中華民國一〇六年

洗錢防制工作年報

法務部調查局

法務部調查局一〇六年洗錢防制工作年報

The Investigation Bureau, Ministry of Justice

Anti-Money Laundering Annual Report,2017

序 言 *PREFACE*

自行政院洗錢防制辦公室成立以來，公私部門協力開展國家洗錢及資恐風險評估工作，本（107）年初終於完成我國風險與威脅評估，將毒品販運、詐欺、貪污賄賂、內線交易與市場操縱、稅務犯罪、走私、第三方洗錢、組織犯罪等 8 項列爲本國「非常高風險威脅」；歷經數次國家風險評估程序，於本年 5 月 2 日完成我國首部「國家洗錢及資恐風險評估報告」，並正式對外發表，顯示我國積極因應亞太防制洗錢組織（APG）相互評鑑，亦展現我國落實國際標準要求之能力。

去（106）年國際地緣政治風起雲湧，東亞局勢起伏，國人因裝載油品轉運予北韓船隻，涉嫌違反聯合國安全理事會制裁北韓之決議，遭我國資恐防制審議會指名制裁，啓動我國《資恐防制法》施行後首次目標性金融制裁措施，履踐我國身爲國際社群成員的義務。面對當前金融全球化與跨境犯罪活動的急遽發展，各國均尋求跨國合作以共同打擊犯罪，本局身爲我國金融情報中心，亦積極對外洽簽情資交換合作瞭解備忘錄，去年已與聖露西亞、匈牙利、教廷、拉脫維亞、迦納等 5 國完成簽署，合作版圖多達 44 國，顯現我國致力於洗錢防制及打擊資恐之成效，廣爲國際社會認可，並彰顯我國與國際接軌之努力。

因應《洗錢防制法》修正後，指定之非金融事業或人員負有申報義務，而《資恐防制法》生效後，則先後有國人與以渠等爲實質受益人之境外公司遭目標性金融制裁，本局洗錢防制處所受理之可疑交易報告與資恐通報數量大增，爲加速處理，經主管機關之同意，信用合作社、中華郵政公司及保險業已繼銀行業後，全面採行媒體申報，可提升業者之申報效率，同時強化資料庫建置與使用效能。

金融服務資訊化、數位化之浪潮勢不可檔，比特幣等虛擬貨幣所引

領之金融科技（FinTech）議題方興未艾，執法機關如何面對日益惡化之數位犯罪問題，本局蘇文杰調查官對涉及虛擬貨幣洗錢之資金清查，以及第一線執法者面對比特幣搜索扣押等挑戰，提供相關建議。而防制洗錢金融行動工作組織（FATF）去年 11 月發布「私部門資訊分享」之指引，本局洗錢防制處特翻譯爲中文收錄於本年報，謹供相關權責機構與私部門參考。

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

蔡清祥 謹識

中華民國 107 年 7 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金融機構及各司法機關執行防制洗錢工作之資料加以統計分析。

二、編輯內容

（一）本年報分下列五個部分：

1. 組織簡介。
2. 工作概況（含統計圖表資料）。
3. 重要案例。
4. 專題研究：涉及虛擬貨幣洗錢之資金清查作爲——兼論比特幣之搜索扣押。
5. FATF 指引：私部門資訊分享（中譯）
6. 洗錢防制處重要記事。

（二）本年報係依據本局洗錢防制工作有關資料、各檢察署依違反洗錢防制法偵結起訴（含緩起訴及聲請簡易判決）案件，加以統計彙整。

三、凡例

（一）本年報所用各項單位，年度以國曆爲準，惟國外資料以西元紀年爲準。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，以及旅客攜帶大額外幣及有價證券入出境之通報，以件爲單位。各檢察署起訴與各級法院審判之洗錢案件以案爲單位，金額以新臺幣元爲準。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）新修正之洗錢防制法已於 106 年 6 月 28 日生效，本年報所引用洗錢防制法之相關規定，若無特別註明，皆爲修正後之條號。

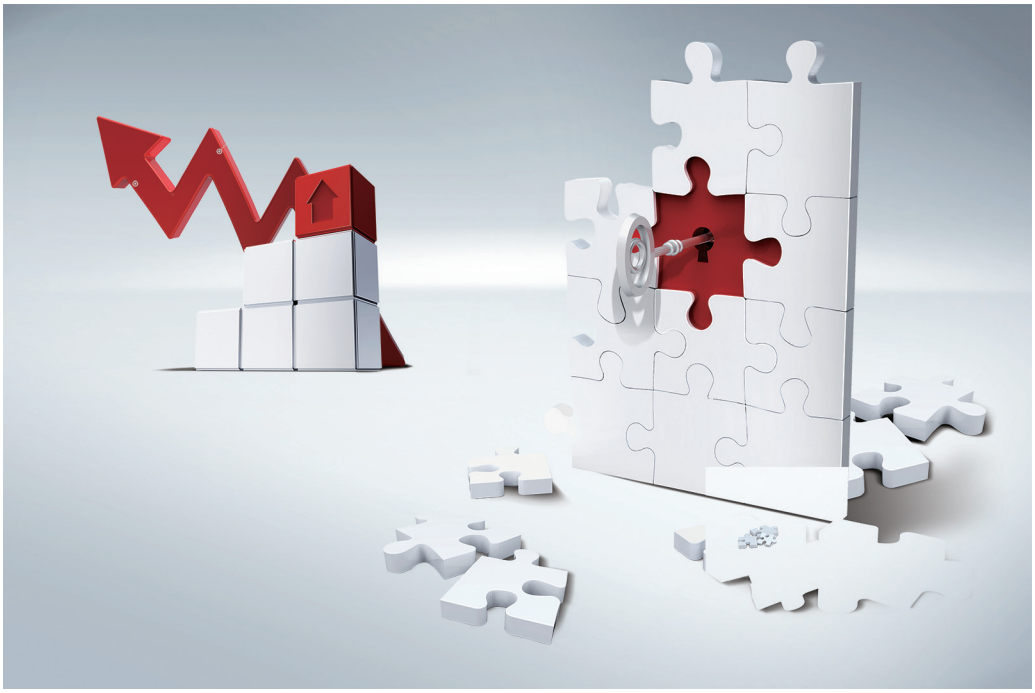
四、本年報倉促付梓，錯誤及未盡周延之處，敬請不吝賜教，俾以訂正。

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，並於1990年制訂40項反洗錢建議，至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的重大犯罪行爲。

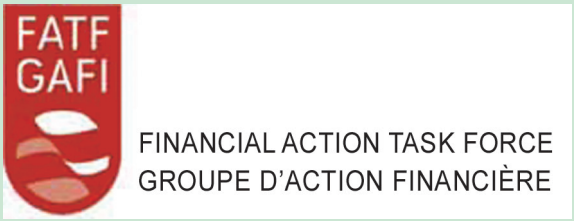
我國政府洞察洗錢犯罪之危害性，順應世界潮流，制定《洗錢防制法》草案，於民國（下同）85年10月23日經立法院通過，並奉總統明令公布，自86年4月23日施行。歷經20年餘的實務運作，已獲國際防制洗錢組織高度肯定，更針對實際所遭遇之問題，先後於92年、95年、96年、97年、98年及105年修法，以符合國際防制洗錢組織的要求並兼顧實務運作之需要。

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，各國防制洗錢法律均課以金融機構申報大額通貨及可疑交易之義務，而負責受理、分析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》，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條規定由本局受理資恐通報及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25位。組織、分工及作業流程，如圖A與B。

依97年10月17日修正之〈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旅客或隨交通工具服務之人員攜帶大額外幣現鈔或有價證券入出國境資料之受理、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。



◎ FATF（Financial Action Task Force，FATF）

七大工業國於 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，並檢查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 37 個會員（35 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 2 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）

依新修訂 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全國性統一受理、分析可疑交易報告及其他有關洗錢、相關前置犯罪及資助恐怖活動之資訊，並分送分析結果」。而依據各國金融情報中心所組成的國際組織「艾格蒙聯盟」（Egmont Group），將金融情報中心定義爲：「負責受理（或經同意可提出請求）、分析下列揭露之金融資訊，並送交權責機關之全國性中央單位：

（i）可疑的犯罪財產，或

（ii）國家法令所定之防制洗錢資訊。」

《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貨幣現鈔、有價證券、黃金及有被利用進行洗錢之虞之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項各款物品出入境者，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 A：洗錢防制處組織圖

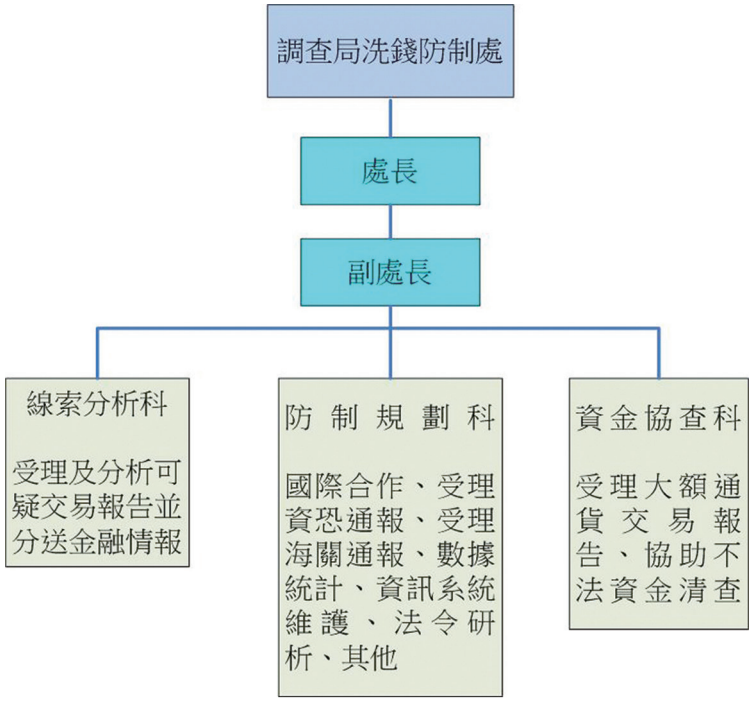
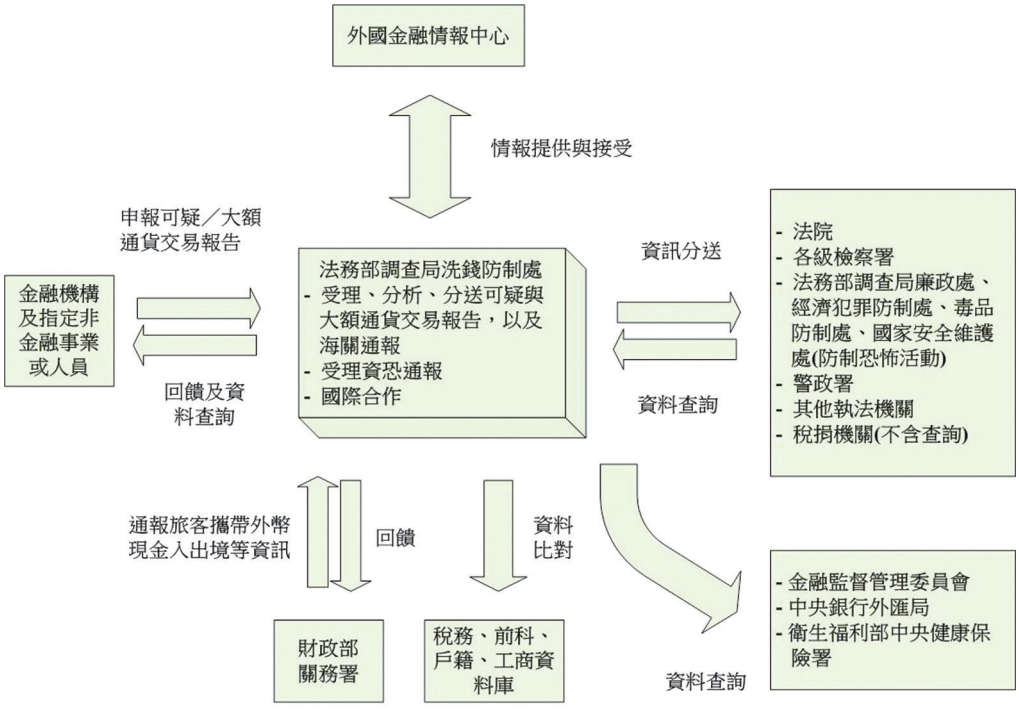


圖 B：洗錢防制處作業流程圖



第二部分

工作概況

壹、策略研究
貳、受理可疑交易報告之申報
參、受理一定金額以上通貨交易之申報
肆、受理財政部關務署通報資料
伍、起訴案件統計
陸、教育訓練與宣導
柒、國際合作

壹、策略研究

一、參與因應 APG 第三輪相互評鑑相關會議

爲推動 APG 第三輪相互評鑑之各項整備工作，本局於 106 年 7 月訂定實施「因應 APG 相互評鑑專案實施計畫」，並成立專案小組，由林副局長擔任召集人，以洗錢防制處爲秘書單位，縝密規劃並統合本局相關執法業務單位及金融情報中心，包括：國家安全維護處、廉政處、經濟犯罪防制處、毒品防制處、資通安全處及洗錢防制處等，召開多次協調會議，全力準備，並由專案小組各單位派員參加行政院洗錢防制辦公室（下稱洗防辦公室）所召開之各項會議，此外，針對完成國家洗錢及資恐風險評估報告、技術遵循與效能遵循之國家報告也隨時提供專業意見，供洗防辦公室參考。

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

APG 於 1997 年設立，其目的在於協助其會員國接受與履行 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 2001 及 2007 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給予高度肯度。法務部調查局作爲我國之金融情報中心獲得最高評等，顯示功能運作良好。

目前 APG 計有 41 個會員國、觀察員 8 國及 31 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、編纂策略性金融情報

本處於受理、分析可疑交易報告之過程中，若歸納出該期間新興之可疑樣態或犯罪趨勢，則進一步蒐集資料後編纂該年度之金融情報，分送相關主管機關與申報機構，亦不定期出版《洗錢案例彙編》，綜整具代表性之案例，提供主管機關與申報單位參考。105 年間，本處從眾多可疑交易報告及實際案例中發現許多陸資企業於我國銀行申設 OBU 帳戶，但因銀行不易審查外國自然人及法人之客戶身分與實質受益人，難以查證交易相對人、交易本質、資金合法性，該等交易之跨境洗錢風險極高，易成爲資金快速進出之中轉帳戶，遂於 105 年 12 月間舉辦「金融機構防制洗錢及打擊資恐業務負責人座談會」，針對陸資企業開立國際金融業務分行 (Offshore Banking Unit；下稱 OBU) 帳戶之風險管理進行簡報與討論。而後本局並據以提出完整之書面報告《OBU 客戶審查罅隙易遭規避致帳戶供非法目的使用》（Circumvention of OBU CDD Measures for Unlawful Purpose）分析我國 OBU 現況、OBU 客戶審查的可能罅隙與遭濫用的風險，彙整 OBU 業務相關的反洗錢與反資恐規範，歸納 OBU 可能遭濫用於洗錢的方法以及遭濫用的表徵，並分送行政院金融監督管理委員會（下稱金管會）與中央銀行參處，協助促成主管機關於翌（106）年 5 月份修正〈國際金融業務分行管理辦法〉，依 FATF 第 17 項建議，授權各銀行得透過海外分行或子行協助確認客戶身分及應符合之規定，要求各銀行先將執行方案及中介機構名單報金管會備查，並規定所有銀行應於同年 12 月底前，完成所有境外法人客戶資料之審查，重新確認客戶洗錢及資恐風險等級，強化法令遵循與風險管理。

三、受理反資助武擴案件申、通報與專案資金協查

106 年間，國人陳○○所經營之比○○油品集團（B ○○ Group）租用香港籍油輪○○永嘉號（○○ Winmore），於南韓裝載油品後，前往公海以船對船方式轉運予北韓船隻，涉嫌違反聯合國安全理事會（下稱安理會）制裁北韓之決議，安理會並於 106 年 12 月 28 日指名制裁比○○ 18 號（B ○○ No. 18）船隻。本處獲悉後立即調閱並清查陳○○個人財務資料與名下公司所有之船舶資料，提交法務部研議召開資恐防制審議會（下稱審議會）參考，審議會即於 107 年 1 月 12 日通過制裁

陳○○（Chen ○○）、○○ Taiwan Group Corporation 及 B ○○ Group Corporation，制裁及於以陳○○爲實質受益人之境外公司○○ Enterprise Ltd. 與○○ Corporation Peru S.A.C.。

另臺灣高雄地方檢察署指揮本局航業調查處，針對陳○○名下公司持有之船隻駁油予北韓是否涉及僞造文書等進行調查。於陳○○及前揭公司遭指名制裁前、後，本處受理金融機構之申報或通報，立即彙整分送相關金融情報予權責機關參處，並協助進行資金清查。

此外，本處亦參與臺灣臺中地方檢察署偵辦之國人涉及多明尼加跨國電信詐欺案、臺灣高雄地方檢察署偵辦○○造船公司承包國防部○○艦標案涉嫌不法案等專案資金協查，並出席相關會議，以協助案件偵辦。

四、接待來訪之洗錢防制業務政府官員

巴拿馬經濟財政部部長戴拉瓜帝亞（Dulcidio De La Guardia）於 106 年 3 月 3 日來局參訪，本局蔡局長親自接待，互贈紀念品，雙方並就防制洗錢業務進行工作會談。

106 年 3 月 3 日蔡局長致贈紀念品予戴拉瓜帝亞先生（Dulcidio De La Guardia）。

聖文森金融情報中心副處長森蒂（LaTeisha Arielle Rachael Sandy）率員來臺參訪，本局受我國外交部委託，於 106 年 10 月 18 日至 20 日辦理防制洗錢講習課程，雙方就金融情報中心之運作實務以及申報情形交換意見。

106 年 10 月 18 日李處長致贈紀念品予森蒂女士（LaTeisha Arielle Rachael Sandy）。

五、持續參與國際活動

本處爲求接軌國際，除積極參與 FATF、APG、艾格蒙聯盟等國際組織之年會、工作組會議，並派員出席 FATF Training & Research Insititute（TREIN）訓練課程、艾格蒙聯盟亞太區策略分析課程，以及 APG 洗錢樣態研討會，促進本處同仁持續進修，掌握國際組織最新訊息，並與他國官員切磋交流，強化我國國際參與。

◎艾格蒙聯盟 (Egmont Group)

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，爲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 1998 年 6 月第六屆年會時加入，現行名稱爲 AMLD（Anti-Money Laundering Division，即洗錢防制處）,Taiwan。該組織迄今（107 年 6 月）有 155 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之宗旨，截至 106 年 12 月底止，業與 44 國簽署合作協定或備忘錄。

本處李處長於 106 年 7 月 15 日至 22 日前往斯里蘭卡首都可倫坡出席 APG 年會，與我國各機關代表合影。

六、辦理業務講習

為精進執法機關對洗錢防制業務之認知，因應《洗錢防制法》修正後相關執法實務需求，本處於 106 年 4 月 20 日舉辦「洗錢防制業務專精講習」，說明《洗錢防制法》及《資恐防制法》新修正條文、洗錢防制處相關資訊系統，並進行案例報告，參加人員為本局內外勤同仁共約 180 人。

106 年 4 月 20 日本處李處長於「洗錢防制業務專精講習」致詞

貳、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。」並要求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。106 年度本局計受理 23,651 件可疑交易報告，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 81.7%，可疑交易有 35.3% 發生於臺北市，交易對象之年齡層有 51.1% 分佈於 31 歲至 60 歲間，交易金額則有 21.8% 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 E）。

一、可疑交易報告申報情形

表 01：106 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	19,329
外國銀行	30
信託投資公司	0
信用合作社	700
農、漁會信用部	234
辦理儲金匯兌之郵政機構	2,303
票券金融公司	0
信用卡公司	13

保險公司	800
證券商	115
證券投資信託事業	17
證券金融事業	5
證券投資顧問事業	0
證券集中保管事業	24
期貨商	9
指定非金融事業或人員	46
大陸銀行	3
電子支付及電子票證機構	23
合計：23,651	

表 02：近 5 年可疑交易報告申報件數統計表

年　度	102 年	103 年	104 年	105 年	106 年
件數統計	6,266	6,890	9,656	13,972	23,651

二、本局處理情形

表 03：106 年受理之可疑交易報告處理情形統計表

處　理　情　形	件　數
移送本局辦案單位	2,660
函移送警政、院檢及其他行政機關	920
結案存參	19,664
分析中	279
國際合作	127
提供情資	1
合計：23,651	

三、可疑交易發生地區分布

表 04：106 年可疑交易發生地區統計表

交易地區	件　數	交易地區	件　數
台北市	8,341	嘉義市	340
新北市	3,874	嘉義縣	119
基隆市	382	台南市	1,202
宜蘭縣	139	高雄市	1,976
桃園市	1,969	屏東縣	200
新竹市	474	花蓮縣	97
新竹縣	279	台東縣	39
苗栗縣	199	澎湖縣	26
台中市	2,849	金門縣	57
彰化縣	711	連江縣	7
南投縣	190	其他[1]	26
雲林縣	155		
			合計：23,651

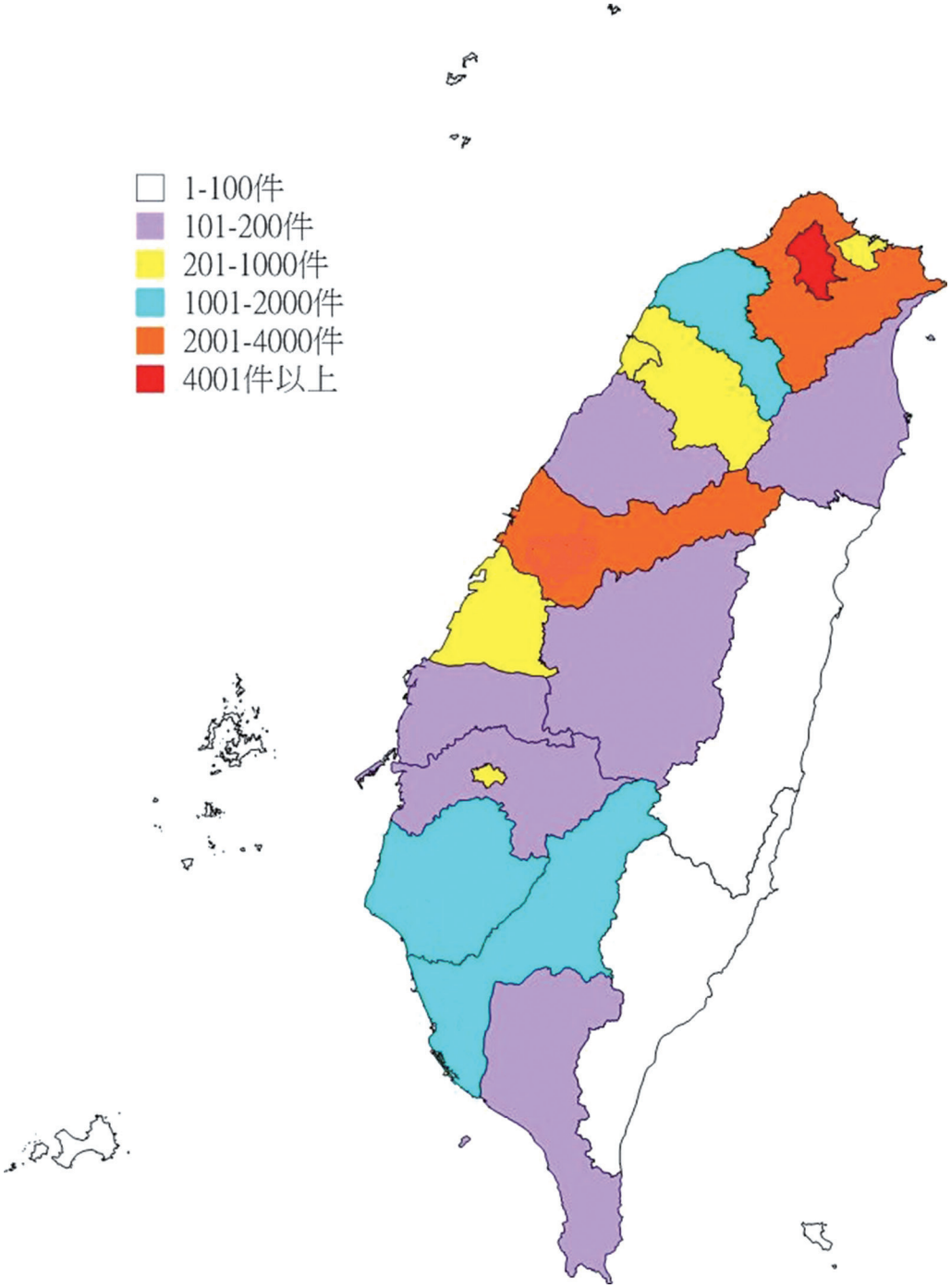
四、可疑交易申報月份分布

表 05：106 年各月份申報可疑交易報告統計表

月份	1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
件數	1,369	1,184	1,663	1,295	1,511	2,038	1,852	2,348	2,483	1,935	3,001	2,972

[1] 指國外地區等

圖 C：106 年可疑交易發生地區分布圖

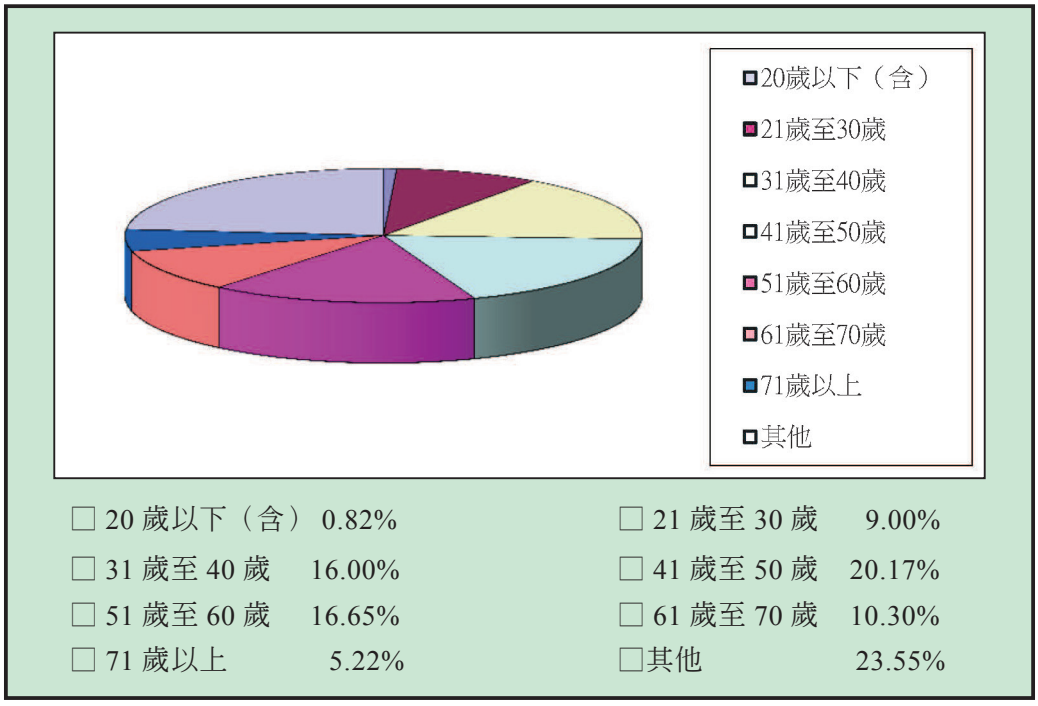


五、可疑交易對象年齡層分布

表 06：106 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）	193
21 歲至 30 歲	2,129
31 歲至 40 歲	3,783
41 歲至 50 歲	4,368
51 歲至 60 歲	3,938
61 歲至 70 歲	2,436
71 歲以上	1,235
其他 [2]	5,569
合計：23,651	

圖 D：106 年可疑交易申報對象年齡層分析圖



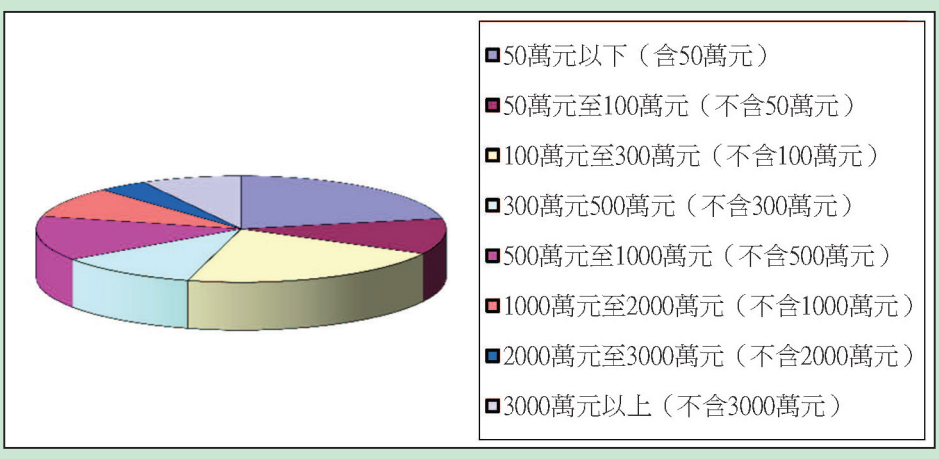
[2] 其他：係指公司行號、非法人團體等。

六、可疑交易金額分布

表 07：106 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）	5,164
50 萬元至 100 萬元（不含 50 萬元）	2,570
100 萬元至 300 萬元（不含 100 萬元）	5,081
300 萬元 500 萬元（不含 300 萬元）	2,628
500 萬元至 1000 萬元（不含 500 萬元）	3,196
1000 萬元至 2000 萬元（不含 1000 萬元）	2,212
2000 萬元至 3000 萬元（不含 2000 萬元）	930
3000 萬元以上（不含 3000 萬元）	1,870
合計：23,651	

