洗錢防制工作年報

中華民國一〇八年

ANTI-MONEY LAUNDERING ANNUAL REPORT, 2019

法務部調查局編印

Investigation Bureau, Ministry of Justice,
Republic of China (Taiwan)

出版日期：109年10月

法務部調查局一〇八年洗錢防制工作年報

Investigation Bureau, Ministry of Justice

Anti-Money Laundering Annual Report, 2019

序 言 *PREFACE*

在 37 個公部門及 31 個私產業傾力合作下，我國順利完成亞太防制洗錢組織（Asia/Pacific Group on Money Laundering，APG）第三輪相互評鑑，經 APG 完成全球審查程序後，相互評鑑報告於 108 年 10 月 2 日正式公布，我國獲得「一般追蹤」（Regular follow-up）最佳成績，為我國防制洗錢及打擊資恐工作樹立重要里程碑，也成為亞太地區會員國效法之標竿。本局洗錢防制處自 86 年 4 月 23 日執行我國金融情報中心任務迄今，持續建構金融情資之受理、分析、分送機制，於第三輪相互評鑑過程中，更以具體成效展現國家金融情報中心之功能與價值，執行效能深受評鑑團肯定，在相關的效能評鑑項目均獲得「相當有效」（Substantial level of effectiveness，SE）之評鑑等級，對於我國取得「一般追蹤」佳績委實功不可沒。

本局洗錢防制處作為全國金融情報的傳遞樞紐，除負責受理金融機構及指定非金融事業或人員申報金融情資，將加值分析後的金融情報分送予執法、稅務等權責機關參考運用外，並與權責機關密切合作，追查有關資恐、洗錢及相關前置犯罪之犯罪所得。在受理金融情資部分，108 年間本局受理之可疑交易報告、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）攜帶或以貨物運送、快遞、郵寄等方法運送用於洗錢物品數量分別為 26,481 件、3,092,985 件及 360,336 件，另就分送金融情報而言，108 年度，經本局洗錢防制處加值分析後，運用 2,881[1] 件 STR 編製成 2,512 件金融情報，分送予權責機關參考運用。

為掌握國際防制洗錢規範趨勢及深化國際合作，本局洗錢防制處積極參與防制洗錢金融行動工作組織（Financial Action Task Force on Money Laundering，FATF）、APG、艾格蒙聯盟（Egmont Group）及亞太區追討犯罪所得機構網路（Asset Recovery Inter-Agency Network of Asia/Pacific，ARIN-AP）等防制洗錢及打擊資恐相關國際組織會務活動，並藉該等活動場合與各國代表共聚一堂，深度研商實質合作議題。同時也透過艾格蒙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。另外 108 年間，我國與瓜地

[1] 統計截止時間：109 年 7 月 13 日上午 9 時 50 分。

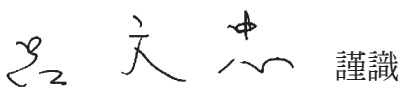
馬拉、東帝汶、東加、巴布亞紐幾內亞及約旦哈希米王國等 5 國金融情報中心完成簽署關於涉及洗錢、相關前置犯罪及資助恐怖主義金融情資交換合作協定 / 備忘錄，進一步深化雙邊合作關係。

全球資助恐怖主義及大規模毀滅性武器擴散（簡稱：武擴）態樣日趨複雜，相關融資行爲與新科技方法之結合，更加劇渠等對國際和平與區域安全之威脅，本局洗錢防制處持續推動打擊資恐及資助武擴工作，於 107 及 108 年受理資恐與武擴相關之可疑交易報告件數共三百餘件，且爲有效汲取國際反恐趨勢及具體策略，該處也派員參加澳洲政府於 108 年舉辦之「不爲恐怖行爲融資 - 打擊資恐部長級會議」，藉由參考他國對抗恐怖主義之成功經驗，強化我國反恐能量。另邀請本局何凱婷調查官針對目前國際間關於打擊資助武擴之國際規範及我國現況相關法制及實際案例撰寫專題報告，以作爲公私部門打擊資助武擴之防制參考。

108 年間，金融監督管理委員會公告 3 家純網路銀行通過審核取得許可設立執照，顯示我國金融服務業的數位時代即將來臨。然而伴隨著更便捷、更有效率的金融服務內容，資安、洗錢及資恐等風險也隨之升高，是以金融業者在推動惠普金融科技之際，必須正視客戶盡職調查的重要性，設法降低相關風險。FATF 於 109 年 3 月發表「數位身分指引」（Digital Identity）指引，協助金融機構強化以風險爲本之數位身分查驗，以期符合 FATF 第 10 項建議關於客戶盡職調查之要求。本局洗錢防制處在徵得 FATF 同意後，特將其翻譯成中文收錄於本年報，謹供相關權責機關及私部門參考。

本年報雖經審愼校訂，仍恐有疏漏、錯誤或淺薄未及之處，尙祈各方先進不吝指正。

法務部調查局　局長



謹識

中華民國 109 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

本年報分下列七個部分：

（一）組織簡介。

（二）工作概況（含統計圖表資料）。

（三）重要案例。

（四）專題研究。

（五）策略分析報告。

（六）國外洗錢防制資料。

（七）洗錢防制處重要紀事。

三、凡例

（一）本年報所用各項單位，年度以國曆爲準，專題研究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，以件爲單位；海關之通報資料，以筆爲單位。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）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。

（三）本年報第二部分工作概況之相關統計數據係以 109 年 3 月 2 日爲基準日。

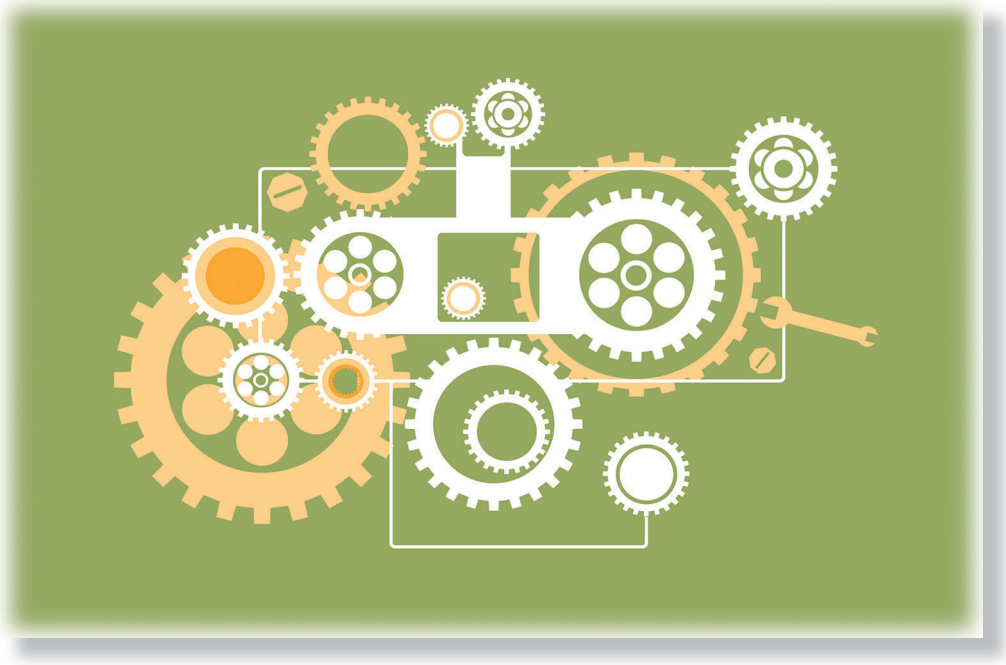
四、本年報倉促付梓，錯誤及未盡周延之處，敬請不吝賜教，俾以訂正。

表目錄

圖目錄

第一部分

組織簡介



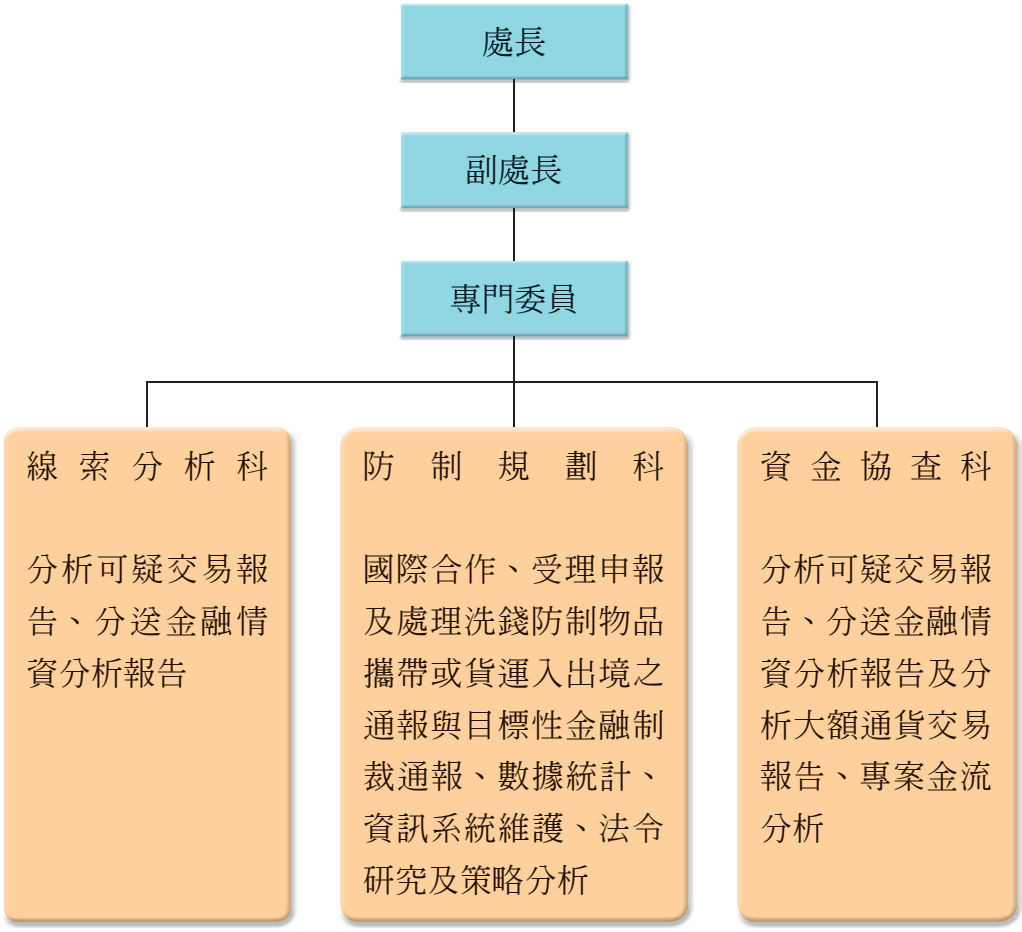
國際間鑑於毒品犯罪所獲得巨額利潤和財富，使得犯罪集團能夠滲透、腐蝕各級政府機關、合法商業或金融企業，以及社會各階層，因此西元 1988 年維也納會議時，訂定《聯合國禁止非法販運麻醉藥品及精神藥物公約》（簡稱維也納公約）即要求締約國立法處罰毒品犯罪的洗錢行爲。七大工業國體認到毒品犯罪所涉洗錢行爲，對於銀行體系與金融機構產生嚴重威脅，於 1989 年之高峰會議中決議設置 FATF，發展並提升國際對於打擊洗錢之回應。FATF 於 1990 年制訂 40 項防制洗錢建議，作爲國際間防制洗錢之標準規範，1996 年 FATF 修正 40 項建議，更進一步將洗錢的前置犯罪擴大至毒品犯罪以外其他重大犯罪行爲，2001 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。

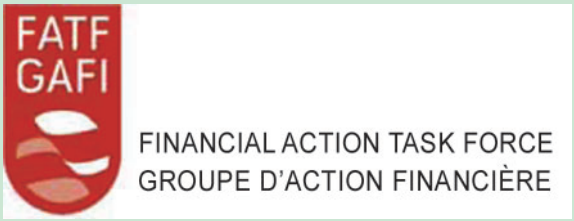
我國政府洞察洗錢犯罪之危害性，順應世界潮流，制定《洗錢防制法》草案，於民國 85 年 10 月 23 日經立法院通過，並奉總統明令公布，自 86 年 4 月 23 日施行。歷經 20 餘年的實務運作，執行成果已獲國際防制洗錢組織高度肯定，更針對實際所遭遇之問題，先後於 92 年、95 年、96 年、97 年、98 年、105 年及 107 年修法，以符合防制洗錢及打擊資恐的國際標準規範並兼顧實務運作之需要。

爲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 日奉行政院核定之〈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，配賦人員 27 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





◎ FATF（Financial Action Task Force，FATF）

七大工業國於西元 1989 年巴黎舉行之高峰會議，體認到洗錢行爲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爲是否業已採取國際標準及制定措施加以防制。爲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爲人利用金融體系，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，爲因應 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爲準會員（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，作爲統一受理及分析疑似洗錢或資恐交易報告及其他與洗錢、相關前置犯罪及資恐有關資訊之國家機關，並分送分析結果」。而金融情報中心應擔任受理申報機關揭露資料之中央機關，包括：

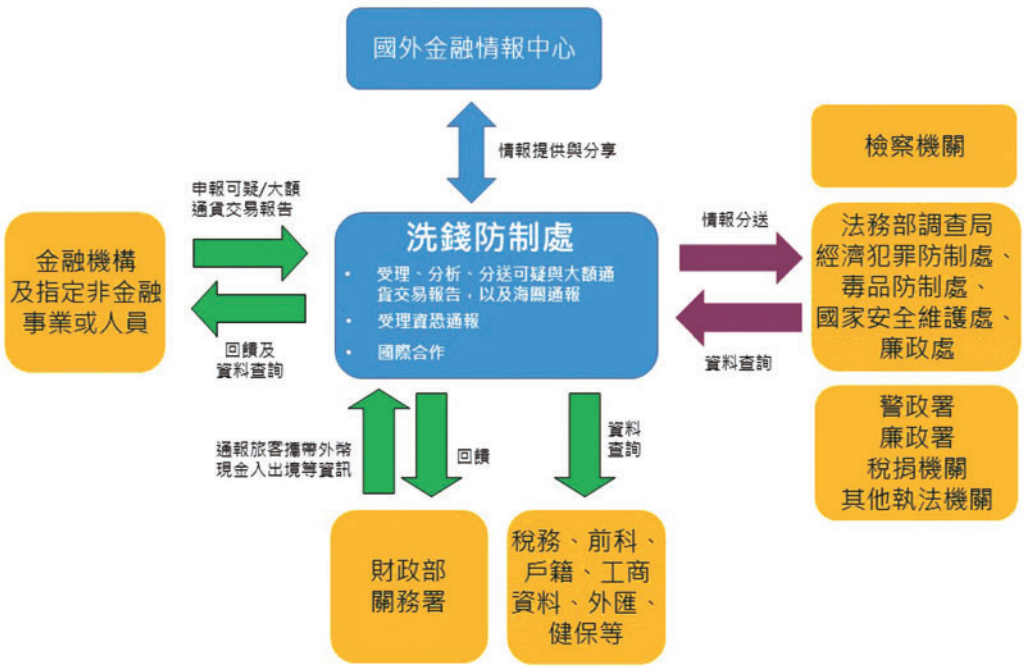
（i）申報機構依「建議第 20 項及第 23 項」申報之疑似洗錢或資恐交易報告；

（ii）國家法律要求之其他資料（如現金交易報告、電匯報告及其他門檻限制之申報／揭露）。

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（目前爲 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、受理一定金額以上通貨交易之申報

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，或爲穩定金融秩序、維護國家安全必要者，即彙編爲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。108 年度本局計受理 26,481 件可疑交易報告，較前一（107）年度受理之 35,869 件，減少 26.17%。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，其中，本國銀行申報件數約占 72.49%，可疑交易有 27.3% 發生於臺北市，交易對象之年齡層有 52.66% 分布於 31 歲至 60 歲間，交易金額則有 18.29% 爲 50 萬元以下之交易（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 01：108 年受理可疑交易報告件數統計表

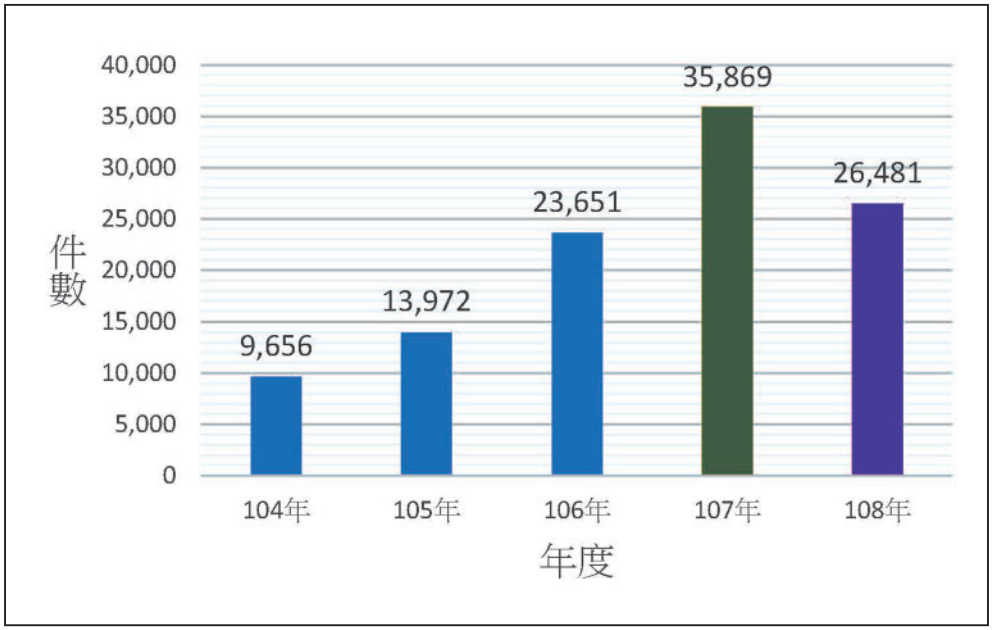
申　報　機　構	申報件數
本國銀行	19,196
外國銀行	22
信託投資公司	0
信用合作社	831

農、漁會信用部	824
辦理儲金匯兌之郵政機構	3,679
票券金融公司	2
信用卡公司	30
保險公司	1,202
證券商	371
證券投資信託事業	34
證券金融事業	5
證券投資顧問事業	0
證券集中保管事業	21
期貨商	49
指定非金融事業或人員	68
大陸銀行	35
電子支付及電子票證機構	107
外幣收兌處	2
創新實驗業	2
融資性租賃業	1
	合計：26,481

表 02：近 5 年可疑交易報告申報件數統計表

年　度	104 年	105 年	106 年	107 年	108 年
件數統計	9,656	13,972	23,651	35,869	26,481

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 03：108 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	1,355
分送警政、檢察署及其他權責機關	1,340
國際合作	11
併入資料庫	23,648
分析中	127
合計：26,481	

三、可疑交易發生地區分布

表 04：108 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	8,270	嘉義市	436
新北市	4,632	嘉義縣	264
基隆市	332	臺南市	1,770
宜蘭縣	294	高雄市	3,298
桃園市	2,362	屏東縣	511
新竹市	678	花蓮縣	201
新竹縣	482	臺東縣	149
苗栗縣	367	澎湖縣	25
臺中市	3,829	金門縣	39
彰化縣	1,220	連江縣	4
南投縣	300	其他[2]	484
雲林縣	344		
			合計：30,291

註：一件可疑交易報告涵蓋發生地區可能包含一個以上。

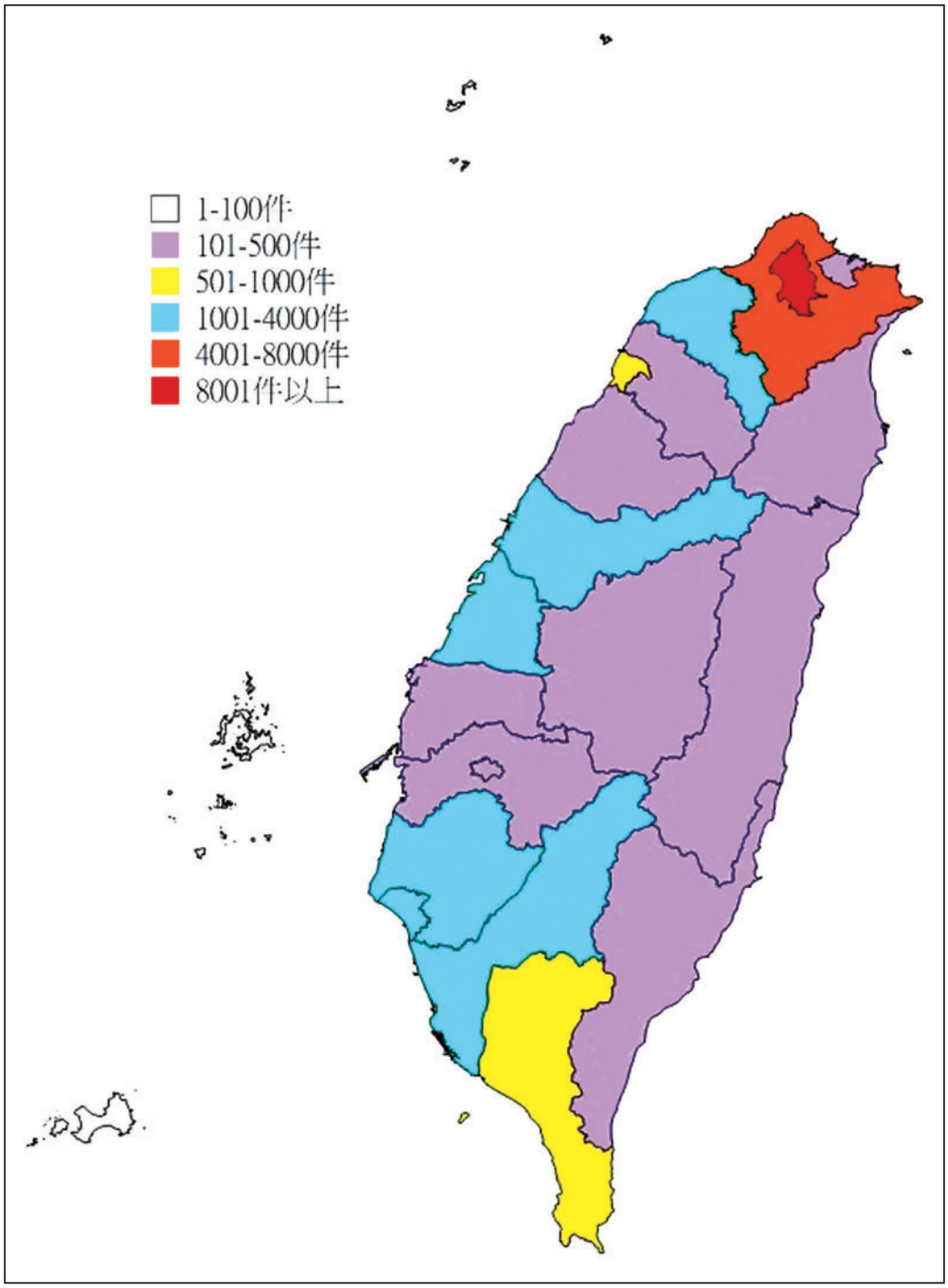
四、可疑交易申報月份分布

表 05：108 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	2,497	1,532	2,056	2,127	2,325	2,054	2,353	2,434	2,178	2,145	2,328	2,452

[2] 指國外地區等。

圖 D：108 年可疑交易發生地區分布圖

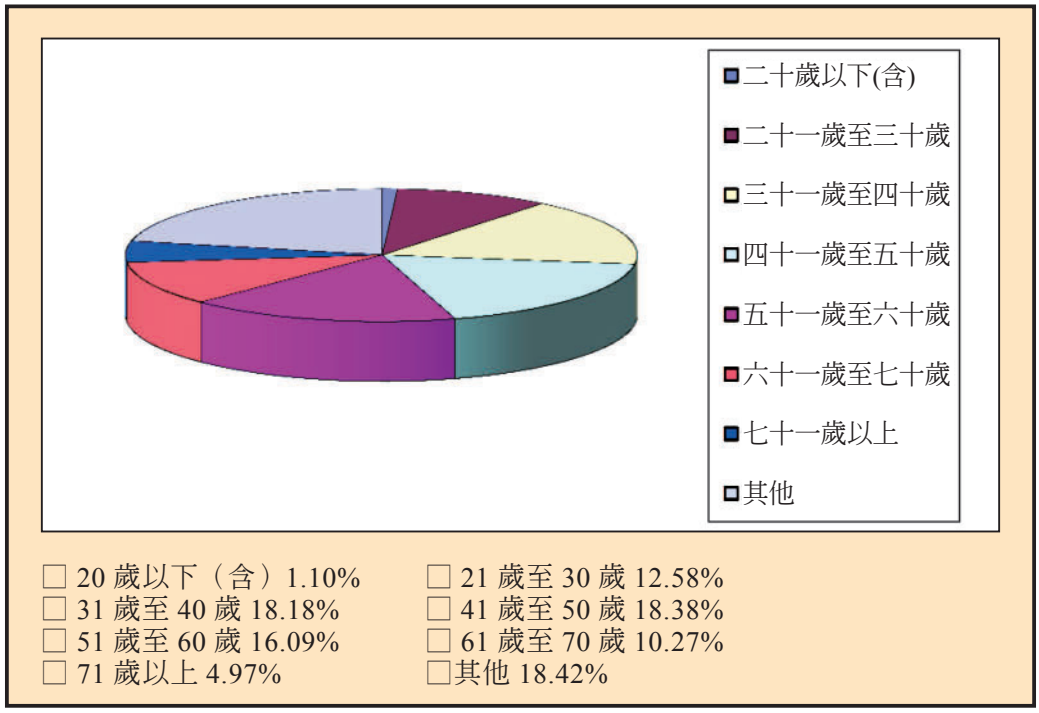


五、可疑交易對象年齡層分布

表 06：108 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）	291
21 歲至 30 歲	3,330
31 歲至 40 歲	4,815
41 歲至 50 歲	4,868
51 歲至 60 歲	4,262
61 歲至 70 歲	2,719
71 歲以上	1,317
其他 [3]	4,879
合計：26,481	

圖 E：108 年可疑交易申報對象年齡層分析圖



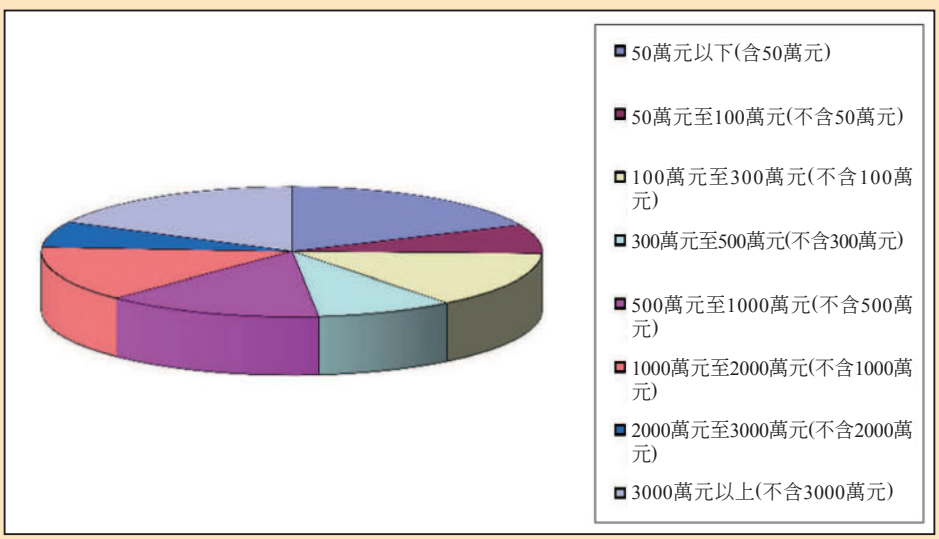
[3] 其他：非自然人。

六、可疑交易金額分布

表 07：108 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）	4,844
50 萬元至 100 萬元（不含 50 萬元）	1,914
100 萬元至 300 萬元（不含 100 萬元）	3,674
300 萬元 500 萬元（不含 300 萬元）	2,362
500 萬元至 1000 萬元（不含 500 萬元）	3,712
1000 萬元至 2000 萬元（不含 1000 萬元）	3,619
2000 萬元至 3000 萬元（不含 2000 萬元）	1,715
3000 萬元以上（不含 3000 萬元）	4,641
	合計：26,481

圖 F：108 年可疑交易申報金額分析圖



- 50 萬元以下（含）18.29%
- 50 萬元至 100 萬元（不含 50 萬元）7.23%
- 100 萬元至 300 萬元（不含 100 萬元）13.87%
- 300 萬元至 500 萬元（不含 300 萬元）8.92%
- 500 萬元至 1,000 萬元（不含 500 萬元）14.02%
- 1,000 萬元至 2,000 萬元（不含 1,000 萬元）13.67%
- 2,000 萬元至 3,000 萬元（不含 2,000 萬元）6.48%
- 3,000 萬元以上（不含 3,000 萬元）17.53%

貳、受理一定金額以上通貨交易之申報

依據《洗錢防制法》第 9 條，本局受理國內金融機構申報一定金額以上通貨交易（下稱大額通貨交易）資料，而依〈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。108 年度共受理申報 3,092,985 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 78.24%，交易金額爲 50 萬元至 100 萬元間之交易則占 73.39%；108 年度受理查詢大額通貨交易之件數爲 44,097 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

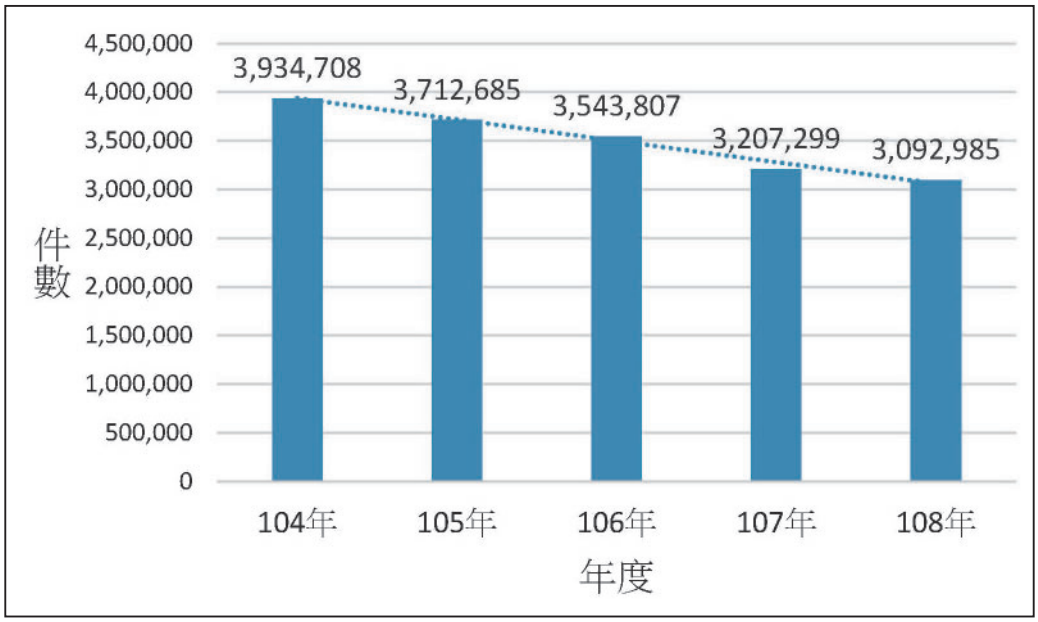
表 08：108 年申報大額通貨交易件數統計表

申報機構	件數
本國銀行	2,420,092
外國銀行	10,892
大陸銀行	0
信託投資公司	0
信用合作社	123,450
農、漁會信用部	260,886
辦理儲金匯兌之郵政機構	271,642
書面申報（金融機構 - 本國銀行）	0
書面申報（金融機構 - 外國銀行）	0
書面申報（金融機構 - 大陸銀行）	0
書面申報（金融機構 - 農會）	0
書面申報（金融機構 - 漁會）	0
書面申報（金融機構 - 其他）	11
保險公司	5,876
書面申報（保險）	1
書面申報（銀樓）	135
其他金融機構	0
合計：3,092,985	

表 9：近 5 年大額通貨交易申報件數統計表

年　度	104 年	105 年	106 年	107 年	108 年
件數統計	3,934,708	3,712,685	3,543,807	3,207,299	3,092,985

圖 G：近 5 年大額通貨交易申報件數統計圖

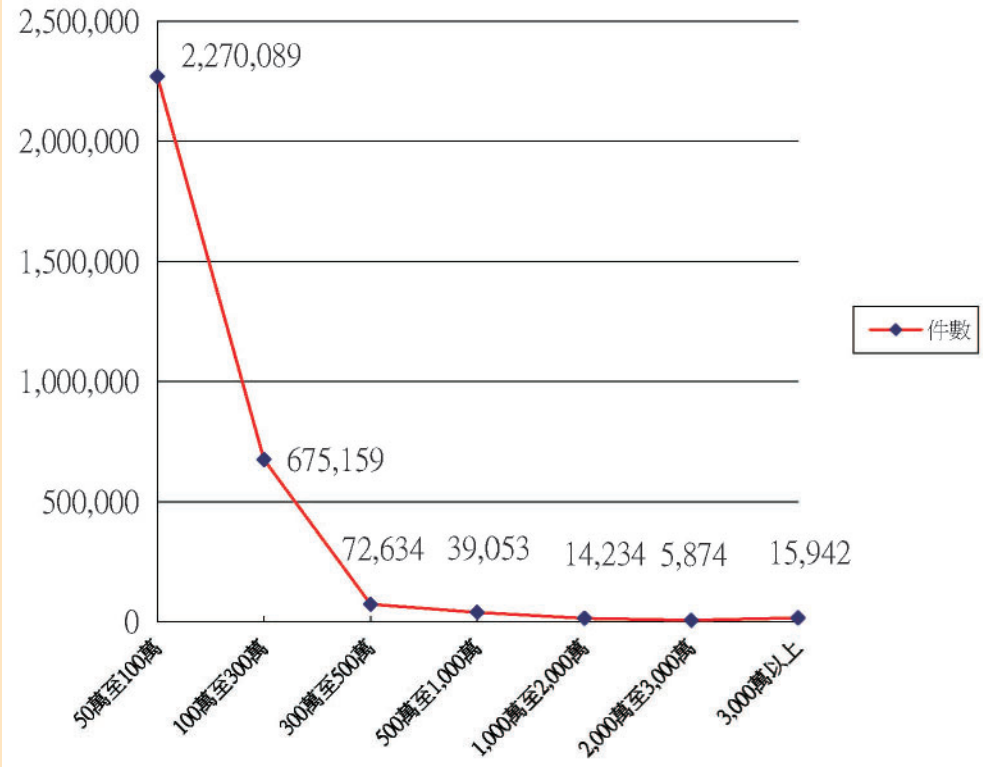


二、大額通貨交易申報金額分布

表 10：108 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）	2,270,089
100 萬元至 300 萬元（不含 100 萬元）	675,159
300 萬元至 500 萬元（不含 300 萬元）	72,634
500 萬元至 1,000 萬元（不含 500 萬元）	39,053
1,000 萬元至 2,000 萬元（不含 1,000 萬元）	14,234
2,000 萬元至 3,000 萬元（不含 2,000 萬元）	5,874
3,000 萬元以上（不含 3,000 萬元）	15,942
	合計：3,092,985

