目次

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。----------146

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

表目次

圖目次

監察院112年度通案性案件調查研究報告

題目：政府防制電信網路詐欺之對策與檢討

壹、通案調查研究主旨

一、研究緣起：

(一)依據臺灣高等檢察署(下稱高檢署)資料顯示，民國(下同)108年以前我國電信、網路詐欺案件，每年新收件數均低於35,000件，新收人數亦低於51,000人，然至109年起，電信、網路詐欺案件及人數即明顯成長，新收件數由108年34,947件逐年成長至112年之229,711件，5年間新收件數增加194,764件，成長657%；另新收人數則由108年之50,560人，成長至111年190,493人，增加139,933人，成長亦高達276.77%，且依據內政部統計顯示111年國人因全般詐欺財損金額達新臺幣(下同)73.3億元，顯示詐欺集團透過電信、網路詐欺已嚴重損及國人財產，成為國安危機。政府相關因應對策及其執行成效如何，均值得本院深入調查研究。

(二)本院陳菊院長於112年12月18日率領全體監察委員巡察行政院[1]時，對時任行政院陳建仁院長指出，目前行政機關對於電商個資外洩嚴重、虛擬通貨成為洗錢管道、通訊軟體成為犯罪工具等偵辦困境迄無有效改善對策。本院對於國內外所發生的詐騙案也依職權進行調查，並促請行政院應督導所屬機關提出對策；並強調希望能透過兩院共同合作，對於境內

[1] 監察院新聞稿。監察院院長陳菊率監察委員巡察行政院 提出多項社會關注議題意見 並建議檢討修正61項法規(https://www.cy.gov.tw/News_Content.aspx?n=792&s=27484)

外求職詐騙案件調查建議事項及早研修配套法令，並建立跨部會合作平臺及專責窗口，挹注相關犯罪偵防人力資源，儘速完備處理機制，以符合國際人權潮流與憲法基本國策，保障國人生命財產及人身安全。

(三)此外，本院自98年起陸續就電信網路詐欺相關情事辦理7件調查案件，並對政府打擊電信網路詐欺提出多項調查意見，請政府相關主管機關確實檢討改進。政府近年亦將打擊詐欺犯罪列為治安重點，然國內電信網路詐欺情事並未有效減少，機關對本院所提調查意見部分亦未澈底改善。為此，行政院嗣於111年7月15日函頒「新世代打擊詐欺策略行動綱領」(下稱打詐綱領1.0版)，透過跨部會合作共同打擊詐欺。又為澈底解決詐欺犯罪現存問題，強化打擊電信、網路詐欺之能力，行政院於112年2月20日再推動升級新世代打擊詐欺策略行動綱領1.5版(下稱打詐綱領1.5版)，相關「打詐五法」及「打詐新四法」亦陸續積極研議修訂(迄至113年7月16日已獲立院三讀通過[2])。如何避免電信網路詐欺持續猖獗，政府相關改革措施是否得以確保國人生命財產安全，實有進行系統性、通案性研究調查之必要。

二、研究目的：

根據打詐綱領1.0版，內政部警政署(下稱警政署)已於105年整合刑事警察局(下稱刑事局)等相關業務單位成立「打擊詐欺犯罪中心」，全力推展跨部會、跨機關及跨領域合作，共同打擊詐欺犯罪；數據也顯示106至110年電信網路詐欺案件發生數及全般詐欺財損

[2] 行政院新聞稿。113年7月16日。行政、司法、立法三院合作 共同為國家打詐法制建立新里程碑。

金額朝向穩定控制趨勢；然而在110年COVID-19疫情期間詐欺犯罪情勢轉趨惡化，因此政府於111年7月15日推出打詐綱領1.0版試圖予以防制。

然而，在打詐綱領1.0版實施近8個月後，詐欺案件發生數及財損金額仍持續高發，顯然打詐綱領1.0版所列措施未能有效打擊電信網路詐欺犯罪，以致成效有限；為此，政府再度檢討打詐措施並於112年6月9日推出「打詐綱領1.5版」;同時推動涉及許多部會之「打詐五法」及「打詐新四法」修法；換言之，政府竟在一年內兩度全面升級政策強度，並於短期之內檢討高達九部法令，此在施政措施中洵屬罕見，除顯示問題之嚴重性之外，更與政府期待之打詐效果有所落差，其原因殊值深入探究。

迄至113年5月，打詐綱領1.5版已實施近一年之際，行政院仍坦承詐欺案件還在高發時期[3]，外界質疑政府打詐政策之聲浪不斷，而直接面對網路詐欺犯罪偵查之基層檢察官亦對上游法令及政策提出建言，顯然縱經政府積極檢討，其政策成效仍未充分彰顯。爰此，本調查研究亟欲透過文獻盤點、機關調卷、專家學者諮詢及實地履勘等研究方法，先對國際趨勢及法制進行了解，接著對詐騙集團之組織及特性如何利用政府治理漏洞詐騙國人，進而嘗試提出政府措施不能充分奏效之原因，包括所潛藏之政府善治各層面之問題，以提供政府施政參考。

具體而言，本調查研究將運用監察職權取得其他多數研究不易獲得之資料，並以之探討我國電信、網路詐欺逐年增加之情形及其對整體社會環境之影響外，亦一併瞭解現行法令與政策對於電信、網路詐欺案件

[3] 行政院新聞稿。113年5月9日。「打詐綱領1.5」執行成效與策進。

之犯罪型態與技術演化之防制是否足夠，並檢討相關政策執行成效，促使相關機關積極面對問題，解決政策盲點，強化對於國人生命及財產安全之保障。

三、研究範疇：

本調查研究範疇之界定參考「打詐綱領1.5版」將反制措施概分為「識詐」(防詐騙)、「堵詐」(毀工具)、「阻詐」(擋金流)及「懲詐」(清集團)等四大面向，凡涉及該四大面向之內容均屬本調查研究範疇；至於研究對象範疇，則基於本院職權行使對象之規範，以機關為調查研究主體。爰本調查研究主要範疇如次：

(一)我國電信網路詐欺案件歷年趨勢與現況。

(二)電信網路詐欺案件犯罪態樣與技術演化之關聯性。

(三)我國防制電信網路詐欺案件相關政策及法令規範。

(四)政府對於防制電信網路詐欺案件對策及執行成效。

(五)其他國家防制電信網路詐欺案件概況及相關規範。

(六)其他調查中發現之相關問題。

貳、問題背景

為達成調查研究目的，本調查研究先對電信網路詐欺之實施者—詐騙集團之組織、特性及社會網絡有相當解構及認知；此外，在政策及問題研析前，亦須針對詐騙集團、政府及民眾三方所處之數位化、網路化及全球化環境彼此之互動關聯提出背景概況，始能對於詐騙樣態或治理漏洞進行演繹或歸納；另為取得調查研究內涵之比較及參照基準，問題背景亦須涵括先進國家對於電信網路詐騙之認知、趨勢、治理及政策等。

一、犯罪條件的形成背景：「打詐綱領1.5版」開宗明義指出，隨著電信、網路之自由化與全球金融交易多元化，詐欺集團利用資、通訊科技發達及金融便利性，不斷衍生新型態之詐欺手法，造成詐欺事件氾濫猖獗，亦有文獻[4]指出1990年代國內金融體制陸續開放，加上1996年1月16日電信法修正通過，促使詐欺犯罪更加興盛蔓延；就宏觀角度而言，前揭現象均為近年來數位化、網路化及全球化之浪潮所產生，然而該等論述尚無量化數據佐證，爰本調查研究先就國人數位化、網路化及全球化之進程綜整[5]如下：

(一)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。

(二)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成反比，年齡愈低則社群媒體使用率則越高。18-29歲年齡層為社群媒體使用

[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。博士論文；國立政治大學國家發展研究所。

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

率最高的族群，高達95.98%。而30-39歲年齡層的社群媒體使用率也在九成以上，達94.84%。

(三)在通訊軟體部分，調查結果顯示LINE是臺灣民眾最常的即時通訊軟體，占77.56%，以懸殊的占比大幅領先其他的即時通訊軟體。

(四)2023年臺灣民眾的上網率為84.67%，18至49歲族群更高達95%。

(五)而國家通訊傳播委員會(下稱通傳會)「112年通訊傳播市場報告」[6]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%。

(六)網路金融服務應用的使用情形，如行動支付使用、持有加密貨幣的比率，持續呈現成長趨勢。

二、電信網路詐騙集團組織：詐騙集團由早期以金光黨面對面現金模式行騙，演變至利用電話、簡訊及ATM轉帳，晚近則大量利用社群平臺、境外來電、網銀、虛擬貨幣等工具，詐騙集團之組織及運作模式也隨著技術及社會變遷而調整適應，迄至105年左右之跨境電信網路詐騙集團，已發展出一套高效運作並充滿查緝斷點之組織架構。

(一)詐騙集團組織分工結構層級分明，不易一網打盡，影響偵查能量：

1、詐騙集團採行層級管理、分工細密，組織結構一般劃分為金主及幕後首腦、核心管理幹部、話務機房、系統商、轉帳水房、車手集團、組織結構完整，且因加入管理要素，使該犯罪組織更具效率。各節點間彼此均透過通訊軟體代號方式聯繫，亟難掌握成員間真實身分，易致警方查緝溯源中遭遇層

[6] 通傳會。112年12月。112年通訊傳播市場報告。

層斷點，鮮少查獲幕後首腦偵破整團犯罪組織。

2、針對躲避境外之詐騙集團，檢警調調閱金融機構金流交易明細回復時間冗長，且回復資料格式不一，彙整作業亦須花費大量人力及時間，形成查緝斷點，影響案件偵辦效能。

(二)詐欺集團之管理與斷點：

1、依曾雅芬[7]之研究，詐欺集團核心組人員屬於強連帶關係，各組成員則屬弱連帶關係，分散合作的各組或各集團之間形成結構洞，第三方則屬橋的連接角色（搭橋者）。

（1）首先是由遠離犯罪者及被害者國家的第三地據點電話組分成三線，透過其他第三地國家的網路跳板平臺連結網路電話，依序對被害者實施詐騙，被害者再依指示將金額匯入指定的第一層人頭帳戶。(聯絡工具包括實體易付卡電話、特殊手機及網路電話或通訊軟體(Skype、LINE、QQ)，分別有不同的取向，所有聯繫工具的使用均是為了形成斷點及躲避查緝。

（2）洗錢機房人員透過網路銀行將大帳戶中的詐騙金額分散轉帳至數個小帳戶，再通知車手集團派數名車手持多張提款卡到自動提款機提款，再存入第二層人頭帳戶由洗錢機房轉帳至第三層人頭帳戶，或由車手頭將提領現金繳交給集團帳房或會計。

（3）集團帳房、會計直接分帳或透過地下匯兌換匯給海外的各大類組負責人，並將帳本及規定成數繳交幕後首腦以核對所得。

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

（4）此種運作流程的關鍵點即在於不斷切割、設立斷點，主要採用切割連結及人海戰術模式，包括人員交流、電信流（通話紀錄）及現金流（轉帳紀錄）；第三方（找人、找地中介者）在過程中，則形同斷點機制。

(三)詐欺集團組織架構：

詐欺集團組織架構參採曾雅芬研究[8]分為前置作業、國外作業、金流作業、電話作業及首腦核心等5大類，詳圖1：

[8] 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。

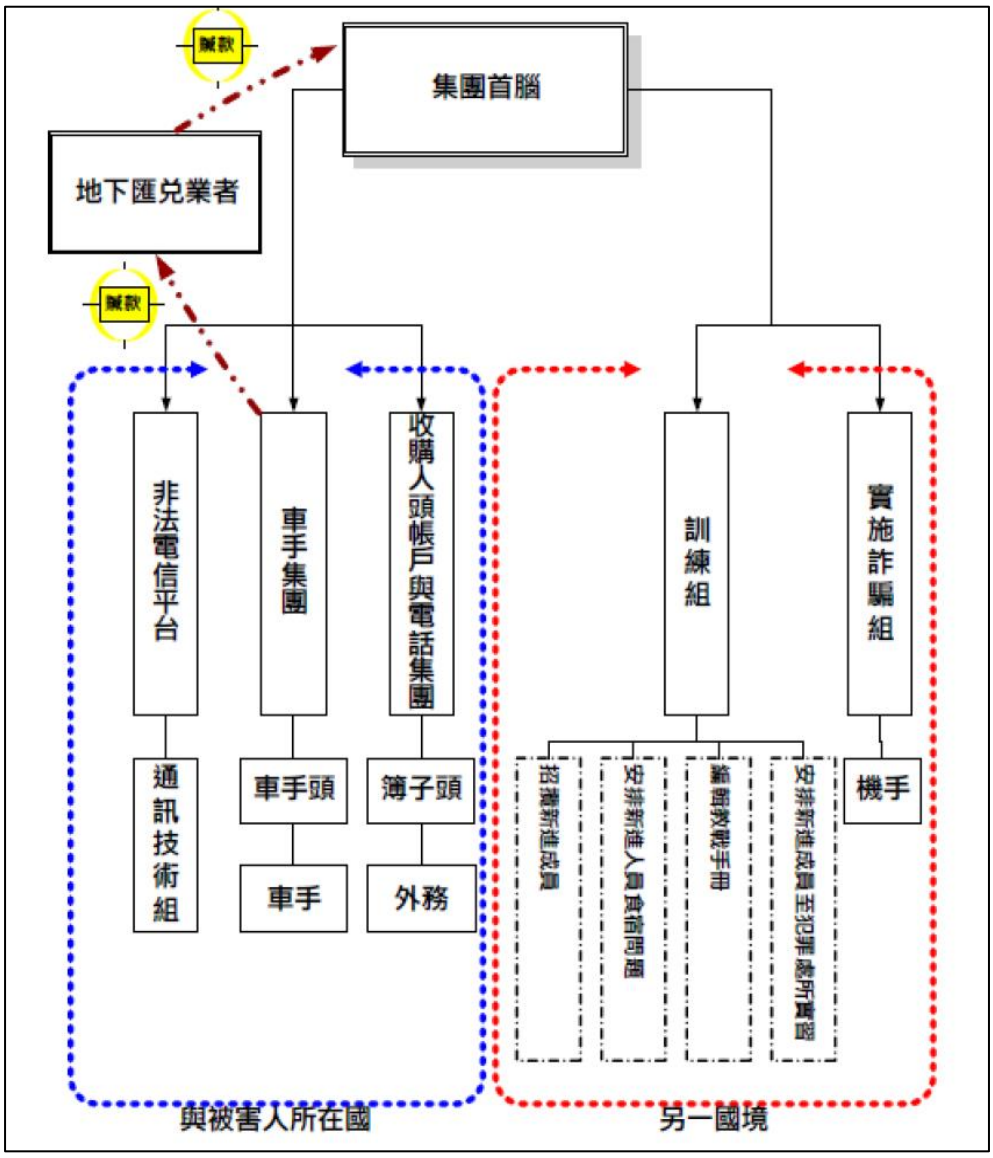

圖1　跨國電信網路詐騙集團分工圖。

資料來源：曾雅芬[9]

