先要務，例如徵收關稅以及制定關稅稅率，也都需要動用大量資源。因此，重點在於確保海關擁有足夠驗證運送文件及國內金融情報中心與執法機關所提供金融情報的能力[23]。舉例來說，這可透過在海關內部設立專屬團隊或部門來達成，由其負責此領域業務，並確保打擊 TBML 活動的效果能夠達到最大化。

海關在其日常業務中，經常遭遇組織性犯罪集團為清洗非法所得而使用許多洗錢方法，尤其是涉及處置（placement）與多層化（layering）階段。具體而言，在 TBML 犯罪中，資金可能透過於國際移動商業資產的方式進行，且該等資產皆屬正常買賣，或為賺取商業利潤之目的而運送。這些資產可能包括多種商品，例如電子產品、原料、服飾、珠寶與食品，如同前述章節所討論。就此方面，海關官員在分析與辨識可能用於 TBML 網絡的商品與貨物方面，扮演了關鍵的角色。

海關機構與金融情報中心之間的密切合作，可透過連結可疑貿易活動與可疑金融活動的方式，大幅度的提升辨識 TBML 的整合能力。在 TBML 案例中，國內層級調查前置犯罪，通常與調查國際洗錢有關，因為執法機關會跟著資金與商品的軌跡，追蹤到海關領域。這點尤其適用於具現金密集性質的犯罪活動，組織性犯罪集團在這些活動中會將非法資金轉換為商品，以進行國際運送。因此，海關單位、金融情報中心與執法機關在 AML ／ CFT 領域共同努力就顯得尤其重要，特別在 TBML 風險較高的國家更是如此。

[23] 部分司法管轄區的海關與執法機關可直接存取金融情報中心所編製的金融情報。

實例參考 4.9 秘魯的海關－金融情報中心合作

秘魯金融情報中心，為秘魯海關單位的官員提供內部實習工作。舉例而言，此做法使得專精海關作業的官員能夠在擔任金融情報中心實習生期間發展其個人技能、充實金融分析知識，及編製最終發送給海關的金融情資報告。用此方法可讓專業人員瞭解雙方機構的運作模式。

資料來源：秘魯金融情報中心

此合作關係應包括在上述權責機關之間快速分享資訊，及互相協調與TBML及相關前置犯罪有關的調查與作業（請參閱下列跨部門工作小組章節）。這類合作形式通常會因國內法律架構不同而有所差異（例如，哪個權責機關負責調查TBML與現金走私；海關單位是否具有調查權，及是否能夠調查洗錢），但仍有特定最佳實務，可適用於大部分國內執法架構。

世界海關組織與艾格蒙聯盟合作發布的「海關與金融情報中心合作手冊」，建議海關與金融情報中心建立國家層級的堅強夥伴關係。這些夥伴關係應建立在高階管理階層、第一線主管及分析師層級。此手冊特別鼓勵每季或每半年進行一次中階主管會議，以制定策略性計畫並打擊TBML，及為情報與操作目的而交換可疑金融資訊。在國內法律與機關政策允許下，這類合作亦可能包含分享貿易與金融資料，包括疑似從事以海關為中心的洗錢活動、海關詐騙或走私活動之個人與法人的相關資訊。許多這類非法活動案例皆包括TBML活動。

實例參考 4.10 德國海關 － 金融情報中心合作

德國海關稽核處（Auditing Service）有一份載明稽核處參與打擊洗錢與資助恐怖分子情況的狀況說明書（information sheet），及一份相關態樣的資料。

當外國貿易稽核、海關稽核、財政稽核、市場組織稽核與稅務稽核顯示出洗錢的證據，則前述狀況說明書會載明稽核人員與稽核處應採行的後續步驟。稽核處尤其須透過goAML網頁應用程式，直接將洗錢嫌疑資料送交金融情報中心。

資料來源：德國

金融情報中心的金融分析專業及海關的國際貿易專業，再加上兩個權責機關之間有效的資訊分享機制，不僅可提高各項 AML／CFT 措施的效率，也有助於達成其他海關目標。舉例來說，蒐集高風險行業及 TBML 活動模式之資訊，及運用金融情報中心策略分析與其他國際貿易貨物相關策略資訊，都可能有助於海關改善其貨物與運送檢查的優先順序。海關引進高階分析技巧，亦有助於提升貿易詐騙活動與其他貿易相關犯罪的辨識能力。這也可協助海關描繪出犯罪者與恐怖分子所運用的「熱門路線（hot routes）」與新興犯罪活動。