圖 H：108 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）73.39%
- 100 萬元至 300 萬元（不含 100 萬元）21.83%
- 300 萬元至 500 萬元（不含 300 萬元）2.35%
- 500 萬元至 1,000 萬元（不含 500 萬元）1.26%
- 1,000 萬元至 2,000 萬元（不含 1,000 萬元）0.46%
- 2,000 萬元至 3,000 萬元（不含 2,000 萬元）0.19%
- 3,000 萬元以上（不含 3,000 萬元）0.52%

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	104 年	105 年	106 年	107 年	108 年
法務部調查局	36,040	21,413	32,402	30,717	21,609
其他執法機關	5,641	13,012	17,929	29,153	19,236
檢察機關及法院	8,987	5,186	9,051	6,628	3,252
筆數統計	50,668	39,611	59,382	66,498	44,097

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」。108 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 39,855 筆，其中 87.02% 爲 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。108 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 320,481 筆，其中 79.23％爲進口申報，進口申報金額逾 2,130 億元（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 12：108 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	5,371
出境	34,484
合計	39,855

表 13：近 5 年旅客通報筆數統計表

年度	104 年	105 年	106 年	107 年	108 年
筆數	27,725	33,555	45,165	47,383	39,855

二、旅客（含隨交通工具服務之人）通報資料月份分布

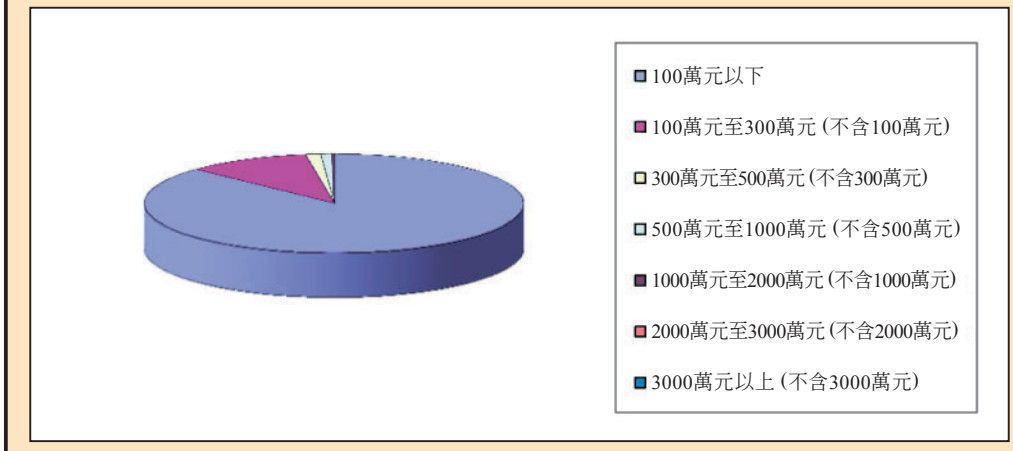
表 14：108 年各月份旅客（含隨交通工具服務之人）通報統計表

月份	1 月	2 月	3 月	4 月	5 月	6 月
一般申報筆數	3,318	3,603	3,534	3,690	3,952	3,367
查獲違規筆數	26	13	18	16	14	16
合計	3,344	3,616	3,552	3,706	3,966	3,383
月份	7 月	8 月	9 月	10 月	11 月	12 月
一般申報筆數	3,221	2,869	2,931	3,537	3,272	2,561
查獲違規[4]筆數	15	14	9	4	8	15
合計	3,236	2,883	2,940	3,541	3,280	2,576

[4] 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

圖 I：108 年通報金額分析圖



- ☐ 100 萬元以下 87.02%
- ☐ 100 萬元至 300 萬元（不含 100 萬元）10.54%
- ☐ 300 萬元至 500 萬元（不含 300 萬元）1.29%
- ☐ 500 萬元至 1,000 萬元（不含 500 萬元）0.87%
- ☐ 1,000 萬元至 2,000 萬元（不含 1,000 萬元）0.23%
- ☐ 2,000 萬元至 3,000 萬元（不含 2,000 萬元）0.02%
- ☐ 3,000 萬元以上（不含 3,000 萬元）0.03%

表 15：108 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	34,680
100 萬元至 300 萬元（不含 100 萬元）	4,200
300 萬元至 500 萬元（不含 300 萬元）	515
500 萬元至 1000 萬元（不含 500 萬元）	348
1000 萬元至 2000 萬元（不含 1000 萬元）	92
2000 萬元至 3000 萬元（不含 2000 萬元）	9
3000 萬元以上（不含 3000 萬元）	11
	合計：39,855

四、以貨物運送（含其他相類之方法）通報數量

表 16：108 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	66,574
進口	253,907
合計	320,481

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	106 年（自 6 月 28 日起）	107 年	108 年
筆數	151,657	290,084	320,481

五、以貨物運送（含其他相類之方法）通報金額

表 18：108 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	117,379,546,222
進口	213,004,843,477
合計	330,384,389,699

六、以貨物運送（含其他相類之方法）通報資料月份分布

表 19：108 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	29,572	14,556	26,186	28,004	24,640	25,845
月份	7 月	8 月	9 月	10 月	11 月	12 月
筆數	29,169	28,297	24,812	27,674	36,379	25,347

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。

■本局臺北市調查處於「臺北科技大學 108 年度校園企業徵才博覽會」辦理洗錢防制工作宣導。

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，特別是有關發掘及申報可疑交易。」爲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爲本之客戶盡職調查。

表 20：108 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

金融機構名稱		小計	
		場次	人次
銀　行	本國銀行（含金控）	42	2,868
	外國銀行	2	33
信用合作社		1	30
農漁會信用部		9	854
證券業		9	1,661
期貨業		3	425
辦理儲金匯兌之郵政機構		1	128
保險業		12	730
指定之非金融事業或人員		2	362
合計		81	7,091

伍、公私協力與策略研究

一、參與 APG 第三輪相互評鑑獲得一般追蹤佳績

「亞太防制洗錢組織」（Asia/Pacific Group on Money Laundering，下稱：APG）第 22 屆年會於 108 年 8 月 17 日至 23 日在澳洲首都坎培拉舉行，計有來自 46 個國家（地區）、13 個國際組織，約 520 位代表與會。我國代表團由行政院洗錢防制辦公室、金融監督管理委員會、外交部、中央銀行、內政部警政署及本局派員組成。本局由洗錢防制處李前處長宏錦率本處同仁與會。

本次年會接受評鑑並採認相互評鑑報告之國家包含我國、巴基斯坦、所羅門群島及菲律賓等 4 國，我國第三輪相互評鑑報告於 8 月 22 日上午獲大會討論一致通過並核列爲「一般追蹤等級」（Regular follow-up）。在 40 個技術法規遵循項目中，達到「大部分遵循」（Largely Compliant，LC）以上共計有 36 項；在 11 個效能遵循項目中，達到實質上「相當有效」（Substantial level of effectiveness，SE）共計 7 項。在效能遵循項目中，直接成果 6 係檢核受評鑑國金融情報中心之執行效能，本局洗錢防制處作爲我國金融情報中心，受評期間充分展現洗錢防制處運用金融情資協助執法與行政機關之具體成效，以及利用資訊科技提高分析效能，並強化與私部門間之橫向聯繫機制。評鑑團及 APG 各會員國對我國金融情報中心執行成效均給予高度肯定，核予我國金融情報中心「相當有效」之評鑑等級。

我國獲得「一般追蹤」佳績實非一日之功，整備期間透過 37 個公部門機關部會、31 個私部門公會及機構相互合作，歷經 4 場大型國家風險評估會議與 2 場公、私部門模擬評鑑會議，共同完成我國「國家風險評估報告」、「技術遵循報告」及「效能評鑑報告」，並順利完成相互評鑑會前會、現地評鑑及面對面會議，始有今日的圓滿成果。而我國將於 110 年提交首次追蹤報告，並於 113 年正式接受追蹤評估，本局洗錢防制處作爲國家金融情報中心，將持續與國內外執法機關、監理機關及私部門申報機構深化資訊交流並推動業務創新，協同各機關（構）發揮綜效，以爭取最佳成績。

■ 我國代表團成員參加 APG 第 22 屆年會，會中正式通過我國第三輪相互評鑑報告，並獲得「一般追蹤」最佳評等。

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

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武器擴散融資之國際標準。

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，並爲 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。

二、協助公會訂定實務指引提升各業別申報品質

爲協助各業別申報機構強化以風險爲本之監理方法，提高辨識疑似洗錢暨打擊資恐之新興態樣，本局洗錢防制處派員參加中華民國證券商業同業公會於 108 年 10 月 16 日召開之「法律事務暨法令遵循委員會會議」，就「證券商防制洗錢及打擊資恐注意事項範本」附錄「疑似洗錢、資恐或武擴交易態樣」提供修改意見，並協助修訂洗錢防制及打擊資恐相關實務指引，新修訂之「疑似洗錢、資恐或武擴交易態樣」預定於 109 年 10 月 1 日施行。本處另於 108 年 10 月 17 日派員參加銀行公會召開之「信用卡業務委員會風險組 108 年第 3 次會議」，就信用卡業可疑交易報告相關態樣及申報方式提供意見，作爲修訂「辦理信用卡業務機構防制洗錢及打擊資恐注意事項範本」之參據，修正態樣業經金管會核定於 109 年 9 月施行。另證券公會於 108 年 11 月 29 日舉辦「證券商防制洗錢及打擊資恐法遵論壇座談會」，參訓人數約計 300 人，本局洗錢防制處受邀分享金融情報中心對證券商申報可疑交易報告相關回饋資料，協助提升證券商申報品質。

■ 本局洗錢防制處陳志成科長受邀參加中華民國證券商業同業公會於 108 年 11 月 29 日舉辦之「證券商防制洗錢及打擊資恐法遵論壇座談會」。

三、舉辦犯罪金流分析與異常交易態樣研討會

107 年國家洗錢及資恐風險評估報告指出，我國深受洗錢非常高度威脅的犯罪共有毒品販運、貪污賄賂、詐欺、證券犯罪、第三方洗錢、稅務犯罪、走私及組織犯罪等八大類型；另 108 年亞太防制洗錢組織第三輪相互評鑑報告亦指出，金融情報中心、執法機關、海關等公部門，應與金融機構或指定之非金融事業人員間持續合作分享特定威脅、弱點及風險趨勢的資訊，協助私部門深化以風險爲本的方法。故爲強化金融機構等申報單位對高風險犯罪之瞭解，有效提升防制洗錢能力，本局洗錢防制處與金融監督管理委員會銀行局、臺灣金融服務聯合總會於 108 年 5 月 24 日共同辦理「犯罪金流分析與異常交易態樣研討會」，共計 140 名洗錢防制專責人員代表 63 家金融機構出席與會。研討會首由時任金管會銀行局莊副局長秀媛及洗錢防制處李處長宏錦致詞開幕，續由本局經濟犯罪防制處伍前處長榮春（現任洗錢防制處處長）、毒品防制處郭守源調查專員及廉政處林宜蒓調查官分享犯罪調查實務經驗，並針對我國深受洗錢非常高威脅之八大犯罪類型，如：操縱股價、虛僞增資、

■ 本局洗錢防制處李前處長宏錦（右三）、經濟犯罪防制處伍處長榮春（現任洗錢防制處處長，左二）、洗錢防制處陳科長志成（右二）與金管會銀行局莊前副局長秀媛（現任銀行局局長）及臺灣金融服務聯合總會許副秘書長銘吉等貴賓合影。

財報不實、吸金、地下通匯、稅務犯罪、毒品犯罪及貪瀆犯罪（如詐領助理費、詐領公款、圍標等案件類型），簡要分析各類犯罪金流模式與異常交易態樣，同時說明本局未來偵辦重點與任務方向。會後由莊秀媛副局長主持與談，與會人員踴躍發問並參與研討，顯示對於犯罪暨洗錢手法都有更深入之瞭解，有助提升可疑交易態樣辨識能力及優化申報機制效能。

四、與金管會檢查局業務聯繫會議

108 年 12 月 4 日由金融監督管理委員會檢查局主辦檢查局與本局洗錢防制處業務聯繫會議，針對金融機構申報可疑交易報告之案例類型、申報品質、風險趨勢及專案檢查重要缺失等議題交換意見，並以下列議題列爲雙方未來關注及研討重點：(一) 探討「其他疑似洗錢交易情形」之概括性態樣持續名列銀行業、證券業及保險業申報可疑交易之前三大可疑交易表徵之因；（二）發展 OBU（Offshore Banking Unit）帳戶疑似洗錢態樣，並強化申報機構就 OBU 帳戶用於洗錢、資恐及資助武擴情形之辨識能力。洗錢防制處持續與檢查局建立常態聯繫機制，促進監理機關與申報機構及執法部門之溝通聯繫，對公私部門深化以風險爲本之防制洗錢及打擊資恐工作甚有助益。

五、研編「貪瀆犯罪」策略分析報告

貪瀆犯罪係我國八大非常高風險之一，惟歷年來相關可疑交易報告（STR）申報件數均低。本局洗錢防制處爲協助申報機構加強辨識貪瀆犯罪可疑指標，並關注相關洗錢態樣，爰參考 105 年至 107 年調查局及廉政署移送之公務員重大貪瀆案件，以相關犯罪事實分析其洗錢或資金移動態樣，評估金融機構或指定之非金融事業或人員（DNFBPs）可能遭利用作爲洗錢管道之風險；另篩選洗錢防制處曾受理與前揭案件相關 STR 進行分析、歸納及彙整，併同前揭重大貪瀆案件，列舉不同類型貪瀆案件之可疑犯罪指標、歸納其洗錢手法，進而提出相關具體建議，供各申報機關作爲研析並申報 STR 之參考基礎。

六、發行洗錢防制處電子報

我國甫於 108 年完成 APG 第三輪相互評鑑並獲得一般追蹤之佳績，然評鑑團於建議中亦不斷強調金融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，爲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，宗旨即在創建防制洗錢、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 3P（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。

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 163 個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。108 年國際情資交換件數（含問卷）共 1,067 件，相較 107 年之 852 件，成長幅度為 20.15%。

表 21：近 5 年從事國際合作之情資交換統計表

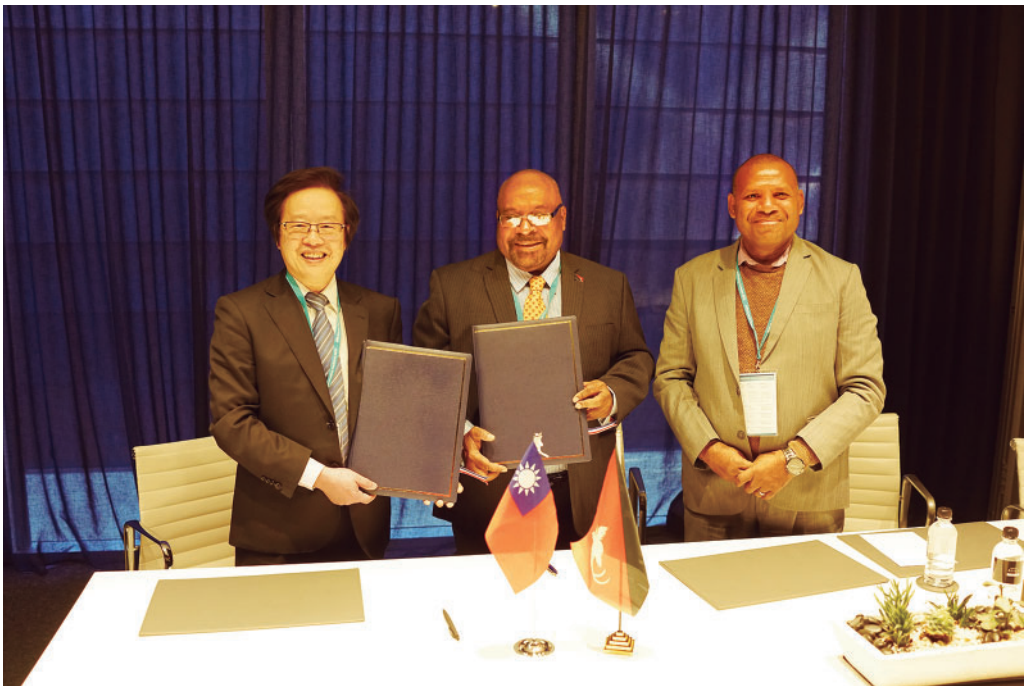
事項	年度	104 年	105 年	106 年	107 年	108 年
外國請求我國協查	案	51	50	55	47	71
	件	152	169	161	162	279
我國請求外國協查	案	45	34	26	23	38
	件	222	165	94	107	292
外國主動提供情資	案	32	25	53	99	81
	件	44	44	100	198	198
我國主動提供情資	案	9	26	45	20	17
	件	18	45	94	46	50
問卷及其他事項	案	0	0	0	0	0
	件	201	262	354	339	248
小計	案	137	135	179	189	207
	件	637	685	803	852	1,067

二、與外國金融情報中心簽署瞭解備忘錄（或協定）

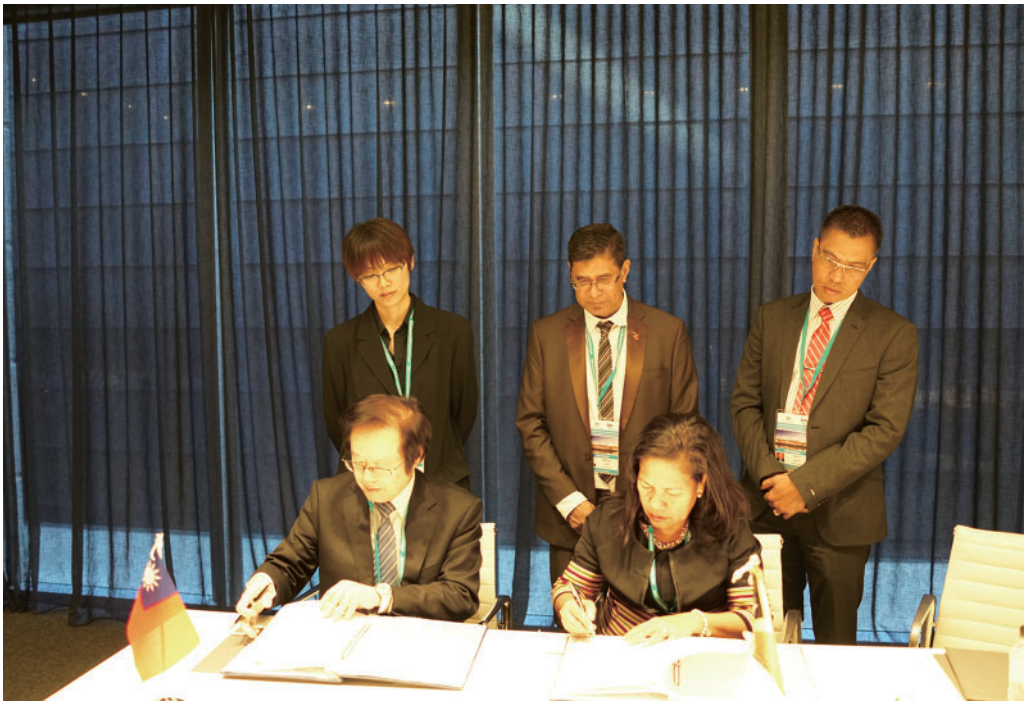
洗錢犯罪常爲跨越國境的犯罪，爲有效打擊跨境洗錢犯罪、資助恐怖主義及資助大規模毀滅性武器擴散等，有賴各國政府凝聚共識並攜手合作，秉持互信互惠原則交換金融情資，共同打擊洗錢犯罪及資恐活動。洗錢防制處於 108 年 7 月 3 日與瓜地馬拉共和國（Republic of Guatemala）金融監督管理局特別驗證處在荷蘭海牙完成「關於涉及洗錢或其他資產清洗、相關前置犯罪及資助恐怖主義金融情資交換合作協定」簽署儀式。另於 108 年 8 月赴澳洲坎培拉參加亞太防制洗錢組織（Asia-Pacific Group on Money Laundering）第 22 屆年會期間，分別與巴布亞紐幾內亞（Independent State of Papua New Guinea）、東帝汶（Democratic Republic of Timor-Leste）及東加（Kingdom of Tonga）簽訂「關於涉及洗錢、相關前置犯罪及資助恐怖主義金融情資交換合作瞭解備忘錄」。另於 108 年 10 月 4 日以異地簽署方式與約旦哈希米王國（Hashemite Kingdom of Jordan）完成「反洗錢及打擊資恐中心關於涉及洗錢、相關前置犯罪及資助恐怖主義金融情資交換合作瞭解備忘錄」。迄 108 年 12 月 31 日止，我國已與 50 個國家或地區簽署此類備忘錄或協定，顯示我國持續推動防制洗錢與打擊資恐國際合作成果深獲各國肯定。

■ 108 年 7 月 3 日我國與瓜地馬拉金融情報中心完成簽署「關於涉及洗錢、相關前置犯罪及資助恐怖主義金融情資交換合作協定」。

■ 108年8月20日洗錢防制處李前處長宏錦於澳洲坎培拉與東加簽署「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」。



■ 108年8月20日，洗錢防制處李前處長宏錦於澳洲坎培拉與巴布亞紐幾內亞簽署「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」。



■ 108 年 8 月 20 日，洗錢防制處李前處長宏錦於澳洲坎培拉與東帝汶簽署「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」。

三、參加艾格蒙第 26 屆年會

我國爲艾格蒙聯盟（Egmont Group）會員，每年應邀參加艾格蒙聯盟年會。本局洗錢防制處於 108 年 7 月 1 日至 7 月 4 日代表我國參加艾格蒙聯盟於荷蘭海牙世界論壇中心（World Forum, Hague, Netherlands）舉行之第 26 屆年會，會議主題爲：「強化公部門間的合作 - 從金融情報中心的視角」，本處同仁獲艾格蒙聯盟亞太區代表邀請，於年會期間以「我國檢察機關、司法警察機關、金融情報中心等共同組成案件偵辦專案小組的運作機制、效益及挑戰」爲主題進行專題報告，與亞太區會員分享洗錢防制處歷年來協助檢察機關、司法警察機關實施專案金流分析的成功經驗、作法、面臨的挑戰及機會等，獲得各會員國高度肯定。洗錢防制處並深度參與艾格蒙聯盟相關業務，持續協助該聯盟審視亞太區候選金融情報中心入會資格，並與法國金融情報中心共同輔導越南金融情報中心申請入會程序，積極拓展我國專業領域合作機會並強化與各國情資交換之效能。

◎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 163 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，截至 108 年 12 月底止，業與 50 國簽署合作協定或備忘錄。

四、參加不為恐怖行為融資 - 打擊資恐部長級會議

澳洲內政部於 108 年 11 月 7 日至 8 日在澳洲墨爾本會議及展覽中心舉行 108 年「不為恐怖行為融資 - 打擊資恐部長級會議」，計邀請 65 個代表團與會，其中包括約 20 國之部長層級代表。本局洗錢防制處李前處長宏錦以我國金融情報中心首長身分應邀參加，並於會中分享我國防制洗錢及打擊資恐「公私部門夥伴關係」之架構及效能，同時介紹我國金融情報中心協助金融機構追蹤可疑交易報告處理情形並與監管機關研擬洗錢及資恐更新態樣等具體作法，發言內容受到各國高度關注。另為充分掌握國際恐怖主義發展趨勢，洗錢防制處派員全程參與該會議「不斷演進之恐怖融資威脅」、「恐怖主義融資及全球對應策略」、「新興科技及恐怖主義融資風險」、「公私部門夥伴關係」及「非營利組織」等 5 大議程，並於會議期間與各國部會首長及幕僚就會議主題交換意見，汲取他國對抗恐怖主義之成功經驗，作為我國制定反恐機制之政策參考。

■ 本局洗錢防制處李前處長宏錦受邀參加 108 年「不為恐怖行為融資—打擊資恐部長級會議」。

五、參加「亞太區追討犯罪所得機構網路」第 6 屆年會

102 年 11 月 19 日「亞太區追討犯罪所得機構網路」於韓國首爾成立，以協助各國交換司法互助情資、提高司法互助效能爲成立宗旨。我國係創始會員，由法務部擔任我國聯繫該組織之秘書單位。該組織第 6 屆年會係於 108 年 9 月 23 日至 24 日在蒙古烏蘭巴托舉辦，洗錢防制處派員與會。會議期間我國、澳洲及巴基斯坦就追討不法所得議題進行專題報告與經驗分享，本處同仁亦就跨境執法合作與犯罪不法所得沒收等核心議題與各國代表交換意見，並藉由參與相關議程吸收各國針對新興犯罪手法如虛擬貨幣洗錢的資金追查技巧與經驗，透由互動交流方式強化與各國之聯繫管道並拓展我國執法觸角。

■ 洗錢防制處同仁參加 108 年「亞太區追討犯罪所得機構網路」第 6 屆年會。

六、參加「防制洗錢金融行動工作組織」第 30 屆第 3 次會員大會及工作組會議

「防制洗錢金融行動工作組織」（Financial Action Task Force，下稱：FATF）係依據 1989 年七大工業國於巴黎峰會倡議所籌組創建之國際組織，主要負責制定防制洗錢及打擊資恐全球標準。FATF 第 30 屆第 3 次會員大會及工作組會議於 108 年 6 月 16 日至 21 日在美國奧蘭多 Wyndham 飯店國際會議廳舉行，本次年會時值我國進行亞太洗錢防制組織（Asia Pacific Group on Money Laundering，下稱：APG）第三輪相互評鑑，於 APG 年會前之重要國際會議，本局洗錢防制處派員全程參與大會會議及工作組會議，汲取關於持續打擊資恐及反武器擴散、虛擬資產監理指引、虛擬資產之金融調查指引等最新國際標準，並借鏡 FATF 會員國審查希臘及香港相互評鑑報告之討論重點，作爲我國未來因應相互評鑑之參考。

第三部分

重要案例

壹、甲集團楊○虎等涉嫌違反銀行法、洗錢防制法等案

貳、吳○霖等涉嫌違反銀行法、洗錢防制法等案

參、乙公司邱○成等涉嫌違反銀行法等案

肆、林○良等涉嫌詐欺案

壹、甲集團楊○虎等涉嫌違反銀行法、洗錢防制法等案

一、案情概述

（一）情資來源

本處於 108 年 6 月間分析金融情資發現：A 公司、B 公司、C 公司及 D 公司爲關係企業（下稱甲集團），108 年 5 月起陸續發生應收帳款融資屆期未清償，且有同一名員工代理不同公司交易或以他公司名義爲匯款人之情形，交易疑有異常，本處遂製成分析報告，分送執法機關參考運用。

（二）涉案人

甲集團楊○虎、王○之、林○如等人、E 公司黃○堂等人、F 公司姜○明、G 公司李○剛、H 公司姚○隆、I 公司劉○達、J 公司歐○亭、K 公司謝○清、L 公司蔡○賢、M 公司蕭○政等人、N 公司蕭○桂、P 法律事務所黃○熹。

（三）涉案情形

楊○虎等甲集團之負責人、經理人、董事及員工，明知甲集團與 E 公司等國內公司、F 公司子公司 Q 公司等境外公司，以及楊○虎及王○之自行設立之 R 公司等註冊於貝里斯等境外紙上公司無實際交易，竟與 E 公司等負有爲其公司及股東利益忠實執行職務義務之人，共同基於詐欺銀行等犯意聯絡及行爲分擔，由楊○虎、王○之指示員工僞造甲集團與 E 等公司不實之買賣合約書、開立不實統一發票及出貨單等文件，營造集團與 E 等公司進銷貨之假象，並由 E 公司配合甲集團，協助製作僞造之海運提單（Bill of Lading），再由王○之、楊○虎持上開不實之買賣合約書、發票、海運提單等文件，陸續向 X 銀行等 9 家銀行申辦國內外應收帳款融資及外銷放款，一方面由王○之以甲集團名義出具保證書予押匯銀行，保證若客戶未付款時由甲集團全額支付，另一方面由 E 公

司黃○堂等人配合銀行訪廠、收受銀行債權轉讓信件及虛偽照會，營造渠等所任職公司與甲集團確有交易假象，使 X 銀行等人員陷於錯誤而核撥款項。迨甲集團與 E 公司等公司之應收帳款向銀行貸款還款期限屆至，楊○虎及王○之即自行或指示員工自甲集團帳戶提領款項，以 E 公司等公司爲匯款人名義，償還向銀行申請貸款之本金，或由員工將款項匯至海外公司指定帳戶後，再由其等協助償還貸款之本金，佯裝交易對手與甲集團之交易還款正常之表象。嗣 108 年 5 月間，甲集團陸續發生國內信用狀、外銷貸款屆期未清償，應收帳款融資延遲入帳等問題，承貸銀行向甲集團廠商催討款項，始發現並無相對應交易事實，而楊○虎、王○之等人無預警失聯，甲集團則暫停營業。

甲集團以前述手法，向銀行詐得款項總計約 386 億元，王○之爲隱匿利用虛偽交易詐貸所獲取之不法利益，乃以詐貸不法所得購置南投縣、臺北市及新竹縣等 16 處不動產，並借楊○晨、楊○海、楊廖○○、蕭○政、林○如等人名義登記，以隱匿該等資產實際所有權；另執業律師黃○熹於 108 年 4 月起，與王○之等人多次就詐貸案共同商討因應對策，明知甲集團向多家銀行詐貸款項之不法犯行，仍於 108 年 4 月、5 月間，以本人及其所主持之 P 法律事務所名下帳戶，收受王○之等人詐欺貸款之犯罪所得，合計約 1,250 萬元；又王○之及楊○虎於 108 年 6 月初潛逃出境後，楊○晨、林○如、莊○芬等人爲隱匿、掩飾甲集團詐貸不法所得，連續臨櫃提領甲集團帳戶款項，將犯罪所得合計逾 2,000 萬元移轉至 P 法律事務所、M 公司、楊○晨、林○如、蕭○桂所使用其胞姐蕭○戎等金融帳戶，另將 600 萬元現金移轉至楊○晨男友王○程所承租之 Y 銀行保險箱，企圖隱匿犯罪所得並規避追緝。

執法機關經調查後，多次對案關對象執行搜索、約談等偵辦作爲，並扣得現金、金融帳戶存款、不動產、車輛等財產。楊○虎夫婦等人於案件爆發前即潛逃出境而遭通緝。109 年 1 月初，檢察官以觸犯銀行法、刑法背信、商業會計法及洗錢防制法等罪嫌起訴以楊○虎夫婦等人，而後執法機關經過多方協調，分別於 109 年 1 月及 3 月間將滯留國外之楊○虎夫婦順利押解返臺，接受審判。

二、可疑洗錢表徵

客戶經常於數個不同客戶帳戶間移轉資金達特定金額；客戶經常代理他人存、提，或帳戶經常由第三人存、提達特定金額以上；客戶突有達特定金額以上存款者；客戶經常自國外收到達特定金額以上款項後，立即再將該筆款項匯回同一個國家或地區的另一個人，或匯至匯款方在另一個國家或地區的帳戶者；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；其他有疑似洗錢交易情形者。

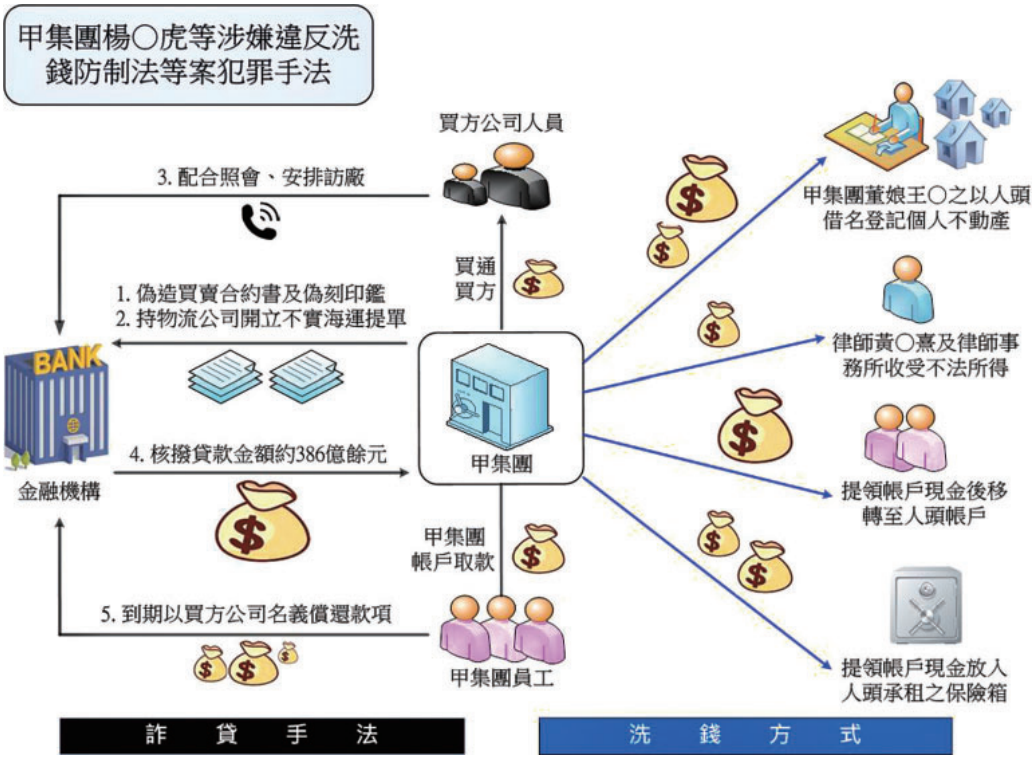
三、起訴情形

臺灣臺北地方檢察署於109年1月9日，以違反銀行法、商業會計法、刑法背信、證券交易法、洗錢防制法等罪嫌，分別起訴楊○虎、王○之及相關涉案人員。

四、經驗參考

（一）代理人常自甲集團旗下公司金融帳戶取款，隨即以其他關係企業名義匯款予取款帳戶同名之他行帳戶，甲集團以自有資金充當其他公司匯入款，且同一人員代理不同公司辦理交易，符合洗錢表徵：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；客戶經常代理他人存、提，或帳戶經常由第三人存、提達特定金額以上。

（二）甲集團與多名任職於知名企業之不肖人士及物流公司由上至下勾串共謀，向多家金融機構詐貸金額甚鉅，部分申報機構因甲集團還款出現異常，且發現部分融資之交易單據有虛偽不實情形，即主動申報可疑交易，其他申報機構於媒體披露相關新聞後，亦主動且持續申報金融情資，符合洗錢表徵：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；其他有疑似洗錢交易情形者。


