監察院112年度通案性案件調查研究報告

壹、題目：政府防制電信網路詐欺之對策與檢討

貳、結論與建議

一、國內112年電信網路詐欺案件數量已突破2萬件，達到歷史新高，經爬梳其脈絡，除與全球電信網路詐欺犯罪情勢相符外，其長期原因包括政府在前次詐欺高發之97、98年期間，相關檢討改進措施未臻澈底，中期原因則係政府法制、規管及政策未能充分跟進數位化、網路化及全球化之進程並加以治理，而衍生諸多犯罪機會及條件；短期因素則因COVID-19疫情爆發後，經濟面不確定性偏高，且民眾已高度依賴行動通訊網路及數位經濟等，以致於詐欺犯罪於近兩年融合短中長期因素後獲得爆發性成長，嚴重侵害國人生命財產安全。政府雖陸續制定「打詐綱領1.0」及「打詐綱領1.5」，以「識詐」、「堵詐」、「阻詐」、「懲詐」四大面向強化打詐效能，並陸續修訂「打詐五法」，並推動「打詐新四法」等，以全面補強規管漏洞並提高嚇阻力，惟迄113年5月為止，詐騙情勢仍不容樂觀，政府允宜持續積極檢視行政面稍嫌薄弱之環節，透過上游清源防制提高整體打詐綜效。

(一)89至112年間電信網路詐欺案件之數量變動趨勢(如下圖1)[1、2]，顯示97、98年間電信網路詐欺案件曾一度攀升至1.9萬件，經政府大力掃蕩，於102年降至6,355件之新低，105至110年起每年穩定於1.3萬件左右，直至111年起快速成長，至112年突破歷史高

[1] 89至104年，曾雅芬(民105) 行騙天下：臺灣跨境電信詐欺犯罪網絡之分析。國立政治大學國家發展研究所博士論文。(該報告引用警政署資料繪製)。

[2] 105至112年，引用警政署資料，本院繪製。

峰至20,958件，年增率達33.1%；對照全球反詐聯盟(Global Anti-Scam Alliance，下稱GASA)於2022年提出之報告[3]指出，2021年全球共收到約2.93億份詐騙案件通報，相比2020年增加了10.2%；可見全球詐欺犯罪情勢在過去兩年持續升溫，而我國之詐欺案件成長率明顯高於國際平均，顯見情勢之嚴峻。

此外，本調查研究必須指出，政府所公布之詐欺案件數據並不包括未報案之黑數，故尚無法完整呈現國人遭詐欺犯罪危害之嚴峻程度。若依GASA推估，根據國家的不同，只有3%~17%的詐騙被通報；此與本院諮詢國立中正大學犯罪防治學系許華孚教授指出:「如果我們以犯罪學的黑數的話，大概要乘以10倍」大致相符。

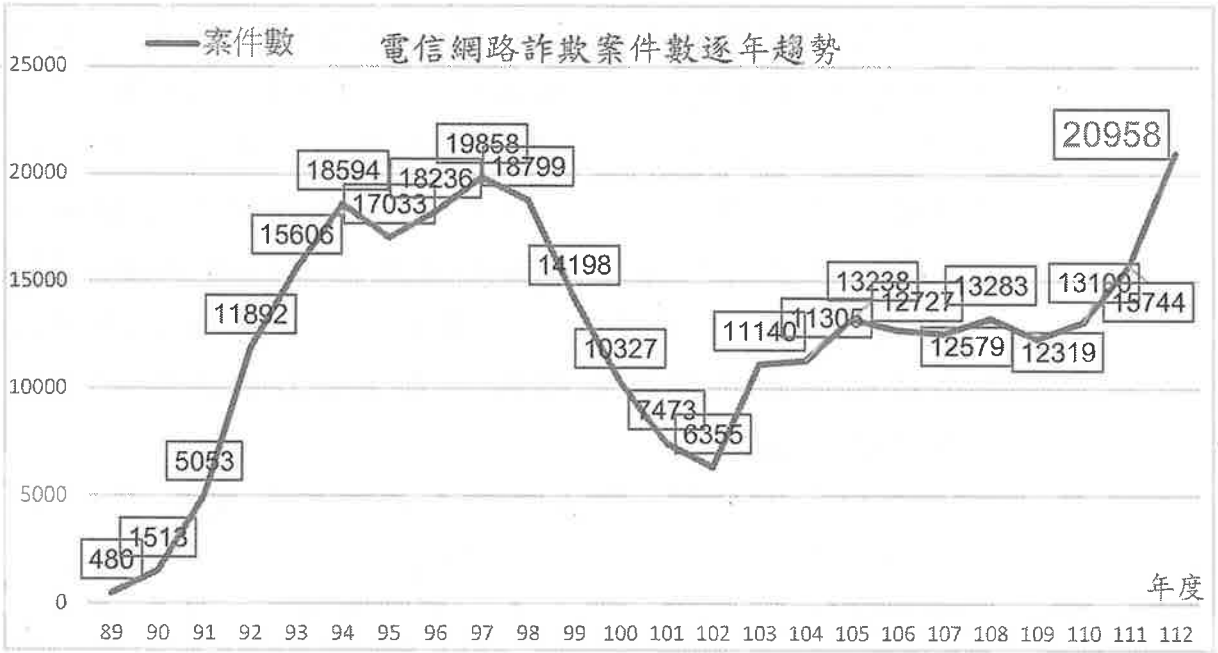

圖1　89至112年間電信網路詐欺案件之數量逐年趨勢（單位:件數）。

資料來源：警政署113年6月19日內授警字第1130878508號函及曾雅芬研究[4]，本院自行整理。

[3] The Global State of Scams Report - 2022

[4] 曾雅芬(民105) 行騙天下：臺灣跨境電信詐欺犯罪網絡之分析。國立政治大學國家發展研究所博士論文。

1、高檢署資料顯示，各地方檢察署(下稱各地檢署)112年電信網路詐欺案件新收案數(229,711件)較前一年度(111年)成長42.9%，相較於警政署112年電信網路詐欺案件(20,958件)成長率33.1%，顯得更為嚴峻；至於警政署發生數係如何由統計資料之2萬餘件，經檢警合作偵查程序後移送案件數達20餘萬件[5]，警政署及高檢署尚難提出具體說明，由於事涉政府對於電信網路詐欺嚴峻程度及檢警機關案件負荷之解讀，本調查研究亦建議警政署及高檢署進一步釐清。

（1）各地檢署110年電信網路詐欺案件新收案數為98,256件，111年暴增至160,803件，112年再成長至229,711件，112年較前一年成長率約為42.9%。

（2）若以身分唯一化處理，新收人數為73,789人，其中初犯電信詐欺案件終結人數經身分唯一化，計14,600人，以單純人頭帳戶9,181人最多[6]。

（3）進一步探究人頭帳戶案件之增長，地檢署112年1月至9月新收案109,476件，較111年同期(1~9月)增加47,722件，成長77.3%[7]。

（4）另查金融機構(銀行、中華郵政)警示帳戶總數，109年第2季31,735戶，至112年第2季已成長至103,767戶，3年間成長3.27倍[8]。

2、在圈存、查扣及返還部分，依據警政署提供111、112年比較數據如表1：

---

[5] 各地檢署電信網路詐欺新收案件按高檢署提供資料，約有85%來自警察機關移送；爰推估112年警察機關移送約20萬餘件電信網路詐欺案件。

[6] 高檢署112年11月13日簡報資料。

[7] 高檢署112年11月13日簡報資料。

[8] 高檢署112年11月13日簡報資料。

表1　111及112年詐騙金額圈存、查扣、返還與財損金額間之關係

單位：元

項目	111年	112年	增減值
圈存部分	3.2億元	3.9億元	0.7億元
查扣部分	22.1億元	39.2億元	17.1億元
返還部分	13.0億元	20.0億元	7.0億元
財損金額	73.3億元	88.8億元	15.5億元

資料來源：行政院於113年6月3日座談提供書面資料。

3、除GASA報告指出，2021年全球共收到約2.93億份詐騙案件通報，相比2020年增加了10.2%之外，尚有其他佐證數據如下：

（1）96%的澳洲人過去5年曾遭遇詐騙，其中半數每週或每天都接觸到詐騙訊息；在法國，有61%民眾曾在過去一年接觸過「另類的」投資機會，在英國，則有半數電話受訪者表示在一個月內收過疑似詐騙的釣魚信件或社群媒體訊息。

（2）新加坡警方表示，90%的詐騙源自海外，並將詐騙者描述為聯合組織、資源豐富且技術先進，案件很難偵破。

（3）在財損部分，平均被詐金額最高的是新加坡（4,031美元/人）、瑞士（3,767美元/人）和奧地利（3,484美元/人）。巨額財損在全球造成了嚴重的財務影響，報告估計損失總計高達1.026兆美元，相當於全球GDP的1.05%，若以國家為單位，肯亞受詐欺打擊最嚴重，其GDP因詐騙損失了近4.5%，其次是越南（3.6%）、巴西和泰國（3.2%），而追回詐款的比率很低，只有約7%成功追回。

4、另據英國2023年6月公布之打詐策略(Fraud Strategy: stopping scams and protecting

the public)[9]指出，2022年每15名成年人中就有1人成為受害者，對社會造成的總成本估計至少為68億英鎊，包括受害者損失的金錢、照顧受害者的費用以及返還、調查和起訴詐欺者的費用。

5、小結：由高檢署、警政署及GASA資料綜合研判，近年全球詐欺犯罪情形均有明顯之快速成長趨勢，且具有「黑數多」、「難追回」之特性；復經比較國內外數據，臺灣近年詐欺犯罪成長率(33.1%)遠高於國際平均，顯見情勢極為嚴峻；然而若以被詐金額追回比率觀察，我國111及112年返還財損金額比率分別為17.7%及22.5%，則遠高於國際平均7%。

(二)在長期原因之分析方面，經蒐整本院電信網路詐欺相關調查報告顯示，本院自98年起即陸續完成7件調查案，研究發現部分調查意見迄未獲有效改善。

1、依據「監察院立案派查原則」第3點第1項規定，如有「發生重大災變或嚴重社會問題，不能迅速處理或處理失當」(第4款)、「怠忽職守，致民眾權益受損」(第9款)等情事，本院得立案調查。經查本院自98年起，共通過7件涉及電信網路詐騙之調查報告，依其時序分別為98至99年間3案，106年1案，111至112年3案，顯示98至99年詐騙案件曾一度猖獗，至111年起電信網路詐騙案件又再度急遽成長，其時間分布與98年迄今之詐欺犯罪案件統計數據顯然具正相關。

2、進一步檢視全部調查意見，部分內容雖因時空變遷及技術演進減損其參考價值；然經分析，本院

[9] https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public

調查意見若依「識詐」、「堵詐」、「阻詐」及「懲詐」進行分類，多數調查意見所指缺失時至今日仍未澈底改進，例如98交調0034已指出二類電信監督不周之失，106司調0019亦已指出個資及洗錢防制方面之缺失，茲將詳情分析如下表2，行政院及相關主管機關實宜予以正視。

表2　監察院過去提出電信網路詐欺相關調查意見概要。

面向	本院相關案件調查意見
識詐	行政院新聞局長期怠於執行反詐騙宣導工作，……難以評估宣導效果，肇致執行成效不彰，均有不當(098交調0034調查意見四)
	教育部校安中心，……顯見該部長期忽視反詐騙校園預防宣導工作，欠缺整體有效之推動機制，致成效不彰，確有不當(098交調0034調查意見六)
堵詐	行政院自93年迄今，長期漠視電話詐騙案件問題之嚴重性，未積極協調電信人頭資料庫……造成嚴重之財產損失，均有不當(98交調0034調查意見一)
	詐騙集團利用二類電信進行詐騙犯罪活動，主管機關通傳會未落實監督管理及行政檢查之責，核有違失(099內調0106調查意見五)
	……通傳會及警政署允宜檢討現行措施，源頭管制人頭電話及採取有效宣導(傳)措施，抑制詐騙集團，避免民眾遭騙(106司調0019調查意見二)
阻詐	銀聯卡……淪為不法集團洗錢之工具，惟其所隱藏之犯罪黑數及是否益趨增加，相關統計資料付諸闕如，有關單位允應儘速建置完整之資料庫……(106司調0019調查意見五)
	……金管會宜評估是否要求金融機構在定型化契約條款中以明顯顏色或粗體字呈現並請客戶特別簽名，或於其請領存摺及提款卡、密碼時簽具切結書，或直接於存摺封面印上「勿遭詐騙集團詐騙匯款」之警語，……又金管會應……更有效地減少人頭帳戶之產生(111司調0027調查意見五)
懲詐	行政院與司法院未能有效遏阻詐欺犯罪案件蔓延，致詐欺犯罪案件起訴率、定罪率、量刑刑度及入監率均有逐年降低之趨勢，實難發揮刑罰應報、嚇阻、隔離與矯正等功能……(098司調0040號調查意見二)
	……詐欺犯罪之起訴率仍偏低，法官在詐欺犯罪量刑上仍有輕判之事實，顯示詐騙犯罪被害情形仍相當嚴重……（099內調0106調查意見二）
	近年電信詐騙集團已組織化並跨境為之，且集團成員再犯率甚高，……允宜加強運用「任務型聯絡官」等機制，建立合作窗口與溝通管道，與國際社會共同打擊不法。(106司調0019調查意見四)

資料來源:本院自行整理。

3、以統計數據及蒐整資料相對完整之量刑部分舉例，本院098司調0040號案調查意見二曾指出略以:「詐欺犯罪案件起訴率、定罪率、量刑刑度及入監率均有逐年降低之趨勢，實難發揮刑罰應報、嚇阻、隔離與矯正等功能」，然而本調查研究無論是由文獻的質化性描述或機關提供之量化資料，均發現該調查報告意見迄今仍未獲澈底檢討，以致於無法有效抑制詐欺犯罪之猖獗。

（1）在質化性描述部分，105年仍有文獻[10]指出，「詐欺案件因罪行輕微或蒐證不易，起訴比率較低，定罪率雖高，刑度卻極輕，……其投資報酬率對於集團成員來說仍是極高」等語。

（2）復以本院112年11月13日赴高檢署辦理履勘時，法務部亦稱:「關於刑度過低部分，因為法官審判獨立，所以在與司法院溝通上稍有困難，……法官只要在法律所規定最低刑度以上量刑都是合法，最後定執行刑只有1至2年」；臺北地檢署劉仕國主任檢察官亦提出量刑及定執行刑之現況仍然無法發揮刑罰應報及嚇阻功能之情形如下；

〈1〉現在司法實務，法院不分案件，幾乎全部都是從最低刑度開始量。

〈2〉在法院定執行刑時，更是容易產生爭議，例如，詐欺車手犯了20次，每次都判1年，……加起來你以為要執行20年，錯！只要法院定應執行刑是1年1個月就已經是合法的，我想這不要說我們檢察官常常無法接受，人民要

[10] 曾雅芬。民105。行騙天下：臺灣跨境電信詐欺犯罪網絡之分析。國立政治大學國家發展研究所博士論文。

是知道了，大概也都無法接受。

（3）在量化數據資料部分，經分析高檢署提供近三年法院審理電信詐欺案件判決刑度，109年時觸犯詐欺罪為法院裁判確定刑度6個月以下者占全體有罪判決35.8%(4,758/13,272)，至112年1至9月，其比率已成長至61.7%(12,380/20,053)，如下表3：

表3　地檢署電信網路詐欺案件-執行裁判確定人數

單位：人

年度	6月以下	6月-1年	1-2年	2-3年	3年以上	拘役	罰金	免除其刑	有罪合計
109	4,758	651	4,996	329	76	2,415	37	10	13,272
110	4,247	514	5,742	284	117	1,661	31	8	12,604
111	10,554	585	7,055	224	71	1,206	29	5	19,729
112 (1~9月)	12,380	594	6,196	183	61	611	28	0	20,053

資料來源：法務部及高檢署112年11月13日簡報資料。

（三）在中期之原因分析部分，研判係因政府法制、規管及政策未能充分跟進數位化、網路化及全球化進程並加以治理，而衍生諸多犯罪機會及條件，符合犯罪學之日常活動理論，其論證如下：

1、臺灣民眾社群平臺以Facebook為主，通訊軟體以LINE為主，普遍而言上網普及率及行動寬頻普及率均高。

（1）調查結果[11]顯示近五成臺灣民眾最常使用的社群媒體仍是臉書（Facebook），達47.27%，大幅領先其他社群媒體。而社群媒體使用率與年齡

[11] 財團法人台灣網路資訊中心。112年6月。「2023年台灣網路報告」。

成反比，年齡愈低則社群媒體使用率則越高。18至29歲年齡層為社群媒體使用率最高的族群，高達95.98%。而30至39歲年齡層的社群媒體使用率也在九成以上，達94.84%。

（2）在通訊軟體部分，調查結果[12]顯示LINE是臺灣民眾最常使用的即時通訊軟體，占77.56%，以懸殊的占比大幅領先其他的即時通訊軟體。

（3）2023年臺灣民眾的上網率為84.67%，18至49歲族群更高達95%；而通傳會「112年通訊傳播市場報告」指出我國行動寬頻普及率於近10年快速成長，已於2016年超越英國，2022年普及率為118.69%，可見民眾(尤其年輕民眾)已相當程度跟進數位化、網路化及全球化之進程。

2、至於民眾數位化、網路化及全球化之進程如何產生詐欺犯罪機會，有文獻[13]係以犯罪學之日常活動理論三要素作為理論依據，本調查研究並以本院諮詢學者專家意見及第一線偵辦案件之檢察官說法做為佐證，可推導出詐欺案件之中期因素，係因政府法制、規管及政策未能充分跟進數位化、網路化及全球化進程並加以治理之結論，至於究竟是哪些法制或政策未充分跟進，本調查研究亦將於後續之結論與建議，依「識詐」、「堵詐」、「阻詐」及「懲詐」各環節逐一分析，並試圖進一步就政府尚未跟進全球化進程之項目，研判電信網路詐欺未來趨勢。

（1）文獻指出，跨境電信詐欺犯罪的發生**符合日常活動理論三要素，包括犯罪者、標的物及監控**

---

[12] 財團法人台灣網路資訊中心。112年6月。「2023年台灣網路報告」。

[13] 曾雅芬。民105。行騙天下：臺灣跨境電信詐欺犯罪網絡之分析。國立政治大學國家發展研究所博士論文。

缺乏，其中監控缺乏部分應擴大至國家管制監控的缺乏來探討。全球化在政治、社會、經濟各層面的影響，也影響著跨境犯罪的變化。**國家治理失靈形成了國家的侷限性、跨國網際網路無法管制、洗錢現象及全球金融系統去管制化，均促進跨境犯罪的盛行**。犯罪者有限度的理性選擇、犯罪流程步驟的考量，犯罪團體日常活動理論三要素的聚合，監控者層面需跨大至國家層面有關國家管制、網路管制及金融管制的缺乏的探討，再加上新興犯罪接觸管道，形成新機會理論中的犯罪機會。

〈1〉跨境詐欺犯罪地點及被害地點，自臺灣到大陸，再轉到東南亞，至今分散到世界各國；犯罪型態從單一國家演變成雙邊合作，再到跨越三地合作。

〈2〉詐欺集團自兩岸據點轉移至東南亞地區發展時，有特殊的集中現象，顯示東南亞地區國家提供了極佳的犯罪機會。

〈3〉集團成員的理性選擇：……透過訪談詐欺犯罪者發現，犯罪者會衡量犯罪種類的刑期長短，隨時瞭解法律修正內容、輕重程度及證據證明力之效力，詐欺犯罪刑罰過輕，其投資報酬率對於集團成員來說仍是極高。

（2）本院諮詢學者專家意見再度印證新科技及所衍生之新服務，同時也製造更多犯罪機會，而當政府治理未充分跟進時，將使犯罪偵查越形困難。

〈1〉犯罪這種社會現象很重要的一個元素就是機會。每當金融機構或電信業者提出了新的商品或是服務，我們研究犯罪的學者第一個

反應，就是又為犯罪增加了很多機會。

〈2〉當業者在開發這些新的商品和服務的時候，在安全上面不會花很大的精力，這種問題不是只存在電信業者或金融機構，過去在汽車製造商也發生過很多的瑕疵車，都是一直要到損害非常嚴重的時候，業者才願意做一些修正。

〈3〉犯罪的機會是只會增加而不會減少。當業者花了很大的經費去研究新的商品跟服務時，我們可能要回頭看看政府部門在新增部門上，在偵查上面，在起訴上面，在矯正上面，我們大概花了多少的預算?你會很清楚地看到我們一直苦苦的在後頭追趕。

（3）基層檢察官團體-劍青檢改則認為詐欺猖獗之因素如下，可見在新科技新服務之外，尚須複合政府治理未充分跟進之因素，始能形塑電信網路詐欺之犯罪機會。

〈1〉金門地檢署施家榮主任檢察官

《1》**詐欺它也是一個產業，它為什麼會蓬勃發展?他錢多當然要求發展，你就沒有法律，沒有科技偵查手段，一直追不到核心幹部，一直追不到他的錢，他錢越來越多，一間公司錢越來越多，他不發展合理嗎?他一定要蓬勃發展嘛!**

《2》人頭帳戶抓了，為什麼他明年還有人頭帳戶可以用?我們就不知道金管會在做什麼?今年被抓了幾萬個人頭帳戶，明年他還有幾萬個，後一年還有幾萬個?永遠源源不絕。

《3》再來說律師涉案、銀行人員幫忙調整轉帳

上限、派出所所長查個資、通傳會前委員當二類電信業者顧問這些，為什麼?因為你永遠查不到他的心臟，那他就可以經驗傳承，越教越多人，他獲利高風險低，**因為人頭帳戶、人頭門號、個人幣商都沒在管，他就挺而無險，他當然要繼續做啊!**

〈2〉臺北地檢署姜長志檢察官

《1》你前端的行政管制呢？你不告訴個人幣商要怎麼登記？怎麼設立？什麼條件都沒有，就跟我說那這樣算犯罪了？金管會說犯罪的潛臺詞是什麼意思？就是那是檢察官的事啊！

《2》我們來盤點一下他有違反洗防法嗎？有違反VASP原則嗎？沒有嘛！所以到現在到今天4月26號，虛擬通貨原則都沒有規定什麼叫個人幣商啊，**各位你可以想像嗎，法院還要自己去想，自己去定義什麼叫個人幣商。**

(四)詐欺集團因上開中長期因素及條件，醞釀利用行動通訊網路、網路金融服務及購物、虛擬貨幣投資、第三方支付等工具進行電信網路詐欺已有數年，並非近兩年才成熟；因此，可推論應有短期因素之複合影響。經綜整文獻及政府公開資料，本調查研究研判短期因素係因COVID-19疫情爆發後，經濟面不確定性偏高，且民眾已高度依賴行動通訊網路及數位經濟等，終使電信網路詐欺犯罪於近兩年獲得爆發性成長。此外，雖然短期因素所導致之電信網路詐欺趨勢係全球皆然，並非我國獨有，然而我國上網普及率優於多數國家，或許是近兩年電信網路詐欺犯罪成長率高於國際平均之部分原因。

1、在短期經濟面因素，根據國家發展委員會2023及2024年1月所公布之「當前經濟情勢簡報」[14]可知，近兩年全球經濟處於成長動能平疲、先進經濟體經濟表現分歧、成長動能趨緩及主要經濟體動能多呈停滯之情況。而我國打詐綱領1.5版亦稱：「觀諸自109年起，COVID-19疫情期間居家辦公、網購等宅經濟興起，嫌犯利用簡訊、電子郵件、投資詐騙網站等網路詐欺案件逐年呈現增長情勢」[15]。

2、在國際上，GASA指出「詐騙案件強勁成長不僅是因為數位化程度加快，而且是複合高通膨、高生活費及高失業率的背景，而迫使人們尋找新的投資方式而維持收支平衡」，英國政府亦均有報告[16]指出，消費者、企業和詐騙集團對新科技的採用幾乎肯定是近期詐欺案件成長的主要驅動力；在在顯示在電信網路詐欺犯罪之短期因素方面，我國情形與全球趨勢概同。