圖 E：106 年可疑交易申報金額分析圖



- 50 萬元以下（含）21.83%
- 50 萬元至 100 萬元（不含 50 萬元）10.87%
- 100 萬元至 300 萬元（不含 100 萬元）21.48%
- 300 萬元至 500 萬元（不含 300 萬元）11.11%
- 500 萬元至 1,000 萬元（不含 500 萬元）13.51%
- 1,000 萬元至 2,000 萬元（不含 1,000 萬元）9.35%
- 2,000 萬元至 3,000 萬元（不含 2,000 萬元）3.93%
- 3,000 萬元以上（不含 3,000 萬元）7.91%

參、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〈法務部調查局洗錢防制處作業要點〉（法務部 100 年 7 月 14 日法檢第 1000804273 號函同意備查）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。106 年度共受理申報 3,543,807 件，依申報機構、申報金額等進行統計及分析，其中，本國銀行申報件數約 77.98%，交易金額爲 50 萬元至 100 萬元間之交易則佔 73.69%；106 年度受理查詢大額通貨交易之件數爲 59,382 件（詳細統計及分析情形詳表 8 至表 11 及圖 F）。

一、大額通貨交易申報情形

表 08：106 年申報大額通貨交易件數統計表

申　報　機　構	件　數
本國銀行	2,763,529
外國銀行	16,240
大陸銀行	1
信託投資公司	0
信用合作社	146,835
農、漁會信用部	29,5670
中郵儲匯處	313,551
保險公司	7,940
銀樓業	32
電子支付及電子票證機構	9
	合計：3,543,807

表 9：近 5 年大額通貨交易申報件數統計表

年　　度	102 年	103 年	104 年	105 年	106 年
件數統計	3,995,726	4,107,745	3,934,708	3,712,685	3,543,807

二、大額通貨交易申報金額分布

表 10：106 年申報大額通貨交易金額統計表

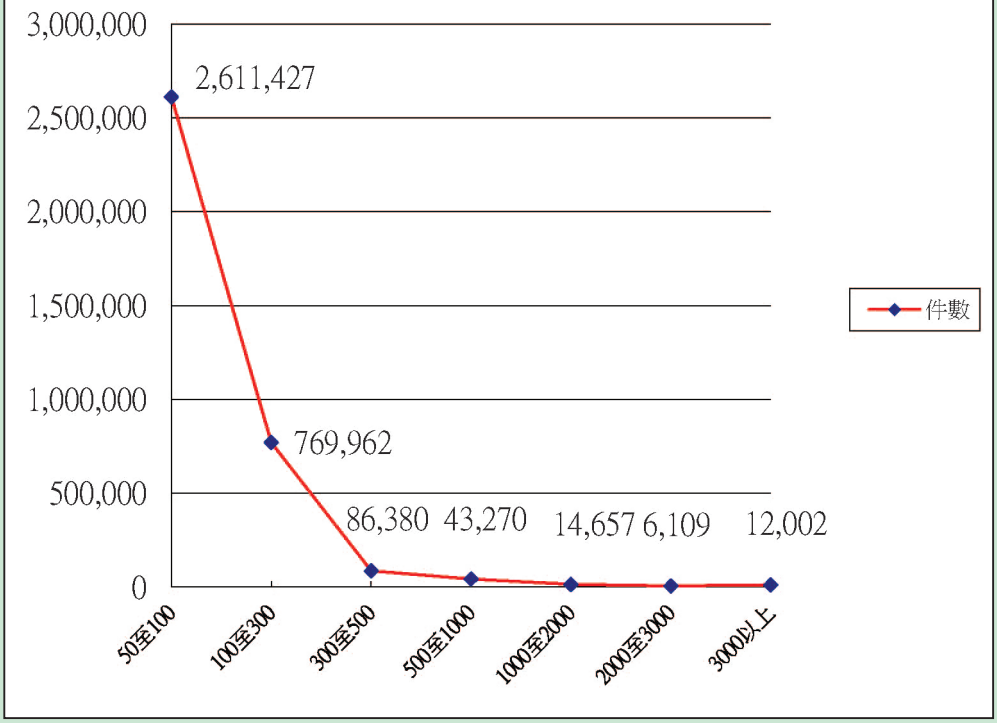
金　　額	件　　數
50 萬元至 100 萬元（含 50 萬元）	2,611,427
100 萬元至 300 萬元（不含 100 萬元）	769,962
300 萬元至 500 萬元（不含 300 萬元）	86,380
500 萬元至 1000 萬元（不含 500 萬元）	43,270
1000 萬元至 2000 萬元（不含 1000 萬元）	14,657
2000 萬元至 3000 萬元（不含 2000 萬元）	6,109
3000 萬元以上（不含 3000 萬元）	12,002
合計：3,543,807	

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	102 年	103 年	104 年	105 年	106 年
法務部調查局	28,205	61,092	36,040	21,413	32,402
其他執法機關	133	10,262	5,641	13,012	17,929
司法機關	16,010	16,635	8,987	5,186	9,051
筆數統計	55,368	88,464	50,668	39,611	59,382

圖 F：106 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） 73.69%
☐ 100 萬元至 300 萬元（不含 100 萬元） 21.73%
☐ 300 萬元至 500 萬元（不含 300 萬元） 2.44%
☐ 500 萬元至 1,000 萬元（不含 500 萬元） 1.22%
☐ 1,000 萬元至 2,000 萬元（不含 1,000 萬元） 0.41%
☐ 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） 0.34%

肆、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。」

另依〈洗錢防制物品出入境申報及通報辦法〉第 3 條規定，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」。106 年度海關受理申報後再向本局通報共 45,165 件，其中 81.41% 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 G）。

一、通報件數

表 12：106 年通報件數統計表

出、入境	件數
入境	39,213
出境	5,952
合計	45,165

表 13：近 5 年通報件數統計表

年　度	102 年	103 年	104 年	105 年	106 年
件數統計	14,273	18,781	27,725	33,555	45,165

二、通報資料月份分布

表 14：106 年各月份通報統計表

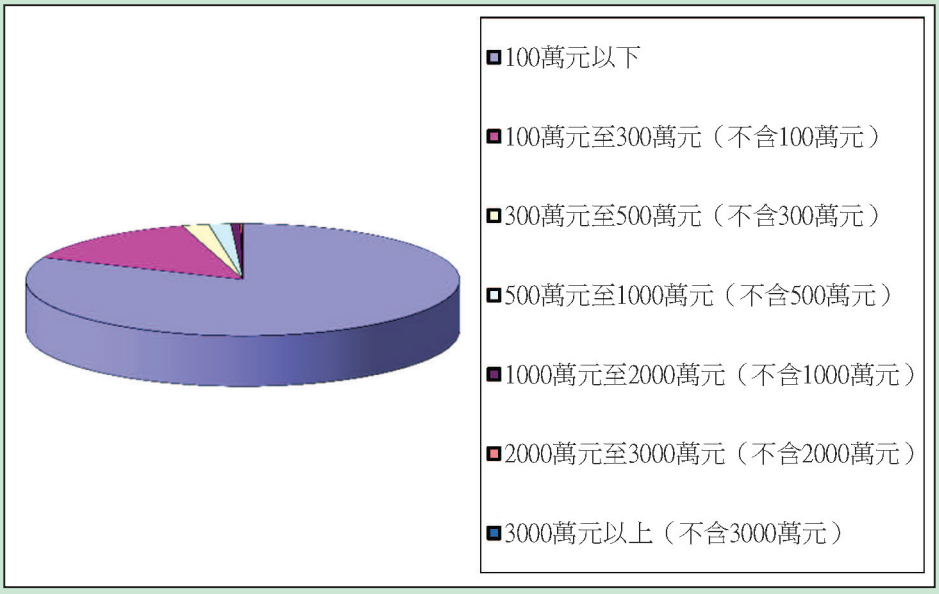
月份	1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
件數	2,575	2,633	3,077	4,154	4,154	3,710	4,537	3,784	3,960	4,583	4,499	3,499

三、通報資料金額分布

表 15：106 年通報金額統計表

金　　額	件　　數
100 萬元以下	36,769
100 萬元至 300 萬元（不含 100 萬元）	6,350
300 萬元至 500 萬元（不含 300 萬元）	892
500 萬元至 1000 萬元（不含 500 萬元）	740
1000 萬元至 2000 萬元（不含 1000 萬元）	315
2000 萬元至 3000 萬元（不含 2000 萬元）	48
3000 萬元以上（不含 3000 萬元）	51
合計：45,165	

圖 G：106 年通報金額分析圖



- ☐ 100 萬元以下 81.41%（含 100 萬元）
- ☐ 100 萬元至 300 萬元（不含 100 萬元） 14.06%
- ☐ 300 萬元至 500 萬元（不含 300 萬元） 1.97%
- ☐ 500 萬元至 1,000 萬元（不含 500 萬元） 1.64%
- ☐ 1,000 萬元至 2,000 萬元（不含 1,000 萬元） 0.07%
- ☐ 2,000 萬元至 3,000 萬元（不含 2,000 萬元） 0.10%
- ☐ 3,000 萬元以上（不含 3,000 萬元） 0.11%

伍、起訴案件統計

經透過法務部檢察書類檢索系統，針對全國各地方檢察署援引洗錢防制法第 14 條及 15 條等洗錢罪起訴（含緩起訴及聲請簡易判決）案件之前置犯罪類型、罪名、洗錢金額、洗錢管道、洗錢方法及被告資料等，列入統計並加以分析，俾瞭解 106 年度我國有關洗錢犯罪之概況及趨勢。106 年度洗錢罪起訴案件共 41 件，洗錢金額總計為 19 億 6,085 萬 1,978 元（詳細統計及分析情形詳表 16 至表 20 及圖 H）。

一、洗錢案件類型

表 16：106 年洗錢罪案件類型、罪名及移送（偵查）機關統計表

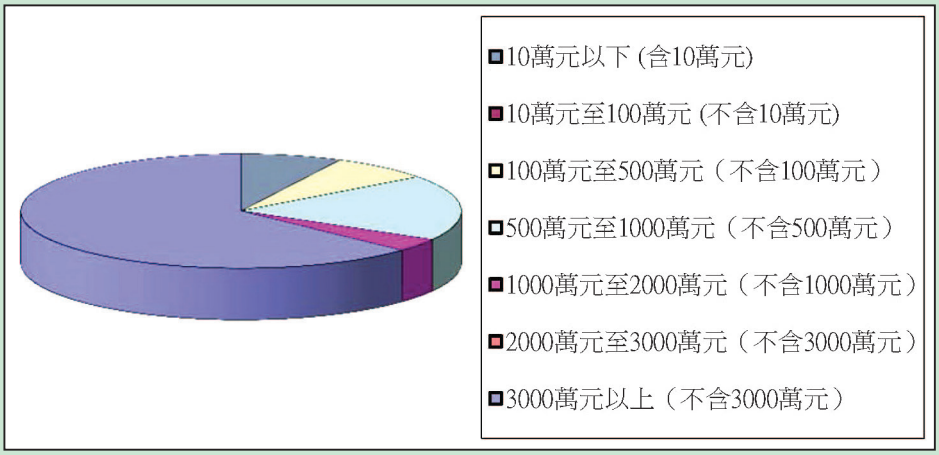
犯罪類型	罪名	調查局	地檢署	警政署	特偵組	總計
一般刑案	賭博	0	1	1	0	2
一般刑案合計		0	1	1	0	2
毒品犯罪	毒品	0	0	1	0	1
毒品犯罪	合計	0	0	1	0	1
貪污犯罪	貪污治罪條例	0	0	0	2	2
貪污犯罪合計		0	0	0	2	2
經濟犯罪	詐欺	1	0	29	0	30
	詐欺、贓物	0	0	1	0	1
	銀行法	1	1	3	0	5
經濟犯罪合計		2	1	33	0	36
總　　計		2	2	35	2	41

二、洗錢案件金額分布

表 17：106 年洗錢罪案件洗錢金額統計表

金　　額	件　　數
10 萬元以下 (含 10 萬元)	10
10 萬元 ～ 100 萬元 (不含 10 萬元)	15
100 萬元 ～ 500 萬元 (不含 100 萬元)	2
500 萬元 ～ 1000 萬元 (不含 500 萬元)	1
1000 萬元 ～ 2000 萬元 (不含 1000 萬元)	2
2000 萬元 ～ 3000 萬元 (不含 2000 萬元)	3
3000 萬元以上 (不含 3000 萬元)	8
合計：41	

圖 H：106 年洗錢罪案件洗錢金額分析圖



☐ 10 萬元以下 (含 10 萬元) 7.14%
☐ 10 萬元至 100 萬元 (不含 10 萬元) 0%
☐ 100 萬元至 500 萬元（不含 100 萬元） 10.71%
☐ 500 萬元至 1000 萬元（不含 500 萬元） 17.86%
☐ 1000 萬元至 2000 萬元（不含 1000 萬元） 3.57%
☐ 2000 萬元至 3000 萬元（不含 3000 萬元） 0%
☐ 3000 萬元以上（不含 3000 萬元） 60.71%

三、洗錢案件使用之管道與方法

表 18：106 年洗錢罪案件洗錢管道統計表

洗錢管道類型	件數
其他	4
銀行	37
	合計：41

表 19：106 年洗錢罪案件洗錢方法統計表

洗錢方法	件數
人頭帳戶	27
地下通匯	3
其他	4
國外匯款	1
寄藏友人	4
親屬帳戶	2
合計	41
	合計：41

四、洗錢案件發生地區

表 20：106 年洗錢罪案件發生地區分布統計表

交易地區	件數	交易地區	件數
花蓮縣	1	彰化縣	4
金門縣	1	臺中市	10
桃園市	12	臺北市	8
高雄市	1	臺東縣	2
新竹縣	1	臺南市	1
			合計：41

陸、教育訓練與宣導

一、防制洗錢宣導

本局各外勤處站對外宣導保防、廉政及洗錢防制工作，係以公益性活動場合爲主，對象爲機關團體、學校、民間團體等單位，以輕鬆活潑等方式，介紹洗錢防制工作的範疇，讓民眾了解洗錢之危害性及洗錢防制工作之重要性。

本局高雄市調查處於「高雄科技大學實習及就業博覽會」辦理洗錢防制工作宣導

■ 本局福建省調查處於「小麥石蚵文化季活動」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，以協助金融機構或特定非金融專業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，並遵守洗錢防制法相關規定，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，闡明可疑交易之模式係屬何種類型交易，如地下通匯、操縱股價、內線交易、企業掏空、詐欺及網路賭博等類型交易，此種分享對於金融機構人員在經驗累積及申報品質上產生極佳的效果，有助於提升金融機構申報可疑交易報告之水準。

表 21：106 年協助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）	48	3,220
	外商銀行	4	118
	大陸銀行	2	50
信用合作社		4	310
農漁會信用部		3	414
證券投資信託		2	76
證券業		6	650
期貨業		0	0
辦理儲金匯兌之郵政機構		0	0
保險業		14	991
票券金融公司		0	0
其他金融機構		3	322
合計		86	6,151

柒、國際合作

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。」

表 22：近 5 年從事國際合作之情資交換統計表

事　　項	年度	102 年	103 年	104 年	105 年	106 年
外國請求我國協查	案	41	32	51	50	55
	件	113	89	152	169	161
我國請求外國協查	案	17	18	45	34	26
	件	62	67	222	165	94
外國主動提供情資	案	17	33	32	25	53
	件	39	58	44	44	100
我國主動提供情資	案	4	6	9	26	45
	件	11	13	18	45	94
問卷及其他事項	案	0	0	0	0	0
	件	100	85	201	262	354
小　　計	案	79	89	137	135	179
	件	325	312	637	685	803

二、與外國金融情報中心簽署瞭解備忘錄（或協定）

洗錢犯罪常爲跨國性的犯罪，爲有效打擊跨國洗錢犯罪、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，本局扮演我國金融情報中心角色，在國際合作防制洗錢方面不遺餘力。我國於 106 年先後與聖露西亞、匈牙利、教廷、拉脫維亞、迦納簽訂「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」，迄 106 年 12 月 31 日，已與 44 個國家或地區簽署此類備忘錄或協定。

106 年 5 月 15 日，本處李處長（左二）於我國駐教廷大使李世明（中）見證下，與教廷金融資訊處處長盧薩（Tommaso Di Ruzza，右二）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」

三、辦理國際講習課程

聖文森金融情報中心副處長森蒂（LaTeisha Arielle Rachael Sandy）率該國金融調查官來臺參訪，本局受我國外交部委託，於 106 年 10 月 18

日至 20 日辦理防制洗錢講習課程，就我國 FIU 運作、可疑交易申報與大額通貨申報、財政部關務署通報資料等之受理、分析及運用、分送進行簡報，並邀請相關單位，簡介法務部調查局國際合作事項，以及偵辦毒品犯罪、貪瀆與經濟犯罪案件之資金清查實務。由於本次聖文森參訓之金融調查官多係警職轉任，具備執法經驗，雙方亦就 FIU 與執法機關之角色與合作交換意見。

106 年 10 月 18 日至 20 日聖文森金融情報中心副處長森蒂（LaTeisha Arielle Rachael Sandy，右一）與該國參訓之金融調查官

第三部分

重要案例

壹、甲公司蔣○○等人涉嫌違反證券交易法等案

貳、乙公司徐○○等人涉嫌短漏贈與稅案

參、丙公司吳○○等人涉嫌違反銀行法等案

肆、丁集團陳○○等人涉嫌違反銀行法及洗錢防制法等案

伍、陳○○目標性金融制裁案

壹、甲公司蔣○○等人涉嫌違反證券交易法等案

一、案情概述

（一）案件來源

本局於 103 年 12 月間受理 A 銀行金融情資分析後發現：石○○代理甲公司臨櫃提領大額現金新臺幣（下同）2,400 萬元，表示係爲購買辦公大樓使用，惟石○○並非甲公司員工。同期間，甲公司員工張○○亦經常有大額提現情形，交易疑有異常。

（二）涉案人

甲公司實際負責人蔣○○、公司秘書張○○、員工陳○○等。

（三）涉案情形

蔣○○爲係股票上市公司甲公司實際負責人，爲調度資金，蔣○○自 103 年起陸續向多家銀行貸款，並以所持有之甲公司股票爲擔保，以每股約 30 餘元價格向銀行設質借款。蔣○○等人拉抬甲公司股價，藉以活絡股票交易量，以利出脫持股獲利，另爲維持甲公司股價，以免高額貸款遭銀行徵提擔保品、追繳或股票遭斷頭，蔣○○竟指示員工張○○、陳○○等多人，並結合股市炒手許○○，共同基於操縱甲公司股價以牟取不法利益之犯意聯絡，利用丙公司、陳○○及石○○配偶等共 34 人之證券帳戶，蔣○○、許○○等並指示張○○、石○○等人進行資金調度，於 103 年 5 月 1 日至 104 年 12 月 31 日期間（合計 415 個營業日），於 405 個營業日進行大量集中且反覆下單交易，合計買入、賣出數量佔該期間甲公司股票市場總成交量之 29.07% 及 26.66%，其中 313 個營業日之買進或賣出數量逾當日市場成交量 20%，同時在 321 個營業日內於上開帳戶內進行相對成交，總計相對成交 8 萬 2,930 仟股，占該期間市場總成交量之 13.46%，藉以製造交易活絡表象，再以連續高於揭示成交價之高價買入方式，直接或間接從事影響甲公司股價，致甲公司股價於該期間漲幅 128.98%。105 年間亦有相同之人爲操縱

股價事實，蔣○○等人因而獲得不法利得共計1億9,450萬8,502元。

二、可疑洗錢表徵

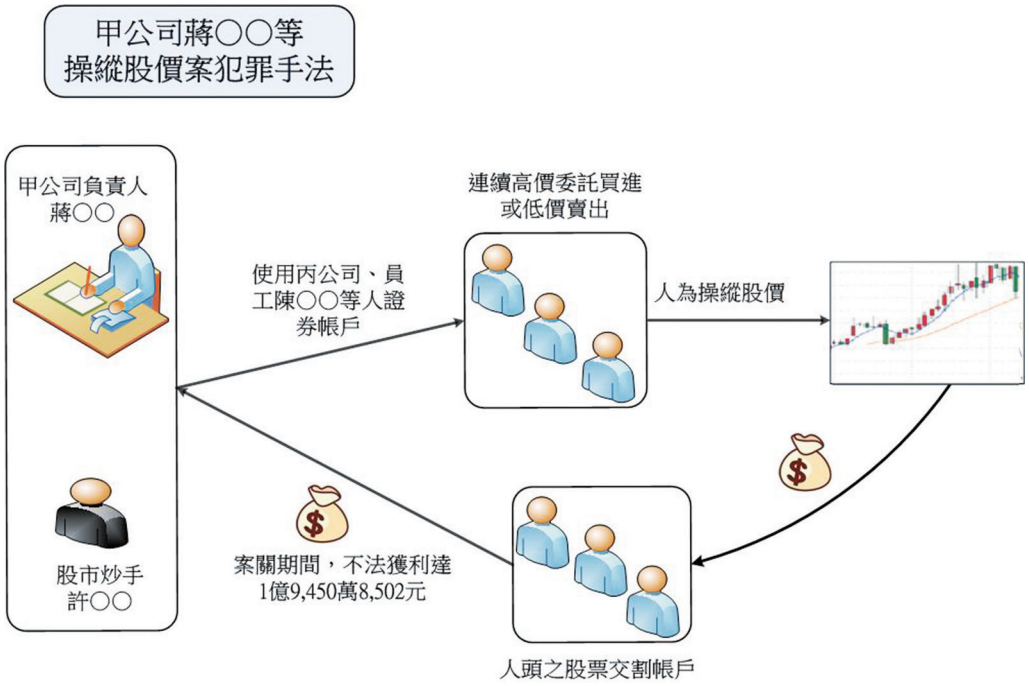
客戶突然提領大額現金，欲阻斷資金來源，符合洗錢表徵。

三、起訴情形

臺灣臺北地方檢察署於106年9月間，以違反證券交易法第155條第1項第4款、第5款對於證券交易所上市有價證券操縱股價等罪嫌起訴蔣○○等人。

四、經驗參考

A銀行警覺客戶交易習慣改變及有大額現金提款，立即申報並持續提供相關交易對象之金融情資，本局因而得於犯罪行為發生時，透過追查金流，勾稽出蔣○○用以買賣操縱該公司股價之投資人集團，同時掌握案關對象金流，使偵辦單位能據以展開偵辦作為。另各金融機構於媒體新聞報導後，亦即刻申報相關人之可疑交易報告，對於後續偵辦作為具有相當之助益。



貳、乙公司徐○○等人涉嫌短漏贈與稅案

一、案情概述

（一）案件來源

本局於 106 年 8 月間受理 B 公司金融情資分析後發現：乙公司向 B 公司之國際保險業務分公司（Offshore Insurance Unit，下稱 OIU）投保美元終身壽險，被保險人係乙公司董事長徐○○之特別助理丙，投保金額美金 383 萬 4,000 元，保費達美金 399 萬 9,740 元。而公司爲職員投保如此高額之保險似不符常情。

（二）納稅義務人

乙公司負責人徐○○之配偶。

（三）涉案情形

賽席爾（SEYCHELLES）商乙公司負責人係我國國民徐○○，唯一股東即徐○○之配偶，該公司實際營業處所設於日本東京，以國際貿易爲主要營業項目。106 年 8 月初，乙公司爲該公司董事長特別助理丙女（日本籍）投保美金 383 萬 4,000 元之 OIU 美元終身壽險，一次躉繳保費美金 399 萬 9,740 元，全數由乙公司負責人徐○○之配偶自 X 國 C 銀行匯至 B 公司設於我國之銀行帳戶。

徐○○爲其日本籍助理丙投保高額保險之行爲似悖於常情，經清查發現，丙女具我國及日本之雙重國籍，實爲徐○○長女，顯見徐○○刻意隱匿渠與丙之親屬關係，再利用境外公司名義，爲擁有雙重國籍之長女投保高額 OIU 保單，並以其自有資金自境外金融機構繳納保費，意圖規避贈與稅。

二、可疑洗錢表徵

其他符合疑似洗錢表徵之交易。

三、裁罰情形

國稅局核定徐○○之配偶（實際繳納保費者）106 年之贈與總

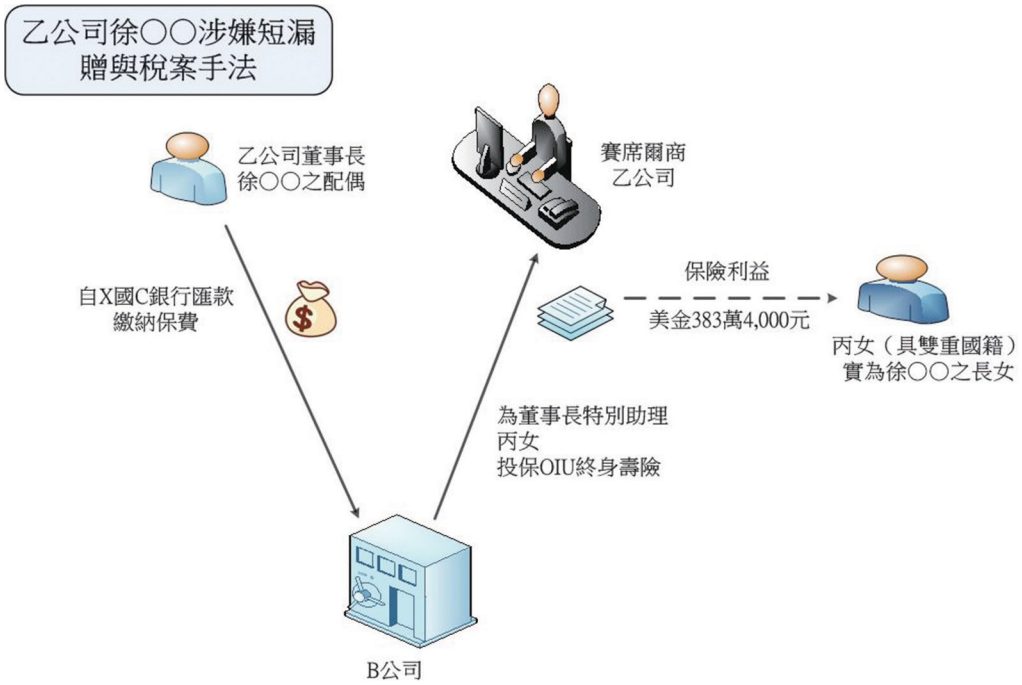
額爲 1 億 2,111 萬 2,127 元，應補繳稅額共計 2,047 萬 3,570 萬元，徐○○之配偶業已全數繳納完竣。

四、經驗參考

（一）我國自 104 年開放 OIU 業務，雖規定要保人須爲中華民國境外之自然人、法人，被保險人須爲中華民國境外自然人，惟要保人、被保險人仍能以境外紙上公司、雙重國籍等方式規避前揭投保限制，藉以逃漏稅賦或隱匿不法資金，故保險公司宜謹慎查核客戶背景、相互關係、交易原因及資金來源等，避免 OIU 產品遭利用爲洗錢工具。

（二）本保單係由要保人乙公司爲助理丙投保高額壽險，顯不符常理，保險公司宜審慎核保並主動申報，以利後續查處作爲。

（三）新修訂之洗錢防制法已將稅捐稽徵法第 41 條、第 42 條及第 43 條第 1 項、第 2 項之罪納入特定犯罪，未來金融機構應更加重視疑似逃漏稅捐之相關異常交易型態。



參、丙公司吳○○等人涉嫌違反銀行法等案

一、案情概述

（一）案件來源

本局於 104 年 3 月間受理金融情資分析後發現，丙公司員工洪○○，頻繁於關係企業丁公司設於 C 銀行帳戶提存大額現金，該帳戶每日維持相同餘額，交易型態異常；另丙公司員工有積極遊說民眾參與投資行為，經營型態可疑。

（二）涉案人

周○○、吳○○及陳○○等人。

（三）涉案情形

周○○明知非銀行不得經營收受存款，亦不得以借款、收受投資、使加入為股東或其他名義，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、利息、股息或其他報酬，竟貪圖不法利益，於 102 年 8 月至 105 年 12 月間，與吳○○、陳○○等人，共同籌組丙投資控股股份有限公司，以及丁、戊公司等諸多關係企業，在未經主管機關核准下，假藉「雜項費」、「顧問費」及「保管費」等名目，給付年利率 14.34% 至 220.8% 不等之顯不相當報酬，並透過高額獎金之多層次行銷網絡，以及辦理說明會或參觀旅遊等公開活動，公然以股票質押借款、附買回交易等方式，包裝吸金事實，投資專案包括「T1」、「T2」、「T3」、「A1」、「M1」及「○○電子商務」等，向不特定大眾違法吸收存款。且周○○、吳○○及陳○○亦明知除政府債券或經財政部核定之其他有價證券外，非經主管機關金管會核准或向主管機關申報生效後，不得為之，竟共同基於非法發行有價證券之犯意聯絡，於招攬投資時，交付丙公司及其關係企業之股票。