1、前置組

（1）網路架設人員：

〈1〉電信機房的前置作業主要由老闆、負責人或其他前置作業人員負責聯絡工人架設網路設備，通常與集團成員錯開、無交集。

〈2〉設備主要包括gateway閘道器、網路線。

〈3〉機房內只需以電話線或網路線連接網路，再

[9] 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。

由系統商聯絡機房人員設定電腦及IP虛擬網路分享。

（2）跳板架設人員：

〈1〉主要由系統商、工程師或其他電腦技術較高人員在各國負責設定跳板機臺或網路系統設置。

〈2〉架設網路主要有三種方式：定點發射、點對點橋接、跳板。目前大多使用跳板，架設國外機房進行遠端控制，可分設多點避免同時被查。

（3）系統商：

〈1〉二類電信系統商或網路系統商屬於幕後人員，由老闆負責聯繫，作業繁複，需於機房運作前完成牽線及租線等系統作業。

〈2〉臺灣、據點國家及被害國家均須有合作的系統商，以完成詐騙網路電話的串聯。

〈3〉系統成員最少，一人可負責十多家、甚至二人可負責上百家集團的網路系統。

〈4〉二類電信系統商負責架設電信平臺，提供語音託播封包及帳號密碼，從話務流量可查出上百團機房IP。

〈5〉網路系統商負責以遠端作業操控國外電腦，設定gateway跳板連接、網路電話、維持通話暢通及群發系統，並以skype聯繫電信機房電腦手解決問題。

（4）代理商：負責遠端控制網路平臺的網路商亦稱為代理商，可在任何地方，負責測試網路電話，維持語音通話平穩暢通。

（5）詐騙清冊管道：

〈1〉包括兩岸駭客及其他內部管道：

《1》兩岸駭客盜取大量個人資料，大陸駭臺灣、

臺灣駭大陸再轉賣詐騙集團。

《2》其他內部管道則包括手機通訊行、保險公司、銀行等，任何有留下個人資料的地方，均可買通內部員工取得個資。

《3》集團首腦大多透過認識的中介者介紹兩岸駭客盜取個人資料，或介紹其他機關內部單位的會計、總機或資訊人員以購買被害對象個人資料。

〈2〉找人中介者：

《1》初期主要由老闆負責找人，後期分散制集團大多透過第三方或黑道幫派引薦成員。

《2》「第三方」即未收仲介費的仲介角色，互不認識的集團間共同認識的朋友；負責介紹合作而不牽涉其中，採分工方式形成斷點，避免出事牽連。

2、國外組:國外組人員包括旅行社、翻譯、廚師、司機、在地中介者等，負責國外事務、處理日常庶務及溝通、尋找據點等工作。

3、金流組：金流組包括車手集團、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。金流組工作流程主要如下：

〈1〉電信機房詐騙所得金額全數匯到洗錢機房帳戶，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，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。

〈2〉金流組架構：

《1》地下匯兌公司：

〔1〕又稱「匯水」，大多透過第三方認識詐欺電信集團或車手集團。

〔2〕匯水通常為當地非銀行業的有錢人士、企業公司、珠寶行、銀樓、當鋪業老闆，同時經營地下匯兌，有充分資金不會私吞款項，可換取便宜匯率。

《2》洗錢機房：又稱「水公司、水車、轉帳中心」。洗錢機房人數最少，只需1～2人，屬於大型集團半負責人，上有老闆，下有電話組頭、車手頭、及臺灣帳房。

《3》車手集團：

〔1〕又稱「車公司」；車手又稱「馬仔、外務」；車手負責人統稱為「車手頭或總頭」，負責監督車手、算錢、與洗錢機房報帳。車手所持提款卡帳戶通稱「車子」，帳戶另稱「冰箱」，均有大小之分及多個備用、長期合作。

〔2〕「大車」為洗錢機房使用，包括銀行帳號、網路銀行、提款卡及密碼鎖，「小車」即為一般車手使用的銀行卡。

《4》人頭帳戶管道：車手公司或水公司負責購買或詐騙人頭帳戶，又稱「騙本子」。

4、電話組：又稱電話機房（電信機房、桶子），包括1至3線電話手及電腦手，負責人則另屬核心人員，電話組主要負責打電話實施詐騙等工作。

〈1〉電話機房：又稱「桶子、電信機房」。電話手（機房成員）屬詐欺集團底層人員，類似臨時工，可取代性高。

〈2〉電腦手：大多由三線負責人擔任，是老闆最信任的部屬。電腦手分紅最多，多無前科、學歷不高（大多22歲以下）、專精電腦、較具技術。主要負責操控電腦，進帳時報帳戶，電腦作業

大多上網設定不需其他設備。

5、核心組：核心人員包括老闆、金主、負責人、會計、帳房等，主要負責管控人員及金流。

〈1〉會計：

《1》負責管帳，屬於核心人物、老闆親信親友，有時身兼電腦手利用網路通知車手集團提款。

《2》電話組、車手組及核心組各為三個會計，需互相對帳。工作內容為記錄三線成員每日進帳，每週發薪。

〈2〉負責人：電話機房（桶子）負責人算是管桶的，又稱「桶仔主、握桶仔（台語）」，屬於現場管理人，也是老闆信任的人，分散各地，隨時與首腦聯絡。

〈3〉老闆：

《1》是整個集團最為關鍵的人物，通常具有特定人脈資源，才能找到據點、成員、合作車手及匯水。

《2》部分為黑道堂口老闆，有幫派背景，堂口當頭、會長或堂主，號召旗下小弟組成詐騙集團。

〈4〉金主、股東：幕後金主包含各界人士，大多與黑道有掛勾。金主通常只負責出錢不管理，也有正當行業，金主主要負責撥款投資，請股東負責管理，將自己風險降到最低。

三、電信網路詐欺面貌：將前述犯罪條件形成背景以及詐騙集團高效運作並充滿查緝斷點之組織架構加以串接連結[10]，可形塑出我國民眾所面對之電信網路詐欺面

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

貌，並呈現出政府治理及打詐綱領所欲反制之各式詐騙樣態。

(一)各類型電信網路詐欺案件之手法。

1、假網拍詐騙：

民眾透過臉書、LINE或知名拍賣網站從事網路購物，詐騙集團便利用當前最新款的3C產品、限量球鞋、名牌包或熱門演唱會門票等，以明顯低於市價之價格誘引民眾下單並要求以LINE或Messenger私下交易。等被害人匯款後卻不出貨，且失去聯繫；或以貨到付款方式取貨開箱後，才發現是劣質商品。

2、假投資詐騙：

詐騙集團透過網路社群或交友軟體主動認識被害人，並假借股票、虛擬通貨、期貨、外匯及基金等名義，吸引民眾加入LINE投資群組，初期會先讓民眾小額獲利，再以資金越多獲利越多說詞，引誘民眾加入投資網站或下載APP並投入大量資金，後續再以繳保證金、IP異常等理由拒絕出金，民眾發現帳號遭凍結或網站關閉才發現遭詐。

3、ATM解除分期付款詐騙：

詐騙集團攻擊資安防護不足電子商務平臺或基金會之後臺資料庫，取得民眾的交易紀錄與個資，再假冒商家或基金會與銀行來電，謊稱因設定錯誤，將重複扣款，要求民眾操作ATM、網路銀行或至超商購買遊戲點數進行解除設定。民眾依照指示操作後，發現帳戶餘額減少，才知道上當受騙。

4、假愛情交友：

詐騙集團透過社群網站或交友軟體等管道隨機加好友，並盜用網路上帥哥、美女照片，假冒戰

地軍官、軍醫、服務於聯合國官員，讓民眾誤入情網，再以境外寄送跨境包裹、禮物需要關稅或儲存結婚基金介紹投資管道等方式詐騙民眾匯款，直到遭對方封鎖才知道受騙。

5、猜猜我是誰：

詐騙集團假冒「兒女」、「親戚」或「多年不見的友人」，透過電話或通訊軟體(如LINE)與民眾聯繫，並以換過手機所以不是原來的號碼、暱稱等方式要民眾加入新手機號碼或LINE ID，過幾天後再以臨時急用、投資周轉等理由詐騙民眾匯款，事後民眾聯絡到當事人確認無此事後才知道被騙。

6、假冒機構(公務員)：

詐騙集團假冒健保局、醫院及中華電信或其他公務機關撥打市內電話予民眾，用語音的方式引導被害人轉接客服人員，並以被害人遭冒用身分辦理開戶、請領健保補助或申辦門號為由，主動協助轉接警察機關製作筆錄，另告知涉及洗錢或其他刑事案件，強調偵查不公開勿告知親友，再要求民眾至超商收取傳真或以LINE須傳送法院偽造公文取信被害人，須被害人配合監管帳戶等話術行騙得逞。

7、假求職：

於報章雜誌或網路訊息刊登求職訊息誘騙民眾，再以設定薪資轉帳等名義騙取被害人之金融帳戶及密碼，續遭詐騙集團作為人頭帳戶之用。

(二)若以詐騙集團接觸受害民眾之管道區分，其樣態可分為：

1、釣魚簡訊及電子郵件：詐騙集團發送看似正常發送的簡訊或電子郵件，試圖引誘被害人進一步提供個人資訊、銀行資訊或進行金錢上交易。獲得的

訊息通常被用於冒用身分或詐騙金錢。

2、電話詐騙:詐騙集團可能撥打騷擾電話,聲稱自己是銀行、政府機關或知名企業,以詐欺、威脅等各種話術誘使被害人透露個人資訊或進行轉帳。

3、社交媒體詐騙：詐騙集團可能會利用社交媒體平臺創建虛假帳號,假造或冒充他人身分,試圖與被害人建立信任關係,要求被害人透露個人資訊、進行金融交易或點擊惡意連結，從而造成損失。

(三)詐欺工具隨科技進步不斷演變之情形：

1、電話詐騙:自電話普及至家戶後,即有詐騙集團利用其便利性進行詐騙，偽造各種情境且受話者難以即時查證;在個人手機普及後,詐騙集團可對個人進行針對性的話術詐騙。

2、簡訊詐騙的興起:隨著手機的普及,詐騙集團開始利用簡訊進行詐騙活動，大量發送詐騙簡訊而觸及更多潛在受害者。

3、行動應用程式詐騙：隨著智能手機和行動寬頻的發展，APP也隨之普及，詐騙集團開始利用惡意APP，以竊取用戶個人資訊或進行其他詐騙活動。

4、社交媒體平臺詐騙:社交媒體平臺的興起,使詐騙集團得以創建虛擬身分,以更具細節、更有說服力的方式偽冒個人或機構進行詐騙。

5、新興科技的引進：隨著新興科技如區塊鏈和加密貨幣的發展，金融詐騙的查調複雜度隨之上升。

(四)一般常見電信網路詐騙案件之特徵：

1、緊急情況：詐騙集團常利用緊急情況來引誘被害人做出急迫決定。如聲稱帳號被盜用，需要立即提供個人資訊或轉帳以避免損失。

2、不明來源的通訊：詐騙集團常使用匿名或虛偽的電話號碼、簡訊號碼或電郵位址進行聯絡,對於被

害人來說，通常為不明來源的通訊。

3、不尋常的要求:與詐騙集團不同,真正的機關或企業通常不會在不安全的環境下要求提供敏感資訊。

4、不正常的付款方式：詐騙集團可能要求使用非常規的付款方式,如匯款、虛擬貨幣、禮物卡等，以減少被警調單位發現的風險。

5、不正常的網址或連結：詐騙集團常常會提供惡意的網址或連結，用以竊取個人資訊或安裝惡意軟體。

四、電信網路詐騙集團利用漏洞：詐騙集團之所以能有效利用數位化、網路化及全球化環境衍生前揭諸多詐騙樣態，肇致國人嚴重損失，部分論者已推論恐存在政府防制政策疏漏之虞，茲以「識詐」、「堵詐」、「阻詐」、「懲詐」面向依序整理如下；惟相關推論尚未進一步將政府治理疏漏進行系統性之爬梳：

(一)識詐面:詐欺訊息氾濫與使用者之風險意識[11]。

1、國人有近7成民眾近3個月內從各式管道(含電話、簡訊、線上廣告、網路購物等)遭遇過詐騙訊息，高達67.68%；且有3.71%民眾甚至因而受騙。

2、國人有高達80.99%有信心可以辨別詐騙手法。

3、國人有81.35%遭遇到詐騙情況時，有信心可以知道如何尋求協助。

(二)堵詐面：

1、宅經濟興起與詐欺訊息氾濫：

（1）109年起新冠肺炎疫情（COVID-19）爆發除衝擊國內各項產業獲利，致營利銳減民眾急迫尋求投資機會,且疫情期間民眾生活型態改變,大量

[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」

減少戶外活動，電信、網路使用量大幅增加，居家辦公、網購等宅經濟興起。

（2）詐欺集團利用簡訊、電子郵件、投資詐騙網站等電信、網路社群平臺，大量散布詐欺訊息。

2、個人資料外洩與詐欺之關聯性：

（1）科技的變遷發展改變國人之交易模式及社會互動方式，因辦理例行性事務或進行交易需要，公私部門經常會持有大量個資。詐欺集團除透過駭客侵入、網路釣魚攻擊等方式盜取個人資料外，然握有個人資料之部門，因對個人資料保護未有積極重視，常發生資料外洩之情事，如，蝦皮、誠品生活等業者涉及消費者個資外洩事件，經數位發展部(下稱數發部)分別處以20萬元及10萬元罰鍰。行政院亦指出近年來利用網路遂行個資或資安駭侵犯罪不斷增加之趨勢。

（2）詐欺犯罪之猖獗與民眾個資外洩事件息息相關，如詐欺集團取得個人資料後，將資訊拼湊整合成完整顧客資訊，以竄改電話、假冒商店客服、銀行行員，利用話術降低國人戒心，使其陷入詐騙陷阱中。

3、電信法規與金融法規相較，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[12]。

[12] 反詐綱領1.5版

(三)阻詐面：

1、詐騙手法日新月異，民眾防詐意識及銀行行員協助攔阻能量不足：當前各主要詐欺手法如投資詐欺及假網路拍賣購物等手法日新月異，各類防詐資訊雖經各機關長年大量宣導及媒體反覆報導，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、提醒親友的警覺性，導致遭詐風險提高。

2、網銀遠端身分認證較為鬆散，歹徒利用金融科技便利，如人頭網路帳戶、第三方支付、虛擬通貨，隱匿贓款流向：

（1）詐欺犯罪集團為躲避警方追緝，多使用人頭電話、人頭帳戶以設立偵查斷點，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[13]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%)〕。

（2）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[14]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，後續則結合(高價值)虛擬通貨[15](諸如比特幣、泰達幣)匯至電子錢包隱匿贓款資金

[13] 虛擬帳號：針對付款民眾所建立與指定企業向銀行申請之帳號，可用於分辨每一筆款項之付款來源

[14] 第三方支付：以個人或公司名義申請之代收款服務。

[15] 虛擬通貨 主管機關為因應金融科技創新，核定虛擬通貨為證券交易法所稱之有價證券 。

流向，因無對應之中央目的事業主管機關，導致警方調閱資料不易，殊難追查。

3、詐欺集團常用之洗錢工具已結合虛擬通貨，藉由其具流通性、且可隨時兌現之特性，要求被害人透過虛擬通貨交易所、BTM[16](Bitcoin Teller Machine, BTM)或個人幣商購買虛擬通貨，續匯入犯嫌指定之人頭電子錢包多層移轉，利用去中心化特性隱匿贓款流向，再透過網路進行跨境洗錢並由車手集團取款，以躲避警方查緝〔案例：警政署刑事局於110至111年間破獲多處詐欺水房，均將贓款層轉至虛擬貨幣錢包，以比特幣、泰達幣、乙太幣等於虛擬幣交易所兌現為新臺幣，隱匿贓款流向作為洗錢管道〕。