(五)針對嚴峻之詐欺情勢，政府雖陸續制定「打詐綱領1.0版」及「打詐綱領1.5版」，以「識詐」、「堵詐」、「阻詐」、「懲詐」四大面向強化打詐效能，但整體詐騙情勢仍然處於高發狀況，本調查研究建議政府持續積極檢視行政先行措施稍嫌薄弱之環節，透過上游清源防制提高整體打詐綜效。

1、研究分析「打詐綱領1.5版」之經費需求簡表，在整體經費需求8.7億元中，懲詐面經費需求約占82%(約7.2億)，復經檢視其經費需求內容，大多

---

[14] https://www.ndc.gov.tw/News.aspx?n=8E8FA34452E8DBC2&sms=40C8FF59B01AC562

[15] 新世代打擊詐欺策略行動綱領1.5版，第4頁。

[16] Fraud Strategy: stoppingscams and protecting thepublic(https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public)

數均係為採購偵查設備及其必要之附屬設施；理論上前述投資有助於犯罪偵查，對於詐欺犯罪之破獲率應要顯著提高。

2、惟進一步檢視行政院於113年5月9日公布「『打詐綱領1.5』執行成效與策進」績效，在懲詐部分包括偵破詐欺集團由上期(111年6月至112年3月)1,481件成長至本期(112年6月至113年3月)之1,909件，同比增幅約29%，查獲犯嫌人數則由上期(111年6月至112年3月)13,484人成長至本期(112年6月至113年3月)之17,068人，同比增幅約為26.6%，其破獲之集團及人數雖有明顯成長，但全未超過112全年度案件成長率(33.1%)，顯示行政院所稱偵破及查獲之成長率，實際上應係隨警政署收案件數等比例成長，而非破獲率有所成長。

3、前述結果不僅不易彰顯「打詐綱領1.5版」於懲詐面之成效，更進一步隱含政府在「識詐」、「堵詐」、「阻詐」等上游治理未臻完善時，即使於懲詐面挹注超過8成經費，仍難以發揮打詐之綜效。

4、另經分析「打詐綱領1.0版」及「打詐綱領1.5版」關於詐騙樣態之數據(如下表4)顯示，假網路拍賣購物、投資詐欺及解除分期付款詐欺案件持續高發，而其中投資詐欺不僅在案件數量方面持續成長，在財損比例竟占全部電信網路詐欺之50.55%，顯示政府應置重點於投資詐欺，始能有效打擊電信網路詐欺。

表4　打詐綱領1.0及1.5版所列詐騙案件樣態比較(單位：%)

	打詐綱領1.0	打詐綱領1.5		增/減幅百分點
	案件比率	案件比率	財損金額比率	案件比率
假網路拍賣	22.74%	23.01%	6.27%	+0.27
投資詐欺	19.8%	22.17%	**50.55%**	**+2.37**
解除分期付款	17.51%	17.23%	10.39%	-0.28
猜猜我是誰	7.11%	-	-	-
假愛情交友	4.75%	-	-	-

資料來源:本院自行整理

5、有關「識詐」、「堵詐」、「阻詐」相關法規及行政規管等上游清源措施重要性之質化性描述，普遍見於本調查研究所蒐整之文獻及報告中，而本院諮詢學者專家及第一線偵辦案件之基層檢察官亦持續針對行政措施缺漏不斷提出建言，爰不贅述；行政院有鑑於此，陸續修訂「打詐五法」，並推動「打詐新四法」等，以全面補強規管漏洞並提高嚇阻力，至113年5月9日公布「『打詐綱領1.5』執行成效與策進」時，已能提出初步法制及成效行政規管成效如下：

（1）112年度分層分眾識詐宣導總觸及人數達3億3千萬人次。

（2）攔阻與圈存金額達93.79億元。

（3）112年6月起至113年3月，建置國際來話攔阻及警示機制後，「+886」國際來話話務量相較實施前已大幅減少96.7%。

（4）推動「111政府專屬短碼簡訊」，目前已經有122個機關完全導入。

（5）有5家業者導入「物流隱碼」技術。

（6）透過強化管理電子支付的帳戶，警示帳戶的數目也下降了91%。

（7）建立「遊戲點數防詐鎖卡平臺」，國內遊戲點數詐騙的案件也減少了94%。

6、行政院113年5月9日公布「『打詐綱領1.5』執行成效與策進」新聞稿坦承「目前詐欺案件仍處嚴峻的高原期」，並說明打詐騙集團隊將持續努力，針對詐欺集團新興手法，提出應處與阻絕措施，滾動式修正，除擬具打詐專法（詐欺犯罪危害防制條例）及配套三法（科技偵查及保障法、通訊保障及監察法、洗錢防制法）[17]，強化防詐法制規範外，亦將研修「新世代打擊詐欺策略行動綱領2.0版」，結合技術面，形成綿密的防詐保護網絡，保障民眾財產安全。

7、復查高檢署提供資料，各地檢署110年電信網路詐欺案件新收案數為98,256件，111年暴增至160,803件，112年再成長至229,711件；換言之110至111年之電信網路詐欺案件新收案件年增率高達63.7%，而111年至112年之年增率則降為42.9%，另查高檢署最新資料，113年1至5月份新收案件數為74,317件，僅112年全年度之32%，亦可佐證電信網路詐欺仍在持續高發，惟其成長率已有趨緩跡象。

(六)綜上，基於「打詐五法」及配套之行政規管措施施行未久，其效益恐尚未充分顯現，而「打詐新四法」雖已陸續於113年7月前完成修法，相關成效亦有待觀察，建議政府持續積極檢視行政先行措施稍嫌薄弱之環節，包括堵詐面之門號核配及數位平臺治理，阻詐面之人頭帳戶及虛擬貨幣控管等等，同時適度檢討削減事倍功半之打詐措施(如網域停止解析等)，本調查研究亦將逐一臚陳於後續結論與建議，俾透過上游清源防制提高整體打詐綜效。

---

[17] 「打詐新四法」截至113年7月16日為止已全數三讀通過。

二、「識詐」主要目標係降低被害人之風險，提升民眾防詐能力，行政院雖已動員16個部會、挹注大量資源且極盡所能透過分層、分眾、分齡進行宣導，112年觸及人數已達3億3千萬人次，卻尚未有效抑制詐欺案件之成長。本調查研究經綜整國內外文獻、機關查復資料及學者專家意見發現，首先相較於國際，我國民眾對自身識別詐騙之能力仍過於自信及抱持冒險心態，有待政府設法扭轉；其次，長期高強度且重複之宣導有邊際效用遞減之虞；最後，政府識詐措施之績效指標均「以量取勝」，缺乏措施與效用間之因果關係連結；為避免識詐相關措施事倍功半，政府允宜在識詐策略方面導入「公私協力」及「循證治理」概念，俾提升政策效果。

(一)識詐為預防之概念，先阻絕可能發生之詐騙於前期，阻止詐騙集團戕害民眾財產乃之於人身之安全，因此，提升全民識詐能力、讓民眾對於詐騙手法有所認知，以及在識詐宣導上達到素材的「質」，與宣導觸及人次的「量」並俱，且「識詐是成本最小，效益最大之良善作法」。因此識詐於「打詐綱領1.5版」列為最上游之詐欺犯罪打擊措施，綱領中敘明，「識詐」由內政部擔任統籌機關，從民眾角度思考如何降低被害風險，強化分層、分眾、分齡犯罪預防宣導工作，提升民眾防詐免疫力，迄至112年底，識詐措施的觸及人數已達**3億3千萬人次，每人每年所接觸到的識詐宣導高達14次，然而詐欺犯罪仍然處於高發狀態，有進一步探討之必要。**

1、依據警政署提供資料，識詐領域由內政部擔任統籌機關，而協辦機關包括法務部、教育部、國防部、勞動部、衛生福利部、金管會、國軍退除役官兵輔導委員會、公平交易委員會、通傳會、原

住民族委員會、客家委員會、農業部、交通部、外交部、行政院消費者保護處及新聞傳播處、經濟部等，高達16個部會，並均訂定工作項目，顯見行政院在識詐方面已全面動員部會。

2、「打詐綱領1.5版」對識詐訂有三大指標，分別為每年宣導資訊觸及3,000萬人次、每年發送防詐簡訊1億4,000萬及每年平均攔阻率提高5%。

3、行政院在113年5月9日公布「『打詐綱領1.5』執行成效與策進」時，指出112年度分層分眾識詐宣導總觸及人數達3億3千萬人次，已遠超原訂目標；如以臺灣總人口[18]2,341餘萬人計算，每人每年所接觸到的識詐宣導高達14次。

4、然而行政院於113年5月9日仍坦承「目前詐欺案件仍處嚴峻的高原期」[19]，亦有金融機構報告[20]指出34%民眾認為「訊息及連結太逼真」，33%「疏忽未留意到是假的」；換言之，有六成電信網路詐欺受害者雖然每年接觸超過14則識詐宣導，但是仍未有效達成降低誤信之目的。

5、小結：政府以超出原訂目標之宣導觸及率仍無法有效降低民眾誤信詐騙訊息，其原因顯有進一步探究之必要。

(二)打詐綱領1.5版雖然指出，許多民眾產生麻木及過度自信心態，甚而對宣導資訊視而不見，亦未有轉告、

---

[18] 中華民國內政部戶政司全球資訊網- 人口統計資料
https://www.ris.gov.tw/app/portal/346

[19] 行政院打擊詐欺辦公室。113年5月9日。「打詐綱領1.5」執行成效與策進。
(https://www.ey.gov.tw/Page/448DE008087A1971/46e7c357-b756-467c-81ab-19e70648ee8d)

[20] 國泰世華銀行。113年6月25日。「每3人就有1人受騙 國泰世華發布首份《反詐行為調查報告》」
https://www.cathayholdings.com/holdings/lastest_news/news_archive/newsarticle?newsID=QkVmzZKnzEy76yPAxNFJJA

提醒親友的警覺性，導致遭詐風險提高。但本調查研究經分析國內外文獻，多數文獻在民眾防詐意識部分均指出，民眾對於自身辨別訊息真偽之能力仍然過於自信，部分民眾更抱持冒險心態，我國更明顯較國際嚴重，值得行政院注意。

1、根據文獻[21]指出，臺灣有高達80.99%民眾有信心可以辨別詐騙手法，僅15.62%民眾沒有信心可以識破詐騙手法，且有49.47%的民眾認為「社群媒體上的訊息不太可信」，而我國電信網路詐欺案件112年相較111年，卻成長了33.1%。

2、對照GASA-2022年報告，全球有69%的受訪者對識別詐騙表示有信心，而2021年相較2020年通報數量增加了10.2%[22]，由上開數據顯示，民眾對自身的識詐能力存在廣泛的自信，而我國民眾對於識詐的信心又顯著高於國際，則其自信心究竟源自何處?又是否存在過度自信之問題?本調查研究限於調查資源無法進一步剖析，有待相關機關進一步研究。

3、另據GASA-2023年報告亦指出，27.9%受害者的受騙原因為「不確定是否為詐騙但選擇冒險」，可見應有相當比例的臺灣民眾抱持冒險心態在面對詐騙的利誘，最典型的例子出現在「投資詐騙」，為了獲得高額報酬，多數受害者選擇採取以小搏大的態度，也再次說明民眾對識詐之自信心與實際受詐脆弱性形成鮮明對比。

4、若以臺灣民眾對識詐之自信及電信網路詐欺犯罪之成長率與GASA報告數據互相參照，可以發現

[21] 財團法人台灣網路資訊中心。112年6月。2023年台灣網路報告。
[22] GASA。2023。The Global State of Scams Report – 2022。(https://www.gasa.org/downloads)

我國民眾識詐信心遠高於國際平均，然而該等信心並未呈現在警政署的電信網路詐欺之案件數上，反而臺灣電信網路詐欺犯罪成長率高於國際平均。換言之，本調查研究似可推導出「**越自信不會被詐騙，越容易被詐騙**」之結論，至於如何避免民眾對識詐能力過度自信，均有待行政院及相關部會進一步研究並提出對策。

(三)其次，長期高強度且重複之宣導有邊際效用遞減之虞，此在行政院於112年8月10日會議已指出相關疑慮；而行政機關雖然已經試圖針對宣導對象執行分層、分眾、分齡之措施，但在精準度及創意性方面似仍不足以在資訊爆炸時代對民眾建立足夠的識詐免疫力；本院諮詢學者專家亦認為，在資訊爆炸的現代數位媒體及平臺，要使全體民眾認知某件事物之重要性確為挑戰；爰此，本調查研究建議行政院於擬訂「打詐綱領2.0」時宜適度調整識詐策略。

1、在經濟學上，邊際效用是指每新增（或減少）一個單位的商品或服務，消費者所獲得增加或減少的效用，而隨著商品或服務的量增加，邊際效用將會逐步減少[23]；若將概念應用於識詐宣導方面，顯然宣導觸及人次並不是越高越有效。在理論上，人均宣導次數到達一定次數後，對於識詐能力之增長極微，而使超出最佳次數之宣導作為成為多餘且缺乏效益之投資；質言之，在國家資源及人力有限的情形下，政府應透過相關剖析或研究以尋求最有效率之宣導策略或方式。

2、行政院在112年8月10日召開「研商『新世代打擊

---

[23] 教育部重編國語辭典修訂本
https://dict.revised.moe.edu.tw/dictView.jsp?ID=18775&la=0&powerMode=0

詐欺策略行動綱領』相關議題(第15次)精進會議記錄」中，有關「識詐」執行具體措施成效部分即坦承：「於各部會齊力合作及多管齊下，雖已拓展鋪天蓋地之宣導通路，惟若僅以量能視之，恐致疲勞效應亦難長久……」等語，顯見政府機關已有正確問題意識，復據本院蒐整機關查復資料顯示，政府識詐宣導確有進行執行分層、分眾、分齡之措施，在「打詐綱領1.5版」中，共動員16個部會即可見一斑。

3、承上，以教育單位為例，係分別針對各教育階段如幼兒園、國小、國中、高級中等學校及大專院校設計打詐宣導，並由內政部派警員入園宣導防詐觀念、幼兒園參與警局防詐微電影拍攝、幼兒園參訪警局防詐宣導等，甚至在高齡長者宣導方面，亦透過警察勤務區系統結合村里鄰長，於村里民大會、辦公處、治安座談會、社區關懷據點及各式活動時機傳遞防詐資訊；然而，本調查研究必須指出，員警本身勤務已非常繁重，近年各式勤務不斷增加，派遣員警進行分齡識詐宣導將使其勤務負荷遽增，更難以要求其具備精準度及創意性，恐非最有效率之宣導方式，內政部於擬訂識詐措施時，宜由策略面思考以避免浪擲寶貴警力。

4、其次，於目前資訊爆炸的情形下，欲獲取民眾之注意力並予以宣導對政府機關而言確為挑戰，本院諮詢國立中正大學傳播學系羅世宏教授，其意見當可歸納為兩大原則，一是必須以實例作為宣導素材，二是必須運用政令宣導以外方式進行，例如戲劇等；而臺灣事實查核中心邱家宜執行長則建議可以與數位平臺(如Google)及非營利組

織進行更深度的合作。

（1）國立中正大學傳播學系羅世宏教授：

〈1〉應蒐集實際案例普為傳播，預先告訴民眾有哪些詐騙類型，看到的話要有警覺性，有點像是打預防針。

〈2〉把詐騙故事戲劇化，像「金派特攻隊」效果很好。尤其**現在新聞疲勞，現在使重要事情讓全國人知道是一件困難的事情**，因此要用有創意的方法，包括戲劇化，包括跟網紅合作，去打造宣傳，傳統政令宣導點擊率應該很低。

（2）臺灣事實查核中心邱家宜執行長:，我覺得整個學校體系或教育部如果能夠多做一點系統性的、結構性的公私協力措施，那會更有幫助。

5、小結：由本調查研究蒐整機關查復資料顯示，政府機關確實已盡其所能進行宣導，然而在策略和方法上似有強化之空間，行政院於擬訂「打詐綱領2.0」之識詐措施時，宜考量邊際效用原則，並參考傳播學者意見。

(四)最後，本調查研究發現「打詐綱領1.5版」所設定之績效指標均係以量取勝，尚乏措施與效用間之因果關係連結，將導致後續政策檢討調整方向或資源時，欠缺用以制定對策之分析資料，即所謂「循證治理」概念；此外，數位行銷在業界乃極為專業之學門，並提供各式指標用以衡量行銷效果及資源，似有用於識詐宣導「循證治理」之潛力，有待政府進一步評估。

1、「打詐綱領1.5版」之識詐績效指標，主要為觸及人數及簡訊發送量，而在113年5月9日公布「『打詐綱領1.5』執行成效與策進」時，亦標榜112年

度分層分眾識詐宣導總觸及人數達3億3千萬人次等，在在顯示政府識詐宣導目前仍主要以數量作為績效指標。

2、行政院在112年8月10日召開會議(第15次會議)檢討識詐措施時，曾指示內政部「應思考認知率調查等驗證方式，更應歸納『未觸及』及『雖觸及惟未理解』之宣導受眾，精準投放渠等產業、族群宣導」等語；另查，在112年11月16日會議(第16次會議)亦曾決議「應確認受眾是否理解防詐宣導內容」；然而迄至113年6月為止，調查研究仍未發現政府在識詐宣導政策檢討或調整時導入認知率調查之明確事證，建議行政院應持續予以追蹤。

3、此外，識詐宣導應可視為某種數位行銷，在業界，數位行銷被視為一門學問，尚有各式績效評估指標，包括流量、曝光量、互動數、參與率等等不一而足，以評估行銷成本是否達成達成行銷目的，並評估行銷投資是否適當；若以公共行政角度則可視為「循證治理」[24]，爰此，識詐宣導似宜導入部分數位行銷之績效評估概念並予以分析，始能對於宣導方向、管道、素材、劇本、對象等進行精準調整。

(五)綜上，本調查研究顯示政府已挹注大量資源及人力，並極盡所能進行識詐宣導，此由前述每年每人觸及高達14次宣導並動員16部會可證，然由行政院112年8月以來多次會議決議，仍可發現政府對於目前宣導措施之侷限性已有所認知，本調查研究則認為可能

[24] 循證治理，指的是以資料、數據分析作為決策依據，而非個人主觀判斷或想法。(https://pa.ntu.edu.tw/News_Content_n_15075_s_233988.html)

原因有三，包括民眾過於自信、宣導邊際效用遞減，以及缺乏「循證治理」之績效指標等，建議政府納入「打詐綱領2.0」之考量，以有效提升識詐效能。

三、「堵詐」主要係減少民眾與詐騙集團接觸，並防堵資通訊服務淪為犯罪工具，然詐騙集團透過電信及網路所具備之大量、便捷及匿名化之特質廣泛接觸民眾並躲避查緝。英國2023年6月公布的反詐綱領已指出，期望大眾對詐欺始終保持高度警覺是不合理的，是以政府的源頭管理更形重要。經本調查研究盤點相關法制補強措施及政策發現，政府於防堵境外來電雖已略具成效，然竟發現有嫌犯可向電信公司申辦逾30萬筆門號情事，顯見電信門號KYC管理上仍有疏漏，而主責機關通傳會雖已發布施行「電信事業用戶號碼使用管理辦法」取代位階及拘束力較低之行政指導作為，然成效仍待觀察，政府允宜積極推動並依執行成效滾動式調整，以杜絕電信門號核配浮濫，此外建議111政府專屬簡訊碼之覆蓋率及黑莓卡之風險宜持續強化控管，以有效提升打詐綱領綜效。

(一)早期詐欺集團以金光黨等傳統詐欺手法與被害人面對面接觸施行詐術，100年間則透過當時流行通訊軟體MSN、即時通及傳送手機簡訊詐騙。伴隨資通訊科技蓬勃發展，近年詐騙集團藉網路資訊工具(如網路電話、通訊軟體、VPN、國際上網卡)來隱匿身分，以跨國通訊方式逃避國內警方查緝[25]；綱領並明確指出電信法規資安防護嚴謹度待加強，致歹徒利用電話、簡訊、社群平臺網站等資通工具詐騙財物：隨著電信網際網路科技迅速發展，犯嫌為躲避警方查緝，即藉由電信業者與簡訊代發商服務發送含惡意連結之釣魚簡訊、或於通訊軟體建立群組引導民眾至假投資網頁，致諸多被害人誤信匯款後血本無歸。為此，綱領訂定「每年攔阻簡訊3,000萬則」及

[25]「打詐綱領1.5版」關於堵詐面向，電信部分之說明。

「每年人頭門號停斷話5,000門」作為績效指標，並責成通傳會為本項目之主責機關，爰本調查研究依詐欺集團主要利用樣態，分為「詐騙集團利用KYC漏洞申辦大量門號」、「防堵境外來電」、「防堵詐騙集團批次發送簡訊」、「易付卡(含黑莓卡)」等項目，逐步檢視通傳會採取對策之適切性及其執行情形。

(二)有關「詐騙集團利用KYC漏洞申辦大量門號」部分。

1、過去在「電信法」施行期間，係將電信事業分為設置電信機線設備並提供電信服務的第一類電信事業，而其他非屬一類電信事業者，則稱為第二類電信事業；換言之，若未自行建置而租用第一類電信業者電信機線設備之電信業者，可泛稱第二類電信。

2、據通傳會說明[26]，我國於109年7月1日起開始施行「電信管理法」，針對電信事業之管理已由原電信法之特許、許可制改為登記制，未有登記者，僅係無法取得電信管理法所賦予之相關權利，以鼓勵事業參進。同時依該法之管理思維已無區分第一類電信事業與第二類電信事業。因此傳統上虛擬行動網路業者（Mobile Virtual Network Operator，下稱MVNO）是否屬電信事業，須視其是否具電信管理法第5條規定[27]應辦理登記之情形；若否，則視該虛擬行動網路服務業者是否自主依電信管理法辦理登記為電信事業而定。然而因電信管理法並未賦予已登記之行動網路業者（Mobile Network Operator，下稱MNO，即五家

[26] 通傳會於本院113年6月3日辦理座談提供書面資料。

[27] 提供電信服務，且有下列行為之一者，應向主管機關辦理電信事業之登記：一、與他電信事業進行互連協商或申請裁決。二、申請核配第五十六條規定以外之無線電頻率。三、申請核配設置公眾電信網路之識別碼或信號點碼。四、申請核配用戶號碼。

行動通信業務經營者)以外業者法定名稱，故五大電信以外之業者，包含門號代辦業等，在「電信法」於112年6月30日落日前，仍得以二類電信稱之，「電信法」落日後則以MVNO業者稱之，先予敘明。

3、經綜整機關查復及文獻盤點，詐欺犯罪無論是直接透過境內外電話及簡訊施行詐騙，或是利用門號作為網購認證或授權碼驗證之工具，均需取得足夠國內門號，而其取得國內電信門號之方式，並不分一類或二類電信，根據高檢署提供偵辦「羅○○案」及「海峽電信案」[28]資料顯示，兩案分別係涉嫌利用MNO之業者台灣之星股份有限公司(下稱台灣之星)及MVNO之業者海峽電信股份有限公司(下稱海峽電信)KYC管理漏洞取得大量門號遂行詐欺犯罪之案例，其中「羅○○案」涉及利用MNO業者未落實KYC之漏洞，竟能取得高達30萬筆門號。海峽電信案本身屬MVNO業者，竟涉嫌與詐騙集團合作向中華電信申請2,000多個門號，此有立法院司法及法制委員會於113年3月「詐欺犯罪防制立法及各部會打詐機制盤點」公聽會報告，台灣電信產業發展協會劉莉秋副秘書長所指：「很多的二類電信或者是特二類電信，在去(112)年6月30日之後就不受電信法的管轄，甚至於也逸脫於電信管理法的管理範圍」等語益證。

（1）在「羅○○案」中，MNO承辦人為詐騙集團申辦門號大開方便之門，以8家企業客戶名義前後申

[28] 讓台灣淪詐欺島！專賣門號給詐騙集團 海峽電信負責人被求重刑20年
https://news.ltn.com.tw/news/society/breakingnews/4419867

請約30萬筆門號，並自112年1月起，分成47次出口SIM卡到中國。

（2）在「海峽電信案」部分，桃園地檢署112年6月1日以桃秀河112他3808字第1129064373號函，指出海峽電信未落實用戶資料審核而大量核發門號，建請通傳會進行相關行政措施。