甲集團楊〇虎等涉嫌違反洗錢防制法等案犯罪手法
買方公司人員
3. 配合照會、安排訪廠
買通買方
1. 偽造買賣合約書及偽刻印鑑
2. 持物流公司開立不實海運提單
BANK
金融機構
4. 核撥貸款金額約386億餘元
甲集團
甲集團帳戶取款
5. 到期以買方公司名義償還款項
甲集團員工
甲集團董娘王〇之以人頭借名登記個人不動產
律師黃〇熹及律師事務所收受不法所得
提領帳戶現金後移轉至人頭帳戶
提領帳戶現金放入人頭承租之保險箱
詐 貸 手 法
洗 錢 方 式

貳、吳○霖等涉嫌違反銀行法、洗錢防制法等案

一、案情概述

（一）案件來源：

本局接獲通報：孫○眞自大陸地區寄送之包裹內含大量人頭帳戶之網路銀行帳號、密碼、銀聯卡及 u 盾等，疑似從事地下通匯業務。

（二）涉案人：

吳○霖、陳○叡、黃○鴻、孫○眞、劉○甫及彭○峯等人。

（三）涉案情形

吳○霖與陳○叡爲夫妻，吳○霖、陳○叡、黃○鴻、孫○眞、劉○甫及彭○峯等人，明知除法律另有規定者外，非銀行不得辦理國內外匯兌業務，卻於 106 年 12 月間起，非法從事以下國內外匯兌業務：

1. 吳○霖指示孫○眞及劉○甫，以每戶新臺幣（下同）1 萬 5,000 元起之價格，收購大陸地區金融機構帳戶（含網路銀行帳號、密碼、銀聯卡及 U 盾等），準備作爲從事非法匯兌行爲用途。
2. 若客戶欲由臺灣匯款至大陸地區，則以通訊軟體 WhatsApp 向吳○霖、陳○叡、孫○眞、劉○甫等人詢價，由吳○霖等人參考當日金融機構之人民幣牌告匯率，加計兌換金額 2% 之利潤後，再向客戶告知客戶應付之新臺幣數額，雙方達成合意後，吳○霖等人即指派陳○叡、孫○眞及黃○鴻等人向客戶收取新臺幣現金並取得客戶指定匯入之大陸地區帳戶，復由吳○霖透過黃○鴻指示彭○峯，以網路轉帳方式，自前揭收購之大陸地區帳戶匯款予客戶指定帳戶，以完成匯兌行爲。倘客戶欲自國外匯款至臺灣，則由吳○霖等人計算匯率及減除 2% 利潤後，告知客戶可換取之新臺幣數額，在彭○峯確認收到客戶匯入吳

○霖等人收購之大陸地區帳戶的資金後，吳○霖即命陳○叡、孫○眞、劉○甫、黃○鴻等人以面交方式支付前揭約定數額之新臺幣現金予客戶。

3. 總計吳○霖犯罪組織非法匯兌金額約 124 億 89 萬 512 元，從中獲得不法匯兌金額 2% 的不法所得。吳○霖等人於臺灣各地向客戶收取之匯往大陸之現金項款均交由陳○叡保管，作爲吳○霖等人事前在大陸向客戶收取人民幣，再代客戶在臺支付臺幣予指定對象的款項。吳○霖等人爲隱匿該等特定犯罪所得，另將其中 2 億 3,999 萬 2,600 元現金分批攜往王○琴 (陳○叡之母) 嘉義縣住所保管。本局於執行案件時搜索王○琴住所時查扣該等現金，事後檢察官以違反銀行法、洗錢防制法起訴吳○霖等人。

二、可疑洗錢表徵

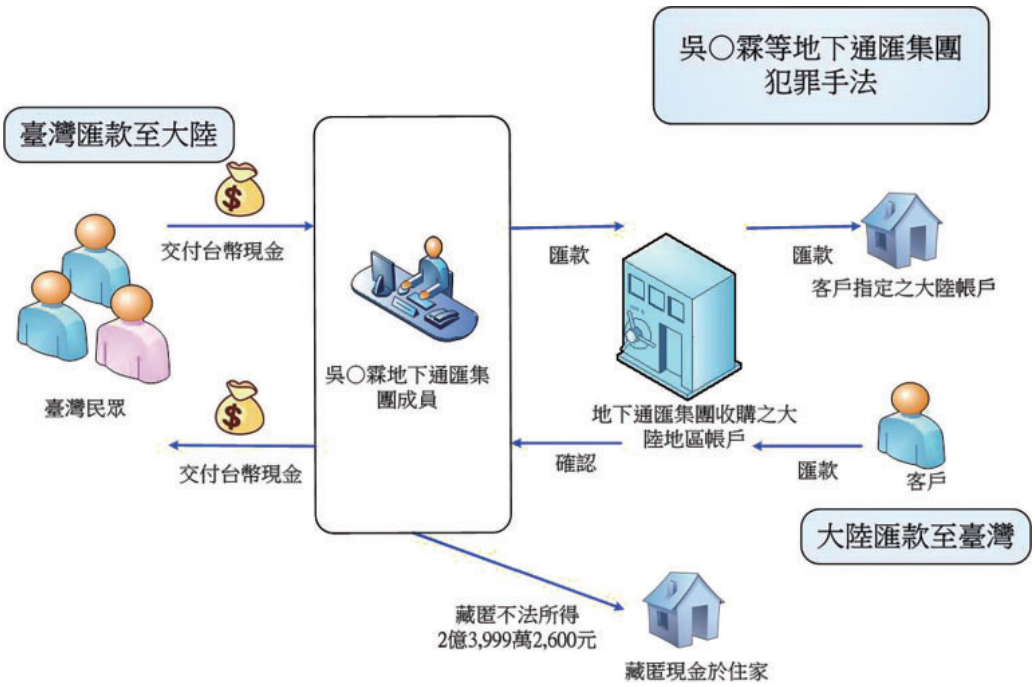
吳○霖等人持有大額現金，但其用途及資金來源不清，符合洗錢表徵。

三、起訴情形

臺灣嘉義地方檢察署於 108 年 12 月間，以銀行法第 29 條第 1 項、組織犯罪防制條例第 3 條第 1 項、洗錢防制法第 14 條第 1 項等起訴吳○霖等人。

四、經驗參考

查緝洗錢或其他犯罪行爲，需各個不同執法機關及金融機構共同協力，方能全面掌握不法訊息，並有效遏止犯罪，本案起源於海關於例行查驗時，查扣一批自大陸地區寄送至臺灣之可疑包裹，內含數十個大陸地區人頭帳戶及銀聯卡等，復經本局追查後，方查出吳○霖等人從事地下通匯，本案即爲各執法機關協力合作打擊犯罪之成果。


吳〇霖等地下通匯集團
犯罪手法
臺灣匯款至大陸
交付台幣現金
臺灣民眾
吳〇霖地下通匯集
團成員
匯款
匯款
客戶指定之大陸帳戶
地下通匯集團收購之大
陸地區帳戶
確認
匯款
客戶
交付台幣現金
大陸匯款至臺灣
藏匿不法所得
2億3,999萬2,600元
藏匿現金於住家

參、乙公司邱○成等涉嫌違反銀行法等案

一、案情概述

（一）情資來源

本處於 107 年 12 月間分析金融情資發現：國人邱○成及其配偶邱○鈞分別爲乙與丙建設公司負責人，帳戶經常有大額現金存入及密集匯入款項，資金來源不明，且有多筆退票情形，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

邱○成及邱○鈞。

（三）涉案情形

邱○成與邱○鈞明知非銀行不得經營收受存款業務，亦不得以收受投資、借款等名義，向多數人或不特定之人收受款項或吸收資金，而約定或給付與本金顯不相當之紅利或利息，因建築資金不足及爲支應渠等高額信用卡等消費所需，竟共同基於違反銀行法之不法犯意聯絡，自 99 年至 107 年間，對外以投資建案名義，向三十餘名不特定人招攬募集資金，並承諾給予年利率 18% 至 27.75% 之利息。邱○成除親自舉辦投資說明會招募投資人投資外，另透過支付佣金方式誘使公司員工及投資人介紹他人投資，並設計數種投資金額及獲利不同的投資方案，邱○成與邱○鈞以帳戶或現金方式收受投資人款項後，即開立含本金及利息之支票交予投資人，投資期滿時，投資人先向邱○成確認本金歸還及利息支付方式後，再依邱員指示，持支票向邱○成領取現金，或將支票存入銀行兌現；如投資人無急迫資金需求時，邱○成則勸誘投資人將本金繼續投入賺取利息，或是保留本金及利息，再額外加碼湊足更高額之投資款繼續投資，邱○成因此無需實際支付現金，僅以換開支票方式供投資人日後兌現，持續向投資人收受資金；107 年 12 月間，因銀行未核准邱○成等申請之貸款，導致資金周轉不靈發生跳票。計邱○成與邱○鈞非法收受投資人資金達 3 億 1,285 萬元。

二、可疑洗錢表徵

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；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。

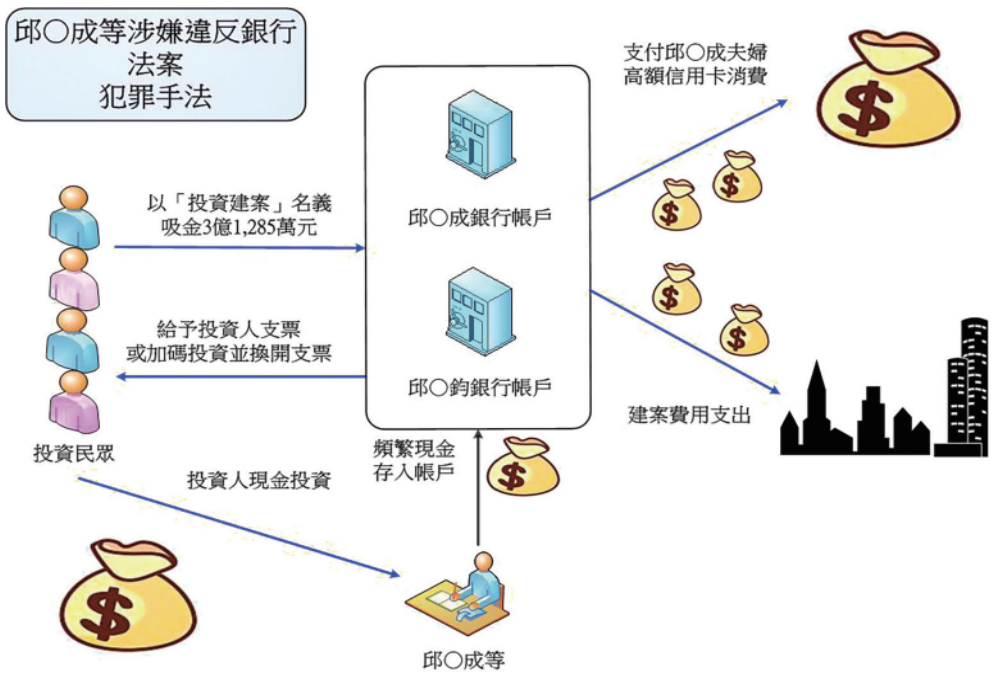
三、起訴情形

臺灣桃園地方檢察署於 108 年 5 月間以違反銀行法第 29 條、第 29 條之 1 而觸犯同法第 125 條第 1 項之罪嫌起訴邱○成。

四、經驗參考

（一）K 銀行對於客戶之大額存現、密集匯款及跳票等情形保持警覺，並持續申報相關往來對象，有助於偵辦單位掌握案關對象之金流及吸金手法，而其他金融機構於媒體報導後，即刻申報相關金融情資，有益於後續追查金流等偵辦作爲。

（二）建築業工程期間資金需求龐大，除向銀行及民間借貸業者貸款外，亦可能向不特定投資人吸金彌補資金缺口，涉案相關帳戶通常資金來源複雜且無法提出具體說明，具有每筆存提款金額相當且相距時間不久，帳戶密集存款達特定金額或筆數又迅速轉移之情形。



肆、林○良等涉嫌詐欺案

一、案情概述

（一）情資來源

本處於 105 年 6 月間分析金融情資後發現，國人廖○謙及陳○陽銀行帳戶於 105 年間存入新臺幣（下同）71.3 億元支票，卻全數遭退票，且相關帳戶留存聯絡方式均爲公司電話，顯有異常，遂製成分析報告分送予執法機關進行調查。

（二）涉案人

林○良、何○來等人。

（三）涉案情形

林○良、何○來等人明知使用人頭公司申領之支票係無兌現可能之空頭支票，竟基於詐欺取財之犯意，先由親屬林○揚、林○薇擔任人頭公司負責人，或以每位 15 萬至 60 萬元代價尋找人頭公司負責人，再透過鄭○女、張○信等記帳士業者協助公司設立登記，陸續成立神○公司、嘉○公司、快○興業有限公司、博○公司、鑫○達公司、怡○公司、神○公司、崛○公司、創○企業有限公司、鮮○實業有限公司、三○興業有限公司、三○興業有限公司、家○有限公司、鎧○有限公司、山○工程有限公司、和○有限公司、得○企業有限公司、寅○有限公司、柏○實業有限公司、三○工程有限公司、町○有限公司、加○公司等 22 間無實際經營之人頭公司，並由前揭人頭公司負責人申辦公司銀行帳戶及存摺，再向金融機構申領支票，俟取得前揭公司支票全數蓋印支票發票人印鑑後，林○良以每張支票 2,800 元價格售予何○來等中盤商，何○來再轉售予買家，該等買家明知向何○來購得之支票並無實際兌現可能，卻仍基於詐欺取財故意，將支票交付予不知情之第三者，作爲支付貨款、調借現金或清償債務之用，嗣後持票人將支票存入金融機構兌現時，該等支票皆因存款不足遭退票，持票人始知受騙。

李○良等人不法虛設 22 間人頭公司販售空頭支票行爲，不法所得共計 1,144 萬 1,600 元，該等支票嗣經下游買家行使後，共退

票 3,172 紙，金額合計爲 50 億 1,492 萬 5,754 元。執法機關執行搜索時，查扣林○良等案關人名下帳戶財產共計 356 萬 1,520 元。

二、可疑洗錢表徵

客戶開立票據其合計金額達特定金額，符合洗錢表徵。

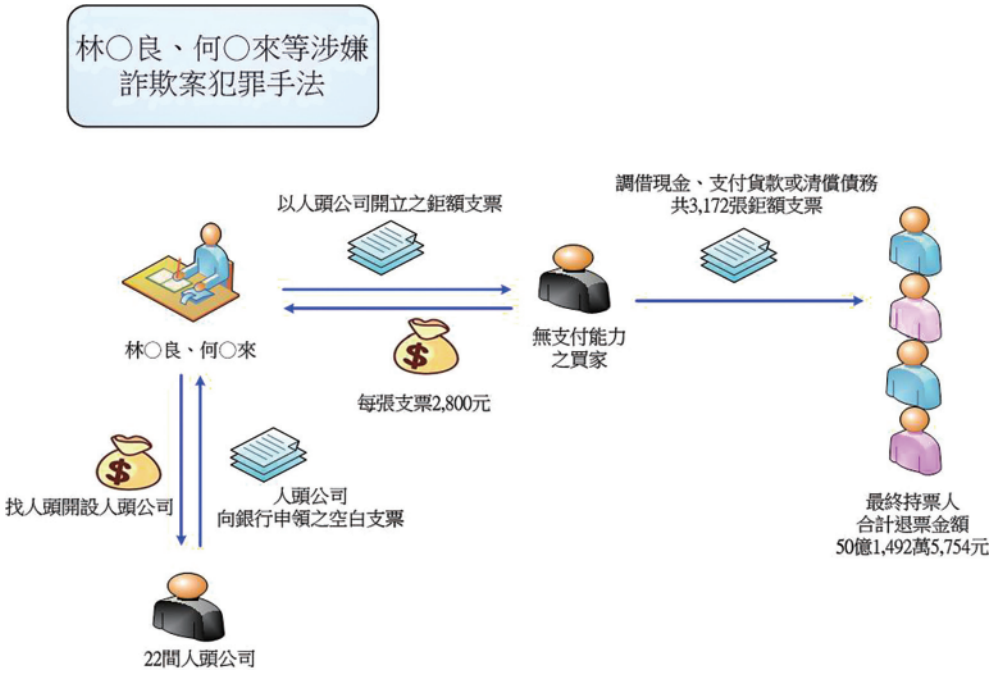
三、起訴情形

臺灣新北地方檢察署檢察官於 108 年 8 月間以觸犯刑法詐欺罪及違反公司法等罪起訴林○良、何○來、謝○章、譚○雄及盧○凱等人。

四、經驗參考

（一）案關人頭公司金融帳戶，經常有小額之整數款項存入，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。

（二）金融機構與客戶建立業務關係時，宜瞭解客戶實際運作情形，落實客戶審查作爲，尤其是法人戶申請支存帳戶之際，應加強查核交易對象及交易眞實性，以避免有心人取得支票後從事不法行爲情形。



第四部分

專題研究

打擊資助武器擴散之國際趨勢及我國執行現況—以查緝國人協助朝鮮民主主義人民共和國爲例

打擊資助武器擴散之國際趨勢及我國執行現況—以查緝國人協助朝鮮民主主義人民共和國爲例

何凱婷[5]

摘要

近年隨著防制洗錢及打擊資助恐怖主義（以下稱「資恐」）、資助武器擴散（以下稱「資武擴」）之國際聲浪驅使下，有關規避大規模毀滅性武器相關制裁決議之非法貿易案件，已成爲打擊資武擴之重要議題。2018 年間，聯合國安全理事會（以下稱「安理會」）第 1718 號決議制裁名單中，更有臺灣公民及相關實體遭指定爲制裁對象[6]，就晚近發生國人協助朝鮮民主主義人民共和國（以下稱「北韓」）規避安理會制裁之案件觀之，雖然臺灣目前並非聯合國會員國，惟身爲國際社會之一分子，對於聯合國通過的相關決議案仍應遵守並配合執行。且由於臺灣位居亞太經貿樞紐，港口航運發達，貿易往來活絡，我國貿易商易爲北韓相關空殼或仲介公司蒙蔽或驅使，進而被利用於協助北韓進行海上駁油，後續衍生協助規避制裁案件，已爲國際間打擊資武擴之關注焦點。因此，如何接軌安理會決議有關打擊資武擴及落實我國資恐防制法義務，實有賴公、私部門攜手合作，熟悉相關決議內容及履行法定義務，始能有效杜絕有心人士利用我國特殊之國際地位或國民，遂行資助北韓等經公告爲國際洗錢或恐怖主義之國家、組織、人員發展大規模殺傷性武器。

---

[5] 法務部調查局中部地區機動工作站調查官。

[6] UNITED NATIONS, 2020. *Security Council 1718 Sanctions Committee Adds 22 Entries to Its Sanctions List, Designates 27 Vessels* [online]. United Nations. [viewed 2 June 2020]. Available from: https://www.un.org/press/en/2018/sc13272.doc.htm

壹、背景緣起：

法務部依據資恐防制法（以下稱「資恐法」）規定，先後於 2018 年 1 月及 3 月間就我國人非法協助北韓從事貿易往來事件，進行相關制裁公告。被指定制裁之個人、法人及實體經法務部公告後，金融機構及指定之非金融事業或人員依洗錢防制法（以下稱「洗防法」）及資恐法相關規定，應立即全面檢覈其客戶身分並進行必要之資產限制處分及通報等措施，藉此達到全面阻斷金流之制裁效果。資恐法自 2016 年 7 月 27 日施行迄今已近 4 年，惟規範內容涉及相關安理會決議，較不貼近民眾日常生活，且因我國並非聯合國會員，國人確實有可能在不瞭解國際規範內容及不諳資恐法之相關法定義務下誤觸法網，進而違反安理會相關決議。有鑑於此，本文將概述打擊資武擴之國際規範、國內相關法制及實際案例，作爲我國未來防制資武擴政策及實務運作之參考。

貳、打擊資助武器擴散之國際規範概要：

依據聯合國憲章第 7 章賦予安理會之職權[7]，安理會依據憲章第 39 條規定就任何和平之威脅、和平之破壞或侵略行爲之存在與否，應予情勢判斷，並作成相關決議，藉以呼籲並課予聯合國會員國共同履行決議內容之義務。安理會爲防止情勢惡化，可先作成臨時辦法，於作成建議或決定辦法後可施以「經濟制裁」。依該憲章第 41 條，「經濟制裁」係指就經濟關係、鐵路、海運、航空、郵、電、無線電及其他交通工具之局部或全部停止，以及外交關係之斷絕；在經濟制裁辦法爲不足或已經證明不足時，始得採取相關「軍事措施」，即憲章第 42 條所賦予之空、海、陸軍示威、封鎖及其他軍事舉動。

聯合國就打擊資武擴係採雙軌制，分爲「全球性作法」（又稱概括條款）及「特定國家作法」（即針對北韓及伊朗），本文主要係就與北

[7] UNITED NATIONS, 2020. *Home/ Charter of the United Nations/ Chapter VII* [online]. United Nations. [viewed 2 June 2020]. Available from: https://www.un.org/zh/sections/un-charter/chapter-vii/index.html

韓相關之打擊資武擴安理會決議及防制洗錢金融行動工作組織（Financial Action Task Force, FATF）之相關建議予以說明。

一、安理會及其相關決議[8]：

（一）「全球性作法」係依據安理會決議第 1540 號（2004 年）及其後續決議案，主要呼籲國家及非國家行爲者（Non-State Actors）[9]，即與政府沒有隸屬關係，未受政府指導或資助之組織及個人，應禁止資助武擴活動，且應就可能挹注武擴品項之出口及轉運等相關提供資金或服務者，建立或制定適當之審查及控制措施。

（二）「特定國家作法」係依據安理會決議第 1718 號（2006 年）及第 2231 號（2015 年）及其後續決議案，分別針對「北韓」及「伊朗」之資武擴制裁。伊朗與北韓在資武擴制裁最大不同之處，在於聯合國於 2015 年已透過安理會決議第 2231 號，終止先前透過安理會決議第 1737 號及其後續決議針對伊朗之制裁，但仍保留相關指定之個人及實體等目標性金融制裁措施。反觀北韓部分，因北韓有持續反覆測試核武、洲際彈道飛彈等違反及挑釁安理會決議情形，故現階段聯合國仍持續擴大對北韓關於資武擴之制裁。

（三）有別於安理會決議第 1540 號（2004 年）著重在出口及轉運管制，第 1718 號決議（2006 年）係聯合國針對北韓第一次測試核武之回應，將制裁重點放在經濟及商業制裁[10]。後續制裁決議尚包括安理會第 2087 號決議（2013 年）、2094 號決議（2013 年）、2270 號決議（2016 年）、2321 號決議（2016 年）、第 2356 號決議（2017 年）、第 2371 號決議（2017 年）、第 2375 號決議（2017 年）及

---

[8] FATF, 2018. *Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction* [online]. Paris, France: FATF. [viewed 30 May 2020]. Available from: www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-counter-proliferation-financing.html

[9] NSCR-NET, 2020. *Resources/Non-State Actors* [online]. International Network for Economic, Social & Cultural Rights. [viewed 2 June 2020]. Available from: https://www.escr-net.org/resources/non-state-actors

[10] Lee, S. & Park, E. 2018, "Maritime Law Enforcement by the Republic of Korea Concerning *Proliferation* of Weapons of Mass Destruction: Search and Interdiction", Pacific Focus, vol. 33, no. 3, pp. 478-496.

第 2397 號決議（2018 年）。制裁措施可略分爲二：

1. 目標性金融制裁（Targeted Financial Sanctions, TFS）：

依據 FATF 方法論詞彙表解釋，目標性金融制裁係指凍結資產及禁止資金和其他由指定之人或團體直接或間接控制之金融資產及經濟資源[11]；我國現有相關法律係資恐法第 7 條。

2. 其他制裁措施（北韓部分）[12]：

(1) 武器、其他大規模殺傷性武器等相關物資之禁運；

(2) 旅行禁令；

(3) 海上攔截和運輸檢查；

(4) 禁止制裁船隻入港及提供海上加油服務；

(5) 禁止北韓供應、銷售或轉讓煤、鐵、鐵礦石、黃金、鈦礦石、釩礦石、銅、鎳、銀、鋅、稀土礦產、鉛、鉛礦、鋼和其他金屬、糧食和農產品、機械、電氣設備、包括菱鎂礦和氧化鎂在內的泥土和石料、木材、船隻、工業機械、運輸車輛、海產食品（包括魚類、甲殼動物、軟體動物和其他一切形式水生無脊椎動物）、紡織品、雕像、直升機；

(6) 禁止北韓國民出國工作；

(7) 禁止會員國提供、銷售或轉讓奢侈品。所謂「奢侈品」依據安理會第 2094 號（2013 年）、第 2270 號（2016 年）及第 2321 號（2016 年）決議附件四所列項目，主要爲首飾、交通工具、豪華手錶、鉛水晶物項、休閒體育運動設備、地毯和掛毯（價值約超過新臺幣 1 萬 5,000 元）、瓷餐具或骨灰瓷餐具（價值約超過新臺幣 3,000 元），細節可參下表：

[11] FATF, 92-2019. *Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems* [online]. Paris, France: FATF. [viewed 30 May 2020]. Available from: http://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html

[12] 同前註 8。

首飾	■鑲有珍珠的首飾； ■珠寶； ■寶石和半寶石（包括鑽石、藍寶石、紅寶石和綠寶石）； ■用貴金屬製作的或用貴金屬包的首飾
交通工具	■遊艇； ■奢侈汽車（和機動車）：（公共交通工具以外的）運送人的汽車和其他機動車，包括箱型車； ■賽車 ■水上休閒性交通工具（如私人遊艇） ■雪地摩托（價值超過 2,000 美元）
豪華手錶	■腕表、懷錶和其他帶有貴金屬或鑲嵌貴金屬的金屬錶盤的手錶
鉛水晶物項	
休閒體育運動設備	
價值超過 500 美元的地毯和掛毯	
價值超過 100 美元的瓷餐具或骨灰瓷餐具	

(8) 禁止會員國提供、銷售或轉讓航空燃料、噴氣機燃油、火箭燃料、冷凝液及天然氣；

(9) 禁止與北韓金融交易或提供金融服務及設立分支機構、子公司、合資、開立帳戶等；

(10) 禁止使用及移轉現金相關，及與銀行及金錢或價值移轉服務機構；

(11) 禁止給予出口信用或提供保險服務；

(12) 部分限制供應、銷售或轉讓原油；

(13) 部分限制專門教育或培訓、科技合作。

二、防制洗錢金融行動工作組織（FATF）：

（一）1989 年間，七大工業國組織（G7）在法國巴黎第 15 屆經濟高峰會議上，體認到洗錢行爲對於金融體系之威脅，倡議成立 FATF，以追查毒品犯罪之洗錢行爲爲設立宗旨。1990 年間，FATF 爲凝聚國際間對於打擊毒品洗錢行爲的共識，遂制定四十項建議，首要著重於金融機構之防制洗錢，以掌握相關不法資金流向。俟因美國於 2001 年發生 911 恐怖攻擊事件，G7 在華盛頓特區召集會議，FATF 因而陸續增加九項特別建議，主要與打擊資助恐怖主義

有關。2012 年 2 月 FATF 會員大會將原四十項防制洗錢建議及九項打擊資助恐怖活動特別建議整併，除加入以風險爲本之監理方法，另加入打擊資助大規模毀滅性武器擴散議題，並綜整爲四十項建議（即用於 2013 年 11 月以後 FATF 第四輪及 APG 第三輪相互評鑑之四十項建議及十一項直接成果）[13]。相互評鑑（Mutual Evaluation）方法包含「技術遵循評鑑」及「效能評鑑」，「技術遵循評鑑」主要檢核會員國之法規、體制架構、權責機關權力及程序等是否符合 FATF 四十項建議，以瞭解該會員國防制洗錢 / 打擊資恐體系。「效能評鑑」則係評估會員國對於 FATF 建議之執行成效，並辨識該國達到完善防制洗錢 / 打擊資恐體系應有的成果 [14]。目前 FATF 評鑑方法論計有四十項建議及十一項直接成果，範圍包含 6 大面項：全國性政策協調機制、國際合作、監理及防制措施、法人與法律協議、執法機關實務議題、打擊資恐及資武擴等。

（二）關於資武擴之目標性金融制裁規範於 FATF 四十項建議中之第七項建議及直接成果第十一項，第七項建議採特定國家作法並呼應安理會第 1718 號（2006 年）及 2231 號（2015 年）及其後續決議案，要求 FATF 會員國對於北韓及伊朗，應就關於資武擴之個人、法人或實體施以目標性金融制裁，相關機制例如須設有專責機關負責指定事宜；辨識資助或支持武擴人士及實體機制；凍結及禁止被指定人士及實體相關資產或其他金融交易；凍結後之報告及調查；解凍程序等。截至本文完稿時（2020 年 6 月 22 日），聯合國公告安理會第 1718 號制裁名單上共有 80 個實體和 75 名個人 [15]，此 75 名個人部分，僅 1 名爲我國國民，其餘皆爲北韓國民。

（三）由於洗錢、資恐及資武擴對於金融體系的威脅，需要全球性的共同回應，爲了達到此一目標，FATF 透過 9 個區域性防制洗錢組織

[13] Beekarry, N. & Edward Elgar Publishing 92, *Combating money laundering and terrorism finance: past and current challenges,* Edward Elgar Pub. Ltd, Cheltenham.

[14] 同前註 11。

[15] UNITED NATIONS, 2020. *Home/ Sanctions/ 1718 Sanctions committee （DPRK),* [online]. United Nations. [viewed 2 June 2020]. Available from: https://www.un.org/securitycouncil/sanctions/1718

（FATF-Style Regional Bodies, FSRBs），範圍涵蓋加勒比海區域、歐洲委員會區域、亞太地區、東部和南部非洲區域、南美區域、歐亞區、西非區域，中東和北非區域以及中非區域，並以相互評鑑方式，督促各會員國確實及有效履行防制洗錢、打擊資恐以及資助大規模毀滅性武器擴散之國際標準。

（四）我國於 1997 年即以創始會員國身分加入亞太防制洗錢組織（Asia/ Pacific on Money Laundering Group, APG），該組織即係前述 FATF 區域性防制洗錢組織之一，因此我國除須遵循 FATF 發布之相關防制洗錢及打擊資恐建議事項，並以 APG 會員身分參與 FATF 之會務活動[16]。我國於 2001 年、2007 年及 2018 年接受 APG 評鑑，2019 年第三輪相互評鑑獲 APG 大會採認，取得最佳之「一般追蹤」（Regular follow- up）評鑑成果[17]。依據 2019 年 10 月公告之我國防制洗錢及打擊資恐之相互評鑑報告，武擴之目標性金融制裁在建議第七項係爲「大致遵循」（Largely Compliant, LC），直接成果第十一項爲「相當有效」（Substantial level of Effectiveness, SE），評鑑報告於技術遵循摘要彙整之相關法制缺失，可作爲未來相關法令修法之參考[18]。

參、我國打擊資助武器擴散之相關法令概況：

一、資恐防制法[19]：

[16] ASIA/PACIFIC GROUP ON MONEY LAUNDERING, 2020. *Home/ Members & Observers/ Members* [online]. APG. [viewed 2 June 2020]. Available from: http://www.apgml.org/members-and-observers/members/default.aspx

[17] 行政院洗錢防制辦公室，https://www.amlo.moj.gov.tw/1506/1507/14969/post （最後瀏覽日：109 年 6 月 2 日）。

[18] ASIA/PACIFIC GROUP ON MONEY LAUNDERING, 2020. *Home/ Publications/ Mutual Evaluation/ Chinese Taipei's measures to combat money laundering and terrorist financing* [online]. APG. [viewed 2 June 2020]. Available from: http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-chinese-taipei-2019.html

[19] 全國法規資料庫，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0030047（最後瀏覽日：109 年 6 月 2 日）。

（一）兼具資恐及資武擴之目標性金融制裁規定：

參酌《制止向恐怖主義提供資助的國際公約》[20] 之精神及 FATF 第六項及第七項建議，各國應遵循制止資助恐怖分子、恐怖主義及有關防制與阻絕大規模毀滅性武器擴散之安理會決議案，對相關決議所指定制裁對象，應施行目標性金融制裁而凍結其資產。我國就資恐及資武擴之目標性金融制裁之落實，係規範於同一法律即資恐防制法，該法相關規定內容包含資恐及資武擴之制裁指定、除名公告程序、受制裁對象之資產及經濟資源限制處分、通報及相關救濟等。

（二）制裁分爲「法定制裁」及「決議制裁」：

法務部爲資恐法之主管機關，相關制裁公告性質係屬行政處分，並於法務部爲指定或除名公告時發生效力，受制裁對象如不服該公告，依資恐法第 12 條規定，得循行政救濟管道。依據資恐法第 4 條及第 5 條規定，制裁可分爲「決議制裁」及「法定制裁」2 類，主要的區分標準爲作成制裁決議之機關不同，前者爲我國資恐防制審議會，後者爲安理會：

1. 「決議制裁」：依資恐法第 4 條第 1 項規定，對於涉嫌犯恐怖活動罪及依資恐防制之國際條約或協定要求，或執行國際合作或聯合國相關決議，認個人、法人、團體有指定制裁之必要者，法務部依調查局提報或依職權，得提請召開審議會，由法務部部長擔任召集人，其餘委員分別由國家安全局、內政部、外交部、國防部、經濟部、中央銀行、金融監督管理委員會之副首長兼任，係採跨部會共同研商機制。個人、法人或團體須經審議會決議，始得指定爲制裁名單。我國人陳○憲制裁案 [21]，即依資恐法第 4 條經審議會決議指定爲制裁名單並公告；因此，經審議會決議指定爲制裁名單者，其除名亦須經審議會決議爲之。
2. 「法定制裁」：係依據資恐法第 5 條第 1 項規定，對於安理會

[20] 行政院洗錢防制辦公室，https://www.amlo.moj.gov.tw/1461/1469/1474/3127/（最後瀏覽日：109 年 6 月 2 日）。

[21] 法務部，https://www.moj.gov.tw/cp-21-50352-a3aea-001.html（最後瀏覽日：109 年 6 月 2 日）。

資恐相關決議案及其後續決議、或依有關防制與阻絕大規模毀滅性武器擴散決議案所指定者，法務部依調查局提報或依職權，應即指定制裁，此類之除名公告亦須安理會決議公告，法務部始得爲我國後續之除名程序。我國人張○源制裁案[22]，即依資恐法第 5 條規定實施制裁。

