

中華民國 113 年

洗錢防制 工作年報

ANTI-MONEY LAUNDERING
ANNUAL REPORT, 2024

法務部調查局——三年洗錢防制工作年報

Investigation Bureau, Ministry of Justice

Anti-Money Laundering Annual Report, 2024

序

本局洗錢防制處作為我國防制洗錢及打擊資恐（AML/CFT）核心機制之金融情報中心（FIU），致力於建構完善策略及強化不法金流偵測，防範金融及支付體系遭濫用，並透過追查及協助查扣不法所得，打擊犯罪集團經濟基礎，從根本上瓦解犯罪勢力。

依行政院「新世代打擊詐欺策略行動綱領」，本局洗錢防制處自 111 年 12 月成立幣流追蹤專責小組，運用專業分析技術，有效整合並分享金融情資，為執法機關之偵查工作提供精準支援。在國際合作層面，本局洗錢防制處透過艾格蒙聯盟（Egmont Group，EG）安全交換網路，協助國內執法機關與全球 182 個司法管轄體 FIU 進行情資交換，為跨境詐欺案件之資金流向追查提供堅實後盾。

近期為遵循亞太防制洗錢組織（APG）相互評鑑建議並與國際標準接軌，我國業於 113 年完成《洗錢防制法》重大修正。為此，本局洗錢防制處迅速啟動內部精進計畫，加強同仁對特定犯罪類型及金融情報分析之專業能力。同時，積極推動跨機關、跨領域合作，舉辦多場洗錢防制專業講習，凝聚政府部門共同打擊金融犯罪之能量。此外，本局洗錢防制處亦與行政院洗錢防制辦公室、APG 秘書處在臺共同舉辦評鑑員訓練研討會，此舉不僅顯著提升我國在國際防制洗錢領域之專業形象，更強化國際能見度及話語權。

本局洗錢防制處於 113 年度就受理申報之金融情資進行加值分析，發掘多起涉及廉政貪瀆、非法吸金、電信詐欺及新興金融科技濫用等重大案件，並就社會矚目案件提供專案資金協查。本年度洗錢防制工作年報特收錄 5 件指標性案例，其中「兩岸銀聯卡集團李○○等涉嫌電信詐欺案」，其跨境洗錢手法與風險態樣，足為殷鑑。基於 P2P 網路借貸平臺潛藏高度洗錢風險，本局洗錢防制處亦完成「P2P 借貸平台現況及洗錢風險」策略分析報告，深入剖析其犯罪態樣及濫用趨勢，並提出相應之防制建議，不僅提供主管機關完善法規及監理機制參考，亦因其對私部門分析洗錢等犯罪手法具參考價值而收錄於本年報。

再者，鑑於防制洗錢金融行動工作組織（FATF）將網路兒童性剝削（Online Child Sexual Exploitation，OCSE）正式列為指定犯罪類別，且近期國內亦頻傳未成年性影像遭散布、販賣之犯罪案件，本局洗錢防制處經 FATF 同意，摘譯其於 114 年 3 月發布之「偵查、打擊及調查網路兒童性剝削：運用金融情報保護兒童免受傷害（Detecting, Disrupting and Investigating Online Child Sexual Exploitation- Using Financial Intelligence to Protect Children from Harm）」報告。該譯文已收錄於本年報，旨在協助執法機關及申報實體發展兒少性剝削犯罪相關可疑交易之偵測、辨識及偵查工具，以有效遏止是類犯罪。

我國健全之洗錢防制體系，有賴於公私部門之齊心協力，本人在此由衷感謝各相關機關及申報實體長期以來對本局業務之支持及指導，並與我們共同持續精進，以維護金融秩序及社會公平正義。展望未來，本局洗錢防制處將持續扮演連結國內外公私部門之關鍵樞紐，並在既有穩固基礎上，與國內外權責機關及申報實體維持緊密合作，朝向科技化、標準化、專業化、國際化及整合化之五大願景穩步邁進，共同提升我國在防制洗錢及打擊資恐領域之卓越成就。

法務部調查局 局長

陳白立 謹識

中華民國 114 年 10 月

編輯說明

一、編輯目的

依據 FATF 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。」，本局洗錢防制處作為我國金融情報中心，彙整 113 年來國內申報機構執行防制洗錢及打擊資恐工作資料，並加以統計分析，編輯出版本年報。

二、編輯內容

本年報分下列七個部分：

- (一) 組織簡介
- (二) 法制新萃
- (三) 工作概況（含統計圖表資料）
- (四) 重要案例
- (五) 策略分析報告
- (六) 國外洗錢防制資料
- (七) 本局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。「疑似犯第十九條、第二十條之罪之交易」（下簡：可疑交易）與達一定金額之通貨交易（下簡：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。
- (三) 各項數字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 113 年 1 月 2 日為基準日。

目錄

序言	II
編輯說明	IV
第一部分 組織簡介	1
第二部分 法制新萃	4
第三部分 工作概況	7
壹、受理可疑交易報告之申報	8
一、可疑交易報告申報情形	8
二、處理情形	10
三、可疑交易發生地區分布	10
四、可疑交易申報月份分布	11
五、對象年齡層分布	11
六、可疑交易金額分布	12
七、可疑交易受申報對象性別分布	12
貳、受理大額通貨交易之申報	13
一、大額通貨交易申報情形	13
二、大額通貨交易申報金額分布	14
三、受理查詢情形	15
參、受理財政部關務署通報資料	15
一、旅客（含隨交通工具服務之人）通報數量	15
二、旅客（含隨交通工具服務之人）通報資料月份分布	16
三、旅客（含隨交通工具服務之人）通報資料金額分布	16
四、以貨物運送（含其他相類之方法）通報數量	17
五、以貨物運送（含其他相類之方法）通報資料月份分布	17

肆、宣導與教育訓練	18
一、專業培訓.....	18
二、跨機關協作	19
伍、公私協力與策略研究.....	21
一、持續維運「防制洗錢打擊資恐及資武擴資訊交流平臺」 ...	21
二、研編「P2P 借貸平台現況及洗錢風險」策略分析報告	21
三、發行洗錢防制處電子報	21
陸、國際合作與交流	22
一、國際情資交換	22
二、國際參與	23
第四部分 重要案例	26
壹、兩岸銀聯卡集團李○○等涉嫌電信詐欺案	27
貳、黃○○等涉嫌違反期貨交易法及銀行法案	29
參、新北市政府警察局○○分局陳○○等涉嫌貪瀆案.....	31
肆、兆○公司涉嫌違反銀行法案	33
伍、鴻○公司曾○○等涉嫌詐欺洗錢案	35
第五部分 策略分析報告	37
壹、P2P 借貸平臺簡介	38
貳、金融情報中心（FIU）觀察	40
參、P2P 借貸平臺常見犯罪態樣及遭濫用風險	43
肆、研析建議	44
伍、參考文獻	45
第六部分 國外洗錢防制資料	46
第七部分 本局洗錢防制處重要紀事	56



第一部分

組織簡介

組織簡介 *Introduction to the Organization*

本局洗錢防制處係依 FATF 第 29 項建議及 EG 章程所設立，並據《法務部調查局組織法》授權，掌理洗錢防制、打擊資恐及資武擴相關業務，不僅是我國金融情報中心，更為我國在 EG 國際金融情資交換網路之單一對口，核心職能為受理可疑交易與大額通貨交易相關金融情資，綜合其依法調取之必要資訊，加值研編之實務性、策略性研析報告，分送相關機關參酌或調查，以查緝犯罪、追討犯罪所得、穩定金融秩序、強化國際合作、維護國家安全與防制洗錢、資恐及資武擴。

洗錢防制處下設線索分析與防制規劃及資金協查 3 科，113 年配置 28 位專業人員。

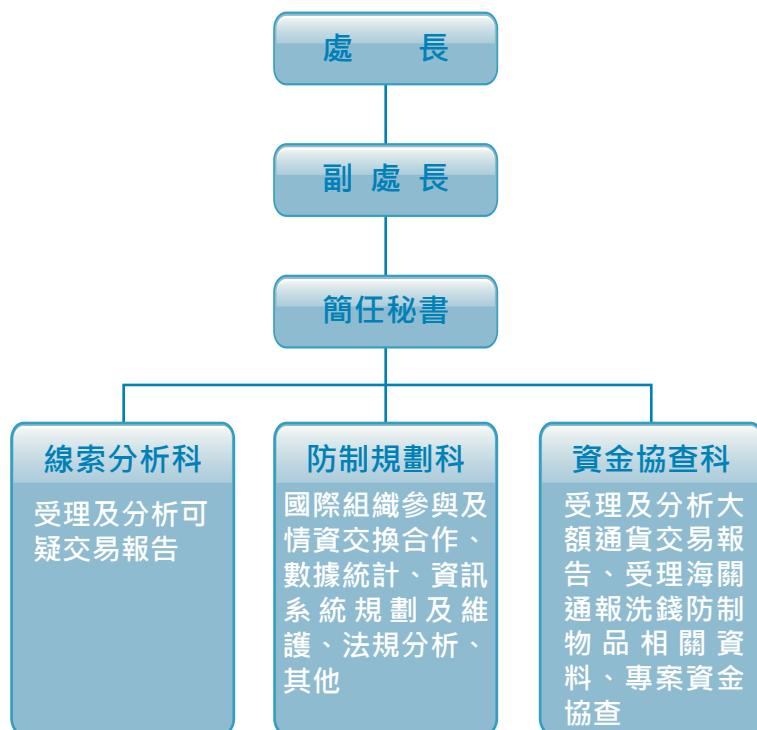


圖 A：洗錢防制處組織圖



圖 B：洗錢防制處作業流程圖



第二部分

法制新萃

我國《洗錢防制法》於 113 年 7 月 31 日完成最新修正，此次修法旨在回應 APG 第三輪相互評鑑建議，全面提升我國洗錢防制體系，並強化執法效能，以有效打擊日益複雜之洗錢手法。

我國於 108 年 10 月通過 APG 第三輪相互評鑑，獲「一般追蹤」最佳等級，惟評鑑報告仍指出多處法制面缺失，例如：洗錢定義不夠全面（如為自己洗錢）、前置犯罪範圍受限（如未納入偷渡犯罪）、信託關係規範不足，以及對非金融事業或人員罰鍰不具比例性。此外，評鑑報告亦建議擴大「控制下交付」適用範圍，並強化公私部門資訊交流。

為此，本次修法著重修正洗錢定義、犯罪構成要件及刑度，並首度將虛擬資產及第三方支付服務納入洗錢防制規範，建立相關登記或登錄制度及刑事處罰，以因應新興洗錢挑戰，修正要點如下：

- 一、擴大洗錢定義與前置犯罪範圍：增訂洗錢行為定義，並納入偷渡犯罪等前置犯罪範圍，以全面追溯不法金流。
- 二、虛擬資產與第三方支付服務納管：強制要求虛擬資產及第三方支付服務業者進行洗錢防制登記或服務能量登錄，對違反者課以刑事處罰，彌補數位金融法規之空白。
- 三、強化信託資訊透明度：增訂非信託業受託人應取得並持有信託基本資訊與實質受益權資料，並於與金融機構建立業務關係時主動揭露信託地位，提升信託關係透明性。
- 四、調整刑度並與前置犯罪脫鉤：一般洗錢罪刑度依洗錢金額區分，並取消與前置犯罪最高刑度之連結，使洗錢罪刑罰更具嚇阻力。
- 五、特殊洗錢罪要件修正與新興犯罪納入：刪除「顯與收入不相當」證明要件，並明確納入利用虛擬資產帳號或第三方支付帳號之洗錢行為。
- 六、加重法人責任與鼓勵自首／配合偵查：提高法人違反洗錢防制規定之罰金，同時，增訂自首、主動繳回犯罪所得及配合偵查之減免刑規定。
- 七、擴大沒收範圍：明確規定洗錢所得不論是否屬於犯罪行為人所有，均應予以沒收。

八、推動國際情資互惠運用與控制下交付：允許我國權責機關基於互惠原則，將取得資訊用於防制洗錢或打擊資恐，此外，亦授權檢察及司法警察機關執行控制下交付。

為有效落實《洗錢防制法》第十七條第四項所定之申報通報資料管理與運用機制，並確保情報交流之順暢與效能，亦同步訂定《洗錢防制法第十七條第四項申報通報資料管理運用辦法》（下稱：本辦法），作為明確法源依據，規範資料受理、分析、調取與分送之程序，其要點涵蓋：

- 一、本局洗錢防制處之權責：本局洗錢防制處負責受理及分析《洗錢防制法》第十二條、第十三條之申報資料及第十四條之通報資料，並規範資料分送之種類與範圍。
- 二、資料調取與補足：規範洗錢防制處向公務機關調取資料之範圍、程序及方式。此外，申報機構對於缺漏之申報資料應行補足。
- 三、國際情報交流：明確與國外金融情報中心相互分享及請求資訊之辦理原則。
- 四、資料查詢原則：規範向洗錢防制處查詢《洗錢防制法》申報通報資料之辦理原則。

本局洗錢防制處就所受理之申報通報資料進行專業分析與分送，若分析結果研判疑涉犯罪，或為維護金融秩序與國家安全所需，基於專業判斷與豐富經驗，並考量情資安全與運用效能，將金融情報區分為實務性、策略性金融情報或研析報告，並即時分送予權責機關參處。

此外，基於國際標準，當洗錢防制處認疑似涉及洗錢、前置犯罪、資恐或資武擴行為時，得向權責機關分送境外金融情報中心主動分享之資訊。本辦法亦明確規範國內司法偵查機關透過洗錢防制處以國際傳遞方式取得金融情資、金融情報及其他資訊時，所需之要件、填具資料及格式，確保國際合作之合法性及效率。