另為取信投資人，周○○支付報酬使 2 共犯更名，將渠等姓名變更與股票上櫃公司○○科技之董事長、董事相同，進而向投資人

誆稱○○科技已與丙公司合作，致不特定投資人陷於錯誤，而參與投資，吸金總額超過 44 億 1,432 萬 6,400 元，上開不法所得除給付後期投資人紅利、公司幹部酬勞之外，周○○等人另以購置房屋、土地等不動產，有價證券與車輛。

105 年 12 月 13 日起，本局臺北市調查處依檢方指揮，執行數次之搜索、拘提及扣押，當場查扣現金 6,453 萬 4,500 元及進口轎車 2 輛，繼而依蒐獲證據，聲請法院裁定凍結 359 個金融帳戶（存款餘額合計 3,584 萬 3,000 元）與有價證券 1 萬 4,051 仟股（價值約 1 億 2,000 萬元），以及 145 筆不動產（含土地及地上物），扣押物總價值逾 18 億元。

二、可疑洗錢表徵

存款帳戶頻繁大額現金交易，且存、提金額相當同時相距時間不久;經常有大額款項匯入後，立即以大額或分散方式提領現金，僅留下象徵性餘額，其款項與客戶之身分、收入顯不相當或本身營業性質無關者。

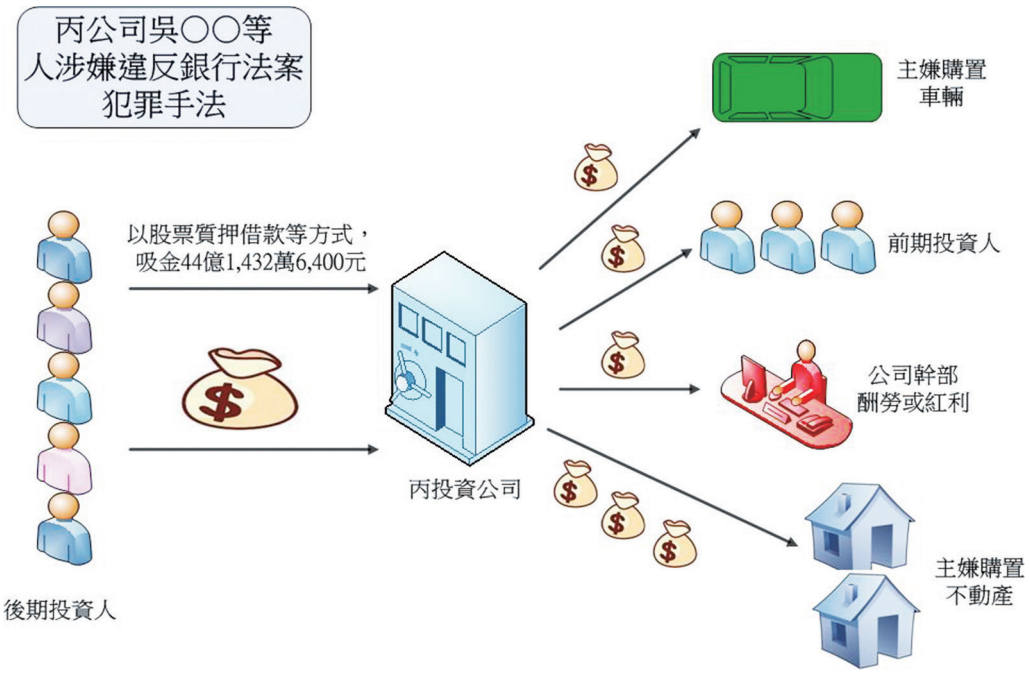
三、裁罰情形

臺灣新北地方檢察署於 106 年 3 月間，以違反銀行法、證券交易法及刑法詐欺等罪嫌，起訴吳○○及陳○○等人，並對周○○發佈通緝。

四、經驗參考

（一）C 銀行對於代交易人頻繁提領現金之交易型態保持警覺，並落實客戶審查作為，主動拜訪此類風險程度較高之客戶，深入了解客戶營業活動，作為研判交易是否疑係洗錢型態之參考。

（二）本案經媒體報導後，各金融機構亦即刻申報相關資料，對於後續偵辦作為有相當之助益。


丙公司吳○○等
人涉嫌違反銀行法案
犯罪手法
主嫌購置
車輛
以股票質押借款等方式，
吸金44億1,432萬6,400元
前期投資人
公司幹部
酬勞或紅利
丙投資公司
主嫌購置
不動產
後期投資人

肆、丁集團陳○○等人涉嫌違反銀行法及洗錢防制法等案

一、案情概述

（一）案件來源

本局於 105 年 8 月起陸續接獲金融情資分析後發現：李○○、丁集團 A 造船公司，及無公司營運資訊之 L3 境外公司有異常大額外匯交易往來情形，依交易對象及交易金額，與李○○身分及收入顯不相當，或與渠營業性質無關，交易型態似有異常。

（二）涉案人

陳○男、簡○○、陳○志、陳盧○○及李○○等人。

（三）涉案情形

陳○男係丁集團總裁，負責該集團及集團旗下關係企業整體營運決策；簡○○係丁集團前任執行長（100 年至 104 年 10 月期間）；陳○志係陳○男次子，爲丁集團 A 造船公司副董事長，以及 AZ、OK、L3、HS 及 QY 等 5 境外紙上公司之登記負責人；陳盧○○係陳○男配偶，爲丁集團 B 投資公司、C 水產公司登記負責人及 A 造船公司董事；李○○係 A 造船公司顧問（104 年 10 月至 105 年 12 月止），負責協助陳○志處理集團財務調度事宜。

A 造船公司於 103 年 10 月 23 日標得我國 X 部門公共工程標案，應於期限內完成建造「○○艦」6 艘並交艦，同年 11 月 3 日與 X 部門簽署「○○艦」合約，總價爲 349 億 3,300 萬元，陳○男、陳○志、陳盧○○遂以 A 造船公司名義取得標案。惟 A 造船公司資本額僅 5 億 3,000 萬元，且該集團於大陸地區另有其他投資，資金嚴重短缺，恐難因應聯合授信銀行團對自有資本之授信審查，陳○男等人明知公司法規定股東對於公司應收之股款應實際繳納，竟仍共同基於違反公司法等犯意聯絡，自 103 年 11 月間起，先後 3 度以不實文件進行虛僞增資，將 A 造船公司實收資本額 5 億 3,000 萬

元陸續增資至 40 億元，藉此陷聯合授信銀行團（含主辦行 F 銀行，共 9 家銀行）於錯誤，而於 105 年 2 月 4 日核准總金額 205 億元之聯合授信額度。

事後，陳○男、陳○志、陳盧○○再基於詐欺取財之共同犯意，於無實際交易下，僞造陳○志設立之AZ、OK、L3、HS及QY等境外公司出售標案相關設備予A造船公司之虛僞採購合約、商業發票、付款申請書等不實交易憑證，向各家銀行申請過渡性融資貸款、撥款，及向聯合授信銀行團管理銀行F銀行○○分行申請動撥款項，致各家銀行承辦人陷於錯誤而核准並動撥款項，渠等分於104年間向Z銀行、F銀行等4家銀行詐取過渡性融資5次，共取得美金6,766萬元；105年3至5月間再向聯合授信銀行團詐取「乙項授信額度（購料周轉金）」共美金5,800萬元；105年間又向聯合授信銀行團詐取「建造專戶」購料周轉金共7,633萬3,020美元。

二、可疑洗錢表徵

開戶後立即有與其身分、收入顯不相當或與本身營業性質無關之大額款項存、匯入，且又迅速移轉者。

三、起訴、判決情形

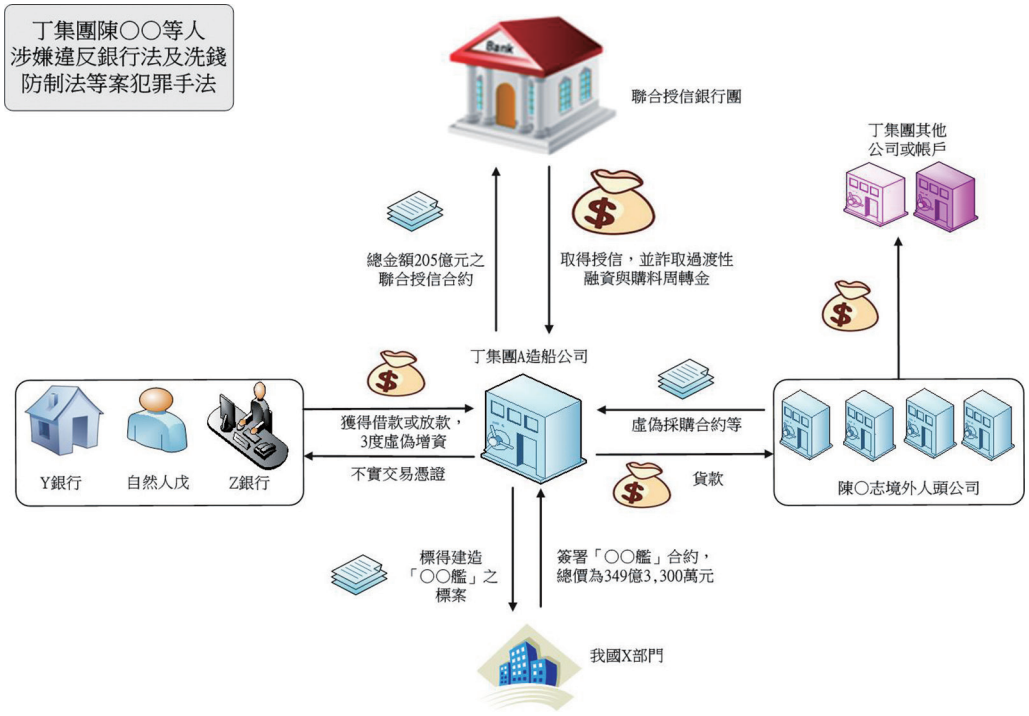
臺灣高雄地方檢察署於 107 年 2 月間，以違反公司法、商業會計法、刑法及洗錢防制法等罪嫌，起訴陳○男等人。

四、經驗參考

（一）犯罪者常利用設立人頭公司或與境外第三方進行假交易，並透過 OBU 帳戶移轉資金，藉此掩飾或隱匿不法犯罪所得。鑑於 OBU 客戶主要爲境外法人或自然人，交易之實質受益人不易辨識，且多來自避稅天堂之國家或地區，並透過網路銀行等非面對面之交易或服務，亟與洗錢或資恐活動相關，經我國評列爲防制洗錢及資恐非常高風險之產業弱點。金融機構如於加強審查客戶身分及交易資訊後，仍無法釐清交易合理性，且客戶又不願提供實質受

益人及交易內容相關資訊以供核實，金融機構應主動申報。

（二）金融機構於辦理授信、貸款及貸後管理等業務上，宜從客戶與交易往來對象之背景資料、營業地址、實際負責人、營業事實、契約內容、交易憑證實質內容（如簽名人員相關資料）、入帳帳戶與賣方之關係等面向，加強審查客戶實質受益人及交易眞實性。



伍、陳○○目標性金融制裁案

一、案情概述

（一）案件來源

106 年 12 月 29 日媒體披露，香港註冊貨輪「○○永嘉號」（○○ Winmore）因於公海駁油予北韓船舶，遭南韓政府查扣，而租用該貨輪之 B ○○ Group Corporation 負責人為我國商人陳○○，各金融機構旋即申報陳○○及其掌控境外公司之可疑交易報告。

（二）涉案人

陳○○。

（三）涉案情形

國人陳○○所經營境外公司馬紹爾群島商 B ○○ Group Corporation，租賃香港籍油輪○○永嘉號，因在東海海域駁油予北韓籍船隻，違反聯合國安全理事會第 2375（2017）號決議，遭南韓政府查扣調查，南韓外交部則於 106 年 12 月 29 日發佈新聞。

中外媒體披露消息後，國內各金融機構迅速申報陳○○及其掌控之境外公司可疑交易報告，經本處分析、彙整後發現，由陳○○ 100%控股之境外公司包括英屬維京群島商○○ Taiwan Group Corporation，以及馬紹爾群島商 B ○○ Group Corporation、○○ Enterprise Co., Ltd.、○○ Corporation Peru S.A.C. 等 4 家；其中○○ Taiwan Group Corporation 所有之權宜籍油輪比○○ 18 號亦因駁運油品予北韓船隻，於 106 年 12 月 28 日即經聯合國第 1718 號有關北韓違反武擴制裁委員會公告違反聯合國安理會第 2375（2017）號決議，籲請會員國對該船採取聯合國安理會第 2371（2017）號決議第 6 段禁止入港措施，故比○○ 18 號船東陳○○暨英屬維京群島商○○ Taiwan Group Corporation 違反聯合國安理會決議事證明確。

經主管機關法務部於 107 年 1 月 12 日邀集相關機關代表，召開「資恐防制審議會」，公告指定制裁對象陳○○及擔任負責人之○○ Taiwan Group Corporation、B ○○ Group Corporation，該公告同時確查○○ Enterprise Ltd.、○○ Corporation Peru S.A.C. 亦以陳○○爲實質受益人，要求對前開陳員 1 人暨 4 家境外公司依資恐防制法第 7 條第 1 項規定採取措施。遭公告制裁後，陳○○及前揭 4 家境外公司名下所有資產應予凍結。

臺灣高雄地方檢察署同時指揮本局航業調查處，針對前揭陳○○名下公司持有之船隻駁油予北韓是否涉及僞造文書等進行調查。

二、可疑洗錢表徵

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

（二）貨物運至或來自洗錢或資恐高風險國家或地區。

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

三、經驗參考

（一）陳○○名下○○ Taiwan Group Corporation 等 4 家境外公司，在數家金融機構開立不同 OBU 帳戶，金融機構於申報時，皆完整提供境外公司註冊證書、股東及董事名冊等，有助於釐清陳○○名下境外公司之設立情形與資金往來狀況。

（二）公告制裁後，金融機構迅速依資恐防制法第 5 條第 1 項及第 2 項規定，通報經指定制裁之個人、法人或團體之財物或財產上利益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，本局依法受理通報並檢視、彙整相關資料，俟彙整完畢後檢陳法務部及相關權責機關參處。

（三）本案爲我國資恐防制法公告實施以來首宗案例，各金融機構於消

息披露後主動申報可疑交易報告、於公告制裁後立即通報經指定制裁對象之財物或財產上利益，且與本局承辦人保持聯繫，協助提供相關資料文件，對於後續偵處及相關金流分析，有莫大助益。

第四部分
專題研究

涉及虛擬貨幣洗錢之資金清查作爲——兼論比特幣之搜索扣押

Funds Investigation Concerning the Virtual Currency with the Procedure of Searching and Seizing Bitcoin Wallets

蘇文杰[1]

摘　要

金融海嘯發生後，區塊鏈之問世帶動許多經濟需求，比特幣作爲應用最成熟的虛擬貨幣，扮演著不可缺的角色，惟其匿名性與全球流通性亦爲犯罪者所喜好；比特幣便捷又快速的支付與交易，與傳統的銀行匯款或地下匯兌方式大相逕庭，甚至造成刑事偵查上資金追蹤之斷點，成爲全球洗錢防制工作不可小覷之風險。本文嘗試從風險管控之角度切入，輔以國內外辦案實務所遭遇之困境與對策，本著科技實證之精神，探討比特幣等虛擬貨幣之搜索扣押程序，並研提因應作爲與建議方向，俾利國內相關執法機關偵查程序之參考。

關鍵字：洗錢（Money Laundering）、扣押（Seizure）、比特幣（Bitcoin）、虛擬貨幣（Virtual Currency）、刑事偵查（Criminal Investigation）

[1] 國立交通大學科技法律學院科技法律研究所碩士，目前任職法務部調查局台北市調查處，曾任洗錢防制處調查官。

壹、背景緣起

5年前，區塊鏈（Blockchain）、比特幣（Bitcoin）等名詞還鮮爲人知，近年來隨著比特幣的價值高漲與廣泛使用，比特幣等虛擬貨幣逐漸進入大眾生活，一般民眾對於比特幣、挖礦[2]、礦工等相關名詞日漸耳熟能詳，且相關應用正在快速普及，故比特幣、首次代幣發行（ICO）[3]、區塊鏈技術等專有名詞逐漸充斥於日常生活。由於比特幣漲勢凌厲，投資者熱衷鑽研如何藉由投資虛擬貨幣而獲利，各種虛擬貨幣投資之廣告亦在網路上隨處可見[4]。在此等科技新興領域，法規監管、如何投資、交易平台，以及相關退場機制，包括產生投資糾紛時如何解決，以及司法途徑是否能夠提供協助等，種種法律議題應運而生，衝擊目前的社會制度與秩序。

這類因新興科技而產生的議題，法規制度尚未完全符合科技應用之發展速度，但在眞實生活中，各種探討虛擬貨幣與區塊鏈技術之相關學術研究與商業運用，正如火如荼、如雨後春筍般展開。尤其，比特幣及區塊鏈最初始和最成熟的應用，即是隱匿金流之追蹤，此一特點遭不法集團或個人所覬覦。美國知名案例即係絲路網路（Silk Road），此一主要從事軍火、毒品、色情及人口販賣等不法事項交易的網站，正因採用比特幣支付交易而難以追查，當時此類新興支付工具尚未廣爲人知，故成爲網站接受付款之首選。該網站已遭美國聯邦調查局（Federal Bureau of Investigation，下稱 FBI）偵辦並下架，且扣押網站負責人所有之比特幣約 17.5 萬枚，約佔當時全球比特幣存量之 2%。

追查不法所得向來是我國刑事偵查之重點，我國法令近年來已與

[2] 根據「Bitcoin Energy Consumption Index」統計，截至 2017 年 11 月 20 日，比特幣過去 1 年挖礦的電力總消耗已累計達 29.51 兆瓦 / 小時（TWh），約占全球總電力消耗的 0.13%，相當於臺灣 1 年電力消耗之 11.64%；若全球的比特幣礦工自成 1 國，該國的電力消耗排名可排到全球第 61 名。另據統計，全球挖礦每年的成本約為 15 億美元，但營收則高達 72 億美元。

[3] ICO － Initial Coin Offering，意即「虛擬貨幣首次公開募資」，概念源自股票市場之 IPO，係指企業或非企業組織在區塊鏈技術的支持下發行代幣，向投資人募集虛擬貨幣（一般為比特幣、乙太坊）之融資活動。差異在於，IPO 係企業為了發展而向公眾發行股票以籌集資金，ICO 係企業為了發展而向公眾籌集資金，將發行的標的由有價證券轉變成虛擬貨幣。

[4] 目前谷歌（Google）、推特（Twitter）及臉書（Facebook）都禁止虛擬貨幣相關廣告。

國際規範同步接軌，惟涉及虛擬貨幣之洗錢、吸金或詐欺等犯罪案件，仍因比特幣之匿名性與流通性，衍生偵查盲點，往往需透過國際合作（如歐洲刑警組織 (Europol) 之歐洲網路犯罪中心 (European Cybercrime Center)，下稱 EC3[5]）或企業互助方式，始得釐清交易來由及去向。但在此之前，執法機關尚面臨另一難題，即在犯罪現場如何扣押虛擬貨幣，如何說服涉嫌人合作交出私鑰，並防止第三人透過已知之私鑰於執法者完成扣押前就將比特幣移轉至其他錢包，以本局於 2018 年 6 月中旬偵破史上最大比特幣吸金案爲例，跨國集團非法吸金逾 15 億元，即使執行前已進行數次沙盤推演，但如何於短時間內有效扣押超過數百枚之比特幣，仍是執法人員的一大考驗。由此可知，實務運作中已發生法律爭議與偵查困境，執法機關必須及早面對，方能有效執法，因此本文重點除介紹基於區塊鏈基礎上比特幣交易之新興議題外，更深入探討執法機關在搜索扣押現場面對案關比特幣等虛擬貨幣應有之對策，並針對扣押流程及數位鑑識工具提出淺見，綜合 FBI、EC3 及本局應對實務案例之作法，期能提出有效作法供國內相關執法機關參考。

[5] EC3，歐洲網路犯罪中心 (European Cybercrime Centre，簡稱 EC3) 成立 2013 年，位置設在荷蘭海牙 (Hague) 的歐洲刑警組織 (Europol) 總部內，專門協調跨國辦案，同時也是電腦犯罪及虛擬貨幣犯罪等專業領域之技術顧問。

貳、虛擬貨幣涉及洗錢等犯罪風險

一、國際組織

虛擬貨幣擁有匿名性、流通性、交易即時性等特點，再加上其全球的影響力，潛在的洗錢與資恐風險包括：交易具高度匿名性；無法有效的識別和驗證交易人身分；允許資金以匿名方式交易（透過無法確認資金來源之虛擬交易平台，接受現金資助或第三方資助），如轉帳人與受款人未經適當辨識，即可匿名轉帳；虛擬貨幣系統可透過網路進行 (包含智慧型手機內裝之應用軟體)，並可被用於跨境支付及資金移轉；在防制洗錢與打擊資恐規範裡，牽涉到數個國家之監管機構和執法單位，其責任的劃分不夠明確；缺乏一個全球性中央監管機構[6]。

「防制洗錢金融行動工作組織」（Financial Action Task Force，下稱 FATF）指出，虛擬貨幣是一個複雜的課題，不僅牽涉防制洗錢與打擊資恐的議題，還涉及其他監管事宜，包括消費者保護、社會安全、國家稅收[7]、穩健的監管制度以及網絡科技（IT）安全。英國國家犯罪局（National Crime Agency）更於 2015 年 6 月的報告指出，雖然現在虛擬貨幣尚未被普遍應用爲犯罪工具，但隨著社會大眾逐漸接受虛擬貨幣作爲支付工具其中一環時，執法部門可以預期，虛擬貨幣所涉洗錢或購買非法商品及服務之不法案件數將因而上升[8]。

二、歐美地區

歐洲刑警組織（歐盟執法機構）於 2015 年 9 月 30 日發布《2015 年度網路組織型犯罪威脅評估報告》（The 2015 Internet Organised Crime

[6] Financial Action Task Force, "Guidance for a Risk-Based Approach Virtual Currencies," June 2015, No.13, pp.31-32.

[7] Robert W. Wood, "Bitcoin: Tax Evasion Currency," FORBES, 7 Aug. 2013. Also see http://www.forbes.com/sites/robertwood/2013/08/07/ bitcoin-tax-evasion-currency.

[8] National Crime Agency, "National Strategic Assessment of Serious and Organised Crime 2015," June 2015, p.22.

Threat Assessment, IOCTA）[9]，陳述關於歐盟所面臨最大網絡犯罪威脅的觀點。該報告在不同犯罪類型中都提及比特幣和虛擬貨幣議題，包括非法融資，以及與此項技術相關的非法活動。據統計，犯罪者間的線上支付，採用比特幣之比例高達 40%，而 PayPal[10] 僅佔 25%[11]。該組織認爲，前揭數據顯示虛擬貨幣在發展「犯罪活動服務」的生態系統中，已成爲重要趨勢。該報告更指出：「儘管目前歐盟的網路犯罪者之間尚未出現共同貨幣，但比特幣將逐漸承擔起此一角色。比特幣具有共同支付機制，此特點將使其可用於所有支付情形，而這種趨勢只會愈演愈烈。」[12]

美國證券交易委員會（Securities and Exchange Commission，下稱 SEC）於 2017 年 7 月規定，以分散式分類帳本、區塊鏈技術爲基礎之貨幣發行或籌碼銷售，均應受聯邦證券法規之管轄；同年 9 月 SEC 進一步宣布，設立專責組織 Cyber Unit 調查網路之犯罪行爲，同月即控告兩家 ICO 業者違反美國證券法之反詐騙與相關註冊規定。SEC 於 2018 年 1 月更公布，針對公司名稱或商業模式突然變更爲區塊鏈，意圖趁勢上市之公司，將展開嚴格監管，避免炒作歪風盛行。

三、中國大陸

2017 年 9 月 4 日，中國人民銀行、國家網信辦、工業和信息化部、工商總局、銀監會、證監會和保監會等 7 個單位，聯合發表「關於防範代幣發行融資風險的公告」[13]，該公告中明確定位首次代幣發行（ICO）爲「未經批准非法公開融資的行爲」，對 ICO 在中國的活動造成極大震撼。該公告之內容分別以：準確認識代幣發行融資活動的本質屬性、任何組織和個人不得非法從事代幣發行融資活動、加強代幣融資交易平台

[9] The European Police Office, "The 2015 Internet Organised Crime Threat Assessment," Europol, 30 Sep. 2015, < https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015>.

[10] PayPal 是全球最大的線上金流系統，目前屬於 ebay 旗下的子公司。

[11] 同註 9，頁 46。

[12] 同註9，頁47；"Although there is no single common currency used by cybercriminals across the EU, it is apparent that Bitcoin may gradually be taking on that role. Bitcoin features as a common payment mechanism across almost all payment scenarios, a trend which can only be expected to increase."

[13] 中國人民銀行，2017年9月4日，〈http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html〉。

的管理、各金融機構和非銀行支付機構不得開展與代幣發行融資交易相關的業務、社會公眾應當高度警惕代幣發行融資與交易的風險隱患、充分發揮行業組織的自律作用等 6 大面向加以說明。本公告一出，當時在中國市場正蓬勃發展的 ICO 金融活動戛然而止，數個知名 ICO 平臺旋暫停 ICO 服務，除各類 ICO 發行的融資活動立即終止之外，ICO 平臺也必須將已發行完成的代幣予以清算、退還用戶。中國政府同時強烈清查 ICO 平臺，ICO 等融資活動自市場完全消失，監管機關可謂雷厲風行。

該篇公告中，對代幣融資的屬性定義如下，「代幣發行融資是指融資主體通過代幣的違規發售、流通，向投資者籌集比特幣、乙太幣等所謂『虛擬貨幣』，本質上是一種未經批准非法公開融資的行爲，涉嫌非法發售代幣票券、非法發行證券以及非法集資、金融詐騙、傳銷等違法犯罪活動。」其中所述及的各種犯罪態樣，與我國金融監督管理委員會（下稱金管會）曾發佈之新聞稿相當接近[14]。金管會於 2017 年 12 月 19 日新聞稿中指出：ICO 行爲如有涉及有價證券之募集與發行，應依證券交易法相關規定辦理；虛擬貨幣或 ICO 發行方如有以虛僞不實的技術或成果，或有以不合理的高報酬，吸引投資人參與，則可能涉及詐欺或違法吸金等刑事案件。顯見各地的監管機構對於 ICO 行爲可能涉及的金融犯罪態樣，例如證交法違法發行、詐欺、違法吸金等，見解大致相同。

四、日本

日本與中國之管制方式反其道而行，該國作爲值得密切留意。日本政府在虛擬貨幣的金融法規限制上較爲寬鬆，日本參議院於 2016 年 5 月 25 日通過《虛擬貨幣法》，2017 年 5 月正式施行。日本將比特幣等虛擬貨幣的定位從「商品」轉變爲「具貨幣功能的財產價值」，同時引進虛擬貨幣與日圓等法定貨幣買賣的交易所登記制度，並修正《犯罪收益移轉防止法》以防制洗錢，同時在《資金結帳法》中新訂定有關虛擬貨幣的章節[15]。綜上，日本於 2016 年即認可比特幣等虛擬貨幣的「類資產

[14] 金管會，2017 年 12 月 19 日，〈https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201712190002&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News〉。

[15] 黃菁菁，〈日本人愛用比特幣〉，《工商時報》，2018年1月4日，〈http://www.chinatimes.com/newspapers/20180107000393-260209〉。

（asset-like）」價值，並允許用以支付與數位轉帳交易，然而，虛擬貨幣交易商必須向政府註冊，受政府稽核監管。

日本政府另於 2017 年 4 月修正支付服務法案《Payment Services Act》，使加密貨幣正式成爲日本市場的合法交易工具，同年 9 月日本金融廳（Financial Services Agency，FSA）針對加密貨幣的交易，制定營運規則並開放業者申請，共釋出 11 張加密貨幣的經營執照。惟日本政府推動金融創新之際，也積極預防洗錢等犯罪，FSA 於 2017 年 10 月成立跨部門團隊，增設虛擬貨幣監管之首長職，負責監管虛擬貨幣交易。根據 FSA 的規定，加密貨幣交易商須建置安全與完善的電腦系統，員工須完成職前訓練，客戶帳號應予隔離，也必須查核客戶身分，避免遭到駭客入侵或淪爲洗錢管道。

日本大開虛擬交易門戶，雖創造商業利益，卻也衍生社會犯罪等問題。日本警察廳近期首次發表虛擬貨幣遭駭之損失統計，總計 2017 年共發生 149 件虛擬貨幣犯罪案件，造成約 6 億 6,240 萬日圓之財產損失。警方亦發現共有 16 家虛擬貨幣交易所因非法轉帳交易蒙受損失，遭駭最多的虛擬貨幣分別是比特幣（Bitcoin）85 起、瑞波幣（Ripple）55 起及乙太坊（Ethereum）13 起。

另根據日本政府公布的資料，金融機構網路銀行業務遭非法轉帳有 425 起，損失金額約 10 億 8,100 萬日圓，但前揭案件數僅爲 2014 年的四分之一，犯罪金額也降至 2015 年的三分之一。專家指出，此一趨勢可能代表犯罪集團將目標轉移至較易入侵的虛擬貨幣使用者[16]。