4、對於前述兩案所彰顯的問題，高檢署認為[29]在門號核配上，無論是對於企業(公司法人)或自然人都有管制失靈問題如下，原因不盡相同。經本調查研究分析，公司法人部分於制度面問題較大，而自然人部分則以內控缺失為主。

（1）企業客戶管制失靈原因，包括企業資格不設限、門號數量不設限、門號異常比例不設限。

（2）自然人客戶管制失靈原因，則包括未落實申辦人身分查核、未落實申辦資料稽核及未落實門號數量控管。

5、對於前述案件所顯露之問題，通傳會遂於112年6月16日依行政程序法第165條訂頒「電信事業受理申辦電信服務風險管理機制指引」，督導電信事業應強化各電信事業落實KYC機制。

6、在業者稽核處分部分，通傳會為督促電信事業加強落實我國電信門號之管理，自112年1月起截至113年4月，針對電信事業未落實身分查核案件，已就台灣之星、亞太電信及海峽電信等3家電信事業共計裁處20件，核處罰鍰金額共計2,625萬元如下表5。

[29] 高檢署112年11月13日簡報資料。

表5　電信事業未落實查核案件裁罰情形

單位:元

業者別	委員會議日期/次號	罰鍰金額	裁處件數
亞太電信股份有限公司	112年3月22日第1058次	450萬	3件
台灣之星	112年7月26日第1076次	100萬	1件
	112年8月2日第1077次	1,600萬	8件
海峽電信	112年7月26日第1076次	30萬	1件
	112年9月6日第1082次	445萬	7件
合計		2,625萬	20件

資料來源:通傳會於113年6月3日座談提供書面資料。

7、為確保MNO及MVNO業者遵循上開指引，通傳會自112年8月起每月定期至各電信事業營業門市及加盟店，就受理申辦電信號碼服務之作業情形進行稽查，並督促電信業者應落實用戶身分查核並加強管理，截至113年5月止，已稽核電信業者門市共337件。

8、通傳會進一步於**113年4月26日訂定「電信事業用戶號碼使用管理辦法」**，將前揭指引精神法制化，明確MNO業者及MVNO業者應遵循之用戶身分查核義務，以減少用戶號碼登錄之用戶資料與實際使用者不同產生之問題。然而前揭辦法施行未久，其成效亦視通傳會之執行力而定，爰仍有待後續追蹤。

(三)在攔阻防杜境外竄改來話詐騙部分，應屬目前為止在堵詐面向最成功的措施；基於境外門號浮濫無法透過境內KYC來控管，因此防制策略係以攔阻為主，按通傳會提供數據，**112年5月國際來話話務量達到5,080萬通之最高紀錄，然而經通傳會一連串措施，截至113年4月份已下降至899萬通，降幅高達82%**，如下圖2。

圖2　112年5月至113年4月國際來話話務量變化趨勢

資料來源：通傳會於113年6月3日座談提供書面資料。

(四)其中「+886」開頭國際來話話務量由最高112年5月份1,642萬通下降至113年4月份44萬通，其中攔阻+886偽冒來話數量約占+886總話務數5成，顯示前述措施已發揮相當成效如下圖3，詐騙集團已大幅減少利用國際來話管道進行詐騙。

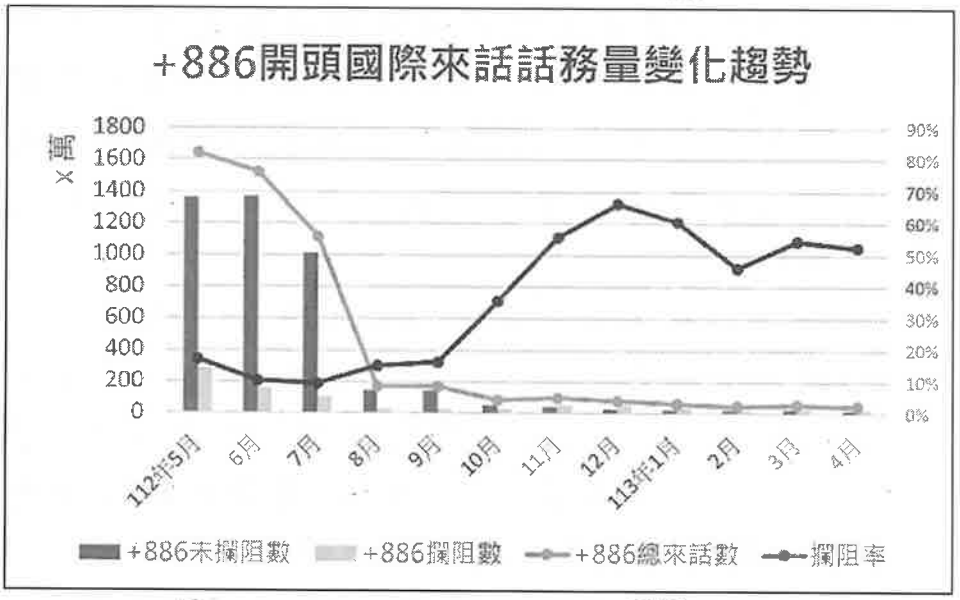

圖3　+886開頭國際來話話務量變化趨勢

資料來源：通傳會於113年6月3日座談提供書面資料。

(五)有關防制詐騙簡訊部分，除由通傳會與電信業者公私協力辦理詐欺簡訊攔阻之外，尚由數發部建立「111」政府專用簡訊號碼，以避免詐騙集團假冒政府服務遂行詐欺，金管會則主要針對OTP簡訊制定範本，由前揭三個部會通力進行。惟目前「111」政府專用簡訊號碼於政府機關之覆蓋率約為67%，換言之，民眾在面對部分機關使用111，部分機關未使用之情形下，仍難以判斷簡訊是否確由政府機關發送，故仍有強化空間，茲將三個主要負責機關之辦理情形說明如下：

1、數發部

（1）「111政府專屬短碼簡訊平臺」自112年9月28日上線試營運，截至112年11月22日已有14個機關透過111簡訊平臺發送逾146萬則簡訊。

（2）截至113年5月已有34個使用111政府簡訊平臺發送簡訊，達成率為67%；其他未使用之機關，主要原因是該機關與原簡訊發送商契約尚未結束之故，數發部後續將透過共同供應契約採購111簡訊，發送其業務訊息。

（3）國營事業及公法人部份，數發部已優先與台灣自來水股份有限公司、台灣電力股份有限公司及台北自來水事業處導入111發送簡訊，每月送簡訊量達60萬則以上。

（4）後續將與教育部、經濟部及財政部等目的事業主管機關合作，鼓勵國立學校與國營事業機構使用111簡訊。

2、通傳會

（1）通傳會督導業者建立惡意簡訊攔阻機制，包含關鍵字攔阻、大量發送檢核機制等措施，同時請業者加強查核簡訊來源。

（2）針對境內個人SMS詐騙案件，通傳會督導行動電信業者建立風險控管機制，如發送簡訊超過上限則暫時關閉發送簡訊功能等。

（3）針對境外SMS詐騙案件，通傳會督導行動電信業者建立惡意簡訊攔阻機制，包含關鍵字攔阻、防火牆大量簡訊偵測、攔阻偽冒「+886」開頭簡訊等。

（4）成效：112年攔阻801萬則簡訊、113年截至4月已攔阻302萬則簡訊。

3、金管會部分，已與金融機構完成研定OTP簡訊範本，簡訊文字應包括「簡訊目的」、「反詐宣導」及「法律責任」等。

(六)有關黑莓卡部分，基於黑莓卡屬於境外電信業務，通傳會雖稱已有通知境外電信公司停止異常門號服務等措施，但不易直接管控，而據臺北地檢署洪敏超檢察官於113年4月26日「劍青檢改」研討會上測試，其實名制設計顯係虛設，雲林地檢署黃薇潔檢察官更指出有部分黑莓卡不是從境外進入的，是臺灣的一些不法的業者在臺灣製作並且販售；在政府對境內MNO及MVNO業者逐漸強化管理強度、強力攔阻境外來電及「111」政府專屬簡訊等措施下，詐騙集團將極有可能轉向管制強度較低之黑莓卡，值得相關機關注意。

1、據通傳會查復資料說明，黑莓卡(含彼特卡)等係於網際網路販售通路之商品名稱，非屬我國電信事業所提供服務，其多為香港聯通[30]所批售之門號在臺灣提供無實名制之國際漫遊服務。其規管方式，目前僅得依GSMA國際漫遊合約第12條(詐

[30] CU HK，香港MVNO業者名稱

欺防止)及第14條(服務暫停)規定，通知他國電信事業配合終止該國外門號之漫遊服務；中華電信並於112年8月起至11月1日已通知香港聯通關閉25.5萬門SIM卡使用。通傳會認為，有關是否對於所有他國漫遊服務採取一致實名制做法，仍需就國際貿易協議(WTO)電信自由化宗旨及他國國民國際跨境個資傳送(如歐盟 GDPR)等議題，瞭解其他國家作法予以整體審慎思考。總而言之，目前通傳會對於黑莓卡之規管能力相當有限。

2、次由偵查實務角度看待黑莓卡，仍有明顯漏洞可鑽，以下臚列113年4月26日「劍青檢改」研討會中，檢察官所觀察到的實際情形，可見目前黑莓卡號稱實名制，卻沒有身分驗證，完全不具實名制功能；另外黑莓卡似有部分係國內製造，並非如同通傳會所稱多為境外流入，亦建議相關機關深入查緝。

(1) 臺北地檢署洪敏超檢察官：我測試給大家看，我花250元在蝦皮買的，實名制根本隨便輸入都可以過關。

(2) 雲林地檢署黃薇潔檢察官:這些黑莓卡都不是從境外進入的，是臺灣的一些不法的業者在臺灣製作並且販售……。

3、至於漫遊門號風險部分，本調查研究所蒐集之檢察官與通傳會說明之間有所出入，建議行政院透過平臺予以釐清，避免機關之間產生不必要之誤解。

(1) 根據113年4月26日「劍青檢改」研討會，有檢察官指出112年1至5月漫遊門號共開放875萬餘門，對照同期實際來臺旅遊人數217萬餘人，有650萬餘門漫遊門號用途不明，恐為詐騙集團所

用，以此推估全年高達1,500萬門漫遊門號。

（2）通傳會則說明，據該會瞭解，所謂「875萬餘門」實為國外門號連網次數，該數量包含同一門號跨月、因移動跨基地台註冊或跨我國不同電信業者網路漫遊之重複計算，以及機器設備所使用之「物聯網」通信次數，非全球來臺觀光旅客持有之漫遊門號數量。因此，該統計數據僅能做為參考，實無法貿然推定漫遊連網次數與來臺旅客之間的關係。

（七）在國內電信流反詐措施方面之小結：經調查研究評估「MNO及MVNO門號核配KYC」、「境外來電及簡訊」及「黑莓卡」等三項主要之堵詐電信風險，其中「MNO及MVNO門號核配KYC」部分過去有極大漏洞，而其規管措施甫上路，其成效尚未顯現；而「境外來電及簡訊」之績效相當卓著；惟111政府專屬簡訊覆蓋率有待持續提升。至於「黑莓卡」部分涉及國外電信事業，尚難由政府機關獨力完成規管，然本調查研究仍建議政府短期內查緝國內違法製造，中長期持續推動實名制之方向而予以防堵，避免再度提供詐騙集團可趁之機。

（八）在國際堵詐相關作法方面，本調查研究蒐集文獻指出，英國政府認為「期望大眾對詐欺始終保持高度警覺是不合理的」[31]，故英國強調「堵詐」之重要性遠勝「識詐」；且其在電信方面的行政措施較我國「打詐綱領1.5版」內容更為激進，包括全面禁止金

[31] Fraud Strategy: stopping scams and protecting the public。(https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public)

融商品推銷電話，以及禁用貓池[32](Modem pool)等等，我國是否有採用之可行性，有待相關機關予以評估。

1、**期望大眾對詐欺始終保持高度警覺是不合理的**，最好的防禦措施是詐騙集團對受害者造成傷害之前阻止犯罪企圖觸及個人和企業。

2、禁止對所有金融產品進行推銷電話，這樣詐欺其團就無法透過假投資欺騙人們。政府將把推銷電話禁令擴大到所有金融產品，……這意味著民眾將知道金融產品的推銷電話必為騙局，若接到此類電話就有信心直接掛斷。

3、禁止犯罪分子利用SIM卡農場（按：即Modem pool，貓池)一次發送數千條詐騙簡訊。

4、讓詐騙者更難「欺騙」英國號碼，使其看起來像是來自合法的英國企業，從而阻止更多詐騙電話。2023年5月生效的強化規則要求所有參與通信的電信網路在技術允許的範圍內辨識並阻擋詐欺來電。Ofcom 也對電信公司應根據其義務採取的措施提出明確的期望，以防止有效號碼被濫用，並期望這些公司建立防範濫用的標準作業程序。Ofcom 也在4月發動諮詢並考慮導入CLI(Calling Line Identification Presentation，發受信號碼顯示)身分驗證技術。

(九)綜上，針對電信部分，112年5月境外來電量高達5,000萬餘通，境內電信業者又陸續爆發業者不當核配大量門號之事件，甚有逾30萬筆門號者，且對

---

[32] 貓池是一種用於重新將傳統類比電信信號轉換為網路信號，並做資料交換和連接的網絡通信設備。此外，貓池還具有批量通話、群發短信、遠程控制、卡機分離等功能。不同型號的貓池設備上可插入8個、16個甚至更多SIM卡，可以批量自動收發手機驗證碼，……也可以同時發送上千條的詐騙簡訊，大大提升詐騙集團的詐騙效率。趨勢科技網站(https://www.nexone.io/zh-tw/card-list/sms-scam/what-is-modempool)

企業客戶幾乎毫不設防，綜合前述數據，無怪乎112年度詐騙案件突破歷史高峰至20,958件，年增率達33.1%，通傳會難辭其咎。惟經通傳會努力之下，境外來電至113年5月已驟減82%，該會已陸續頒布「電信事業受理申辦電信服務風險管理機制指引」，後續並於113年4月26日訂定「電信事業用戶號碼使用管理辦法」，將前述指引法制化，推測已相當程度打擊詐騙集團之通信能力，其成效則尚待113年度全年數據予以證實。爰此，政府有必要將可見之漏洞盡可能予以防堵；目前有賴行政院及相關部會強化者，包括「111」政府專屬簡訊之應用機關覆蓋度僅67%，民眾仍難分真偽之外，尚有黑莓卡實名制漏洞及國內違法製造等項目；按過去防制詐騙經驗說明，當政府針對詐騙集團主要工具予以強力管制後，詐騙集團仍能順應社會變遷並尋得其他漏洞加以利用，爰行政院、通傳會及數發部等相關機關亦應持續與第一線偵辦之檢警密切聯繫，於新型電信詐欺管道尚未氾濫前提出對策。

四、詐騙訊息在社群網站及通訊軟體極為泛濫，雖政府採取綠色通道等下架措施，除其能量在數位平臺巨量訊息中微不足道且緩不濟急外，並常於下架後又立即上架，引發國人對政府打詐作為強烈不滿；政府雖透過打詐專法推動平臺法律代表人制度，然其效果是否等同平臺落地，仍值觀察，至於國家資通安全研究院提出使用AI協助快速辨識詐騙廣告之技術提案，每月檢測量能高達50萬筆，是否可有效改善詐欺訊息氾濫情形，殊值政府評估是否導入。惟以長期而言，歐盟、英國等高度重視人權之國家，已陸續強化平臺治理、個資跨境傳輸並建立自律機制，我國數位平臺目前僅以特定議題分散式立法方式進行治理，除欠完整周密之通盤規劃外，並造成政府數位治理之困難。政府在平臺治理部分允宜考量國情進行縝密規劃，除搭配個資保護委員會之籌設外，並衡平言論自由及個資保護，以公開透明方式，積極與國人溝通以制定相關法制配套措施，強化平臺治理機制，並於平臺治理機制尚未完備前，宜針對數位平臺建立公正、透明、定期之評鑑機制，以揭露風險方式鼓勵平臺自律，抑制數位平臺上泛濫之詐騙訊息。

(一)網路逐漸取代電信作為詐騙集團接觸民眾之管道其來有自，本調查研究文獻[33]指出，我國2013年行動寬頻普及率僅57.08%，遠遠落後英美日韓等國家，但在2022年行動寬頻普及率已成長至118.69%，超過英國，此外我國上網率在全年齡層平均亦有84.67%，足證近10年我國行動寬頻及上網普及性快速成長，與電信網路詐欺之成長趨勢概同，或可部

[33] 通傳會。112年12月。112年通訊傳播市場報告。

分解釋近年電信網路詐欺暴增之客觀因素。此外本調查研究就國內外使用數位平臺情形進行分析，GASA於2023年報告[34]指出WhatsApp與Facebook是詐騙集團最喜歡使用的平臺，近年國際上更屢傳各國政府擬對Meta提告或裁罰之消息；而國內報告則指出民眾使用之社群平臺以Facebook為主（占47.27%）；而通訊軟體部分則以LINE為主（占77.56%），兩大平臺業者均大幅領先其他業者，綜合前述文獻結論顯示，Facebook在我國社群平臺市占最高又最為詐騙集團所慣用，復以我國數位治理法制落後先進國家，其風險不容忽視，本調查研究建議列為首要治理對象，而LINE屬性為即時通訊軟體，其通訊內容涉及隱私權，保護程度較高，惟詐騙集團亦利用此一特點遂行詐騙，本調查研究亦建議政府持續深化合作。

1、根據GASA於2023年報告，有44%受訪者指出，詐騙集團是透過WhatsApp與Facebook與其接觸，遙遙領先其他數位平臺，是詐騙者最常使用的平臺。其後則依序是Gmail(41%)、Instagram(22%)、Telegram(21%)，其餘平臺則均不到20%；值得一提的是，Facebook及Instagram母集團均為Meta。

2、根據通傳會「112年通訊傳播市場報告」：

（1）行動寬頻普及率於近10年快速成長，已於2016年超越英國，2022年普及率為118.69%。

（2）我國16歲以上民眾住處電話使用情形，「僅使用行動電話」者首次超越「市內電話、行動電話均有使用」者。

[34] GASA。2023。The Global State of Scams -2023。

3、根據財團法人台灣網路資訊中心「2023年台灣網路報告」

（1）2023年臺灣民眾的上網率[35]為84.67%，其中18至49歲上網率高於95%，行動寬頻用戶普及率為81.76%，可見民眾之上網(含行動上網)普及率極高。

（2）臺灣民眾最常使用的網路應用服務為「觀看免費的網路影音、直播或收聽音樂」，高達72.36%，其次為「買東西」達50.76%

（3）**近五成臺灣民眾最常使用的社群媒體仍是臉書（Facebook），達47.27%**，大幅領先其他社群媒體。年齡愈低則社群媒體使用率則越高。18至29歲年齡層為社群媒體使用率最高的族群，高達95.98%。而30至39歲年齡層的社群媒體使用率也在九成以上，達94.84%。

（4）調查結果顯示LINE是臺灣民眾最常使用的即時通訊軟體，占77.56%，大幅領先其他的即時通訊軟體。

4、根據本調查研究蒐整，各國政府擬對Meta提出各式調查、裁罰及告訴不勝枚舉，茲舉數例如下：

（1）2024年4月，日本民眾被詐騙廣告詐欺，提訴要求Meta賠償約2,300萬日圓[36]。

（2）美國各州敦促Meta打擊Facebook、Instagram假帳號行為[37]。

---

[35] 該報告中對於上網率(包括寬頻上網率、行動上網率)的計算，係將網路使用者的操作化定義為近三個月內有上網經驗之年滿18歲以上民眾。上網率則是指該調查的網路使用者占總樣本數的比例。

[36] 楊惟敬譯。2024年4月24日。日本民眾被詐騙廣告欺 提訴要求Meta賠償。中央社外電報導。https://www.cna.com.tw/news/aopl/202404250259.aspx

[37] Jonathan Stempel。2024年3月7日。Meta urged by US states to combat Facebook, Instagram account hijackings。路透社

（3）韓國公正交易委員會在去年（2023）底向Meta公司發出一份審查報告，內容主要集中在臉書（Facebook）、Instagram的消費者問題，恐涉違反當地的電子商務法[38]。

5、通傳會綜整透過網路管道詐騙之各式手法約可歸納為7類，包括假網拍詐騙、假投資詐騙、ATM解除分期付款詐騙、假愛情交友、猜猜我是誰、假冒機構(公務員)及假求職等，可見網路詐騙多以Facebook及LINE為主。

(二)我國對於堵詐面向中涉及網路部分之措施，現行已在運作之機制主要係由內政部對社群平臺及通訊軟體所執行之「綠色通道」或「紅色通道」，可下架詐欺廣告、封鎖詐欺帳號等，數發部除居間協調外，並可透過網域停止解析(DNS RPZ[39])攔阻惡意或不當的網域名稱，其目的均旨在阻斷詐騙集團與民眾在網路上之接觸；惟上述措施均在訊息鏈之末端實施，且其處理量能每月平均約為6,855則[40]，在巨量而快速之網路及社群媒體訊息中顯得微不足道且緩不濟急。為此，政府已規劃向更上游管理，包括透過113年7月12日立法院三讀通過之《詐欺犯罪危害防制條例》，要求平臺課以平臺業者更多責任，包括以數位平臺在臺灣之法律代表以及電子簽章為技術基礎之廣告實名制等措施，惟該等措施仍有其

---

[38] FB、IG詐騙太猖狂！「這一國」不忍了 放話要重鋼Meta。TVBS新聞網(https://tw.news.yahoo.com/fb-ig%E8%A9%90%E9%A8%99%E5%A4%AA%E7%8C%96%E7%8B%82-%E9%80%99-%E5%9C%8B-%E4%B8%8D%E5%BF%8D%E4%BA%86-093443856.html)

[39] 回應政策區域（Response Policy Zone, RPZ）是域名系統服務器提供的功能之一、也可以稱為「DNS防火牆」。因有越來越多惡意程式及殭屍網路利用DNS查詢C&C伺服器(Command and Control Server)，RPZ允許遞歸解析器(recursive resolver)以自定義的資訊修改解析的結果後，再回傳給DNS客戶端，藉由修改查詢結果的方式，以防止駭客攻擊、或避免使用者訪問惡意網站。(資料來源：TWNIC)

[40] 據警政署提供資料，112年7月1日至113年5月15日止，共計通報Meta公司限期改善處分54次、10萬9,672則，故以109672/16=6854.5(則/月)呈現。

侷限。

1、有關綠色通道及紅色通道等通報下架措施，警政署主要係依據「警察機關處理違反證券投資信託及顧問法第七十條之一案件統一裁罰基準及實施要點」執行；然而警政署也坦承，相關做法無法阻止平臺詐騙廣告再度上架，並且在行政程序之送達部分也有瑕疵，對平臺業者更是缺乏拘束力，數位平臺顯然成為堵詐措施中，尚無有效治理手段之領域。而有關Facebook上由名人本人檢舉偽冒投資詐欺廣告無效而遭人詬病一事，警政署則表示，若直接向Facebook檢舉，則透過臉書使用政策由Meta公司進行審核處置，建議民眾向警政署165網站檢舉，較能確保透過「綠色通道」予以下架。

（1）警政署於112年7月1日起即開始以「網路巡邏線上蒐報」方式執行蒐報工作，統計至113年5月15日止，共計通報Google公司限期改善處分57次、5,543則；通報Meta公司限期改善處分54次、10萬9,672則。上述通報，網路平臺業者均依限（24小時內）完成下架，故無裁罰之個案。

（2）有關詐欺集團冒用名人進行投資詐欺廣告部分，係依臉書使用政策，由Meta公司進行審核處置，此部分非經綠色通道處理。

（3）警政署建議，民眾如欲檢舉投資詐欺廣告，可向警政署165全民防騙官網/檢舉詐騙廣告專區提出檢舉，如民眾認為平臺資訊涉及詐欺等情，可輸入檢舉專區相關資訊，並檢附完整資料及說明爭點，經警政署審核後移請Meta公司複審下架。