(四)懲詐面：

1、詐欺犯罪高收益低成本：詐欺集團是有組織、有訓練，且具有專業技能之團體，具有成本低、風險低及獲利高之犯罪特性。

2、詐欺案件量居高不下，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。現在有哪個幫派組織不插手詐欺行業？[17]

3、2010年迄今，政府從波蘭、肯亞、菲律賓等地引渡上百名詐欺犯，最高也僅被判6年，多數共犯更只有數月刑期，加上法官給予緩刑，等於繳罰金就不用被關[18]。

五、本院歷年詐欺相關案件調查摘述：本院依憲法第96條規定，得按行政院及其各部會之工作，分設若干委員

[16] 比特幣自動櫃員機(Bitcoin Automated Teller Machine,下稱MBT)

[17] 本院履勘高檢署，臺北地檢署劉主任檢察官仕國說明。

[18] https://www.cryptocity.tw/How-low-is-the-cost-of-fraud-in-Taiwan。

會，調查一切設施，注意其是否違法或失職，爰此，就電信網路詐欺之對策與檢討，本院長期以監督角度加以關心，具體指出政府治理疏漏，茲將歷年詐欺相關案件調查意見摘述如下：

(一)098司調0040號「據報載：詐騙電話橫行，警政署、法務部調查局(下稱調查局)及相關調查單位，未能有效遏止詐騙案件發生，涉有違失等情乙案」：

1、行政院宣布2004年為反詐騙行動年，並訂定反制詐騙犯罪多項策略目標，迄今非但未能有效達成，且詐騙犯罪案件數量、嫌疑犯及被害人數與民眾損失財產均大幅攀升，顯示多年來未能有效遏阻詐騙犯罪，亟應檢討改進。

2、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[19]、嚇阻、隔離與矯正等功能，行政院與司法院允宜積極謀求改善之道，俾以有效遏阻詐欺犯罪案件蔓延。

(二)098交調0034「據報載：詐騙電話橫行，通傳會、行政院新聞局及教育部，未能有效遏止詐騙案件發生，涉有違失等情乙案」：

1、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及各電信業者聯合查詢機制主管機關之爭議，肇致詐騙集團利用電信通訊媒介詐騙民眾財物，造成嚴重之財產損失，均有不當。

2、行政院新聞局長期怠於執行反詐騙宣導工作，除事前未建立明確之綜合性反詐騙預防宣導工作

[19]應報理論目標在於讓犯罪行為人受到與其犯罪行為相同程度的處罰。

外，事後亦未追蹤考核，難以評估宣導效果，肇致執行成效不彰，均有不當。

3、教育部事前未建立內部反詐騙跨單位分工聯繫平臺，及擬定各級學校宣導目標，事後復未建立客觀完整之考評制度，致各單位各行其事，執行成效不彰，核有不當。

(三)099內調0106「據報載：詐騙電話已成為國人日常生活中之恐怖主義，政府情治、檢調與警政單位竟束手無策，國家安全機制仍未啟動，積極緝拿詐騙集團，相關機關涉有違失等情乙案」：

1、本院鑑於政府機關未能有效遏止詐騙案件發生，於98年調查並糾正以來，相關機關業已檢討並有初步成效，並據中正大學犯罪研究中心針對99年上半年度政府對詐騙犯罪的重視及努力已獲得民眾肯定，惟對於詐騙犯罪之被害比例仍有微幅上升趨勢，行政院仍應積極督促所屬持續積極檢討改進。

2、有關電信人頭資料庫及各電信業者聯合查詢機制之事項自93年迄今，通傳會及警政署各執一詞，究應由何機關負責監督管理責任，仍未解決，行政院實應積極督促相關機關檢討處理。

3、海峽兩岸人民往來頻繁，經貿交流日漸密切，衍生之跨境犯罪日趨猖獗，行政院允宜積極檢討，以建構跨國界、跨區域之「安全聯防」及「共同打擊犯罪」合作機制，藉由兩岸司法互助以有效遏阻詐欺及跨境犯罪現象。

4、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。

(四)106司調0019「部分國人於境外涉及電信詐欺，影響

國際形象甚鉅，且逾8成犯詐欺罪者刑度低於1年，亟待就偵查實務面賡續研謀因應措施；又開放銀聯卡於國內ATM提款，便利大陸民眾於國內消費，惟銀聯卡洗錢事件頻仍，亟待強化兩岸金融監理合作等情案」：

1、部分詐騙手法係以民眾個人資料為基礎，致使民眾不易辨別真偽而被騙；經濟部對網路零售業者之維護個資輔導與檢查成效不彰，行政院作為個人資料保護法所定各目的事業主管機關之上級機關，允應與該法之解釋機關法務部提高非公務機關對於資訊安全及個資維護之重視，並導正部分機關在執行該法之認知偏差。

2、源頭管理在防制電信詐欺策略中值得應用，短效期電信門號管理有助於消弭人頭電話以利追緝詐騙集團行蹤，而提高民眾對詐騙資訊警覺性，即斷絕後續轉帳或交易，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。

3、因應目前詐騙集團型態與常見犯罪模式，相關法令已檢討修正，政府整合打擊電信詐欺跨部會平臺，運用電腦科技並採取新式偵辦方式，允宜賡續充實打擊電信詐欺偵辦能量，維護民眾財產安全及國際形象。

4、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，政府除建立集團成員赴海外可疑名單，即時知會可能入境國之移民機關相關情資外，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，俾免國人遭遣送大陸之情事再發生。

(五)111司調0027「據訴，為各級法院對人頭帳戶詐欺案

件之行為人，論罪標準不一，肇致經濟能力、智識等條件較差者，頻遭羅織入罪，涉有不公等情案」：

1、鑒於提供人頭帳戶者究應否無罪或應成立何罪，司法實務上見解分歧，為正本清源，本院諮詢或座談之專家學者多認應以立法方式解決，法務部目前已提出洗錢防制法之修正草案，其中第15條之1規定：「無正當理由交付金融帳戶予他人，從事第2條所列之行為者(即洗錢行為)，處3年以下有期徒刑。」另有專家學者主張得改為第一次違反科處行政罰，第二次始科處刑罰，惟亦有對改採「先行政罰後刑罰」有疑慮者。以何種立法方式為妥，僅彙整本院諮詢專家學者之意見供立法及權責機關參考。

2、提供人頭帳戶之被告，因被騙匯款至該帳戶之被害人可能分處不同縣市，受理報案之警察機關及偵查之檢察機關亦分屬各地，對該被告而言需到處應訊，如管轄權未統一，對其程序保障有所不足。又有些街友成為人頭帳戶案之被告，因居無定所通常無法收到傳票或拘票致影響其訴訟權益。另曾發生民眾帳戶遺失至警察機關報案卻遭拒絕受理之情形，影響民眾權益，警政署應督導各警察機關不得任意拒絕受理民眾報案。

3、目前民眾至金融機構開辦帳戶雖會嚴謹查證個人身分及開辦用途，且對異常帳戶之風險加以控管，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，具體提醒開戶民眾切勿任意將存摺及提款卡交付他人使用或外流密碼，以免遭詐騙集團不法利用而衍生法律責任。又金管會應加強透過各種管道、方式或與其他機關合作宣導讓人更有感的

案例，使交付帳戶者體會到交付後可能面臨之嚴峻刑事責任及鉅額賠償責任，而更有效地減少人頭帳戶之產生。

4、外籍移工抵達我國後通常會有申辦行動電話、金融帳戶之需求，司法實務上時有發生其所申辦之電話、帳戶被詐騙集團不法利用之案例，移民署於其入境及勞動部於其在我國停留期間應加強對外籍移工以其能理解之語言、文字或圖示加以宣導，以避免其所申辦之電話、帳戶被詐欺集團利用為犯罪工具。又有些街友成為人頭帳戶之被告亦時有所聞，衛生福利部應依權責轉請各地方政府社會局(處)協助加強宣導其所申辦之電話、帳戶勿被詐欺集團不法利用。

(六)111財調0039「據警政署刑事警察局統計，同年1月至7月，投資詐騙案高達2,550件，為前一年同期的1倍，將近9億元財產損失，幾乎是109年全年被詐騙總額。多數投資詐騙集團大打美女牌，透過LINE、Telegram等群組……誘導民眾投資或代操，騙取資金。究政府相關機關有無縱容是類詐騙不斷以臉書等社群媒體、隨機電話方式進行？據悉已有不少被害人受騙，甚至傾家蕩產。臺灣已飽受詐騙之苦，此類新興詐騙方法疑未受政府重視……均有深入瞭解之必要案」：

1、金管會及所屬機關業務職責，本於金融消費者保護及維持金融市場秩序，對於非法之誘人「投資詐騙」之擾亂金融市場秩序行為，亦責無旁貸，需主動積極進行前置之行政查察作為及犯罪資料之蒐整後再行移送偵辦，以發揮政府行政一體及共同打擊犯罪之最大效能，而不能將主管法令具有刑罰之附屬刑法部分，均推諉檢方及司法警察進行偵辦。「投資詐騙」不法態樣多元且方式多樣，其

犯罪構成要件，亦較傳統「電信詐欺」類型，更難認定。另詐騙集團透過網路化、科技化，以綿密之分工及熟練之手法，更利用網路虛擬貨幣洗錢，規避資金追查，查扣犯罪所得更加困難。此異常之交易行為資料，實不難由日常執行有價證券監視作業即得以發覺，稍微用心查證就會發現，但卻未受到政府主管機關之重視。誘使民眾投資之訊息仍氾濫於日常生活中，實有待更積極之作為。

2、嚴重特殊傳染性肺炎疫情期間，各類刑事犯罪案件數顯著降低，惟集團性電信詐騙案件卻不減反增。依警察機關受理電信網路詐騙案件資料統計顯示，108至110年間「投資詐騙」案件成長達3倍有餘。111年上半年「投資詐騙」案件已達1,066件，造成財損的金額亦達673,824千元，均已逾110年全年件數及財損金額之5成，顯見該類犯罪行為迄今未見緩和。爰行政院實應正視前揭情形，督促相關機關落實111年7月間該院核定之「打詐綱領」，以避免「投資詐騙」犯罪行為持續惡化。

3、「防制電信詐欺與網路犯罪工作平臺」於109年7月第9次會議，即決議請各家電信業者比照中華電信股份有限公司(下稱中華電信)做法，當發現民眾接獲+碼異常來電時，即分析並自訂邏輯規則，倘系統判斷為詐騙電話則發送關懷簡訊告知其防止遭騙。惟迄111年4月其他行動電信業者仍未見有明顯配合作為，顯有未洽。另依打詐綱領1.0中，「電信網路面向」之策略六「管理及防制VPN業者詐騙」，已要求通傳會監督電信業者配合執法機關，對疑涉詐騙行為之VPN業者停止續約，以防制詐騙行為，亦應確實落實，以減少「投資詐騙」造成民眾重大財物損失。

4、法務部於107年2月間通令各檢察機關實施「檢察機關以電子公文調取金融資料機制」，法務部允應加速推動，以完善辦理「投資詐騙」案件時，相關犯罪金融資料之取得途徑，提升檢察機關追緝金流之效能。

5、「投資詐騙」行為現已結合比特幣等區塊鏈虛擬貨幣作為金流工具，利用其「去中心化、不易追查」之特性，協助犯罪者快速洗錢，以求得遂其等之犯行。我國檢方及司法警察機關雖已購置區塊鏈分析工具以協助金流分析工作，惟所購置之工具並非完整版本，對治安機關偵辦工作恐有難盡周全之虞。

6、現行金管會針對虛擬貨幣之洗錢防制相關規範，僅要求本國公司幣商依法令遵循之程序進行聲明，規範幅度尚未及於自然人幣商或外國幣商，惟為杜洗錢防制漏洞，容有再加檢討必要。

7、國人常運用之網路社群平臺，且遭「投資詐騙」者利用貼文以實施其犯行者計有近十種，因電信事業及設置公眾電信網路者未有留存相關網路足跡之義務，均造成治安機關查緝時，難以有效溯源追查詐騙網站或駭侵攻擊者之真實身分，亦無法利用對數位足跡之分析，發現或預測可能之受害者以提早防範，以控管整體損害之幅度，爰法務部均應針對前揭問題，謀求改善之道。

8、110年8月間行政院發布聯繫作業要點後，仍持續發生重大個資外洩案件，使詐騙集團有得以取得消費者個人資料，遂行其不法作為之機會，造成民眾財物損失。政府允應持續加強杜絕非公務機關發生個資外洩情事，並宜考量參酌先進國家作法及歐盟立法例，配合行政院組織改造時程，考量規

劃設置個人資料保護獨立專責機關，暨於個人資料保護法未來修法時，一併研議於公務機關及部分非公務機關設置個人資料保護官。

(七)112內調0042「新北市政府警察局日前破獲『臺版柬埔寨』32人求職詐騙集中營，另有3人已死亡，震驚社會……詐騙集團祭出『高薪』、『「保證獲利』等誘餌，誘騙民眾上鉤後再行拘禁、虐待甚至集體強行侵犯，民眾不但淪為詐騙集團的人頭帳戶及行騙工具，重則遭虐打、棄屍。本案嚴重損及人身自由、財產及生命安全，相關機關是否有進行跨部會合作積極提供救援？相關主管機關是否積極查處違法求職廣告及犯罪？目前究竟有多少國人受騙？相關機關如何遏止此類犯罪事件一再發生？均認有調查之必要案」：

1、洗錢囚虐犯罪為電信網路詐欺犯罪高度組織化、跨國化、分工化下衍生的重大犯罪模式。犯罪集團為隱匿詐騙金流，採行令人髮指的殘暴手法。行政院特別針對洗錢囚虐犯罪，研商採取多項查緝及防制措施，確有防制成效，相關辦案人員之辛勞付出，應予肯定。然詐欺犯罪越趨殘暴，洗錢囚虐犯罪方興未艾的趨勢。部分查緝及防制措施未能有效針對網路犯罪特性，欠缺強制力的法源基礎，部分措施有待落實跨部會協調聯繫，且對於電商個資外洩嚴重、虛擬通貨成為洗錢管道、通訊軟體成為犯罪工具等偵辦困境，迄無有效的防制方法，行政院仍應督導相關機關速謀因應措施，以有效壓制詐欺犯罪之氣焰。

2、近年來網路詐騙的情形越形嚴重，且有不少社會弱勢民眾及未成年人誤信社群網路不實訊息，被騙遭到囚禁、被販運出國或成為詐欺共犯，檢警雖

與臉書建立通報下架機制，但整體成效有限。鑑於我國並無單一的數位服務法律，現階段對於網路有害行為或犯罪，係由各法令之主管機關依權責，採分散式立法處理。對於網路異常求職、販賣帳戶及招攬車手等有害訊息及犯罪行為，研議採取適度立法管制的可行性。

3、金管會與警政署已協調建立查詢作業，警政署並將警示帳戶之失蹤人口列為重大刑案，雖有積極作為，但迄未建立失蹤人口與異常金融服務的勾稽平臺。金管會與警政署應積極建立相關勾稽平臺，金管會並宜督導金融機關強化行員識詐阻詐之敏感度，落實控管異常交易態樣及帳戶被作為詐騙使用之審核責任。

六、全球面對詐欺犯罪情勢及反制策略：基於電信網路詐欺犯罪之環境背景為數位化、網路化及全球化，則各國政府面對之犯罪情勢及反制策略，亦為研究電信網路詐欺議題所無法忽略之背景，茲綜整全球電信網路詐欺概況[20]如下：

1、2021年全球共收到約2.93億份詐騙通報，損失金額高達553億美元，相比2020年，通報數量增加了10.2%，損失金額則增長了15.7%。數據顯示，詐騙活動不斷增加，而且主要增長來自投資詐騙。