五、其他地區

印度央行（Reserve Bank of India，RBI）於 2018 年 4 月 5 日頒布禁令，認定加密貨幣資產仍然存在消費者保護、市場誠信與洗錢等風險，要求受管轄的銀行業者不得與從事加密貨幣交易的業者或個人往來，已提供相關服務的銀行須於 3 個月內終止服務；然而，RBI 也設立跨部門小組，針對法定的加密貨幣展開研究，預定於本（2018）年 6 月底發布研究結果報告。

[16] 蔡佩芳，〈虛擬貨幣犯罪 日去（2017）年逾百件〉，2018 年 3 月 22 日，《聯合電子報》，〈https://udn.com/news/story/11316/3046692〉。

南韓金融服務委員會（Financial Services Commission，FSC）已於2017年禁止加密貨幣發行上市（ICO），更於2018年初宣布，加密貨幣交易自1月30日起採用實名認證，以預防投機及洗錢行爲。實名制規範加密貨幣用戶之錢包帳號名稱，必須與銀行帳戶戶名一致，方能由加密貨幣錢包提領或存入貨幣。同時南韓也禁止未成年人與外國人在南韓境內設立加密貨幣錢包帳號。此外，南韓財政部自本年3月底，開始向當地之加密貨幣交易平台徵收22%的企業所得稅，並自4月底開徵2.2%的地方所得稅。

六、我國規範

近年來以新興加密貨幣或相關衍生金融商品爲犯罪工具者日益增多，引起國內外執法機關高度重視，本局於2018年6月中旬亦破獲比特幣鉅額吸金案。I○○國際儲備體集團林○桀等人，涉嫌向不特定民眾宣稱可藉投資比特幣賺取價差，只要購買100至7,000美元不等之投資套餐，即可換取等值之「RM」（儲備金），RM每日均固定增值0.35%，1年後即可取回高達355%之本利和。本案以時下新興商品爲標的招攬投資，本局與臺中地方檢察署共組專案小組，抽絲剝繭追查吸金款項及確認比特幣流向，並掌握林○桀等人涉嫌吸金、洗錢之具體不法事證後，於6月13日同步執行搜索集團成員之住居所，並約談林○桀等8名嫌疑人到案。除查扣銀行存摺、投資文件名單等證物外，並順利凍結集團成員26個銀行帳戶及扣押比特幣196枚等（市價逾4,000萬元），初步估計該集團於9個月內，在中國大陸、臺灣吸金共逾15億餘元。而林○桀等人擅長操作比特幣，將大部分吸金款項購買比特幣後移轉至境外，企圖製造金流斷點且隱匿犯罪所得，爲順利執行本案，本局資通安全處更備妥研究多時執行查扣比特幣之利器，由專業調查官至搜索現場協助執行查扣比特幣。

另關於比特幣在法律上之地位，目前國際間多數國家未予明確規範，因而易造成搜扣實務上之爭議。我國中央銀行（下稱「央行」）前總裁彭淮南於2013年11月23日接受立法委員質詢時即表示，比特幣不具法償效力，僅得用於發行者與會員間之交易，目前遊戲廠商發行的遊戲點

數，即類同比特幣之支付應用，對於比特幣的交易，央行將視爲貴金屬交易加以管理[17]。彭淮南於同年 11 月 27 日立法院接受質詢時再次強調，依據《中央銀行法》規定，我國交易工具還是以央行發行的貨幣爲主[18]；在其卸任央行總裁之際，更明白指出虛擬貨幣涉及洗錢問題，應予重視，爲此，法務部於 2018 年 4 月邀集中央銀行、經濟部、金管會、內政部警政署及法務部調查局，就現行法令及實務執行面共同研商，並將於本年底前研擬相關洗錢防制規範[19]。

[17] 蔡怡杼，〈比特幣洗錢　彭淮南：央行密切關注〉，《ETtoday 東森新聞雲》，2016 年 1 月 24 日，< http://www.ettoday.net/news/20131120/298323.htm >。

[18] 盧冠誠，〈比特幣夯 彭淮南：泡沫〉，《自由時報》，2016 年 1 月 24 日，< http://news.ltn.com.tw/news/business/paper/734193>。

[19] 王聖藜，〈彭淮南寫親筆信給邱太三後 虛擬貨幣入洗防法規範〉，《聯合新聞網》，2018 年 4 月 10 日，〈https://udn.com/news/story/7321/3078861〉。

參、比特幣與區塊鏈

比特幣建構於區塊鏈的應用之上，區塊鏈意即「連結區塊的長鏈」，若要瞭解區塊鏈之原理，首先要了解兩個概念，一是交易（transactions），另一則係區塊（blocks）。「交易」係指，所有比特幣曾經在不同比特幣位址移轉的紀錄；每次比特幣的轉移皆係一次交易，無任何例外；「區塊」則是一種裝載的網路空間，「區塊」將比特幣的交易紀錄全部裝載於該空間內。兩者的關聯性是，「交易」會週期性地被抓取並且「裝載」入區塊內。

簡而言之，區塊鏈可以被想像成類似 Excel 活頁簿內的工作簿（worksheet），每次比特幣的交易會被記錄在單一橫列（row）上，而每一個工作表（worksheet）就是一個區塊。區塊鏈則是將資料儲存在電子文件（Flat File），或稱「平面文件」，指一種包含沒有相對關聯式結構的記錄檔，通常以文字型式表現，例如純文字文件（「.txt」檔）格式，並且依照交易時間之先後，進行區塊有條理的排列，而區塊內會儲存所有在比特幣網路中相關移轉過之交易紀錄。區塊鏈與 Excel 活頁簿內的工作表（worksheet）差異點在於，前者係利用數學演算原理所構成之鏈接，將交易儲存在區塊中。

每一個區塊都有一個區塊頭（Header），區塊頭會記載這個區塊的資訊，包含：(1) 前一個區塊的雜湊值 (Hash Value) [20] 會指向前一個區塊，讓兩個區塊間產生無形連結；(2) 區塊高度 (Block Height)：比特幣誕生的第一天是 2009 年 1 月 3 日，當時區塊高度爲 0，區塊高度自那天開始隨著每一區塊的增加而增加，區塊高度於 2018 年 5 月 27 日達到 524,670 [21]；(3) 時間戳（Timestamp）：計入區塊的時間，格式爲 YYYY-MM-DD HH:MM:SS (年 - 月 - 日 時 : 分 : 秒)，並使用 UTC（國際協調時間）時區；(4)

[20] 哈西值係從雜湊函式演算而得，而雜湊函式（Hash function）又稱雜湊演算法，是一種從任何一種資料中建立數字「數位指紋」（Digital Fingerprint）的方法；該函式把訊息或資料壓縮成摘要，使得資料量變小，將資料的格式固定下來。該函式將資料打亂混合，重新建立一個叫做雜湊值（Hash values，Hash codes，Hash sums，或 Hashes）的指紋，雜湊值通常用一個短的隨機字母和數字組成的字串來代表。

[21] 該數值取自網站 Bitcoin Block Explorer，2018 年 5 月 27 日 23 時 58 分，〈https://blockchain.info/〉。

Merkle Root：紀錄該區塊經由 Merkle Tree（默克爾樹，或稱雜湊樹）演算法，計算出區塊中所有交易樹根節點之雜湊值；(5)Nonce（隨機數）與 Difficulty（困難度）：Nonce 在密碼學名詞中係一任意數值，通常只能使用一次，礦工以電腦算力，嘗試將一個 Nonce 代入雜湊函式，再看其結果是否符合難度條件；以此重複計算，就是所謂之挖礦[22]。

區塊是向後鏈接的，而每一個區塊又都會指向在這條鏈中之前一個區塊，技術上來說，即係指向前一個區塊的區塊頭（Block Header）中儲存之雜湊值。如此鏈接的效果在於，確保某區塊可以被其他多個區塊跟隨，且在該區塊之後的全部區塊未被重新計算（Recalculation）時，是無法被改變的[23]；因此區塊中長鏈的存在，能使區塊鏈擁有永遠不會被改變的深遠歷史紀錄，所稱之「永遠不變性」，就是區塊鏈目前尚稱安全之關鍵特徵。故此，若任何一個區塊被惡意的改變，那麼被改變的那個區塊在全球帳本之區塊鏈中將無法生效。

一般來說，透過執法機關調查後之剖析，只有一部分的眞實資訊能從 (Block Header) 被取得，相關資訊包含：(1) 包含在 UTC 時區下之時間戳（Timestamp），即該區塊在什麼日期、時間下被礦工挖出；(2) 每一區塊獨一無二的區塊高度（Block Height）。

除了（Block Header），每一個區塊亦包含交易列表，該交易列表順序通常依據礦工確認交易之紀錄。然而，礦工也必須遵守而不可任意改動相關規則，例如該區塊中的第 1 筆交易必須是礦工的挖礦報酬（Reward）；再者，一連串的交易，必須出現在任何該一連串交易已發生的時序之後，即假設位址 A 傳送比特幣到位址 B，又位址 B 再傳送比特幣到位址 C，那麼這一連串交易所依據的 A 交易，必須第一個生效。

此外，執法人員不需自行從語法上分析區塊鏈的平面文件（Flat Files），包含區塊頭與交易資訊等，該等資料係透過所有主要區塊鏈的開發者來進行，例如比特幣錢包和區塊數據查詢服務提供商 Blockchain.info[24]。

---

[22] ASIC 挖礦機的領導廠商「比特大陸（Bitmain）」係貢獻台積電營收的十大客戶之一，該公司預測 2018 年，加密貨幣將貢獻台積電 5%之營收。

[23] 所謂可以改變鏈接的「重新計算 (recalculation)」，需要一個等於現今所有電腦計算量總和之巨大數值。

[24] 係英國商 Qkos 所提供服務，其網站上可以查詢到最新交易數據、挖礦新區塊產生情況等金融數據。

肆、區塊鏈位址

關於區塊鏈位址（Address），有一重要觀念需先釐清，比特幣的使用者得在任一位址下載比特幣軟體。然而，基於不同預設位置（Default Location）的選擇，因不同作業系統會出現下列差異：

一、Windows：

舊系統儲存路徑：

在Windows XP系統中路徑會是「C:\Documents and Settings\<username>\Application data\Bitcoin」。

新系統儲存路徑：

在較後期的 Windows 作業系統 (例如 Windows Vista、Windows 7、Windows 8、Windows10) 則路徑會變爲 「C:\Users\<username>\Appdata\Roaming\Bitcoin」；若要開啓這些檔案的捷徑爲在一開始在指令區（Command Line）執行「explorer %APPDATA %\Bitcoin」之語法。

二、Mac：

在 Mac OS X 作業系統中路徑爲「~/Library/Application Support/Bitcoin/」。

三、Linux：

在主流的 Linux 版本路徑位址會是「~/.Bitcoin/」。

四、區塊鏈檔案夾之儲存與空間

比特幣區塊鏈會被分割爲數個檔案夾，每個檔案容量一般約爲 134 MB，而存放區塊的檔案夾，亦會將比特幣區塊鏈儲存於同一個檔案夾，其中包含公鑰（Public Key）及私鑰（Private Key）[25] 的錢包檔案「Wallet.

[25] 公開金鑰加密(Public-key cryptography)，另稱非對稱加密(Asymmetric cryptography)，是密碼學的一種演算法，它需要兩個金鑰，一個是公開密鑰，另一個是私有密鑰；一個用於加密，另一個則用作解密。雖然兩個密鑰在數學上相關，但如果知道了其中一個，並不能憑此計算出另外一個；因此其中一個可以公開，稱為「公鑰」；不公開的金鑰為「私鑰」，必須由用戶自行嚴格秘密保管，絕不透過任何途徑向任何人提供。

dat」。如上所述，比特幣的預設位置（Default Location）可以改變，若起初使用容量較小的 SSD [26] 硬碟存放在電腦 C 槽（Drive C:\），可變更區塊鏈資料夾存放的位置，改存放於另一個容量更大的硬碟。應特別留意之處在於，區塊鏈中內含爲數不少之檔案夾，且檔案夾的數量會隨著區塊鏈的增長而增加，因此需要之硬碟空間容量極大，早在 2016 年 6 月間，檔案容量已達到 70GB.

某些公開網站，提供免費資源供大眾利用，例如前述比特幣錢包和區塊數據查詢服務提供商 Blockchain.info 之網站 [27] 亦提供經常性更新的圖表。網站所提供之圖表中，顯示增加的區塊鏈容量空間數據，並非一個函數，亦非一個完全的平面文件 [28]，新的區塊不斷增生，迄至 2018 年 5 月爲止，平均每個獨立區塊新增數 KB 至 1 MB 不等之檔案容量。

另一評價極高之公開網路資源係「WebBTC」[29]，提供簡單卻具有高度實用且經常更新之區塊鏈摘要。依該網站之數據，2016 年 6 月比特幣位址之總數高達約 1.6 億筆，根據相關位址傳送或接收比特幣之過程與紀錄，合計約有超過 1.4 億次的比特幣交易。

一般而言，大額之比特幣交易多爲簡單的付款交易，亦即採用多重簽章位址（Multi-Signature）之方式，完成傳送比特幣到某位址或直接傳送到公鑰，此種傳輸方式約占 5%，僅有 0.02% 的比特幣位址是使用 OP_RETURN（數據輸出操作）的電腦程式語法，儲存非金融資料（Non-Financial Data），當某些傳送者決定需永久保存之資料 [30]。

[26] 固態硬碟或固態驅動器（Solid-state drive 或 Solid-state disk，簡稱 SSD），係一主要以快閃記憶體作為永久性記憶體的電腦儲存裝置，通常容量較傳統硬碟為小。

[27] https://blockchain.info/charts/blocks-size。

[28] Europol EC3(European Cybercrime Centre), “A Guide for Bitcoin Investigators”, “… While we can see the increase is not exponential it is not completely flat either….” , version 1.09, March 2 2017, p.26。

[29] https://webbtc.com/。

[30] 同註 28，頁 65。

伍、比特幣錢包與扣押的關聯

執法機關進行比特幣相關調查工作時，通常追求 2 大重要目標：識別嫌疑犯所利用、扣押遭竊取或用於刑事犯罪活動之比特幣錢包。執法者需認清一重要事實，即比特幣並非儲存於一個裝置（Device）上，而是儲存於內含私鑰（Private Key）的錢包（Wallet），私鑰[31]正是讓比特幣被移轉之關鍵。

欲瞭解如何存取並取得嫌疑人持有的比特幣私鑰，必須先瞭解私鑰的支配機制[32]。私鑰可透過以下方式被控制：(1) 儲存於裝置內的錢包：又稱「軟體錢包」，儲存於嫌疑人的電腦、手機或其他外部儲存裝置之比特幣錢包，包含熱錢包（Hot Wallet，另稱 HW）或 USB 磁碟裝置；(2) 紙錢包：藉由紙錢包（通常使用 QR code 紀錄，某些網站提供免費印製程式）或直接手寫於紙張；(3) 線上錢包：透過第三方管理比特幣錢包，通常爲虛擬貨幣兌換商或線上錢包之服務提供者。各類錢包之說明如下：

一、軟體錢包

目前市面上比特幣錢包種類繁多，最普及的軟體錢包爲 Bitcoin Core 與 Electrum。此類比特幣錢包均可與一般桌上型電腦常用作業系統（如 Windows/Linux/Mac）相容[33]，並提供圖形使用者介面（Graphic User Interface，GUI），讓使用者方便確認比特幣帳戶位址內的結餘（Balance）、近期交易清單，以及可傳送或接收之比特幣。

軟體錢包 Bitcoin Core（前稱「Bitcoin-QT」）與其他比特幣軟體錢包，關鍵差異點在於，是否需要下載完整的區塊鏈來以獲得先前的資料。Bitcoin Core 軟體錢包的結算餘額 (Balance) 並非即時更新，需待完整區

[31] 比特幣之私鑰可以想像成從 1 至 2256 中隨機選一個數字；而因匿蹤之需要，許多比特幣錢包內帳戶都僅使用 1 次，即錢包裡有很多帳戶，但許多帳戶僅使用一次。目前多數錢包都屬 HD（Hierarchical Deterministic）錢包，即由一個種子生成主私鑰，再生出海量的子私鑰及錢包帳號。

[32] 掌握私鑰即掌握錢包控制權。錢包如同銀行帳戶，私鑰如同提款卡，遺失或損毀則無法對該帳戶進行簽章交易；該帳戶之比特幣雖仍紀錄在帳本上，卻無法花用。另私鑰為電子紀錄，容易複製備份，複本亦等同掌握控制權。

[33] 相關適用於各種平台的完整比特幣錢包資訊，可參照下列網址：https://bitcoin.org/en/choose-your-wallet。

塊鏈下載成功後才進行更新，通常需要花費數天。其他多數的軟體錢包被稱爲「輕錢包」（Lightweight Wallet），此類輕錢包只需下載全部區塊鏈中，與使用者有關聯的部分即可，不不需要下載整個完整的區塊鏈（參考下「表一」）。

軟體錢包存放在名爲 Wallet.dat 的檔案中，並儲存於本地磁碟（Local Drive），本地磁碟指連接在使用者電腦上的磁碟或磁帶驅動機，這些錢包的檔案包含未加密（Unencrypted）或加密（Encrypted）的私鑰。國外實務案例指出，需於現場登入嫌疑人電腦，以存取並移轉比特幣到執法機關掌控的錢包中，然而大多數的比特幣使用者，不論所持有比特幣的是合法或非法，均會加密所使用的錢包。

可預期的是，考量到區塊鏈容量龐大且持續增加，而輕錢包（Lightweight Wallet）的客戶端不須下載整個完整區塊鏈，故輕錢包的使用者將更加普及，且主要應用在手機等儲存空間、處理資源、電池等較精巧的裝置上。簡言之，隨著區塊鏈的容量逐漸增加，轉而使用輕錢包程式，或線上比特幣錢包提供商如 Coinbase、Blockchain.info、Xapo 或 Circle 的使用者，會逐漸增加。

研究電腦安全機制之學者也發現，因輕錢包程式運作時會請求相關之連結，導致揭露比特幣位址，進而得鎖定儲存於特定位址之錢包，目前提供相關追蹤數據資料之工具服務商爲 Chainalysis，提供之服務也會紀錄 IP 位址，可用於追查嫌疑人身分。

表一、比特幣客戶端（Clients）主要差異之比較

功能 (Functions)	挖礦者 (Miners)	全部節點 (Full nodes)	輕錢包程式 (Light clients)
確認結算 (Checking balance)	○	○	○
接收或傳送付款 (Receiving or sending payments)	○	○	○
儲存完整的區塊鏈 (Storage of full blockchain)	○	○	
驗證交易 (Validation of transactions)	○	○	
傳播交易 (Propagation of transactions)	○		
確認交易 (Confirmation of transactions)	○		

二、行動錢包

著名的行動裝置錢包程式諸如 Coinbase、Airbitz、Blockchain、Circle、Xapo、Bread、Copay、Blocktrail 等。行動錢包在任何系統皆可使用，這些錢包將私鑰儲存在行動裝置的程式裡，若要存取私鑰，需將手機解鎖，錢包程式也可能透過 PIN 碼或指紋認證加密，與軟體錢包的儲存、管理作法相似，上述私鑰存取通常需要涉嫌人配合，或使用某些可規避安全系統的專業程式。

一般而言，使用者傾向以紙錢包、硬體或軟體錢包，儲存較大數額之比特幣，而將小額比特幣（一日交易量）置於手機錢包中，故若執法機關於執行搜索時發現存有比特幣的手機錢包，則可合理推斷，嫌疑人可能將大量比特幣儲存他處。

三、網頁錢包

存取網頁錢包需登入使用者帳號或是錢包帳號、密碼以及雙重認證碼，目前最廣爲使用的網頁錢包系區塊鏈瀏覽業者 Blockchain.info。多數的網頁錢包業者允許使用者下載錢包或是匯出其私鑰，便於使用者離線（Off-line）儲存。

四、紙錢包

紙錢包以完全離線（Off-line）的方式儲存私鑰，存取比特幣所需的私鑰以紙張列印並隔離，該私鑰通常伴隨著公鑰及 QR 碼。因爲紙錢包生產者會提供比特幣離線的公鑰及私鑰，通常以隔離網絡[34]製造與儲存此等公、私鑰。在紙錢包之公、私鑰被紀錄於實體紙張後時，任何電腦上的資料都可被刪除，無需保留備份。可想而知，紙錢包之特點在免於遭受網路駭客入侵或是惡意程式攻擊，但紙錢包仍需保存於安全處所，避免遭竊或毀損。

紙錢包對密集透過網路交易之使用者而言，相對不便，故使用者採取紙錢包之儲存形式，通常係存放可觀數額之比特幣。對於執法機關而

[34] Air-gapped Computer（又稱「氣隙電腦」），當政府、公共事業與企業想要保護敏感的資料時，他們會創造一種封閉網路（Air-gap network），主要是將資料儲存在永不上網的電腦，以此來保護資料免受駭客侵擾。

言，若在現場搜索到紙錢包，任何與該私鑰相關的比特幣資金，皆可迅速以私鑰匯出匯入方式，將資金移轉到任何使用中的軟體錢包或網頁錢包等。因大多數的錢包均允許將私鑰匯入，在一般電腦選取「檔案→匯入」之指令，即可完成操作。

五、萬能錢包

「萬能錢包」係指形式上是軟體錢包、線上錢包、紙錢包或硬體錢包，但透過創造 10 至 15 字有意義或有次序的句子作爲「種子」（Seed）[35]，來代表及驅動私鑰，此種錢包之優勢在於可讓使用者輕鬆地備份或還原私鑰。

通常萬能錢包也被稱做「大腦錢包」，因爲「種子」不是僅可被電腦儲存、紀錄或列印，亦可留存於使用者的記憶中；但也有某些使用者無法完全記住「種子」，所以通常將「種子」以電腦或紙本紀錄。若使用者能完整記憶或紀錄下萬能錢包的「種子」，則毋須擔心無法還原錢包檔案或遭遇硬碟毀損問題，反之，使用者還可以從「種子」複製出新的錢包。因此種方式可從錢包還原出公、私鑰，故「種子」又被稱做萬能密碼。換言之，若網路攻擊者或執法者發現「種子」，頃刻間得掌握所有比特幣的位址。

此外，萬能錢包亦可能遭受攻擊：「種子」雖講究其長度、獨特性且難以猜想，錢包仍可能暴露網路世界中，而其他使用者能藉由暴力破解密碼。攻擊者透過下載區塊鏈的複製檔案，再以解析（PARSE）的方式取得所有比特幣的位址——高達上億的比特幣位址，部分位址會被識別及擷取，然後以交叉比對的方式確認含有弱密碼的位址[36]，一旦比對出密碼結果，攻擊者可利用該密碼複製出私鑰，進而竊取受害者的比特幣。

六、硬體錢包

硬體錢包係使用者利用硬體設備儲存比特幣私鑰之常見方式，私鑰安全地儲存於錢包之中，避免私鑰遭移轉。硬體錢包認證交易模式如次：

[35] 或稱「還原碼」。

[36] 同註 28，”…Addresses with non-zero balances could be identified and extracted and then cross-matched against addresses that can be generated by using weak passwords (‘passw0rd’, ‘Ford Perfect’, wordlists of popular songs, quotes, etc.)…”, p.31。

（一）硬體錢包從電腦以隨身碟（例如 USB）存取接收交易；（二）硬體錢包驗證交易；（三）驗證後的交易紀錄回傳至電腦，再以廣播（Broadcasting）方式輸出至網際網路。

上述程序並不會洩漏私鑰，因此該程序並不會將私鑰暴露在網際網路，若要存取安裝在硬體錢包上的私鑰，則需要與硬體設備的連結，而硬體設備可利用 PIN 碼加密或他種型式的驗證，得避免惡意程式、鍵盤側錄（KEYLOGGER）之威脅或執法機關的查緝。因若採取暴力破解的方式存取硬體錢包，極曠日廢時，故亟需涉嫌人的合作以便取得硬體錢包中的私鑰與資金。

最知名的硬體錢包當屬 TREZOR[37]，製造商提供「還原種子」（RECOVERY SEED，包含 12 至 24 個空白初始值的記事本）讓使用者紀錄，以便於備份錢包[38]。如上所述，執法機關若於搜索現場取得種子內容就即可重新複製錢包，再將比特幣予以凍結；故於搜索現場時，前述記事本即爲搜索的重要標的。

另一較特別的硬體錢包當屬 BitLox。約爲信用卡大小，依其提供的服務，售價介於美金 200 至 400 元，通常用以儲存大量的比特幣。BitLox 允許使用者創建 50 個隱形的錢包，唯有當使用者輸入錢包號碼及所對應之 PIN 碼[39]，錢包才會顯示，故執法機關無法確知嫌犯的錢包是否已全部扣押。此外，該設備在匿名作業系統（譬如「Tor and Tails」）上運作良好（使用 USB 纜線與電腦介接），而 BitLox 另一吸引犯罪者使用之誘因是，該設備曾於 2016 年 3 月在暗黑網（如「DEEPDOTWEB」）販售過，該網站爲網路黑市中，最普及的線上資源集散地。

[37] Trezor 係於 2013 年由捷克 SatoshiLabs 公司研發（該公司創建第一個比特幣礦池），是一個開放原始碼的錢包，使用 BIP49 (Bitcoin Improvement Proposal) 標準產生私鑰，即使製造商倒閉、硬體錢包遺失或損壞，對產生之私鑰皆無涉。

[38] 為避免硬體錢包損毀無法讀取，故亦有還原種子（Recovery seed，即硬體錢包的備份）之設置。該種子為 24 個英文字，初始設定時由系統亂數產生，需手動記錄，可用以還原錢包私鑰及地址。

[39] 以 Trezor 為例，Pin 碼係由使用者設定 4 位以上純數字，避免硬體錢包遺失遭他人使用，若 Pin 碼輸入錯誤，則須等待一段時間後才能再次輸入，每輸入錯誤 1 次，等待時間以 2 的指數增加，例如輸錯 20 次，須 6 天後方得再次輸入；輸錯 30 次，須等待 17 年。

陸、比特幣扣押程序

一、基本概念

若執法機關辨識出涉嫌人所持有比特幣在區塊鏈上的位址，必須認清：不可能在遠端執行比特幣的扣押（除非嫌犯將比特幣放在網路平台上）。若希望在嫌犯之住居所完成涉案比特幣的扣押，執法人員必須確認：

（一）比特幣錢包儲存在嫌犯的相關硬體設備中，且確認密碼所在，因爲大多數之錢包都經過加密程序；

（二）尋找嫌犯之私鑰至關重要，如此才能匯入至其他錢包；

（三）嫌犯的「還原種子」爲何，通常是 12 至 24 個的隨意字碼。

僅複製另存 wallet.dat 檔案尚無法扣押比特幣，因嫌犯或擁有私鑰之其他第三人來說，尚可移動資金至其他位址，重要關鍵在於將私鑰或「還原種子」匯出至執法機關所控制之錢包，如此方可使執法者找出與之相關的公鑰，以及未移轉或售出之比特幣，並將錢包內比特幣資金「完全」轉移至執法機關掌握之比特幣位址。

爲了保全錢包，執法機關所使用之錢包應具備自身之區塊鏈，且可被區塊鏈社群完整地稽核，故 Bitcoin Core 錢包是個值得推薦之選項。理由在於，該錢包可以在執行搜索、扣押前即預備好，執法人員在扣押之際，可利用其文件鑰匙或隨身碟鑰匙，將比特幣進行立即性且無延遲（without any delay）之轉移。

若非前述情況或執法機關錢包位址未明（即未事先準備），但有立即扣押比特幣之需要時，執法人員可考慮次佳之選擇，即現場立刻建立一比特幣錢包。迄今最快及相對安全之方式，是使用 Bitadress.org 此一純粹使用 JavaScript 程式語言撰寫之網站。該網站可讓使用者以滑鼠或鍵盤自行編撰產生私鑰及相對應之比特幣位址，顯示方式係以亂碼方式進行。再者，該網站只能供有安全連線且經認證之電腦瀏覽，並且網站具有離線儲存與建立私鑰和相對應比特幣位址之功能，如此一來，將比特幣轉移至前述由執法機關建立之比特幣位址後，扣押程序即宣告完成。

其他較爲便利之方案爲，執法機關可以請求交易所提供比特幣位址，

此方式在執法機關要求立即轉換扣押之比特幣至其他法幣（通常爲歐元或美金）時特別實用，因省去了執法機關自行建立並維護比特幣錢包之大額開銷。

二、匯出 / 匯入私鑰相關程序

私鑰可能會印在紙上、手機中、儲存在涉嫌人電腦裡的 wallet.dat 檔案或是隨身碟鑰匙中。若爲上述任一形式，匯出私鑰可以「dumpprivkey」指令進行，該指令顯示之私鑰係以 WIP（Wallet Import Format）形式表達。值得注意的是，加密過的錢包尚須嫌犯提供密碼，俾利執法機關匯出私鑰，匯出過程中不會移除私鑰本身，而是匯出至一般的筆記檔案中。若錢包未包含能代表比特幣位址之私鑰，上述操作將反饋錯誤訊息。

取得私鑰後，必須立即匯入至執法機關之錢包中，比特幣才能完全受執法機關控制，操作方式可能因錢包種類而有差異。私鑰一旦成功匯入，需耗費些許時間，使錢包與該比特幣位址關聯的所有交易紀錄同步，最後錢包亦會顯示交易餘額。

在私鑰匯入錢包及顯示餘額後，全數比特幣應完全轉移到執法機關錢包所代表的比特幣位址；若是執法機關可掌控嫌犯的錢包及密碼，可直接轉移比特幣，與私鑰是否匯出或匯入無涉。