（三）制裁公告之法律效果：

1. 依資恐法第 7 條第 1 項規定，經資恐法第 4 條（決議制裁）及第 5 條（法定制裁）指定之制裁對象，禁止進行任何金融交易、禁止移轉或變更其財物及財產上利益，亦禁止第三人資助受制裁對象。參酌 FATF 評鑑方法論建議第七項第 2 點（b）規定內容，目標性金融制裁凍結義務範圍包含：（i）由被指名之人或團體所擁有或控制之全部資金或其他資產，且不以涉及具體的武器擴散行動、密謀或威脅者爲限；（ii）由被指名之人或團體直接或間接、全部或共同擁有或控制之資金或其他資產；（iii）從被指名之人或團體直接或間接擁有、控制之資金或其他資產所衍生之資金或其他資產；（iv）代表被指名之人或團體執行或受其指示之資金或其他資產，可見凍結資產範圍甚廣，因此 2018 年 11 月 7 日修正通過之資恐法第 7 條第 2 項，明示禁止資產處分範圍，包含第三人受指定制裁之個人、法人或團體委任、委託、信託或其他原因而爲其持有或管理之財物或財產上利益，亦在限制處分範圍。
2. 另關於直接或間接持有資金或其他資產之認定，我國資恐法修正立法理由[23]載明可參考美國財政部海外資產控制辦公室（The Office of Foreign Assets Control, OFAC）對於受指定制裁者所有之資產範圍，即採受指定制裁者直接或間接所有之財物或財產上利益比例達 50% 或以上（directly or indirectly owned 50 percent or more）之標準（即 50 Percent Rule），即屬資金或其他資產禁止處分範圍。

[22] 法務部，https://www.moj.gov.tw/cp-21-101060-369f1-001.html（最後瀏覽日：109 年 6 月 2 日）。

[23] 立法院法律系統，https://lis.ly.gov.tw/lglawc/lglawkm（最後瀏覽日：109 年 6 月 2 日）。

二、洗錢防制法及其相關法令規定（打擊資助武器擴散部分）：

（一）對於涉及「洗錢或資恐高風險國家或地區」，加強審查、拒絕交易或其他必要措施：

1. 依據洗防法第 11 條第 1 項規定，金融機構、指定之非金融事業或人員對洗錢或資恐高風險國家或地區，主管機關可令其強化相關交易之確認客戶身分措施（第 1 款）；限制或禁止金融機構、指定之非金融事業或人員與洗錢或資恐高風險國家或地區爲匯款或其他交易（第 2 款）；採取其他與風險相當且有效之必要防制措施（第 3 款）。北韓因屬國際防制洗錢組織公告之防制洗錢及打擊資恐有嚴重缺失之國家，故金融機構、指定之非金融事業或人員可依洗防法第 11 條第 1 項規定對其交易之客戶身分、金融交易爲相關之加強審查、拒絕交易或其他必要措施。惟須注意的是，由於北韓接連發射飛彈及核武試驗，影響國際秩序甚爲嚴重，因此經濟部於 2017 年 9 月 25 日起依據貿易法第 5 條規定公告全面禁止與北韓貿易。
2. 所稱「洗錢或資恐高風險國家或地區」，依據洗防法第 11 條第 2 項規定，爲經國際防制洗錢組織公告防制洗錢及打擊資恐有嚴重缺失之國家或地區，例如 FATF 所列「黑名單」：北韓、伊朗（FATF 發布日期：2020 年 2 月 21 日）[24]；經國際防制洗錢組織公告未遵循或未充分遵循國際防制洗錢組織建議之國家或地區，例如 FATF 所列「灰名單」：阿爾巴尼亞、巴哈馬、巴貝多、波札那、柬埔寨、迦納、冰島、牙買加、模里西斯、蒙古、緬甸、尼加拉瓜、巴基斯坦、巴拿馬、敘利亞、烏干達、葉門、辛巴威（FATF 發布日期：2020 年 2 月 21 日）[25]；其他

[24] FATF, 2020. *Home/ Publications/ High-risk and other monitored jurisdictions/ High Risk Jurisdictions subject to a Call for Action- 21 February 2020* [online]. Paris, France: FATF. [viewed 2 June 2020]. Available from: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html

[25] FATF, 2020. *Home/ Publications/ High-risk and other monitored jurisdictions/ Jurisdictions under Increased Monitoring- 21 February 2020* [online]. Paris, France: FATF. [viewed 2 June 2020]. Available from: http://www.fatf-gafi.org/publications/

有具體事證認有洗錢及資恐高風險之國家或地區。有關洗錢或資恐高風險國家或地區相關資訊不定期更新，最新資訊可參考法務部調查局洗錢防制處網站[26]。

（二）疑似洗錢或資恐可疑交易申報：

依洗防法第 10 條規定，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。此為我國金融機構及指定之非金融事業或人員申報疑似洗錢或資恐可疑交易之規定。2018 年 11 月 14 日修正公告之「金融機構防制洗錢辦法」[27] 第 15 條規定，有關可疑交易申報時程，參照國際作法及 FATF 標準修正，要求對於符合監控型態者，應儘速完成檢視，另對於經檢視屬可疑交易者，要求應於簽報專責主管核定後立即申報，申報期限不得逾 2 個營業日。上開規定將申報期限由 10 個營業日修正為 2 個營業日，應係為符合 FATF 第二十項建議，規定金融機構懷疑或合理懷疑交易資金係犯罪所得或涉及資恐，應「立即」向金融情報中心（即我國法務部調查局洗錢防制處）申報疑似洗錢或資恐交易，故申報期限修正為 2 個營業日較符合前述「立即」要件。指定之非金融事業或人員依 FATF 第二十三項建議第 1 點規範，亦須遵守第二十項建議關於申報疑似洗錢或資恐交易之規定，故亦有申報疑似洗錢或資恐交易之義務。

（三）制裁對象之財產通報：

依據資恐法第 7 條第 3 項規定，洗防法第 5 條第 1 項至第 3 項所定之機構、事業或人員（即金融機構、辦理融資性租賃、虛擬通貨平台及交易業務之事業、指定之非金融事業或人員），因業務關係知悉其本身持有或管理經指定制裁之個人、法人或團體之財物或財產上利益（第 1 款）及經指定制裁之個人、法人或團體之財物或財產上利益所在地（第 2 款），應即通報法務部調查局。2018 年 11 月 14 日修正公告之「金融機構對經指定制裁對象之財物或財產

high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html

[26] 法務部調查局洗錢防制處，https://www.mjib.gov.tw/mlpc（最後瀏覽日：109 年 6 月 2 日）。

[27] 金融監督管理委員會銀行局，https://www.banking.gov.tw/ch/home.jsp?id=248&websitelink=artwebsite.jsp&parentpath=0,8,246（最後瀏覽日：109 年 6 月 2 日）。

上利益及所在地通報辦法」[28] 第 3 條第 1 項第 1 款，原規定金融機構自知悉之日起算 10 個營業日內向法務部調查局通報，亦同步修正爲應於知悉後即簽報專責主管核定，核定後 2 個營業日內向法務部調查局通報。

肆、我國查緝資助武擴案件與分析：

一、案例分享：

（一）陳○憲制裁案[29]：

法務部於 2018 年 1 月 12 日，依資恐法首次召集資恐防制審議會，將販賣油品給北韓的我國人陳○憲、Bunker's Taiwan Group Corporation（註冊地：英屬維京群島）及 Billions Bunker Group Corporation（註冊地：馬紹爾群島），共計 1 個人、2 境外法人列爲制裁名單。此外，以陳○憲爲實質受益人之 Oceanic Enterprise Co. Ltd. 及 UMC Corporation Peru S.A.C 之 2 個境外法人實體亦爲制裁效力所及，指列本次制裁名單。本案係我國首次對指定制裁之國人實行目標性金融制裁，爲澈底達到全面阻斷金流之制裁效力，法務部及金融監督管理委員會等相關權責機關，於法務部公告制裁後，除透過新聞媒體公播外，並於第一時間加強呼籲金融機構及指定之非金融事業或人員應就其客戶身分進行全面檢覈及進行相關資產限制性處分、通報等措施。依據官方統計資料顯示，本件制裁公告後，就金融機構通報所凍結之被制裁對象相關資產，總計筆數約 60 餘筆，包含存款、股票、保險單，價值估計約爲新臺幣 9 千萬元（約 288 萬美元）[30]。本案因陳○憲已於 2019 年身歿，資恐防

[28] 同前註 27。

[29] 法務部，https://www.aml-cft.moj.gov.tw/media/166635/8112181258454.pdf?mediaDL=true（最後瀏覽日：2020 年 6 月 2 日）。

[30] 行政院洗錢防制辦公室，https://www.amlo.moj.gov.tw/1506/1507/15239/post（最後瀏覽日：109 年 6 月 2 日）。

制審議會於 2019 年 11 月 25 日決議將之除名並公告[31]。

（二）張○源制裁案[32]：

安理會於臺灣時間 2018 年 3 月 30 日更新公告之安理會第 1718 號決議及後續相關決議案制裁名單，其中新增制裁個人及法人名單包含我國人張○源及其百分之百持有之境外公司 Pro-Gain Group Corporation（註冊地：薩摩亞）及 Kingly Won International Co., LTD（註冊地：馬紹爾群島）[33]。本案係國人張○源協助北韓取得煤炭與油品，且業經安理會決議公告指名，故依資恐法規定，由法務部逕予公告指定爲制裁對象。依據官方統計資料顯示，在公告制裁名單後，金融機構通報受制裁之個人和實體的凍結資產，約有 30 項凍結行動，價值估計約爲新臺幣 3 千萬元（約 108 萬美元[34]）。

二、分析：

有關上述二制裁案例發生後，國際間陸續有相關文獻進行探討。例如針對陳○憲制裁案，英國皇家聯合研究所（Royal United Services Institute, RUSI）[35] 於 2018 年就該案分析發現，涉及資武擴船隻通常擁有多國註冊之權宜船旗「Flags of Convenience」，雖然權宜船旗在國際線海運很常見，然而如該船隻頻繁運行地點在北韓附近，此即爲資武擴之紅旗警訊。此外，在複雜的合作脈絡下，對於第三方的租賃船隻通常很難有詳盡的身分查驗流程，因此該機構

[31] 法務部，https://www.aml-cft.moj.gov.tw/624184/624196/624197/740831/post（最後瀏覽日：109 年 6 月 2 日）。

[32] 法務部，https://www.aml-cft.moj.gov.tw/media/166629/%E6%B3%95%E5%8B%99%E9%83%A8107%E5%B9%B43%E6%9C%8831%E6%97%A5%E6%B3%95%E6%AA%A2%E5%AD%97%E7%AC%AC10700057550%E8%99%9F%E5%85%AC%E5%91%8A-1.pdf?mediaDL=true（最後瀏覽日：109 年 6 月 2 日）。

[33] 法務部，https://www.moj.gov.tw/cp-21-101060-369f1-001.html（最後瀏覽日：109 年 6 月 2 日）。

[34] 同註 30。

[35] ROYAL UNITED SERVICES INSTITUTE, 2018. *Underwriting Proliferation: Sanctions Evasion, Proliferation Finance and the Insurance Industry* [online]. United Kingdom: RUSI. [viewed 2 June 2020]. Available from: https://rusi.org/publication/occasional-papers/underwriting-proliferation-sanctions-evasion-proliferation-finance-and

呼籲公部門、保險機構、銀行機構及船運公司等在打擊資武擴領域，皆應扮演重要防線。

探究國人涉嫌資助北韓發展大規模殺傷性武器之實際情形，前揭陳○憲或張○源案應非國人與北韓進行非法貿易往來之首例，然而此兩案確係資恐法立法以來進行制裁之唯二案例。此二案不同之處在於，前者係我國透過資恐防制審議會自行指定制裁名單，後者則係依據安理會第 1718 號決議及其後續決議指列名單更新，主管機關法務部逕予公告制裁名單。

回顧過往事件，國人涉嫌與北韓從事非法貿易往來，可回溯至 1990 年間蔡○泰、蔡○勳父子案，蔡氏父子於美國利用旗下公司協助北韓購買與大規模毀滅性武器有關的貨物，並參與向北韓運送物品以支持北韓的彈道導彈計劃[36]。2008 年 6 月間，蔡○泰經臺灣臺北地方檢察署起訴僞造文書及非法運輸管制貨品，發現其使用至少兩個臺灣的前臺公司「全球○○公司」及其子公司「蓮○興業有限公司」來完成此計劃[37]。隨後美國 OFAC 即於 2009 年 1 月的行政命令（EO）13382 中指列蔡○泰、Global Interface Company 以及 Trans Merits Co., Ltd. 爲制裁對象。2013 年 5 月 1 日，蔡○泰父子遭美國執法機關逮捕，罪名包括共謀欺詐美國、共謀規避 OFAC 禁令及共謀洗錢，全案已於 2015 年確定，蔡○泰對共謀詐騙美國並實施大規模毀滅性武器擴散之事實表示認罪，遭判處 2 年有期徒刑；蔡○勳則對僞造提單認罪，遭判處 250 美元罰款並緩刑 3 年[38]。

我國在資恐法立法前，此類型案件多以涉嫌刑法僞造文書及貿易法偵辦，例如蔡○泰案即係違反貿易法第 27 條第 1 項第 1 款之非法輸往管制地區罪，雖然經濟部於 1994 年公告戰略性高科技貨品輸出入管理辦法並於 1995 年全面施行，針對軍商兩用貨品及技術出口管制清單、一般軍用貨品清單之規格進行貨品管理，如敏

[36] HOMELAND SECURITY DIGITAL LIBRARY, 2018. *The National Proliferation Financing Risk Assessment* [online]. United States. Department of the Treasury. [viewed 2 June 2020]. Available from: https://www.hsdl.org/?abstract&did=820761

[37] 臺灣臺北地方法院 97 年簡字第 2747 號刑事判決。

[38] 同前註 37。

感貨品清單目的地爲北韓或伊朗者，出口人另應於出口前申辦戰略性高科技貨品輸出許可證，並經發證後始得辦理出口[39]；然而於全球打擊資武擴之聲浪下，當時法制確實不足，無法因應國際情勢。有鑑於此，政府遂於 2016 年 7 月 27 日公布施行資恐法，並參酌 FATF 第五項至第七項建議，規範資恐及資武擴之目標性金融制裁等相關機制，俾接軌國際，並對區域安全善盡國際責任。

伍、資助武器擴散之態樣及方法：

一、FATF 在 2018 年發布打擊資武擴指引[40]重點摘要如下：

（一）關於針對北韓制裁之相關決議，擴大資產凍結範圍，包括「資金」（Funds）、「金融資產」（Financial Assets）及「經濟資源（包含船隻）」（Economic Resources）。指名之類別亦從個人、法人或團體，擴及至船隻。

（二）涉及與北韓資武擴活動相關之特徵，可分爲四類：

1. 客戶或交易與制裁國家北韓有所關聯。
2. 可能被使用於資武擴之特定貿易金融商品及服務。
3. 客戶與安理會決議禁止提供之品項、材料、設備、物品或科技有所關聯。
4. 開立貨品之發票明顯與市價不一致。

（三）該指引依據 FATF2008 年出版之資武擴態樣報告，彙整涉及資武擴有關之要素，共計有 20 類態樣，本文僅就較常見之 5 類例示如下：

1. 交易涉及具武擴疑慮及轉運之外國人士或實體。
2. 將貨品運送公司地址列爲產品之最終收貨目的地。
3. 交易涉及與目的地國家技術水平不符之貨物。
4. 客戶活動與業務概況不相同。

---

[39] 經濟部國際貿易局，https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=242&pid=662639（最後瀏覽日：109 年 6 月 2 日）。

[40] 同前註 8。

5. 貨物之申報價值明顯低於運費。

（四）該指引依據聯合國專家小組報告及其他學術研究所發現之潛在資武擴要素，計有 11 類態樣，本文僅就較常見之 3 類例示如下：

1. 涉及大規模毀滅性武器出口管制或國家管制物品之出口。
2. 交易人及其對手留存相同之聯絡資訊，例如同一地址、電話號碼等。
3. 利用個人帳戶購買工業用品。

二、美國 2018 年國家資助武器擴散風險評估報告[41]：

國家資武擴風險評估，雖不在 FATF 第一項建議之必要評估範圍內，但美國財政部打擊資助恐怖主義和金融犯罪辦公室（Treasury's Office of Terrorism Financing and Financial Crimes, TFFC） 於 2018 年會商 8 個部會如財政部、司法部、商務部、國土安全部、國務院、聯邦監理機構、國防大學及國家情報局局長辦公室等所屬下級單位共計 31 個機關及單位共同進行武擴風險評估，本文僅就該報告北韓規避制裁方式摘述如下：

（一）運用複雜多層之網絡關係規避查緝：

美國評估報告指出涉及參與資武擴計畫的實體包含北韓國營企業、銀行、中介機構、經紀人、代理商，甚至是第三國的外交官。這些實體擅於使用複雜的網絡關係，例如透過海外的空殼公司掩飾來自北韓的資金。此外，也會利用成立多個境外銀行帳戶及使用境外銀行系統，將資金匯給供應商以購置相關武器零件。多數的金融交易活動經常發生在境外國家及由非美國公民進行交易，仍多使用美國銀行進行繁雜轉匯，使美國銀行難以辨識資金的不法來源及在獲得客戶資訊上遭遇困境。

（二）透由非北韓之中介機構，利用內部清算與北韓相關貿易進出口交易款項，以減少實際金流轉匯，製造金流斷點：

近期北韓透過中介機構成立非北韓貿易公司，例如貨品買賣中心樞紐，再透過進口北韓天然物資並將相關物資販售至全球市場以賺取資金，部分資金會作爲支付進口的款項，其餘款項則會使用中介者與其他北韓實體在第三國海外銀行的帳戶進行清算。因此，中

[41] 同前註 37。

介者只需追蹤代表其北韓客戶的付款和訂單，並在內部結算多個帳戶（包括不知情的供應商），而無需涉及北韓與其他司法管轄區之間的額外電匯。如此，中介者實質上發揮「斷點」的作用，允許北韓實體得以他國實體作爲掩護並在全球貿易中繼續使用金融體系，也因此中介者能賺取代表北韓一方交易者而獲得的高額佣金。

（三）與北韓貿易往來之前臺公司或空殼公司多設立於中國部分省份：

有關北韓使用的前臺或空殼公司，大多在中國大陸或使用中文的銀行，進行非法資金的移轉。據資料顯示，許多公司與北韓有著緊密關係，且設立登記在中國大陸遼寧、大連、丹東、錦洲及瀋陽。目前遼寧顯然是北韓主要使用進行移轉相關資助資金的熱點。有關前臺或空殼公司的主要登記業務與進出口生意有關，如紡織品、服裝、漁業、海鮮等最爲常見。這些前臺或空殼公司通常會使用同樣的地址、同一經理人或所有人、電話號碼及員工，且沒有明確的商業目的，其產品和服務付款也會出現與其業務範圍無關的交易。此外，此類公司的網站或其他網路相關資訊亦不會定期維護或更新。

三、2019 年美國財政部海外資產控制辦公室、國務院及海岸警衛隊就「處理北韓非法航運方法提出新指導（Updated Guidance on Addressing North Korea's Illicit Shipping Practices）」[42] 摘要如下：

（一）常見規避制裁之航運方法，主要爲掩飾船舶身分以便進行海上船對船過駁或隱匿貨物目的地或原產地等，另有透過關閉船舶自動識別系統、使用變造之自動識別系統（Automatic Identification System, AIS）訊息、改變船名或國際海事組織編號七位數之船舶識別代碼、僞造產地證明等相關文件。

（二）建議航運業及相關利害關係人，包括船東、經理、營運商、經紀人、船旗登記機構（例如在我國係交通部航港局）、石油公司、港口

[42] U.S. DEPARTMENT OF THE TREASURY, 2020. *Home/ Resource Center/ Financial Sanctions/ Programs/ North Korea Sanctions* [online]. U.S. Departments of State and Treasury. [viewed 2 June 2020]. Available from: https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx

營運商、船運公司、海運公司、報關行、保險公司及金融機構等皆須瞭解北韓規避安理會相關決議制裁之方法，並採取適當的控制措施，以降低風險。

四、2020 年聯合國第 1874（2009 年）號決議所設之 1718 號制裁委員會專家小組報告（S/2020/151）[43] — 有關北韓規避制裁之最新情形：

（一）持續非法進口石油、奢侈品（包括豪華汽車、酒和機器人機械等），並透過懸掛外國船旗例如西非國家獅子山共和國（Republic of Sierra Leone）之船隻與海上進行船對船交易，並採用模糊策略，包含關閉自動識別系統（AIS）、夜間進行移交或使用沒有海事組織編號之小船進行偽裝。

（二）持續透過海運出口煤炭、沙子及非法出售捕魚權以增加收入來源並將收入用於核計畫及相關導彈計畫。近期報告指出，北韓不再如同過去方式將煤炭移交到較小的船舶，改將煤炭移交到更大之散裝貨船，以轉運更多非法煤炭。

（三）持續透過第三方中介機構使用國際銀行，並對全球金融機構進行網路攻擊，非法取得虛擬貨幣或虛擬資產。依據美國國務院、財政部、國土安全部及聯邦調查局於 2020 年 4 月共同發布之朝鮮網路威脅通告「Guidance on the North Korean Cyber Threat」[44] 指出，與北韓有關之網路攻擊行動包含：2014 年之索尼影業（Sony Picture Entertainment, SPE）網路攻擊、2016 年孟加拉國銀行竊案、2016 年自動提款機快錢行動（FAST Cash）及 2017 年 WannaCry 2.0 勒索軟體攻擊事件。

（四）安理會決議第 2397 號（2017 年）要求所有會員國在 2019 年 12 月 22 日前，應遣返於國外賺取收入之北韓國民（包含資訊技術工作

[43] UNITED NATIONS, 2020. *Home/ Sanctions/ 1718 Sanctions committee （DPRK)/ Panel of Experts/ Reports* [online]. United Nations. [viewed 2 June 2020]. Available from: https://undocs.org/zh/S/2020/151

[44] U.S. DEPARTMENT OF THE TREASURY, 2020. *Home/ Resource Center/ Financial Sanctions/ Programs/ North Korea Sanctions* [online]. U.S. Departments of State and Treasury. [viewed 2 June 2020]. Available from: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_cyber_advisory_chinese.pdf

者），因此聯合國呼籲會員國就北韓國民在海外賺取工作收入作爲支持北韓核計畫和導彈計畫者，應持續予以遣返，並提交相關報告。此外，亦建議會員國應審查北韓國民各類簽證，並防止有意在海外賺取收入之北韓國民入境。

（五）關於奢侈品出口，專家小組建議在買賣契約中列入禁止轉售予受制裁管轄區（如北韓），另就奢侈品應統一出口管制清單並在考慮轉運風險情況下，建立全面審查收貨人機制。

五、我國因應北韓就非法航運規避制裁之相關措施：

有鑑於資武擴與海上貨物運輸或船舶活動相關，我國金融監督管理委員會於 2019 年 9 月 26 日核定保險業防制洗錢及打擊資恐最佳實務指引「防制透過貨物運輸保險等相關險種進行洗錢資恐武擴等活動之實務建議作法」[45]，並針對「船舶險」及「貨物運輸保險」在招攬、核保及理賠階段分別爲不同之審查措施（摘要如下），以避免潛在資武擴行爲者利用相關管道進行資助行爲。

（一）招攬階段

首重客戶審查，主要係瞭解業務關係與性質，於貨物運輸保險可參考商業發票或信用狀等文書；船舶險則須瞭解船籍國或其他登記文件，如遇客戶爲法人身分，則需使用可靠資源以辨識相關實質受益人等，如係制裁對象應拒絕建立相關業務關係。

（二）核保階段

須瞭解起運港及目的港國家或地區是否位於洗錢或資恐高風險國家或地區，於貨物運輸保險對於收貨人需爲適當之紀錄保存；船舶險需檢覈船舶身分，可使用資料庫系統，如國際海事組織船舶辨識號碼、安理會制裁船名單、美國 OFAC 制裁名單、安理會入港禁令船舶清單、交通部航港局配合安理會北韓制裁委員會公告受制裁之禁止進港船隻清單。相關船舶基本資訊可使用公開網站

[45] 金融監督管理委員會保險局，https://law.fsc.gov.tw/law/NewsContent.aspx?id=7850（最後瀏覽日：109 年 6 月 2 日）。

「MarineTraffic」[46] 或者「Equasis」[47] 進行船舶資料查詢。

（三）理賠階段

如於貨物運輸保險處理貨損時，應注意如與戰略性高科技貨品有關，應審核廠商是否有檢附我國經濟部國際貿易局核發之許可證；如係船舶險理賠，應調查被保險船舶於海上航運期間是否有不正常關閉自動辨識系統，並於理賠階段皆須就受款人名單進行檢覈及相關紀錄保存。

陸、結語：

由於北韓陸續於 2006 年、2009 年、2013 年、2016 年及 2017 年進行共計 6 次之核試驗[48]，造成國際情勢緊張及區域安全疑慮，近年打擊資助武器擴散議題遂備受國際間關注，我國雖非聯合國會員國，但於國際社會中仍占有一席之地，故對於安理會相關決議仍應本於自主精神，完全遵守並配合執行。國內相關公、私部門如能就本文所述相關議題先行瞭解並掌握相關資訊，將能避免涉及資武擴之情事再次發生，希冀本文對國內從事打擊資武擴工作者有所助益，讓我國之打擊資武擴工作推展更爲順利。

[46] MARINE TRAFFIC, 2020. [viewed 2 June 2020]. Available from: https://www.marinetraffic.com/en/ais/home/centerx:120.533/centery:24.291/zoom:13

[47] EQUASIS, 2020. [viewed 2 June 2020]. Available from: https://www.equasis.org/EquasisWeb/public/HomePage

[48] Erol, Eda, and Leonard Spector, 2017. *Countering north Korean procurement networks through financial measures: The role of southeast Asia* [online]. United States: James Martin Center for Nonproliferation Studies (CNS). [viewed 17 June 2020]. Available from: www.jstor.org/stable/resrep17540

參考文獻

中文參考文獻

立法院法律系統 https://lis.ly.gov.tw/lglawc/lglawkm
行政院洗錢防制辦公室 https://www.amlo.moj.gov.tw/
全國法規資料庫 https://law.moj.gov.tw/
法務部 https://www.moj.gov.tw
法務部調查局洗錢防制處 https://www.mjib.gov.tw/mlpc
金融監督管理委員會銀行局 https://www.banking.gov.tw
金融監督管理委員會保險局 https://law.fsc.gov.tw
經濟部國際貿易局 https://www.trade.gov.tw/
臺灣臺北地方法院 97 年簡字第 2747 號刑事判決。

英文書籍

Beekarry, N. & Edward Elgar Publishing 92, *Combating money laundering and terrorism finance: past and current challenges,* Edward Elgar Pub. Ltd, Cheltenham

英文期刊

Lee, S. & Park, E. 107, "Maritime Law Enforcement by the Republic of Korea Concerning Proliferation of Weapons of Mass Destruction: Search and Interdiction", Pacific Focus, vol. 33, no. 3, pp. 478-496.

其他英文參考文獻

ASIA/PACIFIC GROUP ON MONEY LAUNDERING, 2020. *Home/ Members & Observers/ Members* [online]. APG. [viewed 2 June 2020]. Available from: http://www.apgml.org/members-and-observers/members/default.aspx

ASIA/PACIFIC GROUP ON MONEY LAUNDERING, 2020. *Home/ Publications/ Mutual Evaluation/ Chinese Taipei's measures to combat money laundering and terrorist financing* [online]. APG. [viewed 2 June 2020]. Available from: http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-chinese-taipei-108.html

Erol, Eda, and Leonard Spector, 106. *Countering north Korean procurement networks through financial measures: The role of southeast Asia* [online]. United States: James Martin Center for Nonproliferation Studies (CNS). [viewed 17 June 2020]. Available from: www.jstor.org/stable/resrep17540

EQUASIS, 2020. [viewed 2 June 2020]. Available from: https://www.equasis.org/EquasisWeb/public/HomePage

FATF, 92-108. *Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems* [online]. Paris, France: FATF. [viewed 30 May 2020]. Available from: http://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html

FATF, 107. *Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction* [online]. Paris, France: FATF. [viewed 30 May 2020]. Available from: www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-counter-proliferation-financing.html

HOMELAND SECURITY DIGITAL LIBRARY, 107. *The National Proliferation Financing Risk Assessment* [online]. United States. Department of the Treasury. [viewed 2 June 2020]. Available from: https://www.hsdl.org/?abstract&did=820761

MARINE TRAFFIC, 2020. [viewed 2 June 2020]. Available from: https://www.marinetraffic.com/en/ais/home/centerx:120.533/centery:24.291/zoom:13

NSCR-NET, 2020. Resources/Non-State Actors [online]. International Network for Economic, Social & Cultural Rights. [viewed 2 June 2020].

Available from: https://www.escr-net.org/resources/non-state-actors

ROYAL UNITED SERVICES INSTITUTE, 107. *Underwriting Proliferation: Sanctions Evasion, Proliferation Finance and the Insurance Industry* [online]. United Kingdom: RUSI. [viewed 16 June 2020]. Available from: https://rusi.org/publication/occasional-papers/underwriting-proliferation-sanctions-evasion-proliferation-finance-and

U.S. DEPARTMENT OF THE TREASURY, 2020. *Home/ Resource Center/ Financial Sanctions/ Programs/ North Korea Sanctions* [online]. U.S. Departments of State and Treasury. [viewed 2 June 2020]. Available from: https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx

UNITED NATIONS, 2020. *Home/ Sanctions/ 1718 Sanctions committee（DPRK)/ Panel of Experts/ Reports* [online]. United Nations. [viewed 2 June 2020]. Available from: https://undocs.org/zh/S/2020/151

UNITED NATIONS, 2020. *Home/ Sanctions/ 1718 Sanctions committee（DPRK）* [online]. United Nations. [viewed 2 June 2020]. Available from: https://www.un.org/securitycouncil/sanctions/1718

UNITED NATIONS, 2020. *Security Council 1718 Sanctions Committee Adds 22 Entries to Its Sanctions List, Designates 27 Vessels* [online]. United Nations. [viewed 2 June 2020]. Available from: https://www.un.org/press/en/107/sc13272.doc.htm

UNITED NATIONS, 2020. *Home/ Charter of the United Nations/ Chapter VII* [online]. United Nations. [viewed 2 June 2020]. Available from: https://www.un.org/zh/sections/un-charter/chapter-vii/index.html

第五部分

策略分析報告

貪瀆犯罪之策略分析報告

貪瀆犯罪之策略分析報告

壹、前言

107 年，調查局洗錢防制處受理共 3 萬 5,869 件可疑交易報告（Suspicious Transaction report, 下稱 STR），經加值分析後，其中 4,339 件 STR 製作成分析報告分送予權責機關，作爲調查共 2,283 個案件[49] 參考使用，其中僅 62 案與貪瀆及賄賂案件[50] 相關，占全部分送案數約 2.7%（詳圖一），顯然申報機構申報貪污、賄賂相關之 STR 數量甚低。爲強化申報機構偵測公務員貪污、賄賂相關之犯罪資金移動能力，本報告分析近 3 年之重大貪瀆案件，歸納其主要犯罪及洗錢態樣，剖析該等類型犯罪資金移動情形及不易被金融機構及指定之非金融事業或人員 (Designated Non-Financial Businesses and professions, 下稱 DNFBPs) 查覺主因，進而提出相關建議，供各申報機關作爲研析並申報 STR 之參考基礎。

貳、研究方法

本報告參考 105 年至 107 年調查局及廉政署移送之公務員重大貪瀆案件，以相關犯罪事實分析其洗錢或資金移動態樣，評估金融機構或 DNFBPs 可能遭利用作爲洗錢管道之風險。另本處篩選曾受理與前揭案件相關 STR 共 207 件進行分析、歸納及彙整，併同前揭重大貪瀆案件，列舉不同類型貪瀆案件之可疑犯罪指標，提供各申報機構作爲個案研析之參考。

[49] 相關統計數據請參考 APG 秘書處 108 年 10 月出版之相互評鑑報告直接成果 6 各附表所示。

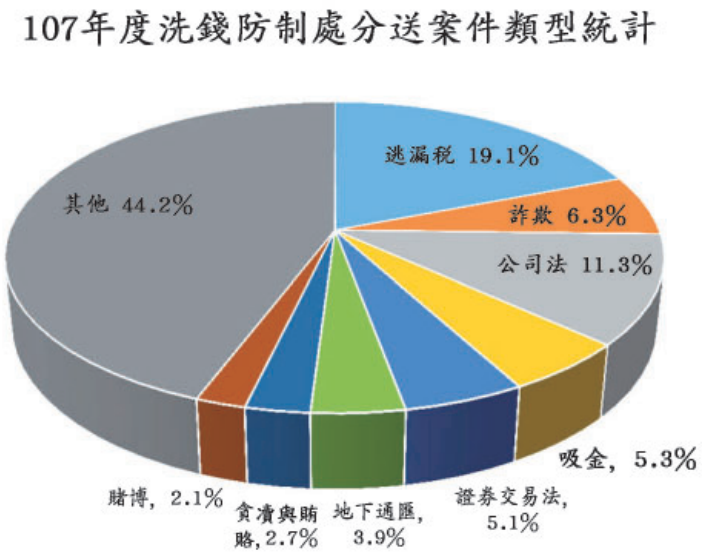
[50] 以下簡稱貪瀆案件。

參、趨勢概述

一、107 年分送權責機關前置犯罪類型之金融情報統計

綜觀 107 年洗錢防制處分送予權責機關之前置犯罪分析報告案件類型 (詳圖一)，排序前 5 名依序爲 (1) 逃漏稅捐，19.1%；(2) 違反公司法，11.3%；(3) 詐欺，6.3%；(4) 吸金，5.3%；(5) 違反證券交易法，5.1%，共占全部分送案件約 47.1%。由於該等案件類型多透過金融機構直接交易，金流軌跡透明，資金用途也較容易辨識。反觀 107 年貪瀆案件僅占全部分送案件約 2.7%，突顯貪瀆案件的識別難度。