（4）雖目前數位平臺業者均依限（24小時內）下架

警方所通報之涉詐廣告，惟相關處分均未合法送達，處分所載之期限均未起算，若業者拒不配合下架，縱超過處分所載之時效，亦無法依證券投資信託及顧問法(下稱投顧法)第113條之1裁罰業者，行政罰之規制效力大打折扣，更遑論發揮督促業者源頭自律之效果，故目前網路平臺業者僅被動接受警方通知配合下架，依前所述新法施行後警方已蒐報下架廣告超過10萬則，惟曾遭通報下架之詐騙廣告文案仍重複上架，多次聲明遭仿冒之名人，仍被利用為詐騙廣告之題材，數位平臺仍可見詐騙廣告充斥叢生。

（5）警政署指出，網路平臺業者均係跨國營運，於我國境內均未落地，難以要求境外業者遵循我國法律，警察機關於偵辦上更難調閱取得相關資料，致歹徒利用網路通訊犯罪時，形成偵查斷點，難以溯源。

（6）165全民防騙官網「檢舉詐騙廣告」專區，係因應金管會訂定投顧法第70之1條而增設，民眾提供內容如非投資詐騙廣告或本人臉書、粉專遭冒用情形，則非165專區得通報之範疇。

（7）至於「一頁式廣告詐騙」，其性質應屬網站而非廣告，且網站刊登內容通常涉及商標侵權或網路購物詐欺之態樣，與目前TWNIC授權警政署得通報網站停止解析之處理範圍（假投資、假冒政府機關、釣魚網站）不符，僅得以向法院聲請扣押裁定方式停止解析相關網域。

（8）另「假求職、真收簿」犯罪態樣多係以貼文方式為之，縱以廣告形式刊播，亦非投顧法之禁止範疇，目前警政署係自行蒐報，針對已有發

生被害案件之貼文，送請臉書公司依其社群使用守則移除。

2、本院於112年12月15日履勘LINE公司，該公司特針對「投資詐騙高風險商業帳號檢舉」下架聯防機制及「投資詐騙刑事案件通報」下架機制提出說明，顯示LINE在保障用戶隱私之虞，亦有因應相關機關需求建置封鎖下架機制。

（1）在「投資詐騙高風險商業帳號檢舉」下架聯防機制主要有三大部分，其機制圖如下圖4：主要特點為「超前部署」，在投資詐騙行為未發生前即封鎖投資廣告相關LINE 帳號；其次為「公私協力」，執法單位及LINE合作建立詐騙廣告聯防機制，共同打擊投資詐騙；最後是「權益保障」，兼顧保障一般使用者權益，於打擊投資詐騙及消費者權益保障間取得平衡。

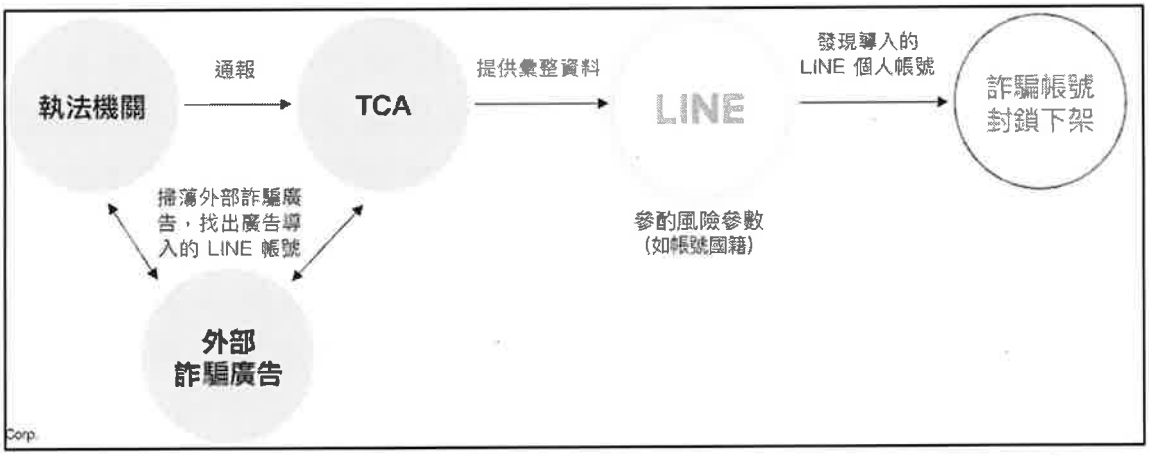

圖4　LINE公司投資詐騙高風險商業帳號檢舉下架聯防機制

資料來源:LINE公司

（2）「投資詐騙刑事案件通報」下架機制主要有兩大部分，其機制圖如下圖5，特點包括「公私協力」，結合CIB(警政署刑事警察局)及LINE資訊，針對投資詐騙涉案帳號聯防下架，避免損失擴

大；其次為「權益保障」，避免錯誤封鎖一般使用者帳號，平衡打擊投資詐騙及使用者權益保障之需求。

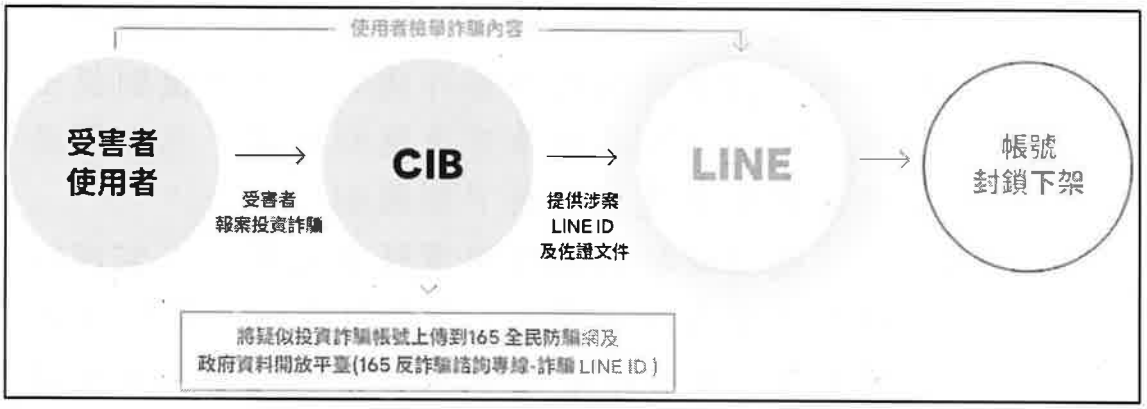

圖5　LINE公司投資詐騙刑事案件通報」下架機制

資料來源：LINE公司

3、就政府目前在數位平臺方面之打詐措施，由於Facebook或LINE每日之訊息、貼文或廣告數量查無公開資料，難以具體分析「綠色通道」或「紅色通道」對於降低民眾接觸詐騙訊息之效益，但根據通傳會「112年通訊傳播市場報告」，-民眾擁「有」社群媒體或即時通訊帳號者，自106年的83.6%逐年成長至112年的99.5%；且「2023年台灣網路報告」指出18至39歲民眾社群媒體使用率均在95%以上，故以警政署「綠色通道」每月透過網路巡邏或受理檢舉，向Facebook平均通報6,855則[41]而言，仍可推測其效益相當有限，復以下架之後仍無機制可阻止其再度上架，宛如「貓捉老鼠」，造成堵詐工作事倍功半，而在通訊軟體部分，LINE公司強調該公司主要屬於通訊軟體，與社群平臺網站多數訊息均屬公開之性質有異，調

[41] 據警政署提供資料，112年7月1日至113年5月15日止，共計通報Meta公司限期改善處分54次、10萬9,672則，故以109672/16=6854.5(則/月)呈現。

取資料方面涉及通信紀錄，故仍有資料保護強度相關考量。

4、為推動數位平臺更向上游之溯源治理，立法院113年7月12日三讀通過《詐欺犯罪危害防制條例》，其中第30條規定網路廣告平臺業者對其網路廣告服務，應以數位簽章、快速身分識別機制或其他安全性相當之技術或方式驗證委託刊播者及出資者之身分，以降低偽冒他人名義刊登或推播廣告之潛在風險。

（1）因各國間存在數位落差，對於數位簽章相關技術的發展情形不一致，為避免跨國驗證技術對接上的困境，爰《詐欺犯罪危害防制條例》第30條規定以數位簽章、快速身分識別機制或其他安全性相當之技術或方式，達到驗證委託刊播者及出資者身分之目的，並避免實務上執行之困難，有效降低偽冒他人名義刊登或推播廣告之潛在風險。

（2）為解決過去未落地之境外平臺無法納管問題，《詐欺犯罪危害防制條例》第29條規定，網路廣告平臺業者及其代表人於中華民國無營業所或住居所，且未設立分公司者，網路廣告平臺業者應以書面指定中華民國境內我國國民、依法登記之法人或設有代表人或管理人之非法人團體為其法律代表，並向數位經濟相關產業主管機關提報法律代表之姓名、名稱、住居所、事務所或營業所、電話及電子郵件信箱，以利文書送達及協助執行防詐措施法令遵循事項，並已研擬相關罰則。

（3）至於廣告在境外上架，所採取之防詐管理措施，如前所述，《詐欺犯罪危害防制條例》第30

條規定網路廣告平臺業者對其網路廣告服務，應以數位簽章、快速身分識別機制或其他安全性相當之技術或方式驗證委託刊播者及出資者之身分，以降低偽冒他人名義刊登或推播廣告之潛在風險。

5、至於數發部已協調TWNIC推動DNS RPZ 1.5透明度：為加速緊急案件處理，TWNIC DNS RPZ（Response Policy Zones）1.5自律機制，針對高檢署、警調機關、數發部數產署等單位認定「選舉期間執法機構緊急申請、重大金融犯罪緊急申請、假冒中央二級公務機關網站、詐騙網站(含電商聯防)」等4種重大案件緊急向TWNIC提出申請，可啟動該機制執行網域名稱限制接取，經統計TWNIC攔阻此類網域名稱之件數110年至111年計2,975件，112年至113年4月底計44,903件。惟數發部亦坦承，網路無國界，現行個人及組織在世界各地申請註冊網域名稱(網站)或經限制接取後更換網域名稱成本低廉，且有關詐騙網站於境外註冊域名，並無法斷源。總而言之，現況實難僅由國內單以DNS RPZ之技術手段達成遏止效果。

6、此外根據本院諮詢臺北地檢署姜長志檢察官指出，詐騙集團開始利用蘋果公司禮物卡，在偵辦時發現，檢察單位必須出具搜索票，蘋果公司才願意提供ID，且回復時間長達半年或一年，難以進行金流查扣等措施，本調查研究建議主管機關應加以重視處理，避免成為堵詐破口。

7、根據「資安院首度發表AI打詐技術，詐騙廣告偵測率超過九成」[42]報導顯示，數發部所屬國家資通

[42] iThome於112年6月20日報導。https://www.ithome.com.tw/news/163576

安全研究院已提出新的技術對策，其技術亮點在於不僅可以進行廣告自動化巡檢，每個月更可檢測超過50萬筆廣告，且準確度高達93%；純就處理量能而言，較目前警政署每月平均通報6,800餘件高出73.5倍，如實際應用時能發揮前述效能，將能大幅提升處理效率，值得政府重視並進一步評估導入；惟若提升通報量能後，平臺業者之下架速度是否能夠跟上，仍有一定挑戰。

（1）根據報導，資安院表示廣告自動化巡檢技術每個月可以檢測超過50萬筆廣告，一旦偵測到詐騙廣告，會進行後續通報。113年5月詐騙廣告數量超過20萬筆創下新高，資安院採用AI偵測詐騙廣告的準確度達93%，而在巡檢的過程中也發現97%詐騙廣告刊登不到兩天，顯示相關的阻擋機制必須跟時間賽跑，因為處理時機稍縱即逝。

（2）數發部則表示，該部刻正積極規劃「打詐通報查詢網」，預計三個月內正式上線，將可便利民眾通報並查詢各種可疑廣告資訊，也會顯示被檢舉詐騙廣告的處理進度。

（3）數發部林宜敬次長在報導中點出，平臺目前雖然也會下架詐騙廣告，但在速度上尚無法令人滿意；平臺雖然可以收到資安院提供的、每天5千至1萬筆的詐騙廣告清單，但因為下架作業仍未做到自動化，所以，平臺每日可以下架廣告的數量或許只有十分之一，顯然下架效率仍有提升的空間。

(三)承上，數發部、警政署及相關機關對於以數位平臺為管道之詐騙方式，相關行政管理手段已較過去遠為積極，惟需再次強調，該等治理措施及能量相較

於跨國平臺巨頭而言，打詐效益極為有限，又因目前分散式立法方式存在治理盲點，此由「假求職、真詐騙」廣告目前尚無妥善機制可予處置可證。是以本調查研究認為，政府之治理高度必須延伸至最源頭之數位平臺管理；由於此前通傳會推動「數位中介服務法」未形成社會共識而遭擱置，以致於目前我國仍缺乏較宏觀而完整之數位治理框架。

1、本調查研究以有關詐騙集團在網路上張貼「假求職、真收簿」貼文為例，說明目前在數位平臺治理之盲點。所謂「假求職、真詐騙」，依據本院諮詢學者專家表示，詐騙集團經常以張貼兼顧工作、育兒與家庭之工作誘使民眾加入LINE群組遂行詐騙(如下圖6)；然而該等廣告既不屬前述「投資詐欺」範疇，又非「兒少性剝削」內容，因此欠缺可將該廣告下架之依據；復經本院函詢相關部會，勞政主管機關勞動部認為未來「打詐專法」可以處理，警政署及數發部則認為貼文並非廣告，故難以運用網路巡邏加以查處或下架；換言之，目前「假求職、真詐騙」之詐騙類型係處於三不管地帶，遑論其他目的事業。此外，非屬投資詐欺性質之廣告或貼文縱經立法通過，其檢舉通報機制及部會分工模式亦尚未建立，更凸顯出我國目前在數位平臺方面採用分散式立法之弊病。

圖6　社群平臺「假求職、真詐騙」廣告範例

資料來源：本院自行蒐整[43]

2、有關最上游之數位平臺管理，通傳會曾於111年6月29日對外公布「數位中介服務法」草案，並辦理多場說明會，然而在平臺規模及涉及言論自由等爭議，欠缺社會共識，目前已暫時擱置，且無立法時程表，其推動概要及擱置原因經通傳會說明如下，顯示我國曾一度試圖以「數位中介服務法」推動數位平臺治理，卻因故擱置，導致目前仍缺乏較宏觀而完整之數位治理框架。

（1）通傳會說明，網際網路快速普及，民眾日常使用的數位中介服務，帶來生活便利的同時，也

[43] 光泉公司官網聲明：近期又有假冒光泉名義之臉書粉絲專頁，並引導民眾另加LINE好友，向民眾傳播不實招募徵才訊息，讓消費者混淆誤認。經過查證，皆屬詐騙集團冒用公司名義，進行不法行為。(https://www.kuangchuan.com/news/newsContent/2024042301)

引發新的風險與挑戰，國際上普遍認為連線服務與線上平臺服務提供者等數位中介服務，具備網路「守門人」(Gatekeeper)特性，認為應針對數位中介服務之行為加以規範，「平臺問責」(Platform Accountability)概念隨之誕生。因此，為保障數位基本人權，促進數位通訊傳播資訊自由流通與服務提供，落實數位中介服務提供者之問責與使用者權益維護，以建立自由、安全及可信賴的數位環境，爰擬具「數位中介服務法」草案。

（2）整體而言，「數位中介服務法」草案與歐盟「數位服務法」所規範對象皆為「網路中介服務業者」，包括連線服務、快速存取服務、資訊儲存服務等，同時也納入問責概念，對於所規範對象，依據類型不同而課予不同義務，例如資訊揭露、透明度報告等，希望能夠降低網路風險，達到安全可信賴的網際網路環境。

（3）網際網路治理不同於傳統廣電之高權監理模式，須仰賴多方利害關係人參與溝通，尋求各級行政機關、網際網路服務提供者、公民團體、學者專家及使用者等多方共識方能奏效，爰網路治理非以監督管理，而是以共同建立治理框架較為妥適。

（4）通傳會於111年6月29日對外公布「數位中介服務法」草案，賡續辦理三場分眾公開說明會，邀集中介服務提供者、公民團體與學者專家等利害關係人與會表達意見，然該草案受外界解讀為涉及影響言論自由的基本權益之爭議，引發諸多批評。未來通傳會將審慎研議與評估，持續觀察產業趨勢及社會脈動，並納入多方利

害關係人意見，以尋求整體社會共識，目前暫無立法時程表。

(四)基於我國目前仍欠缺數位平臺治理之框架性法制，本調查研究特針對國外對於數位平臺治理之看法，並進一步以文獻探討及赴英交流方式，分析歐盟及英國在數位平臺治理方面之法制結構，本調查研究認為，先進國家非常重視數位平臺治理在「堵詐」面之價值，甚至融合「識詐」之功能。整體而言，數位平臺治理不僅是民主國家趨勢，更應視之為平臺業者之社會責任；而其法制是否得以衡平治理需求及言論自由疑慮，其關鍵並不在監理或裁罰強度等高權介入，而是以平臺自律為主，他律制度為輔，並且主責他律之機構必須具備充分之獨立性及社會信任，同時必須有多種法制配套形成複式的治理環境。誠然，無論是歐盟「數位服務法」(DSA) 及其配套之「數位市場法」(DMA)、「人工智慧法」(EU AI Act)及「一般資料保護規則」(GDPR)，以及英國「線上安全法」(Online Safety Act) 等均施行未久，其價值以及潛在爭議尚未完全浮現，仍有待先進國家持續探索；然而，我國在行動寬頻普及率已於2016年超越英國，但數位治理之完整性及法制配套反而遠遠不及，再次證實政府之法制、政策及相關配套長期以來並未跟進數位時代之進程，實有積極凝聚社會共識並建構治理環境之必要。

1、GASA 2022年報告強調需要針對被用於宣傳詐騙之平臺（包括大型搜尋引擎和社交媒體）以及促進其基礎設施的平臺（包括註冊商、註冊管理機構和託管提供者）承擔更多責任。例如，澳洲競爭與消費者委員會已對Meta提起法律行動，指控其在Facebook上發布詐騙名人加密廣告。

2、英國政府亦將包含平臺治理之源頭阻詐（Block fraud）視為組成打詐策略的「三本柱」(Pursue fraudsters、Block fraud、Empower people)之一，其重點如下

（1）期望大眾對詐欺始終保持高度警覺是不合理的，最好的防禦措施是詐騙集團對受害者造成傷害之前阻止犯罪企圖觸及個人和企業。

（2）線上科技巨頭應該採取更多措施阻止詐欺犯罪利用其服務，並且不應從網路犯罪中獲利。

（3）政府將使數位平臺企業為客戶提供額外保護，並對那些不遵守網路安全規定的人實施嚴厲處罰。

（4）政府將確保大型科技公司讓用戶能夠盡可能簡單地通報其平臺上的詐欺行為。

（5）政府將公布哪些平臺最安全，確保企業得有適當的誘因來打擊詐欺。

3、本院透過文獻探討及參加2024台灣-英國『傳播媒體與新聞產製』雙邊交流」，對於先進國家之數位治理生態進行更深入的了解並比較，研究結果顯示，數位平臺治理之建立，至少必須探討「分層治理」、「權力分立」、「平臺落地」、「賦予業者義務」、「建立內容審查標準」、「業者端內容審查機制」、「主管機關職責」、「政府可採取之通知及手段」以及「裁罰額度」等面向，其比較分析如下表6。

表6　歐盟及英國數位治理相關法令分析

面向/法令	歐盟/DSA(Digital Services Act)	英國/Online Safety Act
分類/分層治理	● 託管服務：分四級，用戶數量越多，治理強度越強。 ● 連線服務 ● 快速存取服務	● 依據用戶數量、服務性質及國務大臣認定，分為3類 ● 用戶對用戶：第1類(如社群平臺) ● 搜尋服務：第2A類 ● 用戶對用戶：第2B類(社群平臺以外)
權力分立	● 委員會執行/議會監督/法院救濟	● DCMS立法/Ofcom獨立機關執行/法院救濟
落地	● 要求落地	● 要求落地
賦予業者義務	● 建立風險評估、內容審查、救濟措施等機制。 ● 建立與政府之聯繫管道。 ● 向執法機構通報涉嫌違法內容。 ● 出具透明度報告 ● 簽署行為守則(含KPI以檢驗成效) ● VLOPs接受獨立審計、繳交監管費、對協調員開放內部數據	● 進行適當且充分的非法內容風險評估 ● 有關非法內容和優先非法內容的責任 ● 透明度、報告和補救的職責 ● 保護言論自由(第1類業者另有額外義務)
內容審查標準	● 由其他法律界定(實體世界違法事項在網路上同樣違法)。	● 違法內容:再細分為「優先處理」(明文條列)、「其他違法內容」。 ● 對兒童有害內容:再細分為首要關注、優先關注、非指定有害等三類。
業者端內容管理機制	● 共計有「通知與回應機制」、「回報可疑犯罪行為」、「認證舉報者」、「風險評估」、「降低危害風險」、「危機處理機制」、「違法商品告知」等機制。 ● 業者級別越高，需建置越多機制。 ● 平臺受理審查來源包括認證舉報者、大眾告知、自主調查及政府通知等(不同級別略有差異)。	● 共計有「違法內容風險評估」、「降低和管理違法內容危害風險」、「保障用戶隱私及言論自由」、「通知機制」、「紀錄與檢閱」、「兒童造訪評估」、「向執法機關報告CSEA(兒童性剝削/虐待)報告」等機制。 ● 不同類別業者需建置之機制略有差異。

面向/法令	歐盟/DSA(Digital Services Act)	英國/Online Safety Act
主管機關職責	● 要求平臺處理違法內容：由各國協調員通報平臺處理，需提出證據及理由。 ● 受理平臺處理違法內容之結果報告。 ● 執法機關受理平臺報告之涉嫌違法內容。 ● 協助業者建置各種自律機制。 ● 發布報告，對大眾揭露各平臺風險。	● 違法內容出現前。 ● 訂定各類業者的業務守則/方針。 ● 審查業者的風險評估或透明度報告。 ● 違法內容出現後(不直接干預內容審查)。 ● 監督平臺有無按照機制執行。 ● 發現平臺審查技術問題並予以輔導。
政府可採取之通知及手段	● 平時。 ● 執委會對VLOPs有獨立監督權。 ● 針對「公安」、「公衛」重大威脅，要求平臺採取緊急措施。 ● 業者未盡職責時。 ● 受影響國家可向平臺所在國家之協調員(機構)要求展開調查。 ● 執委會展開調查，要求業者回應，發動訴訟，按DSA予以裁罰。 ● 若認定業者遲不改進，各國協調員有權限制部分接取服務，如無法部分限制，則可能全部限制(原則時限為4週，可依法延長)。	● 通知 ● 技術警告通知(針對恐怖主義及CSEA) ● 技術通知 ● 臨時執法通知 ● 裁定結果 ● 裁罰通知 ● 向法院聲請 ● 服務限制令 ● 暫時服務限制令 ● 接取限制令 ● 暫時接取限制令
最高罰款(NTD)	● 全球營收6%。	● 7億或全球營收10%，另有刑責。

註：本表綜整自以下文獻

- 台灣媒體觀察教育基金會(2023)：「歐洲『網路戒嚴』來臨？數位服務法發威，歐洲會更民主嗎？」(https://vocus.cc/article/6502d286fd89780001f4f530)
- 英國成文法資料庫。(2023)https://www.legislation.gov.uk/ukpga/2023/50/enacted
- 陳寧(2023)，線上平臺與內容之治理—以歐盟《數位服務法》與英國《線上安全法》草案為例。臺灣大學新聞所碩士論文。
- 歐盟官方網站。https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package。

（1）英國在2023年10月通過了「線上安全法」(OnlineSafety Act)，該法是源於「Molly Russell案」而立法，其治理概念與歐盟「數位服務法」(Digital Services Act，2024年2月施行)、加拿大「網路傷害法」(Online Harms Act，正在立法程序)類似，顯示數位治理是國際趨勢，而且治理架構，包括他律、自律、平臺分級、透明化、司法救濟等等，求同存異的程度相當高，都在賦予數位平臺更多的自律機制外，同時強化他律手段，意即賦予主管機關更多的職權並兼顧言論自由，雖然這幾個國家的法律都施行不久，還沒有具體的成功或爭議案件(例如平臺不服處分而尋求司法救濟)據以檢討或修正，但仍可做為我國尚顯貧弱的數位治理規管參考。