第三部分

工作概況

壹、受理可疑交易報告之申報

依《洗錢防制法》第 13 條第 1 項並參照 FATF 第 20 項建議，金融機構及指定之非金融事業或人員，對於涉嫌觸犯同法第 19 條、第 20 條所列罪名之交易，無論其是否完成，均應向本局申報。本局洗錢防制處將就所申報資料進行加值分析，並將分析結果彙編為金融情報，分送權責機關參考運用。

一、可疑交易報告申報情形

表 01：近 3 年受理各申報機構可疑交易報告件數統計表

申報機構	111 年	112 年	113 年
本國銀行	19,521	23,676	23,523
外國銀行	11	3	15
信託投資公司	0	0	0
信用合作社	495	487	457
農會信用部	627	728	695
漁會信用部	16	52	60
辦理儲金匯兌之郵政機構	1,496	1,467	1,545
票券金融公司	0	2	0
信用卡公司	32	93	118
保險公司	1,609	1,662	1,707
證券商	224	248	292
證券投資信託事業	31	14	34

證券金融事業	4	1	10
證券投資顧問事業	1	0	1
證券集中保管事業	26	23	15
期貨商	82	61	78
指定非金融事業或人員	93	294	451
大陸銀行	12	3	28
電子支付機構	209	195	115
外幣收兌處	0	172	580
外籍移工匯兌業	1	35	29
融資性租賃業	2	7	78
虛擬通貨業	227	447	918
合計	24,719	29,670	30,679

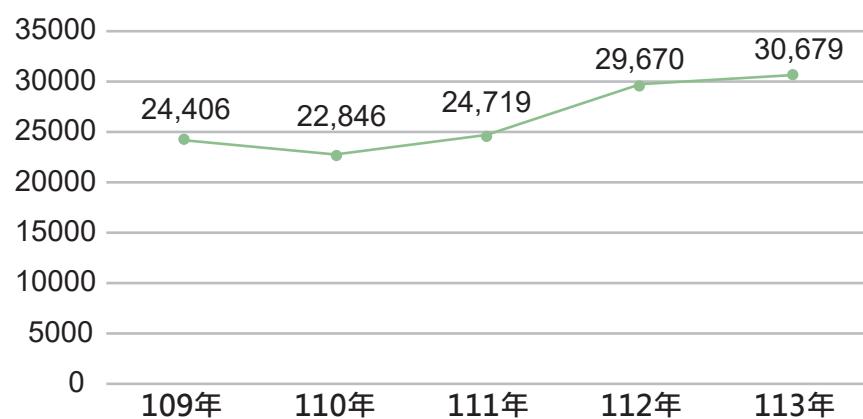


圖 C：近 5 年可疑交易報告申報件數分析圖

二、處理情形

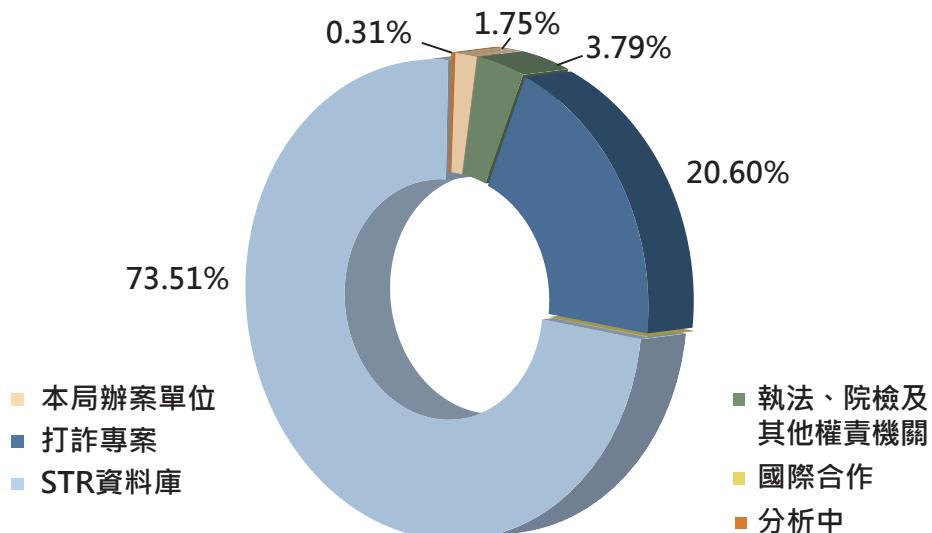


圖 D：113 年可疑交易報告處理情形分析圖

三、可疑交易發生地區分布

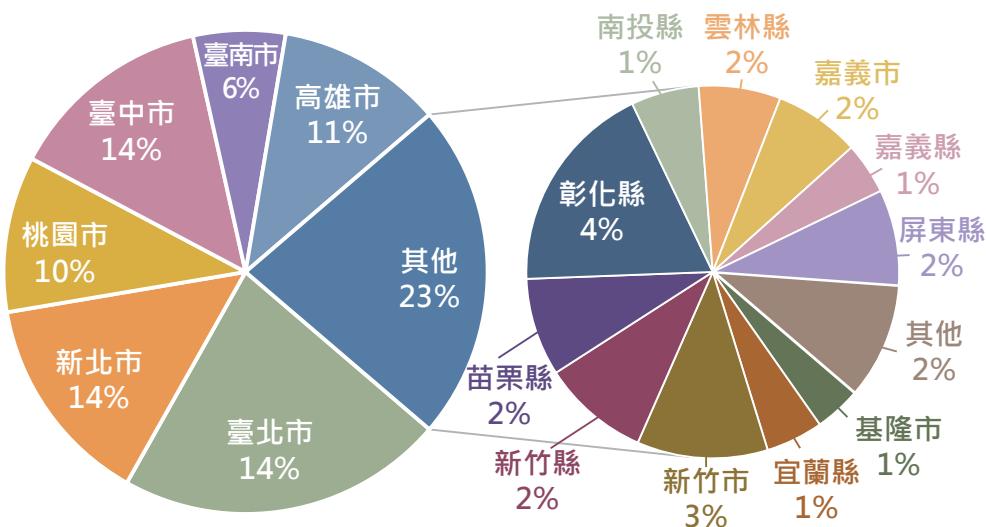


圖 E：113 年可疑交易發生地區分析圖

四、可疑交易申報月份分布

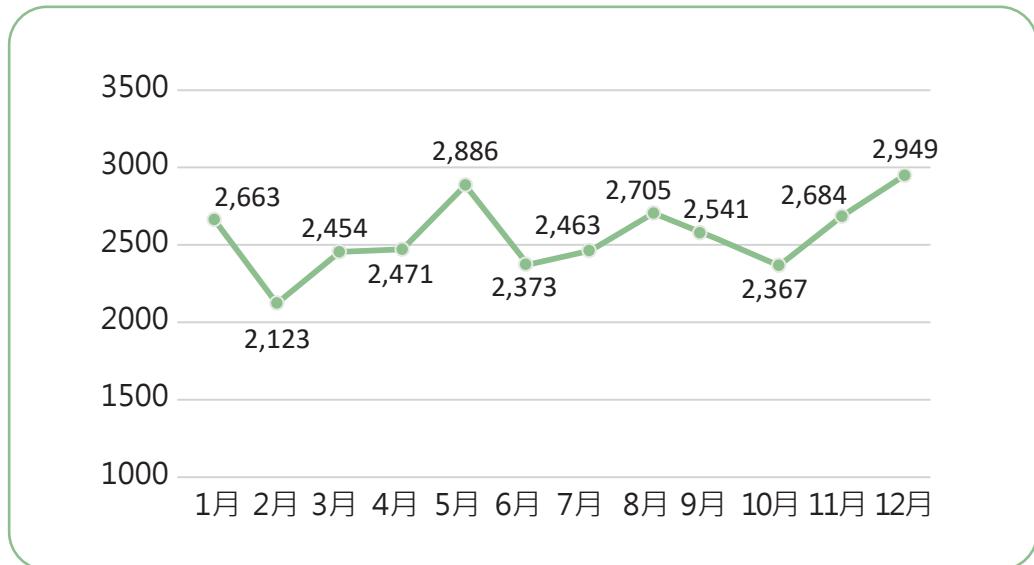


圖 F：113 年各月份申報可疑交易報告分析圖

五、對象年齡層分布

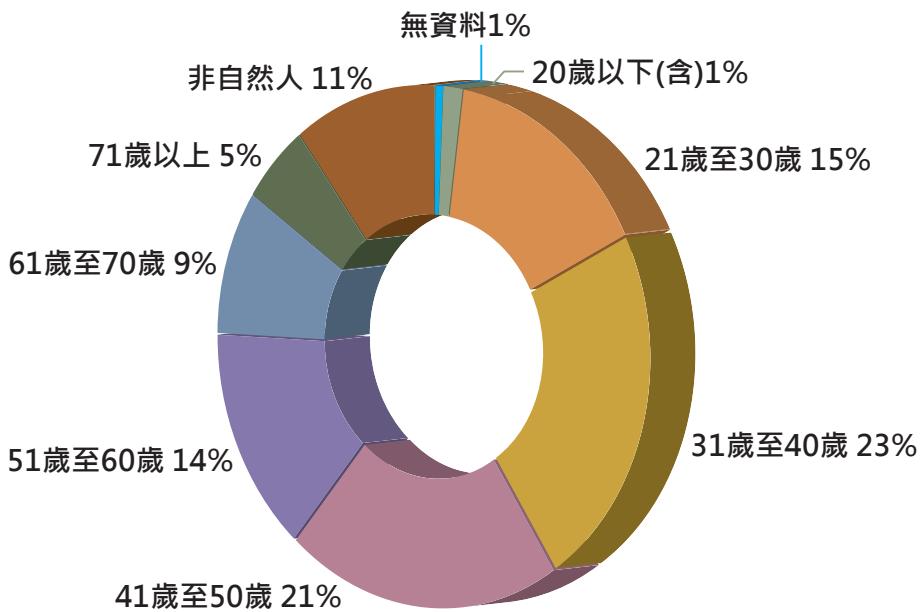


圖 G：113 年可疑交易申報對象年齡層分析圖

六、可疑交易金額分布

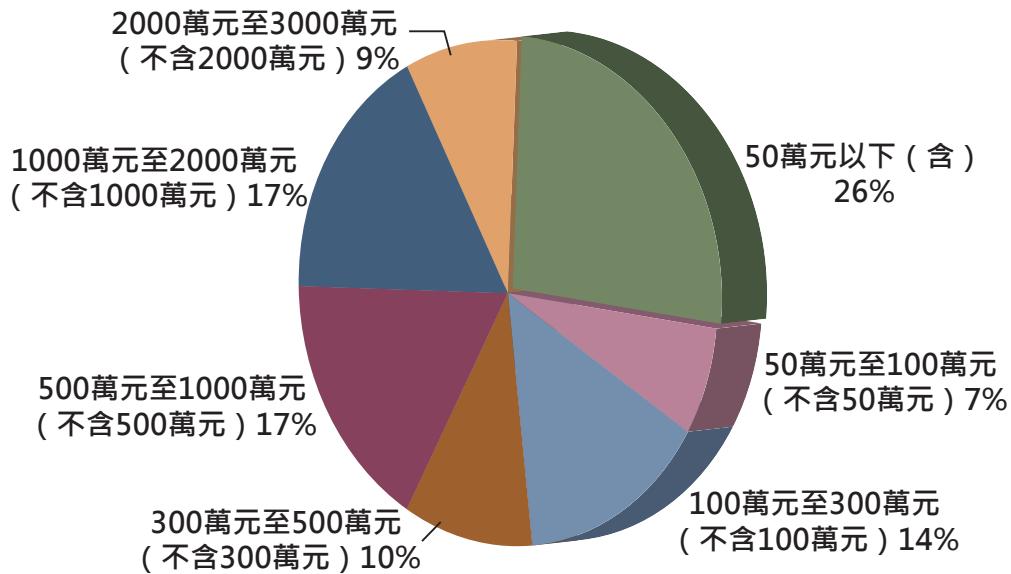


圖 H : 113 年可疑交易申報金額分析圖

七、可疑交易受申報對象性別分布

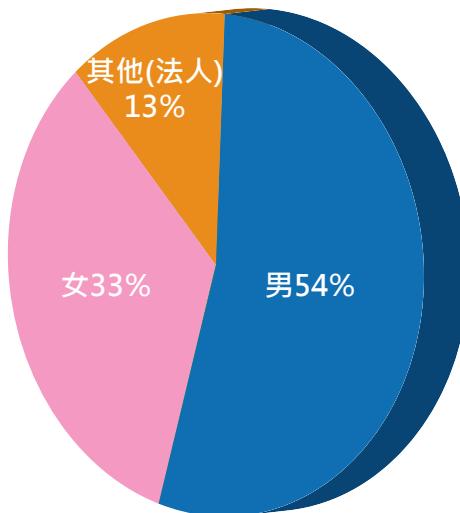


圖 I: 113 年可疑交易受申報對象性別分析圖

貳、受理大額通貨交易之申報

依《洗錢防制法》第 12 條、〈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 條規定，本局受理國內金融機構申報之大額通貨交易。本局洗錢防制處負責建置、保管及運用所受理之大額通貨交易申報資料庫，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，受理本局所屬單位與司法及執法等權責機關查詢。

一、大額通貨交易申報情形

表 02：近 3 年受理各申報機構申報大額通貨交易件數統計表

申報機構	111 年	112 年	113 年
本國銀行	2,532,309	2,607,971	2,703,491
外國銀行	4,727	3,534	298
大陸銀行	0	0	0
信託投資公司	0	0	0
信用合作社	120,800	119,691	124,558
農、漁會信用部	264,213	266,085	272,245
中郵儲匯處	286,579	302,022	310,923
保險公司	4,137	3,799	3,408
銀樓	448	279	555
地政士或不動產經紀業	721	833	736
虛擬通貨業者	105	4,775	3,305
書面申報（投信投顧公司）	5	9	15
書面申報（金融機構 - 其他）	0	0	1
其他金融機構（VASP）	0	0	79
合計	3,214,044	3,308,998	3,419,614