＜圖一：107 年分送案件類型統計＞



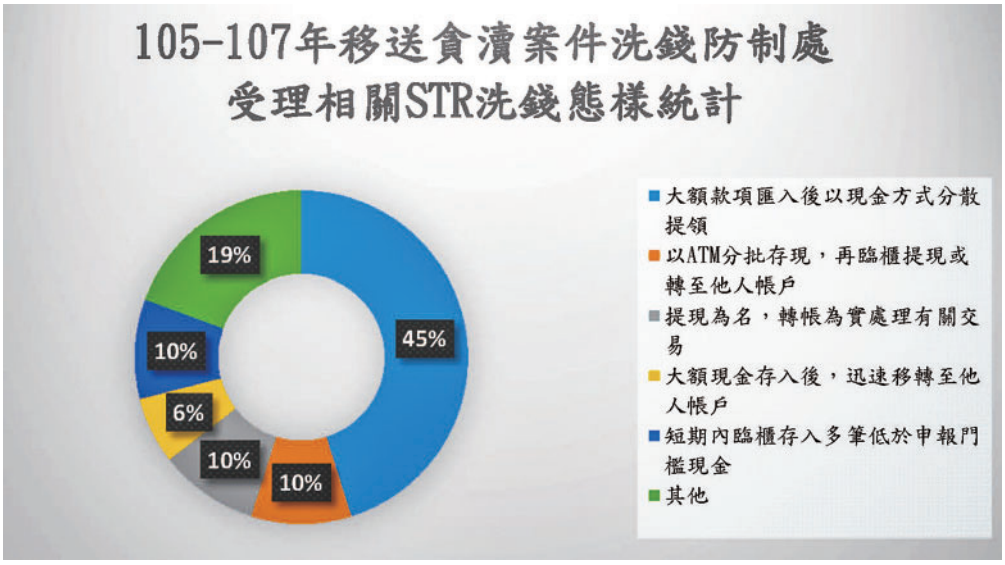
資料來源：洗錢防制處

二、105-107 年分送之貪瀆案件洗錢態樣統計

圖二係統計 105 年至 107 年調查局及廉政署移送各地檢署之貪瀆案件中，洗錢防制處受理申報相關 STR 所歸納之主要洗錢態樣。常見方式爲現金分散提領、ATM 分批存現及以提現爲名，轉帳爲實等方法移轉不

法所得。「其他」類型則包含「以不法利得購買轎車並登記於他人名下」、「大額現金存入後，立即結購外匯或旅行支票」、「自海外帳戶匯入美金，不久即匯款支出美金至海外其他公司帳戶」、「帳戶短期內由特定公司匯入多筆大額款項」及「經常性溢繳信用卡費用」等情形。

＜圖二：105-107 年移送貪瀆案件 AMLD 受理相關 STR 洗錢態樣統計＞



資料來源：洗錢防制處

三、105-107 年移送之貪瀆案件洗錢防制處受理 STR 申報比例：

統計 105 年至 107 間調查局及廉政署移送貪瀆案件共 773 件[51]，其中曾被金融機構或 DNFBPs 申報相關 STR 案件數僅 30 案，占全部移送案件約 3.88%。自該期間重大移送案件觀之，許多交易係透過小額現金存、提或以見面方式交付賄款，使金融機構不易察覺犯罪活動。另有多個案例顯示相關帳戶有「大額現金存、提」、「短期內鉅額財產增加」及「使用人頭帳戶隱匿不法所得」等可疑態樣，惟因調查人頭帳戶之實質受益

[51] 廉政署 105 年至 107 年移送貪瀆案件數為 347 件；調查局 105 年至 107 年移送貪瀆案件數為 426 件。

人及其資金來源、用途有一定難度，執行上尚須仰賴申報機構健全並落實 KYC 及客戶盡職調查程序。

肆、貪瀆及賄賂犯罪可疑指標

以下可疑指標係蒐整 105 年 1 月 1 日至 107 年 12 月 31 日期間，調查局及廉政署移送貪瀆案件及洗錢防制處受理相關 STR 之不同犯罪類型違法態樣。

一、違反政府採購法案件

不具投標資格之 A 公司借用 B 公司名義及證件投標，並得標政府採購案。

B 公司出借公司名義及證件予 A 公司參標，將帳戶存摺及大小章交予 A 公司保管使用。

A 公司借用 B 公司牌照共同參與投標製造競爭假象，並由 A 公司代 B 公司製作投標文件並提供資金以 B 公司名義開立押標金銀行支票。

A 公司借用 B 公司牌照共同參與投標並由 B 公司得標，驗收完成後 B 公司將公庫匯入之公款另以「抵銷貨款」等名目撥款予 A 公司。

A 公司借用 B 公司牌照共同參與投標，B 公司得標後將委託機關匯入之工程款扣除約 8% 營業稅費用後匯入 A 公司控制帳戶。

A 公司借用 B 公司牌照共同參與投標，B 公司得標後，將收到之各期工程款扣除未稅工程款之 3.5% 至 4% 後，全數匯回 A 公司指定帳戶。

公務機關以最有利標方式配合特定廠商招標，公告刊登有利於該廠商之規格及限制條件。

投標廠商協議不為競爭，分配輪流得標順序，並實質影響投標價格。

投標文件內容廠商地址、電話、傳真、電子郵件及聯絡人相同。

投標廠商雖達 3 家以上，但開標後另外 2 家資格明顯不符。

投標廠商押標金支票連號，退還款項後資金回流至同一帳戶。

二、公務員行、受賄案件

（一）工程類

公務員向政府採購案得標廠商收受決標金額 4% 至 15% 不等比例回扣，廠商於領得各期估驗款及尾款時交付賄款。

公務員向得標廠商收取得標金額約 5% 作爲提早通過驗收、請領估驗款及尾款之對價賄款。

第一期估驗款匯入得標廠商帳戶後，即由公司派人領取約定比例之賄款現金，當面交予公務員或白手套。

公務員銀行帳戶存入的支票存款，係由營造商或其他自政府採購案得利的個人或法人開立存入。

負責政府採購案合約的公務員收到來自海外匯入的高額款項，惟款項金額與公務員的身分、職業、背景顯不相當。

公務員利用餐廳包廂、私人座車等隱蔽處所商議、受領廠商承諾之行賄款項。

得標廠商之會計人員自公司帳戶提現交付賄款，並以股東往來、還款之科目作帳。

公務員配合特定廠商將工程標案自「最低價標」變更爲「公開評選」之招標方式並收取回扣。

公務員下修工程總預算金額使特定廠商達到可投標門檻並收取對價。

公務員以「旅遊贊助」及「廟宇祭祀」等地方活動名義向參標廠商索賄。

公務員協助業者加速審查土地開發案並索取對價。

公務員包庇土石方清運業者以不合格之土石方回填並收取利益。

（二）稅務案件

稅務員包庇特定廠商以對開發票或循環開立不實發票等方式協助他人虛增營業額、美化財報或虛增進項稅額逃漏稅捐。

稅務員協助特定廠商填具不實之「營業人銷售額與稅額申報書（401 表）」及「營業人申報適用零稅率銷售額清單」向國稅局申報退稅。

稅務員與不法集團成員共謀以虛設公司行號方式假出口，眞退稅詐取財物。

稅務員使用內部電腦替他人查詢特定公司 401 表及該公司發票有無遭限購或被國稅局查核等資料並索取對價。

三、公務員來源不明財產

公務員短期內現金財產增加，與其收入顯不相當，且無法爲完整、充分、詳實之說明。

公務員或其家庭成員出現異常頻率及金額的現金提存交易。

公務員或其家庭成員以不明現金兌換外幣或購買保險商品。

公務員除個人薪資帳戶外，另使用友人帳戶收受不明來源財產。

公務員將不明財產存入個人帳戶，受行員詢問時表示係繼承長輩遺產，長輩有存放大額現金在家中之習慣。

公務員配偶或子女帳戶於特定期間存款遽增，與該名公務員薪資所得水準不符。

公務員分批將現金存入不同人帳戶，並以贈與方式將款項轉換爲他人名下資金，以清償房屋貸款等。

公務員以兼課、演講費或投資股票所得爲由收受大額資金，企圖掩飾該等資金係貪瀆所得。

公務員收受不明來源現金後直接支付房屋頭期款。

公務員或其家庭成員以成立法人或法律協議之手法購買不動產。

四、賄選案件

候選人招待選民出國旅遊並支付旅費而約其等爲投票權之一定行使。

候選人發放選民免費餐券而約其等爲投票權之一定行使。

候選人以協助發放文宣工作費之名義行賄選區內有投票權之人。

候選人以零用金或補貼油資等名義行賄選區內有投票權之人。

候選人以贊助競選經費爲由交付現金予數名里長候選人固樁。

五、員警涉貪案件

管區員警掩護轄區情色業者規避查緝，並以按月收取賄款及三節補

助費作爲對價。

員警包庇轄區賭博業者並以取得經營股份作爲對價。

員警包庇地下錢莊業者，債務人因無法償還高額利息將名下不動產過戶予警員密友。

員警辦理單位採購案時向特定廠商洩漏參標家數及評委名單並收受廠商回扣。

警員包庇特定對象犯罪行爲不予舉發並要求賄款作爲對價。

伍、個案研析

一、胡○彬法官收賄案

（一）案情概述：

胡○彬係臺灣高等法院臺中分院民事庭法官，黃○蟾係胡員同居人，邱○德係中○大飯店股份有限公司（下稱：中○大飯店）前董事長，邱○珠係邱○德長女，黃○玲係邱○德長媳，鞏○玲係邱○德次媳。101 年 10 月至 102 年 8 月間，胡員利用承審中○大飯店家族股權糾紛之民事案件機會，基於期約與收受賄賂之犯意，同意協助邱○珠保衛其在中○大飯店之經營權，遂以拖延訴訟方式使原告鞏○玲同意和解。102 年 5 月間邱○珠透過黃○玲轉交市值 4 萬 4,800 元之琉璃藝品予胡○彬，嗣胡○彬於該案審理終結後，另於 102 年 8 月，收受邱○珠透過黃○玲在胡員寓所交付賄款 300 萬元。

（二）本案犯罪及洗錢態樣：

1. 租用他人保險箱隱匿不法所得：

胡○彬收受邱○珠轉交之 300 萬元賄款後，將部分款項存放於同居人黃○蟾以其弟媳名義租用之保險箱內，企圖隱匿不法所得。

2. 財產來源不明：

偵辦期間發現前開保險箱內共有 2,300 萬餘元現金，又於胡○彬住處另查獲百萬元現款，總額超出胡○彬受賄款項。經

檢方逐一清查胡○彬犯罪後近 3 年收入來源，認其有異常收入之實，且胡○彬不願清楚交代收入來源，構成財產來源不明罪。

3. 以不法所得購車並移轉他人名下：

胡○彬爲防止購置己用之凌志轎車資金來源遭檢調追查，遂以同居人黃○蟾之父爲購車名義人，先由黃○蟾自前開保管箱取出 177 萬元現金，再將款項分拆成 45 萬元、37 萬及 1 萬 2,000 元分日存入黃○蟾父親帳戶內作爲新車尾款。

二、前鄉長李○煌等收賄案

（一）案情概述：

李○煌爲前屏東縣○○鄉鄉長，蔡○和係李○煌秘書，103 年 12 月 25 日李○煌卸任後由蔡員接任其職務，黃○綸係綠○工程顧問有限公司（下稱：綠○公司）及裕○營造有限公司（下簡：稱裕○公司）實際負責人。李○煌卸任後入股裕○公司成爲股東。該鄉公所於 102 年 12 月 5 日公告招標「屏東縣○○鄉○○國小學童安全通學步道環境改善計畫」之營造標案，李○煌及蔡○和共同基於職務上行爲收受賄賂之犯意聯絡，收受黃○綸所交付「○○國小通學步道一期工程」營造標案之得標金額 15% 約 233 萬元之賄賂款項。黃○綸後於 103、104 年間，分別再就「○○鄉成功路一期工程」之營造標案行賄李○煌賄款 120 萬元、就「○○鄉成功路二期工程」、「○○鄉民族路一期工程」、「○○火車站景觀工程」之營造標案行賄蔡○和賄款合計 300 萬元、就「○ O 火車站景觀工程」之設計監造標案行賄蔡○和賄款 10 萬元。其中黃○綸於 105 年 6 月間爲使爲裕○公司順利得標「○○火車站景觀工程」之營造標案，並爲籌措行賄蔡○和之賄款，遂透過友人所設瑪○公司向第三方 A、B 公司購買建材所需地磚等工程材料，瑪○公司再以高一倍價格轉售該等材料予裕○公司，並以瑪○公司所賺取之材料價額作爲行賄蔡○和資金[52]。

（二）本案犯罪及洗錢態樣：

1. 利用投資行爲清洗不法所得：

[52] 法務部調查局，廉政 106 年工作年報，頁 85-87，民國 107 年 10 月。

蔡○和將朋分所得之賄款，一部分交予友人購買臺灣水果銷售往大陸，另將約 130 萬元賄賂款項，存入其子所開設○○商業銀行○○分行證券帳戶，作爲股票買賣使用，以投資行爲反覆清洗不法所得。

2. 低於大額申報門檻提領現金：

裕○公司爲順利得標，與李○煌等人約定支付得標金額之一定比例賄款，每次皆以現金交付。爲避免引起金融機構之戒心，裕○公司於得標工程前幾個月即採分日提領，每次領現不超過 50 萬元之方式集結賄款，再一次交付現金。

3. 他行轉入後即自動化設備轉出：

瑪○公司配合裕○公司行賄蔡○和，利用高價轉售裕○公司之價額作爲賄款來源，查瑪○公司帳上資金短期間由裕○公司密集存入，存入不久即全數領出或轉出，帳上僅留存象徵性餘額，且交易金額遠大於瑪○公司資本額。

三、前立法院秘書長林○山收賄案

（一）案情概述：

林○山係前立法院秘書長（任期：88 年 3 月 1 日起至 105 年 1 月 31 日止）、劉○蔚係林○山配偶（無任職所得紀錄）、李○承爲網○科技股份有限公司（下稱：網○公司）實際負責人兼總經理、蕭○妮爲網○公司登記負責人，亦係李○承前妻。101 年至 104 年 1 月間，林○山多次基於收取回扣及賄賂之犯意，以其擔任立法院秘書長，具有決定該院行政、採購事務之權限，洩漏立法院「103 年度網際網路服務系統維護案」、「102 年國會憑證管理系統更新暨服務整合案」等 23 件，總額約 2 億元之資訊系統採購標案機密予網○公司李○承，並約定以每件案件得標金額扣除 5% 營業稅，再乘以 20% 作爲對價支付賄款，期間收受網○公司交付賄款 8 次，合計共 2,800 萬餘元賄款[53]。

（二）本案犯罪及洗錢態樣：

1. 利用人頭帳戶洗錢：

[53] 最高法院 107 年台上字第 2483 號刑事判決。

林○山基於掩飾、隱匿不法所得，除利用個人帳戶存放賄款，另使用配偶劉○蔚、兒子林○揚、部屬陳○吟及無實際營運之鼎○公司等帳戶存、提個人所收之現金賄款，或利用將賄款存入不同第三人帳戶，以混同帳戶內合法資金來源之洗錢方式隱匿、掩飾不法所得。

2. 構成財產來源不明罪：

檢方調查林○山於 101 年至 105 年 1 月支領薪資共 1,186 萬 668 元，期間林○山所實際使用之各銀行帳戶共計以現金存入或匯入 2 億 3,304 萬 3,440 元、交予部屬處理個人日常花費共 6,755 萬 8,800 元，又檢調於林○山住處查扣不明現鈔共 647 萬 7,000 元，林○山之來源可疑財產現金收入合計共 3 億 707 萬 9,240 元，扣除現金回流部分及前開所收賄款 2,800 萬元，仍有 2 億 4,078 萬 6,920 元來源不明現金林○山未能詳實交代。

3. 於高鐵上交付賄款：

林○山利用高鐵快速、隱密及不易遭跟監之特性，與綱○公司李○承約定搭乘同班次列車，李○承在車廂內將 700 萬元賄款交付林○山後於次站下車，林○山收取現金賄款後即返回秘書長辦公室，並指示親信蔡○全攜同上開 700 萬元現金與劉○蔚於○銀行會合，再由劉○蔚將現金全數存入渠個人帳戶。

四、局長李○昌包庇賭博電玩業者案

（一）案情概述：

李○昌係高雄市政府警察局三民二分局分局長，99 年 12 月 25 日至 102 年 1 月 28 日止，任職前高雄市政府警察局前行政科專員。渠自 100 年 3 月至 101 年 12 月底，以包庇、不予查緝賭博犯行作爲對價，定期收受電玩業者賄款，期間收受賄款共 1,114 萬元。另檢方針對 100 年 3 月至 102 年 1 月間及其後 3 年期間，查核李○昌及其配偶子女共 4 人名下金融帳戶於前揭期間內新增之定存、現金存款、信用卡刷卡金額、保費繳納金額及外匯支出紀錄，扣除李○昌該段期間薪資收入、收賄金額，全家來源不明金額仍達 1,111

萬 7,164 元[54]。

（二）本案犯罪及洗錢態樣：

1. 以現金、面交方式交付賄款：

電玩業者多透過白手套，直接至警員住處，或相約於校區、員警辦公室內交付賄款，每次交付金額約 3 至 10 萬元。

2. 收賄期間遽增不明來源財產：

分局長李○昌自 100 年至 104 年之薪資所得共 670 萬 4,564 元，查該期間內異常資金收入共 2,355 萬 1,728 元，其中包含定存 1,250 萬元、定期到期未續存之現金 30 萬元、現金存款 275 萬 8,013 元、信用卡支出 236 萬 6,429 元、保險費用 274 萬 7,076 元及出國讀書費用 288 萬 210 元。扣除上開薪資所得及上開期間所收賄款 573 萬元，李○昌全家來源不明財產共 1,111 萬 7,164 元。

3. 以所收賄款購買臺幣及美元保單：

查分局長李○昌將所收賄款部分用於購買終身保險商品，並以年繳或躉繳方式支付保費，或將現款存入臺幣帳戶後結購美金，再匯至個人外幣帳戶購買美金保單。

五、前營建署署長葉○文收賄案

（一）案情概述：

葉○文前於 97 年 8 月 1 日至 102 年 6 月 1 日擔任內政部營建署（下稱：營建署）署長，卸任後復於 102 年 7 月 15 日起至 103 年 5 月 31 日止，擔任桃園縣（現已改制爲桃園市）副縣長，爲具有法定職務權限之公務員；蔡○惠係前國立○○大學教授；趙○雄係遠○建設事業股份有限公司（下稱遠○建設公司）負責人；魏○雄係遠○建設公司開發部副總經理，並爲趙○雄之外甥。葉○文於擔任營建署長任內，基於對職務上行爲要求、期約、收受賄賂之犯意，於 100 年間藉 A7 及板橋浮洲合宜住宅案，收受遠○負責人趙○雄賄賂新臺幣（下同）400 萬元，並協助遠○建設公司以最有利評選之方向進行規畫。葉○文另於桃園縣副縣長任內，藉八德合宜

[54] 高等法院 107 年上訴字第 383 號刑事判決、最高法院 107 年台上字第 3337 號刑事判決。

住宅案擔任評選委員召集人之機會，對於職務上之行爲要求、期約2,600萬元，並透魏○雄轉交關於該案件相關容積率、建蔽率、基本戶數及標售土地地圖等資料，以利於趙○雄等人得於公告前得以事先初步評估，並實際收受1,600萬元賄款[55]。

（二）本案犯罪及洗錢態樣：

1. 分散提領現金並存放金庫：

趙○雄爲支付行賄款項，遂指示不知情之公司財務室協理或副總經理所屬之會計人員自趙○雄本人名下帳戶分多筆小額領現並存放金庫，累計達期約之400萬元後取出，由財務室人員以牛皮紙包裝將現金交予趙○雄，復轉交魏○雄交付予蔡○惠，蔡○惠於收現翌日前往營建署署長室親交葉○文收受。葉○文取得400萬元賄款後分別置於營建署署長室及個人住處供平日花用。

2. 以行李箱裝載現金一次交付：

葉○文就八德合宜住宅案取得之1,600萬元賄款，係由蔡○惠聯繫魏○雄轉知趙○雄一次備妥後，由蔡○惠購入紫色手拉型尼龍材質行李箱包裝上開1,600萬元賄款，並約一特定時間在臺北市某餐廳親交葉○文收受之。

3. 借用他人帳戶存放不明來源財產：

檢方偵查期間，調取葉○文友人陳○玲所出借予葉○文使用之A銀行第○號帳戶及B銀行第○號帳戶交易明細，發現葉○文友人前揭帳戶自100年12月23日起，至103年5月30日經檢察官開始偵查八德合宜住宅案之日止，有多筆現金存入紀錄，或由陳○玲先行以B銀行帳戶自有資金代墊A銀行帳戶支付證券交割款，再由葉○文以現金償還，總計A、B銀行帳戶共存有3,317萬5,678元現金，與葉○文於上開期間之個人收入顯不相當。

陸、貪瀆犯罪特性暨洗錢態樣分析

以下係就前揭所示重大貪瀆案件，歸納分析其中常見之犯罪特性及

[55] 最高法院105年台上字第969號刑事判決、高等法院104年矚上訴字第5號刑事判決。

洗錢態樣：

一、以現金交易製造金流斷點

貪污犯罪具高度隱密性，過程中由行受賄的雙方犯罪行爲人私下合意遂行，受賄者取得金錢對價時，爲避免留下物證，較少直接透由金融機構交付、移轉或存放不法所得，多係雙方當面交付現金賄款。受賄者取得現金賄款後，若欲將現金存入金融帳戶，爲避免引發外界側目，質疑現金來源，也會使用親信或人頭帳戶，以分隔交易時點並分散存入方式規避行員審查。

二、利用保險箱藏匿現金

如前所述，受賄者多半以現金方式取得犯罪所得，爲能隱密保管此等現金犯罪所得，必須找尋安全、隱匿的空間作爲保管處所。其中金融機構提供的保險箱服務，具備高度的安全性與隱密性，經常受到受賄者的濫用於保管現金犯罪所得。尤其受賄者爲避免外界察覺，經常以個人或親友名義租用銀行保險箱藏匿不法所得，避免經常臨櫃存、提現金而暴露身分或遭執法人員查緝。故而申報機構宜加強對於銀行保管箱實際所有人的辨識，同時強化異常使用保險箱的偵測，以避免保險箱服務淪爲洗錢工具。

三、利用自動存款機清洗小額賄款

受賄者對於現金犯罪所得的處置，除了單純的置於保險箱等安全隱匿處所外，也可能設法將現金存入金融機構帳戶中保管，爲規避金融業界防制洗錢措施，受賄者傾向以非面對面交易方式取代臨櫃存入現金交易，金融業所提供之自動存款機服務即容易成爲受賄者處置現金犯罪所得之首選，受賄者可使用非臨櫃交易方式將所收賄款分次、小額的清洗方式，存入不同金融帳戶，避開大額申報規定及臨櫃客戶受盡職調查之交易前階段。故而申報機構宜加強偵測異常的自動存款機交易，尤其是對於固定性的現金交易，更有深入偵測的必要。

四、以人頭帳戶隱匿不明來源財產

公務人員的知識水平甚高，故貪污收賄案件之行爲人（公務人員）多屬智慧型犯罪案件。我國已於 98 年 4 月 22 日通過貪污治罪條例第 6 條之 1「來源不明財產罪」，作爲追討公務人員名下與其收入顯不相當又無法合理說明來源之財產所得，其範圍不僅包含公務員本身，其配偶及未成年子女皆在審查之範圍內。貪污受賄之公務人員亦知此點，因此爲避免因收受賄賂引發財產增加導致外界追查，故而公務人員收受賄賂時，經常使用配偶及子女以外之他人帳戶，作爲隱蔽未合法申報之個人財產收入。

五、藉投資行為清洗不法所得

常見態樣如將不法所得轉入可支配之人頭帳戶，以該資金投資股票或轉至個人臺幣及外幣帳戶購買保險商品，復以解約所得款項或保單所生利息匯入指定帳戶或轉投資其他商品反覆交易。

柒、相關建議

自前揭案例發現，貪瀆及賄賂案件儘管多以現金交易，實案中仍不乏有單筆大額現金存現、透過人頭帳戶隱匿及利用轉投資行爲清洗不法所得等與金融犯罪無異之洗錢態樣，金融機構可透過下列方法鑑別：

一、以身分判別客戶財產收入之合理性

身分識別係檢視客戶是否有異常可疑交易之基礎，由前述案例中可發現公務員收賄後，利用個人或其可支配之人頭帳戶於特定期間內存入鉅額款項，案發後因無法合理解釋異常資金來源，而構成財產來源不明罪。又案例所示交易不乏單筆超過大額申報門檻 50 萬元之現金交易，單月收入或全年收入與帳戶持有人薪資水準顯不相當，申報機構應綜研客戶身份、所任職務內容、歷史交易紀錄，判斷客戶特定交易與其職務之關聯性及對於來源不明財產當事人說詞之合理性，若認異常則應申報。

二、以業別判斷客戶交易行為之異常性

如貪瀆案件之採購類型案件，行賄者與受賄者之間常約定得標金額之一定比例作爲回扣，並以股東往來及資金調撥等名義自行賄者名下公司匯出，或直接自公司提領大額現金後一次交付。申報機構可由特定業別之常態經濟活動及通常收、付款方式判斷客戶交易對象、頻率及金額之合理性，作爲是否申報可疑交易報告之參考。

三、加強人頭帳戶偵測及監控機制

由前開列舉案例可看出，受賄者經常借用友人帳戶作爲收受、寄藏或清洗不法所得之人頭帳戶，對於金融機構而言，因被借用帳戶人之身分背景、職業及活動範圍與受賄者迥異，相關交易難與受賄者直接聯結。然犯罪者借用人頭帳戶洗錢仍有破綻可循，金融機構可調查疑似借出帳戶之人特定期間進、出款項與其資力是否相稱，藉由 KYC 程序探詢客戶對帳戶內資金使用情形是否熟悉，例如某帳戶經常有不明現金存入，用途係交割股款，然帳戶申請人對交易標的、金額等細節一概不知，或相關問題皆由他人代答，據此金融機構人員應能合理研判斷客戶是否爲人頭帳戶，進而調查資金來源及去向，或由代交易人身分推判帳戶實際使用人及交易目的。

四、自特定表徵延展犯罪事實輪廓

由本報告分析個案不難發現，重大貪瀆犯罪洗錢手法並未逸脫金融機構參照之 53 項疑似洗錢或資恐交易態樣範圍，舉前立法院秘書長林○山收賄案爲例，所涉洗錢態樣即符合「客戶經常於數個不同帳戶間移轉資金達特定金額以上者」及「同一客戶在一定期間內，以每筆略低於一定金額通貨交易申報門檻之現金辦理存、提款，分別累計達特定金額以上者」等表徵。申報機構若於系統上偵測到特定表徵，可進一步結合客戶身分、業別及歷史交易紀錄，判斷其交易之合理性，以提升 STR 申報內容之完整度。

捌、結語

貪瀆及賄賂犯罪係屬我國洗錢非常高威脅犯罪，該類型犯罪之金流固然較金融犯罪隱密，金融機構仍可以公務人員之身份及其職業收入作爲指標性之起點，無論交易金額大小，向前追溯資金來源的正當性，向後追查資金流向的合理性，以瞭解客戶財富及資金運用情形，綜合研判對象是否有異常自個人或他人帳戶存、提現金、使用人頭帳戶分散不法所得、借用他人名義租用保險箱，或以來源不明財產轉投資等情形，使行政防制面向更趨完備，以降低金融服務遭犯罪份子利用作爲洗錢管道之風險。

參考文獻

一、中文部分

（一）中文書籍：

法務部調查局，廉政 105 年工作年報，民國 106 年 11 月。

法務部調查局，廉政 106 年工作年報，民國 107 年 10 月。

法務部調查局，廉政 107 年工作年報，民國 108 年 9 月。

法務部廉政署，105 年度工作報告，民國 106 年 7 月。

法務部廉政署，106 年度工作報告，民國 107 年 7 月。

法務部廉政署，107 年度工作報告，民國 108 年 7 月。

（二）法院判決：

最高法院 105 年度台上字第 2478 號判決。

最高法院 107 年台上字第 2483 號刑事判決。

最高法院 107 年台上字第 3337 號刑事判決。

最高法院 105 年台上字第 969 號刑事判決。

高等法院 107 年上訴字第 383 號刑事判決。

高等法院 104 年矚上訴字第 5 號刑事判決。

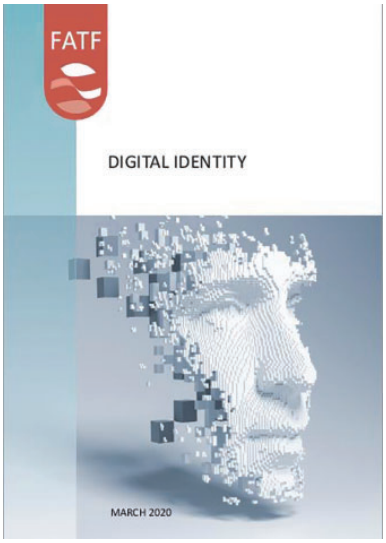
二、英文部分

APG (2019), Anti-money laundering and counter-terrorist financing measures-Chinese Taipei, Third Round Mutual Evaluation Report, APG, Sydney

第六部分

國外洗錢防制資料

FATF 數位身分指引[56]



譯按：

1. 本譯文業經 FATF 秘書處授權刊載於本年報，原文請參閱 http://www.fatf-gafi.org.，最後查閱日爲 109 年 6 月 11 日。
2. 礙於篇幅，本指引之附錄部分未予翻譯。

執行摘要

1. 數位支付每年正以約 12.7% 的速度成長，預計到 2020 年，年度交易量將會達到 7,260 億筆。[57] 到了 2022 年，估計約 60% 的全球 GDP 都將數位化。[58] 對於防制洗錢金融行動工作組織（Financial Action Task Force，FATF）而言，隨著數位金融交易量的成長，有必要進一步瞭解數位金融服務產業中的個人身分識別與確認方式。數位身分（Identity，ID）技術的迅速演進，也帶動了各種數位 ID 系統的興起。本指引旨

[56] The FATF Report "Digital Identity" has been translated into Chinese under the responsibility of the Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice with the authorization of the FATF Secretariat. The official English version of the report is available on www.fatf-gafi.org.

[57] Capgemini & BNP Paribas（2018），2018 年世界支付報告，線上存取：https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf.

[58] 國際數據資訊公司（International Data Corporation，IDC），IDC FutureScape：全球 IT 產業 2019 年十大預測。

在協助政府、受監管實體[59]和其他相關利害關係者，決定如何使用數位 ID 系統，執行 FATF 第 10 項建議關於客戶盡職調查（Customer Due Diligence，CDD）之特定要素。

2. 要運用本指引所建議之風險基礎方法，必須先瞭解數位 ID 系統的運作方式。本指引第二節就附錄 A 對於數位 ID 系統的詳細說明，重點整理其主要特色。

具備適當風險抵減措施之可靠與獨立數位 ID 系統，可被視為一般風險等級，甚至可被視為屬較低風險。

3. 第三節則摘要說明本指引所述之主要 FATF 要求，包括使用「可靠、獨立」之原始文件、資料或資訊，識別及確認客戶身分（第 10(a) 項建議）。在數位 ID 的背景情況下，確保數位「原始文件、資料或資訊」之「可靠與獨立」，代表用於執行 CDD 之數位 ID 系統所仰賴之技術、適當管理、流程與常規，必須可提供一定可信程度，以確保系統可產生準確結果。本指引認爲，仰賴具備適當風險抵減措施之可靠與獨立數位 ID 系統所進行之非面對面客戶身分識別與交易，可被視爲一般風險等級，甚至可被視爲屬較低風險。

4. 本指引所建議之風險基礎方法，仰賴一套已於數個管轄區制定，專爲數位 ID 系統設計之開放來源與共識導向確信架構與技術標準（又稱「數位 ID 確信架構與標準」）。國際標準化組織（International Organization for Standardization，ISO）和國際電工委員會（International Electortechnical Commission，IEC）正對此類數位 ID 確信架構進行標準化的程序，並更新一系列和身分識別、（US National Institute of Standards and Technology，NIST）數位 ID 確信架構與標準（NIST 數位 ID 指引）[60] 和歐盟的 e-IDAS 規章。[61] 針對本指引所提出之方法，各國應考量符合其國內數位 ID 確信架構及其他相關技術標準之做法。[62]

[59] 本指引所稱之「受監管實體」係指根據 FATF 標準所定義以及根據第 22 項建議指定之情況下，需執行 CDD 之金融機構、虛擬資產服務商（Virtual Asset Service Providers，VASPs）和指定之非金融事業或人員（Designated Non-Financial Businesses and Professions，DNFBPs）。在 2019 年 6 月，FATF 對第 15 項建議（新技術）及其注釋進行修訂，規範 VASP 必須履行第 10 項建議之 CDD 義務。

[60] NIST 800-63 數位身分指引包含一套文件：NIST SP 800-63-3 數位身分指引（概述）；NIST SP 800-63A：數位身分指引：註冊與身分證明；NIST SP 800-63B 數位身分指引：驗證與生命週期管理；以及 NIST SP 800-63C 數位身分指引：聯合識別與主張。

[61] 內部市場電子交易之電子身分與信任服務法令 (EU) N° 910/2014

[62] 管轄區可不具備數位 ID 系統指定之數位 ID 確信架構或技術標準，但可具備其他高度相關之技術標準（如：IT 資訊安全性）。

5. 數位 ID 確信架構與標準及防制洗錢／打擊資恐（Anti-Money Laundering / Counter Financing of Terrorism，AML/CFT）規範之起源和目標群眾皆不相同。本指引說明數位 ID 確信架構與標準和 FATF 關於 CDD 要求之關聯性，如下表所示，數位 ID 系統之主要組成要件與第 10(a) 項建議之特定身分識別與確認要求有關。因此，在評估 AML/CFT 用途之數位 ID 系統可靠性與獨立性方面，定義此類要件並爲各確信等級訂立要求的數位 ID 確信架構與技術標準，具高度實用性。

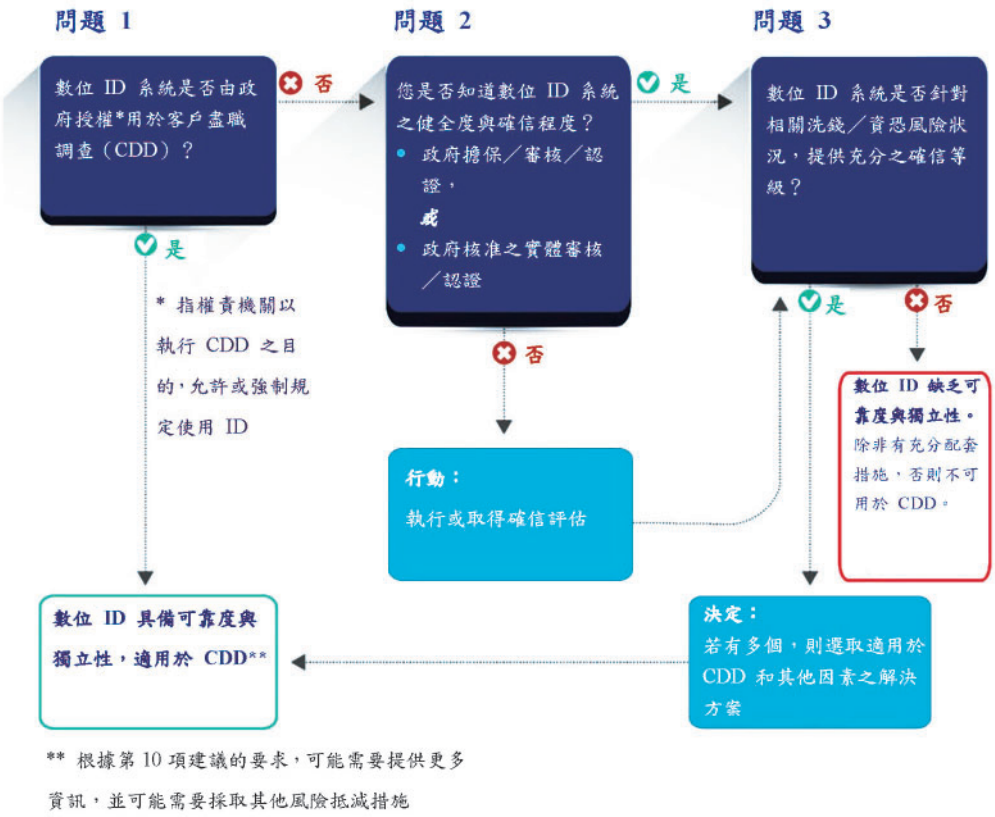
CDD 要求（自然人）	數位 ID 系統的主要要件
身分識別／確認－第 10(a) 項建議	身分證明與註冊（綁定）－您是誰？取得身分要件（姓名、出生年月日、ID 號碼等）及相關證明；驗證並確認 ID 證據，並確認爲身分經過確認之唯一個人。 綁定－核發憑證／驗證因子，將持有／控管該憑證者綁定至身分經過確認之個人 驗證－您是否爲身分經過識別／確認之個人？確定綁定之憑證確實由該身分之主張者擁有及控管。若受監管實體透過確認潛在客戶擁有預先存在之數位 ID 憑證，執行身分識別／確認，則驗證適用第 10(a) 項建議。