（2）「線上安全法」(Online Safety Act)是由英國的DCMS(相當於數發部)所推動立法，但執行單位是Ofcom(相當於通傳會)，相較於我國目前在數位治理層面係由數發部或通傳會主政未有定論，英國的分工情形及其優劣，值得我國進一步加以探討；此外，若以歐盟為例，其數位治理之法制結構並非企圖以「數位服務法」(DSA)作為全方位解決方案來解決數位平臺的所有問題，而是必須搭配「數位市場法」(DMA)、「人工智慧法」(EU AI Act)及「一般資料保護規則」(GDPR)等，以形成複式的規管環境，亦可做為我國陸續修訂「資通安全管理法」及「個人資料保護法」及本院後續監督政府在相關領域執法情形之借鑑。

（3）不分民主及威權國家，數位治理已成為顯學，

相關制度也逐漸完備，我國在這部分似乎因為社會共識和言論自由方面的挑戰尚未跟上國際趨勢。

（4）根據卓越新聞獎基金會轉載牛津大學2023年公布的【2023年度數位新聞產業報告】內容顯示，臺灣民眾對於媒體的整體信任度為調查國家中的後段班（第41名），僅有28%；而被認為可相信媒體則包含：公視、商業周刊、天下雜誌、TVBS與經濟日報等，顯示我國的媒體信賴程度還有許多挑戰有待克服。

(五)至於「數位中介服務法」未形成社會共識而遭擱置之原因，本調查研究經諮詢專家學者認為，通傳會當時提出草案確實未臻周全，包括過度規管小型平臺、高權過度介入等等，結果不僅導致數位治理法制遭擱置，無法建構數位治理環境，也扼殺近年對於數位治理之討論空間，對於堵詐而言更是平添犯罪機會。對此，政府目前雖已統由行政院協調通傳會及數發部辦理數位平臺治理事宜，並逐步要求平臺落地等措施，然本調查研究仍建議，行政院應通盤考量「AI基本法」、「GDPR適足性認定」等法制配套，對於數位治理之法制框架持續討論、以實際行動建立社會信任並凝聚社會共識，俾補強我國在數位治理方面之整體框架。

1、本調查研究經諮詢專家學者看法如下，足證通傳會當時提出「數位中介服務法」草案有欠周全；至於未來推動方向，本調查研究建議政府宜深入研究英國及歐盟法制之設計方式，觀察各國制度近年執行情形及其利弊，並以建立初步寬鬆治理雛型為目標，無須陳義過高。

（1）臺灣對數位平臺的治理，目前其實是沒有法

律。歐盟跟英國做的比較成熟就是他們有數位服務法，可以管網路的內容包括詐騙、霸凌、恐怖主義、仇恨語言或者是假訊息，至少政府可以跟平臺去協商，或者要求平臺採取有效措施。

（2）數位中介服務法如果好好的抄歐盟數位服務法，不會有那麼大問題，……例如超大型平臺的分層定義，通傳會直接抄到臺灣，就變成200萬用戶的平臺就要嚴格監管，……那真正的超大型平臺如Meta跟Google都不用出來反對，網民和各種小平臺就先跳出來了。

（3）當時草案在法律的一致性跟應該要配套的部分沒有考慮清楚。……已經扼殺了我們好好去討論數位內容要怎麼樣去建立治理的機會，但政府有責任去重啟有關數位治理法制的討論。其他國家都已經有這個法律。其實我們就是好好把它研究清楚，然後該學的地方就直接學，不應該直接學的部分做一點調整。

2、數發部則說明現行之數位平臺治理屬於重大政策，行政院也會持續關注，而個人資料保護委員會也以因應111年憲判字第13號判決而成立籌備處，將在114年內建立個人資料保護之獨立監督機制分工機制，此外，通傳會亦有相關之組織編制調整，顯見政府仍在持續跟進數位平臺治理，然而短期內尚無法如同英國或歐盟建立完整架構，有賴政府持續積極推動，俾使堵詐措施獲得實質之源頭管理。

（1）數發部說明，亞洲國家如日本與韓國，都已陸續設置個資保護獨立監督機關，因此，我國於112年12月5日設置「個人資料保護委員會籌備

處」,期能整合各部會力量全力維護民眾個資權益 奠定我國個資保護重要里程碑,以完備憲法第22條對人民「資訊隱私權」的保障，展現政府對國人資訊隱私權的重視。

（2）有關網路平臺治理分工或TikTok平臺治理，係屬重大政策，也涉及適法性與可行性等影響因素評估，行政院所屬相關部會將持續關注美國國會立法進度，並參與行政院跨部會會議，由行政院綜合考量各界意見決定。

（3）而因應網際網路治理新趨勢，通傳會也於111年將「基礎設施與資通安全處」及「射頻與資源管理處」二處之業務項目合併設置「基礎設施處」，進而增設「網際網路傳播治理處」，其負責網際網路傳播相關業務，因目前該會組織法仍在審核中，通傳會目前以「網際網路傳播辦公室」運作，最後由行政院統籌規劃研訂分工與治理策略。

3、最後，數位治理由於涉及之目的事業、樣態及技術極為繁複，對於跨部門協作之要求極高，而我國目前行政院層級無論是何種辦公室或會報，大多數仍由現職人員以任務編組方式兼職辦理，此與英國目前以實際編制機關DRCF(數位監理合作論壇，Digital Regulation Cooperation Forum)之運作方式大相逕庭，至於我國在數位治理方面有無必要參考英國運作模式，以及是否得以因應數位治理需求，仍有待政府進一步評估。

（1）本院諮詢國立中正大學傳播學系羅世宏教授表示，英國的一個跨部會的數位治理的機制叫做DRCF，即Digital Regulation Cooperation Forum 數位監理合作論壇，它是實際的組織，

有行政運作的的人力，然後有專門的執行長，DRCF的執行長需要定期的去對外報告，報告說DRCF幫英國預防處理解決了什麼樣的數位問題。

（2）DRCF有四個固定一定要參加的機構，一個就是Ofcom，也就是臺灣的NCC通傳會，一個就是他們的資訊辦公室（Information Commissioner's Office, ICO），大概是臺灣的數位部數發部這樣的一個性質，第三個是這個金管會（Financial Services Authority, FCA），第四個是英國的公平會（競爭與市場管理局，Competition and Markets Authority, CMA）。

（六）綜上，在堵詐面於網路及數位平臺部分，內政部及數發部等機關之措施如「綠色通道」等，已遠較過去為積極，然而在打詐或其他更廣泛的治理需求層面，我國目前之數位平臺治理仍有加以強化之必要，本調查研究歸納之理由包括：1.民主先進國家亦普遍推動數位平臺治理法制。2.我國行動寬頻上網普及率較英國為高，但治理及規管強度反而較低。3.目前規管方式在打詐方面效益不足等因。考量我國國情確實較易觸及言論自由等疑慮，過度介入監理更不符合人權之普世價值及潮流。爰此，政府允宜參考英國打詐綱領，與具公信力之第三方機構合作，研擬涵括平臺法遵配合度、自律政策嚴謹程度及其執行力、通報檢舉之處置積極程度等指標，辦理公正、公開且定期之評鑑，以揭露風險之方式鼓勵平臺自律，以作為中短期內數位治理法案未獲社會共識之暫時性替代方案，避免各堵詐主責機關持續以事倍功半之方式辦理數位治理事務。

五、詐騙集團詐騙國人之目的不外乎取得金錢，故金流管制及洗錢防制措施實屬打詐政策之核心。本調查研究經盤點政府在金流方面之行政管制措施，在臨櫃阻詐及強化法幣實體帳戶KYC方面略具成效，惟第三方支付方面數發部雖已提出能量登錄制度，然成效仍待觀察。另人頭帳戶及警示帳戶數量仍未有效降低部分，將成為整體政府打詐措施中最薄弱之一環，政府除公布各金融機構人頭帳戶及警示帳戶之情形，並對金融機構管理不力予以課責外，允宜秉持行政先行及公開透明原則，優先檢討打詐不力之金融機構，以避免成為打詐及洗錢防制之破口。

(一)刑法上詐欺罪的定義是犯罪者對他人施以詐術，造成被害人財產上損害。而構成詐欺罪之要件為：行為人有主觀的不法意圖、行為人有主觀的心態故意、行為人傳遞不實資訊（詐術）、被害人誤信不實資訊處分財產、取得財產和損失財產間有關聯。是以，詐欺集團詐騙國人之目的主要係詐取財產與金錢。阻斷詐騙案件之金流及避免詐騙資金經由洗錢管道將資金洗白，實屬政府打詐政策之核心。

(二)查詐騙集團採行層級管理、分工細密，組織結構完整，大致可分為首腦核心、前置作業 、國外作業、電話作業及金流作業等五大類。其中金流作業包括車手集團、人頭帳戶管道、洗錢機房、地下匯兌等，主要負責取款、轉帳及交付詐騙款項。金流工作流程主要為：電信機房詐騙所得金額全數匯到洗錢機房帳戶（金額最多），並由電話組向洗錢機房回報結清帳款，再由洗錢機房分帳到小車（小帳戶提款卡），車手提款後由車手頭收款繳交公司帳房，帳房清算盈利核對報表後再分錢給合作客戶。依據前開

作業流程涉及之金融機構人頭帳戶、警示帳戶[44]、第三方支付之虛擬帳戶及虛擬通貨(詳結論與建議六)等隱匿贓款流向，設立偵查斷點。政府為有效阻詐，透過金融機構與客戶建立業務關係，及辦理一定金額交易時（單筆達50萬元以上）將進行臨櫃關懷，確認客戶身分，並瞭解辦理該筆金流之目的及性質，審視其合理性，如未發現明顯異常，櫃員才可執行帳務交易，經統計111年金融機構共協助民眾攔阻詐騙件數7,979件，攔阻金額42.41億元。112年攔阻詐騙件數更增加為11,300件，攔阻金額提升至75.89億元，避免國人遭詐騙金額較前一年度增加33.48億元、攔阻件數則增加為3,321件。今年(113年)第1季攔阻詐騙件數2,425件，金額15.4億元，近兩年已攔阻超過百億元，金管會稱「金融機構臨櫃關懷客戶攔阻成效顯著」。惟從人頭帳戶增減情形分析，金融機構警示帳戶總數顯示，109年第2季31,735戶，至112年第2季已成長至103,767戶，3年間成長3.27倍[45]。金管會為有效阻詐，以避免成為人頭帳戶詐欺集團之詐騙工具，研提下列強化金融機構帳戶管理措施：

1、為強化金融機構對於確認客戶身分之作業程序，以防杜偽冒開戶及盜領存款致客戶財務損失等情事，修正「防杜人頭帳戶範本」:

（1）臨櫃面(臨櫃應注意事項):增列屬非正職職業類別、共用通訊資料、忽然提高轉帳限額、欲辦理變更負責人，新負責人對於公司營運狀況不清楚或無法正確回答等宜注意事項。

---

[44] 警示帳戶：指法院、檢察署或司法警察機關為偵辦刑事案件需要，通報銀行將存款帳戶列為警示者。

[45] 高檢署112年11月13日簡報

（2）資訊面：客戶申請約定轉入帳戶者，視客戶性質及風險程度高低，評估是否拉長申請審核期間為次二日生效。

（3）教育宣導面：請金融機構於提供客戶之存摺加註相關警語，提醒客戶提供帳戶供非法使用，可能招致各項信用損失。

（4）金融機構接獲司法檢警等執法單位之警示通報，係以公文或警示帳戶簡便式表通知，茲因通報機關未提供詐騙案件類型，故金融機構尚無電信網路詐騙案件警示帳戶相關統計資料。

2、有關對水房以短時多筆分帳之因應措施則包括「可將疑涉詐騙帳戶列為警示」、「建立相關異常交易態樣」及「交易監控」。

（1）「可將疑涉詐騙帳戶列為警示」部分係依法院、檢察署或司法警察機關以公文書通知銀行可將存款帳戶列為警示，金融機構接獲通知後會依「存款帳戶及其疑似不法或顯屬異常交易管理辦法」之規定暫停該帳戶全部交易功能。

（2）建立相關異常交易態樣：所謂異常交易態樣，依據「存款帳戶及其疑似不法或顯屬異常交易管理辦法」中第二類帳戶[46]態樣及「彙整銀行間具共通性之疑似不法或顯屬異常交易態樣」，包括「存款帳戶餘額低，頻繁查詢餘額，有款項入帳隨即領現或轉出」、「短期間內頻繁使用自動化設備交易，且借方總額與貸方總額差額小，

[46] 第二類帳戶：（一）短期間內頻繁申請開立存款帳戶，且無法提出合理說明者。（二）客戶申請之交易功能與其年齡或背景顯不相當者。（三）客戶提供之聯絡資料均無法以合理之方式查證者。（四）存款帳戶經金融機構或民眾通知，疑為犯罪行為人使用者。（五）存款帳戶內常有多筆小額轉出入交易，近似測試行為者。（六）短期間內密集使用銀行之電子服務或設備，與客戶日常交易習慣明顯不符者。（七）存款帳戶久未往來，突有異常交易者。（八）符合銀行防制洗錢注意事項範本所列疑似洗錢表徵之交易者。（九）其他經主管機關或銀行認定為疑似不法或顯屬異常交易之存款帳戶。

僅留下象徵性餘額者」等異常交易態樣。

（3）依第二類帳戶及異常交易態樣進行交易監控：實務上金融機構係依「存款帳戶及其疑似不法或顯屬異常交易管理辦法」中屬於第二類之帳戶及「彙整銀行間具共通性之疑似不法或顯屬異常交易態樣」進行存款帳戶交易監控；經審查如有疑似不法或異常之情事者，除進行存款交易管控外(例:限制自動化交易、交易額度調整等)，並依洗錢防制法等相關法令規定進行相關處理措施。

(三)金管會雖稱在督促銀行強化各項風控機制後，警示帳戶數成長率已趨緩，由110年59%下降至113年第1季31%。惟113年第1季之警示帳戶仍較112年底增加近8,000戶，整體警示帳戶數量仍呈現持續增加之情形。建議政府除應持續研擬相關控管措施以杜絕人頭帳戶外，並評估定期公布各金融機構之警示帳戶數量，以供大眾檢視，藉以強化金融機構源頭控管人頭帳戶。並對金融機構管理不力予以課責外，並應秉持行政先行及公開透明原則優先檢討打詐不力之金融機構，以避免成為打詐及洗錢防制之破口。此外，金融機構防制人頭帳戶目前主要均係針對個人戶，然大量歇業的企業戶，已逐漸成為詐欺集團鎖定之目標，建議政府亦應檢視該等公司存款帳戶成為人頭帳戶之趨勢，評估研擬相關控管機制。

1、按照金管會說明，依「存款帳戶及其疑似不法或顯屬異常交易管理辦法」(下稱疑似不法管理辦法)第3條及第5條規定，銀行係配合法院、檢察署或司法警察機關之通知，將存款帳戶列為警示帳戶；換言之，警示帳戶數量雖未必全數等同人頭

帳戶數量，但人頭帳戶用於詐騙後，經司法警察機關通知而成為警示帳戶，爰警示帳戶數量對於政府及金融機構管控人頭帳戶之良窳，仍具有指標意義，甚至尚不能完全反映人頭帳戶之猖獗程度。

2、茲將金管會提供之各金融機構111年迄今警示帳戶數量統計表臚陳如下表7，內容顯示部分行庫警示帳戶數量明顯偏多。對此，銀行局侯立洋主任秘書於本院113年6月3日辦理座談時表示：「警示帳戶每一季有公布總數，至於個別金融機構，金管會去年有公布1次前10大，銀行局也特別針對所謂前10大、警示帳戶比較多的金融機構，特別找他們過去，要求他們改善，事實上像剛剛提到中信本身也因為這樣，有去設計預防機制，我們發現自從他做了機制後，他的成長率是相對說是比較低的。雖然說他總數來講比較高，可是他的成長率是有下降的」等語，金管會並補充警示機制及趨勢如下。

表7　各金融機構111年迄今警示帳戶數量

單位:帳戶數

金融機構	111年Q1	111年Q2	111年Q3	111年Q4	112年Q1	112年Q2	112年Q3	112年Q4	113年Q1
中○郵政	14,969	16,127	16,253	17,058	17,862	19,511	21,371	23,799	26,379
臺○銀行	2,392	2,621	2,758	2,907	2,997	3,282	3,531	3,793	4,093
臺灣土○銀行	1,710	1,905	1,996	2,201	2,346	2,633	2,851	3,151	3,351
合○金庫商業銀行	3,420	3,755	3,952	4,211	4,417	4,916	5,495	6,115	6,639
第○銀行	3,114	3,570	3,847	4,308	4,648	5,198	5,664	6,191	6,728
華○銀行	2,582	2,922	3,148	3,475	3,672	4,140	4,539	5,012	5,442

金融機構	111 年 Q1	111 年 Q2	111 年 Q3	111 年 Q4	112 年 Q1	112 年 Q2	112 年 Q3	112 年 Q4	113 年 Q1
彰○銀行	2,275	2,447	2,644	2,888	3,130	3,434	3,760	4,100	4,441
上○商業儲蓄銀行	521	551	557	595	605	668	735	766	796
台北富○銀行	1,629	1,787	1,835	1,919	2,120	2,306	2,485	2,726	2,931
國○世華銀行	5,032	5,494	5,823	6,171	6,368	6,728	6,809	7,004	7,335
中○輸出入銀行	-	-	-	-	-	-	-	-	-
高○銀行	206	236	259	284	298	333	345	378	410
兆○國際商銀	1,078	1,184	1,270	1,450	1,644	1,866	2,058	2,312	2,680
花○（台灣）銀行	76	75	79	83	82	82	82	63	53
王○銀行	244	270	284	293	301	333	384	497	566
臺○企銀	1,398	1,495	1,554	1,722	1,867	2,084	2,365	2,706	3,075
渣○國際商業銀行	740	755	766	781	764	775	782	804	863
台○商銀	666	742	796	863	924	1,032	1,157	1,295	1,427
京○商業銀行	269	285	298	314	342	404	445	469	508
匯○（台灣）商業銀行	19	24	26	34	46	61	84	98	123
瑞○商銀	25	27	28	28	26	27	27	32	34
華○銀行	79	89	86	100	104	108	122	126	131
臺灣新○商業銀行	931	1,007	1,042	1,141	1,190	1,316	1,413	1,534	1,583
陽○銀行	319	349	366	389	419	491	514	559	590
板○銀行	173	184	182	188	188	194	205	211	221
三○銀行	85	88	98	102	109	134	163	190	210
聯○銀行	832	913	951	993	1,041	1,144	1,237	1,328	1,459
遠○銀行	430	458	464	510	512	559	592	643	716

金融機構	111年Q1	111年Q2	111年Q3	111年Q4	112年Q1	112年Q2	112年Q3	112年Q4	113年Q1
元○銀行	839	936	1,022	1,110	1,200	1,355	1,465	1,610	1,748
永○銀行	1,725	1,929	2,131	2,336	2,456	2,735	2,868	3,026	3,132
玉○銀行	3,897	4,238	4,365	4,745	5,065	5,467	5,687	5,874	6,103
凱○銀行	260	307	333	381	417	456	506	540	589
星○（台灣）銀行	36	40	39	45	46	55	74	87	102
台○銀行	4,112	4,533	4,881	5,262	5,503	5,952	6,145	6,316	6,723
安○銀行	115	126	121	127	142	149	154	164	180
中○信託銀行	13,415	15,550	17,539	20,213	21,447	22,239	22,332	22,192	22,066
將○商業銀行	-	-	-	587	694	789	850	922	977
樂○國際商業銀行	117	127	150	191	219	245	268	295	304
連○商業銀行	85	153	211	338	439	566	740	902	1,048
合計	69,815	77,299	82,154	90,343	95,650	103,767	110,304	117,830	125,756

資料來源：金管會於113年6月3日座談提供書面資料。

（1）依據「存款帳戶及其疑似不法或顯屬異常交易管理辦法」第9條規定，警示帳戶之警示期限自通報時起算，有效期間為2年，且原通報之司法機關認為有繼續警示之必要者，可再通報延長1年，故**單一存款帳戶警示期間最長可延續3年，爰因警示帳戶統計數為累積餘額，警示帳戶總數量長期會呈現增加趨勢**。

（2）經觀察108年至113年第1季警示帳戶數增加率，在督促金融機構強化各項風險管控機制後，警示帳戶數成長率已趨緩，由108年45%下降至

113年第1季31%[47]。

3、惟查，就警示帳戶總數之成長率而言，所有銀行自111年第1季至113年第1季，兩年約成長1.8倍(125,756/69,815*100%)，中國信託銀行之成長率為1.6倍(164%)，雖低於平均，但其警示帳戶總數仍占總數之17.5%，換言之每6個警示帳戶就有1個屬於中國信託銀行，至於金管會說明「警示帳戶數前幾大金融機構皆為分行家數多、客戶數多、ATM數多及網路銀行便民措施多之銀行」尚非可採，本調查研究認為。規模龐大之銀行反而應有充裕資源建置完善嚴謹之機制。

（1）進一步分析113年第1季之警示帳戶數量，以數量而言前五名分別為中○郵政(26,379)、中○信託銀行(22,066)、國○世華銀行(7,335)、第○銀行(6,728)、台○銀行(6,723)。

（2）如以兩年成長率而言，前五名[48]分別為連○商業銀行12倍(1230%)、兆○銀行2.5倍(249%)、台○企銀2.2倍（220%)、第○銀行2.2倍(216%)、華○銀行2.1倍(211%)。

（3）近兩年控管成長率最佳(低)之銀行[49]則分別為國○世華銀行(146%)、玉○銀行(157%)、台○銀行(164%)、中○信託銀行(164%)、新○銀行(170%)、台○銀行(170%)。

4、另查110年迄今金融機構涉及洗錢防制、人頭帳戶管理缺失之處分情形如下表8，金管會說明:共計11件案件，因涉及洗錢防制、人頭帳戶管理缺失，經金管會核處罰鍰或予以糾正，其中與洗錢

[47] 行政院出席本院於113年6月24日所辦座談會後之免備文補充資料。
[48] 剔除警示帳戶未達1000戶之銀行。
[49] 剔除警示帳戶未達1000戶之銀行。

防制缺失有關部分為6件、帳戶監控缺失部分為5件。然細究及處分事由，絕大多數與房貸及內神通外鬼案件有關，完全看不出有銀行因為控管人頭帳戶不佳遭到處分，對照警示帳戶由111年第一季6.9萬戶成長至112年第一季約12.6萬戶，等於一年增加一倍，顯示金管會對於管控人頭帳戶不佳之金融機構僅憑道德勸說，幾乎完全沒有拘束力及監理功能，實有成為打詐破口之虞。

表8　110年迄今金融機構涉及洗錢防制、人頭帳戶管理缺失之處分情形

金融機構	日期	處分事由 （僅涉及洗錢防制、人頭帳戶管理缺失之相關情形）	處分情形
聯○商業銀行	110.03.02	對一定金額以上通貨交易未申報缺失，核有礙健全經營之虞。	糾正
台○國際商業銀行	110.12.28	有關該行疑似詐欺性質交易款涉及透過該行客戶帳戶進行移轉一案，辦理他行行員開立於該行之存款帳戶之交易持續監控作業相關缺失，顯示該行未能有效執行洗錢表徵交易之審核與通報機制，對於自動化交易之監控態樣及參數設定亦未盡周全。	糾正
中○信託商業銀行	110.12.28	該行南中壢分行及石牌分行前理財專員管員及葉員與客戶間異常資金往來所涉缺失，核有違反銀行法第45條之1第1項規定。	核處1,400萬元罰鍰
花○（台灣）銀行	110.5.13	金管會對花旗(台灣)商業銀行辦理「貿易金融之防制洗錢、打擊資恐及反資助武器擴散」專案檢查報告(編號：108B070)及一般業務檢查報告(編號：109B014)所列防制洗錢及打擊資恐相關缺失，核有違反銀行法第45條之1第1項規定，依同法第129條第7款規定，核處1,000萬元罰鍰	裁罰1,000萬元罰鍰
星○（台灣）商業銀行	110.5.13	辦理一般業務檢查報告(編號：107B069)所列防制洗錢及打擊資恐相關缺失，核有違反銀行法第45條之1第1項規定，依同法第129條第7款規定，核處600萬元罰鍰。	核處600萬元罰鍰