其他扣押比特幣較簡便之選項，是向平台交易商提出請求。若執法機關辨識出嫌犯使用任何交易商所開立的虛擬貨幣帳戶，可要求交易商凍結該犯涉嫌人相關帳戶內之虛擬資產。而虛擬資產除比特幣外，尚包括萊特幣（Litecoin，簡稱 LTC）、乙太幣（Ethereum，簡稱 ETC）、達世幣（Dash）或甚至是法幣（Fiat）；值得注意的是，雖然嫌犯可能將部分虛擬資產留存於線上交易平台之帳戶，但是犯罪者傾向將大部分虛擬資產儲存於其軟體錢包中。

三、取出錢包之的比特幣位址

無論虛擬貨幣之扣押是否順利進行，執法人員應該將涉嫌人錢包裡所有的比特幣位址解析出來，使用相關指令（如「Listaddressgroupings」）可將所有已花費或未花費的比特幣位址列舉出來，此係相當重要的步驟。因操作該指令無需使用者的密碼，甚至在加密的錢包中亦可執行，執法

人員可再進行追查，亦可使用免費或商業版本的資金追查軟體。

交易列表之匯出亦無需密碼，可在 Bitcoin Core wallet 的 GUI 介面的交易欄位執行匯出程序，結果將以具備日期、數額、標籤及交易識別碼的檔案（neat.csv）呈現。

四、處理加密錢包

加密的錢包依舊可以開啓檔案，查看餘額、交易列表與目前比特幣位址數量，惟匯出私鑰及移轉資金仍需要密碼，取得密碼的可行方式如下：

（一）促使嫌犯合作

執法人員需嫌犯提供密碼，無論嫌疑人係出於自願或因受法律拘束而配合提供。但調查人員尚可在一定時間內測試出密碼，錢包不會因爲給予錯誤密碼次數過多而造成難以恢復的鎖死或自刪。

（二）使用資料鑑識手段

當打開比特幣查詢（在Bitcoin Core wallet中，係於Help→Debug Window Section指令中），查詢指令的歷史紀錄可透露最近幾次執行的指令，鍵入「Up Cursor Key」即可瀏覽，每一個指令可能透露出當初使用者的行爲狀態。

在 Linux 系統裡輸入「History」指令，可查出使用者最後的指令，即便無法立即得知密碼，尚有機會可以查出最近使用過的密碼；即便使用者在密碼上做些變化，但相關記錄還是會被儲存下來。

如果可能，建議在關機前進行記憶體傾印（Memory Dump）。現成有許多工具可以擷取正在使用的記憶體，其中一個最爲知名的是 FTK Imager，得擷取隨機存取記憶體 (Random Access Memory，下稱 RAM) 與硬碟的影像檔，該工具軟體可使用 GUI 介面或是單純指令介面。

記憶體傾印後，再使用相關工具（如「Volatility」）擷取出相關比特幣錢包的密碼；另一選項是使用「String」指令，在記憶體中搜尋文字字串（Text String），蒐集相關字串彙整爲「暴力破解」（Brute-Forcing Attack）的資料庫。值得留意的是，所有密碼都會以未加密型式儲存在 RAM 中。

（三）暴力破解法

執法機關可以嘗試使用相關工具（如「John the Ripper」）以及其他密碼破解的軟體，破解錢包密碼，另有些網頁程式碼[40]可下載進行密碼的破解，惟實務上欲破解加密演算法的破解並不容易，尤其是上述程式碼在一般電腦中每秒運算能力並不優異，導致此一方法通常不切實際。故此，在使用暴力破解的方式前，執法機關應對待破解的密碼具一定認知或研究[41]。

此外，此法奏效機率依密碼的複雜程度有所不同。大部分的比特幣使用者對資訊安全均有一定程度的瞭解，設定密碼通常超過10個字元，若密碼係經過設計，不曾在其他電腦程式或軟體服務出現，亦非儲存在RAM、磁碟機或紙本紀錄，使用暴力破解方式取得密碼的難度相當高。

（四）使用EC3解密平台

歐洲刑警組織下轄之EC3數位鑑識實驗室，能輔佐會員國家或第三方機構之調查，該實驗室不僅提供將數位資料擷取出來後的分析與還原服務，亦提供解密的平台。該平台提供解密比特幣錢包的相關程式，雖已揭露之成功破解虛擬貨幣錢包案例極少，惟該機關樂意與各國執法機關交流，並提供協助虛擬貨幣錢包破解密碼的服務，至少可提供錢包或密碼相關之資訊。

（五）外包廠商

公部門亦可轉向企業及私部門求助，網路上有許多線上錢包提供相關服務且功能強大[42]，其提供的服務在比特幣社群中亦享有盛譽，惟該服務並非免費。另提供服務之網站不要求將所有的錢包內容（例如Wallet.dat檔案）或私鑰都上傳，相反地只要求擷取上傳可助於解密之資訊，大幅降低了私鑰遭竊取之風險。

[40] 例如 https://github.com/gurnec/btcrecover。

[41] 例如嫌犯的出生日期、手機號碼、身分證字號、車牌號碼等容易猜想之數字或字母組合。

[42] 例如 walletrecoveryservices.com，。

柒、策進作為

一、制定虛擬貨幣搜索扣押流程

因比特幣具備「去中心化架構」及以「電磁紀錄儲存」之特性，執法機關無法對單一負責單位執行凍結，而私鑰對比特幣錢包又至關重要，可謂「私鑰在，錢包活；私鑰失，錢包死」，故執法人員無法以傳統方式進行搜索扣押程序，如何「移轉錢包控制權」更爲關鍵。執法機關亦需制訂嚴謹之前置程序，以確保控制權移轉之「唯一性」。

由於硬體錢包具有「易於管理」及「保留彈性」之優點，執法機關可於執行搜索扣押[43]時（下稱「搜扣」）使用。「易於管理」係因硬體錢包可確保硬體錢包本身及其還原碼之存取；「保留彈性」係指可將封緘之硬體錢包直接移送至檢方。以下對案件承辦人與現場執行人之搜索前後及扣押作爲（包含移送及發還）提出建議：

（一）案件承辦人

1. 搜扣前：

（1）申請搜扣用比特幣帳號。

（2）備妥「扣押物品目錄表」填寫範例（參考「表二」）、「比特幣搜扣移轉紀錄表」（參考「表三」）及「比特幣搜扣移轉金額明細表」（參考「表四」）。

（3）依搜索現場數準備下列物品，發交各搜索現場帶隊官：本案搜扣用比特幣帳號儲存於防寫隨身碟／光碟中；列印對應之 QRcode 紙本；於「比特幣搜扣移轉紀錄」填寫本案搜扣用比特幣帳號後列印；查詢並記載當時可 20 分鐘內確認轉帳之手續費率[44]；攝影器材（移轉比特幣時全程錄影）。

2. 搜扣後：

（1）再次確認總入帳金額並製表。

[43] 需於錄影環境下初始化硬體錢包、記錄帳號 Bitcoin Address 並封緘，搜扣時僅需攜帶帳號供移轉。

[44] 可於 https://bitcoinfees.earn.com 查詢，手續費依確認時間而有不同；為節省時間及確保比特幣不被第三方移轉，建議選擇「20 分鐘內可確認」之費率。

（2）取得並保管該封緘之硬體錢包及還原碼信封。

（二）現場執行人

1. 搜扣前[45]：

（1）向案件承辦人領取：防寫隨身碟／光碟 (內有本案搜扣用比特幣帳號)；QRcode 紙本；「比特幣搜扣移轉紀錄表（含移轉金額明細表）」數份（上已載明本案搜扣用比特幣帳號）；當時比特幣手續費率；攝影器材（移轉比特幣時全程錄影）。

（2）下載比特幣搜扣手冊。

2. 執行當日：

（1）於電腦／手機等裝置中搜尋 Bitcoin 錢包。

（2）取得密碼後，轉帳至執法機關錢包位址（全程錄影）[46]。

（3）確認移轉成功（當場照相或列印），並回報案件承辦人。

（4）填寫「扣押物品目錄表」、「比特幣搜扣移轉紀錄表」及「比特幣搜扣移轉金額明細表」。

（三）移送

1. 移送前再行查詢帳戶內幣額並列印附送。

2. 檢方建立比特幣錢包，案件移送時將扣案比特幣，由司法警察機關將錢包內比特幣移轉至檢方錢包內。

（四）發還[47]

1. 會同當事人，於錄影環境下開啓硬體錢包信封。

2. 輸入 Pin 碼並核對發還位址後完成移轉。

3. 列印移轉證明，請當事人簽署領據。

[45] 建議於每個搜索現場預備相關設備。

[46] 收款帳號為執法機關帳號（Bitcoin address），轉帳金額為「全部移轉」（Amount:Max）；確認交易完成後回報外勤案件承辦人，即刻上網確認（網址：https://blockchain.info/，搜尋關鍵字：交易 ID）。

[47] 直接發還仍存有困難，即受搜索人可能主張錢包內比特幣毀損或與扣押數額不符。

表二、「扣押物品目錄表」填寫範例

法務部調查局（單位全銜）扣押物品目錄表—範例

編號	品名	單位	數量	所有人/持有人/保管人	備考
○	○○○存於手機之比特幣	BTC	0.36	○○○	詳編號○○比幣搜扣移轉紀錄表
○	○○○存於個人電腦之比特幣	BTC	1.58	○○○	詳編號○○比幣搜扣移轉紀錄表

表三、比特幣搜扣移轉紀錄表

法務部調查局比特幣搜扣移轉紀錄表

一、移轉紀錄編號：_____

二、由○○○所有/持有/保管之**比特幣帳號** Bitcoin addres 共計移轉____筆

三、移轉至搜扣用**比特幣帳號** Bitcoin address（如下）：

_____

四、移轉總金額：_____ BTC

五、移轉總手續費（係由所有人/持有人/保管人帳號支出）：_____ BTC

所有人/持有人/保管人 簽名：_____

移轉人/搜扣人 簽名：_____

日期：_____年_____月_____日

表四、比特幣搜扣移轉金額明細表

法務部調查局編號_____比特幣搜扣移轉金額明細表

1. 交易代碼後5碼_____，移轉金額_____BTC，移轉手續費_____BTC，
   移轉區塊BlockChain編號_____，區塊BlockChain時間_____
2. 交易代碼後5碼_____，移轉金額_____BTC，移轉手續費_____BTC，
   移轉區塊BlockChain編號_____，區塊BlockChain時間_____
3. 交易代碼後5碼_____，移轉金額_____BTC，移轉手續費_____BTC，
   移轉區塊BlockChain編號_____，區塊BlockChain時間_____
4. 交易代碼後5碼_____，移轉金額_____BTC，移轉手續費_____BTC，
   移轉區塊BlockChain編號_____，區塊BlockChain時間_____
5. 交易代碼後5碼_____，移轉金額_____BTC，移轉手續費_____BTC，
   移轉區塊BlockChain編號_____，區塊BlockChain時間_____
6. 交易代碼後5碼_____，移轉金額_____BTC，移轉手續費_____BTC，
   移轉區塊BlockChain編號_____，區塊BlockChain時間_____
7. 交易代碼後5碼_____，移轉金額_____BTC，移轉手續費_____BTC，
   移轉區塊BlockChain編號_____，區塊BlockChain時間_____
8. 交易代碼後5碼_____，移轉金額_____BTC，移轉手續費_____BTC，
   移轉區塊BlockChain編號_____，區塊BlockChain時間_____
9. 交易代碼後5碼_____，移轉金額_____BTC，移轉手續費_____BTC，
   移轉區塊BlockChain編號_____，區塊BlockChain時間_____

另執法機關可能同時於多個現場執行搜索扣押，如何保全數位證據，執法機關需前置預備錢包數量及成本爲何、現場管理錢包之作爲、扣押物送往地檢署之方式及發還或變現可能遭遇之問題，以下分別論述：

（一）以現場區分：

此方案係「一現場一錢包」，且直接將硬體錢包視作扣押物，故執法機關需先行準備硬體錢包攜至現場，命當事人將擁有錢包內之全數比特幣移轉至執法機關之錢包中，待移轉完成，將硬體錢包

貼上封條，並於扣押物品目錄表載明當事人簽名，而當事人僅能目視密封袋上執法機關錢包帳號之標識，無法檢視錢包內之電磁紀錄。保管方面，經確認移轉程序完結後，再將一個或多個錢包（依該案搜索現場數量而定）逕送地檢署贓物庫。

發還之際，需開啓已封緘之硬體錢包，且執法機關需辨識應發還之帳戶係儲存於何處之硬體或軟體錢包。若因故有立即變現之需要，變現後，需進行第二次之封緘程序。

（二）以案件區分：

此方案採取「一案一錢包」，此方式之優點在於，節省錢包使用數量，可節約經費與時間[48]，亦毋須將錢包攜至搜扣現場，避免錢包在運送途中遺失或毀損之風險，只需要求涉嫌人將所持錢包內之案關比特幣移轉至指定之錢包位址，移轉完成後，由執法機關於扣押物目錄表載明並請當事人簽名確認。

結案發還時，開啓封緘之硬體錢包，若因故有立即變現之需要，變現後，需進行第二次之封緘程序。此外，一案一錢包之方式尚須與檢方溝通並協調移交方式，譬如於地檢署時再進行第二次移轉至檢方錢包，或由檢方直接認扣執法機關之硬體錢包。

前述兩方案，各有其優劣，除預算成本之考量外，值得討論之相關問題包括：（1）若需扣押不同種類之虛擬貨幣，其硬體錢包之工作初始化程序不同，例如比特幣與乙太幣應存放於不同硬體錢包，若臨時發現應予搜索之新現場，而現有硬體錢包數量不足或載送路途遙遠，恐無法進行有效之扣押程序。（2）因硬體錢包無法開啓封緘確認所儲存之電磁紀錄，如何取得當事人同意並完成簽名確認。（3）若檢方不認同司法警察機關所檢附之硬體錢包爲正式扣押物，無法由贓物庫保管時，有無其他扣押方式（4）若單一涉嫌人擁有數個比特幣錢包且分散於不同搜索地點，發還程序將牽涉數個硬體錢包，執法機關恐難以應對，若發生需部分發還或部分變現問題，數個硬體錢包亦增加管理難度。兩方案之簡介及差異統整如下：（參考「表五」）

[48] 以硬體錢包 Trezor 為例，每個價位約為 4,500 元，而錢包工作初始化需費時 4 小時。

表五、搜扣二方案之簡介及差異比較表

	方案一	方案二	爭點 / 補充說明
區分方式	依現場 （一現場一錢包）	依案件 （一案一錢包）	若扣押不同種類之虛擬貨幣，其硬體錢包工作初始化程序不同，例如比特幣與乙太幣就需要存放於不同硬體錢包
成本 / 時間支出	依現場數量購置錢包數量	4,500 元 / 個 4 小時 / 初始化	每支 Trezor 售價約 4,000 元，訂購時間 1 至 2 個月，每次初始化需使用 24 張拍立得，費用約 480 元；每一硬體錢包初始化工作包括錄影等約 4 小時
執行方式	錢包「需」攜至現場；當事人移轉 BTC 至至執法機關錢包；載明於扣押物品目錄後請當事簽名確認（當事人無法檢視錢包內之電磁紀錄）	錢包「不需」帶至現場；當事人移轉 BTC 至至執法機關錢包；載明於扣押物品目錄後請當事簽名確認	若臨時新增搜索現場，且錢包數量不足或載送路途遙遠時，恐無法進行有效扣押程序；因硬體錢包無法開啓封緘確認，如何取得當事人同意並完成簽名確認
搜扣管理	依現場數量保管多個錢包	一案管理一錢包	中心化管理或分散式管理，前者易生遺失之風險
檢方認定	視爲扣押物逕送檢方贓物庫	移送檢方方式待確認	若檢方不認同司法警察機關所檢附之硬體錢包爲正式扣押物，有無其他扣押方式
發還 / 變現	辨識應發還之帳戶原儲存之硬體錢包；開啓該等硬體錢包封緘；移轉比特幣進行發還或變現；需要第二次封緘	打開硬體錢包之封緘；移轉比特幣進行發還或變現；需要第二次封緘	若當事人擁有多個比特幣錢包且分散在不同搜索地點時，發還亦將牽涉多個硬體錢包；部分發還或部分變現時，多錢包亦將難以處理

二、加入國際組織訴諸跨國合作

如前所述，歐洲刑警組織已於 2015 年相關文件中指出，多數網路犯罪或洗錢、詐欺及吸金等犯罪均與比特幣等虛擬貨幣相關，包括非法融資和與該技術相關之非法活動。其中，EC3 扮演至關重要之角色，其與各會員國之執法機關保持良好之合作關係。

EC3 成立於 2013 年，係歐盟跨區域網絡犯罪專家小組，主要協助執法部門因應網絡攻擊，尤其是比特幣等虛擬貨幣相關之洗錢犯罪；該組織曾於荷蘭海牙的歐洲刑警組織（EUROPOL）總部舉行多次會議，探討虛擬貨幣跨境犯罪問題，除歐洲各國執法機關齊聚一堂外，美國 FBI、FinCEN 等機關亦與會；會議中，曾爲全球最大虛擬貨幣交易平台業者 Bitfinex（執行長 Jean-Louis van der Velde，EC3 主要技術諮詢顧問）倡議由該組織發起，建立一全球執法網絡以對抗虛擬貨幣相關之犯罪。

EC3 於 2017 年 6 月 22 日至 23 日舉行「第 4 次虛擬貨幣會議」（4th Virtual Currencies Conference），主題爲「進一步加強打擊濫用虛擬貨幣進行犯罪交易和洗錢的活動」，參與者除歐美各國之執法機關，尚包括私部門業者如 Bitcoin.de、Bitfinex、 Bitpanda、Bitonic、Bitstamp、Bitpay、 Coinbase、Cubits、LocalBitcoins、Spectrocoin and Xapo 等， 惟該次會議僅日本、新加坡 2 亞洲國家參與。該次會議論及，鑑於虛擬貨幣洗錢等犯罪活動的發展日益全球化，亟需各執法機關建立全球情資交換網絡。

我國 IT 產業發達、資訊人才充沛，2016 年更破獲○○銀行之 ATM 遭跨國犯罪集團盜領案，顯示執法人員於網路安全、資安鑑識領域之專業素養。2017 年中全球爆發勒索病毒 WannaCry 之一連串事件，受害者遭勒索支付比特幣爲贖金，臺灣更名列於全球第三大數位重災區，正因比特幣之匿名性易造成資金追查之斷點，而「電腦犯罪無疆界、數位國土需捍衛」，我國更應積極尋求納入如前述之虛擬貨幣跨境犯罪情資交換平台。

捌、結論

刑事偵查程序方面，因比特幣係去中心化之特性，無法透過一專責機構凍結涉嫌人不法所得，唯一之扣押方式即「移轉錢包控制權」，即將涉嫌人之比特幣錢包中之餘額與公、私鑰，一併移轉至執法機關之錢包中；目前實務上除比特幣外，尚有乙太幣、萊特幣、比特幣現金（Bitcoin Cash）等較爲流通之加密貨幣，是否採取前述之搜扣流程，有待執法單位與院、檢機關進一步整合相關辦法。

跨國合作方面，FBI、EC3 等國際間重要之網路犯罪專責單位，皆致力於虛擬貨幣等洗錢相關犯罪之國際情資交換與技術協助。以 EC3 爲例，目前僅爲數不多的亞洲國家參與，我國或可探詢加入該執法網絡與情資交換平台之可行性。

另本局職掌包括洗錢防制與國際合作等業務，亦爲我國之金融情報中心，跨國合作係全球防制洗錢不可或缺之環節，面對虛擬貨幣等相關犯罪態樣多樣化、全球化之趨勢，而我國虛擬貨幣之法律定位仍未明，應於虛擬貨幣犯罪如日本般嚴重惡化前[49]，應及早擬定相關犯罪防制策略及刑事偵查程序（即本文比特幣之「搜索扣押程序」），以防患未然。

[49] 同前註 16。

參考文獻

期刊論文

蘇文杰，〈論新興洗錢犯罪手段之實證研究－以比特幣之虛擬貨幣爲研究中心〉，國立交通大學碩士論文，2016 年。

臧正運、曾宛如、方嘉麟，〈從區塊鏈融資論眾募規範趨勢〉，《月旦法學雜誌》，第 273 期，2018 年 2 月。

中文書籍

杜宏毅，〈BLOCKCHAIN 的前世今生與未來－一本 BLOCKCHAIN 的閱讀筆記〉，臺灣網路認證股份有限公司出版，臺北（2016 年 8 月 1 日第三版）。

外文期刊

Wood, Robert W., Bitcoin: Tax Evasion Currency, FORBES, 7 August 2013.

其他外文參考文獻

Financial Action Task Force, "Guidance for a Risk-Based Approach Virtual Currencies," June 2015.

National Crime Agency, "National Strategic Assessment of Serious and Organised Crime 2015," June 2015.

The European Police Office, "The 2015 Internet Organised Crime Threat Assessment," Europol, 30 Sep. 2015.

第五部分

國外洗錢防制資料

FATF 指引[1]：私部門資訊分享[2]

譯按：

本譯文業經 FATF 秘書處授權刊戴於本年報，原文請參閱 http://www.fatf-gafi.org.，最後查閱日為 107 年 5 月 30 日。

一、前言

（一）背景與架構

1. 有效的資訊分享係洗錢防制 / 反資恐（AML/CFT）架構運作良善的基石，建設性與即時的資訊交換係 FATF 建議之重要要求，並涵蓋許多建議與直接成果，為了洗錢防制 / 反資恐（ML/TF）風險管理的目的，金融機構不應無理地被排除於資訊分享之外。
2. 金融機構例如銀行，基於 AML/CFT 目的之資訊分享，在同一集團內可能發生在不同層次，其他金融機構諸如金錢與價值移轉服務業（主要經由營業員與其他分銷管道操作）也存在不同的業務模式與結構。有效資訊分享的基本目標，適用於所有以不同結構營運的金融機構。

[1] The FATF Report "FATF Guidance：Private Sector Information Sharing" 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.

[2] 本文係由本局洗錢防制處翻譯。

3. 資訊分享也發生於不同的主體與部門間，例如在非屬同一集團之金融機構與公部門間，反之亦然。這樣的資訊流可能發生於國內也可能跨越疆界，公部門間的資訊分享同樣重要，也是當地協調與合作機制效能的重要組成。
4. 資訊分享對防制洗錢、資恐及資助武擴極爲重要，跨國洗錢計畫無視國界，資訊分享的障礙會對 AML/CFT 機制的效能產生負面影響，反而協助犯罪網絡的運作，因此突顯對跨國與全球範圍之多元來源資訊有著快速、有意義、全面分享的重要性。
5. 藉由提供情報、分析、必要數據予金融機構與相關權責機關以預防並打擊 ML/TF，資訊分享成爲提升金融透明度、保障金融體系整合的重要關鍵。同樣地，金融機構尋求公部門協助，以分享趨勢分析、行爲模式、制裁對象、地緣弱點，俾更好地管理所曝風險、監測交易金流、向執法機關提供更有用的訊息，公、私部門均可作爲資訊流之源頭與標的，此種模式的資料運用係著重在公、私部門的持續對話。對資訊分享的仰賴，亦表現出日益著重於辨識出可能侵害體系效能之資訊分享障礙的國際努力，並以發掘可能的政策路徑與實務作法克服之。
6. 依據與資訊分享相關的 FATF 建議及注釋，FATF 於 2016 年 6 月提出資訊分享整合標準[3]。該套整合標準包含既存且尚未修訂的相關期待，其目的在增加其價值並釐清有關資訊分享的要求，涵蓋達 25 項建議的內容，並影響效能評鑑方法論中 7 項直接成果，本件指引即爲該議題之起始點。

（二）指引的目的、目標讀者、內容與地位

7. 指引的目的：
   - i 聚焦於私部門主體（特別是金融機構）間資訊分享對其提升反洗錢及反資恐效能的益處。
   - ii 辨識出抑制集團範圍內或非屬同一集團之金融機構間資訊分享的關鍵挑戰。
   - iii 釐清 FATF 關於資訊分享的標準，包括：a）集團範圍內

[3] 請參照 FATF 網站。

AML/CFT 的計畫，及在此架構下，關於集團內可疑交易的資訊分享，STR 如何保密及資訊分享相關的揭密條款；b）非屬同一集團金融機構間者。

iv 突顯資料、隱私保護（DPP）及 AML/CFT 權責機關間協調以達成共同整合目標之國家範例。

v 提供促進集團範圍內及非屬同一集團金融機構間資訊分享，與公、私部門間建設性合作之國家範例。

vi 支持經由國家或國際層級資訊分享以有效執行的 AML/CFT 機制。

8. 指引的目標讀者：

i 各國政府及其 AML/CFT 權責機關。

ii 私部門的參與者，包括必須履踐集團內 AML/CFT 計畫義務及與其他機構間處理客戶交易的金融機構。

iii 國家與超國家 DPP 主管機關。

9. 本報告指出資訊分享的挑戰，並爲集團範圍及非屬同一集團金融機構提供指引。附錄 1 說明 DPP 機制的差異及其施行對資訊流的影響，附錄 2 內容爲因應這些挑戰的國家範例與途徑，包括國家 DPP 及 AML 主管機關合作並符合各自的目標，也提出各國創新的實踐以提升集團範圍及非屬同一集團金融機構間的資訊分享，該章節包含各國相關機制建立及確保爲私部門提供指引與回饋的流程範例，俾有助於所有參與者間的資訊分享。須注意的係這些範例僅供參考，僅屬說明性質，並非 FATF 建議的方法，這些範例在本報告不同章節中前後參照。當思考本報告所呈現的一般原則時，主管機關必須思考國家層級的問題，包括法制架構。本報告不具拘束力，其彙整各國及私部門的經驗，協助權責機關及金融機構更有效能地執行 FATF 建議。

二、一般資訊分享議題

10. 資訊分享扮演了重要的角色，使金融機構、監理機關及執法機關得以依據風險爲本方法，更妥善地分配資源，並發展創新的技

術以打擊 ML/TF，國際金融體系的規模與地緣因素使所有參與者的協調與合作不可或缺，若要讓辨識並預防 ML/TF 措施成功的話。落實資訊擴大分享係合作的要素，無論是否爲跨國性或涉及金融集團內、非屬同一集團金融機構間，或公私部門間。

11. 強化資訊分享，對於可行之 AML/CFT 防範改善措施的完全實現，以及享用具備新技術和創新商業模式之金融服務，亦至關重要，然而限制有效資訊分享的障礙仍然存在，足以妨礙進步並導致法令規章的不確定性。已知的挑戰探討如下：

A. 法規議題

12. 法律限制可能阻礙基於 AML/CFT 目的之資訊取得、使用與提供，這可能導因於不同的政策目標、客戶資料保護及紀錄保存的要求，在某些案例中，受規範主體不確知法規是否允許資訊分享，這種認知不足限制了資訊的有效分享。各國應克服挑戰並執行有效的資訊分享法制，在相關領域運用不同的法律條款，提供指引以釐清法令規章並減少分享相關的困惑。
13. 這些困難尤導因於下列問題：

    i. 相異的 DPP 法律架構及其執行

14. 各國的 AML/CFT 的法規係設計以預防、偵測、阻斷、調查、追訴 ML/TF，個人有權[4] 保有隱私與保護個人資料，這在許多國家都是基本權，這些權利展現出與各國國內法基礎原則相符的重要政策目標，而 AML/CFT 的目標亦符合國家重大安全與公共利益，應盡力實現，但須與保護個資及個人隱私達成平衡， AML/CFT 與 DPP 的政策目標並非相斥，而須瞭解、支持並求取平衡。
15. 不同司法管轄的 DPP 法令差異會在執行上造成問題，特別是對私部門的資訊分享，當該國缺乏法令指引或缺乏對於 AML/CFT 要求與 DPP 義務一致性時，這個問題將進一步複雜化，AML/CFT 與 DPP 的衝突可能肇因於不同主管機關在立法階段缺乏協

[4] 個人資料意味著與自然人相關的所有資訊，足以直接或間接地識別，透由諸如姓名、ID、位址、線上識別或其他與該自然人相關一個或多個物理、生理、基因、心理、經濟、文化、社會識別的識別因子。

調，在資料保護與預防及打擊犯罪間未能求取妥適的平衡，目前相異 DPP 法制的複雜性、規避裁罰與風險，對私部門資訊的取得、分送與分享造成重大衝擊，即使這樣的分享是法律允許的。

16. 然而在某些情況下，DP 主管機關試著支援公、私部門參與者，許多案例顯示，立法者與權責機關知悉有效地管理法規的差異將有助於協調工作，如當資料保護主管機關作出清楚的釋示或指引，指出基於公共利益，爲 AML/CFT 目的進行個人資料跨國傳輸係法所允許的，或係減少資料傳輸的限制（如允許基於 AML/CFT 目的進行之資料傳輸），跨國金融機構將因此獲益。
17. 各國應檢視，如需要的話，應修正或釐清法規以確保平衡，資料與隱私保護機關以及 AML/CFT 主管機關間的對話係有益的，採取兼容一致的政策有助於金融機構遵循法律要求，如有必要，政府亦應發展並分享國家法令的分析以支援有效的資訊分享。（附件 2 第 3 至 7 段）

ii. 金融機構秘密揭露

18. 金融機構秘密法能限制資訊分享，如某些國家法律，金融機構秘密保護有時不因合法利益或安全顧慮而免除，就此，應注意依第 9 項建議要求，各國政府應確保金融機構秘密法不應限制 FATF 建議的落實。