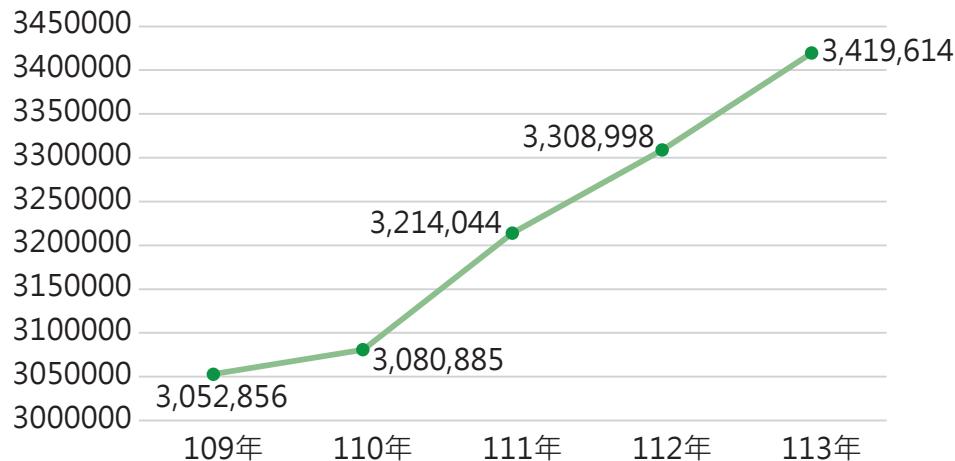


圖 J: 近 5 年大額通貨交易申報件數統計圖

二、大額通貨交易申報金額分布

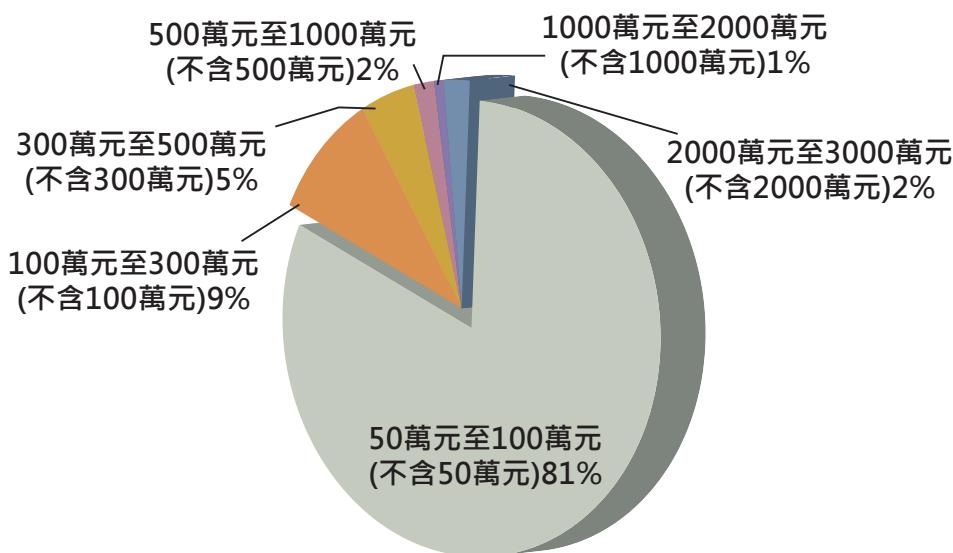


圖 K：113 年申報大額通貨交易金額分析圖

三、受理查詢情形

表 03：近 3 年受理大額通貨交易查詢筆數統計表

年度	111 年	112 年	113 年
法務部調查局	28,624	56,459	19,512
其他執法機關	34,523	20,319	21,655
檢察機關及法院	3,037	3,251	1,990
其他行政機關	6,328	4,703	4,941
筆數統計	72,512	84,732	48,098

參、受理財政部關務署通報資料

依《洗錢防制法》第 14 條第 1 項及〈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、隨交通工具服務人員或透過貨運、快遞、郵寄等方式入出境，若攜帶或運送達一定金額之外幣、港澳貨幣、人民幣、新臺幣現金、有價證券及黃金等，均須向海關申報，並由海關通報本局。此與 FATF 第 32 項建議宗旨一致，該建議要求各國應建立跨境運輸現金或無記名可轉讓金融商品申報或揭露系統，並確保適用於所有實體運輸方式。

一、旅客（含隨交通工具服務之人）通報數量

表 04：近 3 年旅客（含隨交通工具服務之人）通報筆數統計表

出、入境	111 年	112 年	113 年
入境	1,603	3,207	2,969
出境	4,603	30,884	38,861
合計	6,204	34,091	41,830

二、旅客（含隨交通工具服務之人）通報資料月份分布

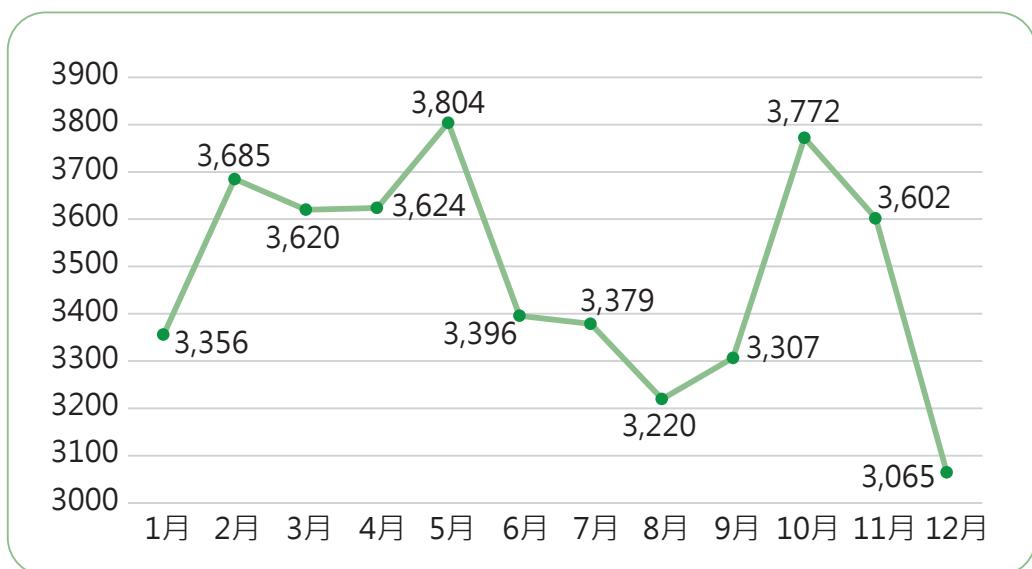


圖 L：113 年各月份旅客（含隨交通工具服務之人）通報統計圖

三、旅客（含隨交通工具服務之人）通報資料金額分布

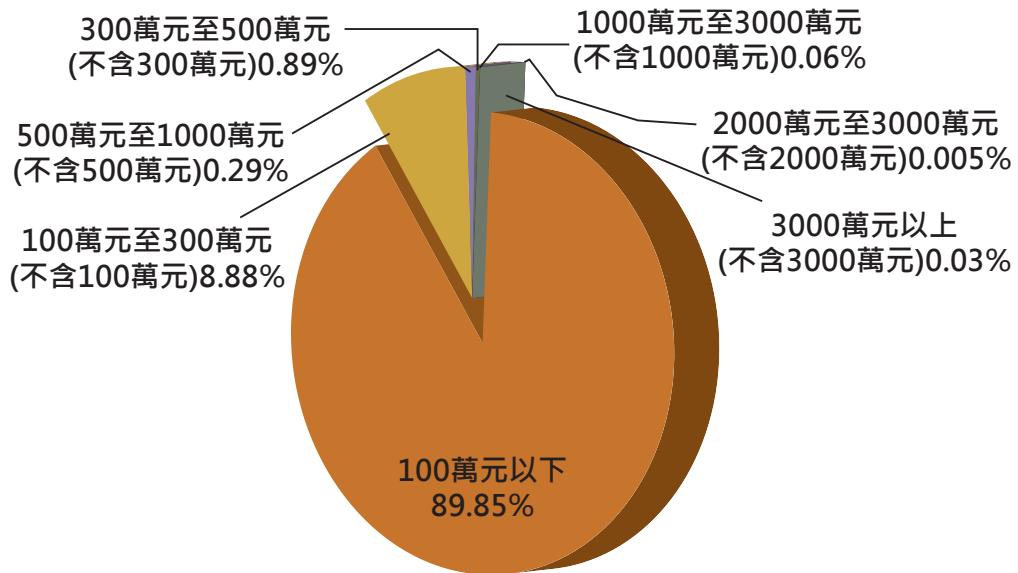


圖 M：113 年旅客（含隨交通工具服務之人）通報金額分析圖

四、以貨物運送（含其他相類之方法）通報數量

表 05：近 3 年以貨物運送（含其他相類之方法）通報筆數統計表

出、進口	111 年	112 年	113 年
出口	75,468	71,372	84,277
進口	284,782	337,768	289,797
合計	360,250	409,140	374,074

五、以貨物運送（含其他相類之方法）通報資料月份分布

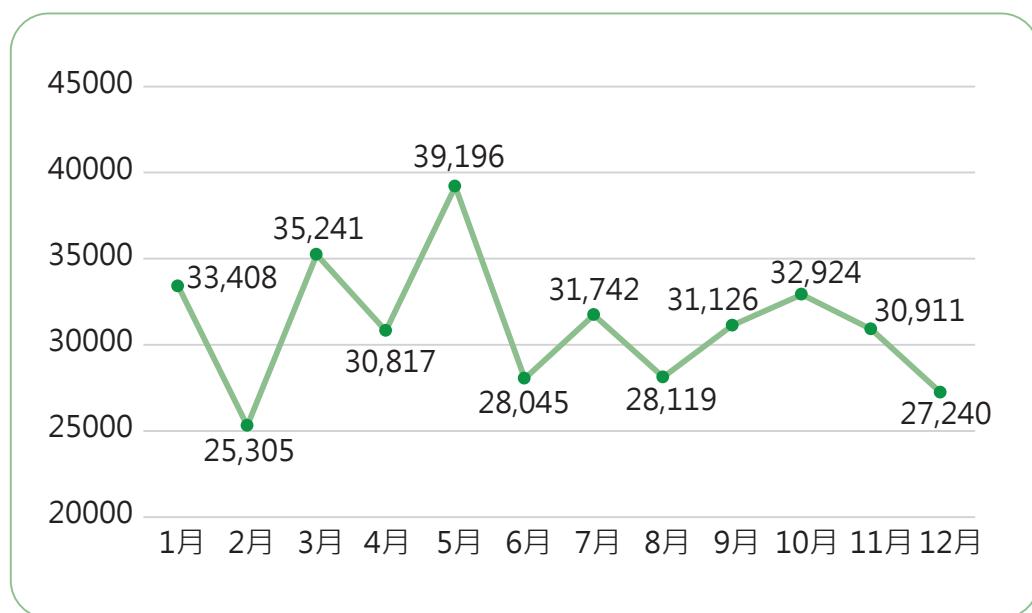


圖 N：113 年以貨物運送（含其他相類之方法）各月份通報統計圖

肆、宣導與教育訓練

一、專業培訓

為因應 APG 相互評鑑結果並與國際標準接軌，我國《洗錢防制法》於 113 年進行大幅修正，主要聚焦「強化虛擬資產服務監管」、「落實第三方支付服務監管」及「提高洗錢行為罰則並加重法人責任」三大重點。新修《洗錢防制法》上路後，本局洗錢防制處立即啟動組織學習機制，深化同仁對特定犯罪之掌握能力及金融情報分析技巧，並不定期對申報機構提供專業教育訓練，講授洗錢、操縱股價、內線交易及詐欺等常見犯罪手法，增進申報機構辨識異常交易之能力，並強化其以風險為本之客戶盡職調查效能，期提升我國整體金融成效，順利通過 APG 第四輪評鑑。

113 年 8 月，舉辦
新興犯罪與異常
交易態樣研討會



113 年 9 月，洗
錢防制法修法概
述組織學習



表 06：113 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		113 年	
		場次	人次
銀行	本國銀行(含金控)	26	2,502
	外國銀行	0	0
信用合作社		1	39
農漁會信用部		5	408
證券投信投顧業		2	77
票券金融業		1	62
保險業		10	513
指定之非金融事業或人員	會計師公會	5	873
合計		50	4,474

二、跨機關協作

本局洗錢防制處連續 3 年參與外交部舉辦之「國際組織日」活動，藉此提升國人對洗錢防制議題之認知，並增進對我國參與洗錢防制相關國際組織、結合跨國力量共同打擊犯罪之瞭解與支持；同時，亦積極推動跨機關、跨領域合作，如與法務部、行政院洗錢防制辦公室以及本局新世代打擊詐欺督導中心辦理多場洗錢防制相關研習課程，展現政府部門共同打擊金融犯罪之決心。



113 年 11 月，本局洗錢防制處同仁與外交部田政務次長中光、駐臺使節團團長聖文森及格瑞那丁大使 Andrea Clare Bowman 共同參與外交部「國際組織日」活動