6. 本指引說明 (1) 若受監管實體針對已擁有數位 ID 憑證（即非內部數位 ID 解決方案）之客戶開立帳戶，則該驗證適用第 10(a) 項建議，以及 (2) 在數位金融與數位 ID 背景下，爲授權帳戶存取而對客戶身分進行有效之驗證，有助於 AML/CFT 行動。

將風險基礎方法運用於使用數位 ID 執行 CDD：(1) 瞭解數位 ID 系統的確信等級，並 (2) 在該確信等級情況下，評估 ID 系統是否具有與 ML/TF 風險相應之適當可靠度與獨立性

7. 第五節爲本指引核心，並爲政府機關、受監管實體與其他相關當事方提供指引，說明如何將風險基礎方法運用於使用數位 ID 系統進行符合第 10(a) 項建議之客戶身分識別與確認，以支援第 10 (d) 項建議所述之持續性盡職調查。本文所建議之做法爲技術中立（即未偏好任何特定類型之數位 ID 系統）。此做法包含兩個部分：
   a. 瞭解數位 ID 系統主要要件之確信等級（包括技術、架構與治理），以確認是否爲可靠獨立之資訊來源。
   b. 做出更廣泛且基於風險之決策，不論特定的數位 ID 系統，根據其確信等級，是否針對潛在之洗錢、資恐、詐騙及其他非法金融風險提供適當程度之可靠性與獨立性。
8. 第五節說明如何運用數位 ID 確認架構與標準，評估可靠度／獨立性。此外也爲受監管實體提供決策流程，根據 FATF 第 10 項建議，使用數位 ID 滿足 CDD 之部分要素是否恰當提供指引。政府與受監管實體將需要根據管轄區和個別實體之特定情況，調整此決策流程。視特定管轄區之數位 ID 系統和法規架構而定，政府以及受監管實體在評估身分系統確信等級，以及執行 CDD 合適度方面所扮演的角色與職責可能各有不同，如以下受監管實體之決策流程圖所示。
9. 本指引不具約束力；僅說明現行技術中立之 FATF 標準。

圖 1. 受監管實體之決策流程



10. 本指引第四節探討數位 ID 系統之若干效益與潛在風險。許多與數位 ID 系統相關的風險，也同樣存在於紙本 ID。然而，在開放的通訊網路（網際網路）上進行個人身分證明和／或驗證，使數位 ID 系統具有特有的風險，尤其是和網路攻擊和潛在大規模身分竊取相關之風險。另一方面，根據數位 ID 驗證架構與標準管控此類風險之數位 ID 系統，則十分有助於強化 CDD 和 AML/CFT 管控、促進普惠金融、改善客戶體驗以及減少受監管實體成本。

11. 本指引說明許多使用數位 ID 系統執行 CDD，有助於普惠金融的方式。首先，數位 ID 系統可讓政府在制定證明官方身分所需要件、身分證據與流程時，採取更彈性、更細膩及更先進的做法，包括爲了在首次開戶時，以能夠促進普惠金融目標的方式，執行客戶身分識別與確認的做法。其次，數位 ID 確信架構與標準，在流程中便已提供若干可用於證明與驗證個人身分之彈性，利於進一步客

數位 ID 系統有助於普惠金融

製化，以實現普惠金融目標。最後，監管人員與受監管實體以風險基礎方法執行 CDD 之後，有助於推展普惠金融，包括根據 2017 年 FATF 之 CDD 和普惠金融補充條款，使用與該做法同等級之數位 ID 系統。

針對政府機關之建議

12. 擬定明確的準則或法規，允許受 AML/CFT 義務監管之實體使用適當並以風險爲基礎之可靠、獨立數位 ID 系統。在一開始時，應瞭解管轄區可用之數位 ID 系統，以及該系統就現行對於客戶身分識與確認及持續盡職調查相關要求與指令（以及記錄保存與依賴第三方相關要求）之適用程度。
13. 評估所有相關機關之現行 CDD 法規與指令是否適用於數位 ID 系統，並視情況根據管轄區背景條件和身分生態系統進行修改。例如，相關機關應考慮說明，若使用具備適當確信等級之數位 ID 系統進行遠端客戶身分識別／確認與驗證時，則非面對面首次開戶客戶之 CDD 風險程度，可能爲一般至低風險。
14. 在制定 CDD 官方身分證明所需要件、證據與流程時，採用以原則、績效和／或結果爲基礎之標準。隨著數位 ID 技術迅速演進，如此將有助促進負責任的創新，以及與時俱進的法規要求。
15. 採用可讓受監管實體擬定有效整合式「風險基礎」方法之政策、法規與監督和檢查程序，此做法會在所有相關數位 ID、AML/CFT、反詐騙和一般風險管理活動中，運用資料流、技術架構與流程，強化所有風險相關功能。
16. 擬定一套整合式的、適用多方利害關係者做法，藉此瞭解和數位 ID 相關的機會與風險，並擬定管控此類風險的相關法規與指引。在適當情況下，評估並使用由身分識別、網路安全性／資料保護和隱私權之主管機關採用之現行數位 ID 確信架構與技術標準（包括技術、安全性、治理與資源考量），以供評估用於執行 CDD 之數位 ID 系統確信等級。根據 FATF 第 2 項建議與相關機關合作協調，以便形成瞭解及解決數位 ID 生態系統風險之全面一致做法，並確保數位 ID 系統之 AML/CFT 相關要求與資料保護與隱私權規定之相容性。

17.AML/CFT 主管機關可考慮採用相關機制，藉此強化與相關私部門利害關係者之對話與合作，包括受監管實體與數位 ID 服務供應商，以協助識別關鍵的身分相關機會、風險與管控措施。此類機制可包括監理「沙盒」做法，即在受監督的環境下，測試數位 ID 系統與國家 AML/CFT 法律及法規之相互關係。相關機關亦可考慮擬定可促進跨產業合作之機制，識別並解決現有數位 ID 系統之弱點。

18. 考慮以透明化之數位 ID 確信架構與技術標準，對數位 ID 系統進行審核與認證，或透過核准之專家組織執行此類作業，協助開發與執行可靠、獨立之數位 ID 系統。若相關機關未審核或自行提供身分服務供應商（Identity Service Provider，IDSP）認證，則建議透過適當之專家組織協助確信測試與認證，[63] 以便爲該管轄區提供值得信任之認證。建議相關機關支持數位 ID 驗證架構與標準之整合作業，以形成「可靠、獨立」數位 ID 系統構成要件之共識。

19. 開發及執行政府提供的數位 ID 時，採用適當之數位 ID 確信架構與技術標準。相關機關應對國內的數位 ID 系統運作方式與確信等級，保持透明化。

20. 建議採取較具彈性及以風險爲基礎之數位 ID 系統執行 CDD，以促進普惠金融。考慮提供準則，說明如何使用不同確信等級之數位 ID 系統，進行身分證明／註冊以及分級 CDD 之驗證。

21. 從分享知識與最佳做法及制定可促進國內外負責任創新法律架構的角度，監督數位 ID 空間之發展，並使境內與境外數位 ID 系統更有彈性、效率與功能性。

針對受監管實體之建議

22. 瞭解數位 ID 系統的基本要件，尤其是身分證明與驗證，以及這些基本要件如何應用於必要之 CDD 要素（參見第二節及附錄 A）。

23. 仰賴數位 ID 系統執行 CDD 應採取有根據的風險基礎方法；此類做法包括：

    a. 瞭解數位 ID 系統的確信等級，尤其是身分證明與驗證，以及

    b. 確保確信等級適用於與客戶、產品、管轄區、地理位置觸及率相關之洗錢／資恐（Money Laundering/Terrorist Financing，ML/TF）風險。

[63] 此類專家認證組織可為特定管轄區或區域提供服務，或於全球提供服務。

24. 考量低確信等級之數位 ID 系統，是否足以因應低 ML/TF 風險之簡化盡職調查。例如，在許可情況下，採用分級的 CDD 做法，透過具備不同確信等級之數位 ID 系統，促進普惠金融。
25. 若內部政策或做法一律將非面對面業務關係或交易歸類爲高風險活動，則可考慮審查並修改此類政策，表示當採用具適當風險管控措施之可靠獨立數位 ID 系統，執行客戶身分識別／確認時，風險程度爲一般或甚至更低。
26. 在許可的情況下，可運用反詐騙和網路安全性流程，協助 AML/CFT 行動之數位身分證明和／或驗證（首次開戶和持續盡職調查之客戶身分識別／確認與交易監控）。例如，受監管實體可使用數位 ID 系統內建之保護機制防範詐騙（即監控驗證事件，以偵測數位 ID 之系統性不當使用以存取帳戶，包括因數位 ID 憑證／驗證因素遺失、遭到入侵、遭竊或出售所造成之情況），以便反饋至系統，進而對業務關係執行持續盡職調查，並監控、偵測以及權責機關申報可疑交易。
27. 受監管實體應確保具備存取權限，或擬定流程以利相關機關取得基本身分資訊與證據、或個人身分識別與確認所需之數位資訊。建議受監管實體與法規單位、政策制定者以及數位 ID 服務供應商商談，探索如何在數位 ID 環境下，有效確實地實現上述目標。

針對數位 ID 服務供應商之建議[64]

28. 瞭解執行 CDD 之 AML/CFT 要求（尤其是客戶身分識別／確認與持續盡職調查）以及其他相關法規，包括受監管實體之 CDD 紀錄保存要求。
29. 尋求政府或經核准專家組織之確信測試與認證，如無法取得，則尋求其他國際聲譽良好之專家組織執行。如情況允許，可參與公部門之監管「沙盒」（或其他相關機制），藉此評估數位 ID 系統之確信等級。
30. 針對數位 ID 系統確信等級之身分證明、驗證以及適用之聯合識別／互相操作性，將相關透明化資訊提供予受 AML/CFT 監管之實體。

[64] 雖然 FATF 標準僅適用於受監管實體（即金融機構、虛擬資產服務商和指定之非金融事業或人員），但對於向（FATF 所定義之）受監管實體提供服務之數位 ID 服務供應商而言，本指引仍可提供相關背景。最後，受監管實體必須負責符合 FATF 要求。

第一節：前言

31.FATF 致力於確保全球 AML/CFT 標準，以促進負責任的金融創新。爲此，FATF 強烈支持金融產業採用符合、並可強化 AML/CFT 標準與惠普金融目標之新科技。[65]

32. 數位 ID 空間的迅速創新步調已達轉折點，隨著數位 ID 標準、技術與流程的演進，數位 ID 系統已經大規模普及或可能很快就會達到大規模普及的階段。相關技術包括：各種生物辨識科技；近乎無所不在的網際網路與行動電話（包括配備相機、麥克風及其他「智慧型手機」技術的「智慧型手機」之迅速演進與普及）；數位裝置識別碼與相關資訊（如：媒體存取控制【Media Access Control，MAC】和 IP 位址；[66] 行動電話號碼、SIM 卡、全球定位系統（Global Position System，GPS）地理位置定位）；高畫質掃描器（用於掃描身分證、駕照和其他文件）；高畫質影音傳輸（允許遠端識別與確認以及證明「存活」狀態）；人工智慧／機器學習（如：用於確認政府核發 ID 之有效性）；以及分散式帳本技術（Distributed Ledger Technology，DLT）。

快速的創新步調已達反曲點…數位 ID 系統已經或可能很快就會大規模普及。

潛在效益

33. 符合高科技、組織與治理標準的數位 ID 系統，有助於在數位時代，廣泛應用於全球經濟體的金融服務、健康與電子化政府等用途，大幅提升識別自然人身分的可信度、安全性、隱私性與便利性。這些數位 ID 是指具備較高確信等級者。

34. 就 FATF 標準而言，適當且可靠之獨立數位 ID 系統可：

- 協助首次開戶時的客戶身分識別與確認；
- 有助於整個業務關係期間之持續盡職調查與交易審查；

[65] 關於 FATF 的立場，請參閱 FinTech and RegTech （2017 年 11 月 3 日），網址：www.fatfgafi.org/publications/fatfgeneral/documents/fatf-position-fintech-regtech.html。

[66] MAC 位置識別裝置、IP 位址識別連線。

・利於其他 CDD 措施；以及
・協助以偵測與申報可疑交易爲目的之交易監控，以及一般風險管理與反詐騙作業。

35. 獨立數位 ID 系統也可幫助受監管實體降低成本並提高效率，同時允許將資源重新分配，以供其他 AML/CFT 職能使用。

36. 數位 ID 系統可協助無法取得服務或無法取得周全服務之族群在各種情況下證明其官方身分，包括透過遠端方式，以便取得受監管的金融服務，因此，可靠、獨立[67]的數位 ID 系統亦有助於普惠金融的推行，讓更多人能夠接觸受監管的金融產業，進一步強化 AML/CFT 防護措施。

潛在風險

37. 數位 ID 系統亦會構成 ML/TF 風險，務必詳加瞭解並設法管控，未能預防或管控此類風險之受監管實體，將無法滿足第 10(a) 項建議所述要求及其他 FATF 標準之規定，亦即受監管實體必須識別、評估並管控因對新型或現有產品導入新技術或開發中技術所引致之相關洗錢或資恐風險。[68]

38. 上述風險將於第四節詳加說明。未能符合相關確信等級之大規模數位 ID 系統會構成網路安全性風險，包括意圖使金融產業大規模癱瘓、或導致數位 ID 系統癱瘓的網路攻擊。此外，由於網路安全性漏洞會導致嚴重的身分遭竊事件，進而危及每個人的個人可識別資訊（Personally Identifiable Information，PII），因此也將引發重大隱私權、詐欺或其他相關金融犯罪風險。[69] 與治理、資料安全性和隱私權相關的風險，也會對 AML/CFT 措施造成影響。這些風險隨數位 ID 系統的組成要件不同而異，但就可能引發的攻擊規模看來，結果可能比傳統 ID 系統來得更爲嚴重。運用進步的科技與設計完善的身分證明與驗證流程有助於管控此類風險，請詳見第四節與第五節的說明。

39.FATF 基於對數位 ID 系統潛在風險與效益之瞭解擬定本指引，說明如

[67] 本文在某些情況下，會以「可信賴」取代「可靠、獨立」，以增加閱讀靈活性。
[68] 第 15 項建議（適用金融機構與 VASP）和第 22 建議（適用 DNFBP）。
[69] PII 包括任何本身或搭配其他資訊後，可用於識別特定個人之資訊。

何根據其標準使用數位 ID 系統，以遵守特定之 AML/CFT 要求。

宗旨與目標讀者

40. 本指引旨在協助政府機關進一步瞭解數位 ID 系統之運作，並說明如何在遵循全球 AML/CFT 標準的情況下使用數位 ID 系統。此類政府機關包括受監管實體之政策制定機關、法規主管機關、監理機關以及檢查機關；隱私權、資料保護及網路安全性（相關）機關；以及其他具備相關政策目標（如：提高普惠金融）之政府機關。
41. 本指引也希望提供幫助予私部門利害關係者，包括受監管實體和數位 ID 服務供應商。此外，國際組織、非政府組織（Non-Governmental Organisations，NGOs）以及其他針對金融服務與人道協助而提供及使用數位 ID 系統之相關單位，亦可參考本文件內容。

範疇

42. 本指引著眼於說明根據第 10(a) 項建議，使用數位 ID 系統對客戶執行首次開戶（開立帳戶）身分識別／確認時，如何遵循第 10 項建議（客戶盡職調查）。此外亦探討數位 ID 在協助執行第 10(d) 項建議之持續盡職調查（包括交易監控）的可能性。本指引也說明了受監管實體在向其他受監管實體提供客戶身分識別／確認之數位 ID 系統的情況下，應如何遵循第 17 項建議（依賴第三方）。
43. 基於技術中立的原則，第 11 項建議（紀錄保存）要求同樣適用於數位與實體（紙本）形式之紀錄保存。事實上，關於受監管實體如何保存及提供取得必要 CDD 資訊以遵循第 11 項建議要求，數位 ID 系統可能產生特定議題。數位 ID 的記錄保存方法，隨數位 ID 系統的類型與設計、系統組成元件供應商類型與職責，以及各國相關法規與合約架構不同而異。例如，當政府提供數位 ID 系統時，會收集或產生用於身分證明／註冊之基本身分證據（原始文件、資訊與資料），因此可預期政府部門會基於法規或執法用途取得此一資訊，即可遵循第 11 項建議。若受監管實體使用非政府業者提供之數位 ID 系統，基本身分證據係由數位 ID 服務商（IDSP）和／或其他實體完全或部分保存。

此外，私部門之數位 ID 服務供應商可從數位來源（如：政府資料庫或私部門公用事業紀錄）取得／確認部分或所有基本身分資料。在此情況下，說明特定證明用途之身分證明類型，包括資料來源、日期／時間與存取方式等數位化紀錄，可能與第 11 項建議一致。以上情況會由相關機關，在其 AML/CFT 和數位 ID 監管架構下，以及受監管實體透過標準機關和金融服務業者的合約關係，獲得適當處理。因此，紀錄保存和此類要求將不在本指引中贅述。

44. 本指引專注於個體客戶（自然人）之身分識別，不探討數位 ID 系統在對法人客戶進行身分識別／確認時，用於協助識別與確認法人代表身分，或其他協助執行 CDD 流程其他要素之使用方式；尤其是識別及確認第 10(b) 項建議之實質受益人身分，或依第 10(c) 項建議瞭解並取得基於業務關係目的與預期本質之資訊，雖然對所有上述 CDD 作業而言，可靠、獨立之數位 ID 系統均十分重要。

45. 本指引所指之數位 ID 系統涵蓋由政府提供、或以政府名義[70] 提供，以及由私部門提供者。關於政府提供之數位 ID 系統，本指引專注於一般用途數位 ID 系統（即：對於在該管轄區所有或大多數用途中，可有效證明官方身分之 ID），但本指引亦探討當政府授權可基於 CDD 用途使用，並提供給受監管實體和數位 ID 服務供應商之受限制用途 ID（即：特定用途有效之 ID），如：社會安全註冊或其他資料庫。更多關於本指引所涵蓋之數位 ID 系統類型，請參見第二節。

46. 本指引不會就技術、流程與架構，制定用於評估數位 ID 系統獨立性、或可靠度之確信架構或技術標準。反之，本指引仰賴由其他組織和各管轄區擬定、或正在擬定之數位 ID 確信架構與技術標準（稱爲數位 ID 確信架構與標準）。關於技術標準之說明，請參見第二節，如需更詳盡資訊，請參閱第五節和附錄 E。

47. 本指引包含五個附錄和一份有助於後續閱讀的詞彙表：

- 附錄 A：基本數位身分系統與其參與者說明：針對第五節所述之數位 ID 系統組成要件所述概念提供更詳盡的概述。
- 附錄 B：個案研究－提供數位 ID 在各管轄區使用的範例，包括

[70] 當政府與國際組織（如：UNHCR）或其他實體簽訂合約、協議或授權，以提供並管理該數位身分系統時，則該數位 ID 系統即以「政府名義」提供。非政府參與者在此類身分識別作業中，係代表政府立場。

CDD 和取得金融服務。

- 附錄 C：永續發展的身分識別原則－說明由各管轄區和組織處理的治理／當責、隱私權和其他管理操作議題。[71]
- 附錄 D：數位 ID 確信架構與技術標準制定組織－列出許多制定相關數位 ID 確信架構或標準之組織（不包含國內或區域組織）。
- 附錄 E：美國與歐盟數位 ID 確信架構與技術標準概述－提供如美國及歐盟國內與區域數位 ID 確信架構之詳細資訊。
- 詞彙表－說明本指引所使用的數位 ID 術語。

第二節：數位 ID 術語和主要特色

[71] 這些原則是透過合作流程擬定，並且經過 25 位發展夥伴、國際組織、NGO、私部門協會和政府實體認可。

本指引所指之「身分」為何？

官方身分的概念

48. 身分是一個具有許多意義的複雜概念。就 FATF 而言，第 10(a) 項建議所述之「識別客戶並確認客戶身分」，其中「身分」是指官方身分，而非可能與非官方用途（如：未受監管的商業或社會用途、親自或網際網路的同行互動等）有關之更廣義個人與社會身分概念。本指引涵蓋使用數位 ID 系統，證明「官方身分」以取得金融服務。
49. 本指引[72]所指之官方身分是指以下定義之唯一自然人：
    a. 以在該人口族群或特定背景中，建立個人獨特性之個人特徵（要件或識別碼）爲基礎，以及
    b. 受到國家法規和其他官方用途認可。

官方身分證明

50. 官方身分證明一般取決於由政府提供或核發之若干形式註冊、說明文件或證明（如：出生證明、身分證或數位 ID 憑證），而此類文件構成建立與確認官方身分之核心要件（如：姓名、出生年月日和出生地）。
51. 證明「官方身分」的準則，依管轄區不同而異。在行使統治權時，政府會制定證明官方身分的必要要件、證明與流程，這些因素可能隨時間改變。隨著身分的科技與文化概念演進，政府可授權各種身分要件。在建立證明官方身分的準則時，政府可使用固定、規定、規則基礎方法，或者以原則、績效和／或結果爲基礎的方法，後者做法較具彈性。在數位 ID 技術與標準迅速演進的情況下，管轄區得以與時俱進地跟上證明官方身分的要求，並促進負責任的創新。

使用以結果為基礎的做法建立身分要件，可讓管轄區與時俱進地跟上證明官方身分的要求。

52. 在歐盟，仰賴共同的確信架構可讓歐盟成員國因應不同的國家要求，例如：在遵循 eIDAS 架構要求情況下，接受各種國內適用之官方 ID 文件與流程。視需要確認的身分證據層面背景而定，授權來源可以有

[72] FATF 對官方身分之定義僅適用於本指引，並非用於限制其他 SSB（Secure Scuttlebutt）之替代定義。

許多形式，如：註冊簿、文件以及相關組織等。即便背景類似，但各歐盟成員國的授權來源各有不同，而 eIDAS 架構利於協調整合與互相認可。國際標準化組織（ISO）[73] 目前正針對自然人的身分識別，研擬適用於金融服務之全球標準，包括在數位環境內。

53. 在許多國家，官方身分證明是透過一般用途 ID 系統提供（有時又稱基礎 ID 系統），如：國家 ID 和市民註冊系統。此類系統一般提供文件紀錄和／或數位憑證，這些憑證廣爲政府機構與私部門服務業者認可與接受，可作爲各種用途之官方身分證明，並非所有管轄區都有一般用途 ID 系統。
54. 管轄區一般也有各種「限定用途」ID 系統（又稱功能性 ID 系統），此類系統之建置係針對特定服務或產業提供身分識別、驗證與授權，如：稅籍、取得特定政府福利與服務、投票、機動車輛操作授權，以及（在某些管轄區）取得金融服務等。限定用途 ID 證明之範例，包括（但不限於）：納稅人身分識別碼、駕照、護照、選民登記卡、社會安全碼和難民身分文件。在某些情況下，尤其在沒有一般用途 ID 系統的國家，此類功能系統與憑證，也可用於提供官方身分證明。
55. 一般而言，官方身分證明是由政府、或以政府名義提供。在數位時代，除了由政府核發的傳統式數位憑證（如：電子國民身分證）之外，也開始出現新的模式，包括經政府認可之私部門提供或與私部門合作提供之數位憑證（如：丹麥的 NemID），該等憑證可作爲線上環境官方身分證明。
56. 若爲難民，則官方身分證明，亦可由經國際間認可具備此權限之國際組織提供。[74] 參見說明方塊 8。

本指引適用之數位 ID 系統為何？

57. 數位 ID 系統使用電子方式斷定並證明在各種確信等級之線上（數位）和／或現場環境之個人官方身分。
58. 本指引的重點在於端對端數位 ID 系統（即：涵蓋身分證明／註冊與

[73] 第 7 工作小組技術委員會 68，ISO 標準諮詢小組（Standard Advisory Group，SAG）。

[74] 請參閱《1951 難民地位公約》第 25 和 27 條以及《1950 聯合國難民高專署法令》。

驗證流程之系統）。數位 ID 系統可涉及不同的操作模式，並且可能仰賴眾多技術、流程與架構實體及類型。本指引所述之數位 ID 系統係指整體系統，而非系統之組成部分。

59. 數位 ID 系統並不一定要完全由數位化元素構成。有些身分證明與註冊組成要項，可以是數位化或實體（紙本）或兩者之組合，但綁定、認證、驗證和可攜性／聯合識別（如適用），必須爲數位要項。這些概念將於下一節中詳細說明。
60. 數位 ID 系統可以各種方式使用數位科技，包括但不限於：
    - 使用包含分散式帳本在內之電子資料庫，以取得、確認、儲存和／或管理身分證據；
    - 用於驗證身分以存取行動、線上和離線應用程式之數位憑證
    - 協助識別和／或驗證個人之生物特徵；以及
    - 可促進線上身分識別／確認與身分驗證之數位應用程式介面（Application Program Interfaces，APIs）、平台與協定。

數位 ID 系統的主要組成？

61. 如 NIST 數位 ID 指引所述，數位 ID 系統涉及兩個基本組成要件，加上一個選擇性的第三組成要件，如下所述。次要組成要件之管理可由不同實體負責，包括可結合政府實體與私部門實體。視所述系統而定，各管轄區和組織所使用的術語可能略有出入。各階段之詳盡說明，請參閱附錄 A：基本數位身分系統與其參與者說明。

組成要件一：身分證明與註冊（含初次綁定／認證）（必要）

62. 此組成要件說明：您是誰？並且負責收集、驗證與確認和個人相關之身分證明與資訊，建立身分帳戶（註冊），以及將個人的唯一身分綁定至由此人所擁有及管控之驗證因素。
63. 此組成要件與第 10(a) 項建議的身分識別／確認要求直接相關，也最爲接近（重疊）（參見第三節）。

圖 2. 身分證明與註冊

附註：此圖僅供參考，實際之身分證明與註冊階段順序可能有所不同，此流程之目的在於識別及確認個人身分，並將身分與驗證因素連結。關於此圖所使用之關鍵術語說明，請參見附錄 A。

64. 舉例來說，組成要件一所採取的行動可能包括：

- 收集：於現場和／或線上呈現及收集身分要件與證據（如：透過填寫線上表單、傳送自拍照、上傳護照或駕照等證件照片）。
- 驗證：以數位或實體方式檢驗，確保文件之眞實性以及資料或資訊之準確性（例如：檢查實體安全性特徵、有效期限、以及透過其他服務確認要件）。
- 刪除重複資料：確定該身分要件及證明與 ID 系統中的唯一個人相

關（例如：透過重複紀錄搜尋、生物特徵識別和／或重複資料刪除演算法）。

- 確認：連結個人與所提供之身分證據（例如：使用人臉辨識與活體偵測等生物辨識解決方案）。
- 身分帳戶註冊及綁定：建立身分帳戶並核發一個或多個與該身分帳戶連結之驗證因素（如：密碼、智慧型手機上的一次性密碼（One Time Code，OTC）產生器、PKI[75] 智慧卡、FIDO【Fast Identity Online】認證等）。此過程將啓用驗證（如下所述）。

組成要件二：驗證與身分生命週期管理（必要）

65. 驗證的目的在於回答以下問題：您是否爲經過識別與確認身分的本人？此要件會根據驗證因素之持有權與管控權，確認聲稱某身分之個人（首次開戶客戶或該身分之主張者）與經過證明及註冊之個人爲同一人
66. 個人身分的驗證因素共有三種類型（參見圖 3）：(1) 所有權因素（您所持有的某物，如：密碼金鑰）、(2) 知識因素（您所知道的事物，如：密碼）、(3) 先天因素（您與生俱來的條件，如：生物特徵）。[76]
67. 驗證，可仰賴各種類型之驗證因素與協定或流程。此類驗證因素具備不同等級之安全性，請參閱第五節關於驗證風險之探討。單一驗證因素，通常不被認定爲具備充分可信度。一般認爲採用多種類型驗證因素之驗證流程，較爲健全可靠。[77]

---

[75] 公共金鑰基礎結構（Public Key Infrastructure）。

[76] 本指引所述之驗證組成要件，並非指歐盟法律架構所規定之「嚴格用戶認證機制」（Strong Customer Authentication，SCA）。是否構成歐盟 2015/2366 指令（支付服務指令 II，Directive on Payment Services II，PSDII）所稱之有效 SCA 因素，必須根據 PSDII 和依 PSDII 所訂之嚴格用戶認證機制與安全通訊之法規技術標準（Regulatory Technical Standards on strong customer authentication and secure communication，RTS on SCA & CSC）評估，而不是依 FATF 指引斷定。

[77] 隨著數位 ID 系統演進，此一理解也變得更具細微差異。當驗證有效且保持其有效性時，驗證強度會偶爾受到評估，但並非就不同驗證因素與類型的數量進行評估，而是評估其因使用多種來源之動態數位用戶資料所達到的整體健全度，包括預期的登入管道、地理位置定位、使用頻率、使用類型、IP 位址以及生物力學矩陣行為模式。

圖 3. 常見的驗證因素

資料出處：世界銀行 ID4D

說明方塊 1. 客戶盡職調查和其他 AML/CFT 措施中，驗證所扮演的角色

- 一旦個人在數位 ID 系統的身分經過證明並註冊後，便可使用與自己身分綁定之憑證與驗證因素，向第三方「依賴方」（如：受監管實體）「主張」此身分。身分證明與註冊流程的強度，爲依賴方提供身分資訊眞實性的信任等級（如：姓名與年齡等要件正確，並且與實際個人關聯），而驗證流程則可使依賴方確信提出該憑證之個人確實爲本人，而非竊賊或冒充身分者。因此，數位 ID 系統驗證個人的能力，是系統功能性的重要一環，俾受監管實體在開立帳戶期間使用數位 ID 系統於 CDD 身分識別／確認流程。

・請注意，既有客戶之「驗證」也是持續盡職調查與帳戶存取權限授權的重要安全性措施之一。在某些情況下，受監管實體可於開戶期間，使用相同的數位 ID 憑證與驗證服務核予帳戶存取權限，但此非必要之舉。例如，許多受監管實體會核發自有憑證／驗證因素（如：用於登入線上帳戶的 PIN 和權杖），和／或將此類憑證或驗證因素連結至與手機或瀏覽器整合之終端驗證因素（如：使用 FIDO 標準）。

68. 身分生命週期管理是指爲了因應可能於身分生命週期，發生可對驗證因素之使用、安全性與可信度造成影響的事件時（如：遺失、遭竊、未經授權複製、過期、驗證因素和／或憑證廢止），所應採取的行動。

組成要件三：可攜性與互相操作性機制（選擇性）

69. 數位 ID 系統可包含能夠使身分證明具可攜性的要件。可攜式身分代表個人的數位 ID 憑證，可在不具關聯的私部門或政府實體中，用於證明官方身分以便建立新客戶關係，進而省去此類實體必須逐次取得並確認個人資料，以執行客戶身分識別／確認的麻煩。可攜性可由不同的數位 ID 架構與協定支援。歐洲的 eIDAS 規章，提供數位 ID 系統互相認可之架構。
70. 聯合識別是允許官方身分具可攜性的方式之一。聯合識別是指使用聯合架構與聲明協定，在一套連線的系統之間，傳輸身分與驗證資訊。此方式使得獨立的網路具互相操作性。英國的 GOV.UK Verify 就是聯合識別數位 ID 其中一種方式，參見說明方塊 16 。

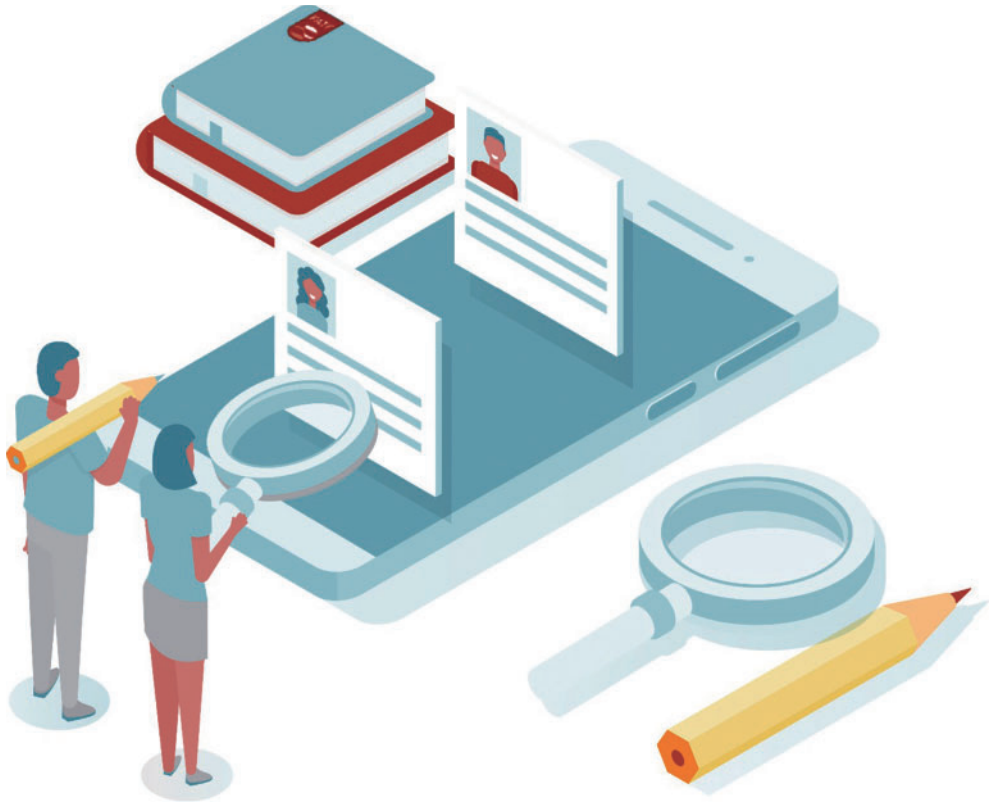
數位 ID 確信架構與技術標準

71. 數位 ID 技術、流程與架構可靠度之確信架構與技術標準，是由以下各方擬定或研擬中：
    - 各管轄區或超國家管轄區（如：歐盟、加拿大與澳洲）
    - 國際標準組織或業界特定組織，如：國際標準化組織（International Organization for Standardization，ISO）、國際電工委員會（International Electrotechnical Commission，IEC）、線上快速身