2、96%的澳洲人過去5年曾遭遇詐騙[21]，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1年接觸過「另類的」投資機會，在英國，有半數電話受訪者表示在1個月內收過疑似詐騙的釣魚信件或社群媒體訊息。

[20] 全球反詐聯盟(GASA)The Global State of Scams Report－2022及2023報告。
[21] 澳洲競爭與消費者委員會(Australian Competition & Consumer Authority)統計。

3、社群媒體成為詐騙者的重要工具。在巴基斯坦，23%的網路犯罪報告源自Facebook，而在美國，2021年有超過1/4的詐騙起源於社群媒體上的廣告、貼文或訊息。

4、巴西移動支付方式Pix導致詐騙激增；沙烏地阿拉伯62%的消費者曾經收到垃圾郵件和詐騙信息，14%的受訪者承認自己上當受騙。

5、投資詐騙持續增加：

（1）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。

（2）加密貨幣大量運用於投資詐騙，土耳其政府被迫暫停加密貨幣交易，凍結超過20億美元的資產。

（3）加拿大投資詐騙是成長最快的樣態，從2020年的501則報案成長至3,442則，財損金額則從1,650萬美元成長至1.64億美元。此外，詐騙集團還會偽冒「詐款追討」公司，進一步欺騙受害者支付管理費。

6、詐欺案件只有3%~17%的受害者通報：

（1）通報詐騙比例方面，澳洲約為13%，加拿大約5%，以色列約9%，荷蘭及法國則約在12%~17%之間，而部分國家已經在將詐騙通報機制中心化。

（2）一些國家開始投資於更便利的報告系統。例如，法國推出了新的網路詐騙報告平臺。比利時、波蘭、紐西蘭和英國等國家則允許市民檢舉轉發可疑郵件和簡訊以便進一步分析和行動。

7、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。

8、經濟損失外，全球範圍內的情感創傷也很嚴重，調查發現59%的受害者表示遭受了巨大的情感創傷。

七、小結：就本調查研究所蒐整之文獻及公開資料，電信網路詐欺犯罪因應近數十年之數位化、網路化及全球化之浪潮，已發展出一套高效運作並充滿查緝斷點之組織架構，而所衍生之詐騙管道、手法及模式，包括投資、網路購物等等，亦針對民眾數位化、網路化及全球化所改變日常生活而設計；並且詐騙集團、政府及民眾三者彼此之關聯及所呈現之犯罪面貌，亦非臺灣所獨有；而回歸本院監督政府之職權所在，文獻雖已有部分論者零星指出電信網路詐欺犯罪涉及政府規管及治理有所疏漏或不完備。然而，目前尚無針對政府反制電信網路詐欺之政策、法規或治理有階段性之通盤檢討，縱以本院過去曾具體指出部分政府違失，仍屬於個案研究或年代過於久遠；為此，本調查研究擬以前述背景為基礎進行調查，以瞭解現行法令與政策對於電信、網路詐欺案件之犯罪型態與技術演化之防制是否足夠，並檢討相關政策執行成效，促使相關機關積極面對問題。

參、研究方法與過程

一、文獻蒐集及盤點：

本案主要係採文獻蒐集、調卷、函詢、邀集有關機關簡報與座談、諮詢專家學者，以及就前述所得資料加以歸納、比較、分析等調查及研究方法，俾歸納整體研究背景。

(一)文獻蒐集部分，蒐集相關法令、專書著作、學術論文等並研閱國內外政府有關電信網路詐欺之資料，以歸納整體研究背景。

1、相關法令：國內法部分，根據法源法律網，行政院、立法院及主責部會之公開資料；國外法部分，包括歐盟數位服務法(DSA,Digital Services Act)、英國線上安全法(Online Safety Act)、學術論文。

2、政府公開資料：國內部分包括打詐綱領1.0版、打詐綱領1.5版、立法院「詐欺犯罪防制立法及各部會打詐機制盤點」公聽會報告、國發會「當前經濟情勢簡報」；國外部份包括英國反詐綱領(Fraud Strategy: stopping scams and protecting the public)，全球反詐聯盟(The Global Anti-Scam Alliance, GASA)「The Global State of Scams Report – 2022」、「The Global State of Scams Report – 2023」。

3、專書著作及學術論文包括:政治大學國發所博士論文「行騙天下：臺灣跨境電信詐欺犯罪網絡之分析。」、中正大學犯罪防治學系碩士論文「從金光黨到跨境電信詐欺詐騙犯罪的理性化決策與福特

主義分工」[22]、逢甲大學公共事務與社會創新研究所碩士論文「新興詐欺犯罪偵查實務與防治策略之研究-以假投資詐欺為例」[23]等。

(二)調卷部分：函請行政院、司法院、內政部、通傳會、金管會、數發部、法務部、經濟部、教育部等，共9個院部機關提出相關說明資料。

二、調查研究過程：

茲將本案採取之調查研究方法、步驟、時程及架構說明如表1：

表1　本案調查研究方法、步驟及實施期程

調查研究方法、步驟	實施期程
一、初步蒐集相關資料並撰擬本案調查研究計畫初稿	112年9月18日至9月30日
二、召開本案調查研究計畫討論會議	112年10月1日至12月31日
三、蒐集、研析參考資料及查詢相關法令規定 (一)蒐集並研閱本院相關調查案件 (二)蒐集並研閱平面媒體、電子媒體相關報導及相關主管機關、單位發布之新聞資料及網站刊載內容 (三)蒐集並研析相關調查、研究及統計報告 (四)蒐集並研析相關專書、學術論文、機關公報、研究報告、出版品及期刊等文獻	112年10月1日至112年12月31日
四、函詢調卷 函請行政院、內政部、通傳會、金管會、數發部、法務部、經濟部、教育部等提出相關說明資料。	112年11月16日、113年4月22日
五、第一場座談及履勘 前往高檢署、警政署刑事警察局辦理座談，以瞭解第一線執法人員執行打擊電信網路詐欺案件所面臨之困境。 履勘165反詐中心，以瞭解政府反詐執行情形。	112年11月13日
六、第一場諮詢	112年12月13日

[22] 童元泓，民111年。從金光黨到跨境電信詐欺詐騙犯罪的理性化決策 與福特主義分工。中正大學犯罪防治學系碩士論文。

[23] 吳易泉，民112年。新興詐欺犯罪偵查實務與防治策略之研究-以假投資詐欺為例。逢甲大學公共事務與社會創新研究所碩士論文。

調查研究方法、步驟	實施期程
邀請犯罪學、電信網路詐欺、司法、金融相關法令領域及實際打擊電信網路詐欺之學者專家就我國防制電信網路詐欺之推動及所面臨之問題等相關議題提供諮詢意見。	
七、第二場履勘 前往戴夫寇爾股份有限公司(DEVCORE)、台灣連線股份有限公司(LINE)等。	112年12月15日
八、第二場諮詢 邀請跨國電信網路詐騙研究者及基層檢察官，針對詐騙集團組織及查緝所面對之挑戰提供諮詢意見	113年1月26日
九、研討會 參加台灣媒體觀察教育基金會與英國西敏寺民主基金會合作主辦之2024台灣-英國『傳播媒體與新聞產製』雙邊交流」。	113年2月19日至29日
十、第三場諮詢 分別邀請抑制不實資訊的負面影響、犯罪學、傳播學之學者專家就我國防制電信網路詐欺之推動及所面臨之問題等相關議題提供諮詢意見。	113年4月24日
十一、研討會 派員參加檢察官打詐實務暨修法研討會。	113年4月26日
十二、邀集機關簡報及座談 分別邀請行政院、司法院、內政部、金管會、法務部、通傳會、數發部相關業務主管人員，就相關議題進行座談提出說明。	113年6月3日
十三、撰擬研究報告初稿	113年5月1日至7月15日
十四、研究報告送請本院交通及採購委員會暨聯席會審議	113年8月13日

資料來源：本調查研究整理。

肆、研究發現與分析

本調查研究將先分析電信網路詐欺於檢方及警方之案件量化數據，以發現其長期趨勢；嗣將政府近年相關防制政策及法規依據「識詐」、「堵詐」、「阻詐」、「懲詐」進行歸納，與前述犯罪趨勢進行綜合分析，並臚陳學者專家意見，以發現政府防制電信網路詐欺相關措施及現行法規可能盲點所在。

一、電信網路詐欺案件變動趨勢：

以下就警政署及高檢署在電信網路詐欺犯罪之相關量化資料進行分析，以明其變動趨勢。

1、警政署106至110年電信網路詐欺案件概況[24]：

（1）106至110年電信網路詐欺案件發生數，平均發生約12,800餘件，其中以108年13,283件最高，109年12,319件最低，詳圖2。

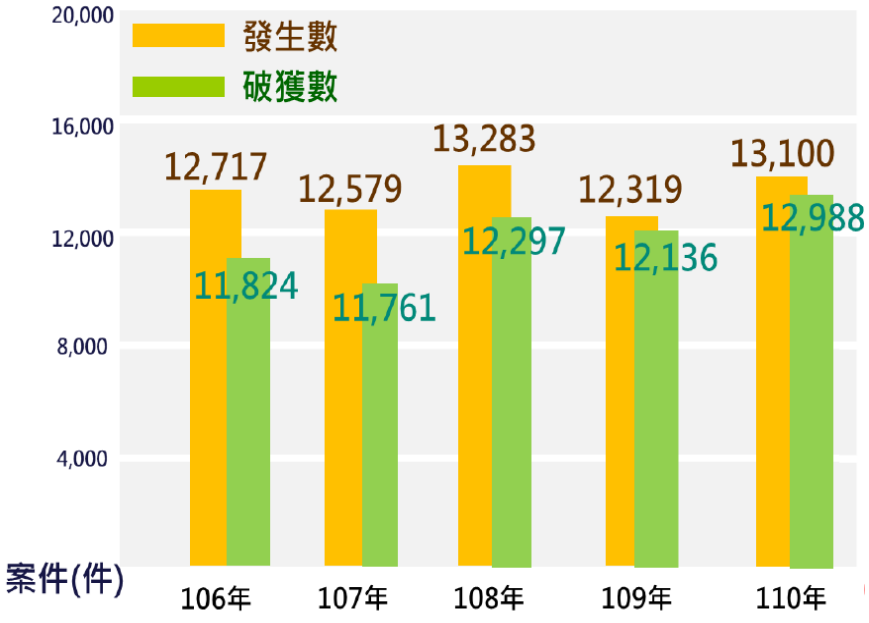

圖2　106至110年電信網路詐欺案件發生及破獲情形

資料來源：打詐綱領1.0版。

[24] 打詐綱領1.0版。

（2）106至110年全般詐欺案件財損金額平均約44.3億餘元，其中以110年56.1億元最高，107年39.7億元最低，詳圖3。

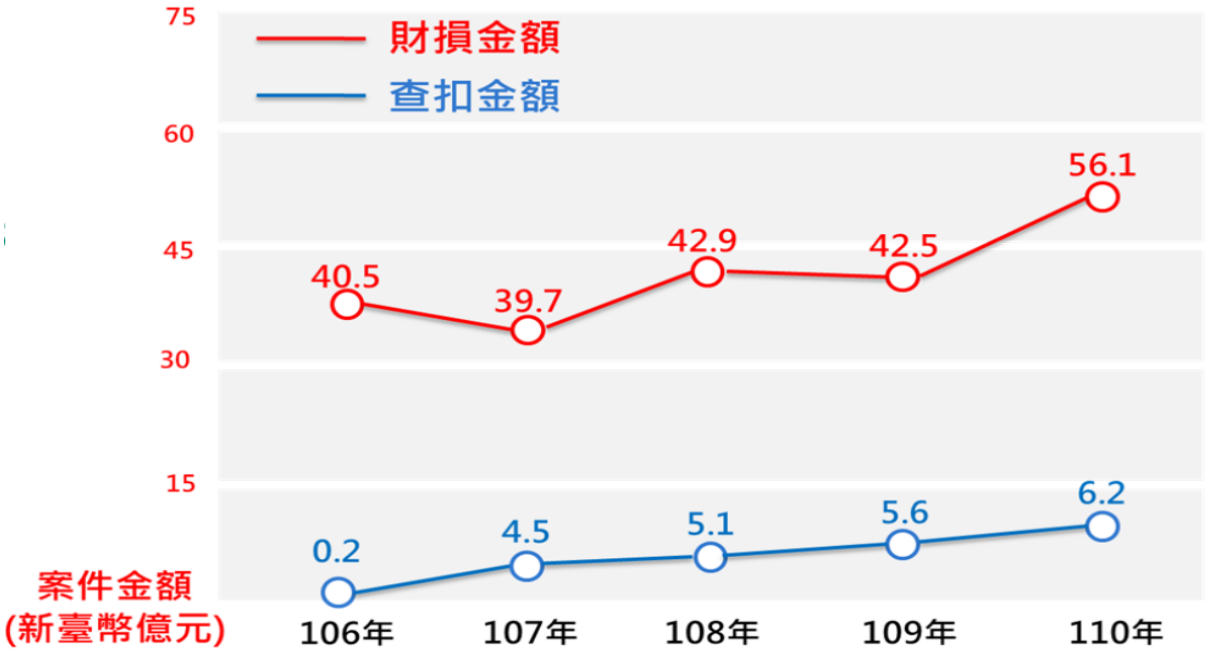

圖3　106至110年全般詐欺案件財損及查扣金額情形

資料來源：打詐綱領1.0版。

2、111至112年間：

（1）打詐綱領1.0版實施近8個月後，詐欺案件發生數及財損金額仍持續增加，其中111年全般詐欺發生計2萬9,509件，詐欺財損73.3億元，分別較110年發生數增加4,785件(+19.35%)、財損增加17.2億餘元(+30.66%)，且全般詐欺發生及財損數為近5年最高。

（2）112年全般詐欺發生數前3名案類，依序為「投資詐欺」(發生數計1萬1,775件，財損53.7億元)、「假網路拍賣（購物）」(發生數計8,246件、財損5.8億元)，「解除分期付款詐欺(ATM)」(發生數計7,351件、財損9.4億元)，此三類案件發生

數與財損金額即占全般詐欺案件近7成。

3、依89至112年共24年間電信網路詐欺案件數量變動趨勢(詳圖4)[25、26]，歷年共出現2次高峰，第1次發生於93至98年間，件數一度攀升至1.9萬件，經政府大力掃蕩，於102年降至低點6,355件，然後續又逐步上升，105至110年間約維持1.3萬件，直至111年起電信網路詐欺案件又快速成長，至112年突破歷史高峰至20,958件，較111年增加比率高達33.1%，較110年更成長近6成，電信網路詐欺案件迅速爬升，形成第2次高峰，且尚未有減緩現象。另依警政署統計各種詐欺案件類型統計更可發現，比較100與112年，其他類型詐欺案件成長28%，財損金額負成長約2成，然電信網路詐欺案件成長高達1倍(103%)，財損金額增加比率更高達4.36倍(436%)，以上均顯示當前電信網路詐欺案件之氾濫，及政府打詐情勢之嚴峻。