對海關而言，認知打擊 TBML 為業務執行優先目標，並基於雙邊與多邊基礎互相合作，是同樣重要的。TBML 犯罪通常會產生大量的證明文件。這類文件有一部分是貨物從海關管轄區通關前往其他地區所必需。這些海關文件也會用來佐證運送商品之款項支付。進口司法管轄區的海關文件，可能與出口司法管轄區所提示的文件有所不同，因為犯罪者通常會偽造這些文件來賺取非法利潤或移動非法價值。因此，相關海關對進口與出口運送文件的比較，可能導致察覺貿易異常狀況，且其中某部分可能屬於 TBML 犯罪活動。

實例參考 4.11 CBSA：貿易詐騙與 TBML 專業中心

認知到加拿大境內 TBML 活動的威脅，及加拿大海關單位「加拿大邊境服務局（Canada Border Services Agency，CBSA）」所扮演關鍵角色的情況下，加拿大為處理該問題，授權在 CBSA 內部成立「貿易詐騙與貿易型洗錢專業中心（Trade Fraud and Trade-Based Money Laundering Centre of Expertise）」。該中心自 2020 年 4 月開始運作，負責提升 CBSA 辨識、封鎖與調查複雜貿易詐騙的能力，及將 TBML 檔案送交「皇家加拿大騎警（Royal Canadian Mountain Police）」的能力。透過成立一個由情報分析師、貿易專家與犯罪調查人員共同組成的跨部門團隊，CBSA 更能夠辨識與調查指向 TBML 的異常貿易交易，及填補對威脅行為者與「犯罪手法（modi operandi）」知識方面的差距。

資料來源：加拿大

跨部門小組與配合機構

各權責機關之間的合作與配合，是成功察覺與瓦解任何洗錢與資助恐怖分子活動的關鍵因素。就 TBML 來說，執法機關、檢察官、金融情報中心、海關與其他權責機關之間的有效配合及快速的資訊分享機制，則是更為重要，主要因實際 TBML 犯罪的複雜度與多樣性所致。就 TBTF 而言，能夠有效地與情報機構合作及資訊分享也是必要的，主要因資助恐怖分子相關情報與察覺 TBTF 犯罪具有固有關聯性。本報告之目的雖然並非制定必要架構，且 TBML 也並無「靈丹妙藥」般的解決方案，但各司法管轄區在設立全新跨部門小組以打擊 TBML 或擴大既有小組權限時，仍可能會想將下列某些要素納入考量。

TBML 的多面向特性，讓權責機關擁有察覺洗錢的額外機會。如上所述，犯罪者會結合 TBML 技巧及其他洗錢方法，例如運用掛名公司及掛名負責人，或透過共謀金融機構移轉資金。因此，辨識出其中一個洗錢犯罪，或可進一步發現整個犯罪活動。依據犯罪者濫用行業別與所採用特定技巧之不同，不同權責機關可能更能夠察覺 TBML。同時，完整辨識 TBML 犯罪及追蹤犯罪所得，則須整合多個金融與貿易資訊，且只有相關權責機關互相提供協助才能達到此目標。為了有效率地執行此項作業，權責機關必須設置相關機制，讓他們能夠及時將 TBML 知識與專業傳達給執法機關，反之亦然。考量 TBML 調查可能涉及多個機構，設立配合機制或工作小組（無論是在同一機構下，或採用獨立平台）可以提升執行效率。

各司法管轄區可能選擇採用不同模型來架構此合作關係，例如專責 TBML 或在廣泛洗錢機制中處理 TBML 的工作小組或「整合中心（fusion centre）」，重點在於確保依據 TBML 對國家金融與貿易體系所帶來風險的嚴重性，決定 TBML 之處理先後順序。該先後次序應視為保障機制，可讓權責機關能夠分配並有效率地運用其專業與資源，無論是貿易或金融或其他 TBML 面向皆同。

如同任何其他犯罪活動一樣，辨識 TBML 可能帶來特定挑戰，因為可能並無受害者會向權責機關提出告發。權責機關通常必須採用其他方法察覺 TBML，且部分方法可能需要比對大量資料。此外，某些使用