分識別（Fast Identity Online ，FIDO）聯盟、OpenID Foundation（OIDF）、國際電信聯盟（International Telecommunications Union，ITU）和全球移動通訊系統（Global System for Mobile Communications，GSMA）。

72. 關於上述組織之更深入整理介紹，請參見附錄 D：數位 ID 確信架構與技術標準訂立組織。
73. 就目前而言，各管轄區所擬定之數位 ID 確信架構與標準所使用的確信等級級次和／或名稱各有不同，但基本上大致相同。各國目前正互相對應彼此數位 ID 技術標準，以解決任何重大之差異。ISO 與國際 IEC 在 2018 年共同發布了自然人身分證明與註冊的國際標準（ISO/IEC 29003:2018）。ISO 目前正在修改其實體驗證確信架構（ISO/IEC 29115:2013），並說明如何就身分相關風險，運用其風險管理方針（ISO 3100:2018）。此外，ISO 也正努力更新、對應以及同步化所有其他 ISO 標準，以制定全方位的國際化數位 ID 確信架構。
74. 有鑒於不斷演進的標準，本指引主要參考 NIST 數位 ID 方針和 eIDAS 架構。AML/CFT 權責機關應與數位 ID 與網路安全性權責機關和其他相關機構單位密切合作，識別適用之數位 ID 確信架構與標準。
75. 隨著數位 ID 技術、架構與流程不斷演進，數位 ID 系統本身的確信架構與技術標準也需要與時俱進，否則很可能趕不上數位 ID 系統的進步速度。政府和私部門應盡快密切掌握可提供更健全身分證明或驗證之新興數位 ID 技術／流程，並將架構與標準視爲實用的評估工具，而不是使用既有的更高確信等級制定上限。

第三節：FATF 客戶盡職調查標準



76. 閱讀本節前，須對數位 ID 系統的運作方式有基礎的瞭解。建議讀者回顧第二節與附錄 A，瞭解一般數位 ID 系統基本步驟的簡要說明，以便就本節對第 10 項建議所探討之內容具備基礎瞭解，尤其是在「可靠、獨立」準則方面。
77. 根據第 10 項建議，各國必須要求受監管實體執行客戶盡職調查（CDD）。以下討論說明在數位 ID 系統的背景環境下如何適用第 10(a) 項建議。受監管實體必須根據第 10 項建議和第 1 項建議中的注釋，使用風險基礎方法（RBA），確認 CDD 措施之涵蓋範圍。此外也簡要說明可靠的數位 ID 系統，如何支援根據第 10 (d) 項建議應執行的其他 AML/CFT 要求。

客戶身分識別／確認要求（首次開戶）

78. 與客戶建立業務往來關係時（即首次開戶），受監管實體必須使用可靠、獨立之原始文件、資料或資訊（第 10 項建議與第 10(a) 項建議），識別及確認客戶身分。

紙本或數位形式身分證明與流程

79. 第 10 項建議爲技術中立，第 10(a) 項建議允許金融機構使用「文件」和「資訊或資料」執行識別與確認客戶身分，第 10(a) 項建議並不限制所取得之身分證據－「原始文件、資訊或資料」－之形式，紙本／實體或數位均可被接受。
80. 雖然第 10(a) 項建議確實要求金融機構將已確認之客戶身分，透過若干「可靠」方式與個人連結，但 FATF 標準中並未明訂應如何在首次開戶的身分識別／確認過程中，將身分經過確認之客戶連結至唯一實際個人。因此，第 10 項建議並不構成使用數位 ID 系統執行該程序之限制。關於此一問題，FATF 標準不提出任何意見，由各管轄區依其國家法律架構決定執行 CDD 時之官方身分證明。

「可靠、獨立」的身分證據

81. 決定數位 ID 系統如何用於客戶身分識別／確認的關鍵，在於瞭解第 10 項建議對於「使用可靠、獨立原始文件、資料或資訊」這項要求，於數位環境中所代表的意義。數位 ID 確信架構與標準是指描述系統健全度之「可確信程度」。因此，確信等級在確認特定數位 ID 系統是否可發揮基於 AML/CFT 目的之「可靠、獨立」，是非常實用的評判標準。
82. 以下討論探討 FATF 現行「可靠、獨立」要求之發展，以進一步說明其根本意涵與目標。
83. 在原版的 FATF 40 項建議（1990 年 7 月）中，第 12 項建議要求受監

管實體「根據官方或其他可靠之身分識別文件」識別客戶身分。[78] 該建議於 1996 年 6 月和 2003 年 6 月的修訂版本中仍沿用此用語，直到 2012 年 2 月才修正爲現行版本。FATF 在 2012 年新增了「身分確認」要求，並要求身分證據除了「可靠」之外，還必須滿足「獨立」之特性要求。同時，2012 年的修訂版也針對可用於識別／確認客戶身分之身分證據類型，採取更具彈性、更廣泛的做法，除原始文件外，亦接受數位資料或資訊。此修訂版亦捨棄先前建議對於「官方身分識別文件」之明確參照。

84. 在數位 ID 背景環境下，數位「原始文件、資料或資訊」必須「可靠、獨立」之要求，代表用於執行 CDD 之數位 ID 系統須採用可提供適當信賴等級之科技、適當管理、流程與程序，方可產生準確之結果。這表示系統設有可防止第四節所述風險之抵減措施。

CDD 之風險基礎方法

85. 第 10 項建議要求受監管實體使用風險基礎方法（RBA），決定欲實施之 CDD 措施之強度，包括客戶身分識別／確認。根據第 10 項建議和其注釋，受監管實體必須識別、評估並採取有效之行動，以抵減其 ML/TF 風險（針對客戶、國家或地理區域；以及產品、服務、交易或支付管道）。如遇較高風險需採取強化的措施，若確定爲低風險狀況，則可採取簡化措施。FATF 已發布指引，說明管轄區／受監管實體可如何使用風險基礎方法實施 CDD 措施，以促進普惠金融目標。[79]

86. 第五節將詳細探討，根據第 1 項和第 10 項建議以及其注釋，受監管實體應視 ML/TF 風險類型和等級，採取相應的 CDD 措施。第 1 項建議之注釋強調，受監管實體在決定整體風險等級以及欲採取的適當風險管控等級之前，應考量所有相關風險因素。除了第 10 項建議與其

[78] 原版 FATF 40 項建議（1990 年 7 月）規定金融機構必須識別客戶身分，以強化此類機構在打擊非法毒品交易不法所得之洗錢（ML）行為所扮演的角色。第 12 項建議（1990 年）更在相關方面規定（新增重點項目；引自原文）：金融機構不應保有匿名帳戶或明顯虛設之帳戶；而應（依法律、規範、監管機關和金融機構訂定的監管合約或金融機構之間訂定的自我監管合約），以官方或其他可靠之身分識別文件，作為身分識別之依據，並且不論在臨時或一般情況下，在建立業務關係或執行交易（尤其是開戶或辦理存摺、進行信託交易、租用保險［按原文］箱、執行大額交易）時，均應保存識別客戶身分之資料。

[79] FATF (2013-2017)，防制洗錢與資恐措施及普惠金融－客戶盡職調查補充條款，FATF，巴黎 www.fatfgafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

注釋外，第 1 項建議之注釋具體規定受監管實體可視各種風險因子的類型和風險等級，採取差異化做法（如：在特定情況下，可針對接納客戶措施採取一般 CDD，但對持續監控採取強度較強的 CDD，反之亦然）。

非面對面業務關係與交易

87.FATF 使用面對面和非面對面對業務關係（包括首次開戶）和交易進行分類，根據 FATF 所定義，面對面互動是指由本人親自執行的，代表互動／交易相關方均處於同一實體位置，並透過實體互動執行活動。非面對面互動是指遠端發生的互動，表示相關當事方未處於同一實體位置，並透過數位或其他非實體存在之方式（如：郵件或電話）執行活動。[80]

88. 第 10 項建議之注釋將「非面對面商務關係或交易」列爲執行 CDD 時的潛在較高風險範例。根據其文字說明，該注釋並不要求相關機關和受監管實體一定要將非面對面業務關係或金融交易列爲具較高洗錢與資恐風險之活動，而是認爲非面對面業務關係具較高潛在洗錢與資恐風險之例。

89. 隨著數位 ID 技術、架構、流程不斷演進，加上以共識爲基礎之開放來源數位 ID 技術標準興起，因此有必要說明仰賴具適當風險管控措施之可靠、獨立數位 ID 系統所執行的非面對面客戶身分識別與交易，可被視爲具一般等級風險，但若運用更高確信等級和／或適當 ML/TF 風險控制措施（如：產品功能性限制和 第 10 項建議注釋和 FATF 普惠金融準則所討論之措施）時，甚至可被視爲低風險（可參閱本指引稍後關於〈普惠金融、遠端身分證明和註冊之特殊考量〉之說明）。

業務關係之持續盡職調查

90. 此外，根據第 10(d) 項建議，受監管實體必須「在該業務關係存續期間，對該關係執行持續盡職調查與交易審查，以確保所執行之交易與該機構對該客戶、其業務與風險概況之瞭解一致，包括必要時，瞭解其資金來源。」

[80] 視各國法規而定，面對面和非面對面互動之定義可能有所不同，例如，有些國家認為視訊身分識別屬於面對面互動。

91. 如第二節中的解說及附錄 A 之詳細說明，驗證是指建立某人即爲身分經過證明且爲經核發相關憑證之本人之確信度。對於在帳戶授權過程中，使用數位 ID 系統驗證既有客戶身分之受監管實體，建議使用由驗證和相關資訊所產生的資料，[81] 以利後續之持盡職調查與交易監控。該等資訊傳統上係基於使受監管實體免於詐騙而取得，然而，數位金融系統普及速度加快，使用數位 ID 驗證授權帳戶存取的依賴性也隨之提高，因此使用數位 ID 系統驗證也有助於 AML/CFT。

92. 針對受監管實體，首次開戶客戶之持續驗證，可提供合理的風險基礎確信度（即：可信賴程度），證明今日聲稱該身分之個人，與之前開戶或啓用其他金融服務者爲同一人，並且確實爲首次開戶時，經過「可靠、獨立」身分識別與確認之個人。客戶身分之持續數位驗證，會將該客戶與其金融活動連結。因此有助於加強執行有意義持續盡職調查與交易監控之能力，進而滿足第 10(d) 項建議之要求。

依賴第三方之要求

93. 本節說明基於 AML/CFT 目的之受監管實體，可 (1) 在數位 ID 背景條件下，仰賴由另一受監管實體執行客戶身分識別／確認（在第 17 項建議範疇內），以及 (2) 可作爲另一受監管實體代理人或受另一監管實體之委託執行客戶身分識別／確認（在第 17 項建議範疇以外）。

94. 根據第 17 項建議，若滿足以下條件，各國可允許受監管實體於首次開戶時，[82] 仰賴第三方執行客戶身分識別／確認：[83]

- 第三方亦必須爲遵循第 10 項建議 CDD 要求之受監管實體，並且受到法律遵循之管理、監理或監督。
- 受監管實體應：
  - ○ 立即取得關於客戶身分識別／確認之必要資訊；
  - ○ 採取充分步驟，確保身分識別資料和其他與第 10(a) 項建議要求

[81] 驗證是授權帳戶存取的過程之一。受監管實體亦可收集其他補充資料（如：地理位置定位、IP 位址等），供授權決策使用。

[82] 第 22 項建議規定第 17 項建議之依賴性要求，適用於 DNFBP。

[83] 第 17 項建議允許依賴第三方執行第 10 項建議 CDD 措施 (a)-(c)；未允許依賴第三方執行業務關係之持續盡職調查。本指引僅探討與第 10(a) 項身分識別／確認相關之第 17 項建議。

相關之文件複本，在經要求時，將可由第三方即時提出；

○ 確保第三方受到管理、監理或監督，且訂有相關措施，以符合第 10 與 11 項建議關於 CDD 與紀錄保存之要求。

○ 在決定該國有哪些第三方符合上述條件時，應考量國家風險資訊。

95. 在允許此類依賴性的情況下，CDD 措施的最終責任，仍舊落在依賴第三方之受監管實體。

數位 ID 環境下的依賴第三方（受監管實體亦為數位 ID 服務供應商）

96. 若該國允許受監管實體依賴滿足上述條件之另一受監管實體，於首次開戶時使用數位 ID 系統執行客戶身分識別／確認，該第三方之數位 ID 系統，必須可讓依賴之受監管實體：

・立即取得關於客戶身分之必要資訊（若可適用，包括確信（可信度）等級）。例如，數位 ID 系統可讓潛在客戶向依賴第三方之受監管實體主張身分，並可由該第三方驗證個人身分及提供如個人姓名、出生日期、國家提供之唯一身分證號碼、或其他證明官方身分之必要要件等資訊，以便在該國建立業務關係。

・採取充分步驟，確保第三方在經要求的情況下，可立即提供或供受監理實體以其他適當方法取得與第 10(a) 項建議相關之身分證據（文件、資料及其他相關資訊）複本。例如，依賴方實體可採取適當步驟，以便 (1) 確保在身分證明與註冊過程中，第三方爲已識別身分之個人建立數位 ID 帳戶，其中包含充分之身分要件證據和其他身分資料與資訊，並且 (2) 第三方之驗證流程可使其在經要求的情況下，向依賴方即時提供該資訊。

受監管實體作為第 17 項建議範疇以外之數位 ID 服務供應商

97. 自行開發數位 ID 系統之受監管實體，可透過作爲其他受監管實體之代理或委外實體，尋求成爲數位 ID 服務供應商的機會。取得許可後，則可接受委託進行首次開戶之客戶身分識別／確認與客戶驗證。在此情況下，不適用第 17 項建議所述之依賴第三方，因爲第 17 項建議並未涵蓋委外或代理關係。

98. 如同其他作爲代理或委外實體的數位 ID 服務供應商，作爲數位 ID 服務供應商之受監管實體可代表委託之受監管實體，使用其數位 ID 系統執行客戶身分識別／確認（與驗證）。此外，如同其他數位 ID 服務供應商，此類受監管實體亦可在遵循該管轄區政府審核與認證架構之情況下，尋求認證，抑或尋求著名私部門認證組織之審核與認證。
99. 原則上，無論是任一情況，仍將由受委託之實體，使用由數位 ID 服務供應商所提供之數位 ID 系統，執行有效之客戶身分識別／確認及有效驗證，並且需要將第五節所述之風險基礎方法納入使用數位 ID 系統進行客戶身分識別／確認與驗證。

第四節：使用數位 ID 系統於 AML/CFT 法遵與相關議題之效益與風險

100. 本節說明數位 ID 系統可爲受監管實體、其客戶及政府所提供之若干效益，並提出需要加以識別、瞭解、監控、以及充分管理或抵減之潛在風險。這些效益與風險與實施 AML/CFT 保護措施和普惠金融相關。
101. 本節旨在提醒利害關係者，瞭解數位 ID 技術特有潛在風險，以便透過套用第五節所述之 RBA 加以避免或有效管理。以下關於風險討論之用意並非不鼓勵使用可靠獨立－即符合適當確信等級（即政府協議與技術標準）－之數位 ID 系統，而是探討如何以適當方式解決潛在風險；也不表示使用數位 ID 系統，尤其用於客戶身分識別／確認，就一定比傳統紙本做法更容易遭到濫用。
102. 本節亦指出許多數位 ID 系統所呈現的更廣泛挑戰。回應這些挑戰通常不直接落在 AML/CFT 主管機關的工作範疇內，但這些挑戰可能會對 AML/CFT 工作帶來間接影響。
103. 本節就此類風險與挑戰提供一般概述，而數位 ID 確信架構與標準則提供數位 ID 系統風險管控措施之評估架構。建議各國審查現行可用於解決廣泛風險之標準（除技術相關標準外，另包括其他組織與治理標準），及應如何抵減該等風險。

數位 ID 系統的潛在效益

強化 CDD

104. 數位 ID 系統可在提供金融服務時，幫助改善個人身分識別可靠度、安全性、隱私權、便利性和效率，因而有益於客戶、受監管實體以及金融產業的完整性。如下文所討論，可靠獨立之數位 ID 系統可提供重大效益，改善首次開戶之客戶身分識別／確認，並驗證客戶身分眞實性，以授權帳戶存取。此外，準確的客戶身分識別也有利於其他 CDD 措施，包括就業務關係和交易監控進行有效之持續盡職調查。

將人為控制措施的缺點降到最低

105. 傳統紙本式客戶身分識別／確認方式主要仰賴人爲管制措施，如：比對官方身分文件的照片與開戶本人的樣貌，並判斷身分文件之眞僞。然而，第一線人員可能缺乏可靠識別僞造、經過改造或遭竊文

件所需的工具、技術、訓練、相關技能與經驗。

106. 使用可靠且獨立之數位 ID 系統，可減少識別與確認個人身分之人爲疏失的可能性。

- 首先，即便數位 ID 系統的身分證明組成要件是由本人執行[84] 並且仰賴人爲判斷，該流程也通常會由可取得用於偵測僞造與遭竊 ID 文件的先進技術工具之專業人員執行。例如，遠端身分證明－至少須具備較高之確信等級－一般採用日益精密且有效之數位 ID 技術，以確認紙本身分證據之眞實性，並驗證其他有助可靠證明個人身分之資料與資訊。[85]
- 其次，數位 ID 系統之驗證組成要件可大幅省去確認該客戶爲其主張個體之主觀人爲判斷作業。配備多重認證因素與安全流程之數位 ID 系統，可持續可靠地確認尋求開戶或存取帳戶之個人，與原始核發身分憑證之個人爲同一人。

提升客戶體驗並節省成本

107. 可靠獨立的數位 ID 系統也可爲首次開戶的潛在客戶及欲存取帳戶的客戶，提供更有效及便民的措施。客戶接受度與便利性是完成申請與交易，進而留住客戶的關鍵因素。爲客戶提供便捷使用性，加上爲受監管實體提供的潛在效率提升，均有助減少首次開戶的成本。一份報告指出，使用數位 ID 系統之受監管實體，其客戶首次開戶成本最多可減少 90%，而且原本要花費數天或數週的時間進行身分識別／確認以及其他 CDD 流程，現在只要幾分鐘即能完成。[86] 這些省下的成本可讓受監管實體將資源分配給其他 AML/CFT 法遵部門，還可透過減少首次開戶成本促進普惠金融，使被排除或無法取得周全服務之人取得金融服務。

[84] 如第二節及附錄 A 所述，在數位 ID 系統中，身分證明是可以由本人親自進行的要素（即不需要一定透過遠端執行，才可視為數位 ID 系統）。

[85] 就目前而言，安全性功能（如僅可由紫外線（UV）光線讀取，或者為該文件實體構成元素之一，如：安全性縫法、蝕刻或穿過好幾頁的打孔）可能較難或無法透過遠端方式驗證，但大多數身分文件，其健全之安全性功能均經由遠端有效核實。

[86] McKinsey Global Institute (2019)， 數 位 身 分 識 別，www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx。

交易監控

108. 如上述，針對持續帳戶存取授權所使用之健全客戶 ID 數位驗證，可幫助受監管實體確認當日存取帳戶並執行交易之個人，與先前存取帳戶者爲同一人，而且即持有該帳戶之已識別／確認客戶，故可促進身分識別以及申報可疑交易。此外，視操作模式和使用者同意書和資料保護／隱私權法等相關因素而定，授權帳戶存取之數位 ID 驗證可使受監管實體掌握額外資訊，如：地理位置定位、IP 位址或用於執行交易的數位裝置身分。該等資訊有助於受監管實體對客戶行爲有更詳盡的瞭解，並在其金融交易疑似出現異常或可疑情況時作爲判斷的基礎，並且或可協助執法單位調查犯罪。例如，由受監管實體根據當地法規（包括資料保護和隱私權規定）的各種方式及管道（包括網際網路和行動電話）取得之補充說明資料，可幫助判斷帳戶管理使用者、該人名下是否有多個使用中的帳戶，以及使用這些帳戶進行金融交易的相關個人與實體關係。

普惠金融

109. 隨著金融服務的迅速數位化，可靠獨立數位 ID 系統對於促進惠普金融的重要性也與日俱增，對於數位 ID 系統和數位金融服務已成爲普惠金融主要推手的開發中國家而言，[87] 更是毋庸置疑。[88] 數位 ID 確信架構與標準的發展較具彈性，並以結果爲基礎，可使得缺乏護照與傳統駕照等官方身分證明文件，而被金融服務排除在外的族群，能以較低的身分確信等級（僅要求較不嚴謹的身分證據與確認）取得數位 ID，並藉此在適度低風險情況下取得金融服務。確信架構與標準也使得金融排除個體能夠透過使用替代身分證據（如：以「受信任推薦人」擔任申請人之擔保人，作爲身分證據的形式之一）取得數位 ID。此外，數位 ID 系統亦可觸及偏鄉地區之金融排除人口，就客戶身分識別／確認，提供更安全的非面對面身分證明／註冊。這

[87] 在 2017 年的全球普惠金融指數調查中（Global Findex Survey），26% 低收入國家中的無銀行帳戶個人指出，缺乏官方身分文件是取得金融服務的主要障礙之一。

[88] FATF (2013-2017)，防制洗錢與資恐措施及普惠金融－客戶盡職調查補充條款，FATF，巴黎 www.fatfgafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html.

些議題將於本指引之「普惠金融特殊考量」小節，更進一步之探討。

110. 在開發中國家，包括社會福利轉帳（如：條件式現金轉帳、兒童撫養費用及學生津貼）、政府薪資與退休金、以及退稅等政府對個人（Government-to-Person，G2P）之付款，均和商業活動和零售消費者付款一樣，已大幅數位化。在人道救援方面，救命援助也逐漸透過數位方式發放現金援助。上述所有活動均需要交易帳戶之存取，而此存取可透過數位 ID 系統之使用提升效率。

111. 使用可靠獨立之數位 ID 系統可減少 CDD 成本，並讓更多無法取得服務或無法取得周全服務之個人，使用受監管的金融服務（參見說明方塊 4 關於印度 Aadhaar 的說明，以及說明方塊 5 關於秘魯全國身分與公民地位註冊處的說明）。如此可促進普惠金融，並促進達到 AML/CFT 政策目標及提升效能。

數位 ID 系統的風險與挑戰

112. 本指引著眼於執行特定 CDD 要素之數位 ID 系統，而非探討傳統紙本身分系統之使用。以下所討論之風險，不代表數位 ID 系統之風險高於效益，也並非意味數位 ID 系統相較於傳統紙本身分證明系統而言，更具風險性。

113. 如同任何 ID 系統，數位 ID 系統的可靠度取決於用於證明身分、認證與驗證以及持續身分管理之文件、流程、技術與安全性措施的強度。舉例來說，無論是紙本或數位 ID 系統，可靠度均可能因身分竊取而減弱，而原始文件也可輕易被僞造或竄改。某些類型的詐騙較不容易發生在本人或需要人爲介入的過程，包括較可能透過遠端發動的「大規模詐騙攻擊」。雖然數位 ID 系統設有安全性功能，如：安全性驗證，可減輕使用紙本系統所產生的若干風險，但同時也會提高某些風險，如：資料遺失、資料損毀或因未經授權存取導致的資料濫用。

114. 數位 ID 系統構成各種技術挑戰與風險，因爲此類系統通常需要在公開的通訊網路上（網際網路），進行個人身分證明與驗證。因此，數位 ID 系統所採用的流程與技術，會在相關當事方（IDSP、客戶與依賴方）之間，出現許多遭受網路攻擊之機會。若未審愼考量相關

風險因子與運用適當的技術架構防護措施，加上缺乏有效治理與解決此類風險之當責措施，則犯罪者、洗錢者、恐怖分子和其他不肖份子，均可濫用數位 ID 系統僞造身分或利用數位 ID 系統（入侵系統或假冒）連結至合法身分之驗證因素。

115. 數位 ID 確信架構與標準，可作爲識別與評估上述若干風險的關鍵工具，並可透過對數位 ID 每一個組成要件，提供適當可信度之數位 ID 技術與流程管控風險。[89] 以下風險討論適用於就數位 ID 確信架構與標準所述之風險管理架構而言，缺乏充分可靠度之數位 ID 系統。此外亦廣泛地探討數位環境中，會對數位 ID 系統執行 CDD 的完整性或可用性造成影響的連線能力、網路安全性和隱私權挑戰。

116. 以下討論涵蓋身分證明／註冊風險與驗證風險。身分證明階段的風險可能產生「假的」數位 ID（即透過蓄意惡行在虛假的前提下取得），並可用於促進非法活動。這些風險可透過適當的身分確信等級加以管控。身分證明風險與驗證風險不同，後者是合法核發的數位 ID 遭到外洩，而且其憑證或驗證因素是由未經授權之個人控制。此類風險可透過適當的驗證確信等級加以管控。

身分證明與註冊風險

117. 註冊流程的威脅有兩大來源：(1) 導致個人可識別資訊（Personal Identifiable Information，PII）外洩以及僞造身分證據之網路攻擊與安全漏洞；此類事件可能透過竊取眞實個人身分（冒名）或創造一個合成 ID 而得逞，以及 (2) 因 IDSP 遭受侵害或 IDSP 本身處理不當，或者更廣泛的數位 ID 基礎架構受到侵害。本節著眼於第一類威脅，因爲 IDSP 遭受侵害／處理不當、網路安全性和更廣泛的基礎架構威脅，可直接由數位 ID 確信架構與標準以及傳統電腦安全性控制（如：入侵保護、紀錄保存、獨立稽核）所建構之更廣泛治理／組織要求改善，故不在本指引討論範疇內。

冒名風險與合成 ID（涉及網路攻擊、資料保護和／或安全性漏洞）

118. 在某些情況下，因在數位 ID 系統出示造假身分證據（遭竊或僞造）

[89] 關於在每個基本階段用於評估與管控風險的身分確信等級（Identity Assurance Levels，IAL）、驗證確信等級（Authentication Assurance Levels，AAL）、聯合識別確信等級（Federation Assurance Levels，FAL）之詳細討論，請參閱附錄 E。

所造成之風險，會以更大的規模呈現。[90] 冒名是指一人假裝具備另一眞實個人之身分，這可能只要使用長相相似者的失竊身分文件就能達成，但也可能結合僞造或捏造之身分證據（如：將個人正版護照上的照片，換成冒名者的照片）。合成身分是由犯罪者透過結合眞實（通常透過竊取取得）和造假資訊，建立一個新的（合成）身分，此身分可用於開立詐騙帳戶並進行詐騙購買。有別於冒名，犯罪者會假裝成實際世界不存在的某人，而不是假冒既有身分者。舉例來說，犯罪集團會從事身分竊盜，然後產生大量合成數位 ID，這些合成 ID 有部分是以實際個人的身分要件、和其他透過線上交易或入侵網際網路資料庫竊取的資料爲基礎，有部分則是完全造假的資訊。合成 ID 也可用於取得信用卡或線上貸款並提取資金，並在達成目的後立即將帳戶棄用。數位 ID 專家指出，合成身分之使用對美國數位 ID 系統的身分證明與註冊階段，帶來最大程度的風險。[91]

119. 下表針對上述風險類型所舉之例，並提出國家標準暨技術研究院（National Institute of Standards and Technology，NIST）指引中，可用於管控身分證明與註冊流程威脅之若干策略，僅供參考。

表 1. NIST －身分證明／註冊風險管控策略

風險類型	說明	可行的風險管控策略
造假的身分證明證據	申請者透過使用僞造的駕照主張不實身分。	IDSP（CSP）驗證出示證據之實體安全性特徵。 IDSP（CSP）比對核發單位或其他官方來源，驗證證據中的個人詳細資訊。
僞冒使用他人身分	申請者使用連結至不同個人之護照	IDSP（CSP）就核發單位或其他官方來源取得之資訊進行比對，確認申請者之身分證據與生物特徵。

資料出處： NIST 800-63A

[90] 在網際網路上搜尋「造假 ID」，便會顯示數以百計專門僞造駕照、護照、出生證明、移民文件以及其他官方文件的網站，而且造假文件的逼真程度與合法身分文件不相上下。

[91] FATF 專題小組與數位 ID 專家會議，2019 年 9 月。

驗證與身分生命週期管理風險

120. 與各種驗證因素類型與數量相關的弱點，可能會增加無法辨識及無預警風險，使得不肖份子藉由向依賴方主張某一個人（如：客戶）之合法身分開立帳戶，或在未經授權情況下取得產品、服務與資料。

121. 舉例來說，此類弱點可能包括：

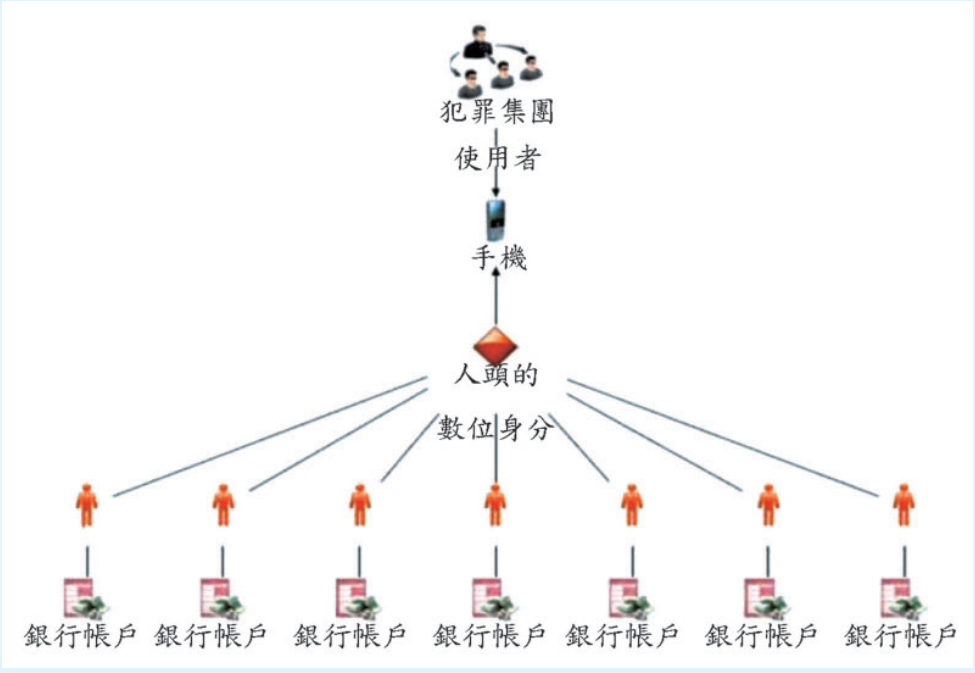
- 帳密填充（又稱洩漏個資重送或列表清除）：是一種將竊取的帳戶憑證（通常來自資料洩漏）試圖登入在其他系統上的網路攻擊類型。若受害者使用同一組密碼（在資料洩漏中遭竊的）存取其他帳戶，則此類型帳戶便可成功入侵。
- 釣魚詐騙：是指透過社交工程攻擊（如：詐騙電子郵件、電話、簡訊或網站），向不知情的受害者索取憑證的詐騙行爲。例如，犯罪者試圖誘騙受害者對看似可信任之來源，提供姓名、密碼、官方身分證號碼或憑證。
- 中間人或帳密攔截：試圖達到和釣魚詐騙相同的目的，並可作爲執行釣魚詐騙的工具，但係透過攔截受害者與服務供應商之間的通訊達成目的。
- PIN 碼擷取與重送：指運用鍵盤側錄擷取 PC 鍵盤所輸入的 PIN 碼，然後在使用者不知情的情況下，使用擷取的 PIN 碼，在智慧卡插入讀卡器時存取服務。

122. 大多數驗證漏洞會在身分持有者不知情的情況下發生，但濫用則可能涉及用戶或 IDSP 之蓄意參與。例如，共享密鑰驗證（如：密碼）可能遭不肖份子竊取利用，但也可能由身分憑證持有者基於非法用途而蓄意分享出去。

123. 舉例來說，犯罪組織可向個人購買數位 ID 憑證，藉此存取該個人於受監管實體持有之帳戶，使得這些人成爲犯罪組織的數位錢騾（digital mules）。這些個人可以是已持有帳戶者，也可是同意以售出之身分憑證開立連結帳戶之人（請參閱以下個案研究）。

說明方塊 2. 空頭保證人之數位 ID 不當使用

瑞典指出因犯罪者有系統地利用人頭的數位 ID 對清洗犯罪收益，提高了數位 ID 的 ML/TF 風險。雖然此類風險亦可能存在於面對面交易，但以下就此類攻擊如何發生於數位環境進行說明。犯罪者特別傾向使用可提供即時交易的付款服務業者所提供之服務，因爲此類服務搭配遭到不當使用的數位 ID 之後，可迅速在不同帳號之間轉帳。



當犯罪集團想要透過不當使用之數位 ID 進行洗錢時，需要先由人頭開立銀行帳戶。人頭的角色就是開立銀行帳戶、取得數位 ID 和安全密碼，然後將個人憑證交給犯罪集團換取現金。多個數位身分可在一支手機、或一部平板電腦上使用（如上圖所示）。之後便由犯罪集團接管開立之銀行帳戶。務必注意一點，受到犯罪集團濫用的數位 ID，有絕大多數都是以合法的身分證據（即身分證明）爲基礎所核發。

資料出處：瑞典

124. 以下就與 AML/CFT 行動特別相關之特定類型驗證因素／流程，說明有關的若干主要已知風險。

125. 多因素驗證（Multi-Factor Authentication，MFA）之弱點：密碼—照理應爲「共享密鑰」的知識驗證因素－很容易受到暴力破解攻擊、網路釣魚攻擊以及大規模線上資料外洩，而且非常容易攻破。在資料洩漏的案例中，超過 81% 以上爲密碼遭竊、密碼強度不足、或僅使用預設密碼。[92] 如傳送一次性簡訊密碼至用戶手機的多因素驗證（MFA）解決方案，可爲密碼提供額外的安全性保護，但也可能受到網路釣魚和其他攻擊。防網路釣魚的驗證因素，至少有一項因素使用公開金鑰加密 [93]（如：使用 PKI 憑證或 FIDO 標準建立之驗證因素），可幫助防範此類漏洞。