金融機構	日期	處分事由 （僅涉及洗錢防制、人頭帳戶管理缺失之相關情形）	處分情形
台北富○商業銀行	110.8.19	香港分行107年7月辦理總經理原為實質受益人之久未往來帳戶重新恢復啟用作業，案關客戶之新實質受益人未依該行規定之書件提出申請，該分行即同意解除久未往來帳戶狀態，且匯入、匯出款項，並於108年2月始完成對案關客戶帳戶重新啟用之確認客戶身分作業，相關缺失已違反該行所定外匯存款辦法及防制洗錢作業等規定之作業原則，涉總行未建立久未往來帳戶重啟之流程與相關作業程序，及未確實督導香港分行辦理久未往來帳戶重啟之確認客戶身分作業，核有違反銀行法第45條之1第1項規定	核處200萬元罰鍰
聯○商業銀行	112.03.31	辦理自然人購屋貸款業務，未完善建立及落實執行洗錢防制作業，核有違反洗錢防制法第7條第1項，同條第4項授權訂定之金融機構防制洗錢辦法第5條及第9條規定。	核處150萬元罰鍰
聯○商業銀行	112.09.15	該行集賢分行辦理國外匯出匯款作業，對於符合疑似洗錢表徵之交易未能有效執行洗錢表徵交易之監控、審核及通報機制，核有礙健全經營之虞。	糾正
聯○商業銀行	112.11.24	辦理存款開戶及臨櫃提領大額現金作業所涉缺失一案，核有違反銀行法第45條之1第1項及授權訂定之「金融控股公司及銀行業內部控制及稽核制度實施辦法」第3條、第8條規定。	核處1,200萬元罰鍰
臺灣○光商業銀行	112.3.31	該行辦理自然人購屋貸款作業，未完善建立及落實執行洗錢防制作業，核有違反洗錢防制法第7條第1項、同條第4項授權訂定之金融機構防制洗錢辦法第5條及第9條規定，依洗錢防制法第7條第5項規定。	核處150萬元罰鍰
中○信託商業銀行	112.8.4	該行前理財專員挪用客戶款項、推介客戶短期間進行多筆交易及代客戶辦理網路銀行交易所涉缺失，核有違反銀行法第45條之1第1項及其授權訂定之「金融控股公司及銀行業	核處1,000萬元罰鍰

金融機構	日期	處分事由 （僅涉及洗錢防制、人頭帳戶管理缺失之相關情形）	處分情形
		內部控制及稽核制度實施辦法」第3條第1項、第8條第1項及第3項等規定，依同法第129條第7款規定。	

資料來源:金管會提供，本院自行整理

（四）小結：「打詐綱領1.5版」將銀行臨櫃攔阻率列為績效指標，本院諮詢專家學者表示「銀行行員阻詐做得很累，就給他頒獎，這樣子做一直循環，其實就不會有效果」，顯見臨櫃攔阻仍然是屬於下游措施；本調查研究認為，政府僅進行道德勸說，任由源頭之金融機構警示帳戶以3年暴增3.27倍之速度成長，而不以對銀行造成實際影響之業務縮減或評鑑作為監理工具，卻命行員進行有時極為擾民之阻詐措施而列為績效，實屬本末倒置，金管會難辭其咎。

（五）再查，民眾對於有償或無償提供帳戶予他人使用，未具可能淪為詐欺幫助犯意識，而詐欺集團多利用「代辦貸款」等話術取得人頭帳戶進行詐欺，近年並有轉向利用虛擬帳號收款趨勢〔110年警示帳戶計4萬8,526筆，其中虛擬帳號計2萬1,722筆(44.76%)；111年警示帳戶計7萬1,331筆，其中虛擬帳號計4萬2,016筆(58.9%)〕。且分析110至111年間警示帳戶中虛擬帳號遭利用之公司行號，其中約40%集中於第三方支付或電商業者，顯見犯嫌多利用審核較寬鬆之第三方支付代收款虛擬帳號，作為進行收取贓款之主要帳戶工具，為防制詐騙集團將第三方支付業者使用之虛擬帳號成為詐騙工具，政府對於第三方支付業者使用虛擬帳號服務管控機制如下：

1、數發部於112年7月啟動第三方支付服務業能量登錄制度，要求申請業者提出洗錢防制及法遵聲明書始能登錄，並審查其人力配置與素質、實績、執行管理能力、財務狀況等項目。

2、金管會於同年11月2日函請銀行公會轉知會員機構配合數發部所定第三方支付業者能量登錄機制，督導金融機構強化提供虛擬帳號服務之控管。金融機構將配合上開登錄機制，就第三方支付業者未完成能量登錄，金融機構在受理其開戶時（即新戶），則不受理。

3、若為銀行既有客戶（即舊戶），在數發部訂定之緩衝期內（112年12月31日前）未申請能量登錄者，則不提供虛擬帳戶服務。未先完成能量登錄之第三方支付業者，銀行在受理其開戶時就不會受理；若是銀行現有客戶，未申請能量登錄之業者，銀行將會視為高風險不提供虛擬帳戶服務。

4、完成修訂《第三方支付服務業防制洗錢及打擊資恐辦法》第5之1條，第三方支付服務業應依數發部指定之程序及方式，申請辦理洗錢防制暨服務能量登錄；其經審查通過者，由數發部通知並予公告。截至113年5月21日止，送件申請登錄業者總計81家，通過審查業者計53家，廢止登錄1家，審查後尚待補件業者計16家，未通過業者計9家；尚在資格審查中業者計2家。

5、第三方支付的登錄制度已屬類特許制度，基於洗錢防制目的之管理，更進一步於洗錢防制法第6條增訂：第三方支付服務之事業或人員未向中央目的事業主管機關完成洗錢防制、服務能量登錄者，不得提供第三方支付服務。違反規定者將處二年以下有期徒刑、拘役或科或併科五百萬元以

下罰金。

(六)茲因第三方支付業者申請之虛擬帳號占警示帳戶極高之比率，數發部業已提出能量登錄制度以改善虛擬帳號成為人頭帳戶之情形，該部並與金管會達成部會聯防共識，由金融機構配合第三方支付業者能量登錄機制，強化提供虛擬帳號服務之控管，然成效仍待觀察。建議政府持續觀察第三方支付業者虛擬帳號之管控成效。

(七)綜上，詐騙集團詐騙國人之目的不外乎取得金錢，故金流管制及洗錢防制措施實屬打詐政策之核心。本調查研究經盤點政府在金流方面之行政管制措施，在臨櫃阻詐及強化法幣實體帳戶KYC方面略具成效，惟第三方支付方面數發部雖已提出能量登錄制度，然成效仍待觀察。另人頭帳戶及警示帳戶數量仍未有效降低部分，將成為整體政府打詐措施中最薄弱之一環，政府除宜公布各金融機構人頭帳戶及警示帳戶之情形，並對金融機構管理不力予以課責外，並宜秉持行政先行及公開透明原則優先檢討打詐不力之金融機構，以避免成為打詐及洗錢防制之破口。

六、虛擬貨幣具去中心化、高度匿名及快速跨境移轉等特性，成為詐騙集團詐欺洗錢犯罪之工具。金管會雖已訂定虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法，以管理虛擬通貨平臺及交易業務事業（下稱VASP)，然基層檢察官指出當前各類詐騙案件中，以虛擬貨幣之詐騙金額最大，被害人損失最重，且質疑幣商之定義不明，導致基層檢察官對虛擬貨幣管理多有詬病。主管機關允宜詳細審視檢察官所提出之疑義，修正虛擬貨幣管理之疏漏，以避免於後續懲詐時，衍生更多紛亂，引發更大之民怨。

(一)按「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」第2條規定：「……虛擬通貨：指運用密碼學及分散式帳本技術或其他類似技術，表彰得以數位方式儲存、交換或移轉之價值，且用於支付或投資目的者。但不包括數位型式之新臺幣、外國貨幣及大陸地區、香港或澳門發行之貨幣、有價證券及其他依法令發行之金融資產。」，因此虛擬通貨並非由各國中央銀行以黃金等準備做為擔保，所發行之法償國幣，而是在非特定國家、地區發行，並在全世界通用，且不需支付手續費，更可規避監管，自由地轉移之資產。故虛擬通貨具有匿名性、易於跨境流通、可隨時兌現，及去中心化方式運作等特性，已為詐欺集團作為洗錢或詐欺之工具。

(二)詐欺集團要求被害人透過虛擬通貨交易所、BTM或幣商購買虛擬通貨，並將款項匯入犯罪集團指定之電子錢包，經多層移轉及去中心化特性隱匿贓款流向，使執法機關難以追查到資金來源。最後再將資金流回一般金融體系，裝成合法活動取得之金流，再由車手集團取款。「此種方式與以往使用贓款購買鑽石、珠寶的洗錢手法相似，但因虛擬貨幣無國

界、流通簡易，更方便去化犯罪所得，一旦現金被兌換成虛擬貨幣，查緝前就已被轉出，加深檢警查緝的難度。[50]」。另，詐騙集團亦將虛擬貨幣包裝成新興金融商品，誘人誤入陷阱，詐騙受害人身家財產，檢察官亦指出「當前各類詐騙案件中，以虛擬貨幣之詐騙金額最大，被害人損失最重，許多家庭破碎。此類案件追查困難，原因在於前端行政管理缺漏，導致後端司法難以調閱勾稽，且因為缺乏管理規則」[51]。是以，虛擬通貨因其特性，已成為詐欺集團作為犯罪之工具，雖金管會已針對虛擬通貨訂有洗錢防制等相關規範，然如BTM等是否已訂定相關管理機制，建議政府仍應審視詐騙集團利用虛擬通貨進行詐欺、洗錢之各種模式，並檢視現有政策是否足以防制虛擬通貨成為洗錢及詐欺之工具。

(三)由於各國對於監管虛擬貨幣的態度仍有分歧，多數將其當作商品看待，交易也多由民間組織經手。當前購買虛擬貨幣的方式，包含透過虛擬貨幣兌換所、交易所和場外市場（Over-the-counter, OTC）3種管道，但因未經官方認證、擔保，日前就發生全臺第3大虛擬貨幣交易所「ACE王牌交易所」，坑殺客戶的詐騙案件，許多無辜投資人蒙受重大損失[52]。金管會已就虛擬通貨平臺及交易業務事業VASP參考國際防制洗錢金融行動工作組織（Financial Action Task Force on Money Laundering，下稱FATF）訂定相關管理規範：

1、110年6月30日發布「虛擬通貨平台及交易業務事

[50] 青年日報113年5月2日【社論】提升識詐防詐知能 守護財產安全。
[51] 113年4月26日「檢察官打詐實務暨修法研討會」報告資料。
[52] 青年日報113年5月2日【社論】提升識詐防詐知能 守護財產安全

業防制洗錢及打擊資恐辦法」（下稱VASP洗防辦法），規範為他人從事下列五類活動[53]之一者（包含自然人及法人）即屬VASP範疇，應向金管會提交文件完成洗錢防制法令遵循聲明（下稱法遵聲明）後始得從業：

2、個人幣商核屬VASP事業範疇，應完成法遵聲明後方得從業。

3、為他人從事前揭虛擬資產活動為業之個人幣商（自然人），應依前揭規定向金管會完成法遵聲明，方得從事VASP業務，如未完成法遵聲明即從事VASP活動者，金管會將依洗錢防制法第6條第4項規定令其限期改善；屆期未改善者，將處50萬元以上1,000萬元以下罰鍰。

4、為避免外界誤解以個人名義從事VASP業務者免依洗錢防制法及VASP洗防辦法規定向金管會辦理法遵聲明及遵循洗錢防制義務，金管會已於洗錢防制法修正草案調整VASP名詞，由「虛擬通貨平臺及交易業務事業」改為「提供虛擬資產服務之事業或人員」，納管對象仍與現行相同。

5、未符合洗錢防制標準而向金管會辦理法遵聲明者，金管會將函復其未完成法遵聲明，其仍應待完成法遵聲明後，方得從事VASP活動。

6、VASP執行業務時應執行確認客戶身分、紀錄保存及可疑交易申報等措施，以因應可疑犯罪金流及作為司法機關認定不法活動之證據，未依規辦理者，金管會將依洗錢防制法相關規定予以處置。

---

[53]（1）虛擬通貨與新臺幣、外國貨幣及大陸地區、香港或澳門發行之貨幣間之交換；
（2）虛擬通貨間之交換；
（3）進行虛擬通貨之移轉；
（4）保管、管理虛擬通貨或提供相關管理工具；
（5）參與及提供虛擬通貨發行或銷售之相關金融服務。

7、為防止不法集團利用人頭帳戶收取犯罪所得，洗錢防制法第15條之1及第15條之2已禁止無正當理由收集或提供虛擬資產帳號，金管會亦於洗錢防制法第15條之2訂有違反前開規定經警察機關裁處告誡者，VASP將限制其虛擬資產帳號之功能或拒絕開立新帳號之規範。

8、為強化VASP業者之防詐作為，金管會已於「詐欺犯罪危害防制條例草案」(即打詐專法)賦予VASP與金融機構一致之防詐義務，未遵守相關規範者將處以罰鍰，草案於113年5月9日經行政院通過，並於7月31日公布，重點包括：及時攔阻可疑幣流、警察聯防通報機制、源頭斷詐宣導、加速返還遭詐款項，以及未遵守相關規範之罰鍰，金管會可處20萬元至200萬元之罰鍰，其情節重大者，罰鍰金額將提升至100萬元至1,000萬元。

(四)查金管會雖已就虛擬通貨訂定相關規範，且法務部亦積極優化境內外虛擬通貨交易所資料調取、凍結與扣押效率，強化執法機關追緝虛擬通貨金流效能。警政署亦與部分國家及香港地區建立緊急攔阻管道，增加被害人取回款項之機會。然本調查研究蒐整基層檢察官基於實際偵辦案件經驗之觀察，仍發現源頭管理措施有所不足。首先是對於VASP業者欠缺層級化管理，對於不同規模之業者以同一套定義加以規範，以致於缺乏對於個人幣商之定義，除有將個人幣商逼入地下化經營之虞，更導致後端懲詐階段時缺乏足夠證據連結而加以定罪，其次為VASP業者之違規查處機制幾乎全由金管會以外之機關發動，如檢調、稅務、公司登記等，金管會作為主管機關反而沒有足夠的監理措施；另查高檢署亦稱「虛擬貨幣」成為重要詐欺手段及洗錢手法，

大量詐欺車手以「個人幣商」抗辯等等。在在顯示虛擬貨幣之治理與其他打詐環節相同，都存在上游治理不足導致下游案件暴增又無法定罪之通病，主管機關金管會似均有改善空間。

1、根據本院蒐集劍青檢改於113年4月26日辦理「檢察官打詐實務暨修法研討會」，部分檢察官直言打詐困境包括：

（1）發生問題全部把它刑事化送去判刑，送去判刑有效嗎？我要怎麼證明他跟這些詐騙罪有勾結？

（2）虛擬通貨原則都沒有規定什麼叫個人幣商，各位可以想像嗎?法院還要自己去定義。

（3）金管會說什麼違反商業登記規則，沒做稅籍登記，問題是金管會罰得到嗎？金管會是主管機關嗎？這全部都在甩鍋給別人。

（4）個人幣商的管制，應該是要由主管機關先訂好行政規範，甚至哪一些等級的虛擬資產服務提供者，必須要符合哪一些等級的這個規範。行政管制甚至要做第2層的輔導，輔導之後如果還有不足，那行政機關的裁罰要先行，刑事手段其實是放在最後。

2、其次，法務部及高檢署認為目前在懲詐方面的挑戰包括「虛擬貨幣」成為重要詐欺手段及洗錢手法，但管理虛擬資產平臺及交易業務事業VASP指導原則未臻完善，導致大量詐欺車手以「個人幣商」抗辯，而使法院做出對被告有利之認定。

3、對於基層檢察官之意見，行政機關則認為有所誤解如下，本調查研究建議行政機關對劍青檢改所提疑義仍宜有效處理。

（1）行政院稱「金管會與法務部多次研商，參考美

國、英國、澳洲、南韓及香港對於未取得執照或註冊之VASP訂有刑事責任之立法例，於洗錢防制法修正草案增訂未依規登記而從事VASP活動者之刑事責任，將可有效避免不法份子佯稱其為個人幣商以規避刑事責任之情形。該草案業經行政院審查通過，刻由立法院審議中(按:已三讀通過)。」

（2）金管會亦稱「為避免外界誤解，金管會已於洗錢防制法修正草案修正文字，……由『虛擬通貨平臺及交易業務事業』改為『提供虛擬資產服務之事業或人員』，納管對象仍與現行相同」等語。

4、惟經本調查研究進一步檢視金管會以金管證券字第1120385668號令所訂虛擬通貨幣商之洗錢防制法令遵循聲明書，所應檢附之文件包括「業務章則及業務流程說明」、「經會計師複核之防制洗錢及打擊資恐內部控制與稽核制度檢查表，並出具審查意見書」，顯係針對業者，且非個人幣商所能提出，此與基層檢察官意見相符，是否同樣得以規範個人幣商頗有疑義，似非金管會修改文字即可；而在個人幣商無法提出相關文件後，勢必將其逼入地下化經營，對於整體打詐更為不利。

5、此外，臺北地檢署羅韋淵檢察官奉法務部指派赴美國哈佛大學做訪問學者，研究題目即為網路犯罪以及虛擬貨幣犯罪，渠於113年4月26日「劍青檢改」研討會上直言，國際防制洗錢行動組織FATF從2021年10月的時候就已經發布了相關的指引，去描述虛擬資產服務提供者應該要有所規範，如果沒有這個遵循FATF相關指引的話，未來

可能嚴重的是影響我國的評鑑，甚至我國對外的經貿，值得行政院及相關部會注意。

（1）國際防制洗錢行動組織FATF從2021年10月的時候就已經發布了相關指引，去描述虛擬資產服務提供者應有所規範，他們是針對法人公司做規範?還是說連自然人也要規範?關於這一點在我國其實是有很大的爭議。

（2）個人以跑單幫方式，不做公司登記、商業登記，或稅籍登記，那就不受辦法規範，那既然不受辦法規範，則主管機關也無法依照辦法去裁罰。

（3）如果沒有這個遵循FATF相關指引的話，未來可能嚴重的是影響我國的評鑑，甚至我國對外的經貿。

6、小結：為解決懲詐階段無法對涉詐之個人幣商進行起訴定罪，並建立足夠之上游治理強度，調查研究建議金管會審視虛擬通貨於詐欺及洗錢所運用之各種模式，檢視現有法規是否足以防制虛擬通貨成為洗錢、詐欺之工具。

(五)綜上，虛擬貨幣具去中心化、高度匿名及快速跨境移轉等特性，成為詐騙集團詐欺洗錢犯罪之工具。金管會雖已訂定虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法以管理平臺VASP，然基層檢察官指出當前各類詐騙案件中，以虛擬貨幣之詐騙金額最大，被害人損失最重，且質疑幣商之定義不明，導致基層檢察官對虛擬貨幣管理多有詬病。本調查研究建議主管機關仍應詳細審視檢察官所提出之疑義，修正虛擬貨幣管理之疏漏，以避免於後續懲詐時，衍生更多紛亂，引發更大之民怨。

七、懲詐面於偵查部分屬於整體打詐環節之末端，檢警在偵破集團、移送案件及查扣返還金額上持續進步，但在近兩年上游行政規管措施及法制配套未臻完善前，各地檢署新收詐欺案件由110年9.8萬餘件暴增至112年近23萬件，對整體偵審體系之處理量能形成巨大壓力，由各基層檢察官每月新收案件超過一半屬於詐欺案件而言，已排擠檢調體系對其他重大犯罪之偵查量能；對此，法務部及高檢署雖已對內提出檢察官助理、AI智慧輔助系統、被告總歸戶、建置全國反詐騙資料庫分析、設立科技偵查支援辦公室等措施，雖可一定程度紓解檢警負荷及提高偵查效率，然而該等內部措施無法解決過去科技偵查法制落後及欠缺證據力之痛點。在立法院陸續三讀通過通保法，及將科技偵查內容增訂於刑事訴訟法「特殊強制處分」後，將可有效縮短檢警與詐騙集團在科技上之差距，惟其效益有待驗證；民間團體雖尚未對刑事訴訟法新增科技偵查內容提出意見，但仍就通保法部分條文提出疑慮，對此，法務部允宜就內控或相關配套審慎評估，以力求懲詐面之周妥。

(一)有關詐欺案件已對檢警調偵審之作業量能產生嚴重排擠一節，本調查研究分別由巨觀之統計數據及微觀之檢察官陳述說明如下。此外，懲詐相關措施已是打詐政策的最後一道防線，然而由懲詐量能已無力負荷之現象，顯示上游之「識詐」、「堵詐」、「阻詐」等環節需要善盡源頭管理職責，避免因控管鬆散而使案件全由檢警調偵審系統承擔。

1、在巨觀上，根據高檢署提供資料，地檢署110年電信網路詐欺案件新收案數為98,256件，111年暴增至160,803件，112年再成長至229,711件，而據

法務部鄭銘謙部長受媒體訪問表示[54]，112年詐欺新收案件數占全國各地檢署總收案的刑案比將近36%，其中電信詐欺及人頭帳戶案件新收案件數，與111年相較分別又增加42.9%、67.3%。換言之，全國各地檢署在兩年之間新收電信網路詐欺案件暴增達13萬件。

2、在微觀上，據本院訪談基層檢察官及摘錄劍青檢改研討會與會者發言，目前詐欺案件已占檢察官偵查案件約半數，其中又有超過半數屬於人頭帳戶，本調查研究認為，基於前述「識詐」、「堵詐」及「阻詐」之上游治理不足，而造成下游案件爆量之推論已十分明確，並已嚴重影響檢警偵辦其他重大犯罪或偵破詐騙集團之能力。

（1）臺北地檢署姜長志檢察官

〈1〉多數檢察官每月收案80到100件，身上背著3、4百件在轉，哪有能力去追詐騙源頭。

〈2〉我手上案子至少半數以上是詐騙，詐騙案又有8成都是人頭帳戶。

（2）金門地檢署施家榮主任檢察官

〈1〉如果要你一個月要寫100份起訴書或不起訴處分書，你還有時間去做其他事嗎?有可能召開專案小組要深入追查嗎?

〈2〉詐欺它也是一個產業，它為什麼會蓬勃發展?他錢多當然要求發展，你就沒有法律，沒有科技偵查手段，一直追不到核心幹部，一直追不到他的錢，他錢越來越多，一間公司錢越來越多，他不發展合理嗎?他一定要蓬勃

[54] 高檢署打詐會議 鄭銘謙：嚴懲重罰詐欺犯罪。聯合新聞網。113年5月29日 https://udn.com/news/story/7321/7996882

發展嘛!

〈3〉再來說律師涉案、銀行人員幫忙調整轉帳上限、派出所所長查個資、通傳會前委員當二類電信業者顧問這些,為什麼?因為你永遠查不到他的心臟,那他就可以經驗傳承,越教越多人,他獲利高風險低,因為人頭帳戶、人頭門號、個人幣商都沒在管,他就挺而無險,他當然要繼續做啊!