[25] 89至104年係曾雅芬(民105)行騙天下：臺灣跨境電信詐欺犯罪網絡之分析引用警政署資料。
[26] 105至112年引用警政署提供資料。

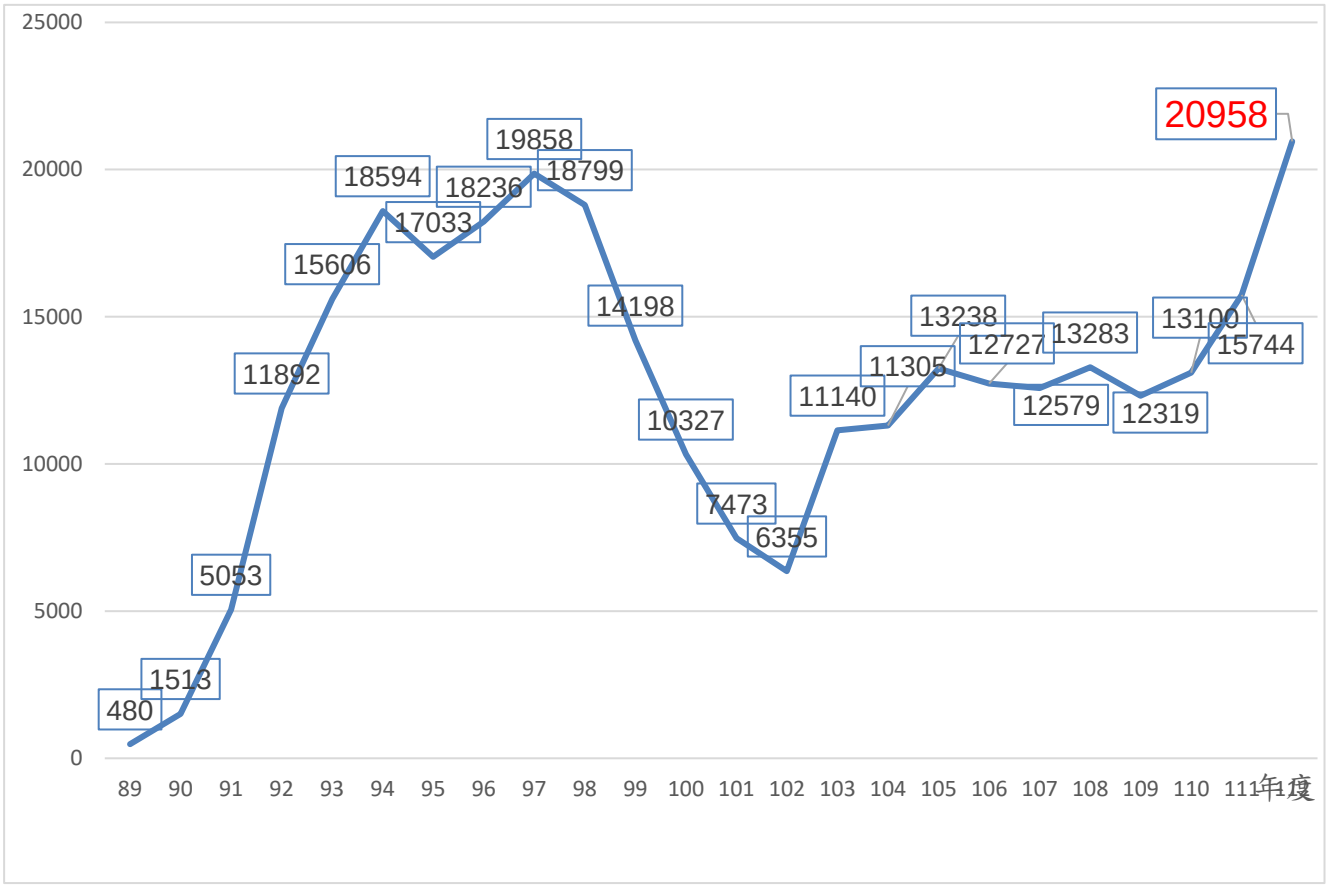

圖4　電信網路詐欺案件數逐年趨勢

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[27]研究，本院自行整理。

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

表2　100年起各類型詐欺案件發生、破獲及財損統計表

電信網路詐欺案件													
年度	100	101	102	103	104	105	106	107	108	109	110	111	112
發生件數	10,327	7,473	6,355	11,140	11,305	13,238	12,717	12,579	13,283	12,319	13,100	15,744	20,958
破獲件數	7,179	5,242	3,477	5,091	8,478	11,116	11,824	11,761	12,297	12,136	12,988	15,396	20,366
財損金額	11億6990萬0842元	10億8940萬4811元	11億5955萬4549元	16億2217萬3621元	20億5655萬2591元	22億4476萬5164元	23億1662萬8767元	22億4991萬2572元	25億8027萬1161元	26億4593萬5649元	35億5245萬1878元	42億9921萬4593元	59億7707萬8060元
其他類型詐騙案件													
年度	100	101	102	103	104	105	106	107	108	109	110	111	112
發生件數	13,285	12,948	12,417	11,913	9,867	9,937	9,972	10,891	10,364	10,735	11,624	13,765	17,026
破獲件數	10,647	10,742	9,362	10,081	9,480	8,696	9,009	9,917	9,639	10,511	11,496	13,322	15,914
財損金額	37億1020萬1714元	31億7204萬0257元	25億4627萬6595元	17億5764萬9003元	15億0423萬5688元	15億8684萬9523元	17億3128萬1272元	17億1922萬9320元	17億1321萬2600元	16億0912萬7675元	20億5792萬5446元	30億2890萬9005元	29億0187萬5021元
全般詐欺案件													
年度	100	101	102	103	104	105	106	107	108	109	110	111	112
發生件數	23,612	20,421	18,772	23,053	21,172	23,175	22,689	23,470	23,647	23,054	24,724	29,509	37,984
破獲件數	17,826	15,984	12,839	15,172	17,958	19,812	20,833	21,678	21,936	22,647	24,484	28,718	36,280
財損金額	48億8010萬2556元	42億6144萬5068元	37億0583萬1144元	33億7982萬2624元	35億6078萬8279元	38億3161萬4687元	40億4791萬0039元	39億6914萬1892元	42億9348萬3761元	42億5506萬3324元	56億1037萬7324元	73億2812萬3598元	88億7895萬3081元

資料來源：內政部警政署[28]。

(二)檢調機關電信網路詐欺案新收件數變動情形：

1、各地檢署電信網路詐欺案件新收件數由109年之50,239件逐年成長至112年新收件數229,711件，累計4年電信網路詐欺新增加收件數達526,030件，且112年較109年新收件數增加179,472件，成長逾3.5倍(357%)，顯示電信網路詐欺案件新收件數並未有減緩之情形。

2、各地檢署電信網路詐欺案件新收件數占全部偵查案件比率，由109年10.1%逐年成長至112年之31.3%，顯示地檢署偵辦案件，電信網路詐欺案件由109年約占1成，至102年，已成長至3成，檢察官偵辦電信網路詐欺案比率大幅增加。(詳表3、圖5)。

[28] 113年6月19日內授警字第1130878508號函。

表3　各地方檢察署電信網路詐欺案件偵查新收件數

單位：件數；%

	電信網路詐欺新收件數	全部偵查新收件數	電信網路詐欺占全部偵查新收件數比率
109	50,239	499,607	10.1
110	98,256	533,569	18.4
111	160,803	639,301	25.2
112	229,711	733,505	31.3
小計	539,009	2,405,982	22.4
113年1-6月	88,137	349,753	25.2
總計	627,146	2,755,735	22.8

資料來源：法務部(https://www.rjsd.moj.gov.tw/RJSDWEB/visualize/Visualization.aspx?kind=PC&d=12)

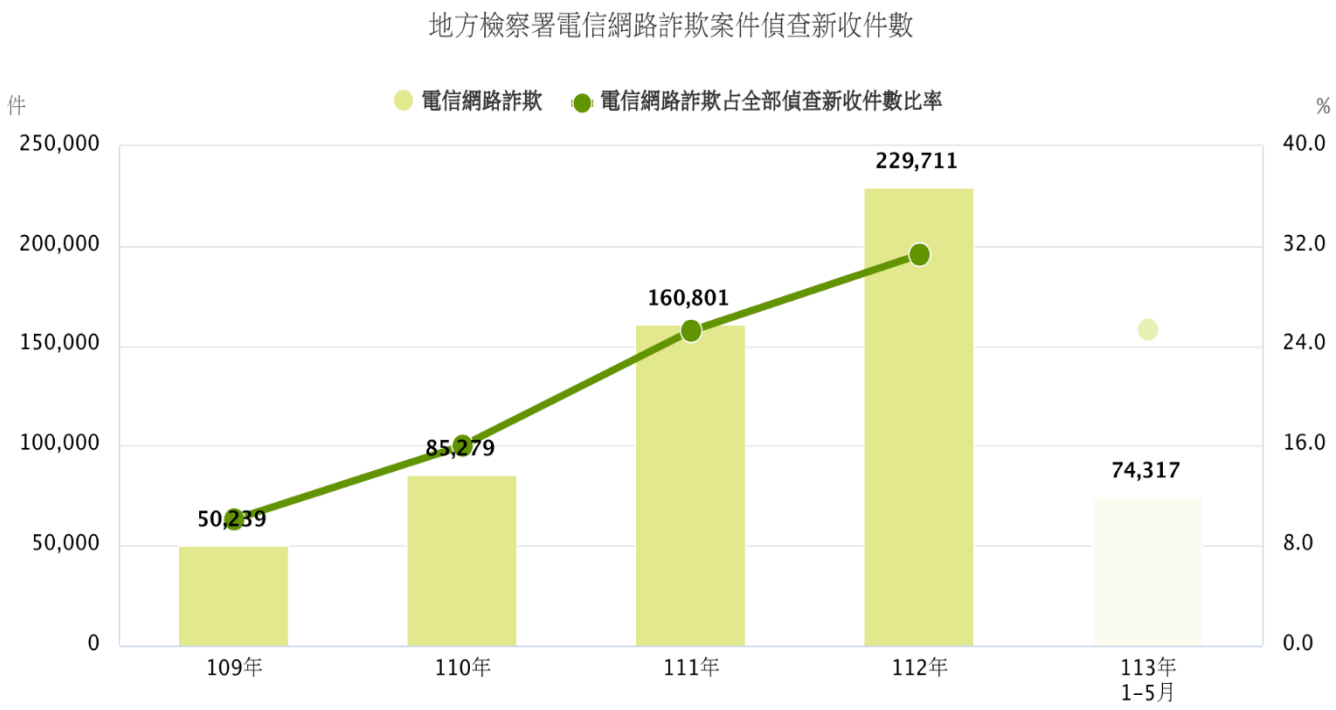

圖5　地方檢察署電信網路詐欺案件偵查新收件數變動趨勢圖

資料來源：法務部(https://www.rjsd.moj.gov.tw/RJSDWEB/visualize/Visualization.aspx?kind=PC&d=12)

(三)電信網路詐欺案件，經地檢署偵查終結之人數變動情形：

1、因電信網路詐欺案件遭偵辦之人數由109年之84,263人逐年成長至112年之265,377人，4年間因電信網路詐欺遭偵查之人數共計652,238人，其中112年較109年遭檢察官偵查人數增加181,114人，成長逾2倍(215%)，且113年1至5月遭偵查之人數仍達94,202人，顯示，電信網路詐欺案件仍十分嚴峻，相關數據及變動趨勢，詳表4、圖6。

2、因電信網路詐欺案件遭起訴之人數由109年之24,746人逐年成長至112年之76,482人，4年間因電信網路詐欺遭起訴人數共計200,475人，其中112年較109年遭因電信網路詐欺案件遭起訴之人數增加51,736人，成長逾2倍(209%)，且113年1至5月遭偵查起訴之人數仍達30,879人，顯示，電信網路詐欺案件遭起訴之情形仍未有趨緩之情形。

3、109至112年地方檢察署辦理詐欺罪案件偵查終結，經檢察官不起訴處分之人數共計252,609人占電信網路詐欺案件全部偵查數達38.7%，且不起訴比率約占4成，相較遭起訴之200,475人，約占3成為高；另依據法務部106至110詐欺統計分析顯示，不起訴處分之理由主要為犯罪嫌疑不足(占88.5%)。另，詐欺罪且屬電信詐欺恐嚇案件，依據法務部統計106至110年資料顯示，單純車手起訴比率59.0%較高，「單純提供人頭帳戶」18.0%較低。

表4　地方檢察署電信網路詐欺案件偵查終結人數

單位：人；%

	總計	起訴	占比	緩起訴	占比	不起訴	占比	其他	占比
109年	84,263	24,746	29.4	337	0.4	29,432	34.9	29,748	35.3
110年	115,558	38,478	33.3	420	0.4	46,443	40.2	30,217	26.1
111年	187,183	60,769	32.5	294	0.2	68,355	36.5	57,765	30.9
112年	265,377	76,482	28.8	345	0.1	108,379	40.8	80,171	30.2
小計	652,238	200,475	30.7	1,396	0.2	252,609	38.7	197,901	30.3
113年1-5月	94,202	30,879	32.8	125	0.1	37,695	40.0	25,503	27.1
總計	746,583	231,354	31.0	1,521	0.2	290,304	38.9	223,404	29.9

資料來源：法務部(https://www.rjsd.moj.gov.tw/RJSDWEB/visualize/Visualization.aspx?kind=PC&d=12)

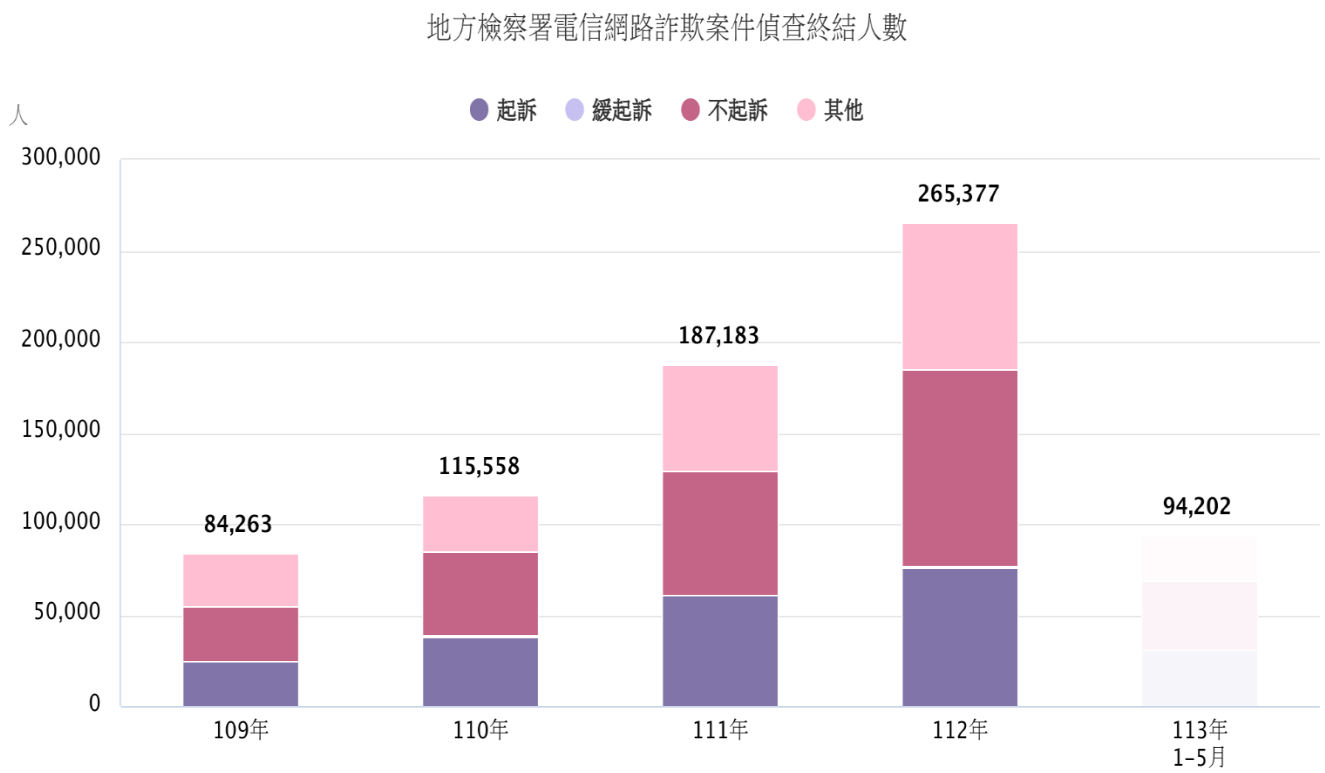

圖6　地方檢察署電信網路詐欺案件偵查終結人數變動趨勢圖

資料來源：法務部(https://www.rjsd.moj.gov.tw/RJSDWEB/visualize/Visualization.aspx?kind=PC&d=12)