126. 生物特徵驗證因素：比起傳統驗證因素，如指紋與虹膜掃描等生物物理驗證因素較難以攻破，而且也越來越普及。大多數智慧型手機均內建指紋掃描器；某些智慧型手機內建虹膜掃描器；許多個人電腦系統和高階智慧型手機，也均內建人臉辨識功能。

127. 生物特徵可透過駭入中央資料庫進行大規模竊取，[94] 也可透過拍攝高解析度影像（照片）取得、自個人觸碰過的物品（如：隱約指紋）採集，或透過高解析度影像（如：虹膜特徵）擷取，達到瞞天過海的目的。然而，目前這些類型的攻擊在執行上有一定難度，而且／或需要大量資源，因此不會大規模展開。例如，需要終端匹配的生物特徵驗證因素，便無法以詐騙方式大規模使用，因爲此類驗證因素要求本人親自存取該客戶裝置。

128. 用於驗證用途時，生物特徵還有許多其他可能導致可靠性疑慮的弱點，也因此使得某些技術標準限制使用此類驗證因素（相對於身分

[92] Verizon 2018 年資料外洩調查報告（Data Breach Investigation Report，DBIR），資料內容連結：https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf。

[93] 在公開金鑰加密情況下，會為一實體－個人、系統或裝置－產生一對金鑰，並由該實體嚴加保管私密金鑰，並可任意將公開金鑰發布給其他實體。任何持有該公開金鑰者，均可使用該金鑰對訊息進行加密，以傳送至知道唯有自己能夠開啟該訊息之私密金鑰持有者。

[94] 在 2015 年美國人事管理局（Office of Personnel Management，OPM）所遭遇的駭客攻擊中，有 560 萬筆指紋影像遭竊。

證明）。[95] 指紋可能會無法讀取或讀取錯誤。人臉辨識因素可能會因爲不同情緒所呈現的臉部表情、髮色或彩妝顏色改變、以及燈光條件變化，而影響可靠度。由於資料蒐集不完整，深色膚色以及特定種族特徵者之人臉辨識較不可靠，儘管這種情況正在改善。相對於以知識或擁有權爲基礎之驗證因素，遭竊的生物辨識驗證因素難以撤銷或更換。[96]

129. 身分生命週期風險：身分生命週期與存取管理欠妥，可能會在蓄意或在無形之中，導致驗證因素喪失完整性，並使得未經授權人士得以存取並濫用客戶帳戶，使得保護金融系統免於濫用的客戶身分識別／確認與持續盡職調查和交易監控機制無法達到其目的。

130. 未知風險：數位 ID 系統不斷發展演進，在許多情況下，技術設計的改變會帶來運作的改良，但同時也帶來未知的弱點，而這些弱點要等到被不肖份子利用之後，才會知道數位 ID 系統是如何被侵害的。

存取身分資訊以利持續盡職調查和交易監控之潛在阻礙

131. 數位 ID 環境之驗證，可用於持續 CDD 和交易監控。當受監管實體採用第三方數位 ID 系統，而且本身未自行收集交易模式、地點、裝置存取等資訊時，可能無法基於確認交易之執行是否與機構對該名客戶之認知、其業務與風險概況（包括於必要時，掌握其資金來源）相符之目的，取得分析客戶行爲與交易模式所需之必要資訊。基於反詐騙目的收集此類資訊時，亦有助於 AML/CFT 用途。受監管實體可能會考慮取得其帳戶存取驗證資料之存取權限（或第三方對其帳戶存取驗證資料之分析），以利於偵測數位 ID 系統是否被不當使用，其中包括數位 ID 資料外洩、遭竊或遭售。此資訊可用於識別及決定是否要申報可疑交易活動。聯合識別身分模式的重要效益之一，在於身分詐騙偵測可在身分供應者和依賴方合作架構上共用。

[95] 請參閱 NIST 800-63-3, NIST 800-63 (b) 和附錄 E。

[96] 雖然有方法可撤銷生物特徵憑證，但就目前而言，此類方法之可用性有限，而且用於測試之技術標準也仍在研發當中。

數位 ID 系統可對 AML/CFT 行動造成衝擊之更廣泛議題

連線能力問題

132. 缺乏可靠的基礎架構，可能會破壞管轄區或特定地理區域的數位 ID 系統，並持續一段時間。然而，數位 ID 系統可設計爲用於同時支援離線與線上交易，以便確保無論系統是否可存取網際網路或行動網路，均可維持正常運作。受監管實體在決定是否要使用數位 ID 進行 CDD 時，應將應變能力納入考量。

官方身分之國內架構

133. 就數位 ID 系統仰賴官方身分文件進行身分證明的程度看來，紙本身分證據可靠度所存在的弱點，會對數位 ID 系統所構成的風險帶來骨牌效應。純紙本身分證明方法的「可靠度與獨立性」，可能會因身分竊取和常見的官方身分文件僞造而大受影響，包括官方身分文件缺乏可防篡改或防僞造之先進防盜功能，或在缺乏充分身分證明的情況下核發該文件。自線上資料庫竊取身分資料，對於數位 ID 系統和紙本身分證明所構成的風險十分相似。

134. 非金融產業 CDD 用途之有限或特定用途之數位 ID，可能無法因應其他狀況之用途需求，或者用途有限，受監管實體可能需要付出更高的成本，或該數位 ID 經證實過後確認無法作爲 CDD 用途之用（請參閱附錄 II 說明方塊 7 之範例）。

資料保護和隱私權問題

135. 數位 ID 涉及個人資料（PII）之收集與處理，包括生物特徵。重要的是，數位 ID 的確信架構與標準可能基於管轄區和／或國際標準組織制定之個別標準而包含了資料保護與隱私（Data Protection and Privacy，DPP）之要求。此外，正在開發的以技術爲基礎的創新解決方案（如：去中心化的數位身分），使個人對於與他人共享之 PII 有較佳的管控能力，以及進一步解決隱私權和資料保護相關問題。

136. 政府肩負在管轄區建立 DPP 制度的重責大任。這些用於保護資料機密性、準確性與完整性的要求，一般適用於數位 ID 服務業者，如要求業者執行資料保護衝擊評估（Data-Protection Impact Assessment，DPIA），以便識別潛在挑戰與適當之風險控制措施。DPP 保護措施對於降低身分竊取風險和網路安全性風險而言很重要，因爲這些風險會削弱數位 ID 系統的可靠度。因此，根據 FATF 第 2 項建議，AML/CFT 和 DPP 權責機關應尋求合作並互相協調，以確保要求與規定之兼容性。

金融排除考量

137. 當數位 ID 系統未能涵蓋某一管轄區所有人或大多數人，或者排除特定族群的情況下，可能會導致（或至少不能減輕）金融排除，這是 AML/CFT 的風險。若強制使用無法普遍用於 CDD 之特定數位 ID，將導致與規定使用未普及整個族群的紙本 ID 類似的挑戰。無法使用數位科技或技術素養不足，均可能會增加排除風險。舉例來說，缺乏手機、智慧型手機或其他數位存取裝置，或缺乏網路覆蓋率和／或連線能力不穩定等因素，均可能會將貧困或偏遠地區族群或女性排除在外，還有生活在脆弱與受衝突影響地區的人們，例如：難民和流離失所者。如果數位 ID 系統使用生物特徵驗證，但卻未提供替代的驗證機制，則也可能導致金融排除，因爲某些生物特徵形式對於部分弱勢族群而言，失敗率較高。手工勞動者的指紋一般磨損的較爲嚴重，通常無法由生物辨識讀取器讀取；年長者也因爲臉部特徵改變、掉髮或其他老化跡象、疾病或其他因素，而經常出現特徵匹配失敗的情況；還有某些種族的群體以及具備深色膚色、眼睛形狀或臉部毛髮等特定相關生理特徵者，其臉部辨識失敗的比例也較高。

第五節：評估數位ID系統，是否具備充分可靠度與獨立性以執行風險基礎方法之CDD

138. 如第三節所述，必須使用可靠獨立之「原始文件、資料或資訊」執行客戶身分識別／確認之要求，在數位 ID 環境下代表數位 ID 系統應仰賴技術、流程、治理以及其他保護措施，提供適當等級之可信度。這表示數位 ID 系統之運作具備預期應有之適當可信等級（確信等級），並可產生準確之結果。此外亦應針對內部或外部操縱或篡改，採取充分保護措施，防止有人捏造身分或憑證，或對未經授權使用者進行驗證，包括透過網路攻擊或內部人的違法行爲。

139. 爲確認數位 ID 系統之使用是否符合第 10(a) 和 (d) 項建議之要求，政府、金融機構以及其他利害關係者應執行以下評估：

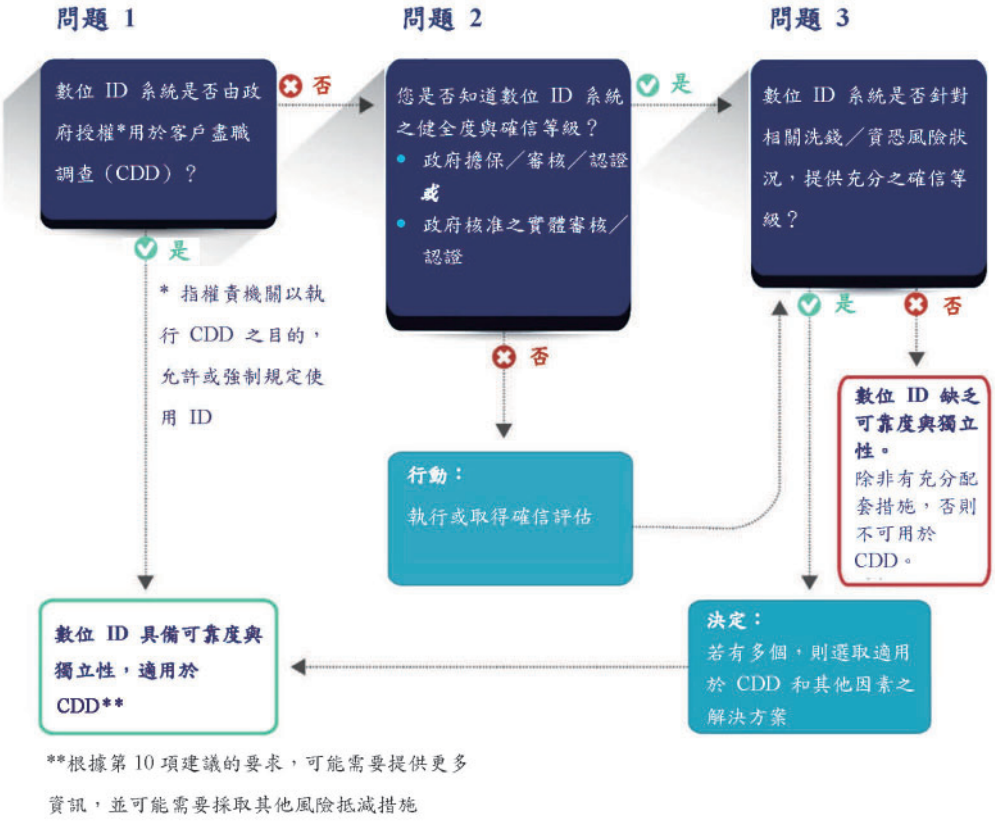
a. 瞭解數位 ID 系統根據其技術、架構及治理所提供之確信等級，以確認可靠度／獨立性；以及

b. 在既定之數位 ID 確信等級下，根據潛在的洗錢、資恐、詐欺及其他非法金融風險，以風險爲基礎決定數位 ID 系統是否具備適當之可靠度與獨立性。

140. 根據特定管轄區之數位 ID 系統和法規架構，政府以及受監管實體在評估身分系統確信等級及執行 CDD 的合適度方面所扮演的角色與職責可能各有不同，如以下受監管實體的決策流程圖所示。

141. 流程圖的決策流程說明，受監管實體在決定是否要使用數位 ID 系統進行客戶身分識別／確認及持續盡職調查之路徑。上述兩項評估則分別如問題二和三所示。

圖 4. 受監管實體之決策流程



**根據第 10 項建議的要求，可能需要提供更多資訊，並可能需要採取其他風險抵減措施

問題一：數位 ID 系統是否由政府授權用於 CDD ？

142. 在問題一當中，若政府「支持」數位 ID 系統，並且認定該系統適合用於執行 CDD，則受監管實體可使用該數位 ID 系統，而不需要執行問題二和三的評估。政府實際上已爲受監管實體執行建議評估之兩個步驟；至少針對標準之 CDD 風險，則決策流程之其餘部分不適用。然而，視管轄區之 AML/CFT 法律及數位 ID 生態系統而定，受監管實體可能必須採取其他措施（參見以下第 147 和 148 段說明）。
143. 政府可藉頒布法規或爲受監管實體提供指引的方式，明確地認定數位 ID 系統適合用於 CDD，允許或要求受監管實體使用數位 ID 系統執行特定層面之 CDD。舉例來說，若數位 ID 系統是由政府開發及運作，並對該系統有信心，或者政府設有機制取得其他供應商之數位 ID 系統確信等級之審核及認證資訊，便可明示授權。
144. 政府亦可透過隱喻方式「支持」數位 ID 系統，認定數位 ID 系統適合受監管實體用於執行 CDD。例如，當該國有需要時，政府應提供通用型數位 ID 系統用於證明官方身分。政府應對於其數位 ID 系統之運作方式及相關確信等級保持透明，授權供金融產業使用之限定用途身分系統亦同。
145. 根據各國國內 AML/CFT 法律及法規，受監管實體在某些情況下，如較高風險的情形下，將需要搭配使用經授權的數位 ID 系統，並收集其他本指引所未涵蓋之其他 CDD 層面資訊（即：瞭解業務關係之目的與預期本質）。某些管轄區之法規可能僅授權在低風險情況下使用數位 ID 系統。
146. 除了管轄區法規要求之外，鼓勵受監管實體根據金融機構自身之 AML/CFT、防詐騙及整體風險管理政策，考慮是否應採取額外的數位 ID 風險抵減措施（如果可用），如：額外的身分要件資料點或增加驗證因素，以及／或 ML/TF 風險管控措施。

問題二：您是否知道數位 ID 系統的相關確信等級嗎？

147. 若政府未明示或透過隱喻方式授權特定數位 ID 系統執行 CDD，則受監管實體必須先就其考慮採用之任何數位 ID 系統，確認其系統確信等級。[97]

148. 若政府（不論直接或透過指定組織代表政府[98]）擔保、審核或認證數位 ID 系統，則受監管實體可根據此類評估回答決策流程的問題二。同樣地，政府亦可核准國內或海外專業機構，對受監管實體可能採用之數位 ID 系統，就其確信等級進行測試／審核與認證。關於此類專業機構之概述，請參閱附錄 D。數位 ID 系統可經認證爲符合最低限度之確信等級，亦可具備不同的、日益健全之確信等級（無論是整個系統或其個別組成要件），但授權資訊應可公開取得。

149. 若政府既未授權數位 ID 系統執行 CDD，亦未提供取得關於數位 ID 系統確信等級授權資訊之機制，則受監管實體必須透過以下任一方式，自行決定系統之可靠度與獨立性：

    a. 自行執行確信評估。

    b. 使用專業機構（雖然並非政府官方核准）就確信等級所判定之審核或認證資訊。

150. 若受監管實體自行執行確信評估，則應對數位 ID 系統供應商執行適當之盡職調查，包括既有之治理方式，並且應格外謹慎爲之。

151. 唯有在專業機構基於合理基礎，斷定受監管實體可準確套用適當之公開揭露數位 ID 確信架構與標準的情況下，受監管實體方可使用該機構之資訊。例如，受監管實體可由其他政府機關批准類似用途，亦可由該管轄區、區域或國際之相關領域專家廣泛認定爲可靠實體。

---

[97] 如本指引先前所述，「確信等級」係指可信賴程度或數位 ID 流程各組成要件可靠性之可信度。

[98] 這些活動可能不是由該管轄區之 AML/CFT 監管機關執行，因為決定某一實體是否適用適當、且公開揭露之確信架構與技術標準之資格，很可能屬於政府其他部門。執行此任務之權責機關，由各管轄區自行決定。舉例來說，美國總務署（General Services Administration，GSA）已經核准許多信任架構業者，認證政府專用之 ID 系統。

問題三：數位 ID 系統是否適用於 ML/TF 風險狀況？

152. 一旦受監管實體相信其瞭解數位 ID 系統的確信等級之後（透過問題二所述流程），則應分析該數位 ID 系統在相關非法金融交易風險情況下，是否可滿足 FATF 以風險基礎方法執行 CDD 之風險基礎方法要求。換句話說，鑑於與客戶、產品與服務、營運地理區域相關之潛在 ML/TF 風險，某確信等級之數位 ID 系統是否適用於客戶身分識別／確認及持續盡職調查？受監管實體應考量相關非法金融交易風險之背景，分析該確信等級之數位 ID 系統是否適足。視管轄區的 AML/CFT 要求及可用之數位 ID 系統而定，受監管實體可從具備不同確信等級的多個數位 ID 系統中選擇，用於執行身分證明與驗證。在此情況下，根據潛在非法活動類型和 ML/TF 風險等級，受監管實體選擇之系統所具備之身分證明和／或驗證健全度應與風險等級相襯。

153. 在某些國家，政府已針對一般或高 ML/TF 風險情況，規定必要（整體）之確信等級。受監管實體仍可在一系列具備必要確信等級的數位 ID 系統中進行選擇，或者也可選擇同一系統所提供之各種不同等級的身分證明、和／或特定憑證與驗證因素。若爲此一情況，受監管實體在決定時應考慮其 ML/TF 風險之特殊性，因爲這攸關身分證明和驗證。受監管實體亦可在較低風險情況下，選擇適當之數位 ID（另請參見本節稍後關於普惠金融之探討）。

運用數位 ID 確信架構與技術標準執行 RBA

154. 如上所述，政府（作爲 IDSP 和／或作爲監管者、監督者與決策制定者）和受監管實體（作爲依賴方）應就相關之 ML/TF 風險因子與 AML/CFT 管控措施，充分考慮相應之數位 ID 風險因子與確信等級。如以下更詳盡說明所述，數位 ID 確信架構與標準爲執行此一評估提供了實用的工具。

155. 因此，建議政府與受監管實體在評估數位 ID 系統是否滿足第 10(a) 項建議之「可靠、獨立」標準時，將確信架構與標準所提供之資訊納入考量。此外亦當個別考量各系統主要數位ID組成要件之可靠性。

因爲視潛在之 ML/TF 風險因子與管控措施而定，數位 ID 系統的每一個組成要件（身分證明／註冊、驗證，或在可能的情況下，聯合識別），未必需要具備相同程度之可靠度。

156. 瞭解數位 ID 系統各組成要件的確信等級，有助受監管實體在仰賴數位 ID 執行 CDD 時，採取更細膩的風險基礎方法。按流程評估確信程度之做法，在普惠金融的情況下尤其重要。GOV.UK Verify 技術標準和最終版本之 US NIST 800-63-3 數位 ID 準則，均已針對 ID 系統之個別基本流程，採納獨立「確信等級」。[99] 對於整個數位 ID 系統採用單一確信等級之確信架構與標準（如：eIDAS 規章），可透過檢驗流程各組成要件如何滿足各確信等級要求，實施按流程逐步評估之做法。

157. 數位 ID 科技與架構以及數位 ID 確信架構與標準是動態且不斷進化的，[100] 爲了加速創新，其標準本身也十分具彈性、並以結果爲基礎。除了允許不同技術與架構，以滿足當前特定確信等級之要求外，也以盡可能與時俱進的方式建構。管轄區應避免採用將當前確信等級要求，設爲可靠度上限（而非下限）之固定制式做法。

使用數位 ID 確信標準與架構

158. 數位 ID 確信架構與標準通常會對數位 ID 系統中三大步驟的每一項，制定各種可靠度越來越高的確信等級，並搭配日益嚴謹的技術要求。

159. 如同第 10 項建議注釋所提出的潛在較高與較低風險 ML/TF 因子範例，技術標準以確信等級的形式，爲數位 ID 系統之基本構成流程，提供了 ID 可靠度因素。每一個確信等級都反映了所述流程特定程度的確信與信心。具備較高確信等級之流程，可靠度較高；具備較低確信等級之流程，則構成較大之失效風險，可靠度亦較低。相關機關與受監管實體可使用確信等級，評估特定數位 ID 系統之可靠度。本指引並未要求或建議任何特定確信等級。

[99] 例如，NIST 指引便為數位 ID 流程的每一個階段，制定不同的確信等級（1-3）：ID 確信等級（IAL）、驗證與憑證生命週期管理確信等級（ALA），以及聯合識別確信等級（FAL）。

[100] 各國應體認，數位 ID 標準不一定會跟上不斷進步的科技革新。例如，在本指引最終定稿時，數位 ID 確信架構與標準尚未能滿足持續驗證之要求，也未能因應漸進式身分識別之概念，因為它與持續的動態身分證明相關。

160. 部分技術標準支持採用按流程進行之可靠度評估，並且認爲不同的數位 ID 流程可以但不必要處於全部相同的確信等級（AL）。從更基本的角度來看，RBA 係要求根據 ML、TF、詐騙以及其他非法金融交易風險，決定各流程所適用之確信等級。即便是指派單一確信等級之架構，受監管實體亦可檢驗該流程個別組成要件，是否符合每一個確信等級之個別要求。

161. 爲說明相關機關、金融機構以及其他利害關係者，在評估數位 ID 是否可靠獨立、以及數位 ID 確信架構與標準所允許的彈性時所使用之評估因子類型，附錄 E：美國與歐盟數位 ID 確信架構與技術標準概述，以美國與歐盟爲例列出確信等級。此概述就廣義層面描述身分證明（數位 ID 系統第一階段）之若干技術要求，亦簡要指出與驗證確信等級相關之數項重要考量。

普惠金融之特殊考量

基於 AML/CFT RBA 之數位 ID 風險管理與 ML/TF 風險抵減措施之關係

162. 在理想的情況下，數位 ID 系統之採用將可讓個人以更高的確信等級證明官方身分，尤其是在尚未爲大多數群眾提供健全官方身分的國家。然而，由於數位 ID 通常是以紙本身分證據爲基礎，在官方 ID 系統覆蓋率低的國家，部分族群可能因難於證明身分，而無法取得更高確信等級之數位 ID。

163. 如本文先前所強調的，面臨普惠金融挑戰之管轄區，在建立證明官方身分之必要身分要件、證據和流程時，應採用彈性做法。如此將可確保原來無法取得金融服務的人，在身分證明的要求中不被排除（例如：將永久居住地址設爲選擇性要件，並允許受信任個人證明該人之身分）。爲了解決此類議題所擬定的更廣泛國際、政府或 NGO 行動方案中，包括藉由增加獲取身分證據途徑等，AML/CFT 權責機關和受監管實體應考慮如何在數位 ID 系統上執行以風險爲基礎之 CDD，尤其是在金融排除已被認定爲 ML/TF 風險之管轄區或特定族群。

164.FATF 在 2017 年就「2013 年 AML/CFT 措施與普惠金融指引」發布

了補充條款，特別著重於 CDD 和普惠金融。[101] 該文件強調受監管實體根據已識別的風險本質與等級，所應採取之風險管控措施，亦提到可消除與確認客戶身分有關的普惠金融障礙之各種 CDD 做法，例如：對於可靠與獨立資訊來源之廣泛理解，或採取簡化的盡職調查措施。本指引指出，在許多國家當中，數位金融服務的擴展是透過分級的 CDD 做法執行。舉例來說，在此做法下，先前受到排除或未能享受周全服務的個人，將可取得具 AML/CFT 風險管控措施的帳戶，如：限制帳戶的總價值和／或限制特定時間範圍內的交易金額與次數，客戶身分之確認作業延遲至達到指定的門檻值爲止。

165. 將 2017 年普惠金融指引中的指示應用至數位 ID 系統，係指當特定潛在客戶的首次開戶 ML/TF 風險較低時，便適用較低身分證明確信等級之數位 ID 系統。爲確保 ML/TF 風險受到管控，可能需要採取額外措施，包括如上所述對帳戶之使用施加限制。同樣地，當與未經授權帳戶存取相關的非法金融交易風險較高（如：因管轄區時常發生使用者名稱與密碼遭竊情況），但客戶爲低風險時，則適用身分證明確信等級較低（用於首次開戶客戶身分識別／確認），但與驗證有關之組成要件則選用確信程度較高之數位 ID 系統，以預防帳戶遭到未經授權者使用。即便是低額帳戶，在授權帳戶存取以執行交易之前驗證客戶的身分，對於打擊詐騙轉帳而言很重要，也可確保分級 CDD 價值、交易流通速度與交易量不受影響。

166. 根據 FATF 標準採用彈性作法使用數位 ID 系統的能力，對於普惠金融而言，也具備重要意涵。此能力可促進分級 CDD 與延遲身分確認之實施，因爲在數位 ID 確信架構和標準下，身分證明／註冊具備較低確信等級之數位 ID 系統，其對個人身分之身分證據或確認要求較不嚴謹（請參見附錄 E）。這表示先前受到排除或未能享受周全服務的個人（首次開戶時，缺乏特定文件以證明自己的官方身分），仍可註冊於數位 ID 系統中。然後，此個人可使用數位 ID 的驗證因素進行客戶身分識別，進而開立帳戶，並視指定管制措施與門檻值而定，可省去身分確認的步驟。

[101] FATF（2013-2017），防制洗錢與資恐措施及普惠金融－客戶盡職調查補充條款，FATF，巴黎 www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

167. 此外，數位ID系統可使之前未能享受周全服務或遭金融排除之個人，逐漸發展更健全的數位化足跡與風險概況，使其能夠取得更廣泛的金融服務。視管轄區對證明官方身分要求的做法而定，數位 ID 系統可改變官方身分本身的概念，從固定物件轉變成可隨時間強化之物件，即漸進式身分。有了漸進式身分後，當個人（如：客戶）從事數位金融與其他線上活動並建立數位化存在時，其他身分要件與驗證因素便爲可用，並可強化個人的數位 ID，進而提高客戶身分之可信等級。

168. 即便數位 ID 系統無法互相操作，且數位 ID 亦無法攜帶，漸進式身分仍有助於普惠金融，因爲它使特定的受監管實體對於個體客戶有更進一步的瞭解，並對業務關係建立信心，以提供更廣泛的金融服務。然而，當漸進式身分可攜之後，其價值將可大幅提升（包括出於普惠金融目的），因爲如此將可利用由單一受監管實體所蒐集之個人行爲模式、交易資料與相關驗證資訊，建立更健全的身分，並用於個人金融往來及未關聯受監管實體之客戶身分識別／確認。但在缺乏可攜性的情況下，客戶將必須在一段時間內重新於各受監管實體建立個人的漸進式身分，而在此期間他們僅可存取低價值／低風險產品與服務。

說明方塊 3. 分級使用數位 ID 與漸進式 CDD，如何促進普惠金融之說明

一名遭金融排除之個人使用所取得之數位 ID 申請基本銀行帳戶，無需出示身分證據。數位 ID 在身分證明方面具備較低的確信等級，但具備可信的驗證確信等級，證明與已識別個人綁定之驗證因子，係由主張者所管理使用。

受監管實體爲客戶開戶並提供較低風險的銀行帳戶，該帳戶總額門檻、交易量和交易流通速度都非常低，並且無跨國交易功能（這些風險抵減措施是以風險分析爲基礎）。客戶使用此帳戶取得合約手機，並可直接以該帳戶收取進行其他活動所獲取之數位薪資。

受監管實體使用與直接存入工資、社會福利轉帳或津貼關聯的資料，以確認就業狀態、職業與資金來源，並以手機話費和水電費的定期扣款帳戶，藉此建立負責任的金融行爲模式。受監管實體也會收集其他交易與關聯的驗證資訊，以確認客戶的住址。隨著時間增加，受監管實體會使用客戶的一致金融活動與行爲模式（如：交易時間、一般交易金額、目的／交易對方與地理位置定位），以強化帳戶存取驗證與防詐騙措施。

管轄區的 AML/CFT 法律架構是以原則、績效與結果爲基礎，其客戶身分識別／確認法規要求受監管實體應基於合理基礎使他們知道自己的客戶是誰，但未嚴格規定達成此目標的方法。受監管實體將隨著客戶活動產生的資料，視爲客戶之身分證據，並用於建立掌握客戶身分以及客戶風險概況之信心。當此可信度使受監管實體確信已滿足客戶身分識別／確認義務，並滿足受監管實體其他金融服務之風險胃納與風險管理做法及程序時，受監管實體便會提供具備較高門檻值及更多功能之一般銀行帳號，之後提供小額貸款，以供客戶創業。

此數位 ID 做法仿效 FATF 2017 年 CDD 與普惠金融指引所述之相同流程，其中未具備充分身分文件之個人可經過分級 CDD，從受限制的低風險帳戶開始享有金融服務，循序漸進地擴展個人的取得金融服務的範圍。

資料出處：美國財政部

數位 ID 標準與架構可促進普惠金融

「受信任的推薦人」

169. 在部分數位 ID 確信架構與標準允許沒有傳統身分證據者的其中一個例子，是允許透過受信任推薦人－如：里長、當地政府機關、法官／地方法官、雇主、在社區內信譽良好者（如：商務人士、律師、公證人），或依各國相關法令、規範或機構政策以其他某種形式的經過培訓、批准或認證之個人，爲申請人之身分證據做擔保。[102]

170. 舉例來說，在 NIST 規範下，IDSP 如要使用受信任推薦人，則必須：
- 制定書面政策與程序，說明受信任推薦人之決定方式（遴選標準），以及受信任推薦人作爲有效推薦人之生命週期，以將各種限制、撤回與擱置要求納入考量。
- 證明與申請者相同等級之受信任推薦人身分，並決定在受信任推薦人與申請人之間建立關係所需之最低限度身分證據。

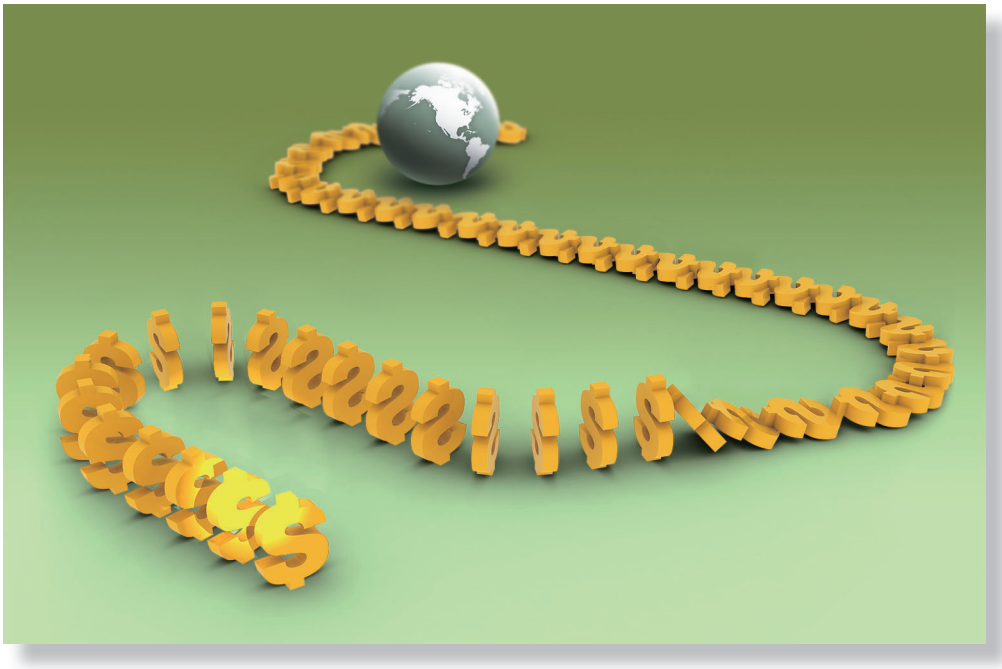
遠端身分證明與非面對面首次開戶

171. 如前述，數位 ID 系統可讓遠端客戶身分識別／確認，並支援一般或低風險等級之遠端金融交易。即便是較高的確信等級，技術標準亦允許遠端身分證明與註冊。請參閱附錄 E。

[102] NIST 800-63A 4.4.2. IAL2 Trusted Referee Proofing Requirements.

第七部分

本局洗錢防制處重要紀事



108/1/21	舉辦「國境執行洗錢防制工作協調會議」。
108/1/28-2/1	派員赴印尼雅加達參與艾格蒙工作組會議。
108/2/26	舉辦「國境執行洗錢防制工作第二次協調會議」。
108/3/14-3/15	出席洗防辦舉辦之「相互評鑑面對面會議之模擬會議」。
108/3/18-3/21	出席 APG 第三輪相互評鑑面對面會議。
108/5/8-5/9	出席美國在臺協會舉辦之「再參與國際制裁執行及強化研討會」。
108/5/10	出席美國在臺協會舉辦之「政策及企業國際制裁執行及強化研討會」。
108/5/13-7/9	派員至本局各處站進行洗錢防制與打擊資恐巡迴講習。
108/5/24	與金融監督管理委員會銀行局及臺灣金融服務聯合總會共同舉辦「犯罪金流分析與異常交易態樣研討會」。
108/6/11	出席法務部舉辦之「108 年洗錢防制法實務座談會」。

108/6/17-6/21	派員赴美國奧蘭多出席 FATF 第 30 屆第 3 次大會及工作組會議。
108/6/28-7/6	派員赴荷蘭海牙出席艾格蒙聯盟年會。
108/7/3	於荷蘭海牙與瓜地馬拉共和國金融監督管理局特別驗證處簽署「關於涉及洗錢或其他資產清洗、相關前置犯罪及資助恐怖主義金融情資交換合作協定」。
108/7/10-7/11	出席法務部舉辦之「108 年度國際刑事司法互助實務研習會」。
108/8/18-8/23	派員赴澳洲坎培拉出席 APG 第 22 屆年會暨相關工作組會議。
108/8/20	與東帝汶、東加及巴布亞紐幾內亞等 3 國金融情報中心於澳洲坎培拉簽署「關於涉及洗錢、相關前置犯罪及資助恐怖主義金融情資交換合作瞭解備忘錄」。
108/9/23-9/24	派員赴蒙古烏蘭巴托出席「亞太區追討犯罪所得機構網絡（ARIN-AP）」第 6 屆年會。
108/10/14	與約旦哈希米王國反洗錢及打擊資恐中心簽署「關於涉及洗錢、相關前置犯罪及資助恐怖主義金融情資交換合作瞭解備忘錄」。
108/11/6	出席銀行公會舉辦之 108 年度「防制洗錢實務案例研析」法遵論壇。
108/11/6-11/9	派員赴澳洲墨爾本出席 108 年「不爲恐怖行爲融資」打擊資恐部長級會議。

中華民國一〇八年

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：109 年 10 月

GPN：4310901239

ISBN：978-986-5443-37-5 (光碟片)

洗錢防制工作年報
法務部調查局

Anti-Money Laundering Annual Report, 2019
Investigation Bureau, Ministry of Justice,
Republic of China (Taiwan)

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

ISBN：978-986-5443-37-5
GPN：4310901239