(二)根據高檢署張斗輝檢察長於112年11月13日本院辦理履勘時說明:「這一、兩年詐欺案件暴增,癱瘓檢警偵查量能,高檢署身處第一線,馬上承受到檢察官的壓力」,為此,高檢署除協調各機關推動源頭管理外,已對內推動檢察官助理、AI智慧輔助系統、被告總歸戶、建置全國反詐騙資料庫分析、設立科技偵查支援辦公室以分析幣流等措施,或可部分紓解偵查量能之負荷。

1、在法務部極力爭取的檢察官助理部分,法務部雖於112年先行聘用100名,然後續仍有法制化之必要性,據悉[55],行政院人事總處於113年6月24日立法院司法法制委員會審查攸關增設檢察官助理的「法院組織法修正草案」時表示,檢察官助理去年10月開始才開始陸續進用,其效益有待觀察,建議1年後再進行評估是否法制化,法務部鄭銘謙部長則表示,檢察官助理今年開始才再增聘150位,到年底才能達250位,但仍是臨時性的人員,若法制化對於打詐等相關工作會有很大幫助。顯見檢察官助理法制化議題暫時無法達成,

[55] 檢察官助理法制化 人事總處:效益有待觀察盼1年後再評估。中央廣播電台。1113年6月25日

有賴法務部持續溝通，而法務部既已臨時進用250人，對於紓解檢察官相關文書作業負荷，仍具一定效益。

2、有關檢察官指出製作詐欺相關起訴書附表極為繁瑣一節，法務部自110年起，開發AI智慧輔助系統功能，已介接司法警察機關相關165反詐騙平臺資料庫及案件管理系統，以系統自動產製詐欺案件附表，以取代人工製作。

（1）介接警政署165反詐騙平臺、辦案資料庫資料：

〈1〉警政署165反詐騙資料庫係將詐騙或疑似詐騙之受理資料均建置至系統內，內容繁多，經與警政署多次召會協調，向警政署165反詐騙資料庫產出之「警政署反詐騙諮詢專線紀錄表」（含報告紀錄）、移送書及警詢筆錄電子檔等資料及相應系統欄位進行介接，警政署已於112年6月21日函復同意介接，並配合系統功能增修，目前已介接完成。

〈2〉完成介接警政署辦案資料庫之當事人資料、移送書及電子筆錄，檢察機關可代入至內勤庭前筆錄系統製作，書記官製作筆錄時，毋庸再重複繕打當事人基本資料等事項，提昇偵查庭訊進行之效率。

〈3〉開發AI系統產出酒駕案件結案書類初稿。透過自然語言處理(Natural Languange Proccessing, NLP)技術，解讀移送書、警、偵訊筆錄及卷證內容後產出起訴書、聲請簡易判決處刑書、緩起訴處分書之結案書類初稿，並自動判讀累犯。

（2）上開功能開發完成後，已於112年11月底於桃園地檢署及臺中地檢署轄區部分分局及署內特

定承辦股試辦測試，並於113年5月間與刑事局協調於桃園及臺中警察局全區擴大試辦，獲刑事局、桃園及臺中警察局同意配合上傳相關數位資料。復於113年6月13日完成桃園地檢署及臺中地檢署署內擴大試辦AI系統功能教育訓練，並預計於113年6月20日開始全署試用。將於試用二個月後，調查及蒐集使用者回饋意見。

3、在總歸戶措施方面，113年3月、4月較112年同期新收案件數明顯減少39.6%、24.3%，可見總歸戶計畫對於減少幫助詐欺案件數已獲致初步成效。高檢署另補充說明，單純提供人頭帳戶之幫助詐欺案件，被告所提供同一帳戶可能造成多數被害人衍生複數案件，各地司法警察機關接受被害人報案後，應將被害人報案資料統一歸戶至被告戶籍地司法警察機關彙整移送所屬地方檢察署。

4、高檢署所建置之「全國反電信詐騙資料庫」，項下功能包括境外停留交集、嫌疑人關聯分析、可疑共犯名單、人脈網絡分析、通聯分析等，除提供資料查詢外，並結合入出境資料、艙單資料、通聯資料與詐騙資料庫豐富資料進行碰撞分析、比對，藉此產出可疑犯罪情資供進一步追查，其功能架構如下表9，高檢署亦提出兩案說明資料庫績效。

表9　高檢署「全國反電信詐騙資料庫」功能列表

主功能	子功能
整合查詢	165反詐騙查詢
	艙單查詢、交集查詢
	入出境個資模糊查詢
	境外停留交集
情資分析	人脈網絡分析
	集團關聯分析
	嫌疑人關聯性
	可疑共犯名單
金流分析平臺	資金流向分析
	扣押裁定附件
	資金清查表
	金融轉置
警示預判	入出境警示
	警示訂閱
	警示分析

資料來源：高檢署提供，本院自行整理

(三)至於科技偵查手段鬆綁部分，基於詐騙集團大量運用科技手段，傳統偵查手段已相形見絀，故在延宕6年之後，科偵法及通保法終因打詐之嚴峻需求，而與「詐欺犯罪危害防制條例」一同納為「打詐新四法」，於113年5月9日通過行政院會並送立法院院審議，通保法嗣於7月12日通過，科偵法草案則因立法政策，將相關內容改於刑事訴訟法增訂「特殊強制處分」，亦於7月16日三讀通過，則未來在通訊使用者資料、GPS及M化車方面將可成為偵查利器，以縮短檢警與詐騙集團之科技落差；然而人權團體仍不免對其鬆綁程度及授權情形有所疑慮，本調查研究除爬梳雙方見解之外，原則上仍認為，我國詐騙情勢之所以如此嚴峻，本調查研究於結論與建議一已敘明，主要原因就在於政府法制、規管及政策未能

充分跟進數位化、網路化及全球化之進程並加以治理，相同推論亦可適用於科技偵查，是以證據力與時效性兼備之偵查方法與工具，宜隨技術演進及犯罪模式與時俱進，如同通保法並未拘泥於電話尚未普及之紙本書信時代一樣，然無論人權團體意見是否涉及科技偵查手段適切性，若有部分條文確有需要其他內控或法制配套時，亦請行政院及法務部等相關機關審慎研議。

1、本院諮詢學者專家對於科技偵查之見解:

（1）可不可以有好的科技工具分析出來他們跑的這個脈絡和路徑，也就是「以科技對付科技」，用傳統偵防是沒辦法逮到它的。

（2）政府要給執法部門「科技對付科技」的資源量，我們現在的執法部門比不上這些犯罪集團的科技量，有足夠的科技量，才有辦法提高我們的刑罰的確定性。

2、臺灣大學林鈺雄教授於劍青檢改研討會中對科技偵查之重要論述：

（1）沒有科技偵查，就什麼東西都不用談，這叫做現代科技的武器平等原則。依照研究的結果，我們是全球唯一一個明文規範禁止使用GPS的國家。

（2）中央一方面每年編列六、七千萬在M化車預算，但是一方面禁用M化車。

（3）據說我們的科技偵查裡面將不會有設備端的通訊監察，也就是說，以後詐騙集團的車手要跟上面的聯絡可以很放心。

3、科偵法及通保法係分別於109年及107年即由法務部提出草案，然經行政院多次召會研商條文，期間不乏招致人權或隱私權疑慮，惟在延宕多年

後，終於經調整條文內容後在113年5月9日通過行政院會，並送立法院審查，據悉[56]《通訊保障及監察法》已完成三讀，而《科技偵查及保障法》之內容則改於刑事訴訟法部分條文修正案增訂「特殊強制處分」。

（1）於106年行政院海岸巡防署士官長裝設GPS案件被判有罪確定後，法務部經多次內部研商會議後，提出「科技偵查法草案」，並於109年9月8月對外預告。鑑於外界對草案有諸多修正建議，法務部再經蒐集國內外實務發展及立法例，並舉辦2次國際研討會，召開2次跨機關及3次學者專家研商會議，於112年7月11日將「科技偵查及保障法」草案送請行政院審議。由行政院召開7次跨部會審查會議後，於113年5月9日行政院院會通過，立法院則於7月16日將《科技偵查及保障法》相關內容改於刑事訴訟法部分條文修正案增訂「特殊強制處分」並經三讀通過。

（2）法務部於107年提出通訊保障及監察法修正草案，刪除調取通訊使用者資料及通信紀錄之規定，並增訂GPS條款及電信業者保存網路連線資料之義務，並送請行政院審查。嗣法務部於110年11月23日再度提出修正草案送請行政院審查，刪除GPS條款，並修正通訊使用者資料及通信紀錄之規定，明定保存及調取網路流量紀錄規定，俾利執法機關藉由分析數位足跡，有效溯源、追查網路犯罪。草案經行政院召開逾10次跨部會審查會議後，於113年5月9日經行政院院會通過，業於7月12日立法院三讀通過。

[56] https://www.cmmedia.com.tw/home/articles/47732

4、財團法人民間司法改革基金會(下稱司改會)則於113年6月4日發布「監控開大門，國會同意嗎？民間團體聯合記者會新聞稿」指出對於「詐欺犯罪危害防制條例」及「通保法」提出仍存有人權及隱私權疑慮，包括巨幅擴增監控項目、下修監控門檻：《通保法》草案(按:通保法已於7月13日三讀通過)侵害隱私、資訊自主等，本節摘述司改會對於「通保法」大幅放寬監控項目及門檻之疑慮如下。本調查研究並發現，過去經常遭受質疑的科偵法目前尚未出現質疑聲浪，惟仍建議法務部持續對外溝通，並評估建立適當內控或子法配套機制之可行性。

〈1〉本次修法，行政院認為不需要「檢察官保留」或「法官保留」，警察偵辦所有的刑事案件，皆可逕行取得嫌疑人的使用者資料；對此重大變革，行政院提出的理由僅為「使用者資料涉及隱私程度較低，因此並非秘密通訊自由的保障範圍」。司改會認為此一政策轉變的正當性有疑問，說明也不充足。

〈2〉草案如通過，9成的案件都不會經過法院，檢警便可取得上開「網路流量紀錄」。對此，行政院也未公布對人權的負面影響，缺乏有具體的評估及說明，僅是舉起「打詐」的大旗，便要人民及立法院同意這張空白的政策支票。

5、法務部認為科偵法及通保法通過後，對於檢警使用M化設備將產生偵查實務上的變革包括：

（1）行政院版草案就M化車之利用規範於「科技偵查及保障法」草案第3條，即調查行動通訊設備之位置、設備號碼或使用之卡片號碼。因考量

行動通訊設備—如手機，與個人之連結性高，且個人對之有較高隱私期待，故採法官保留原則，實施調查前應由檢察官依職權或由司法警察官報請檢察官許可，向法院聲請核發許可書後為之。調查過程中，因技術無可避免取得第三人個人資料，僅得供調查目的之比對，且於調查實施結束後應即刪除。

（2）未來檢、警即可合法利用M化車進行調查，合法蒐證所得之證據亦可為證明詐欺犯罪之有力證據。其中對於車手去向、水房或機房位置，甚至首腦身分、位置，均有一定之查緝效用，助益甚大

（3）在無法律授權之情況下，使用M化設備執行偵查工作，除可能涉及侵害人民權益外，以往使用M化車定位追蹤手段進行偵查之案件，亦曾有經法院裁定不具證據能力，致犯罪集團最終判決無罪情形。若相關法案按行政院版本通過，在法律規範之要件與程序下授權執法人員使用科技偵查工具，可依比例原則調和偵查目的與科技設備運用手段，避免犯罪調查手段落後科技發展，同時強化對各類犯罪案件之查緝力道，應能兼顧社會安全與民眾權益。

（4）使用M化設備可有效精準掌握犯罪地點：利用M化車調查行動通訊設備資訊，能讓執法人員得以掌握可能犯罪處所，如詐欺機（水）房、嫌犯或受拘禁被害人藏匿處所等，透過科技偵查設備可大幅縮短偵查時間，有效掌握犯罪現場狀況並精準打擊犯罪，對於後續溯源追緝集團上游核心具正面幫助。

(四)經研析英國於2023年6月公布之打詐策略(Fraud

Strategy: stopping scams and protecting the public)發現，英國政府在懲詐面欲推動之科技偵查、人員招聘、數位證據處理等方向與我國相符；而在情報合作、警務訓練、資料調取方面則優於我國，值得行政院於擬定「打詐綱領2.0」時予以評估。

1、在強化科技偵查方面，英國政府認為現代科技使得從境外實施詐欺變得容易，這使傳統的偵查方法受挫，並阻礙了將詐欺者繩之以法的能力，政府必須加以因應，是以我國科偵法及通保法之修法方向應屬合乎世界潮流。

2、其次，英國成立一個由400多名新專業調查員組成的新的國家反詐欺小組，在這部分確實優於我國檢警單位多以任務編組或臨時聘僱方式增加人力，卻未實際增加員額之方式，值得法務部及高檢署於爭取檢察官助理時參考。

3、此外，英國內政部和警務學院(College of Policing,CoP)將促進警方數位技能的整體培訓，非常值得警政署進一步了解英國具體作法及訓練方式。

4、在偵辦詐欺案件方面由於資訊流及金流均已數位化，故特別需要處理數位證據，英國政府僅指出需使擁有大量數位證據的案件的揭露制度現代化，具體作法並未詳述，有待檢警調進一步了解或交流。

5、英國政府擬在英國情報界部署一個以詐欺情資為重點的部門，以更好的情資驅動調查；換言之，英國已將懲詐提升至國安層級，至於對於我國懲詐措施有無參考價值，則有賴相關機關評估。

6、英國政府擬整合使用英美資料存取協定：所有調查人員從美國科技公司取得資料都是困難且耗

時的，對於依賴大量數位數據的詐欺調查尤其如此。英國政府正在讓檢察官更輕鬆地獲取偵查和調查詐欺並確保起訴所需的數位證據。2022年10月生效的英美數據存取協議允許英國公共當局直接從美國公司獲取數據，以預防、偵查、調查和起訴包括詐欺在內的嚴重犯罪。這部分之規劃在我國雖不具類似條件，但仍建議相關部會應持續透過合作關係強化爭取類似協議。

(五)綜上，在懲詐面之偵查部分，檢警在偵破集團、移送案件及查扣返還金額上持續進步，惟詐欺案件持續高發及欠缺科技偵查工具的情況下，對檢警正常偵辦量能、效率及證據力仍極具挑戰，本調查研究建議行政院協助法務部及高檢署持續積極推動及爭取內部措施，如檢察官助理、AI智慧輔助系統、被告總歸戶、建置全國反詐騙資料庫分析、設立科技偵查支援辦公室等措施；而為因應打詐之嚴峻需求並縮短檢警與詐騙集團之科技差距，行政院在「通訊保障及監察法」及刑事訴訟法「特殊強制處分」三讀通過後，宜驗證其成效，並同時評估內控及配套措施，以降低侵害人權之疑慮。

八、在懲詐面，甫於113年7月12日立法院三讀通過之「詐欺犯罪危害防制條例」(打詐專法)，業於113年7月31日公布，雖已加重詐欺相關刑責，但仍不足以對犯罪形成足夠之嚇阻力，尚賴審判體系作為整體打詐環節的最後一道防線，本調查研究經蒐整有關懲詐面於審判階段之各界意見，發現立法院於113年7月16日將科技偵查內容增訂於刑訴法「特殊強制處分」條文後，已部分解決立法政策爭議，然而詐欺犯罪量刑及想像競合犯、數罪併罰定應執行刑之議題則尚有爭論；本調查研究於涉及審判獨立原則部分，僅歸納各界及先進國家之意見或作法供審判機關參考，至於其他與司法行政相關之研究發現，例如詐欺專業法庭等，亦一併臚陳供參。

(一)在加重詐欺犯罪刑責以增加嚇阻力部分，英國於2023年6月公布之打詐策略敘明將檢討該國2006年《詐欺法》是否能夠應對現代詐欺的挑戰，包括處罰是否仍與犯罪相符等議題；而我國先於112年5月透過「打詐五法」修訂「刑法」，以因應經常發生(強)控車[57]事件，甚至導致死亡；另因應Deepfake等新科技成為新詐騙術；行政院復於113年5月9日於行政院會通過「打詐新四法」送立法院審議，詐欺犯罪危害防制條例至113年7月12日已三讀通過，已納入高額財損加重詐欺罪與三人以上複合型態及在境外對境內之人犯詐欺罪加重刑責之規定。顯見各國國情及法制架構雖然不同，但加重刑責在打詐環節中仍具重要意義。

(二)由各界有關科技偵查應於刑訴法或專法中規範之意見加以綜整，顯示立法院雖然於113年7月16日將科

[57] 意指詐騙集團運用暴力控制人頭帳戶行動

技偵查內容增訂於刑事訴訟法「特殊強制處分」條文，然而過去對於科技偵查應於專法或刑事訴訟法中規範，學界及立法者迭有爭論，論者認為訂於刑事訴訟法則適用範圍較廣，目前每遇新型態之社會問題即立一專法，似非合理作法；但法務部則認為專法修法速度較快且能適切回應執法機關需求；刑事訴訟法主管機關司法院則認為科技偵查規範於專法或刑事訴訟法係屬立法選擇等。本調查研究調查首先認為，立法院透過修訂刑事訴訟法新增科技偵查事項，確為我國科技偵查法制之重要里程碑，惟其成效或潛在問題仍待後續驗證。

1、林鈺雄教授於劍青檢改研討會中對科技偵查之重要論述：德國從1992年開始就形式鬆綁開始使用GPS，德國刑事訴訟法的條款這30幾年修了100多條，裡面絕大部分、最重要的就是在修科技偵查；我們臺灣從1992年到現在修法次數已經破了法條的數目(512條)，但我們科技偵查到現在為止，修的是0條，臺灣還要這樣下去嗎?

2、黃國昌立法委員:

（1）我們為什麼要立特別法?因為臺灣政治上面的需求?還是立法技術拙劣?我們不斷的有特別法肥大症，而不管是GPS、 M化車，甚至其他的科技偵查的手段，本來就是在刑事訴訟法裡面應該要規範的對象，為什麼不修在刑事訴訟法?

（2）我們出現一個新型態的社會問題，就立一部專法來加以處理，從整個法規範秩序裡面是完全沒有道理。

3、對此，行政院函轉法務部意見表示，修訂專法主要考量修法速度且較能回應執法機關之期待。

（1）法務部因考量專法較能反應執法機關對立法

期程之期待，刑事訴訟法為刑事程序根本大法，修正速度較難預期，而法務部就偵查實務面，較為了解第一線執法機關運用科技偵查方法之技術面及實務發展情形，故提出科技偵查專法，且未來修法較易，較能反應快速變化之新興科技犯罪。另我國亦有就強制處分另訂專法之立法前例，且專法亦能就特別事項為較完整之規範，故法務部於評估後提出科技偵查及保障法。

（2）專法能就相關事項做完整規範：以特別法規定，針對特定事項立法規範，較能劃分基本法與特殊事項之區別，也較有空間對科技偵查之種類、聲請要件及程序、資料保障及銷燬、其他行政控管措施等事項，做較為完整之規範，就落實對人民隱私權保障可更為完善。

（3）強制處分性質訂立專法亦有前例，且不致刑事訴訟法過於龐大：專法或定於刑事訴訟法，均為政策選擇，我國就具強制處分性質之事項，以專法另外訂定之前例，亦不在少數，例如羈押法、通訊保障及監察法，均為著例，就該事項本身幾乎全為刑事訴訟程序，仍另訂專法者，亦有前例，如國民法官法。我國刑事訴訟法之法條實際上已逾600條，是否要將有關刑事訴訟之事項均訂入刑事訴訟法，致其條文數過於龐大，亦可慎思。

4、對此，司法院於本院113年6月3日辦理座談前書面說明重點如下：

（1）科技偵查手段究係規定於刑事訴訟法或專法中，乃立法政策。

（2）以專法同時規範民刑事實體法及相關程序與行政管理、民事責任等事項，在我國亦有諸多

前例。我國因刑事特定犯罪或民事特定法律關係而制訂包含實體法、程序法及行政程序的專法，所在多有，諸如性侵害犯罪防治法、毒品危害防制條例、家庭暴力防治法等，均是如此。

（3）就現階段而言，以專法方式規範科技偵查作為，為最佳途徑。

(三)其次有關量刑及想像競合犯、數罪併罰定應執行刑之議題，按現行作法，無論涉犯多少詐欺犯罪，經前述審探及量刑過程後，仍可定執行刑為最低刑責，復以詐欺犯罪刑責本低。綜合前述因素，詐騙集團基於理性選擇自然前仆後繼犯罪，致使懲詐毫無嚇阻力可言，縱然「打詐專法」已設計三振條款以加嚴重複犯罪之假釋，然而嚇阻力恐極為有限，並有目的手段不當連結之疑慮，值得司法機關思考；法務部雖已承諾未來審慎研議，然而本調查研究認為本項議題短期內將不會獲得有效解決，因此仍必須仰賴打詐措施上游各環節發揮綜效，以彌補量刑及定執行刑方面的問題。

1、本院112年11月13日履勘高檢署座談時，已有檢察官指出過去已向司法院反映刑責問題，但迄今似乎尚未獲有效處理，以致有「臺版柬埔寨」一案因首腦被判31個加重詐欺，卻連一天也不用關而遭人詬病的事件：

（1）高檢署劉檢察官海倫：我於2017年參加跨部會會議時，針對法院量刑過低議題進行報告，司法院當時回應會設計相關機制，然而今年我也因法院定應執行刑刑度過低提起3件抗告，但都遭最高法院駁回。

（2）臺北地檢署劉主任檢察官仕國

〈1〉現在司法實務幾乎全部都是從低度刑開始

量刑，只要法官在法律規定範圍內量刑就是合法的，上訴都會被駁回。

〈2〉法院定執行刑時更是容易產生爭議，例如詐欺車手犯了20次，每次都判1年，這20次合起來定一個執行刑時，加起來你以為要執行20年，錯！只要法院定應執行刑是1年1個月就是合法的，不要說我們檢察官常常無法接受，人民要是知道了，大概也都無法接受。

〈3〉其實為何詐欺案件量居高不下，如果從一個犯罪者角度思考，這幾年來詐欺案件迅速增加，以及犯罪者年齡逐漸下降，與犯罪成本低廉但獲利豐碩密切相關。

2、對此，法務部說明如下：

（1）有關刑法「想像競合」及「數罪併罰」規定可能之修正方向，法務部已將此議題納入刑法研究修正小組會議討論，有待凝聚各界共識，法務部將審慎研議。

（2）本議題除涉及刑法想像競合犯、數罪併罰定應執行刑之修法議題外，另涉及刑事訴訟法第288條、第289條及第477條有關量刑調查及量刑辯論程序之規定是否有修正必要，另在宣告刑部分，更涉及司法院目前已建置之量刑資訊系統（包括但不限於量刑趨勢建議系統、事實型量刑資訊系統等）是否確實能對個案法官量刑上產生正面指引效果，以及審判機關量刑時，是否從最低刑度往上量刑，或能從中間刑度依個案情節往上或往下量刑，凡此均屬審判機關之量刑職權，並非單純修正刑法即可完全解決此一爭議。

（3）詐欺犯罪危害防制條例第50條：「檢察官提起

公訴認有必要時，得於起訴書記載對被告科刑範圍之意見，並敘明理由」，當更能達成審慎監督法院量刑程序，以符罪刑相當原則。

3、司法院則針對前揭議題於本院113年6月3日辦理座談前書面說明重點如下：

（1）憲法第80條明定：「法官須超出黨派以外，依據法律獨立審判，不受任何干涉」，因此法院審理具體訴訟案件，是由承辦法官根據調查所得的卷證資料，依據法律，並遵循論理法則與經驗法則，本於確信，獨立判斷。。

（2）為增進量刑及定執行刑之妥適性，司法院業已訂定「刑事案件量刑及定執行刑參考要點」，提供法官可資參考之具體審酌事項。

（3）司法院為提升量刑之妥適性，適當發揮刑罰之功能，擬具「刑事案件妥適量刑法草案」，研議未來設立「刑事案件量刑準則委員會」（簡稱「量準會」），並由量準會制定「刑事案件量刑準則」（簡稱「量刑準則」），法官若依照量刑準則所劃定之各項量刑因子及刑度分布區間而為量刑，將可減少量刑歧異過大之問題，並有助於提升量刑結果之透明及公正。

（4）前揭草案司法院業於110年12月14日第198次院會通過，並於同年12月22日以院台廳刑二字第1100036472號函請立法院審議。惟因113年立法院改選，前揭草案審查屆期不連續，司法院刻正續為研議妥適量刑之相關法制。

(四)最後有關司法行政面部分，本調查研究蒐整英國打詐政策涉及司法行政面之推動方向，包括「偵審全生命週期之評估」、「增加法官員額」、「詐欺專業法庭」等等，均為我國目前所無，至於是否有其可行