工作概況 Work Overview

本局洗錢防制處持續與財政部北區及臺北國稅局等稅務機關交流溝通，雙邊就近期稅務法規及案例交換意見，並就未來偵蒐重點及合作需求進行討論。

113 年 4 月，
財政部北區
國稅局來訪



113 年 6 月，
財政部臺北
國稅局來訪

本局洗錢防制處亦持續與金融監督管理委員會各局密切互訪聯繫，針對洗錢防制與打擊資恐成果、虛擬資產服務事業洗錢防制登記辦法規範進展等議題進行討論。



113 年 1 月，金融監督管理委員會檢查局來訪



113 年 9 月，金融監督管理委員會證期局來訪

伍、公私協力與策略研究

一、持續維運「防制洗錢打擊資恐及資武擴資訊交流平臺」

為強化我國防制洗錢、打擊資恐及防制武擴機制，本局洗錢防制處於111年9月26日啟用「防制洗錢打擊資恐及資武擴資訊交流平臺」，整合30個公部門機關及逾500個私部門機構資源。本局洗錢防制處持續維運，不定期上傳預警資訊、洗錢罪起訴案例分析及可疑交易報告範例；監理、執法及行政機關亦不定期公告裁罰、去識別化案例及法規宣導。本平臺已開放私部門主動上傳預警及高風險態樣資訊，以增進申報主體對詐欺犯罪威脅、弱點及風險趨勢之掌握，強化從業人員可疑交易辨識能力。

二、研編「P2P 借貸平台現況及洗錢風險」策略分析報告

為掌握國內洗錢犯罪風險趨勢，並協助監理機關及金融機構完善防制洗錢機制，本局洗錢防制處有鑑於P2P借貸平台為洗錢高風險管道，遂研編「P2P借貸平台現況及洗錢風險」策略分析報告，深入分析私人投資借放款相關犯罪態樣。報告完成後，亦即時分送相關機關及申報實體，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，彰顯本局洗錢防制處在風險評估與情報分析之專業職能。本報告全文詳年報第五部分。

三、發行洗錢防制處電子報

本局洗錢防制處作為國家金融情報中心，為強化定位及功能，自108年11月持續發行中英文電子報，旨在創建防制洗錢、打擊資恐及防制武擴相關知識交流平臺，並拓展公私部門夥伴關係（PPP）。電子報內容彙整統計資料、犯罪趨勢、交易態樣及防制重點等專業意見，供各界參考，俾提升整體風險辨識能力，最終目標為協助各方採取與風險相稱之防制措施，有效配置資源，聚焦高風險活動，從而全面強化防制洗錢、打擊資恐及武擴機制。

陸、國際合作與交流

一、國際情資交換

本局洗錢防制處據 FATF 第 40 項建議，持續強化跨境情資協查，確保國內權責機關迅速有效進行國際合作，並依循「新世代打擊詐欺策略行動綱領」推動，聚焦跨境電信詐欺集團追緝，協助檢調警機關請求情資協查案件量顯著增長，足見本處在當前打擊犯罪國際合作中擔任重要角色。

本局洗錢防制處透過 EG 保密網路高效交換洗錢、資恐及資武擴情資。為積極響應政府打擊跨境詐欺犯罪政策，本局洗錢防制處於 113 年請求國外協查案件數與聯繫頻次劇增，反映跨境犯罪挑戰日益嚴峻。本局洗錢防制處專業處理每項情資請求，確保資訊即時分送與有效運用，充分展現金融情報中心專業職能及支援執法之能力。

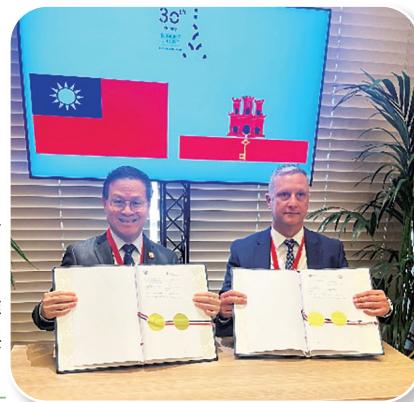
表 07：近 5 年從事國際合作之情資交換統計表

事項	年度	109 年	110 年	111 年	112 年	113 年
外國請求	案數	58	56	62	59	54
	次數	197	176	192	199	206
我國請求	案數	32	7	52	55	113
	次數	110	39	149	175	335
外國主動 提供情資	案數	66	49	35	25	39
	次數	132	95	63	40	73
我國主動 提供情資	案數	12	8	7	4	15
	次數	23	20	16	6	26
問卷及 其他事項	案數	0	0	0	0	0
	次數	261	379	448	440	406
小計	案數	168	120	156	143	210
	次數	723	709	868	860	1,035

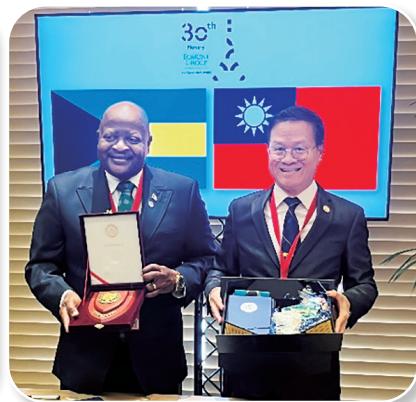
二、國際參與



113年1月，出席EG工作組會議，並與開曼群島金融申報管理局簽署金融情報交換合作瞭解備忘錄



113年6月，出席EG第30屆年會，並與巴哈馬、直布羅陀簽署金融情報交換合作瞭解備忘錄



113年9月，直布羅陀金融情報中心首長來訪

工作概況 Work Overview



113 年 9 月，出席 APG 第 27 屆年會



113 年 10 月，本局洗錢防制處與行政院洗錢防制辦公室、APG 秘書處合作在臺舉辦評鑑員訓練研討會



113 年 10 月，
APG 副秘書長來訪



113 年 10 月，出席亞太地區追討犯罪所得機構網絡 (ARIN-AP) 第 9 屆年會



113 年 11 月，出席 APG 態樣研討會



第四部分

重要案例

壹、兩岸銀聯卡集團李○○等涉嫌電信詐欺案

一、案情概述

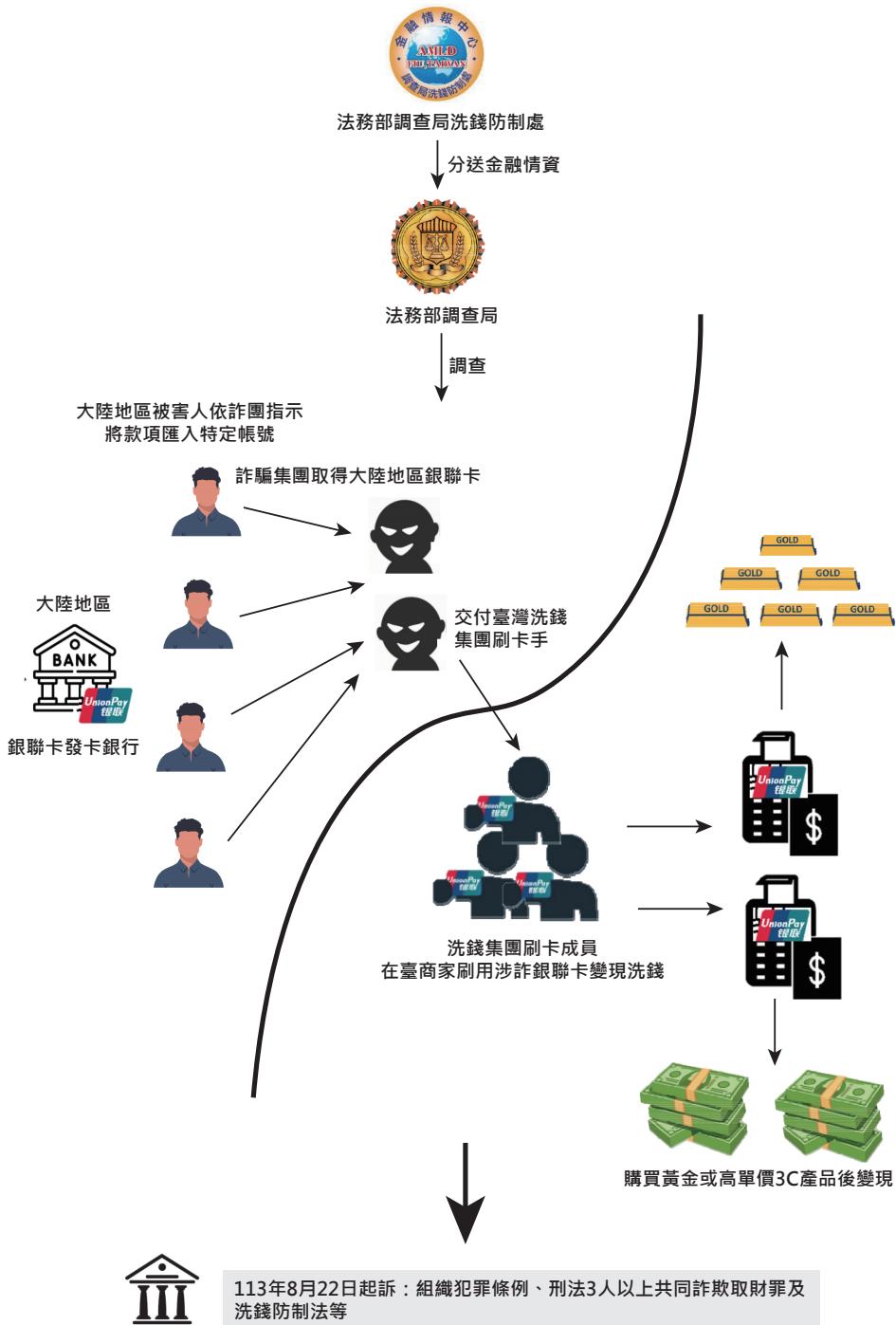
本局於 112 年 8 月間根據洗錢防制處分送之金融情報，獲悉多筆大陸銀聯卡在臺消費交易顯有可疑，經財團法人聯合信用卡中心聯繫中國銀聯國際有限公司，確認該等銀聯卡帳戶涉入電信詐欺案件。循線追查，偵知李○○等人所屬詐欺集團自 112 年起假冒大陸地區執法人員身分，誘騙大陸地區被害人相信其涉入詐欺及洗錢犯罪，並指示將款項匯入指定之大陸地區銀行帳戶；隨後，集團成員持大陸銀聯卡在臺刷卡消費，並偽簽刷卡簽單，藉此規避洗錢防制法修正前對指定之非金融事業或人員（DNFBPs）之客戶身分確認及可疑交易申報之義務，進而將購得商品變現以遂行洗錢。自 112 年 3 月至 113 年 8 月止，李○○等 8 人以此手法洗錢金額達新臺幣（下同）2 億 992 萬餘元。

二、經驗參考

- (一) 詐欺集團利用大陸銀聯卡跨境支付特性，由在陸同夥取得開戶人銀聯卡及密碼後，交由在臺成員持卡消費並偽簽，透過規避 DNFBPs 之客戶盡職調查義務，增加司法機關查緝真實刷卡人身分之難度。
- (二) 該集團於被害人存入特定金額後，即指示在臺刷卡手迅速購入高單價易變現商品（如黃金、3C 產品），為典型洗錢態樣。金融機構及 DNFBPs 應提高警覺，並主動向本局洗錢防制處申報 STR。本案由最初 26 筆可疑交易開展偵查，擴大偵破近 200 筆、逾 2 億餘元之犯行，凸顯高品質 STR 及金融情報中心即時加值分析對於執法機關調查及打擊犯罪之關鍵作用。
- (三) 本案藉兩岸共同打擊犯罪機制獲取相關資訊，對釐清案情、追查金