TBML犯罪跨國移動資金的PML網絡，可能會仰賴大量交易與貿易作業，及許多掛名與空殼公司，且其目的僅在掩飾所移轉資金的非法性質，並使權責機關感到迷惑。因此，設置一個能及時比對與匹配大量資料的機制非常重要，不僅在察覺TBML方面，還是辨識與追蹤資產。無論相關機制由哪個單位負責，且無論是設立在單一機構內或成立跨部門小組，都應確保該機制能夠使用多種資訊來源，例如STRs、貿易資料、基本與實質受益人資訊、犯罪紀錄及財產登記資料（土地、汽車等）。

實例參考 4.12 全國貨物診斷中心

以色列於2014年成立了「全國貨物診斷中心（National Cargo Diagnostic Centre）」，以監督國際貿易運作，並將重點放在恐怖分子所運用的商品。此中心設立於以色列稅捐機關內，且由來自其他執法機關與安全機構的代表所組成。此中心採用專屬的風險評估IT系統，辨識用於走私恐怖主義相關商品及用於資助恐怖分子商品的貿易活動。若發現與洗錢活動有關的可疑交易，則將資訊發送給相關調查單位進行後續調查。

資料來源：以色列

公私協力夥伴關係

PPP是公部門機關與特定私部門實體合作及有效率地達成共同目標的一個機制。在AML／CFT方面，PPP通常被視為既有洗錢／資助恐怖分子種類、辨識全新與新興風險及交換資訊的資訊與知識分享平台。在某些司法管轄區，PPP也可作為權責機關與申報實體間交換金融情報的額外管道。

FATF建議考量了公部門與私部門間就AML／CFT議題所進行的合作[24]，但未明文要求各司法管轄區應建立PPP以符合此規定。同時，PPP可能適合用於提升相關行業之間的溝通，甚至有助於更廣泛對話。

[24] 例如，各主管機關應為各金融機構與DNFBPs提供應用AML／CFT措施的指南與回饋意見。

對 TBML 犯罪來說，該等溝通可能更為重要，因為打擊此洗錢形態需要權責機關及私部門行業提供許多專業。

對於希望在 AML／CFT 領域建立 PPP 機制或希望提升既有協力夥伴關係有效性的各司法管轄區，或許可以選擇採用其他模式，且應將國內 AML／CFT 領域的各項風險與其他特性納入考量。某些司法管轄區可能選擇建立以具體因應 TBML 為主要目標的 PPP，其他司法管轄區則偏好採用將 TMBL 視為許多洗錢議題其中一項的 PPP 模型。無論選擇什麼模式，各司法管轄區皆須將下列因素納入考量：

- 儘管部分 PPP 可能採用非正式架構，並無規範其活動之正式規則或程序，但重點在於各參與方就這類合作的目標與角色劃分達成清楚的協議。此協議應作為建立公部門與私部門行業之間信賴關係的基礎。
- 建立 PPP 本身，不應視為目標，而應視為處理國內 AML／CFT 特定領域疑慮或提升國內 AML／CFT 措施有效性之工具。確保達成此目的的一個方式，是在建立 PPP 之前找出短期與長期目標。就 TBML 而言，這些目標可能包括提高對貿易與金融系統弱點的瞭解以及改善資訊分享機制。
- 依據 PPP 目標與優先順序的不同，參與方數量及其行業或權責機關層級亦可能有所差異。若 TBML 落在 PPP 優先範圍內，則重點在於確保 PPP 擁有相關專業，包括貿易、海關與貿易融資。
- 雖然 PPP 的概念意味有限數量的私部門參與者直接參與，但不代表這類合作的成果（例如指引文件與紅旗指標）不適合用於廣泛大眾。各司法管轄區可能須考量將所達成的成果（尤其是與風險辨識及評估有關的部分）分享給未直接涉及 PPP 的私部門實體，以改善各行業對 TBML 風險的瞭解。
- 若 PPP 涉及操作層面的資訊交換，例如分享可追蹤至個體的資訊（個人可識別資訊、金融交易等），權責機關應確保該等交換符合國內資料隱私及其他相關法律與規範。