(四)依起訴人區分各種電信網路犯罪類型變動趨勢(詳表5)：

1、單純提供人頭帳戶[29]：統計因提供人頭帳戶遭起訴人數由109年之8,566人逐年成長至112年之40,956人，4年間共計增加32,390人，成長近4倍(378%)，雖113年1至5月遭起訴人數12,326人，似有下滑之情事，然提供人頭帳戶供電信網路詐欺之情事，仍十分嚴峻。

2、單純車手[30]：統計擔任電信網路詐欺案件車手遭起訴人數由109年之7,250人逐年成長至112年之8,522人，4年間共計增加1,272人，成長近2成(18%)，雖相較因提供人頭帳戶及一般電信詐欺之情況稍佳，然113年1至5月遭起訴人數亦達6,104人，顯示，擔任車手遭起訴案件有增加之趨勢。

3、一般電信詐欺[31]：統計因一般電信詐欺遭起訴人數由109年之8,930人逐年成長至112年之27,004人，4年間共計增加18,074人，成長逾2倍(202%)，且113年1至5月遭起訴人數仍12,449人，顯示，一般電信詐欺仍未有效抑制。

[29] 單純提供人頭帳戶：為提供帳戶或手機門號給詐騙集團作為犯罪工具，無論自願或被騙提供均屬之，而未參與其他犯罪階段者。

[30] 單純車手：為詐騙集團中負責領取被害人交付款項者。

[31] 一般電信詐欺：非屬單純車手及單純提供人頭帳戶者，皆列入一般電信詐欺。

表5　各地方檢察署電信網路詐欺案件偵查起訴人數-按犯罪類型分

單位：人

資料時間	單純提供人頭帳戶	單純車手	一般電信詐欺
109 年	8,566	7,250	8,930
110 年	17,792	8,276	12,410
111 年	32,743	8,039	19,987
112 年	40,956	8,522	27,004
113 年 1-5 月	12,326	6,104	12,449

資料來源：法務部(https://www.rjsd.moj.gov.tw/RJSDWEB/visualize/Visualization.aspx?kind=PC&d=12)

(五)司法偵辦情形

1、電信網路詐欺案件定罪情形

（1）電信網路詐欺案件經司法機關裁判確定有罪人數由109年之13,272人逐年增加至112年之26,700人，判定有罪人數成長超過1倍。

（2）電信網路詐欺案件經司法機關判定有罪之定罪率由109年之93.1%逐年成長至112年之94.9%。

表6　電信網路詐欺案司法機關定罪情形表

單位：人；%

	裁判確定有罪人數	定罪率
109 年	13,272	93.1
110 年	12,604	93.6
111 年	19,729	94.8
112 年	26,700	94.9
113 年 1-5 月	13,460	95.3

說明：定罪率=有罪人數/(有罪+無罪人數)*100%。

資料來源：法務部(https://www.rjsd.moj.gov.tw/RJSDWEB/visualize/Visualization.aspx?kind=PC&d=12)

2、政府懲治電信網路詐欺集團之情形(詳表7、圖7)

(1)109年判決6個月以下刑度者占全體有罪判決35.8%(4,758/13,272)。

(2)112年1至9月，判決6個月以下刑度之比率已成長61.7%(12,380/20,053)。

表7　地檢署電信網路詐欺案件-執行裁判確定人數(人)

年度	6月以下	逾6月-1年未滿	1年-2年未滿	2年-3年未滿	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

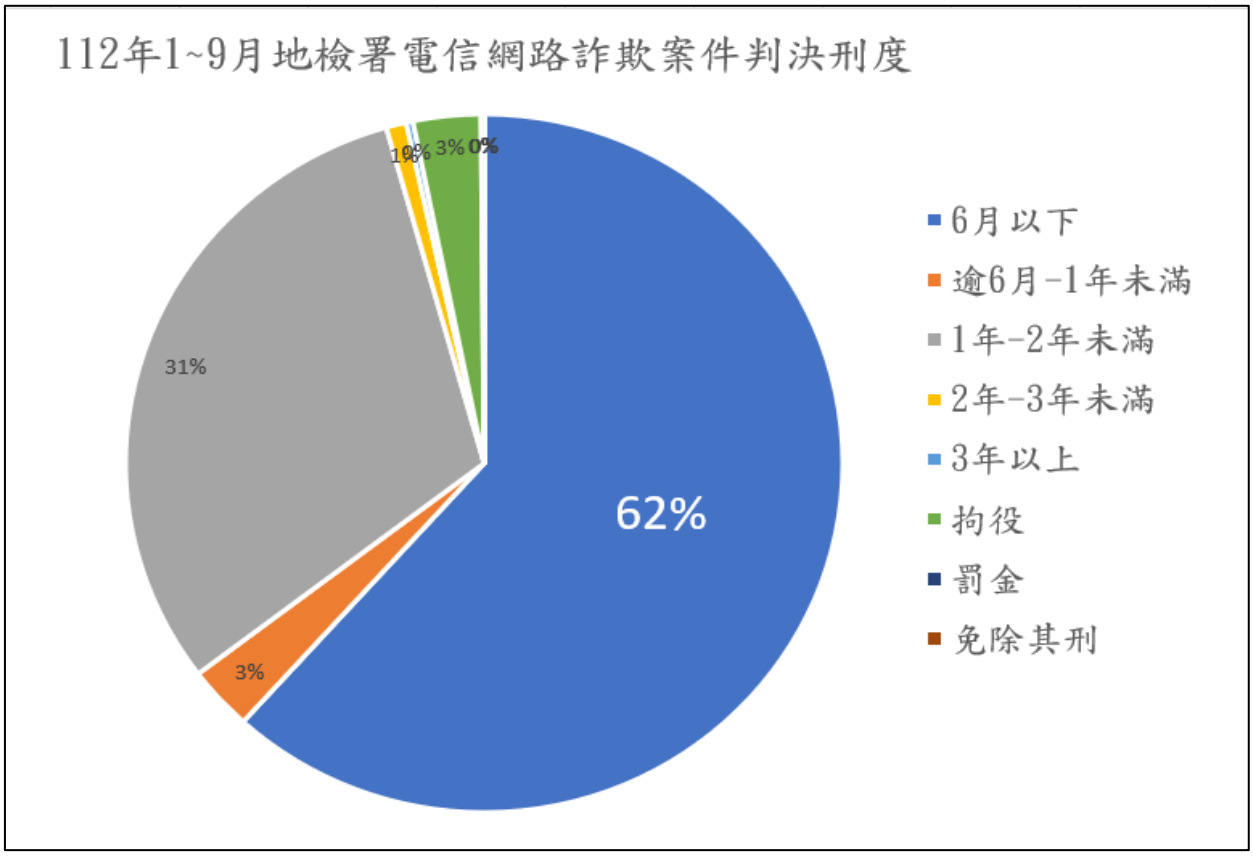

圖7　地檢署電信網路詐欺案件-執行裁判確定人數(人)

資料來源：法務部高檢署112年11月13日簡報資料，本院自行整理。

二、犯罪樣態、趨勢、反制措施及打擊重點:針對前述檢方及警方量化數據所呈現出之犯罪樣態及趨勢，政府於111年7月15日核定打詐綱領1.0版，嗣因無法有效抑制電信網路詐欺持續高發，又於112年6月9日核定打詐綱領1.5版，調查研究其措施及打擊重點如下：

(一)打詐綱領1.0版：106至110年電信網路詐欺案件平均每年約1萬2,800餘件，於COVID-19疫情期間(110年)，國內電信網路詐欺發生數更增加至1萬3,100件、全般詐欺[32]財損56.1億元，分別較109年發生數增加781件(+6.34%)、財損增加13.6億餘元(+32%)，且110年全般詐欺財損數為5年最高，顯示打擊詐欺犯罪面臨嚴峻挑戰。為展現政府打擊詐欺犯罪決心，行政院111年7月15日核定打詐綱領1.0版。

1、本綱領之規劃係經由「識詐-宣導教育面」、「堵詐-電信網路面」、「阻詐-贓款流向面」及「懲詐-偵查打擊面」等四大面向，以「增加詐欺犯罪成本，減少民眾財產損害」為目標，由各部會齊力提升政府防制詐欺犯罪能量，達到保護民眾財產安全與降低犯罪損害之「減害」終效：

(1) 識詐(宣導教育面)→防詐騙：

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。

(2) 堵詐(電信網路面)→毀工具：

由通傳會擔任電信網路面之統籌機關，自源頭完善管制機制，防堵資通訊服務淪為犯罪工具，毀斷詐欺犯嫌施詐之管道。

(3) 阻詐(贓款流向面)→擋金流：

[32] 全部詐欺案件總數。

由金管會擔任資金面之統籌機關，強化金融監管功能，推動各項金融防詐減損策略，建構良好完善之金警合作機制，以保護國人財產安全。

（4）懲詐(偵查打擊面)→清集團：

由法務部擔任統籌機關，結合檢警全面查緝各類詐騙犯嫌，並強化贓款查扣工作，俾阻斷詐騙集團金流，協助被害人贓款返還減少被害損失。

2、打詐綱領1.0具體策略：

（1）識詐：

〈1〉分項指標：

《1》每年宣導資訊觸及1,000萬人次。

《2》每年發送防詐簡訊1億2,000萬則。

〈2〉具體策略：

《1》分齡分眾主題式反詐宣導。

《2》落實金融機構關懷提問、即時攔阻。

（2）堵詐：

〈1〉分項指標：

《1》每年攔阻簡訊3,000萬則。

《2》人頭門號停斷話5,000門。

〈2〉具體策略：

《1》防杜境外竄改來話詐騙。

《2》遏止人頭門號詐騙工具。

《3》防杜簡訊業者幫助詐騙及建立惡意簡訊攔阻機制。

《4》加強電商業者資安維護。

《5》遏止詐騙網頁刊登。

《6》管理及防制VPN業者詐騙。

（3）阻詐：

〈1〉分項指標：

《1》本國銀行全體(100%)將銀行公會彙整之共通性異常交易態樣納入內部預警指標。

《2》本國銀行全體(100%)設立「疑涉詐欺境外金融帳戶預警機制」。

〈2〉具體策略：

《1》防制人頭帳戶進行詐騙。

《2》防制第三方支付詐騙。

《3》制定虛擬通貨洗錢防制管理規範。

《4》防制遊戲點數成為詐騙工具。

《5》防制貨到付款、一頁式詐騙。

（4）懲詐：

〈1〉分項指標：每年電信詐騙案件查獲集團數提高3%。

〈2〉具體策略：

《1》瓦解電信網路詐欺集團。

《2》強化查緝跨境詐欺犯罪能量，遏止境外犯罪。

(二)打詐五法：政府訂定打詐綱領1.0版，然電信網路詐騙案件數量仍持續暴增，為有效遏止詐欺犯罪，政府陸續修訂《刑法》、《人口販運防制法》、《個人資料保護法》、《洗錢防制法》、《證券投資信託及顧問法》等打詐五法修正草案，並於112年5月30日經立法院三讀通過。

1、刑法修正：

（1）為因應詐欺犯罪型態之轉變，增訂加重剝奪行動自由罪，並新增刑法加重詐欺罪之加重處罰事由，使我國刑法規範面與時俱進，周延保障民眾之人身、自由及財產安全。

（2）修正重點如下：

〈1〉增訂加重剝奪行動自由罪。

〈2〉增訂加重詐欺罪之加重處罰事由，將利用深偽影像及聲音之犯罪手法納入規定，以強化我國刑法之規範密度。

2、人口販運防制法：

（1）國人遭詐騙至境外拘禁從事具勞動性質之犯罪活動事件層出不窮，為嚇阻人口販運行為並強化被害人權益保障。

（2）修正重點：

〈1〉擴大人口販運之行為態樣明確化人口販運行為之定義。

〈2〉增訂「實行依我國法律有刑罰規定之行為」之不法作為樣態，係由勞動與報酬顯不相當工作衍生而來，故應與涉及持續剝削勞動力之不法行為相關者，方屬之；另所實行之行為僅須為我國刑法所禁止，並不以確實構成刑事責任為必要，否則無從涵蓋未達刑事責任年齡之兒童實施犯罪行為，或其他不具備違法性或責任能力之情形。

〈3〉擴大處罰範圍並提高人口販運罪刑責。

〈4〉增訂以強暴、脅迫、恐嚇、拘禁、監控、藥劑、催眠術、詐術或其他相類之方法，使人提供勞務者，屬犯罪行為；意圖營利犯前開之罪者，加重處罰。

〈5〉增訂人口販運被害人對鑑別結果不服之救濟程序。

〈6〉增訂人口販運被害人及疑似被害人之「非機構式安置服務」。

〈7〉增訂人口販運被害人或其家屬為假扣押或假處分之聲請時，得以被害人鑑別通知書代替

保全原因之釋明，並免提供擔保金。

〈8〉增訂犯人口販運罪經有罪判決確定者，自判決確定之日起5年內不得參加政府採購投標或作為決標對象或分包廠商。

3、個人資料保護法：

（1）鑑於詐騙犯罪之猖獗實與民眾個資外洩事件息息相關，降低個資外洩情形確實有助於防堵詐騙案件發生，為促使民間企業確實履行個資安全維護義務，並強化非公務機關對於個資保護的重視。

（2）修正重點：

〈1〉設立「個人資料保護委員會」為本法之專責主管機關。

〈2〉提高非公務機關未善盡個資安全維護義務之罰則。考量企業違反安全維護義務導致個資外洩而遭詐騙集團不當利用，所衍生之後果不堪設想，本次修法爰賦予主管機關於非公務機關違反安全維護義務時，得逕予裁處罰鍰同時命其改正之權限，無須待屆期未為改正始予處罰，同時提高罰鍰數額之上限，得處2萬元以上200萬元以下之罰鍰；屆期未改正者，並得再按次處15萬元以上1,500萬元以下之罰鍰。

4、洗錢防制法：

（1）因現代網路科技日新月異，詐騙集團經常透過收集大量民眾之金融帳戶或帳號，作為洗錢及詐欺民眾財產的犯罪工具，為阻斷詐騙集團之洗錢管道並填補法律處罰漏洞。

（2）本次修正重點：

〈1〉增訂無正當理由收集他人帳戶罪。

〈2〉增訂向他人交付、提供帳戶罪。本次修法考量現行實務上交付、提供帳戶之原因眾多，且各原因之惡性高低不同，為達教育人民妥善保管個人帳戶法律上義務之目的，並有效遏止人頭帳戶氾濫問題，爰採取寬嚴並進之處罰方式。