重要案例 Significant Case Studies

流至關重要，彰顯跨境執法情報合作在瓦解跨國組織犯罪及洗錢網絡、維護金融秩序及提升全球反洗錢與打擊資恐效能方面之核心價值。



貳、黃○○等涉嫌違反期貨交易法及銀行法案

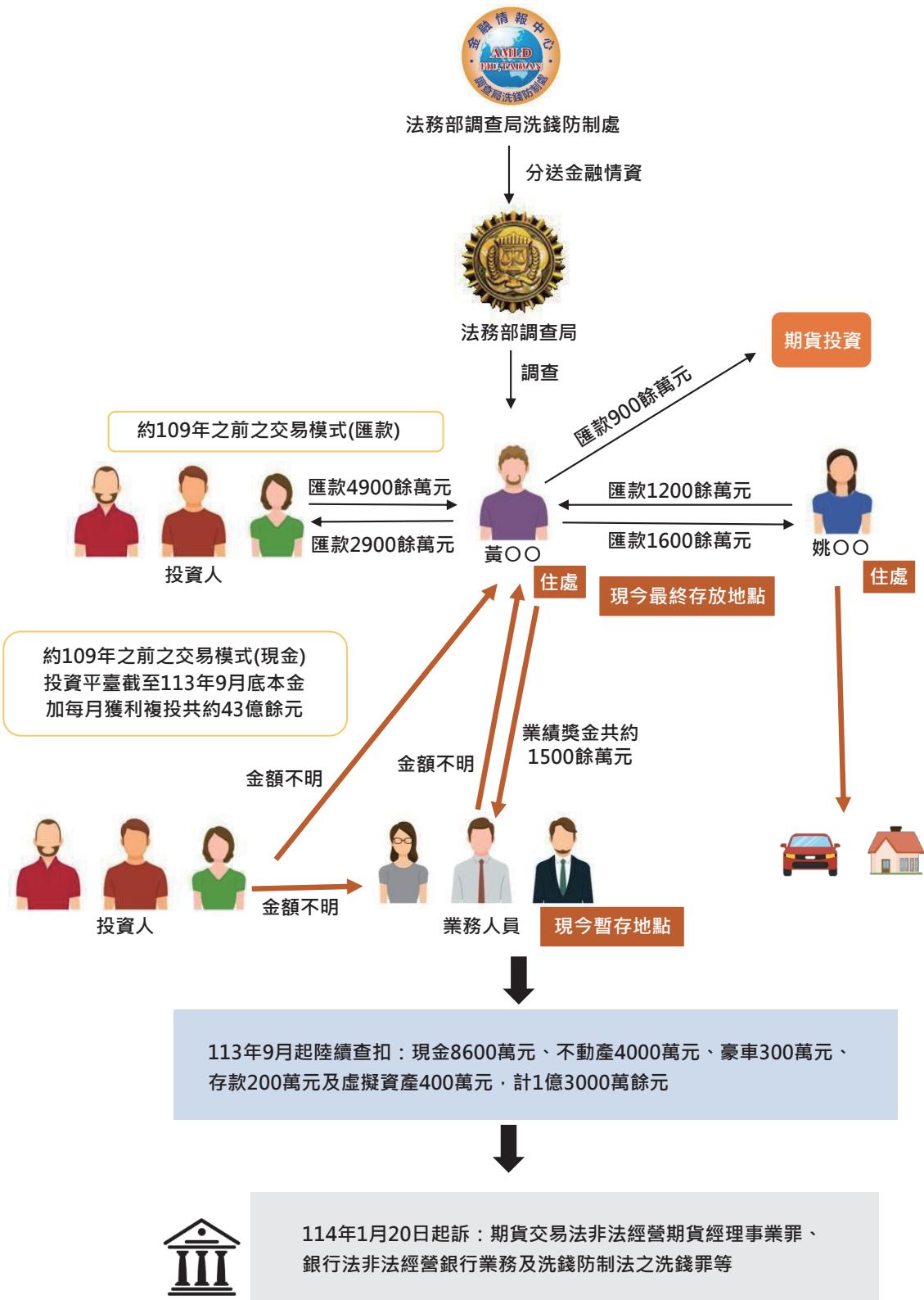
一、案情概述

本局於 108 年 6 月間根據洗錢防制處分送之金融情報，顯示黃○○經常在 LINE 群組宣傳期權交易績效，與其實際期貨對帳單損益不符，疑似透過散布不實獲利資料，誘使他人委託代操並交付款項；另黃○○個人銀行帳戶亦有多筆不特定人匯款，並備註「獲利」、「本金」等字樣，本局據以展開偵查。查悉黃○○以期貨代操名義向不特定人吸收資金，允諾每月 5% 之高額報酬，為掩飾挪用投資款，黃○○將部分資金移轉至女友姚○○帳戶。自 108 年起，因部分投資人帳戶金流受執法機關關注後，黃○○為規避金融機構洗錢防制監控及司法偵查，改與投資人約定以現金收付投資款及獲利，藉此隱匿不法金流。統計黃○○收取投資本金及利息總額逾新臺幣（下同）43 億餘元，該不法所得多用於黃○○個人消費、支付投資人帳面獲利及招攬業務獎金等，而非實際用於期貨投資。此外，黃○○更花費不法所得購置房產供姚女居住，並用以藏匿大量現金投資款。本局自 113 年 9 月起，在黃、姚及核心幹部住處查扣現金逾 8,600 萬餘元及名錶等奢侈品，後續再查扣渠等名下存款、虛擬資產、不動產及名車等，不法資產總值達 1 億 3,000 萬餘元。

二、經驗參考

本案前期交易均係使用黃○○個人帳戶與眾多不特定人頻繁交易，呈現資金往來與其身分顯不相當等可疑洗錢表徵。多數投資人對金流交代不清，且否認委託期貨代操，顯與黃○○等串證以規避查緝。其後轉採現金交易，旨在隱匿犯罪所得並規避金融監管及司法單位調查，徒增偵查難度。為避免證據湮滅或資產轉移，偵查團隊長期低調蒐證，俟證據充分始執行全面搜索約談，將犯嫌繩之以法，並查扣犯罪所得。本案偵辦成功瓦解該犯罪集團及其洗錢網絡，對維護金融秩序、健全洗錢防制機制及遏止經濟犯罪均具重大意義與參考價值。

重要案例 Significant Case Studies



參、新北市政府警察局○○分局陳○○等涉嫌貪瀆案

一、案情概述

本案線索情資係本局洗錢防制處提供，揭露新北市政府警察局○○分局○○派出所員警陳○○，設於 A 銀行等多家金融機構之帳戶，自 109 年起，出現與薪資顯不相當之鉅額資金進出及頻繁現金存提。經調查發現，陳○○涉嫌利用職務之便，長期包庇陳○銓在轄內經營甲麻將賭場，其本身亦參與賭博及招攬賭客，並利用上開 A 銀行等個人帳戶處理代賭場管理之賭資及賭債，藉此掩飾該不法款項與賭場間之關聯。此外，陳○○濫用 M-POLICE 系統非法查詢賭客個人資料，協助乙賭場業者呂○○非法催討賭債並從中牟取報酬。

二、經驗參考

- (一) 陳○○年薪約 130 萬元，然於 109 年 1 月至 112 年 1 月間，其名下 8 個金融帳戶累計存入非薪資款項達 9,782 萬餘元，支出 9,796 萬餘元，資金流量遠逾其合法收入。其中，現金存款達 1,057 萬元，現金提領達 2,214 萬餘元，顯示其頻繁利用現金交易製造金流斷點，規避追查。次查，陳○○管理以胞弟為會首之民間互助會資金，金流進出頻繁且交易對象繁雜，此模式符合「同一客戶一定期間內多筆現金存提分別累計達特定金額以上」之洗錢表徵。
- (二) 分析 ATM 交易紀錄，偵知陳○○常於深夜或清晨在其任職派出所週邊存提大量現金，且部分現金存入係由不同第三人在陳○○生活圈外之 ATM 執行，款項存入後迅速移轉，具典型洗錢特徵。
- (三) 陳○○利用警政系統非法查詢賭客個資，脅迫賭客將賭債以每月小額現金存入在 A 銀行帳戶，此種將大額債務拆分多筆小額存現之方式，屬結構化交易，旨在隱匿資金來源與性質。

重要案例 Significant Case Studies



法務部調查局洗錢防制處



法務部調查局



員警陳○○

匯入賭資或
償還賭債



甲賭場
經營者陳○銓

現金償還其他賭客賭資



甲賭場賭客



乙賭場賭客

員警陳○○以
MY-Police系統
查詢基資而
掌握行蹤



現金16萬5,000元



現金20萬元



員警陳○○
A銀行帳戶等8帳戶



現金8萬4,000元



乙賭場經營者
呂妻
A銀行帳戶



挪為私用



113年8月22日起訴：
刑法營利賭博及意圖營利供給賭博場所聚眾賭博罪、洩密罪、
貪汙治罪條例違背職務收賄罪及圖利罪等

肆、兆○公司涉嫌違反銀行法案

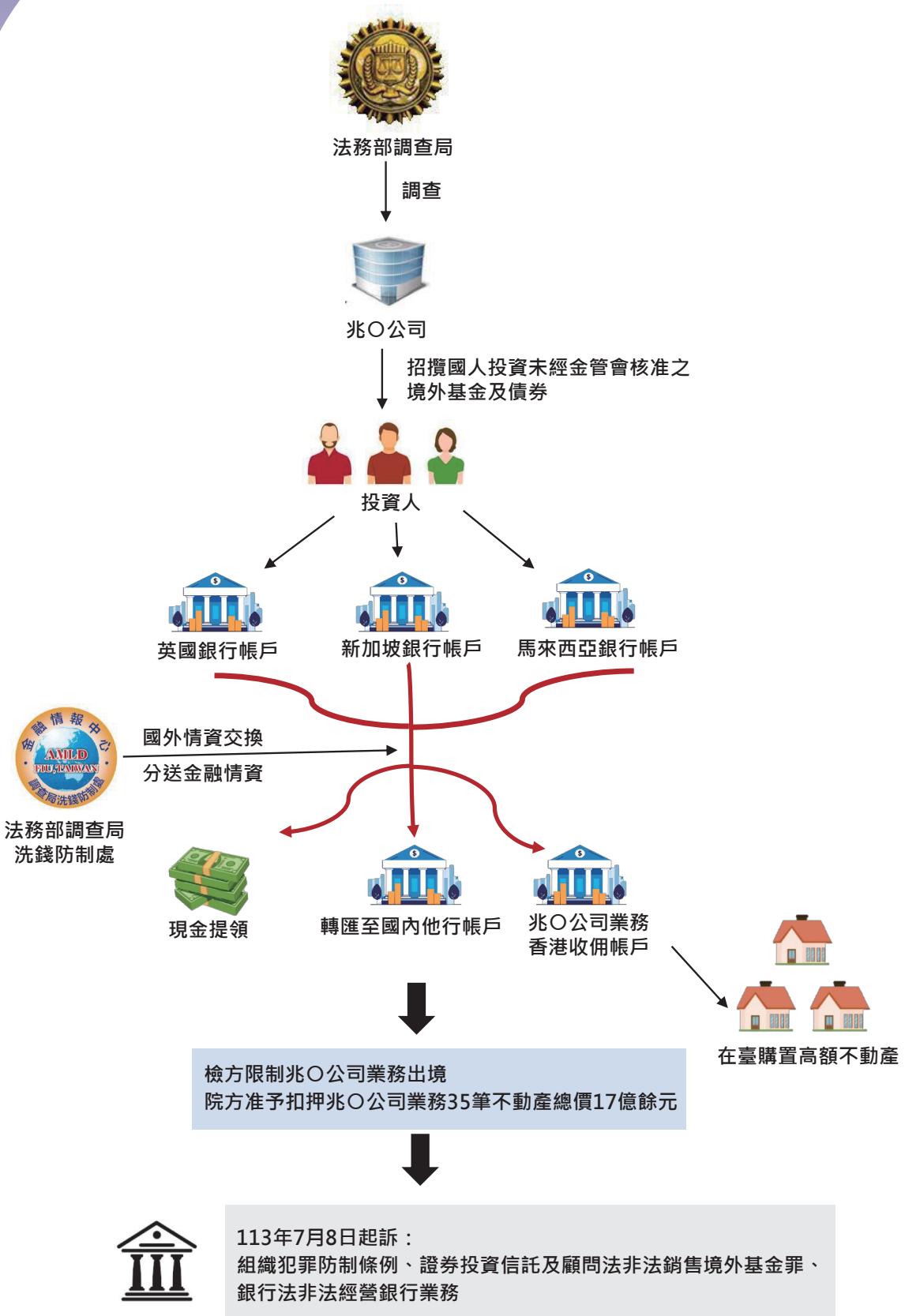
一、案情概述

112 年間，本局針對兆○公司展開調查，該公司涉嫌向不特定國人招攬投資未經金融監督管理委員會核准之基金及債券等金融商品，並約定保本且每年可獲 8% 至 15% 利息。調查發現，兆○公司銷售之金融商品係由境外公司發行，其投資款項收取及業務佣金發放均透過外國銀行帳戶進行。該公司業務人員嗣將其藏匿於海外之不法佣金，用於在臺購置高額不動產。本案所涉犯罪金額約新臺幣（下同）130 億元。同年 9 月，本局洗錢防制處透過國際合作，掌握案關金融商品境外發行公司在英國、新加坡及馬來西亞等地收受投資款之銀行帳戶資訊，藉此獲悉帳戶實質受益人資料，進而確認涉案外籍人士身分，亦透過洗錢防制處分送金融情報，了解該等帳戶資金主要源自我國投資人匯款，惟經本案犯罪嫌疑人以現金提領或匯款轉出，餘額所剩無幾，並進而即時掌握犯罪嫌疑人試圖移轉犯罪所得之動態，此亦為院檢迅速作成限制出境及扣押裁定程序提供關鍵依據。本案最後順利扣押本案犯罪嫌疑人名下 35 筆不動產，總價值約達 17 億餘元。

二、經驗參考

本案中，兆○公司非法銷售金融商品之發行公司、投資人投資款收款帳戶及業務佣金收款帳戶均位於境外，凸顯透過金融情報中心跨境交換金融情資對涉外案件偵辦之重要性。此外，銀行對可疑交易之偵測與申報，協助檢調機關確信兆○公司高層及業務人員已實際獲取佣金並著手進行不法所得之轉移與藏匿，促使執法機關有效防止犯罪嫌疑人潛逃，並成功扣押其不動產以利日後追徵犯罪利得。本案彰顯金融機構落實客戶盡職調查、持續監控及即時申報可疑交易報告，洗錢防制處迅速研編成金融情報提供偵辦單位掌握金流動向，對於打擊複雜金融犯罪及跨境洗錢活動之核心作用。