下列實例概述了以 AML／CFT 議題為重點的不同種類 PPP，包括與 TBML 相關的部分。

實例參考 4.13 德國 PPP 以及與私部門行業的合作

2019 年 9 月，德國成立了一個公私協力夥伴關係「金融犯罪防制聯盟（Anti Financial Crime Alliance，AFCA）」，以因應德國 NRA 所發現的風險。此聯盟的主要目的，在改善德國公部門與私部門行業間就打擊洗錢與資助恐怖分子方面的合作狀況。此 PPP 的成員來自德國聯邦刑事警察署（Federal Criminal Police Office）、聯邦金融監理局（Federal Financial Supervisory Authority）、金融情報中心以及 14 名私部門銀行業代表。AFCA 在 2019 年 12 月召開的會議中，決定要成立一個由私部門主導且專門負責 TBML 議題的專案小組。

為了能夠以有目標、公開且有效的方式提升打擊洗錢的成效，德國在 2019 年 11 月執行了首次全國性「防制洗錢同步行動（Concerted Action against Money Laundering）」，成員來自其金融情報中心及商品貿易主管機關，行動鎖定汽車零件與汽車行業。

金融情報中心也與 DNFBPs 的權責機關共同舉辦了兩場座談會。此外，金融情報中心亦出席了商品貿易權責機關召開的數場會議。這些活動之目的在於說明金融情報中心的作業內容，及啟動與提升各方的合作，並規劃未來進一步合作。

資料來源：德國

實例參考 4.14 金融科技聯盟貿易型洗錢工作小組

2020 年初，澳洲的公私協力夥伴關係「金融科技聯盟（Fintel Alliance）」成立了一個 TBML 專責工作小組，目的在建立具彈性、分享知識及發展一致性的策略，以打擊與瓦解澳洲 TBML 活動。此工作小組每月開會一次，成員涵蓋政府部門、執法單位與金融產業合作夥伴的各領域專家。

工作小組成立的其中一個目的，在辨識與記錄金融活動與產品如何被利用於 TBML 的情況。工作小組也負責考量與檢視用於降低 TBML 風險的各項控制措施是否適切。工作小組將負責建立國內與國際合作夥伴關係，並制定態樣與指標，以建立可協助強化與協調打擊 TBML 活動能力的各種

最佳實務。此工作小組在成立後的簡短期間內，就發動了幾個行動，包括：

- 編製有關 TBML 指標的報告，收錄公私部門合作夥伴的回饋意見。
- 在澳洲邊防署（Australian Border Force）指導下，建立公部門與私部門合作的資訊分享架構，以辨識與報告特定高風險產業公司的可疑活動。
- 創定與提供金融機構貿易融資專責訓練計畫。

資料來源：澳洲

實例參考 4.15 強調現金整合的公私協力夥伴關係

自 2018 年起，防制洗錢中心（Anti Money Laundering Centre，AMLC）就持續邀請相關公部門與私部門組織，進一步發展 TBML 的知識與瞭解。

2020 年，這些作業演進成結構性合作關係，並成立了「金融專業中心（Financial Expertise Centre，FEC）」。在此合作關係中，公部門與私部門各方合作打擊汽車產業的 TBML 現金整合活動。此 PPP 涵蓋多個參與方，包括財政資訊調查局（Fiscal Information and Investigation Service，FIOD）、荷蘭四大銀行、金融情報中心、國家警察署（National Police）、檢察署及稅捐機關。

此合作關係的重點，在於打擊汽車產業各種形式的非法現金整合。除了瞭解你的客戶外，重點在於瞭解你的行業（know your sector，KYS），而且荷蘭的汽車產業被視為是以現金交易為基礎的。然而，此 PPP 的初步結果顯示，汽車產業並非如一般人想像的以現金交易為基礎。只有幾家公司接受大額現金，現金付款僅為偶發現象，而非普遍狀況。

荷蘭 PPP 整合了公部門與私部門的專家，編製了強化行業法規的提案，例如有關企業間現金付款的論點。此 PPP 也依據該行業的特性，編製了 TBML 活動的各種態樣與指標，應可協助權責機關察覺欺詐汽車賣方與買方，及強化對整個行業的瞭解。