性，有待行政院研擬「打詐綱領2.0」時酌予評估。

1、英國於2023年6月公布之打詐策略(Fraud Strategy: stopping scams and protecting the public)涉及司法行政面之措施。

（1）對詐欺案件偵審的全生命週期進行全面評估，利用證據庫增加此類案件的處理數量和速度。

（2）政府連續第二年取消刑事法院開庭總天數的限制，另在各個轄區招聘約1,000名法官，至2025年總共將招募約2,000名新法官。

（3）審理詐欺案件的法官和治安法官在司法學院接受專門訓練。這種訓練會定期進行審查，確保法院系統能夠應對詐欺和不斷變化的犯罪性質所帶來的獨特挑戰。

2、本院諮詢國立中正大學犯罪防治學系許華孚教授則認為「在美國有毒品法庭、家庭暴力法庭、精神障礙犯罪法庭等，所以我認為可不可以成立一個專門打詐的法庭，然後速審速決，我覺得這是刻不容緩的。」。

3、法務部則說明，基於提升專業性及效率，司法院賡續於民、刑事庭設置各類專業法庭。有關詐欺案件是否需成立專業法庭，宜審慎評估相關案件所涉之罪嫌、審理程序及專業性需求，是否有別於其他未以專庭審理之刑事案件，並應考量各地院之人力資源分配狀況。此涉及司法行政，法務部尊重司法院之意見。

(五)綜上，在完成「打詐新四法」之修法後，確為我國打詐、乃至懲詐相關法制建立重要里程碑，而基於獨立審判及各國司法制度不同，本調查研究所蒐整之意見係提供參考，仍有賴司法院及法務部自行評估妥處。

九、經歸納相關研究及經驗，在政府強化管制力道後，詐欺犯罪仍將試圖開發嶄新模式持續製造犯罪機會，本調查研究研判詐騙集團轉型方向，首先是收買電信、金融及司法檢警人員與律師，其次是電信、網路或金流人頭法人化，最後是逐步開始運用人工智慧及深偽技術，政府允宜提前擬定對策，以收防微杜漸之效。

(一)根據本調查研究蒐整文獻[58]指出「跨境詐欺集團隨著國家金融及刑事政策的轉變而有不同應對之道，甚至不斷研發創新技術，挑戰司法機關判決基準、偵查單位辦案能力，測試各國刑罰制度及容忍力，並掌握法律程序及證據能力上數位證據的漏洞，持續走在刑事司法單位前方，讓偵查體系疲於追趕。」等語顯示，縱使政府進行強力而完整的規管，詐欺犯罪仍無法根絕而順應社會演進伺機成長；此由詐欺犯罪曾於97、98年大力掃蕩後趨緩，又因獲得犯罪機會及成熟之主客觀條件，於111年、112年再度快速成長可以佐證。為此，本調查研究認為，政府若無法於犯罪機會出現端倪時開始研謀對策，詐欺犯罪勢將隨社會或技術演進而呈現週期性之爆發。

(二)經本調查研究蒐整文獻資料、機關說明及諮詢專家學者，可歸納出近期或未來詐欺犯罪所可能獲得之犯罪機會，包括「勾結各打詐環節關鍵人員」、「電信、網路或金流人頭法人化」以及「逐步開始運用人工智慧及深偽技術」，茲分陳如下。

(三)「勾結各打詐環節關鍵人員」部分，在近兩年已陸續出現電信、金融及司法檢警人員與律師為詐欺集團吸收之案例，甚至出現被害人、被告、起訴檢察

---

[58] 曾雅芬(民105) 行騙天下：臺灣跨境電信詐欺犯罪網絡之分析。國立政治大學國家發展研究所博士論文

官及涉嫌協助藏錢之法官均曾為大學室友之荒謬案情[59]，基於政府機關、電信及金融機構之薪資與詐騙集團獲利差距極鉅，收買將是詐騙集團極具破壞力之反偵查手段，而成為整體打詐措施尚未受控之風險。

1、金門地檢署施家榮主任檢察官：再來說律師涉案、銀行人員幫忙調整轉帳上限、派出所所長查個資、通傳會前委員當二類電信業者顧問這些，為什麼?因為你永遠查不到他的心臟，那他就可以經驗傳承，越教越多人，他獲利高風險低。

2、臺北地檢署姜長志檢察官：我必須講有些不肖的律師已經在幫詐騙集團做串證的動作，我們目前手上已經有相關的資料在處理。

3、文獻[60]指出，幕後金主包含各界人士，黑道大哥、台商、演藝人員、政治人物、民意代表、情治單位人員或部分國內外執法人員等，大多與黑道有掛勾。

4、對本項潛在之犯罪機會，行政院函轉權責機關說明如下，惟均屬目前既有之機制，且未針對律師部分提出對策，恐成為未來打詐環節之破口，尚賴政府重視。

（1）關於檢察官的究責或監督考核機制，依法官法規定，概分有內部監督及外部監督機制，內部監督機制有「首長職務監督權」，外部監督機制則有「檢察官個案評鑑制度」、「監察院的彈劾」及「職務法庭的懲戒」機制。

---

[59] 涉案人都室友！法官協詐騙集團藏3百萬　「超諷刺舊合照」流出（https://news.tvbs.com.tw/local/2486512）

[60] 曾雅芬(民105) 行騙天下：臺灣跨境電信詐欺犯罪網絡之分析。國立政治大學國家發展研究所博士論文

（2）法務部透過內部及外部監督機制，若查有不法，絕不寬貸，以貫徹對檢察官品德操守的嚴格要求，並維護民眾對司法之信心。

（3）警政署針對是類破壞民眾信任之案件至為重視，除針對違法人員涉案情節持續刨根溯源並依法究辦外，並飭請各所屬機關依公務人員考績法、警察人員人事條例，針對違法人員即時予以記二大過與免職處分，並追究相關人員考核監督不周責任。

（4）此外，為防止員警不當使用警政資訊系統查詢資料，警政署訂有相關使用管理作業規定及稽核制度，不定期實施專案清查，發掘員警疑似異常查詢徵候，並從嚴究責，且為強化警政資訊系統稽核制度，有效防杜各項漏洞及避免衍生不法弊端。

5、小結：在「勾結各打詐環節關鍵人員」之潛在犯罪機會方面，政府似乎尚無研擬對策，推測詐騙集團將擴大利用本項漏洞。

（四）「電信、網路或金流人頭由自然人轉向法人化」部分，茲將本院諮詢專家意見摘錄如下，顯示由金融第一線觀察，已開始出現法人化之端倪；復對照「堵詐」面屢傳MNO及MVNO電信業者浮濫核配門號予法人公司之案件，顯示詐騙集團在人頭門號及帳戶方面已開始由自然人轉向法人化，若此趨勢不予防堵，將使「洗錢防制法」對於無正常理由提供帳戶之修法無效化，而無法壓制人頭帳戶之增長，復對照行政院及經濟部之回應，政府雖有研擬輕度規管措施，惟仍建議政府持續關注相關案情樣態並滾動檢討。

1、諮詢專家意見如下：

（1）臺灣以經濟立國，所以很重視公司發展，現在有86萬間公司但有四分之一都是假公司，所以我預測從明年開始所有的人頭帳戶會轉到法人戶，因為現在金融機構，現在全都在防個人戶。

（2）個人戶現在慢慢減少，那我們每天都在看嘛，現在全部都是法人，他們都去收購歇業的公司，那歇業的公司都沒有人管，因為經濟部也沒有任何的查核。

2、行政院回應：

（1）防杜是類情形發生，金管會業於打詐新四法之詐欺犯罪危害防制條例內納入身分強化辨識機制，針對疑似涉及詐欺犯罪之異常存款帳戶、電子支付帳戶、信用卡或虛擬資產帳號強化確認客戶身分，並得採取對客戶身分持續審查，以利對於疑似涉及詐欺犯罪之異常帳戶、信用卡及虛擬資產帳號有一致性之規範。

（2）另考量犯罪集團可能利用人頭公司大量申辦用戶號碼或電信服務從事詐騙，並透過成立不同法人、非法人團體、商號規避申請電信服務之身分核對措施，通傳會業於打詐新四法之詐欺犯罪危害防制條例中納入相關規範，針對曾受停話、斷話之法人、非法人團體、商號之代表人，於一定期間內再向電信事業以不同法人、非法人團體、商號名義申請電信服務時，應受申請用戶號碼及電信服務之數量限制。

3、經濟部則回應：

（1）按公司登記主管機關對於設立(變更)登記之申請，如公司所提出之申請書件審核符合公司法之規定，即應准予登記。關於同一人設立多家公司，公司法並無限制。

（2）有關二家以上之公司登記於同一地址一節，公司法亦無禁止之規定，惟於申請登記時，須依公司登記辦法規定，檢送登記地址之「建物所有權人同意書」及「所有權證明文件」供審查，且應以戶政機關編訂之門牌為依歸，並非可由公司任意登記門牌號碼。

（3）另查美國之「企業透明法」與英國之「經濟犯罪與企業透明法」均係企業申報對公司有實質控制權、擔任董事等資訊之相關規範，尚非用以規範或限制同一人申設多家公司或同一地址登記多家公司，併為敘明。

（五）「逐步開始運用人工智慧及深偽技術」部分，GASA及英國政府亦均提出相關憂慮，隨著人工智慧及深偽技術之技術門檻及取得成本將逐漸降低，預期詐騙集團將開始採用相關技術，其用途十分廣泛，不僅在偽冒身分騙取金錢，也可能夠透過偽冒ChatGPT應用App收集個人資料，造成個資外洩，亦可用於駭入資訊系統等；政府雖然已開始因應，然而人工智慧可能涉及之層面太廣，未來仍恐成為打詐之棘手問題，本調查研究建議政府宜考慮積極推動諸如「AI基本法」之基礎法制工作，以因應廣泛威脅。

1、GASA在2023年11月在臺灣辦理亞洲防詐高峰會（Anti-Scam Asia Summit，ASAS），邀請多位講者均提及AI詐騙之風險：

（1）從2019年就看到，Deepfake技術門檻開始有大幅降低情況，甚至首起AI軟體偽裝老闆聲音指示匯錢的案例。

（2）現場講者更直接示範運用AI技術建立假網路拍賣網站以騙取個資及施行購物詐騙。

2、英國反詐網領則指出，ChatGPT等新型人工智慧大型語言模型和巧妙的機器學習工具的出現，使詐騙集團能夠更有針對性地進行詐騙。

3、對於人工智慧及深偽技術前在之威脅，行政院表示：

（1）經分析近期涉及AI與深層偽造技術影音之刑事案件，以妨害名譽為主要案類，尚無發現應用於詐騙案件之實際案例，惟為因應處置深度偽造影音案件，警政署刑事局業自111年10月起陸續採購荷蘭及美國商用數位鑑識軟體，如各警察機關受理涉及深度偽造假影音內容之刑事案件，可依將證物送交警政署刑事局檢測真偽，以利後續溯源偵辦，未來除持續更新購置最新數位影音鑑識技術與軟體，及加強員警教育訓練外，如經檢測確認屬假影音案件，亦將主動發布新聞強化宣導，避免更多民眾誤信。

（2）數發部就目前遭遇AI或Deepfake詐騙之案例情形及趨勢，主要是集中在假冒名人或投資專家，透過網路平臺或社群媒體，向受害者推銷虛假投資商品或服務。

（3）針對投資廣告或假冒名人部分，已由金管會修正《證券投資信託及顧問法》第70條之1，針對不法投資廣告進行規範，要求刊登社群平臺之投資廣告必須要實名制。

（4）另在詐欺犯罪危害防制條例中，亦針對網路廣告業者刊登廣告部分，必須進行實質內容審查及廣告主、出資者身分確認及實名制。

（5）數發部將於近期建構「打詐通報查詢網」，讓民眾可以透過此一網站進行網址是否為詐騙網址，未來系統將以AI技術對抗詐騙AI生成訊息。

（6）近期偵辦具體個案包括調查局高雄市調查處於花蓮縣偵破電信詐欺機房案：該案係「以AI深偽技術假扮大陸公安之大型電信詐欺機房」案件。

(六)綜上，本調查研究初步觀察「勾結各打詐環節關鍵人員」、「電信、網路或金流人頭法人化」以及「逐步開始運用人工智慧及深偽技術」將成為詐騙集團躲避政府規管及查緝之可能轉型方向；其中「電信、網路或金流人頭法人化」以及「逐步開始運用人工智慧及深偽技術」兩項雖然尚待持續滾動檢討，然政府已有相關之問題意識；但在「勾結各打詐環節關鍵人員」方面，政府似顯束手無策，恐成為未來打詐環節中相對薄弱之一環，允宜提前研謀善策妥處，以收防微杜漸之效。

十、由於電信網路詐欺為世界趨勢且組織分散遍布全球，國際互助及合作較過去更顯重要，政府在外交艱困情形下仍努力簽訂司法互助協議、深化交流及增派常駐或臨時聯絡官等，112年更成功爭取主辦全球反詐聯盟在臺灣辦理，足見我國在資通訊產業發達及公私協力無間之優勢，爰政府宜善用此一優勢，爭取更多國際合作機會，以突破詐欺犯罪利用國際隔閡所製造之偵查斷點。

(一)本調查研究蒐整之多數文獻均將電信網路詐欺集團描述為全球化且以弱連結達成各司其職效果之犯罪集團，其分工描繪如下圖7，並有研究並透過個案分析，對於詐騙集團之空間及社會分工有詳細描述，並點出「跨境電信詐欺犯罪的查緝常會產生司法管轄權競合的問題。依照領域原則，電信詐欺集團的詐欺行為在當地國並無受害者，且並未觸犯當地法律，頂多以違反電信法相關法條處分」之問題：

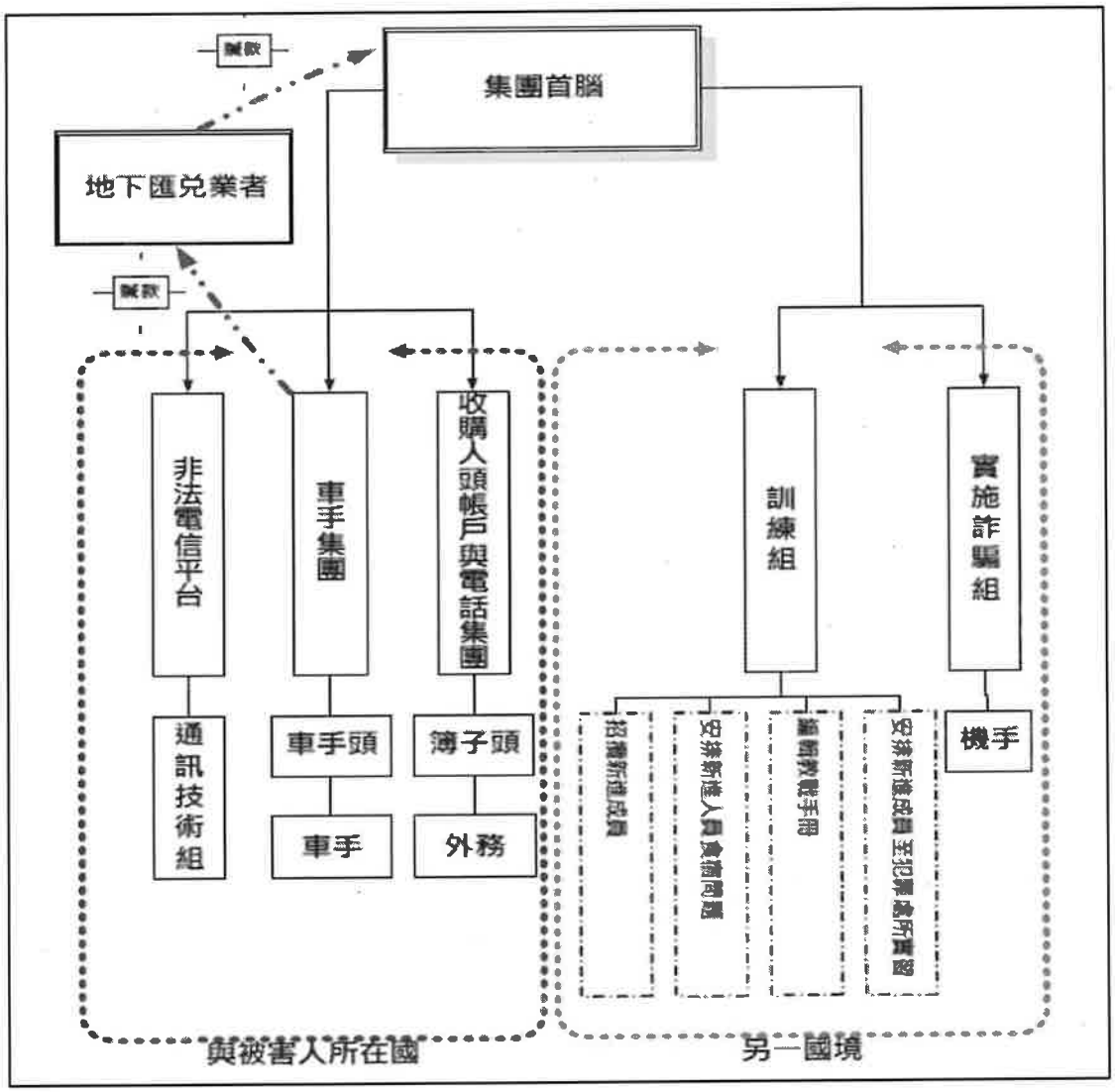

圖7　跨國電信網路詐騙集團分工圖。(資料來源：本院蒐整文獻[61])

(二)詐欺集團空間分析發現可分為幕後首腦、招募組、電話機房、洗錢機房、車手集團、系統機台等[62]；除最底層之車手集團及招募組以外，其餘部門流竄世界各地，利用網路無國界之特性規避國內之規管及查緝。

---

[61] 曾雅芬(民105) 行騙天下：臺灣跨境電信詐欺犯罪網絡之分析。國立政治大學國家發展研究所博士論文。引用李宏倫（2009)。跨國電信詐欺發展趨勢。刑事雙月刊，第32期，頁21。

[62] 曾雅芬(民105) 行騙天下：臺灣跨境電信詐欺犯罪網絡之分析。國立政治大學國家發展研究所博士論文。

1、幕後首腦通常隱匿行蹤在各地流竄。

2、招募組大多在集團成員所在國家，例如在兩岸招募兩岸成員或泰籍、越籍外勞，或在韓、泰、越招募該國成員。

3、電話機房據點早期在兩岸，後移至其他國家，只要可拉網路線的地方，不限大都市、偏遠鄉下或觀光景點。

4、洗錢機房（轉帳中心）：早期多在兩岸，後因金融科技發達，透過網路銀行或轉帳匯款，則無需限於同一國家。

5、車手集團：臺灣多在車手居住地以外縣市、偏僻鄉鎮或工業區等人煙稀少地區的便利商店取款

6、系統機台：所形成的網路跳板則遍布全球各大洲，系統商利用遠端操控可在國內控制，通常一次設定10～20個伺服器據點，偵查機關查到最後三個即出現警示，可立即逃跑，較難查獲。

(三)GASA在2022年提出之報告對於國際合作有以下建議，而我國亦由民間企業成功爭取GASA於2023年11月在臺灣辦理亞洲防詐高峰會（Anti-Scam Asia Summit，ASAS)；邀請到聯邦調查局(Federal Bureau Investigation,FBI)網路犯罪投訴中心（Internet Crimime Complaint Center,IC3）擔任主管的Donna Gregory出席，國內則由資安院、高檢署及調查局等派員出席，向國際分享我國查緝電信網路詐欺之經驗。

1、應建立全球共享的詐騙情資系統，包括網域、電子郵件地址、加密貨幣地址和銀行帳戶等信息，這些資料不僅能幫助消費者檢視風險，還能用於主動封鎖或移除犯罪所得資產

2、新加坡警方表示，90%的詐騙源自海外，並將詐騙

者描述為聯合組織、資源豐富且技術先進，案件很難偵破，其偵查和起訴的成敗取決於國際司法的互助程度。

(四)另據本院諮詢學者專家意見表示，駐外執法人員的派駐與破案率有正相關，因此，本調查研究建議內政部應與外交部協調評估增派駐外執法人員。

(五)根據警政署說明現行打擊跨境犯罪之機制如下，目前我國已有駐外警察聯絡官及任務型聯絡官等執行打詐相關勤務，同時可透過日本獲悉國際刑警組織情資，亦有部分打擊跨國犯罪協議，顯示政府已有基本功能之國際合作機制，但挑戰與困境也相當嚴峻，包括索資(境外犯罪資料)、情資時效性及合作意願等，甚至多種文獻指出詐欺集團與當地政府及機構有所勾結，進一步增加偵查難度，有待政府持續努力克服。

1、警政署目前國際合作概況如下：

(1) 設置駐外警察聯絡官：警政署迄今在美東(華府)、美西(洛杉磯)、南非、印尼、馬來西亞、泰國、越南、菲律賓、日本、韓國、澳洲、荷蘭及新加坡等12國家(13地區)派駐警察聯絡官，負責情資傳遞交換、分析協處及追緝外逃等工作。

(2) 與國際刑警組織合作：目前我國雖無國際刑警組織會員地位，仍透過日本東京中央局接收總部發出及傳遞與我國有關之加密電郵，與國際刑警組織各國中央局及各國執法機關保持密切互動與各會員國相互協助，推展業務、請求協查等工作。

(3) 遇案派遣任務型警察聯絡官：藉由案件協查、共同偵辦，派遣任務型警察聯絡官赴他國執行

協查蒐證等方式，發展跨國偵查合作機制。

（4）簽署警政合作或共同打擊跨國犯罪協定(議):警政署自92年迄今已陸續和友邦及聯絡官駐在國簽定多項共同打擊犯罪協定及備忘錄，包含臺美「強化預防及打擊重大犯罪合作協定」、臺泰「共同打擊跨國經濟及相關犯罪協議」、臺菲「共同打擊跨國犯罪瞭解備忘錄」等，以及112年5月簽定「駐印尼台北經濟貿易代表處與駐台北印尼經濟貿易代表處共同預防毒品、管制類精神藥物及先驅原料非法販運瞭解備忘錄」，目前積極與友邦各國簽訂共同打擊犯罪協定（議），強化國際協議支持。

2、警政署認為面臨之困境如下：

（1）境外犯罪資料(如網路IP，金流紀錄等)取得不易：現今資通訊發達，金流快速轉移，跨境犯罪瞬息萬變，涉境外IP或帳戶等案件遽增，惟各國法令、司法制度、行政效率與國情不同，調閱資料請求經常受限於上述限制，或需透過司法互助等繁複程序始能調閱(例如：美國、日本)，或因駐在國本身對於相關資料管理不全(例如：東南亞國家)，無法有效調閱，造成案件追查之困難與斷點。

（2）非國際刑警組織之會員國，無法在其所建立之國際執法架構下進行跨國合作：

（3）因陸方阻撓，臺灣持續被排除在國際刑警組織之外，迄今仍未獲授權使用其「I-24/7全球警察通訊系統」等19個犯罪資料庫，致與各國情資交流常無法獲得即時回覆，影響是類案件偵辦，並不利全球合作打擊犯罪。

（4）各國法制不同，合作意願因案而異：由於各國

對於跨境詐欺案件之法律構成要件及國家社會民情等而有相當差異，治安重點也不盡相同，導致各國與臺灣合作意願因案而異，需要依案件繫屬國家來逐一建立合作模式。

3、本院諮詢學者專家對於詐欺集團與當地政府機構勾結情形描述。

（1）公司會打點好軍隊、水電、網路這些東西。

（2）即便他們手上的網域都被封掉，通常也可以直接通知系統商，通常二到三天就會開一批新網域。

(六)綜上，國際合作在所有打詐環節中，屬於較難透由政府本身積極處理即可解決之議題，此為臺灣特有之挑戰，政府在官方管道經營困難之情形下，建議繼續加強非官方之合作管道；此外，臺灣基於資通訊產業發達、資通安全環境特殊及公私協力無間，向受國際矚目，此由臺灣近年密集主辦相關國際會議及大型資通訊產業展覽可證，爰本調查研究建議政府應善用此一優勢，以另闢國際合作反詐之蹊徑。