重要案例 Significant Case Studies



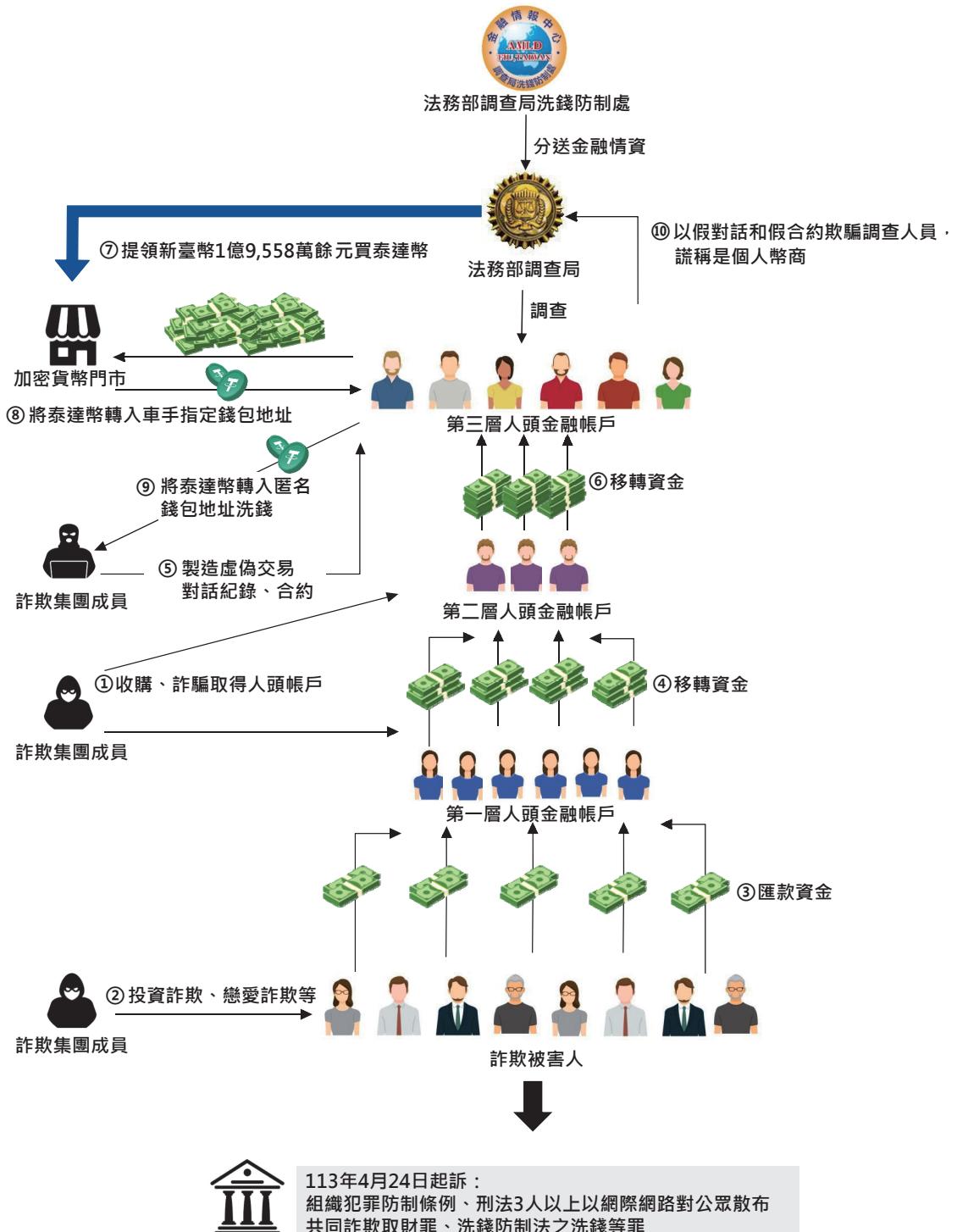
伍、鴻○公司曾○○等涉嫌詐欺洗錢案

一、案情概述

本局依據洗錢防制處於 112 年 9 月間分送之金融情報，查悉李○○等涉嫌人以大額現金（新臺幣 [下同] 50 萬元至 600 萬元）向虛擬資產服務提供商鴻○公司購買泰達幣（USDT）。調查顯示，李○○等人之操作模式為：其個人金融帳戶接收不明第三方大額轉帳後，隨即提領現金用以購買 USDT。該等虛擬資產隨後經多層匿名及非託管錢包轉移、分散，部分最終匯集至特定錢包，呈現典型洗錢之處置、多層化及整合特徵。李○○等人辯稱為「個人幣商」交易模式，並出示加密貨幣交易所 C2C (Customer to customer) 招攬廣告、偽造之 KYC 資料、LINE 交易對話及買賣合約佐證，惟調查發現，渠等實為詐騙集團操控之洗錢車手，利用個人或公司帳戶作為收受詐欺贓款之第三層帳戶。贓款經第一、二層人頭帳戶層轉後，由李○○等集團成員迅速提領購幣，並存入詐欺集團指定之非託管錢包。為掩飾犯行並取信金融機構，李○○等人復依集團指示偽裝為合法幣商，製作不實交易紀錄。統計自 112 年 2 月至 8 月，涉案 6 名「假幣商」以此手法洗錢金額近 2 億元。

二、經驗參考

詐欺集團透過分階段支付酬勞，誘使人頭帳戶提供者配合開通網路銀行約定轉帳功能並應對銀行照會，以利快速移轉贓款。本案中，人頭帳戶蘇○○（外送員）為詐欺集團第二層收款帳戶，其以偽造憑證（如進貨單）誑稱從事網路拍賣，成功設定李○○等車手帳戶為約轉帳戶（日限額達 300 萬元）。嗣後，蘇○○帳戶因密集大額轉出（兩週內近千萬元）觸發銀行照會，其再依指示謊稱購置虛擬資產，前後說詞不一，顯著提升洗錢風險。此外，詐欺集團亦利用公司帳戶以收付貨款外觀掩飾大額贓款移轉。建議金融機構強化對約轉帳戶設定之客戶盡職調查及交易審查，以降低人頭帳戶利用約轉功能快速移轉犯罪所得之風險。





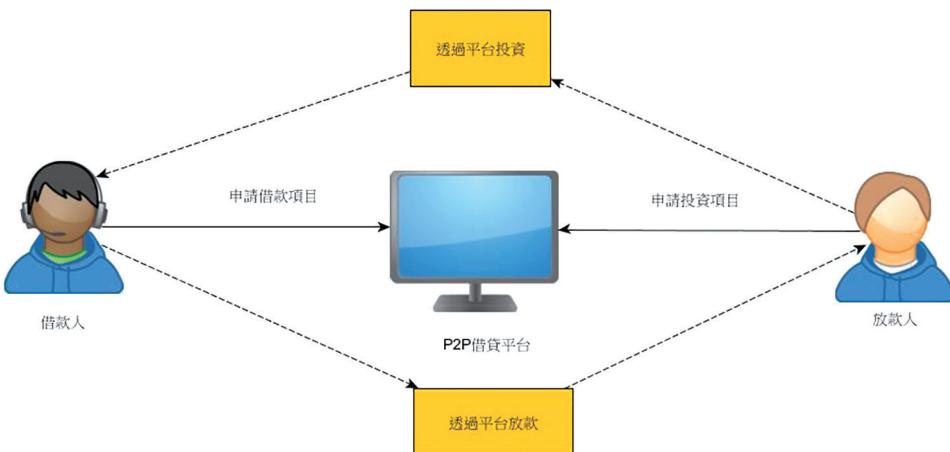
第五部分

策略分析報告

P2P 借貸平臺現況及洗錢風險

壹、P2P 借貸平臺簡介

P2P(peer-to-peer lending) 借貸平臺係指透過網路平臺，為出借人及借款人提供借貸媒介或債權轉讓媒介之中介機構¹，傳統借貸主要係由銀行或民間業者、營利法人或私人取得借款，現今因資訊科技推動新興金融服務多元快速發展，亦出現經由網路平臺媒介，即所謂點對點借貸模式，使一般人也得參與對不特定人放款而獲利。相較傳統銀行需信用聯徵、審查償還貸款能力等審慎、冗長申貸作業流程，P2P 借貸平臺使借款人能更快速、更容易取得借款，惟借款人藉此特性作為投資² 貸款利息較高，因此使得 P2P 借貸平臺較傳統銀行面臨更高風險。



國際組織金融穩定委員會 (Financial Stability Board) 及全球金融體系委員會 (Committee on the Global Financial System) 在 2017 年曾針對金融科技 (FinTech) 發表研究文章³，其中將 P2P 借貸平臺分為 5 種類型，臚述如下：

1 金管會 112 年 10 月 19 日「金管會發布網路借貸平臺業務事業指導原則」，網址 https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dateid=202310190002&dtable=News。

2 游子鈞，《臺灣 P2P 網路借貸之監理建議》，碩士論文，國立政治大學會計學系，108 年。

3 BIS 2017 年 5 月 22 日「FinTech credit: Market structure, business models and financial stability implications」，網址 https://www.bis.org/publ/cgfs_fsb1.pdf。

一、傳統模式 (Traditional Model)

傳統模式主要係提供訊息及媒合等服務，以資訊處理為主，本身不承擔風險，借款人申請為平臺會員，提供信用資訊等，投資人透過網站尋找借款標的，借貸合意不透由平臺，由投資人直接放貸給借款人，因為投資平臺未經手資金管理，通常會依照民事及商事法等規定處理。

二、公證模式 (Notary Model)

平臺與銀行合作，平臺作為投資人與借款人間媒合媒介，由銀行放款給借款人，平臺向銀行購回債權，再將收益憑證售予投資人，風險仍舊轉嫁至投資人身上，此種方式可規避借貸相關法律，並於美國、德國、韓國間盛行。

三、保證收益模式 (Guaranteed return model)

平臺為吸引投資人放貸，提供投資人本金或利息收益保證，在中國因為 P2P 借貸平臺競爭，曾有部分業者提出高達 12% 投資報酬率以吸引投資人參與放貸，惟 2016 年間中國銀行業監督管理委員會 (2018 年改制為「銀行保險監督管理委員會」) 發布「網路借貸資訊仲介機構業務活動管理暫行辦法」，規定平臺業者不可再向投資人直接或間接保證收益，期減少惡性競爭及詐騙案件。

四、資產負債表模式 (Balance sheet model)

平臺以自有資金放款與借款人，借款人也還款予平臺，平臺以出售債權方式出售予投資者以取得資金；美國頗盛行此種模式交易，例如美國學生借貸平臺 SoFI 即採此種模式。

五、發票交易 / 應收帳款承購 (Invoice trading model)

平臺業者出售發票⁴ 或應收帳款予投資人，投資人可以折扣金額得到全額票據或應收帳款，惟投資人須自行承擔跳票風險。

⁴ 我國多以票據提供給投資者

P2P 借貸平臺因低利率（對借款人）、高利息（對投資人）、簡化申請流程、快速獲得資金等特性，吸引許多被拒於傳統金融機構或借貸市場門外之借款人，以及想賺取高於銀行利率獲利之投資人，惟其面臨借款人違約風險也相對提高。在我國，P2P 借貸平臺非特許行業，亦無主管機關，故金融監督管理委員會於 113 年 10 月間公告「網路借貸平臺業務事業指導原則」⁵ 以協助、健全網路借貸平臺產業之正向發展，建議平臺業主對於借貸雙方提升風險控管機制，例如借貸雙方實名制、訂定借貸金流控管程序、如自有資金與客戶資金隔離，或以信託方式交付信託業管理等，然因風險評估過程中仍存在資訊不對稱等情形，投資人難以正確評估投資風險，故在 P2P 平臺業者或者借款人端仍暗藏滋生不法情事之疑慮。

貳、金融情報中心（FIU）觀察

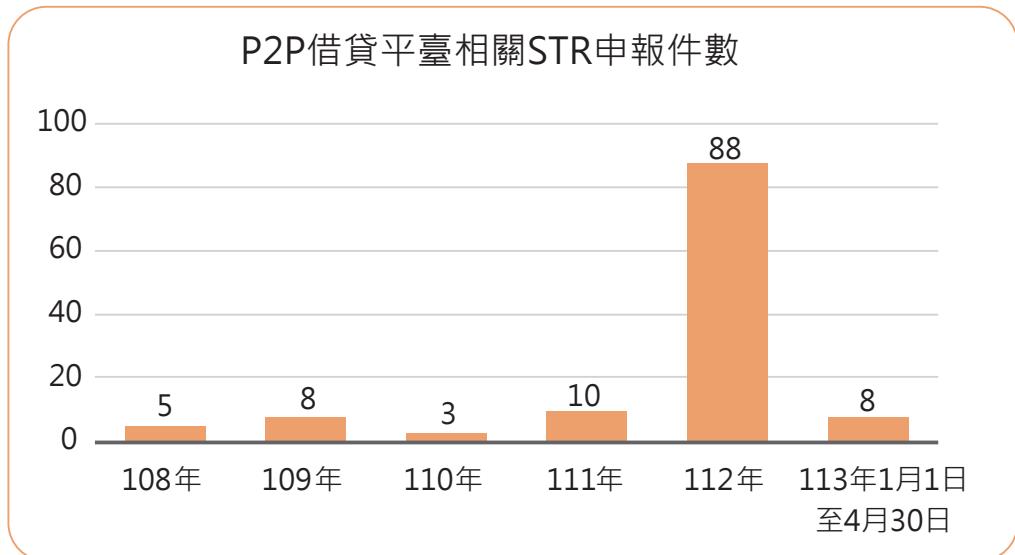
本報告係以 108 年 1 月 1 日至 113 年 4 月 30 日為統計期間，自受理申報之可疑交易報告中，篩選涉及「P2P」、「借貸平臺（台）」及「借貸媒合」關鍵字等可疑交易報告（下稱 P2P 借貸平臺相關可疑交易報告）進行分析。

一、可疑交易報告（STR）申報件數統計

（一）依申報年份：

本局於統計期間受理申報機關申報 P2P 借貸平臺相關可疑交易報告共計 122 件；其中 108 年間 5 件、109 年間 8 件、110 年間 3 件、111 年間 10 件、112 年間 88 件，113 年間（統計至 4 月 30 日）計 8 件。112 年間 P2P 借貸平臺相關可疑交易報告申報數量急遽增加，研判係因當年度「借貸媒合平臺 im.B」爆發不法情事，並經司法機關偵辦，進而推升申報數量。