資料來源：荷蘭

參考資料

FATF（2012）, FATF Recommendations 2012

Egmont/WCO（2020）, Egmont/WCO Customs - FIU Cooperation Handbook

Wolfsberg Group（2019）, Wolfsberg Group Trade Finance Principles 2019

FATF/Egmont（2018）, Concealment of Beneficial Ownership

FATF（2013）, National money laundering and terrorist financing risk assessment

APG（2012）, APG Trade-Based Money Laundering Report

FATF（2008）, Best Practices on Trade Based Money Laundering

FATF（2006）, Trade Based Money Laundering

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

FATF

www.egmontgroup.org | www.fatf-gafi.org

2020 年 12 月

貿易型洗錢：趨勢與發展

本防制洗錢金融行動工作組織 — 艾格蒙聯盟聯合報告，旨在協助公部門與私部門因應察覺貿易型洗錢的各項挑戰。本報告運用了 FATF 全球網絡的各種案例研究，說明犯罪者運用貿易交易移動資金而非商品的方法。其中並強調可因應貿易型洗錢風險的各項建議。這些建議包括運用國家風險評估與其他風險基礎資料，提升涉及國際貿易之各公部門與私部門實體的認知、持續改善金融與貿易資料之資訊分享機制，以及權責機關與私部門行業的合作，包括透過公私協力夥伴關係。

第六部分

本局洗錢防制處重要紀事

109/1/8	出席「目標性金融制裁審議諮詢會議」。
109/1/14	與海洋委員會海巡署舉辦業務聯繫座談會議。
109/1/24-2/1	派員赴模里西斯巴拉克拉瓦參與艾格蒙工作組會議。
109/2/14	出席「犯罪防治研究發展諮詢會議」。
109/2/18	舉辦「強化金融情資分享及運用效能會議」。
109/6/1	完成與科索沃共和國（Republic of Kosovo）金融情報中心簽署「關於涉及洗錢、相關前置犯罪及資助恐怖主義金融情報交換合作瞭解備忘錄」。
109/7/13	與財政部關務署舉辦業務聯繫座談會議。
109/7/20、8/3	出席「亞太防制洗錢組織第三輪相互評鑑缺失改善會議」。
109/8/4	與財政部北區國稅局舉辦業務聯繫座談會議。

109/8/5、12/7	出席「地政士及不動產經紀業防制洗錢及打擊資恐辦法修正草案會議」。
109/9/2	出席「法務部與金融監督管理委員會第 37 次工作聯繫會報」
109/9/17	與警政署刑事警察局舉辦業務聯繫座談會議。
109/9/25	與財政部臺北國稅局舉辦業務聯繫座談會議。
109/9/25、10/19	出席「第三方支付服務業防制洗錢及打擊資恐辦法草案會議」。
109/10/13	與法務部廉政署舉辦業務聯繫座談會議。
109/10/14	舉辦「109 年度金融機構基層負責人員聯繫研討座談」。
109/10/14、12/8	出席「指定之非金融事業及人員效能缺失改善會議」。
109/10/23	與財政部中區國稅局舉辦業務聯繫座談會議。

109/11/26	出席「我國開放政府國家行動方案承諾事項：執行洗錢防制—實質受益人透明研商會議」。
109/12/10	舉辦「109 年犯罪金流分析與異常交易態樣研討會」。
109/12/18	與金融監督管理委員會檢查局舉辦業務聯繫座談會議。
109/12/23	出席「與伊朗交易應行注意事項宣導會籌備會議」。
109/12/28	與財政部高雄國稅局舉辦業務聯繫座談會議。
109/12/29	與財政部南區國稅局舉辦業務聯繫座談會議。

國家圖書館出版品預行編目 (CIP) 資料

洗錢防制工作年報. 中華民國一〇九年 = Anti-money laundering annual report,2020/ 法務部調查局洗錢防制處編. -- 新北市：法務部調查局, 民 110.10
面；　公分

ISBN 978-986-5443-66-5(平裝)

1. 洗錢　2. 犯罪防制　3. 中華民國

548.545　110016892

中華民國一〇九年

洗錢防制工作年報

出版機關：法務部調查局

發 行 人：呂文忠

編　　者：法務部調查局洗錢防制處

地　　址：新北市新店區中華路七十四號

電　　話：(02)29112241

網　　址：http://www.mjib.gov.tw

承 印 者：財政部印刷廠

地　　址：臺中市大里區中興路一段二八八號

電　　話：(04)24953126

出版年月：110 年 10 月

GPN：1011001613

ISBN：978-986-5443-66-5

洗錢防制工作年報
法務部調查局

ANTI-MONEY LAUNDERING
ANNUAL REPORT, 2020
INVESTIGATION BUREAU, MINISTRY OF JUSTICE,
REPUBLIC OF CHINA (TAIWAN)

http://www.mjib.gov.tw/mlpc

ISBN 978-986-5443-66-5
GPN 1011001613