B. 執行挑戰

19. 執行挑戰可能發生在國際或國家層次，金融機構的 IT 能力與其紀錄保存程序可能阻礙即時有效的資訊分享，例如，有些客戶資訊可能對客戶審查（CDD）目的有效，惟並未整合入金融機構 AML/CFT 系統，因爲該資料係因其他目的而蒐集。外包法規可能訂定離岸業務的上限，避免業務集中他國，而資料與資料管理則適用本地法規，本地的 IT 系統與操作可能產生侷限性，因而導致操作的複雜性與流程的斷裂。
20. 不適宜的 IT 技術、相異的資料格式、資訊處理政策與程序的缺

乏及公、私部門對資料價值理解的不足，均對資訊分享造成障礙，儘管這些資訊都是可以取得的，IT 能力與 IT 整合的議題將持續升溫，尤其當金融機構成長並跨足全球，不同 IT 系統的整合對併購機構而言是必需的。

21. 在特定的個案中，公、私部門間或私主體間的資訊交換常仰賴預先設定好的規則俾進行資訊的自動分析與整合，這些規則應有足夠彈性以考量其他金融機構可取得之資訊（如 IP 位址、電話號碼、使用者姓名、職銜、任職單位等），資訊格式的標準化，透由資訊整合得以促進資訊分享。

C. 監理者的挑戰

22. 依監理者的觀點，缺乏資訊分享會限制基於 AML/CFT 目的之統合性監理的執行（如第 26 項建議的要求），例如透過不同國家或地區分行或子行網絡營運的金融機構，所在國法律（分行或子行所在國）可能不會允許母國監理機關取得或檢視分行、子行保管的所在客戶資料，各國監理機關之間因此須進行個別安排，或由所在國監理機關代表母國監理機關檢視客戶資料，這可能阻礙即時且全面性的交易紀錄審查，相對地影響基於 AML/CFT 目的之統合性集團監理的有效執行[5]。

23. 因此監理機關應推動雙邊或多邊協定的簽署以推動以有效支持基於 AML/CFT 目的之資訊分享，尤其著重在統合性或集團範圍對資訊分享的監理，以及對即時性的定義。然而該等安排無法完全克服影響資訊分享的法律障礙，因此集團的統合性監理可能被任何因素所阻礙（包括無法取得相關資訊），或集團過度曝險而無法有效管理，母國的監理機關可能因此限制其分行或子行的交易致使集團調升其監理措施，包括在極端情形下令該集團關閉國外營業據點。

三、FATF 建議下的資訊分享

[5] 巴塞爾銀行監理委員會（BCBS）第 13 項核心原則第 8 項基本準則（母國與所在國關係）要求母國監理機關應獲准現地進入銀行集團分行或子行單位，以評估銀行的安全性、健全性及對客戶審查要求的遵循。

24. 本節說明重要的 FATF 建議（第 18 項、第 20 項及第 21 項建議）及其對金融集團內資訊分享的期許，本節亦涵蓋非屬同一集團金融機構間資訊分享，一如 FATF 建議所要求。

A. 金融集團內資訊分享

> 第 18 項建議—內部控制與外國分支機構
> 金融機構應執行防制洗錢及打擊資恐計畫，金融集團應執行集團範圍之防制洗錢及打擊資恐計畫，包含集團範圍內基於 AML/CFT 目的之資訊分享政策及程序。
> 金融機構應確保其外國分支機構適用與母國要求一致之 AML/CFT 措施，經由集團防制洗錢及打擊資恐計畫執行 FATF 建議。

i. 資訊分享架構有關「金融集團」與「集團範圍」的定義

25. 金融集團防制 ML/TF 計畫應適用於金融集團[6]內所有分行與子行，該計畫應包括基於 ML/TF 風險管理與 CDD 目的要求之資訊分享政策及程序。當基於 AML/CFT 之目的[7]，分行與子行的客戶、帳戶及交易資訊應提供予該集團，方能發揮法遵、稽核、AML/CFT 等集團層次 ML/TF 風險監督 / 管理的角色功能，惟僅限於特定目的且應在足夠的安全防護下提供以確保資訊秘密。
26. 依 FATF 詞彙表，第 18 項建議下金融集團 AML/CFT 計畫要求內所稱之「金融集團」，包括集團內所有主體（本地或海外機構），這符合 FATF 建議中有關金融集團係爲一個整體的原則，集團成員單一主體的活動會讓整個集團曝露於 ML/TF 風險下，而這樣的風險須在集團層次辨識、管理並抵減。
27. 如 FATF 詞彙表，金融集團意指一集團由一母公司或其他形式之法人對集團下其他公司行使控制及協調，俾依據核心原則實施集團性監理，包含分公司及子公司應遵循集團層級之 AML/CFT 政策及程序。

ii 集團範圍計畫要求分享之資訊

28. 金融集團內的資訊分享意味著集團有效地辨識、管理及抵減

[6] 第 18 項建議注釋第 4 段。
[7] 第 18 項建議注釋第 4 段。

ML/TF 風險，這應包括異常交易或活動的資訊與分析（如已進行分析），可能包括 STR、其附屬資訊及 STR 申報訊息。政府應以資訊的機敏性及其與 AML/CFT 風險管理的關聯性，決定資訊分享的範圍與內容（詳情參閱第 50 至 54 點），前項要求應與法規訂定（包括當地及分支機構所在國）之資訊分享的範圍、內容和機制相符。

29. 下表說明資訊分享所追求之 AML/CFT 目標，指出集團遵循的資訊分享係爲了確保全面且有效的 ML/TF 風險管理與遵循，下表所列資訊也許無法在每一個案或通案中皆可取得、蒐集或被需求，將視提供予客戶的產品與需求、地理區位、法制架構、風險與內容而定。然而，集團內的區域分享將引導產生有效的集團遵循計畫。

表格 1 資訊分享的 AML/CFT 目的

資訊形式	資訊要素範例	集團內資訊分享目的
客戶資訊	客戶辨識與聯絡資訊（姓名與 ID）、法人與法律安排、營業本質、所有權與控制結構、法律形式與登記證明、註冊地址與主要營業處所、法人識別編碼（LEI）、資產證明、繳稅證明、不動產持有、資產來源、經濟／專業活動、帳戶資料、是否爲 PEP（包括密切關係之人與家屬）、其他經開戶或更新程序取得文件獲知的相關資訊、目標性金融制裁及其他相關資訊，與 ML/TF 相關之公開來源及內部調查辨識，客戶風險分級	管理客戶與地區風險，依據機構內各成員評估全球曝險，更充足的客戶資料紀錄保存。
實質受益人資訊	實質受益人辨識與聯絡資訊、不動產持有、資產來源、經濟／專業活動、帳戶資料、是否爲 PEP（包括密切關係之人與家屬）、其他經開戶或更新程序取得文件獲知的相關資訊	管理實質受益人與地區風險，辨識集團內不同主體之相同實質受益人，更有效的客戶資料紀錄保存。
帳戶資訊	銀行／其他帳戶細節、包括帳戶的預期用途、客戶與企業通聯表示的可能活動／交易地點	集團層次有效的客戶與交易審查，面對面交易所在，集團內警訊與異常交易模式的追蹤。
交易資訊	交易紀錄、信用與借記卡紀錄及使用情形、過去債信，數位軌跡（IP 位址，ATM 使用）、嘗試／失敗交易資訊，現金交易報告、關戶或因可疑終止商業關係、偵測異常或可疑交易之分析	全球交易監控，發出警訊與辨識可疑交易，標識並確認集團內相同交易模式。

iii 集團範圍計畫資訊分享的重要性

30. 廣義而言，集團範圍之資訊分享對於金融集團有效辨識、抵減及管理 ML/TF 風險非常重要，也使集團得以更好地進行內部控制，並改善客戶審查、交易監控及可疑交易申報的決策品質。集團內主體包括總公司、子行與分行的資訊分享，使集團遵循得以落實全面性的風險管理程序。取得制裁名單與集團內不同機構的客戶活動資訊，方能以統合性的檢核與監控客戶及交易，辨識可能違反目標性金融制裁之處。

31.BCBS 於 2017 年公布「洗錢及資恐相關風險的健全管理」指引[8]，亦爲銀行提供關於集團範圍及跨境 ML/TF 有效風險管理的全面性指引，它說明了統合性風險管理的合理性與原則，集團範圍的 AML/CFT 政策與程序應如何在集團內持續地進行，在反映當地商業利益考量及所在國要求的同時，亦應符合並支持集團內更廣泛的政策及程序，及銀行應如何應對母國與所在國要求的差異性。該指引亦爲集團成員提供詳細資訊，銀行應如何以通知並加強集團範圍風險評估，與更有效執行集團範圍 AML/CFT 政策及程序的角度[9]，和其他成員進行資訊分享。

32. 以下爲集團範圍計畫資訊分享預期的成果：

a) 全球風險評估

33. 對有效的集團範圍遵循計畫而言，金融機構應理解其在全球基礎上曝露的 ML/TF 風險，這些風險可能來自其營運的客戶、產品及地緣概況，交易模式或集團內其他主體之因素。這些風險的全面性理解與辨識將使金融機構更妥善地組織其風險圖像並採取全面性的措施。分行、子行及其他部門提供的資訊，應匯入全面性的風險評估，此將有助於辨識並判別集團內各主體對該集團造成的 ML/TF 風險本質與程度，以及該集團於全球基礎上的 ML/TF 風險程度，特別是跨境關係的資訊分享。因此，能夠即時獲得或使用相關資訊，對集團遵循至關重要，國外營運

[8] 參照 BCBS「洗錢及資恐相關風險的健全管理」指引。

[9] 無論其所在位址，各個單位應維持有效的監控政策與程序，並與該地與該機構的風險相符，地方性的監控應透過與總部的資訊分享達成。

處所亦應配合提供。舉例來說，設在 X 國的 A 銀行辨識出洗錢者並關閉其帳戶，但同一人在 A 銀行 Y 國子行也有帳戶，該子行如果並不知道 X 國 A 銀行所採取之行動，將持續爲該洗錢者提供銀行服務。當金融機構評估其在全球基礎上曝露的 ML/TF 風險時，也應該審酌可能有礙 FATF 建議落實之資訊分享障礙，將其視爲自主風險，並據此考量抵減的措施。

34. 集團遵循的資訊分享（如在總公司層級）不預設 ML/TF 的風險只應藉由集團遵循對集團內所有營業單位進行評估，每個營業單位應有權負責評估本身 ML/TF 的風險，並應掌握其個別風險評估的相關資訊。故而跨國集團內某一特定國家的營業單位也同等有權取得來自集團遵循或其他部門與其風險評估相關的資訊。一個跨國集團因此應建構一套風險評估與管理的機制，以決定何時應要求其營業單位進行與客戶往來相關的跨國風險評估，以及何時要求其營業單位跨域分享客戶或交易資料方爲正當。

35. 此外，紀錄的集中保管不等於集團範圍內的資訊共享。電子 / 集中儲存資料的使用，應符合機密及其他管理義務，全球交易監控須以強化集團內所有營業單位之風險管理與申報義務的遵循來落實，因此，對某地營業單位的監控，不會弱化集團內其他營業單位的法遵義務，但應考慮各地機密資訊取得的法律限制，並配合金融集團執行的相應措施以應對全球風險。

b) 客戶、產生、服務及地域風險的有效抵減

36. 發展妥適的措施以抵減客戶、產品、服務及地域風險，需要取得經由客戶、產品及服務所顯現之客戶、交易模式、交易 / 活動預期位址等有關資訊，需要時，亦包括資金的來源與流向。金融集團獲得的資訊將有助於設計妥適的措施以管理並抵減風險，舉例來說，以客戶的全面風險評估或客戶評等爲基礎，金融機構得以設計政策在額外的或強化的客戶審查措施，更嚴密的交易監控程序，與特定客戶面對面互動，或更頻繁地檢視客戶資訊。

37. 同樣地，金融機構落實集團遵循分享關於已辨識新興或既存的商品或服務的資訊，及爲抵減風險採取的措施，將有助於該集

團在跨國市場採取一致的方法，惟有集團遵循能取得客戶及其交易與活動程度，和基於客戶資訊的任何異常模式等資訊，集團層次的抵減措施方能有效落實。舉例來說，X 國係貪腐之高風險國家，而該國某 PEP 指示匯出與其背景不符的大額匯款，且對銀行的詢問欠缺合理說明，銀行最終關閉其帳戶，惟同一人在同一銀行集團的 Y 國帳戶進行匯款交易，並謊稱資金來源與交易目的，Y 國的分支機構如未知悉 X 國帳戶已關閉，將影響其對該客戶妥適的風險管理，亦不利於辨識潛在的跨境 STR，此類 STR 係以集團內不同來源之資訊爲基礎。

c) 一致性的控制運用

38. 全球企業的地方營業單位必須遵守地方的法規，同時也須遵守集團範圍的遵循計畫，以確保跨集團層次一致性的控制運用。集團範圍控制的執行與程序，有賴金融機構集團遵循的相關資訊分享，假設分支機構所在國之 AML/CFT 規範較母國寬鬆，當所在國法令允許的情形下，金融機構應要求外國分支機構落實母國的法規要求。如所在國不允許內部控制的妥適執行（包括資訊分享，如 FATF 建議要求），金融集團應採取額外的妥適措施以管理 ML/TF 風險，並通知母國監理機關，若額外措施仍有不足，母國的權責機關應考慮額外的監理行動，包括對金融集團施加額外的控制。例如，當風險超乎機構的承載能量，無法採取相應措施以管理風險時，適時要求金融集團結束在該國的營業關係[10]。

39. 資訊有關於客戶辨識，及接收政策、內部及外部稽核報告、監理機關的現地檢查報告、裁罰、採取的改善措施、紀錄範例以證明完成的客戶審查措施、申報及遵循的紀錄保存等，當合宜地與集團遵循分享，將有助於執行情形的評估，並可強化企業的全球控制，將每個國家與地點的特性納入考量。舉例來說，缺乏 X 國 A 子行的 CDD 與紀錄保存措施，將會削弱銀行集團控制的整體效能，全球規模的金融機構可釐清這些措施的執行，如果集團遵循得以取得這些紀錄爲樣本基礎。

[10] 注釋 18.5。

d) 多元產業金融集團之共通方法

40. 金融集團經常跨產業經營（銀行、證券、保險、商品等），集團範圍的遵循意味著這些集團必須監控並分享整個集團客戶辨識、交易及帳戶活動的資訊。因爲每個部門有不同的 AML/CFT 要求，故須加以調整，資訊分享有助於在一致性的基礎上推動整體性的風險管理，舉例來說，A 金融集團下有銀行、證券及保險部門，高風險客戶 X 有不明現金存入銀行帳戶，該交易應發出警訊並傳知集團各部門，如果缺乏這類的資訊，該客戶將得以在其他部門繼續交易而不會遭遇相同的監控或額外的客戶審查。

B. 金融集團內疑似不法金流或資恐相關資訊分享

> 第 20 項建議－申報可疑交易
> 金融機構如懷疑或合理懷疑資金係犯罪活動的不法所得，或涉及資恐，應即依法向金融情報中心申報。

41. FATF 第 20 項建議要求金融機構申報可疑交易，如其懷疑或合理懷疑資金係犯罪活動的不法所得，或涉及資恐。第 20 項建議僅要求出於誠信地申報可疑活動，是否涉及刑事責任，是由國家的權責機關來決定（如執法機關）。
42. 近年的科技進步已提升金融機構的分析與處理能力，來自不同的營業處、產品、服務及部門的資訊流，得以更深入地辨識交易趨勢與態樣。數據科技與分析的進步，使金融機構得以從大量結構性或零散的數據中篩選，以辨識模式與趨勢。充分運用現代數據科技符合公、私部門的利益，也需要儘可能匯聚更多的資訊，通常形成一資訊庫。
43. 異常交易或活動資訊與分析的分享，包括 STR、其附帶資訊、分支機構所申報 STR 之事實，將提升集團範圍遵循計畫的落實[11]，同樣地，當與風險管理相關且適宜時，分支機構應自集團

[11] 艾格蒙聯盟於 2011 年 2 月發布「集團範圍 STR 分享白皮書：議題與方法」，該報告列出跨境分享 STR 體制的議題，也介紹可能的方法推動企業分享 STR，該報告結論認為企業範圍 STR 跨境分享需要相關司法管轄體協調相關領域的行動。

層級的部門接收此類資訊。此原則同時適用於國內與跨境的情形，因爲客戶可能跨越集團各服務部門或跨越集團的不同營業處，前述的作法可以使金融機構跨業別辨識高風險客戶，並採取特別的監控機制或強化措施，也能突顯金融機構對該類客戶的全球曝險狀態，進而落實有效的風險基礎方法。這樣的分享可能發生在金融機構申報 STR 的前後，促使集團遵循在集團跨層級、跨業別、跨國營業處所均關注該可疑客戶的活動或交易，這也讓集團得以採行對可疑活動的精密分析、評估對顧客的分析，並設想全球營運的各種可能性（附錄 2 第 8 點）。

44. 在資恐的框架下，即時分享極爲重要，金融集團內相關資訊的立即分享係關鍵，特別是與高風險客戶（因其交易紀錄或來源國）相關時。若能取得集團內相同客戶的交易或受款人資訊，金融機構對某筆可能涉及資恐交易的初步懷疑才可能進一步被確認；也唯有客戶或受款人引起注意，初步懷疑在集團內分享時，前述的交易鏈才會被檢視。然而，疑似資恐相關的資訊分享以及獲取進一步確認資訊的流程，不應造成可疑交易發生地立即申報 STR 的遲延。

45. 法律上對資訊分享的限制，可能導致同一集團內，集團範圍遵循計畫的執行不一致。舉例來說，某分支機構對特定客戶或交易提交 STR，如另一部門並未獲知，可能疏於注意相似的可疑行爲，而未審視或提交 STR，這將限制集團範圍全球遵循計畫的執行。此外，也可能造成這樣的情形：當前述狀況可能使整個集團被其他國家視爲未充分遵循時，最初察覺可疑交易的分支機構將成爲眾矢之的。然而，當資訊分享的法律障礙導致有效溝通的困難時，金融集團的故意不遵循不應被歸咎。金融機構亦有義務建立資訊分享的文件標準化（符合在地國的法律要求）以支持集團範圍的風險管理遵循計畫，確保資訊秘密的保護並限於 AML/CFT 目的的使用。集團範圍的風險管理仍存在挑戰，金融機構應採取合宜的額外措施管理 ML/TF 風險，並適時通知母國的監理機關。

C. STR 的保密與揭露及其與集團範圍分享的關係

> 第 21 項建議－揭露與保密
> 金融機構及其董事、經理人及職員應：
> (a)…
> (b) 法律應禁止洩露已向金融情報中心申報可疑交易報告（STR）或相關資訊，本規定並未禁止第 18 項建議的資訊分享。

i. 集團內可疑交易資訊分享的疑慮與可行方案

46. 分享 STR（或分享已申報之事實或其相關資訊）的主要疑慮在於確保其機密，這是申報機制有效運作的關鍵，STR 保密故而申報對象與第三方不被告知，反之會對情報蒐集與調查產生不利影響，使持有人隱匿或移置資產。保密也能維護申報對象的名譽，也保障並維護申報者的安全。機密的破壞可能損及整個可疑交易申報機制，金融機構未經允許地揭露 STR 在許多國家可能構成刑責，相關疑慮必然阻礙了 STR 分享。
47. 如跨境分享將使 STR 機密性的議題趨於複雜，因爲涉及不同國家的法律，舉例來說，可取得之紀錄（包括在當地國申報 STR 後與母國集團遵循分享）揭露及使用於母國司法程序相關的法律規定，國家准許使用金融機構資料庫等。
48. 另一與 STR 分享相關的疑慮，係資訊如何在國內與國際分享，疑慮亦產生在外國 STR 的處理方式或揭露外國 STR 的資訊如何進入訴訟程序，該等流程尚不明確且因各國民、刑事案件而有所不同。有些國家的法規明定，若與當地 STR 相關，應有主管機關之司法請求與傳票，故主管機關得干預並確保 STR 在合法程序中的機密性，但可能無法保障向外國 FIU 申報的國外 STR。此外，有些疑慮也常存在於 STR 跨國分享的機密保護，包括在請求目的之外的濫用可能，爲政治利益洩露予媒體，以及違反正當法律程序的分享。由 FIU 的觀點，一個主要的疑慮係希望避免第三方（包括第三國政府當局）不合理地取得相關資訊，特別是若 STR 爲自動跨境分享，而非因該等 STR 含有跨國資訊。爲確保跨境分享 STR 的機密性，各國應考量在其法律

架構內，擴張對外國 STR 提供等同於本國 STR 的法律保護。

49. 最後，集團範圍的可疑資訊分享，可能導致金融集團常態性地僅向母國申報 STR，而非向分支機構的所在國政府申報。相關的疑慮是，儘管已向相關的國家申報 STR，金融集團的內部調查可能只會在一個國家（母公司）展開，致所在國的 FIU 無權向該金融機構取得額外的資訊。集團內的協調與內部調查應迅速進行，避免延誤向所在國 FIU 及時申報 STR；而無論是否分享，金融機構應向所在國 FIU[12] 申報 STR，以避免這些疑慮。

ii 金融集團內可疑資訊分享的可能機制

50. 依據一國國內或相關之跨國法律架構，金融集團內異常交易或活動相關資訊分享有不同的方式，作法並非放諸四海而皆準，因爲分享STR之內容在某些國家是禁止的。分享可採行之方式有：(a)；異常交易或活動的資訊與分析之分享，若分析已完成（如事實、交易、背景及文件，含個人資訊），這些資訊內容係說明性的而非細目式的清單，此類資訊的分享不會揭露STR申報與否；(b)揭露STR已申報；(c)揭露STR已申報並分享附屬資訊（如有關可疑的資訊、內部分析或審查的結果，惟不含STR本身）；(d)STR及其附屬資訊的分享。圖表如次：

表格 2. 金融集團內可疑資訊分享的可能方式

可能方式	可疑資訊、內部分析或審查	STR 申報事實	STR
(a)	∨		
(b)		∨	
(c)	∨	∨	
(d)	∨	∨	∨

[12] 在歐盟架構下，金融機構必須向提交資訊主體所在的會員國 FIU 申報可疑交易，如果不存在跨境服務的情形，本即應向母國申報 STR，惟如金融機構在另一會員國有營業據點，仍必須向所在國申報 STR。在某些特例，國家法律會超越走在歐盟的要求之前，歐洲法院已確認，如會員國間尚未建立適足有效的協調機制以有效防制 AML/CFT 犯罪，在法案符合直接提供所需資訊予會員國俾打擊 ML/TF 的情形下，歐盟的法律不會阻礙國家法律規制在該地營業惟並未設置據點的信用機構。

51. 前述資訊分享的重要目標之一，是在跨國集團所有的營運處所強化風險管理及申報義務的遵循，基本原則是，所分享的資訊與集團遵循相關，以完成整個集團及集團內的特定機構 ML/TF 風險管理全面評估。因此，分享的資訊必須有跨境的因素，諸如一客戶於集團內有跨國交易，或其交易或金流涉及跨國之不同營運所，這樣的分享應由集團遵循採取合宜的控制與監控，以保護資訊的秘密並確保其運用僅用於 ML/TF 風險管理。

iii 金融集團內部資訊分享的標準

52. 金融機構應決定以集團遵循爲目的之資訊分享的妥適標準，至於申報 STR 毋須採取此一標準，例如，對某些個案的合理懷疑，可能還不足以申報 STR，但經由集團遵循對該等案例分析的資訊分享，或能揭露額外資訊俾作成申報的決定。據此，金融機構可以在初步偵測到異常或可疑活動時（甚至在交易完成前），即到達 STR 的申報門檻。甚至在許多個案中，爲確認是否達到可疑的門檻，常須更深入的分析，但該等分析結果未必導向 STR 的申報。此外，交易或與客戶間業務關係的本質，可能產生許多與集團遵循目標無關的資訊，例如在地交易，與其他分支機關或部門完全無關時。金融機構應依據其內容、複雜性與實質作出妥適的決定。

53. 每一個案的常態性跨集團分享可能並非必要，對風險管理與申報義務的落實亦不具建設性，金融機構應明確地因應其風險評估與管理架構，爲集團分享時機與類型的決定奠定基礎，以集團遵循爲目標的申報標準應定期評估（諸如集團範圍的稽核與檢視），並接受監理審查。

iv 分享資訊的安全保障

54. 金融機構應建立有關分享資訊足夠的安全保障，以確保 (a) 分享資訊的機密性獲得保障（包括防止被揭露）(b) 資訊僅用在於 AML/CFT 目的，這應包括分享、設定使用之權限及防火牆的政策、協定及程序，例如集團內不同主體間資訊交流之條件（當集團內不同機構有相同的客戶時），因此相關資訊限於在機構範圍內，僅得由專責人員基於 AML/CFT 目的取得。此外，集團

內某機構客戶存在可疑，並不必然自動 / 系統地觸發集團內相關機構申報 STR，但會成爲業務關係風險分析與風險評估的重要要素，並在必要時採取強化的 CDD 措施。

v. 解決法制障礙並與私部門合作

55. 各國應尋求集團內資訊分享法制障礙的解決方案，該等障礙亦限制 FATF 國際標準實踐，應對限制資訊分享的既有法令進行全面檢視與評估（DPP、金融機構秘密、AML/CFT 及其他法規）。與私部門積極的合作，亦得以彰顯公、私部門間對現行法令要求的歧見，對此應提供指引和說明文件，以形塑資訊分享的環境。

四、非屬同一集團金融機構間的資訊分享

56. 在國家與國際層次，有效的 AML/CFT 體系有賴非屬同一集團之金融機構間資訊分享，這包括單一國家內不同金融機構間的資訊分享，及跨國的分享，但同樣面臨前述的所有限制與障礙。要求非屬同一集團間金融機構資訊分享的主要 FATF 建議包括，第 13 項建議（通匯銀行）、第 14 項建議（金錢與價值移轉服務業，MVTS）、第 16 項建議（電匯）及第 17 項建議（依賴第三方），這些建議要求提供或取得特定資訊，以採取必要的預防措施。
57. 第 3 與第 4 節說明不同金融機構間依據重要 FATF 建議的資訊分享，並敘述主動分享額外資訊之益處與如何推動。

A. FATF 建議下的資訊分享

i. 通匯行關係（第 13 項建議）

58. 金融機構應蒐集足夠的資訊以充分瞭解其委託機構的業務本質，評估委託機構的 AML/CFT 控制，並對其過渡帳戶的使用模式感到滿意，包括瞭解委託機構經此業務關係所希望服務之客戶類型，所預期的交易性質與金額等，特定個案中，某些交易觸發通匯行交易監控系統之警訊，通匯行可能要求委託機構提供額外資訊以審視受委託之交易。然而，通匯行對相關資訊的檢視，

並非是對委託機構的客戶進行 CDD，也不應導因於此，僅是通匯行對與委託行間往來交易之審視結果[13]。

59. 委託機構應能回應通匯行的請求，就特定客戶與交易提供額外資訊，惟囿於資訊分享的限制，導致相關資訊不足，通匯行可能無法採取妥適的 AML/CFT 控制以管理此種業務關係的風險[14]。此類狀況下，如果缺乏進一步的資訊，通匯行別無選擇只能中止業務關係，最終導致交易被延遲甚至是通匯業務關係的終止，因此加劇去風險化的現象（附錄 2 第 12 點）。

60. 爲避免上述狀況，應有合宜機制使委託金融機構與通匯行分享所請求的資訊，爲此，委託機構之主管機關應理解並釐清在何種情形下，通匯機構得請求資訊以及得請求資訊的形式，方能建立合宜的分享機制俾使委託機構進行資訊交流，各國政府亦應鼓勵委託銀行的回應性，並明確地規範其與通匯行分享資訊的義務。

61. 必要時，各國政府考量應評估其現有法制架構以因應其此領域資訊分享的挑戰，確保關於資料保護、金融秘密條款或其他法規不致令其金融機構失去通匯服務，而公、私部門的對話與合作，有助於進一步辨識需要特別指引的領域與議題。

ii 金錢與價值移轉服務業（MVTS，第 14 項建議）

62. 依據第 14 項建議，透過代理人提供服務的 MVTS（無論其地點）應納入 AML/CFT 計畫，監控對其對計畫的遵循，並要求代理人分享資訊予其 MVTS 服務提供者，俾使其得有效審查其交易。代理人所回饋與分享的資訊除有助於 MVTS 服務提供者善盡審查義務，亦有益於交易審查與申報機制。

63. 適當情形下，針對可疑交易的資訊分享，可協助 MVTS 服務提供者妥善地管理其 ML/TF 風險，確保對現行風險管理與申報義務的遵循，各國應考慮發布相關必要的指引，以辨識並因應任何影響資訊分享的障礙。

iii 電匯（第 16 項建議）

[13] 參照 FATF 通匯行指引（特別是第 3、第 4、第 5、第 18 點）。

[14] 參照 FATF 通匯行指引（特別是第 32、第 4、第 5、第 18 點）。

64. FATF 第 16 項建議要求各國，應確保金融機構對國內及跨境匯款交易取得正確的匯款人資訊、受款人資訊與相關電文，並確保該等資訊留存於完整支付鏈中的匯款或電文。第 16 項建議的目的，係確保 FIU/LEA（Law Enforcement Agency，執法機關）可立即取得電匯交易匯款人與受款人的基本資料，也讓匯款行、中介行、受款行執行交易審查並申報 STR，檢核制裁名單、凍結並追蹤匯款金流[15]。