⁵ 同註 1。



(二) 依申報業別：

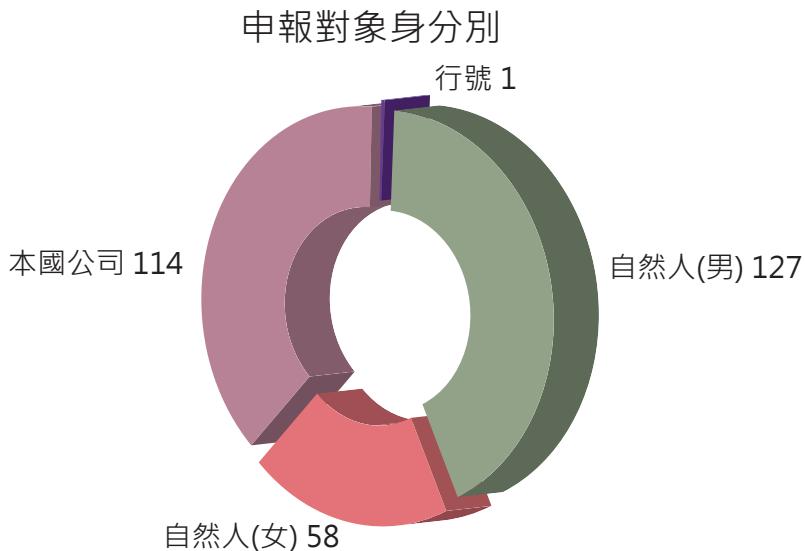
統計期間申報 P2P 借貸平臺相關可疑交易報告之申報機構主要為本國銀行，其餘包含保險公司、期貨商、證券商、農會及信用卡公司等，詳細數據如下表：

申報機構	申報件數
本國銀行	109
保險公司	4
期貨商	4
證券商	3
農會	1
信用卡公司	1

二、可疑交易報告申報對象

統計期間受理 P2P 借貸平臺相關可疑交易報告中，申報對象⁶共計 300 名，其中自然人 185 名(男性 127 名、女性 58 名)、本國公司 114 間、行號 1 家。

⁶ 每件 STR 可申報 1 個以上對象。



申報機構多經由向客戶 KYC、查詢公開資訊或媒體負面報導等，辨識客戶本身或其交易對象與 P2P 借貸平臺相關，其中法人部分多係主營 P2P 借貸平臺或與 P2P 借貸平臺公司有資金往來，自然人部分則係 P2P 借貸平臺公司負責人、董監事、員工等或與 P2P 借貸平臺間有資金往來人員，經研認其交易情形異常進而申報可疑交易報告。

三、可疑交易報告疑似洗錢表徵

各洗錢防制主管機關針對不同行業別，均提供「疑似洗錢或資恐交易態樣」作為辨識異常金融交易及評估申報可疑交易報告指標，申報機構再自行依以風險為本之方法（Risk-based approach）進行交易審查、分析及評估，統計期間受理 P2P 借貸平臺相關可疑交易報告相關洗錢表徵主要包含：

- (一) 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。
- (二) 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。
- (三) 其他有疑似洗錢交易情形者。
- (四) 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。
- (五) 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。

四、可疑交易報告常見申報態樣

歸納各申報機構指涉之 P2P 借貸平臺營運模式，包含：

(一) 個人小額信貸 P2P 債權：

借款人為個人戶，部分借貸平臺有特定借款人客群，如學生或外籍移工等。

(二) 企業應收帳款（票據）轉讓：

借款人為法人戶，主要由企業借款人將其應收帳款（票據）轉讓予借貸平臺，再由投資人單獨或集資提供借款。

(三) 不動產借貸媒合：

以不動產作為擔保品，由借貸平臺承作不動產抵押設定借貸媒合，並提供債權讓與等相關手續服務；亦有部分借貸平臺以海外不動產債權作為投資標的。

(四) P2P 標會借貸：

主要運作模式與民間合會雷同，借款人與投資人均須繳交保證金成為會員，每期由欲借款者共同競標，得標之借款人取得當期所有標金，之後每期繳交固定會費直到會期結束，未得標的人則每期繳交活會會費（固定會費扣除當月標息）。

五、可疑交易報告分送運用情形

統計期間受理 P2P 借貸平臺相關可疑交易報告經加值分析後，產製計 54 件金融情報並分送予執法機關（包含法務部調查局、內政部警政署、臺灣高等檢察署等）及監理機關（金融監督管理委員會）參處，108 年至 113 年（迄 4 月 30 日止）各年度分送件數分別為 3 件、4 件、2 件、3 件、38 件及 4 件。

參、P2P 借貸平臺常見犯罪態樣及遭濫用風險

一、以 P2P 借貸之名，行詐騙吸金之實：

P2P 借貸平臺作為借款人與投資人中介，其主要營運收入應來自借款人及投資人利用該平臺服務而繳納之服務費，惟當營運狀況不如預期，

不肖 P2P 借貸平臺恐利用製造假借款人或偽造假債權，讓投資人誤認有高利息之出借款項投資機會，或另利用業務員以實體或網路管道宣稱「高報酬率」或「期滿保本回收」等宣傳手法，向不特定民眾吸收資金，實則將收到之投資款項作為下一批放款之本金，持續以後金養前金；另因 P2P 借貸平臺上所有借款人與投資人資訊均掌握在平臺業者手中，致生嚴重資訊不對稱情況，不肖 P2P 借貸平臺為吸引投資人，亦可能製造假投資人認購債權，營造出投資活絡之表象，藉此誘使投資人投入資金。112 年間經偵辦之「借貸媒合平臺 im.B」案，其犯案手法即包含前述態樣。

二、背信及破產風險：

P2P 借貸平臺之借款及投資，其收款及繳款方式依平臺營運模式而有所不同，部分 P2P 借貸平臺係由投資人將出借款項匯至 P2P 借貸平臺帳戶後，再由 P2P 借貸平臺統一轉予借款人，此種運作方式優點在於投資人無須與借款人間有直接金錢往來，惟若 P2P 借貸平臺內部發生不法，例如負責人或員工挪用投資人投資或借款人返還款項，抑或平臺經營不善，則可能產生平臺人員背信或公司破產風險，造成投資人損失。

肆、研析建議

一、P2P 借貸平臺資金信託：

因 P2P 借貸平臺業者與借款人及投資人間資訊不對稱，為避免因管理不當而產生之風險，建議相關平臺應透過類似基金信託方式，將客戶資金與業者自有資金進行隔離，以避免款項遭到挪用。

二、第三方查核：

P2P 借貸平臺應定期由諸如會計師等第三方專業人士進行查核，認證包含其媒合借貸案件雙方資訊、債權來源及金流等真實性，並宜將相關資料公開。

三、加強民眾正確投資觀念：

P2P 借貸平臺雖具有普惠金融效益⁷，惟在高報酬的誘因下，其風險實則可能高於金融機構所提供之金融商品，爰認 P2P 借貸平臺應充分向投資人揭露相關風險，且政府相關單位及金融機構亦宜持續向民眾宣導正確投資理財觀念，避免民眾誤信不實吸金廣告而血本無歸。

伍、參考文獻

一、期刊論文：

- (一) 鍾郁婕，《台灣 P2P 網路借貸之研究》，碩士論文，國立政治大學金融學系，105 年。
- (二) 游子頡，《臺灣 P2P 網路借貸之監理建議》，碩士論文，國立政治大學會計學系，108 年。
- (三) 林梨華，《歐美 P2P 借貸平台規範之研究—兼談我國未來法制之發展》，國會季刊，第 52 卷第 1 期，113 年。

二、網路資料：

- (一) 金管會 112 年 10 月 19 日「金管會發布網路借貸平臺業務事業指導原則」，網址 https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202310190002&dtable=News。
- (二) BIS 2017 年 5 月 22 日「FinTech credit: Market structure, business models and financial stability implications」，網址 https://www.bis.org/publ/cgfs_fsb1.pdf。

⁷ 中央銀行 107 年 9 月 27 日「主要國家 P2P 借貸之發展經驗與借鏡」，網址 <https://www.cbc.gov.tw/public/attachment/892717204371.pdf>。



第六部分

國外洗錢防制 資料

FATF 報告

偵查、打擊及調查網路兒童性剝削犯罪： 運用金融情報保護兒童免受傷害¹

2025 年 3 月

註：本文業經 FATF 畘書處授權法務部調查局摘譯為中文並載於本年報，非 FATF 官方正式文件，仍以英文原版內容為準。

網路兒童性剝削（Online Child Sexual Exploitation，OCSE）是一種令人髮指之犯罪行為，受害者是最脆弱之群體—我們的孩子。隨著兒童接觸網路、社群媒體及遊戲平臺之機會增加，加上現代科技提供之內容幾無限制，OCSE 已成為當今兒童面臨之重大風險，近年情況尤為猖獗。

OCSE 已被 FATF 列為「指定犯罪類別」，所涉犯罪行除對兒童之性剝削外，亦可能涉及組織犯罪、詐騙、人口販運及勒索等不法。司法管轄體追查 OCSE 相關資金流動及不法所得之成果，將可望納入相互評鑑報告中洗錢／資恐風險評估。

FATF 針對此議題成立專題小組進行研究，由澳洲和英國代表團共同主持，小組成員由來自巴西、加拿大、象牙海岸、歐盟委員會、印度、印尼、愛爾蘭、盧森堡、墨西哥、荷蘭、新加坡、西班牙代表團等，以及亞太防制洗錢組織（APG）、艾格蒙聯盟（EG）、國際刑警組織（Interpol）等。研究內容涵蓋對 OCSE 進行背景分析，提出金融交易及相關檢測技術的指標，檢測、破壞與調查 OCSE 的較佳作法及所面臨之挑戰等項目，期有助於 FATF 等相關國際組織、各國權責機關、政策制定者、從業人員、金融機構、指定非金融事業或人員、虛擬資產服務提供者、非營利組織等對 OCSE 相關資金流動及相關調查查緝行動之瞭解。專題報告於 2025 年 2 月通過，並於同（2025）年 3 月發布。

本報告所指 OCSE 細分為兩種犯罪，分別為直播兒童性虐待（Live-

¹ 文獻引用格式：防制洗錢金融行動工作組織（2025），偵查、打擊及調查網路兒童性剝削（Detecting, Disrupting and Investigating Online Child Sexual Exploitation），FATF，法國巴黎，<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html>

streamed Sexual Abuse of Children, LSAC) 及兒童經濟性虐待 (Financial Sexual Extortion of Children, FSEC)，定義如次：

● **網路兒童性剝削** (Online Child Sexual Exploitation, OCSE) :

利用網路實施或助長對兒童之性剝削，此定義可指所有 OCSE 犯罪類型，有時則專指對兒童之直播性虐待及經濟性勒索。

● **直播兒童性虐待** (Live-streamed Sexual Abuse of Children, LSAC) :

基於經濟利益直播兒童性虐待片段，具體而言，係指即時傳輸或分享任何描繪兒童獨自或與他人進行性行為之素材，供消費者付費線上觀看。

● **兒童經濟性勒索** (Financial Sexual Extortion of Children, FSEC) :

以曝光兒童之色情圖片或影片為要脅，強迫受害者滿足其財務要求。

(以下為摘譯專題報告第二、三部分偵測及調查網路兒童性剝削犯罪提及偵測不法金融交易與運用金融情資展開調查之成功案例)

第二部分：偵測網路兒童性剝削

透過金融指標偵測 OCSE

因偵測 OCSE 之金融指標須與時俱進，各司法管轄體應與金融情報中心² (Financial Intelligence Unit, FIU) 、申報機構³ 、執法機關及其他相關單位持續合作，藉此強化該些指標。

識別與直播兒童性虐待相關之金融交易

LSAC 之消費者通常使用金錢或價值移轉服務 (Money /Value Transfer Service , MVTS)，例如 PayPal 等線上 P2P 支付系統支付費用，少數則透過銀行存款或虛擬資產服務商 (Virtual Asset Service Provider , VASP) 付款，其中使用 Grab 或 OnlyFans 等支付應用程式之比例日益增加。申報主體若有提供此類金融服務，可結合以下指標偵測疑涉 LSAC 案件之交易：

直播兒童性虐待相關金融交易之整體指標

- 從已開發國家匯款至兒童性剝削高風險之司法管轄體。

2 我國之金融情報中心為法務部調查局洗錢防制處。

3 我國之申報機構為《洗錢防制法》第五條規定之金融機構及指定之非金融事業或人員。

- 匯款人與受款人年齡差距大。
- 小額（每次 10 至 200 歐元等值金額）交易，以來源國或目的地國貨幣計價，或等值法定貨幣金額之虛擬資產交易。
- 受款人位處另一司法管轄體，且匯款人與受款人間無明顯合法關聯。
- 不定期交易，但於同一日或連續數日重複匯款至相同帳戶。
- 於深夜或清晨進行交易（顯示消費者可能處於不同時區）。
- 交易備註社群媒體、使用者名稱、性或色情術語，或收到資料之日期／時間。
- 詳細之金融歷史紀錄顯示是長期付款，且消費者與服務提供者間已建立長期關係。
- 交易可能被描述為醫療或生活費用，或指涉匯款人與受款人間關係，例如「家庭支持」、「學費」、「援助」、「醫療費用」、「住宿」、「禮物」、「購買衣服／玩具」、「制服」、「男友」、「女朋友」或「贊助商」等。
- 購買線上加密工具、VPN 服務、反追蹤軟體或其他線上隱私與匿名工具或服務。
- 與 Facebook、Microsoft、Google Play、OnlyFans、TikTok、Instagram 或其他社交媒體網站（如 Micous）有大量交易之帳戶或客戶。
- 與性犯罪者有關之交易。

消費者進行之交易

- 與設於 LSAC 高風險司法管轄體之帳戶進行交易，或在該些司法管轄體登入帳戶（例如以 ATM 提現或從該些司法管轄體 IP 登入）。
- 在約會平臺或成人娛樂平臺上消費。
- 在網路攝影／直播平臺（包括成人娛樂平臺）上消費。
- 在線上遊戲平臺或遊戲商店消費。
- 購買影片截圖軟體。
- 向涉犯兒童性剝削（包括任何引誘）相關罪行之個人及／或共同交易方匯款或收款。
- 與因兒童性剝削相關犯罪而遭媒體負面報導之個人有關之交易。