5、證券投資信託及顧問法：

（1）鑑於投資詐騙廣告於各大網際網路媒體及影音平臺四處流竄，投資詐騙案件多係透過網路平臺投放不實廣告或以偽冒知名人士名義推介有價證券之方式誤導投資人，為提供我國民眾更安全之投資環境。

（2）修正重點：

〈1〉明定「非證券投資信託及顧問業者」從事涉及有價證券投資或業務招攬廣告之禁止行為態樣。

〈2〉增訂網路傳播媒體業者應以實名制方式刊登或播送涉及有價證券投資或業務招攬廣告。

〈3〉增訂網路傳播媒體業者與委託刊播、出資者之連帶損害賠償責任與例外減輕、免責規定。

(三)打詐綱領1.5：打詐綱領1.0版實施近8個月後，詐欺案件發生數及財損金額仍持續增加，其中111年全般詐欺發生計2萬9,509件，詐欺財損73.3億元，分別較110年發生數增加4,785件(+19.35%)、財損增加17.2億餘元(+30.66%)，且全般詐欺發生及財損數為近5年最高。除民眾對於詐欺犯罪深感威脅外，復因詐欺集團據點已擴及到海外第三地國家，年輕人遭誘出國從事詐欺機房或領款車手等工作，甚至淪為國際人口販運被害人，影響我國國際形象，顯示政府在防制詐欺犯罪上還存在許多待解決的課題，為強化政

府打詐效能，行政院於112年6月9日核定打詐綱領1.5版。

1、本綱領之規劃賡續透過「宣導教育」、「犯罪通路」、「贓款流向」及「偵查打擊」等四大面向，由警政署結合各面向之統籌機關共同研擬因應對策，運用「增加詐欺犯罪成本，減少民眾財產損害」之概念，分由「識詐-宣導教育面」、「堵詐-電信網路面」、「阻詐-贓款流向面」及「懲詐-偵查打擊面」等四大面向著手，分工協力制定偵防策略。

2、為提升我國打擊詐欺犯罪效能，並統籌督導四大面向執行作業，特設行政院打擊詐欺辦公室，高檢署成立查緝詐欺及資通犯罪中心、調查局成立北部、中部、南部、跨境詐欺防制中心，另6都直轄市調查處機動工作站成立打詐專案組，警政署成立專案指揮暨資料研析協作平臺北、中、南工作站。另中央結合各縣市政府打詐地方隊及民間團體力量，公私協力，以全力遏阻詐欺犯罪，將打詐效能極大化。

3、打詐綱領1.5具體策略：

（1）識詐：

〈1〉分項指標：

《1》每年宣導資訊觸及3,000萬人次。

《2》每年發送防詐簡訊1億4,000萬則。

《3》每年平均攔阻率提高5%。

〈2〉具體策略：

《1》分齡分眾防詐宣導。

《2》落實金融機構關懷提問、即時攔阻。

《3》加強網路推播能量。

《4》多元管道擴大觸及。

《5》建立正確法治觀念。

（2）堵詐：

〈1〉分項指標：

《1》每年攔阻簡訊3,000萬則(採滾動修正)。

《2》每年人頭門號停斷話5,000門(採滾動修正)。

《3》開發2種以上數位防詐工具。

《4》輔導三大公協會會員辦理網購程序之防詐相關警示措施及物流隱碼技術。

〈2〉具體策略：

《1》防杜境外竄改來話詐騙。

《2》遏止人頭門號詐騙工具。

《3》防杜簡訊業者幫助詐騙及建立惡意簡訊攔阻機制。

《4》加強電商業者資安維護。

《5》遏止詐騙網頁刊登。

《6》管理及防制VPN業者詐騙。

（3）阻詐：

〈1〉分項指標：

《1》本國銀行全體(100%)將銀行公會彙整之共通性異常交易態樣納入內部預警指標。

《2》本國銀行全體(100%)完成申請約定轉帳加強防詐措施。

〈2〉具體策略：

《1》防制人頭帳戶進行詐騙。

《2》防制第三方支付詐騙。

《3》制定虛擬通貨洗錢防制管理規範。

《4》防制遊戲點數成為詐騙工具。

《5》防制貨到付款、一頁式詐騙。

《6》修法解決網路平臺假投資廣告。

（4）懲詐：

〈1〉分項指標：每年電信詐騙案件查獲集團數提高5%。

〈2〉具體策略：

《1》瓦解電信網路詐欺集團。

《2》強化查緝跨境詐欺犯罪能量，遏止境外犯罪。

(四)在「打詐綱領1.0版」、「打詐綱領1.5版」及「打詐5法」之外，尚有其他打詐強化措施如下：

1、主管機關強化電信事業辦理防制電信詐欺措施：

(1)督導電信事業辦理防制電信詐欺措施：

〈1〉強化電信設備防制詐騙功能。

〈2〉設定國際話務攔阻名單。

〈3〉國際話務改接NGN(NextGeneration Network)提升攔阻效能。

〈4〉發送反詐騙宣導簡訊。

〈5〉統一國內簡訊來電顯號格式。

〈6〉強化行動電話預付卡之申請管制。

〈7〉建置國際來話語音警示系統。

〈8〉建置國際來話攔阻系統。

〈9〉大量門號管制。

〈10〉165防詐平臺連線合作。

(2)強化電信業者內部控管機制：

〈1〉通傳會於112年6月16日訂定「電信事業受理申辦電信服務風險管理機制指引」，並於6月30日邀集各電信業者進行宣導。

〈2〉「電信事業受理申辦電信服務風險管理機制指引」重點：

《1》電信事業提供電信服務應確實落實雙證查核，且針對初次申辦行動電信門號者，應現場拍照留存。

《2》電信事業應自主建立獨立於業務部及通路部門外之稽核部門，自行訂定稽核抽測計畫，並向通傳會報告。

《3》非本國籍人士申辦行動通信之電信門號以1門為原則，倘申請人簽證期日少於1個月，僅能申辦提供30天內之短效期預付卡；且於國外所申請之門號，於入境後始得開通。

《4》受理初次申請之企業客戶申請電信門號或服務數量，以不逾員工人數為原則，並責成電信事業查證該企業客戶實際使用情形。

《5》曾受有關機關通知停、斷話或服務之企業客戶，於1年內至多僅能申請1門電信門號或1項電信服務；倘再受通知停、斷話或服務之企業客戶，電信事業均不再受理申請。

《6》督導電信業者加強用戶KYC(Know Your Customer, KYC)。

〈3〉為確保獲核配用戶號碼之電信事業，提供用戶號碼予從事批發轉售服務業者時，該等業者具備足夠能力落實KYC義務及風險管控，通傳會已著手研訂「電信事業用戶號碼使用管理辦法」草案，針對從事批發轉售之業者，進行資格限制並強化行政管理。

2、強化聯防電信網路詐欺措施：

（1）強化犯罪情資即時連結，包括165反詐騙資料庫增加超商代碼、遊戲點數資料，以及增修詐欺機房情資分析及錢包地址監控功能；並能整合跨機關、跨資料庫之資料，以達成快速勾稽詐、毒等不同案件關聯性之目的。

（2）健全金融資料取得管道，包括統一全國金融機構資料電子檔格式(CSV檔)，以及查調金融資料

線上平臺，可調取94.75%全國金融機構之開戶資料、交易明細、保管箱等金融電子化資料。

（3）在提升通訊軟體網路社群平臺資料調取方面，法務部與高檢署在112年3月17日、4月17日、9月26日三度與LINE公司召開業務聯繫會議，建立投資詐欺群組封鎖下架機制(包括主動查核及投資詐騙刑事案件通報下架)，使得LINE每月提供檢警調調舉之件數由80件上升至200件。

3、防杜境外竄改來話詐騙：

（1）督導業者配合建置國際來話語音警示系統：

〈1〉固網部分：112年9月起中華電信市話接聽所有國際來話均提供語音警示服務。

〈2〉行動網路部分：國內5家行網業者於112年10月起對接聽「+8869」開頭國際來話提供語音警示服務。

〈3〉實施上開國際來話攔阻及警示機制後，國際來話數量明顯下降，自最高112年5月份5,080萬通國際來話，下降為10月份1,503萬通，大幅減少3,576萬通，減少比率達70.39%；「+886」開頭之國際來話數量則自最高112年5月份1,642萬通，持續下降至10月份84萬通，減少比率達94.88%。

（2）配合檢警調查與停斷話：

〈1〉112年1月至10月詐騙門號停斷話1,264門。

〈2〉召開「如何精進電信防詐措施以降低語音及簡訊詐騙案會議」23次，持續邀集165打詐中心與電信業者分析詐騙電話話務與路由特徵。

4、下架詐欺訊息：

（1）因國際平臺業者所提供之網路服務，其服務據

點所在地通常位於其母公司所在國，故檢警單位如遇有需該業者協助事項，常有雙方聯繫不易或信任基礎不足之情形。112年上半年度數發部、高檢署、調查局及刑事局與網路數位平臺及通訊軟體業者（例如 Meta、Google、LINE）共同就打擊詐欺犯罪與資訊交流進行意見交換，並建立聯繫管道持續協助檢警調機關與Google、Meta及 LINE業者溝通。後續更由刑事局與Meta建立「綠色通道」下架涉詐廣告，與Google建立打詐聯繫管道，加速冒名投資廣告下架，也與 LINE建置「紅色通道」下架涉詐帳號、公私協力聯防詐騙措施。

（2）數發部自113年4月15日起主管「網路廣告平臺業」，並就網路詐騙廣告充斥問題開發「詐騙樣態分析」防詐工具，透過大數據分析、機器學習與自然語言處理等技術，每日巡查逾萬筆影片類網路廣告（於Meta、Google、LINE等平臺），透過公私協力機制自動化通報，由受信任機構檢核後，再通知社群平臺業者，以加速下架作業。

（3）以國內主要大型數位平臺如Google、Meta為例，前開平臺目前於我國均有另依公司法投資設立子公司，惟依公司法規定，其子公司均具獨立法人格，並皆表示其未擁有、經營、控制或主辦該數位平臺服務，相關服務係由位於美國總公司經營，並為與國內使用者具契約關係之主體。

（4）手機、網路社群媒體遭不法使用之管理機制：

〈1〉調取資料之管道有下列社群媒體公司Apple、LINE、Meta(FB、IG)、X公司(前身為Twitter)等資料。

〈2〉如需調閱非上開社群媒體公司資料，需由各警察機關自行以公函至該公司進行調閱，警政署將積極與各相關業者增設調閱管道。

〈3〉調閱資料流程及說明如下：

《1》Apple公司:

〔1〕檢具資料：調閱單、搜索票、清冊(5個以上即建立清冊)。

〔2〕流程：系統投單-審核通過-email給Apple公司-Apple公司以email回復結果。

《2》LINE公司:

〔1〕檢具資料：調閱單、搜索票。

〔2〕流程： 系統投單-審核通過-email給LINE公司-LINE公司email回復告知搜扣日-警政署email給調閱單位告知搜扣日-調閱單位持搜索票於搜扣日來警政署-警政署於當日下午3時與LINE公司以搜索票交換資料(不符LINE公司規定須重新安排搜扣日)。

《3》Meta公司:

〔1〕檢具資料：調閱單、相關截圖。

〔2〕流程： 系統投單-審核通過-上傳Meta平臺-自行於Meta平臺下載回復資料。

《4》X公司(原Twitter公司)：

〔1〕檢具資料：調閱單。

〔2〕流程：系統投單-審核通過-上傳X平臺-X公司以email回復結果。

〈4〉未能取得資料原因：以上4個社群公司若無資料回復原因皆位於境外、需司法互助協議取得資料或帳號已刪除等，調閱情形詳表8。

表8　主管機關調得社群公司情形表

社群平臺／年度	Apple			LINE			臉書			X(前Twitter)		
	調閱次數	調得次數	調得率%	調閱次數	調得次數	調得率%	調閱次數	調得次數	調得率%	調閱次數	調得次數	調得率%
106				256	256	N/A	1,078	1,043	96.7			
107	927	927	100.0	280	280	N/A	1,671	1,527	91.3			
108	1,089	1075	98.7	296	296	N/A	2,597	2,390	92.0			
109	2,120	1949	91.9	318	318	N/A	3,056	2,561	83.8	47	33	29.8
110	2,483	2376	95.6	261	261	N/A	3,501	2,976	85.0	54	12	22.2
111	2,775	1649	59.4	843	843	N/A	6,303	5,534	87.8	186	50	26.8
112 (10月底)	5,436	2677	49.3	1066	1066	N/A	6,627	5,315	80.2	155	59	38.1
合計	14,830	10653	71.8	3,064	3064	N/A	21,725	18,671	85.9	442	135	30.5
各公司調閱情形。註：LINE調閱率N/A係LINE公司以光碟回復資料												

資料來源：內政部。

5、電子支付帳戶申請

（1）電子支付機構採「實名制」確認客戶身分：依「電子支付機構管理條例」規定，電子支付機構應建立使用者身分確認機制，對於使用者申請註冊及開立電子支付帳戶，係採「實名制」方式確認身分，包括：徵提基本身分資料(姓名、國籍、身分證明文件種類與號碼、出生年月日等)、向財團法人金融聯合徵信中心確認國民身分證領補換資料及警示(存款及電支)帳戶資訊、確認使用者可利用該行動電話號碼操作並接收訊息通知、確認使用者本人之金融支付工具(如存款帳戶或信用卡)等。現行民眾存款帳戶經警示後，無法開立電支帳戶。

（2）增加本人金融支付工具原留門號之驗證機制：為避免遭詐騙集團利用不法取得之個人資料冒開電子支付帳戶，金管會已請中華民國銀行商業同業公會全國聯合會(下稱銀行公會)於111年8月25日召開「防堵電子支付詐騙」意見交流

會，並於111年11月21日開會研議強化確認使用者本人之金融支付工具，增加驗證使用者開立存款帳戶或信用卡原留手機門號機制(下稱核驗原留門號機制)，並納入電子支付機構之資安自律規範，各電子支付機構已於112年3月31日前調整核驗機制。

（3）高檢署於111年12月26日召開之「電子支付帳戶遭詐欺集團不法利用策進作為研商會議」，銀行公會代表說明部分電子支付機構已先行增加核驗原留門號機制，並有顯著成效(此機制係透過使用者親臨銀行櫃檯完成開戶時所留門號進行比對，相較使用者手持身分證拍照上傳影像檔後，由電支機構憑肉眼辨識影像檔是否為其本人，應較為有效)。會議決議：將視增加驗證原留門號機制整體執行情形，再行研議是否增加其他身分驗證機制。依警政署統計資料，於電子支付機構全面採行此機制後，112年6月新增警示電支帳戶案件數，已較111年12月案件數最高峰下降超過9成，顯示採行核驗原留門號及相關防詐機制已具成效。

（4）金管會於112年5月4日與相關執法機關及銀行公會召開「金融機構所發送一次性動態密碼(OTP)簡訊內容研商會議」，會中決議請銀行公會擬訂OTP簡訊範本，並提供各會員機構參考，若發送OTP簡訊之業務涉及開立電子支付帳戶、電子支付帳戶約定連結存款帳戶等，則OTP簡訊文字應包括「簡訊目的」、「反詐宣導」及「法律責任(例如：『避免遭不法利用』)」。銀行公會已於112年5月26日提供各金融機構OTP簡訊範本，並請各機構依上開會議決議辦理。電子支付機