65. 在相關資訊漏失情形下，中介行與受款人應採行風險爲本的政策與程序，以決定 (a) 何時執行、拒絕或中止欠缺匯款與受款資訊的交易，及 (b) 合宜的後續作爲。例如，要求支付鏈上前一金融機構儘速提供漏失或不完整的資訊，更基本地是，匯款人與受款人的基本資料對金融機構而言，係辦理電匯的必要資訊，而相關資訊的遞送一般而言，並非由 AML 相關法規所授權。

66. 阻礙金融機構分享相關資訊的限制，會嚴重拖延處理流程，各國應建立合宜的法制，移除相關領域資訊分享的障礙，妥適的指引與回饋可以進一步釐清金融機構對法規的期待。

67. 此外，如同第 16 項建議注釋，MVTS 服務提供者應直接或經由其代理人，遵循其營運所在國有關第 16 項建議所有的要求，當 MVTS 服務提供者同時提供匯款方與受款方服務時，MVTS 服務提供者應：(a) 考量雙方所有的資訊以判定該交易是否可疑；(b) 必要時向適當的 FIU 申報 STR，並提供相關的資訊予 FIU[16]。MVTS 服務提供者若辦理跨境交易應提供資訊交流。各國政府應移除資訊分享的現行法律障礙，規劃提供合宜的指引，俾使 MVTS 服務提供者遵循相關要求。

iv. 依賴第三方（第 17 項建議）

68. 依據第 17 項建議，金融機構得要由第三方（無論是國內或跨境）執行第 10 項建議 CDD 措施 (a) 款至 (c) 款之要求或推廣業務，這些要求包括：(a) 客戶辨識；(b) 實質受益人辨識；(c) 業務關係之目的與性質。委託之金融機構應能立即獲得前述相關之必

[15] FATF 第 16 項建議注釋第 1 段、第 2 段。

[16] FATF 於 2016 年 2 月發布 MVTS 風險基礎方法指引第 67 點。

要資訊，並採取妥適的措施，以確保當其提出請求時，可毫無延誤地自第三方取得辨識資料與其他 CDD 文件。

69. 採行依賴第三方程序的前提在於金融機構可自第三方取得相關資訊，爲了解業務關係的目的與性質，可能需要分享額外資訊，例如客戶財務狀況。這有助於研判執行的交易是否符合金融機構對於客戶的認識，營業與風險認知，而資訊分享限制或法制上的不確定性將使金融機構無法依賴第三方，尤其是跨境關係。基於該依賴關係，當母國已准許該金融機構提供資訊時，有賴第三方所在國政府介入，以移除阻礙第三方分享資訊予金融機構的既有障礙。

v. 金融機構的規範與監理（第 26 項建議）

70. 在 FATF 建議有效執行的架構下，爲求跨境的監理，在兩國法律架構允許的範圍內，金融機構母國的監理機關有權取得海外分支機構所持有之客戶、帳戶與交易資訊，這應包括 STR 與相關的資訊，因爲這對 AML/CFT 義務遵循及風險管理程序穩健性的評估是必要的。如同所在國監理機關評估金融機構對當地法律及義務的遵循，母國監理機關應可評估集團範圍 AML/CFT 政策與程序的遵循。若缺乏該等評估，將減損母國監理機關有效評估集團遵循的能力，進而影響 FATF 建議的有效執行。如果資訊分享的障礙無法克服，且無其他滿意的替代方案，母國的監理機關應使所在國監理機關明確瞭解，將對該金融機構採取額外的監理作爲，諸如集團內強化的監理措施，包括合適時，要求母國集團結束在當地國的營運[17]。

五、資訊分享的創新

(一) 超越 FATF 建議的資訊分享

71. 金融機構間額外資訊的分享—超越前述 FATF 建議所要求的資訊—可能更有助於強化對風險與弱點的認知，亦確保私部門具

[17] 參照 BCBS，2017 年 6 月出版，洗錢及資恐相關風險健全管理指引，第 4 部分。

備更佳遵循與調整能力，防止犯罪者有機可趁。

72. 舉例來說，有些國家已經發現分享警訊或關於因 ML/TF 而拒絕往來或被排除的客戶資訊，可防止罪犯的心存僥倖，渠等企圖與多家金融機構往來。綜合不同機構的付款資訊，可辨識出犯罪者藉由不同機構，未被其他工具偵測到的結構性支付模式。
73. 然而，這樣的資訊分享也觸發公共政策上對於資訊利用（或濫用）的憂慮，包括不對等的商業競爭、鼓勵去風險化或金融排除、違反 STR 機密的可能性與增加洩密的風險、洩露客戶秘密、破壞個資與隱私保護，以及本指引前述一般有礙資訊分享的法規範等。
74. 舉例來說，金融機構間的客戶資訊分享可能提高競爭的憂慮，導因於僅與小部分成員選擇性的資訊分享。去風險化與防禦性申報的行爲可能因此惡化，如金融機構可能只因爲發現其他金融機構已經申報而決定對同一客戶申報 STR（未經內部調查）。對於系統內可疑資訊分享或共通平台的過度信賴，導致道德風險，即金融機構可能在完成客戶審查前即認定特定客戶爲可疑客戶，並因此阻礙該客戶進入金融體系取得服務。
75. 各國應審愼考量前述法制、政策、執行上的問題，規劃抵減的措施，這些方法例如考慮採取措施以避免分享機制濫用、未經授權的資訊使用、違反分享機制原則及前述問題帶來的負面影響。
76. 各國應依所分享資訊的機敏性，以及秘密保護的需求，提供明確規範可分享的資訊形式、分享的對象、分享的條件、分享的目的及其限制。對資訊的瞭解應採書面形式，並符合資訊安全指引與使用協定，這可避免解讀歧異、理解矛盾與執行的不一致等，造成妨礙資訊分享的狀況。而合宜的監督機制與透明性可使所有參與者有信心並負起責任。
77. 但各國與私部門近年在偵測 ML/TF 活動與趨勢的數據分析上，已有長足的進步。爲了分享此類資訊，在既有的法制架構下，已採行有效的保障措施與機制，提供更好、更即時與足以起訴的資訊，並獲致積極的成果，這類機制與程序請參照附件 2。

A. 資訊分享的形式

78. 許多資訊可以不同的方式分享，分述如下：

i. 風險、犯罪趨勢與態樣資訊的分享

79. 金融機構可以協調分享有關於金融體系濫用之風險、犯罪趨勢、方法論、技巧、一般態樣與犯罪手法的分析與策略資訊。這樣的資訊，抽離個人資訊，因此不會違反個資、隱私或其他個人識別資料的保護，也不至於洩密。此類資訊分享可提供良好的理解，使參與的金融機構利用於其營運，除提供參與者更佳的合作環境，並協助渠等針對當前的趨勢與手法，持續更新其風險評估。

80. 執法機關經常也參與此類作爲，爲犯罪趨勢與態樣提供更全面的更新，包括案例和 ML/TF 風險的特定資訊，藉此可提升對當前財經犯罪情勢、相關犯罪策略性與實務性的風險，及其對金融業整體所造成衝擊的全面認知。

ii 交易與客戶資訊的分享

81. 某些國家依其國內法制度，特別允許非屬同集團之金融機構間分享特定交易資訊，及其他關於可疑交易的資訊（惟不必然爲該 STR 本身）。所分享的資訊可能包括 2 個或多個金融機構或相關實體之客戶、代表人或實質受益人的資訊，及疑涉 ML/TF 的個人或實體的資訊。舉例而言，這種作法適用在金融機構有相同的客戶時（參照附錄 2 第 10 至第 14 點）。

82. 這樣的資訊分享可以提供額外的要素以更有效地評估客戶的風險，也能促進可疑的認定，舉例來說，甫開立數月的新帳戶突然收到大額匯款，有必要向匯款行請求資訊以確認資金來源及其他相關資訊，各國應考量鼓勵金融機構與其他同業分享特定威脅與高風險客戶資訊，這有助於情報分享，並協助相關權責機關及私部門決策。

B. 資訊分享的機制

83. 目前已發展許多可行模式以鼓勵主動的資訊分享，包括各金融機構與 KYC 應用程式、集中化資料庫之間的分享，這些程式或

資料庫存有客戶與交易的重要資訊，並以合宜的機制與使用管制，分送予參與之金融機構。這些程式爲 AML/CFT 目的，取得不同形式的資訊，包括客戶與實質受益人的識別資訊及額外資訊，以支援風險評估及金融機構對客戶的風險認知。這些程式可用於與客戶建立交易關係時，用以取得客戶資料，及在此基礎上，採取進一步的客戶審查措施，也可取得委託機構的更新資訊，如此有助於風險評估與通匯機構現行之交易審查，惟在上述各情形中，最終的審查責任仍在於使用該等程式的金融機構。

84. 這些程式或資料庫可由主管機關、私部門或公私協力來主持，例如某些國家已創建資料庫可分享有關國際電匯、是否已申報 STR、STR 本身或其他相關資訊，於適當時機促進申報主體與行政機關及執法機關間之資訊分享。然而該等應用程式或資料庫無論由何者主持，都可能面臨此一問題，即誰應承擔最終的監控責任，並對失敗負責——這也是另一種形式的道德風險。
85. 不同國家在某些情形下，已達成特定的資訊分享協議，基於 AML/CFT 目的，促進金融機構間的資訊分享。爲跨境情境下，提供法定的管道，協助金融機構間基於 AML/CFT 目的之資訊分享。
86. 某些國家已發展出資訊分享的公私協力，並已獲致積極成果，經由這樣的夥伴關係，執法機關、FIU、特定的私部門參與者，甚至某些個案中包括外國的參與者，得以分享資訊，提供對交易及客戶行爲更完整的理解。這樣的分享常在安全的環境中進行，以推動私部門更進一步的數據挖掘、實務分析及審視，彌補潛在的情報落差。
87. 產業論壇或平台——金融機構可發起某些作爲，例如創建跨銀行間的論壇，或經由同業公會將有關當前犯罪趨勢、犯罪手法與態樣的資訊分享予會員，執法機關與監理機關的代表亦可共同參與以提供支援。
88. 金融機構可透過避風港條款以促進客戶與可疑交易的資訊分享，

規範該條款不被濫用，建構並維持妥善的程序以確保資訊的機密與安全，避風港條款可合法保障金融機構間基於 AML/CFT 目的進行資訊分享。

89. 本指引的附錄 2 提供各國強化資訊分享所採取的方法，細節詳述於附錄的第 10 點至第 22 點、第 29 點至第 30 點及第 32 點至第 34 點，但只提供資訊，該等說明不由 FATF 背書，此外，附錄僅爲說明，未包含所有範例的詳細清單，該等案例可能有完全相反的結果，主要是強調不同形式的資訊（策略、實務或客戶相關）可基於 AML/CFT 目的，在不同的架構下經由不同的模式或機制分享。

90. 金融機構間的資訊分享有很大益處，同時也存在可能的風險必須去面對並抵減，也受到前述挑戰的影響。我們鼓勵各國政府評估，超越 FATF 建議的主動資訊分享如何提升其 AML/CFT 體系，以發展促進資訊分享的法制架構。

六、指引與回饋

91. 若公部門對於私部門資訊分享，未提供相關的指引與回饋，有礙私部門有效監控交易並向 FIU 完整申報的能力。於適宜的情形下，各國應考慮設置強化的「反饋迴圈」，提供私部門關於 STR 更一致且更充分說明的回饋意見，進一步地發展溝通渠道，如此私部門可針對專案接收回饋意見與特定領域的資訊，有助於釐清法規的期待（附錄 2 第 23 至第 28 點），各國應考慮與面臨 ML/TF 威脅的部門共同發展合作方案（附錄 2 第 31 點）。

92. 公部門欠缺指引與回饋，亦有礙私部門主體間，或公、私部門間的資訊分享，包括因法律預期不明確，或關於風險的資訊不足，公部門應該藉由對資訊分享機制的指引與回饋，明確地進行溝通。各國應考慮出版關於既有法律架構、通訊協定與准許金融機構於集團範圍或跨機構間進行資訊分享的訊息，這將有助於私部門釐清、確保並推動理解的一致性。

七、結論

93. 國內與國際有效的協調與合作體系，著重在不同的參與者，包括公、私部門如何互動與相互合作，交換情資、資訊及分析。

94. 法律的限制，諸如對於數據保護與隱私不同的法律架構及其執行、金融機構的保密條款及實務上的挑戰，可能阻礙集團範圍及非屬同集團的金融機構間資訊分享。隨著所涉威脅與風險情勢的急遽變化，尤其是資恐相關問題，政府當局及私部門以一致性的態度提出克服資訊分享障礙的解決方案，是很重要的，這些措施包括權責機關的合作（例如 AML/CFT 及 DPP 主管機關間），達成共識，這樣的合作亦有助於辨識認知不清，與公、私部門間之歧異，相關議題的釐清與指引可促進相關義務的有效實踐。

95. AML/CFT 及 DPP 都是重要的公益議題，都是國家法制架構維護的目標，因此當預防洗錢、恐怖分子、武擴或其他財經犯罪時，應以保障個人隱私與資料保護之方式爲之，爲金融機構提供明確的法制以確保 AML/CFT 及 DPP 不致相互牽制。當務之急是，AML/CFT 及 DPP 的主管機關應承認，避免矛盾的法律有所不足，並向私部門提供明確且一致的指引，預防在 AML/CFT 目的下，對資訊分享產生誤解或保守的態度。

96. 私部門是打擊 ML/TF 的重要夥伴，渠等持有對執法及其他權責機關相當重要的寶貴情資，相關情資有效且即時的交換，有益於執法機關達成其目標，此外，公、私部門間係雙向關係，若透過合宜機制，使執法機關與私部門分享策略性、實務性、戰術性及特定的資訊，該雙向關係方能達成。建構一個網絡，營造政府與私部門得相互信任、持續對話的環境，將有助於在此領域獲致積極的成果。

附錄 1—DPP 法制及其應用的差異

1. 誠如報告第一部分所陳述，各國 DPP 法律架構的差異，可能造成執行上的困難，特別是對私部門在集團範圍及跨機構的資訊分享，這些問題來自下列因素：
   i. 集團範圍資訊分享的障礙。某些國家將集團範圍含有個人資料的資訊分享，等同與第三方分享，這是因爲相關資料保護的法律將機構的其他分支機構，視爲第三方。這樣的法律也適用於跨國設立的集團營業處所，因此其間的資訊移轉也須適用相同的法規範，限制了金融集團總部、母公司與其分支機構間，基於 AML/CFT 風險抵減目的，所進行的集團層次資訊分享。對於全球性企業而言，不同的區域及司法管轄權對資料保護的要求，嚴重影響企業內部資訊流動。
   ii. DPP 架構下的資料最小化原則係要求組織僅可取得足以完成資料處理需求之個資，但並未提供明確定義及特定方式，這也常導致資訊分享合法性的模糊不清。當依據 AML/CFT 法制要求處理個人資料，而法律並未明確規範處理個資之義務，模糊性因此產生，尤其針對基於該等目的，資訊應如何進行資料蒐集、處理及分享等，未提供法規指引。對這類情況，主管機關正致力發展一遵循架構，會將集團範圍資訊分享的需求納入考量。
   iii. 個人資料處理發生在所有金融機構，當開戶時辦理客戶審查，及其後因應客戶交易爲抵減風險，以及 AML/CFT 目的所需。在某些國家，個人資料的處理需有客戶具體且明確的同意，依相關資訊形式而定。在此情形下，同意應於自由意志下提供，藉由聲明或清楚肯定的作爲，具體且明確地表達個人的意願，對其個人資料的處理與傳遞表達同意。但究竟金融機構可於開戶時取得概括性同意或須於每次資料處理時皆取得同意，規定仍然不明確。此外，某些國家完全禁止個人資料（甚或部分個資）的移轉，即便係客戶同意的情形下。對於金融機構而言，基於概括性同意或公益的豁免，傳遞客戶資料以打擊金融犯罪，並非易事。公告法規或發布指引以明確定義個資跨境傳遞的要求，將有助於推動資訊分享。
   iv. 某些情況下，傳遞個資至第三國是違法的，除非母國的主管機關確認送至第三國之資料，透過某些保障機制，符合資料保護的要求

（舉例來說，在集團內部移轉資料，依據企業約束規則可能獲得政府的同意），欠缺明確性會影響資訊的交換。當法規因公益目的作出妥協，但適用卻需依個案而定，而非通案的制度，因爲後者需有特定的法律架構。即時資訊的傳遞，需取得主管機關與相關權責單位的事前同意與授權，對資訊分享有不利影響。

v. 當實質受益人納入金融機構的業務關係時，取得實質受益人相關資訊將會受到限制，因某些金融機構或其分支機構設立於禁止處理相關個資的國家。因此，在此類情形下，依前述規定金融機構無法取得實質受益人的同意，對其個人資料蒐集、處理及分享，這會造成 AML/CFT 及 DPP 規範的衝突。實務上，這意味著金融機構在分享實質受益人資訊時，面對額外的問題，在集團範圍的層次，阻礙了金融機構透過建構關聯性以偵測異常模式的能力（例如同一實質受益人持有 2 間或多間公司間交易），並侷限可疑活動模式的辨識。有時金融機構所持有的實質受益人辨識資訊，係由第三方（法人的代表人）揭露或提供，實質受益人本人並未參與時，將造成許多額外問題。在此種情形下，通常無法取得當事人的具體同意。

vi. 對 PEPs 家庭成員及有密切關係之人，執行額外措施以符合資料保護原則之要求，並不容易。因資料保護與隱私的考量，從不同來源蒐集個資辨識的細節，包括有關客戶間已知的關係（諸如家庭成員、密切關係之人等），相當困難。舉例來說，有關 PEP 擔任特定政黨的重要黨職或 PEP 同性伴侶的資訊，將揭露客戶的政治立場或性別傾向，這都被視爲敏感的個資，無論基於何種目的，均不得處理此類個資，除非得到本人的明確同意或爲具體的公益需要。然而，這仍限制金融機構直接向客戶或自公開來源取得相關資訊。對此，重申金融機構應有妥適的風險管理體系並採取合理的措施以辨識客戶或其實質受益人是否爲 PEP，該等要求同樣適用於 PEP 的家庭成員或有密切關係之人。

vii. 匿名權與資料刪除權，對紀錄的保存期限與供 ML/TF 調查的可得性，造成限制。依據 FATF 標準，客戶及交易紀錄至少應保存 5 年，惟依據資料保護法，資料最長保存期限，可能比 FATF 標準要求的基本保存期間還短。在某些國家，資料保存要求，與資料保護法律間，以及與被視爲資料保護權必然作用的「被遺忘的權利 / 匿名權」間，如何交互作用，仍存在不確定性。

附錄 2—入選範例與實踐經驗

2. 本節聚焦各國有關 AML/CFT 與 DPP 主管機關建設性的合作範例，及其他促進金融機構內、公私部門間、金融機構間資訊分享的實踐經驗。所提供之各國範例僅作爲參考說明，納入這些入選範例並不意味著 FATF 的正式要求，本節內容基於資恐風險指標報告第 3 章，與各國提供的額外範例與實踐經驗，這些範例與實踐經驗與下列議題相關：

A. AML/CFT 與 DPP 法規架構的交互作用

3. 某些國家已對金融機構發布指引，以確保金融機構得以調和並遵循這 2 種法令規範。另在某些國家，AML/CFT 監理機關也相互會商以改善對法規目標之釋明。這樣的對話，開始於 DPP 主管機關法規制定前，並持續進行中，以提供進一步的指引或回應常見問題。監理機關、DPP 主管機關、立法者、FIUs、金融機構亦得組織工作小組，確保對法規要求提供協調一致的方法與指引。

法國

法國 AML/CFT 監理機關於相關指示、指引及立場文件施行或發布前，均先蒐集反洗錢與反資恐顧問委員會（CCLCBFT）的意見，這個顧問委員會係由監理機關理事會組成，包括法國財政部、金融情報中心及其他相關機關，例如資料保護與公民權利主管機關（公民權利與自由委員會，CNIL）即受邀參與 CCLCBFT 的會議，尤其是當法國監理機關發布有關金融集團內或跨集團資訊交換的指引時。

此外，當政府公告有關資料保護或創建 ML/TF 相關新法的草案時，CNIL 亦會發表意見。自 2005 年以來，法國 DPP 主管機關已採取單行法（一般標準），俾與公、私部門代表合作，該單一法規定期修正，其目標係使參與的各方，經由更一致性、全面性的架構，在執行 AML/CFT 措施與資料保護要求時取得平衡。目前約有 1,800 個組織聲明遵循此協議，此外，該法規授權打擊 ML/TF 之主管機關，准許分享客戶的資料。

4. 許多國家的 DPP 主管機關受邀對 AML/CFT 措施提供意見，避免法令的矛盾或不確定性，政府亦支持 DPP 主管機關與 AML/CFT 主管機關相互協商，以發展新的措施，此種實踐促進機關間的合作夥伴關係的發展，並強化了相關政策目標不必然互斥的論點。

加拿大

DPP 與 AML/CFT 主管機關起草相關法規前，爲例行性合作。個人資料保護與電子文件法（PIPEDA）係加拿大聯邦之私部門隱私權法，加拿大隱私權委員辦公室於機關網站上發布指引「隱私與 PIPEDA：如何在客戶的隱私權與機構反洗錢、反資恐的申報義務間取得平衡」。加拿大金融情報中心（FINTRAC）18 也開發出一系列的問答集，該指引承認不法所得（洗錢）與資恐法案（PCMLTFA）可對相關機構課予義務，需依法採取遵循行動，諸如客戶辨識與紀錄保存，此外，應向 FINTRAC 申報某些交易，該指引重申加拿大隱私權委員辦公室支持反洗錢與反資恐的努力，惟相關的計畫應認知隱私的機敏性，並遵守隱私權法案。

5. 某些國家，資料保護主管機關即 AML/CFT 組織架構的成員，並直接參與 AML/CFT 立法過程，部門間密切的互動有助於促進合作與不同觀點的整合。

西班牙

西班牙 AML/CFT 政策發展與協調的主要協調機制，係洗錢與金融犯罪預防委員會，該委員會納編 20 個重要機關，包括西班牙資料保護署，該委員會的主要功能之一，係對於預防洗錢及資恐相關法律草案發布意見，高層協調，可加速未牴觸資料保護法相關規定的立法。

6. 在某些國家，資料保護法提供必要的豁免或例外規定，以落實其他法規範的執行義務，這些規定可能與主體資料的使用權、取得同意權、事先通知及被遺忘權等限制相關，豁免之目的在於平衡資料安全與隱

[18] 參照加拿大隱私權委員辦公室網站。

私權顧慮。若情況適宜，政府機關應考慮提供相關領域更多的指引。在歐盟的架構下，統合歐洲資料保護法的工作正進行中。

歐盟

2016 年 2 月 14 日歐盟公告一般資料保護法（GDPR），直接適用於歐盟架構下的所有國家，取代歐盟與其成員國原有的資料保護法，並將於 2018 年 5 月 25 日生效，這對整合歐盟資料保護法規的目標而言，係一長足發展。GDPR 規範了多數情形下的位址資訊，IP 位址及線上識別個資等，這些資料可運用於識別主體，特別是含有獨特識別碼時，GDPR 也引介其他的移轉工具（執行與認證碼）俾便執行資訊交換。

義大利

國內法爲基於 AML/CFT 法規遵循目的，而處理與分享個人資料提供明確的渠道。在某些情形下，爲更求明確，國家資料保護主管機關已針對集團範圍之資訊分享發布一般性的指引，並以金融中介機構推動集團範圍的資訊分享，而該等分享毋須取得資料主體的同意。

7. 在某些國家，金融機構在資料保護法的豁免條款下，可分享客戶資訊，基於 AML/CFT 目的，資訊分享得不受限制，金融機構依其程序執行資訊分享時，應將豁免規定列入考量。

新加坡

金融機構間客戶資訊的交換應依據新加坡銀行法與信託公司法，該法取代個人資料保護法（PDPA）的資料保護通則性規定。爲打擊洗錢與資恐（如遵循監理機關指示、內部稽核或總公司所要求之風險管理目標），可不受金融秘密條款的約束。此外，亦放寬 PDPA 的規定，依據新加坡金融管理局 AML/CFT 通告的要求，基於洗錢及資恐風險管理目的之必要，在金融集團內，各機構應與其總公司及分支機構分享資訊。

B. 集團範圍的資訊分享

8. 分支機構向總公司分享 STR 資訊，可強化集團範圍的風險管理程序，

並履踐了總公司的監督責任。此外，集團內深化分享 STR 能促進有效的內部控制程序與風險管理，在合宜的機密管理下，某些國家允許這樣的作法。

美國

2006 年 1 月，金融犯罪稽查局（FinCEN）與聯邦銀行監理部門包括通貨監理局（OCC）、聯邦儲備銀行（FRB）、聯邦存款保險公司（FDIC）與儲蓄機構監理局（OTS），決定外國銀行在美分支機構得與其總公司分享 SAR。2006 年 1 月的指引亦說明，美國銀行與儲蓄機構得與其控制公司（無論在本地或外國）分享 SAR。與總公司或控制公司（包括在海外者）分享 SAR，甚或任何揭露 SAR 申報之相關資訊，總公司或控制公司以集團範圍風險管理的角度並落實儲蓄機構所遵循的相關法規，可履行其監督責任，進而強化銀行秘密法規定（主要之 AML/CFT 法令）的遵循。

此外，FinCEN 與聯邦銀行監理部門於 2010 年 11 月發布共同指引，指出基於 SAR 相關規定，已申報 SAR 之儲蓄機構，得分享或提供該 SAR，或其他可揭露該 SAR 之資訊予其他分支機構。該等機構間 SAR 的分享，有助於辨識儲蓄機構各分支單位所發生的可疑交易，而該等分支機構亦受 SAR 相關法令所規範。

法國

法國貨幣與金融法第 L561-20 條授權資訊交換，此外，金融機構須填報年度問卷，說明其與分支機構交換資訊面臨之法律障礙，若他國法律禁止或限制金融機在其海外分支機構執行同等 AML/CFT 措施，須向法國監理機關申報，監理機關須將該等問題轉知 FIU。

9. 在某些金融集團，係由監測與分析中心與集團遵循分享可疑資訊分析，該中心設置於集團內部，俾整合資訊聚焦於可疑客戶並減少資訊節點以避免資訊的洩露。此中心對於不同情況的可疑交易，得立即採取行動並經由集團系統警示其他部門，以防止該客戶於不同地點或參與金流的不同環節，影響相關司法主體的運作。

C. 非屬同集團之金融機構間的資訊分享

10. 以足夠的避風港條款或法律豁免的保護，俾金融機構得即時並自主地相互分享資訊，將更有助於有效地打擊 ML/TF，促進金融體系的整合，並預防其被犯罪者利用，也使金融體系足以提供更好、更全面性的情報予執法機關。某些國家有特殊法制設計與避風港條款，以推動金融機構間於該法制下的資訊分享。

> 美國
> 美國愛國者法案第 314(b) 條（金融機構間資訊分享），規定 2 間或 2 間以上之金融機構或其協會間，得彼此分享疑涉資恐或洗錢活動相關個人、法人、組織及國家的資訊。基於辨識或申報疑涉恐佈活動或洗錢之目的，金融機構或協會對相關資訊所爲之移轉、受理或分享，以及相關揭露、未通知遭揭露之主體對象或於該揭露中可資辨識之人，不受任何美國法令、憲法、法律、州法、自律團體規範、契約或其他法律協議（包括任何仲裁協議）所歸責。

11. 某些國家允許特定條件下，非屬同一集團之 2 個金融機構間進行資訊交換。

> 法國與羅馬尼亞
> 若符合特定條件，在法國非屬同一集團之 2 個金融機構間的資訊交換係屬合法（貨幣與金融法第 L561-21 條），依所設條件，金融機構應確保其合作機構所採取之 AML/CFT 措施，與法國執行之 FATF 建議相符。羅馬尼亞 AML/CFT 法案第 25(4) 條許可金融機構與其他金融機構交換資訊，特別是 (b) 段允許信用與金融機構交換保密資訊，當 (1) 屬於同集團，(2) 位於歐盟、歐洲經濟區或執行相同 AML/CFT 要求第三國時，(3) 採取與 AML/CFT 法相同之 CDD 與紀錄保存措施時，(4) 接受 AML/CFT 監理時。非屬同一金融集團之信用與金融機構亦得交換保密資訊，若 (1) 位於歐盟、歐洲經濟區或執行相同 AML/CFT 要求第三國時，(2) 與同一客戶或交易相關的資訊，(3) 屬於同一產業類型，(4) 遵循同等之秘密與資料保護的要求。

12. 某些國家爲追求基於 AML/CFT 之目的，簽署金融機構間推動資訊分享的雙向協議，透過雙向或多邊安排之機制，強調抵減特定國家 / 地區 ML/TF 風險的重要性。

美國與墨西哥

美國與墨西哥正持續努力，以共同提昇金融透明度，並在通匯行的架構下預防 ML/TF。

持續監控的部分要求是，美國銀行作爲中介金融機構時，應審查所有交易並適時申報 STR，美國銀行規律地向委託機構提出資訊請求（RFIs），要求與異常交易相關的額外資訊，這較接近明確的警示而非申報 STR。但因爲依據墨西哥的銀行秘密條款與資訊隱私法，墨西哥銀行無法回應，因此導致更大量的 STR 或代理帳戶的結束。墨西哥銀行回應美國 RFI 能力的缺乏，致使美國銀行申報 STR 並可能關閉通匯帳戶，爲因應此問題，墨西哥 AML/CFT 總則於 2014 年 12 月修正，首度准許墨西哥銀行基於 AML/CFT 目的與外國銀行分享資訊。