協助者 / 濫用者進行之交易

- 款項匯入後通常會立即提領。
- 受款者因涉嫌協助 OCSE 而遭執法機關調查。
- 為社群媒體平臺之高級功能或服務付費。
- 購買可用於網站或社群媒體之影片截取軟體。
- 在線上遊戲平臺或遊戲商店進行交易。
- 購買間諜軟體或監控應用程式。
- 多筆來自國外（特別是 LSAC 消費高風險國家）相似金額之存款，包括在相同或相近時間之存款。
- 向線上文件託管服務提供商／平臺付款。
- 在創作者內容串流網站上消費（包括會員費、訂閱費，或付款予該些網站其他直播主）。

儘管單一指標未必與潛在 LSAC 犯罪案件有關，惟結合上開指標與交易及客戶相關之其他因素，可協助申報機構觀察可疑活動模式。

透過金融交易辨識兒童經濟性勒索犯罪

多數兒童經濟性勒索受害者表示，他們支付贖金之方式是透過前述 PayPal 等線上 P2P 支付系統、銀行轉帳、VASP 或禮物卡。申報主體若有提供此類服務，可結合以下指標發現可能存在兒童經濟性勒索犯罪之相關交易：

兒童經濟性勒索相關交易之一般指標

- 兩個人之間進行交易，但無明顯關聯（例如無共同姓氏、無明確商業目的）。
- 交易金額通常少於 500 歐元，但有時高達 1,500 歐元。
- 匯款人（受害者）與受款人（犯罪者）之第一筆交易通常少於 250 歐元。
- 匯款人與受款人在短時間內進行多筆交易，之後完全停止。
- 與兒童經濟性勒索常見國家（即象牙海岸、奈及利亞、菲律賓等）進行之交易。申報機構應注意該等高風險司法管轄體變動之趨勢。
- 交易目的提及社群媒體或使用者名稱、性或色情術語、威脅／懇求語言或收到資料之日期／時間。
- 交易受款人與匯款人非同一地區。

- 付款附言看似慈善捐款。
- 交易與性犯罪者有關。

受害者進行之交易

- 由青少年或年輕成年男性支付予年紀較小之青少年或年輕成年女性之交易。
- 若為跨國交易，主要源自英語國家。惟申報機構應注意，隨著協助者日益老練世故，語言將逐漸不再是判斷指標。
- 客戶舉報交易涉及性勒索。
- 付款通常發生於晚間 7 點至早上 7 點間（通常是性勒索發生時）。
- 匯款人（受害者）未輸入受款人姓名（僅輸入收款人之一般稱呼）或受款人姓名與實際帳戶持有人不符。
- 匯款人帳戶中之資金在數小時內減少（通常少於 24 小時）。
- 異常購買數位禮物卡或遊戲點數。
- 個人 P2P 平臺帳戶使用方式異常。
- 異常之虛擬資產購買行為。
- 當銀行行員關懷時，匯款人閃爍其詞或無法提供合理解釋。
- 購買多張禮物卡之客戶（例如亞馬遜、PlayStation 或其他遊戲提供者）。

犯罪者進行之交易

- 單一帳戶接收多筆明顯不相關之匯款。
- 收款帳戶之款項存在多個互無關聯之匯款理由。
- 收到之款項立即移轉。
- 向提供隱私與／或匿名性之線上服務付款（即加密、VPN、虛擬電話號碼等）。
- 與多張預付信用卡或禮物卡相關之付款。
- 從不同司法管轄體之多個線上文件託管行銷服務（如按次下載付費模式）接收款項。
- 在收到款項後短時間內購買商品（車輛、房地產、家用電器），且無法說明正當理由。
- 生活方式及消費與其工作收入不符。

儘管單一指標未必與潛在經濟性勒索行為有關，惟申報機構應考慮所有交易因素，以及交易是否符合上述指標。

第三部分：調查網路兒童性剥削

偵測並識別針對兒童之直播性虐待及經濟性勒索

許多犯罪之所以能偵破，有賴於受害者報案，但就 OCSE 犯罪卻不然。對於 FSEC，雖然受害者舉報係偵測之重要來源，但他們經常因尷尬及害怕私密圖像曝光被勒索，而不願報案，這導致 FSEC 成為被嚴重低估之犯罪行為。

受害者報告在 LSAC 偵測中更為罕見，歸因於受害者年齡、脆弱性、報案管道限制，以及虐待環境中存在之脅迫或家庭關係等因素。

鑑於 LSAC 和 FSEC 受害者主動舉報不易，金融交易及資訊成為偵測 OCSE 之關鍵資源，然而，這並非唯一偵測手段，各國亦強調私部門轉介及網路臥底工作等偵查方法之功能。就 LSAC 案件而言，偵測消費者或協助者活動最主要之方式是取得來自其他國家之情報。

運用金融資訊

第二部分已列出可用於識別 LSAC 或 FSEC 相關交易之指標，將識別出之交易即時通報予 FIU 及執法機關，是偵測 OCSE 之關鍵。

於調查期間或透過 FIU 獲得之金融情報，均有助發現及打擊跨國犯罪。澳洲聯邦警察之經驗顯示，大部分 LSAC 消費者會持續與海外犯罪分子聯繫。當與其他資料來源（例如美國國家失蹤與受虐兒童中心 [NCMEC] 之 Cyber Tipline 報告）結合時，金融情報可協助建立更準確之潛在罪犯檔案，進而與國內邊境安全機構或國際執法夥伴共享資訊。

以南半球某 VASP 業者為例，他們不僅嚴格監控交易，亦部署廣泛之風險指標、員工教育訓練，並與主要商業夥伴、政府及執法機關合作，以解決 OCSE 相關問題。該 VASP 業者投入大量員工與客戶積極互動，藉此更加瞭解客戶使用其平臺之目的，並在其交易模式發生變化時進行更妥善之監督，從而提高偵測高風險行為之能量。一旦懷疑或發現有勒索行為，該 VASP 即提交可疑活動或交易報告予 FIU，並將問題轉交給保護機構。

運用金融資訊調查 OCSE 案例分享

印尼金融情報中心（PPATK）運用金融資訊

據 PPATK 收到之資訊，紐西蘭公民 X 先生自 2021 年開始匯款至菲律賓、越南、阿拉伯聯合大公國及印尼，這些交易涉嫌用於支付與兒童性剝削相關之圖像費用，交易備註包括「禮物」、「照片及樂趣」及「測試轉帳」。

PPATK 資料庫顯示，X 頻繁與印尼女性進行小額且重複性交易，其中一位受款人 A 女士常用「byr amer」、「bayar room」等可疑交易描述，並與旅館、卡拉 OK 及娛樂等產業老闆及員工交易，A 就住在峇里島這個 OCSE 案件密集發生之旅遊區，她接收來自多個國家男性之匯款，總計 1.73 億印尼盾（約 10,000 歐元）。

加拿大影子計畫

SHADOW 計畫是加拿大豐業銀行與加拿大兒童保護中心共同主導之公私合作項目，旨在打擊網路兒童性剝削，並獲得加拿大執法機構及金融情報中心 FINTRAC 之支持。FINTRAC 藉此識別與共享金融指標，協助申報實體識別出與 OCSE 相關之洗錢交易。

FINTRAC 之金融指標曾應用於 FSEC 案件，受害者向網友傳送自己之色情影片，對方威脅若不支付 400 加元就會散播出去。受害者支付款項後向執法機關報案，執法機關復將犯罪資訊提交 FINTRAC。

同時，根據 FINTRAC 開發之 OCSE 指標，申報實體亦會標註這些交易。FINTRAC 藉此確認相關非法資金之流向，並將涉案之加拿大各銀行帳號及個人身分識別資訊提供給執法機關，俾其利用這些資訊進行犯罪調查。

澳洲反兒童剝削中心（ACCCE）開發即時偵測疑似兒童經濟性勒索付款金融交易

澳洲國民銀行（NAB）與澳洲聯邦警察主導之澳洲反兒童剝削中心（ACCCE）開發出幾乎即時主動偵測疑似兒童經濟性勒索付款之方法，NAB 每天向潛在之兒童經濟性勒索受害者發出警報，主要是針對尚未報案之受害者。每個工作日都會對警報進行分類，一旦發現潛在受害者，就會向 ACCCE 披露，隨後 ACCCE 會致電受害者。NAB 透過深夜付款給新受款人、一夜之間花光積蓄等跡象，成功辨識出一名受害者，並在轉帳完成數小時內將此資訊轉交 ACCCE。ACCCE 對 NAB 之直接回饋，佐證近乎即時辨識之正面影響：

「我可以確認，（受害者）確實是性勒索之受害者，我已經與在（某地點）之他和他母親談過了。我們非常感謝你們（NAB）的警報功能，因為（受害者）尚未向當局報案，且仍然受到詐騙者之壓力—甚至於我們通話期間亦然。我很高興他現在獲得了適當的支持，也不再需要與騙子打交道。我已經舉報這個違規社交媒體帳戶並要求將其刪除。（受害者）說他已經與澳洲國民銀行之代表談論過付款事宜。」

此法成功打擊此類犯罪行為，並為受害者提供支持之有效方法。

其他偵測機制—私部門之轉介

LSAC 與 FSEC 均是仰賴網路基礎設施進而促進犯罪發生，OCSE 相關基礎設施包括社交媒體平臺、網路服務供應商、行動網路營運商、訊息應用程式、雲端服務、內容發送網路、瀏覽器及應用程式商店等。此私部門基礎設施，或根據美國全國失蹤與受剝削兒童中心 (National Center for Missing & Exploited Children, NCMEC) 分類稱為電子服務提供商，可直接偵測 OCSE，在某些情況下，還可以即時偵測。

大多數司法管轄體規定私部門須配合執法機關並提報所發現之犯罪嫌疑或活動；當局應與私部門合作，並確保資訊受到適當保護，特別是機密或敏感資訊。

NCMEC 之 Cyber Tipline 是一家總部位於美國之非營利組織，可作為電子服務提供商向美國或其他司法管轄體提交疑似 OCSE 報告之管道，之後這些報告會再提供給各國執法機關，這對於偵測及調查 OCSE 至關重要。

NCMEC 於 2023 年收到近 3,600 萬份疑似兒童網路性剝削之 Cyber Tipline 報告，但這些報告來自 245 家公司，其中 5 家公司佔報告總數九成以上，且並非所有報告均具參考價值。舉報之公司應提供充分資訊（例如用戶詳細資訊或其位置），並採取行動識別及保護所涉及之受害者。報告品質欠佳不僅無法提供有意義之偵測，反會增加分析之報告數量，徒增 NCMEC 或其他對等機構之負擔。儘管尚有前述之改善空間，Cyber Tipline 報告仍為調查人員提供具體、及時且可操作之線索，美國以外之國家經常運用 NCMEC 資訊，採取措施將其與其他國內來源之資訊結合運用，並獲得良好之成效。



第七部分

本局洗錢防制 重要紀事

❖ 第一季

出席法務部召開「洗錢防制法修法會議」

赴韓國首爾出席「對抗俄羅斯先進常規武器與國防技術在物流及半導體產業之擴散研討會」

赴馬爾他參加 EG 工作組會議

參與法務部召開「資恐防制法修法研商線上會議」

與史瓦帝尼金融情報中心首長進行線上會議

參與美國國務院在臺辦理「資助武器擴散特徵分析工作坊」

出席行政院召開「打詐專法審查會議」

❖ 第二季

參與 FATF 與國際證監會組織 (IOSCO) 「虛擬資產及虛擬資產服務提供商之 AML/CFT 規範線上研討會」

出席行政院洗錢防制辦公室召開「防制洗錢打擊資恐及資武擴資訊交流平臺策進會議」

參與「APG 重大貪瀆案件線上研討會」

赴法國巴黎參加 EG 第 30 屆年會

出席美國在臺協會 (AIT) 在臺辦理「商業和國防供應鏈中軍民兩用技術採購之 KYC 研討會」

赴新加坡參加 FATF 6 月大會暨工作組會議

❖ 第三季

出席行政院洗錢防制辦公室召開「2024 年國家洗錢資恐及資助武擴風險評估報告草案會議」

出席數位發展部數位產業署召開「第三方支付服務業防制洗錢精進措施及聯防機制研商會議」

出席美國駐臺機構舉辦「International Sanctions Compliance and Due Diligence for the Oil and Gas Industry 研討會」

與賴索托金融情報中心代理局長業務會談

舉辦「新興犯罪與異常交易態樣研討會」

❖ 第四季

直布羅陀金融情報中心首長來訪

參與「APG 相互評鑑委員會線上會議」

赴阿拉伯聯合大公國阿布達比出席 APG 年會

APG 與行政院洗錢防制辦公室及本局洗錢防制處共同在臺舉辦評鑑員訓練研討會，APG 秘書處代理副秘書長 David Shannon 來訪

赴澳洲雪梨出席「ARIN-AP 年會」

赴馬來西亞吉隆坡出席「APG 洗錢態樣研討會」

赴柬埔寨暹粒出席歐盟防制洗錢及打擊資恐全球合作機構 (EU AML/CFT Global Facility) 等組織合辦「藝術品及文物犯罪調查運用防制洗錢及打擊資恐機制研討會」

舉辦「金融機構防制洗錢人員聯繫業務研討工作餐敘」

中華民國 113 年

洗錢防制工作年報

出版機關：法務部調查局

發 行 人：陳白立

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：中華民國 114 年 10 月

版權所有，如有引用，請詳載出處

GPN：1011401052

ISBN：978-626-7220-76-4