墨西哥政府特別修正其 AML/CFT 總則，提供該國銀行與外國銀行資訊交換之合法機制，基於 AML/CFT 目的，分享客戶與過路客的資訊及其交易。依墨西哥的信用機構法，銀行應將其客戶及過路客之資訊視爲機密，因此除帳戶持有人、實質受益人、受託人、債權人及法人代表外，銀行不得洩露其客戶及過路客之交易紀錄或個人資料予任何人，惟以下情形例外，銀行應提供前述資訊若請求來自：(i) 法官開立令狀；(ii) 檢察總長辦公室；(iii) 軍事檢察總長辦公室；(iv) 財政部授權因 AML/CFT 或稅務目的；(v) 聯邦監理機關，同樣地，銀行得基於 AML/CFT 目的，與其他同業分享有關其客戶及過路客暨其交易之相關資訊。

於分享相關資訊前，墨西哥財政部須授權予外國銀行；同樣地，墨西哥銀行與外國銀行開始交換資訊前，必須簽署資訊保密協議，並註明授權資訊交換官員的職務及資訊，此協議應送交國家銀行及證券委員會見證。

美國、墨西哥政府及銀行業已合作開發出一份問卷，作爲資訊交易機制之模式，資訊交換前或交換時，墨西哥銀行應提供交換資訊及相關資料的副本。

在此機制下，墨西哥銀行遵循相同的協定，現亦得與非美國銀行分享資訊。

13. 其他情形下，國家明定金融機構應經由該機構或金融機關所建置之中心式資料庫分享特定金融交易資訊，並將相關資訊納入應對客戶執行之風險考量。

墨西哥

2017 年，基於與信用機構有關的相同理由，墨國政府公布 AML/CFT 法規，要求銀行提供代理顧客所收付之國際電匯或境內外幣匯款之資訊，予中央銀行或該等銀行之中心式資料庫。此外，依據本法，銀行應自前揭資料庫取得該匯款人於銀行體系辦理電匯之所有資料，據此執行當次電匯之客戶審查與風險評估，客戶必須同意個別銀行向該資料庫提交或取得資料。該 AML/CFT 現行法規明定銀行必須向該資料庫提交的資料，以及該資料庫提供予銀行之統計數據。中央銀行已發展出相應的資料庫，各銀行將可於 2017 年底前交換客戶之交易資訊；而在第二階段，銀行須提供特定客戶的 KYC 資料與文件，並核對該資料庫內的前述資料。

14. 此爲私部門對外分享特定威脅及高風險客戶資料的案例。在某些國家已建置可分享 STR 及相關資訊的資料庫，以促進申報義務主體與行政及執法機關之間的資訊分享，並分享情資以協助權責機關、私部門與相關主體進行決策。

西班牙

ML/TF 防制法第 33 條允許當個案被拒絕交易之交易特性或模式顯示可能與後續交易完全相同或部分相似時，義務人得爲預防或阻斷 ML/TF 目的，將已向 FIU 申報之可疑交易相關資訊予以分享。

爲此，中心式資料庫有助於相關資訊分享，義務人及司法、執法、行政等權責機關，基於防制 ML/TF 目的，得查詢資料庫內所建置之資料；對義務主體而言，可取得之資料，限於義務人所設立之內部遵循單位。

D. 金融機構與政府機關間的資訊分享

15. 公、私部門間的緊密關係，爲 AML/CFT 體系運作順利的關鍵因素，

FATF 標準要求各國發展出健全的法制與實務架構，告知私部門 ML/TF 風險，並確認私部門將 ML/TF 風險納入營業考量，基於 TF 之目的，尤其應將來自私部門之訊息，與來自權責機關之相關聯及經處理的資訊，予以整合。

俄羅斯

依據聯邦AML/CFT法律，由FIU與聯邦金融監理局（Rosfinmonitoring）、監理機關（俄羅斯銀行）及申報主體所組成的合作體系，接收有關拒絕交易、開戶及結束交易關係的資訊。上述所有情形，申報主體均應向FIU申報，相關資訊經分析後分送俄羅斯銀行，俾透過安全管道與信用機構或非信用金融機構分享；申報機構接獲相關訊息後，應納入執行客戶風險評估，確認風險等級並訂定相應的風險抵減措施。

a) 公 / 私夥伴關係

16. 私部門所掌握之大量數據資料，可由執法機關於調查使用。某些國家已建立公私夥伴關係，以推動參與者在公私部門間或金融機構間的資訊交換，此一正式或非正式平台的目標，係營造一個有利公、私部門提供回饋或指引的環境，同時分享實務情資、風險資訊，並預防、偵測、阻斷可能的威脅。

瑞士

瑞士透過不同的機制或平台與私部門相互交換資訊。2010 年，因 FATF 標準修訂，瑞士政府在發展 AML/CFT 法律架構時，與私部門（ISFIN）合作建立一個工作組，而 2013 年更增設打擊 ML 與 TF 之跨部會協調小組與私部門聯繫，亦負責編撰國家風險評估報告。此小組由不同部門熟知 AML/CFT 相關法規的資深專家所組成，包括銀行、保險與 MVTS，係常設性平台，目的在交換對革新、對既存與新興 ML/TF 風險的認知與抵減的意見。該小組並已規劃公、私部門未來的工作重點，諸如 TF 態樣與通匯行。該小組可促進私部門的交流，以及提升對 AML/CFT 業務的認識。

中國香港

詐欺與洗錢情報工作組，係一公、私部門情資分享的機制，納入警察、金融管理局、銀行業等，其目標在強化偵測、預防及阻斷詐欺、洗錢等其他與香港經濟密切相關的金融犯罪。此一爲期 12 個月的前瞻計畫始於 2017 年 5 月，該工作組奠基於既有非正式的合作與分享關係，預備會議於 2016 年間進行，俾爲銀行業及權責機關開發出一正式架構，以改善對威脅的集體認知，爲執法機關強化攻擊與干預行動，並爲銀行優化風險管理。該工作組係採策略性與實務性的運作，經由安全平台，向更廣泛的金融部門分送特定威脅的警訊。

澳洲

2017年3月3日，澳洲金融情報中心（AUSTRAC）成立金融科技聯盟（Fintel Alliance），邀集政府、產業、學界及國際夥伴參與具協調性及安全性的資訊交流環境，建構全面整合方式，藉由金融情資之分析，進而發現、瞭解並阻斷重大與組織犯罪、賄賂與貪瀆及恐怖主義。金融科技聯盟目前仍續接受新的成員並擴大發展，迄2017年4月止，金融科技聯盟已有19名成員，包括AUSTRAC、聯邦警察、新南威爾斯州警察、稅務局、澳洲銀行——澳盛銀行、澳洲聯邦銀行、麥格里銀行、澳洲國民銀行、西太平洋銀行、西聯匯款、及PayPal，英國國家犯罪調查署均已加入，AUSTRAC仍續與其他可能的國際夥伴接洽中。

金融科技聯盟已成爲一實務樞紐，政府與產業之情資分析人員部門可參與聯合執行計畫，近乎即時分享資訊，現有 3 項執行計畫進行中：

- 檢視巴拿馬文件。
- 辨識並研判線上車手。
- 推廣澳洲線上申報網絡資料的使用。

17.這些夥伴關係的建立體認私部門參與的重要性，私部門不僅是資訊來源，也是公部門機敏情資的接收者，該等情資有助於偵測潛在的資恐者。此類分享通常經過適當查核後，在安全的環境中進行，俾利私部門進一步挖掘資料、實務分析並檢核，以補足可能的情報漏洞，該等安排必須持續進行，不僅限於交易，亦可能由其他特定事件所引發，私部門對於持續變動的風險環境亦應有正確認知，使執法機關的成果更完善。

加拿大

提升申報機構的TF警覺與STR申報:魁北克渥太華的攻擊事件發生後，加拿大金融情報中心（FINTRAC）立即對申報機構發布警示，強調對疑涉 TF 威脅交易申報 STR 的重要性，渥太華攻擊事件當月，STR 的申報增加 22%（2014 年 10 月逾 8,700 件）。除於 ISIL 相關攻擊後發布備忘訊息外，FINTRAC 亦與申報機構合作發展並分享 TF 監控指標。與申報機構發展眞正的夥伴關係並分享實務警訊及簡介：FINTRAC 於過去幾年間，已與主要金融機構緊密合作以對抗 ML/TF，並發展出一系列成果，包括「實務警訊」，其目的在提供可疑交易表徵的即時更新，與 ML/TF 特定交易模式相關的高風險因子。這些訊息很重要，因爲這代表著新興的、再現的與歷久不衰的交易方式，皆爲特定挑戰。其目標在於，對申報機構在辨識、評估、抵減相關風險時，以及向 FINTRAC 申報相關可疑交易時，提供實務協助。FINTRAC 亦發展出「實務簡介」，對相關議題提供說明與指引，該等議題可能影響申報機關維持有力架構以遵循加拿大法規之能力。更爲特別地是，這些成果著眼在遭 ML/TF 利用的風險與弱點，以及符合 STR 申報義務。FINTRAC 目前正發展一套 TF 相關的「實務警訊」，提供 TF 相關之重要背景知識予申報機構，並試圖提供可操作或可運用於內部交易監控及內部調查程序之表徵 / 紅旗指標，最終提升來自申報機構 TF 相關情資的質與量。

18. 私部門經常尋求協助，而來自公部門更爲詳盡的背景資料，將有助於私部門解讀已持有的資料。舉例而言，可能包括特定對象（如受監控、跟監或調查對象）可疑行爲清單，這種表列式有助於辨識特定交易並偵測清單所列對象交往網絡或關係人，然而，分享對象清單爲敏感的議題，涉及執法機關維護調查中案件機密的優先性。這也可能導致該客戶被提列爲高風險，未經合法程序或審愼判斷即暫停或終止業務關係，並引發合法性的爭議。儘管不可能洩露個案的特定事實，該類型活動的一般表徵仍得協助提供可起訴的金融情資，監控表徵的分享，使申報機構優化偵測可疑活動及向 FIU 提供情資的能力。

19. 私部門因執行 CDD 而掌握客戶某些非金融資料，諸如 IP 位址、行動電話、電郵、居所及網路銀行使用者的即時所在。這些資訊若與權責機關的資訊結合，將有益於執法機關從事偵測與調查。

b) 可疑帳戶與交易的資訊分享

20. 某些避風港條款，或特定的論壇及渠道，容許可疑交易資訊的分享，惟不必然是該 STR 的完整內容，在保護資訊機密性的嚴格條款之下，該等特定渠道改善了非屬同集團金融機構間，以及跨機關間之資訊分享，其目的在於相關資訊有效且即時的分享，並協助執法機關實現打擊洗錢與資恐之目標。

EU-OF2Cen

EU-OF2Cen 倡議係歐盟挹注義大利針對網路詐騙的計畫，目前正在歐盟層級執行，其目標在推動銀行與執法機關間，系統性的、歐盟範圍的網路詐騙相關資訊分享，俾阻止詐騙者與車手，協助相關犯罪者的調查與起訴。該計畫係由歐盟執委會共同出資，由銀行部門與執法機關等重要參與者提供支援。

21. 合作並分享風險指標的資訊、經驗及趨勢，例如與 TF、外國恐怖戰士（FTF）及小型恐怖團體相關的對象，由政府機關協助建構私部門的能力，以積極的態度提升警覺。FATF 與艾格蒙聯盟成功的公共夥伴關係已獲致有意義的成果（例如 FATF 完成當前 TF 風險指標報告，艾格蒙聯盟有關 FTF 之公告等）。

美國

美國愛國者法案第 314(a) 條之金融犯罪稽查局（FinCEN）條例，使 FinCEN 得在逾 22,000 個金融機構中，設立超過 43,000 個聯絡點，進而定位涉嫌洗錢或資恐對象之所在。FinCEN 爲分析與調查之目的，代表聯邦、州、地方及特定國家或地區（如歐盟）的執法機關提出請求，愛國者法案第 314(a) 條僅授權提供指引訊息（金融情報），且無須法院令狀或其他法律程序，這些程序通常是在辨識相關資訊後，爲獲致更多調查性或證據性目的之資訊時才適用。

透過加速的通訊系統，愛國者法案第 314(a) 條的 FinCEN 程序授權調查者直接將機敏的調查指引訊息提供予申報機構，FinCEN 建構安全的電郵系統分送機敏資訊。以金融機構提供的原始資訊爲基礎，調查者得以快速地聚焦於相關的位址與活動，此外，FinCEN 將組織並主持資訊分享，與適宜之金融機構共同研討，並依據愛國者法案第 314(a) 條發出資訊請求，這種執法機關與金融社群間的合作關係，可使分散的資訊得以獲得辨識、集中並快速地評估。

此外，美國國內安全聯盟委員會（DSAC）係由聯邦調查局（FBI）、國土安全部與私部門所發起之安全、情報情資分享計畫，參與者包括美國較大規模的銀行，DSAC 於 2005 年組成，促進 FBI 與其他參與者對調查資訊的雙向交流。

創設歐洲銀行家計畫

歐洲銀行家聯盟計畫始於 2015 年，成員包括於歐盟營運的領導性國際金融機構，以及歐洲刑警組織。其目的係協助金融機構與執法機關共同發展與人口販運相關紅旗指標，於內部系統篩選可疑交易並警示警察機關。

22. 恐怖主義活動與 TF 訊息，本質爲高度機敏性並需防護，權責機關與私部門之間若缺乏互信，將限制機敏資訊的分享。公部門在保密任務資訊以及建立參與者有關 TF 風險認知的事項上，難以取得平衡，這顯示緊密關係的建立係奠基於彼此的信任與保密。與私部門間正式及非正式的關係有助於打破取得資訊的障礙 / 延遲，例如在某些國家，主管機關與金融機構的防制洗錢主管維持個人聯繫管道，以取得相關資訊。

英國

洗錢情報聯合任務小組係英國結合金融機構、監理機關、政府與執法機關的機制，於 2015 年 2 月間建立，目前係英國因應洗錢及資恐的常設性機制，其目的在於使金融部門與政府交換並分析情報，以偵測、預防並阻斷威脅英國的洗錢及其他經濟犯罪，其任務係將金融機構所發展出有關一般洗錢與資恐方法、風險與態樣的策略性資訊，經由目標警訊作更廣泛的分享。若疑涉洗錢行爲發生於多家金融機構，可透

過戰術性資訊分享的功能，填補情報落差。戰術性的資訊分享功能，係由集中辦公之任務小組執行，金融機構的專責人員每週與執法官員集會討論，以進行共通利益之調查。這業務建構於明確法律架構（犯罪與法院法案第 7 章規定）與正式資訊分享協議之上，該小組所進行之調查，可能有逮捕、不法所得返還、銀行內控及內部體系修正，新增銀行主導調查事項等結果。

c) 指引與回饋

23. 對私部門提供指引與回饋也很重要，包括釐清有關落實 AML/CFT 要求的法律期待，以及對申報有所回饋，如此可強化私部門投入資源以遵循並與執法機關合作的意願。分享新興資訊的趨勢、行爲模式與威脅，對私部門極爲重要，據此可執行或調整交易監控系統，關注當前情況，並警醒在前端每日與客戶來往的銀行職員。
24. 政府機關可探討並分享資訊與情報予私部門，該等寶貴訊息有助於辨識可疑活動。洗錢及資恐相關態樣與案例研習，可由 FIU 以年報、快訊、電子公告等方式提供，案例研習的詳細版本或前案模式的分析，可經由合宜的管道與特定主體分享，諸如前述的論壇與夥伴關係。其他可有效分送案例與態樣的機制爲國家風險評估報告，評估結果用於與私部門的初階合作和提高特定的風險警覺，相當有幫助。
25. 政府機關可與私部門分享資恐高風險國家或高風險產業的資訊，在某些個案，政府可以提供更詳實的資訊分析，包括有關邊境、後勤及運輸的地緣資訊；其他個案中，由執法機關扣押之金融資訊（如提單與收據等），亦得與金融機構分享，可運用於其系統進行紀錄比對，以辨識任何相關可疑交易。

法國

法國 FIU 對所有申報 STR 的主體，提供回饋，而回饋機制分爲一般性與個案性回饋。一般性回饋與指引，係經由會議、年報、銀行業 AML 小組、保險公會及金融機構的遵循會議，個案性回饋與指引係經由與公司專責同仁非正式的接觸，對申報個案予以確認及檢視。此外，自 2016 年 6 月 3 日以來，爲強化打擊 TF，彙整金融機構所提供之資料後，

FIU 有權指名自然人或法人具有較高 ML/TF 風險，亦使金融機構應採取強化 CDD 措施，針對特定交易或個人進行特別監控。

俄羅斯

基於強化權責機關資訊分享與回饋之目的，與私部門參與者建立一般性合作，該合作關係爲規律性運作，由跨部門委員會委任 AML/CFT 顧問理事會所組成，該顧問理事會可代表境內最大金融機構協會，並藉著此一可代表特定主體之跨部會工作組織，執行金錢及其他資產之運作。

26. 爲協助私部門優化可疑活動的申報，指引、回饋與推廣計畫可提供申報主體有意義與具目標性的資訊，此一迴圈（回饋循環）最終可使權責機關將改善之申報標準，推廣至申報機構，也滿足私部門於不同參數中建構態樣的需求，並可用於保持關注資訊的機敏性及來自私部門請求的類型。

中國

中國人民銀行（PBC）綜整 TF 相關可疑交易的主要特徵，發展疑似 TF 交易監控模式，將該等模式與重要的金融機構及關鍵地區的金融機構分享，這種模式使金融機構所申報之資恐相關 STR 件數大增，並成功調查或起訴數起 TF 犯罪。某商業銀行成功檢核出與 ISIL 相關人員的交易，迄今，PBC 仍致力於在實務上持續改善並調整此模式。

澳洲

與相關私部門機構的定期會議，如澳洲金融情報中心與私部門產業之合作，經由每季的論壇，與主要的申報者及參與者，分享行爲模式之資訊。

羅馬尼亞

羅馬尼亞 FIU 的年報係策略性分析的成果，主要目標係提供相關的回饋予申報主體，這顯示羅馬尼亞 FIU 將自己視爲金融與非金融體系資訊的蒐集者。以 STR 申報資料爲基礎，相關資訊爲對可疑金融行爲主要分類的敘述。透過 FIU 與申報主體間的夥伴關係，FIU 儘量滿足其知的需求：應該申報什麼？其他主體申報的內容？回饋可增加信任，並協助申報主體調整可疑行爲偵測系統，此外，報告亦與執法機關的共同努力有關。

27. 對申報品質提供回饋資訊，有助於金融機構發展參與感，並更新其系統及程序。這也能使監理機關明確說明其監理期待，使金融機構更妥善回應以符合其目標。廣泛分送的指引，亦有助於該部門發展出良好產業實務經驗。

法國

爲強化金融機構申報的質與量，許多 FIU 與部門之管理者定期提供回饋。例如法國，在與申報機構舉行年度雙邊會議時提供回饋，並在產業論壇時亦提供一般性回饋。

土耳其

該國金融犯罪調查委員會（MASAK）定期與銀行的遵循幹部就 AML/CFT 及資恐風險議題，舉行會議。在這些會議中，銀行的遵循幹部將獲得最新的發展訊息並彼此交換意見。

澳洲

澳洲定期向許多的重要參與者，提供有關 STR 的指引與回饋。FIU 每季與執法機關、四大銀行舉行會議，討論遵循議題並提供 STR 回饋訊息。相關會議使資恐相關的 STR 數量，增加達 300%，並發展出目標 TF 風險表徵。

中國香港

聯合財富情報小組（JFIU）與香港金融管理局（HKMA）共同合作以提升 STR 申報的質與量。JFIU 與 HKMA 於 2013 年 12 月發布的指引，提供特定審查的回饋（例如申報品質與一致性之指引），2014 年共同發布特定產業訓練，此後，STR 數量由 2013 年的 27,328 件增加到 2014 年 31,095 件，增幅達 14%。因相關需求，JFIU 在對所有部門進行年度 AML 訓練時，提供部門回饋；HKMA 亦持續透過銀行的現地檢查，檢視 STR 的申報品質。JFIU 與 HKMA 均對私部門提供一般性回饋與指引，例如經由 JFIU 網站公布的 STR 季報、會議或 AML/CFT 研討，個案的回饋與指引亦經由非正式聯繫，以及與申報主體間之特別會議，就申報個案提供意見。

28. 在相關機關發布正式指引前，私部門對初步風險概況及風險指標的回饋，可精進最終版本。爲此，某些國家已發展出 TF 平台，同時可提供 STR 的回饋，並分享新趨勢與方法。
29. 即時事件需要更細部與特定之資訊，私部門方能採取立即的行動。私部門所掌握的資訊，亦有助於權責機關辨識特定的威脅，並在恐怖活動之時或其後提供即時資訊。然而，與特定個人和事件相關的具體資訊常受限，實務挑戰經常出現於進行中或活躍的恐怖主義，或資恐調查。在某些個案中，政府機關與私部門受限於法令規範、隱私權保護與責任問題，無法眞誠相待時，應考慮建立例外規定或程序，允許政府機構向私部門分享資訊，尤其爲因應緊急狀況，當前事件持續發展中，或已發生、可能發生傷亡時。
30. 某些國家已發展出個別的線上入口網站與其他工具，以向私部門請求資訊，或以安全有效的路徑分享資訊，這樣的機制確保相關請求優先並即時處理，特別是涉及恐怖主義與資恐事務，其目標係在預防攻擊。

中國與土耳其
用於向私部門提出請求及向私部門提供資訊的線上入口網站，已在許多國家建立（如中國的數位資訊請求系統）。在土耳其，MASAK 要求每家銀行透過專線網絡，以電子方式傳輸金融資料，經由妥適的安全協定與認證，確保資料的安全。

d) 特定部門的合作、宣導計畫與指引

31. 某些國家已與私部門發展出特定合作計畫，這些私部門對威脅，包括資恐威脅，暴露出弱點。這些部門未必是受規範的對象，但以新興模式與分析的觀點而言，卻很重要。當地的政府機關與存在弱點的參與者，例如 NPO，也能參與合作，以判別出可預防及其他措施來因應威脅。

法國與瑞士

對易遭受攻擊部門之宣導計畫，係許多國家對抗恐怖主義與 TF 的重要策略，例如，法國財政部（MoF）與藝術及古董交易商協商，使其瞭解其產業相關之特定 TF 風險，特別是與 ISIS 現行資助活動有關。MoF 已公布對 NGO 之指引，邀集金融機構執行具體的措施，對其客戶的特定風險（與伊拉克的古董、石油貿易）保持警覺。同樣地，瑞士的 NRA 出版後，瑞士當局與藝術品貿易部門展開對話，商討該部門的 AML/CFT 措施，並舉行個別會議以提高業者警覺，由該產業主要的國際拍賣機構代表參加。

加拿大

慈善團體的宣導計畫，係對其法律義務提供建議，應如何自保免於被恐怖恐怖活動濫用。該計畫包含完善的內部治理、財務程序、透明性申報及特定工具如檢查清單、國際架構可使用的網頁等一般指引，以避免恐怖主義濫用。該計畫可採不同的形式，包括網頁、消息來源訂閱、電子郵件分送清單、線上研討會、面對面的會議等。

e) 資訊分享機制

32. 公、私部門間的雙向關係，對打擊 ML/TF 是必需的，資訊分享的機制可包含正式會議與非正式簡報，可以是一對一層級也可能是多數主體，許多國家與私部門間至少舉辦年度會議或研討，以討論新興的風險、威脅與趨勢。諸如執法或安全機關等任務主體常被納入，以提供實務案例或特定風險資訊。其他情形下，洗錢及資恐風險的討論，均爲申報主體會議、研討、訓練的一部分。此外，私部門亦可能發起此類計畫，以促進對潛在犯罪活動更廣泛的討論。
33. 也有可能是一國建立某機制或程序，供私部門近乎即時地將疑似 TF 交易，或顯示即將發生恐怖行動之表徵，申報予執法機關或安全部門。這說明權責機關有管道受理這類資訊並採取相應行動，例如專用電話熱線，或金融機構有即時申報此類案件的法律義務，而非僅有在時限內申報 STR 的義務。
34. 當公、私部門間已建立特別的 TF 工作團隊或任務小組，此時，這類

工作組爲任務協調提供平台，有助於所有參與者提升分析與調查功能。

埃及

埃及銀行聯盟（FEB），作爲一個獨立的非營利團體，聯繫所有的本國銀行與在埃及營運的外國銀行。其宗旨爲所有會員間得討論並分享共同議題，對銀行部門相關之現行法律提供修正意見。

2003 年，FEB 發起成立遵循負責人協會，所有在埃及營運的銀行遵循部門負責人均係該協會會員，該協會定期舉行有關打擊 ML/TF 的會議，中央銀行及 FIU 亦受邀出席，針對會員關注的議題，提供回饋與技術協助。

第六部分

洗錢防制處重要記事

106/1/9	與聖露西亞（Saint Lucia）金融情報局局長保羅・湯普森（Paul Thompson）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」。
106/1/18	協助接待美國國土安全部移民及海關執法局駐香港參贊彭德傑（Christopher Q. Pater），雙方就未來洗錢防制之合作交換意見。
106/1/29-2/3	派員赴卡達多哈參與艾格蒙聯盟工作組會議。
106/1/31	與匈牙利國家關稅管理局匈牙利金融情報中心首長蓋博・西蒙卡（Gábor Simonka）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」。
106/3/3	巴拿馬經濟財政部部長戴拉瓜帝亞（Dulcidio De La Guardia）及駐華大使馬締斯（Alfredo Martiz）來局參訪，本處陪同接待，雙方並就防制洗錢業務進行工作會談。
106/4/13	匯豐銀行集團總經理（大中華區行政總裁）黃碧娟率臺灣區總裁李鐘培等人拜會本處，雙方就匯豐銀行相關申報業務交換意見。
106/4/20	舉辦本局 106 年洗錢防制業務專精講習。
106/5/11-12	派員赴瑞士日內瓦參與艾格蒙委員會。 國防部海軍司令部計畫處處長黃惠明少將率員至本處拜會，就專案資金協查事項交換意見。
106/5/15	於我國駐教廷大使李世明見證下，與教廷金融資訊處處長盧薩（Tommaso Di Ruzza）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」。

106/6/14	星展銀行新加坡總部執行董事（洗錢防制業務最高主管）Chris Wilson 率員來處拜訪，雙方就洗錢防制業務交換意見。
106/6/18-23	派員赴西班牙瓦倫西亞出席 FATF 第 28 屆第 3 次大會。
106/7/2-9	派員赴澳門出席艾格蒙聯盟第 24 屆年會。
106/7/17-21	派員赴斯里蘭卡出席 APG 第 20 屆年會。
106/7/24-28	派員赴韓國釜山參與 FATF TREIN 訓練課程。
106/9/8	臺中地方檢察署林主任檢察官映姿率員來局拜訪，於拜會局長後，與本處進行業務會談。
106/9/20	臺灣臺中地方檢察署郭主任檢察官景銘、張檢察官時嘉拜會局長，就本局於多明尼加電信詐欺案中協查金流表達謝意，本處陪同接待。
106/9/26-28	派員前往日本東京出席 ARIN-AP 第四屆年會。
106/10/2	與拉脫維亞共和國（Latvia）清洗犯罪活動不法所得防制辦公室主任比斯圖氏・勃肯斯（Viesturs Burkāns）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」。
106/10/6	香港上海匯豐銀行亞太區金融系統風險顧問委員會主席 David Irvin 率員來訪。
106/10/18-20	聖文森金融情報中心副處長森蒂（LaTeisha Arielle Rachael Sandy）率員來臺參訪，本局受我國外交部委託，辦理防制洗錢訓練課程。
106/10/22-28	派員赴馬來西亞吉隆坡參與艾格蒙聯盟亞太區策略分析課程。

106/10/29-11/3	派員赴阿根廷布宜諾斯艾利斯出席 FATF 第 29 屆第 1 次大會暨工作組會議。
106/10/30	臺灣高等法院檢察署宋主任檢察官國業拜會林副局長研商跨境電信詐欺專案資金協查事宜，本處陪同接待。
106/11/8	舉辦「106 年金融業防制洗錢及打擊資恐業務承辦人座談會」。
106/11/13-16	派員赴韓國釜山出席 FATF TREIN 及 APG 合辦之「APG 洗錢樣態研討會」。
106/11/26-12/1	派員赴香港出席 2017 年財富調查課程國際中文班。
106/12/26 起	受理比利恩集團疑涉運輸油品予北韓案之相關申報與資金清查。
106/12/27	與迦納共和國金融情報中心（FIU, Ghana）執行長夸庫・杜阿（KWAKU DUA）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」。

國家圖書館出版品預行編目 (CIP) 資料

洗錢防制工作年報 . 中華民國一〇六年／法務部調查局
洗錢防制處編 . -- 新北市：調查局， 民 107. 08
面； 公分

ISBN 978-986-05-6652-9 (平裝附光碟片)

1. 洗錢 2. 犯罪防制 3. 中華民國

548.545 107013963

中華民國一〇六年

洗錢防制工作年報

出版機關：法務部調查局
發 行 人：林玲蘭
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：107 年 8 月

GPN：1010701314
ISBN：978-986-05-6652-9 (平裝附光碟片)

法務部調查局

ISBN 9789860566529
GPN 1010701314

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