構於112年12月31日前完成。

6、強化人頭帳戶管理機制：

（1）考量金融機構之客戶倘於聯行已開戶時，應向「原第一開戶行」照會之作法，部分留存之文件常為年代久遠之舊式身分證及簽樣，106年修正後，已調整為向「前一開戶行」照會比對留存之身分證明文件、照片、筆跡是否相同等內容。

（2）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。

（3）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。

（4）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。

（5）對水房短時多筆分帳因應措施：

〈1〉將疑涉詐騙帳戶列為警示：依法院、檢察署或司法警察機關以公文書(含報案三聯單等)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〉已有相關異常交易態樣：經查「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」列有「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，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。

7、強化虛擬通貨管理機制：

（1）金管會已於110年6月30日發布「虛擬通貨平台及交易業務事業(Virtual Asset Service Provider, 下稱VASP)防制洗錢及打擊資恐辦法」，並自110年7月1日施行。

（2）依金管會110年9月30日金管銀法字第11002729181號令之規定，VASP應依金管會指定之文件、資料及方式完成洗錢防制法遵聲明，應檢附之文件包括：聲明書、聲明人資料表、登記機關證明文件、章程、董監事名冊及股東名冊、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控與稽核制度檢查表及審查意見書等。對於未完成法遵聲明而有從事虛擬資產活動之業者，金管會將依洗錢防制法要求該等業者限期改善，若屆期未改善者，得處50萬元至1,000萬元罰鍰。

（3）金管會係以循序漸進方式推動業者管理，以強化客戶權益保護，並已於112年9月26日發布「管理虛擬資產平臺及交易業務事業(VASP)指導原

則」，從交易資訊透明、客戶資產保管方式、平臺業者內控管理、外部專家輔助等方面加強平臺對客戶保護。後續將洽請虛擬資產平臺業者推動業界自律，由相關公會依據指導原則訂定自律規範，以引導業者強化內部控制，提升客戶權益保障。

（4）經查截至112年10月31日為止，已有25家虛擬通貨平臺及交易業務事業，完成洗錢防制法令遵循聲明。尚未完成洗錢防制法令遵循聲明而以虛擬通貨活動之業者，自屬違法。金管會將持續與執法機關密切配合，共同精進防制詐騙措施，保護民眾財產。

8、強化第三方支付管理：

（1）法遵面：已訂定「第三方支付服務業防制洗錢指引手冊」及其範本，協助業者進行法遵作業以及落實KYC，指引內要求業者應有審查客戶網站是否為詐騙或賭博網站等義務。並同時於8月底規避查核者，將依洗錢防制法相關規定進行裁罰。

（2）業務經營面:已訂定「第三方支付服務業能量登錄制度」，將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；未完成登錄者將請金管會要求銀行基於其未完成法遵以及確認客戶身分(KYC)等重要考量，不提供虛擬帳戶服務，僅提供低風險之信託或履約保證金專戶等業務服務。另數發部綜合財政部、臺灣集中保管結算所股份有限公司(Taiwan Depository & Cleaning Corporation, TPCC, 下稱集保中心)、銀行公會及與第三方支付服務業有業務聯繫關係之相關機關及公協會資料，

國內目前實際經營第三方支付服務業之公司行號家數尚不足100家，數發部數產署目前已受理46家業者申請能量登錄制度，包括國內主要第三方支付業者，將陸續召開審查會議，並於官網公告通過業者名單。

（3）行政協助面：透過能量登錄制度掌握實質經營第三方支付服務業者名單，並提供通過登錄業者介接內政部戶役政系統及集保公司實質受益人資料庫，未來亦協助開發掃描外部網站的系統工具，協助業者完成法遵規定，另透過合法第三方支付業者的公示制度，減少詐騙案件之發生。

（4）金融面對虛擬帳號管控措施：

〈1〉已持續督導銀行落實第三方支付業者申請虛擬帳號服務之事前開戶審核作業與加強事後監控管理，110年對於高風險客戶採取強化虛擬帳號控管措施，112年上半年再請銀行公會研訂銀行提供虛擬帳號服務之強化客戶身分審查措施，並已函請各銀行配合辦理。

〈2〉配合數發部能量登錄制度：金管會已於112年11月2日函請銀行公會轉知會員機構配合數發部於112年10月25日函知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。若為銀行既有客戶（即舊戶），在該部訂定之緩衝期內（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。

（5）建立第三方支付異常交易態樣：111年金管會已

請銀行公會建立第三方支付業者及其賣家異常交易態樣，並提供予金融機構納入「存款帳戶及其疑似不法或顯屬異常交易管理辦法」第16條所定之預警指標及內部作業規範加強控管。

9、物流隱碼措施:

（1）「加強電商業者資安維護」建構數位信任，推動電商資安健檢，並推動主要電商導入國際FIDO(身分識別，Fast IDendity Online, FIDO)標準與應用，導入隱碼技術，提升民眾對電商資安信心，安心購物，從源頭降低詐騙風險。

（2）經盤點電商業者與其外部企業合作過程中，傳遞客戶電話資訊物流配送為其中一大宗，物流隱碼技術即是針對該程序所規劃的防堵機制。物流隱碼技術係將原訂單收貨人的聯絡電話號碼轉換為代碼，宅配單上同步進行隱碼處理，經由電商平臺提供2項資訊(訂單編號、客戶電話)給物流隱碼服務商供轉接，經服務商回傳代表號、撥接代碼，送貨單只需列印系統代表號、撥接代碼，即可與訂單收貨人聯繫，確保物流運送過程民眾電話個資安全，解決過去宅配單上會顯示客戶電話，容易不慎落入詐騙集團問題，進而擴及後續如釣魚、各種詐騙攻擊等發生。

（3）數產署於112年7月13日舉辦「推動物流隱碼服務研商會議」，三大電信業者一致同意配合推動隱碼共通介接標準，以「分享隱碼技術，推動共通標準」為辦理主軸。另數產署並於112年8月9日邀集三大電信及14家電商業者召開物流隱碼服務之推動辦理說明會，分享隱碼技術及執行方法。至112年10月底已有3家（MOMO、博客來、遠時[friDay購物]）業者導入，3家業者（東森、

PChome、酷澎）進行場域驗證，另有2家業者（Yahoo、蝦皮）積極洽談評估中。

（4）推動零信任架構即是基於「永不信任，持續驗證」理念，重複、多方驗證身分資訊，利用不同的驗證工具（例如：TW FIDO、電子簽章）來查驗經手的交易或文件，提高身分驗證的安全性和效率，讓假帳號或電子郵件無法通過身分驗證，避免網路身分遭冒用，確保個人資訊不會被未經授權的單位或個人濫用，從訊息源頭杜絕詐騙。

10、建置「111政府專屬短碼簡訊平臺」：

鑒於有心人士偽冒政府機關發送手機簡訊，誘使民眾點擊惡意網站連結，導致民眾個人資料或財產被竊之詐騙案件頻傳。數發部建置「111政府專屬短碼簡訊平臺」，提供各級機關發送政府簡訊，讓民眾識別111短碼，即可確認簡訊安全無虞，達到打擊詐欺策略行動綱領「減少接觸、減少誤信、減少損害」3減目標，以全面降低詐騙受害事件。

三、打詐措施之效益：在政府從111年7月啟動「打詐綱領1.0版」，乃至於後續「打詐綱領1.5版」及「打詐五法」，調查研究發現在「資訊流」、「金流」及「懲詐國際合作」方面，所產生之直接影響如下：

(一)遏止人頭門號詐騙工具：

1、完成修訂電信服務契約：用戶使用電信服務涉詐時，電信事業得配合有關機關通知，暫停或終止該用戶之電信服務。已督導完成話務契約9家、IASP(網際網路接取服務，Internet Access Service Provider, IASP)契約4家、電路出租契

約4家。

2、已訂定業者受理申辦電信服務風險管理指引，強化電信事業落實KYC。

3、配合刑事局建置境外門號網卡比對分析系統：透過比對分析詐騙案件網路參數協助偵查。

4、行政檢查電信業者落實KYC：落實電信門號申辦之審核機制。

（1）每季行政檢查固網1家，112年已執行6家次。

（2）每半年行政檢查所有行網業者，112年已執行9家次。

（3）業者運用人工智慧(Artificial Intelligence,下稱AI)分析詐騙行為篩選高風險或可疑門號：配合警調分析涉詐異常行為，112年篩選7,127門。

(二)防杜簡訊業者幫助詐騙及建立惡意簡訊攔阻機制：

1、完成修訂電信服務契約：用戶使用電信服務涉詐時,電信事業得配合有關機關通知,暫停或終止該用戶之電信服務。已督導完成簡訊契約5家。

2、電信業者及財團法人台灣網路資訊中心(Taiwan Network Information Center,下稱TWNIC)配合司法警察機關通知,攔阻惡意網址:停止解析避免民眾接觸，112年1至11月間設定惡意詐騙網址32,329組。

3、電信業者依通知設定詐騙關鍵字及分析以攔阻詐騙簡訊：透過比對分析詐騙案件網路參數協助偵查，112年1至10月間攔阻731萬餘則。

4、精進詐騙簡訊攔阻機制：

（1）實施單日簡訊超量(30則以上)提醒及超過門檻後限制發訊機制。

（2）實施發送大量商業簡訊時，利用測試門號接收

檢查該簡訊是否為釣魚簡訊(含連結)，將可疑訊息轉送165，並配合警調作為。

（3）實施針對非綠色通道門號，系統自動篩選大量發送相同內容且內容含URL(Uniform Resource Locator)連結之簡訊，輔以人工檢核判斷是否有釣魚簡訊之疑慮。

（4）已召開「研商遏止大量簡訊詐騙會議」23次，並持續邀集165打詐中心與電信業者，研商詐騙簡訊樣態演變及應對措施。

5、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(One Time Password)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%，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(Short Message Service,下稱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。

〈5〉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。

6、協助偽基地台詐騙案件查調：召開「偽基地台偵測技術研討會議」2次。請業者配合實驗偵測偽基地台之技術可行性，並與電信偵查大隊間建立聯繫管道，每日通報疑似偽基地台出沒位置，並於追緝時即時提供資訊。

7、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%，詳圖8。

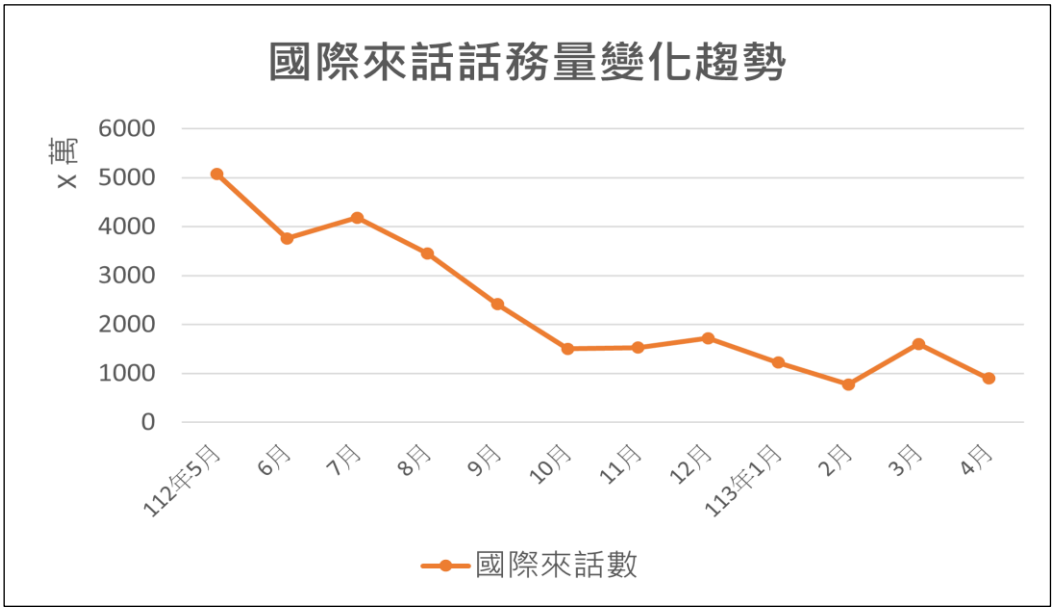

圖8　112年5月至113年4月國際來話話務量變化趨勢

資料來源：通傳會於113年6月3日座談提供書面資料。

8、「+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9，詐騙集團已大幅減少利用國際來話管道進行詐騙。

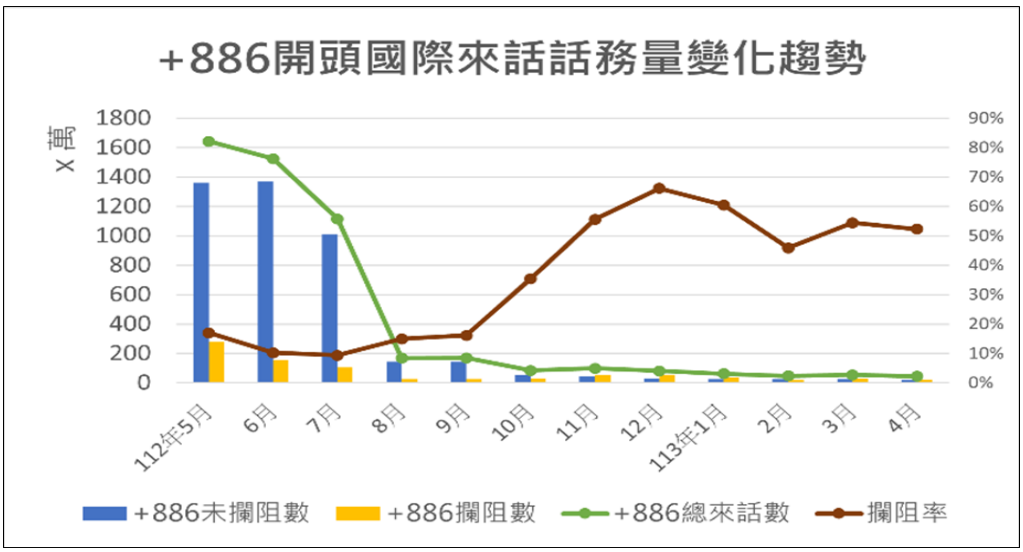

圖9　+886開頭國際來話話務量變化趨勢

資料來源：通傳會於113年6月3日座談提供書面資料。

9、「電信事業受理申辦電信服務風險管理機制指引」頒布後，主管機關已組成查察小組，截至112年11月27日辦理成果：

（1）宣導防制詐騙與電信門號管理共計228場。

（2）通傳會定期或配合檢警通知進行行政訪查共計34場。

（3）112年6月至10月間電信事業拒絕未符合KYC企業客戶之申辦約112家(約8,000餘門號)。

(三)網域停止解析部分：

1、TWNIC為利詐騙網站緊急處置，降低民眾遭受詐騙之風險，已擴大DNS RPZ(Domain Name System Response Police Zone, DNS RPZ)自律機制之處理範圍，針對高檢署、警察單位或調查機關、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或詐騙網站(含電商聯防)等4種重大案件，亦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。

2、詐騙案件常以詐騙網頁欺騙民眾洩漏個資、信用卡等資訊，以達其騙取金錢之目的。為降低詐騙集團以大量簡訊或廣告方式誘使民眾上當，透過屏蔽網站方式防止詐騙資訊進一步傳播，並提醒民眾注意確有必要。

(四)金管會110年迄今，就金融機構涉及洗錢防制、人頭帳戶管理缺失情形，詳表9。

表9　金融機構違反洗錢防制情形表

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(如予以糾正、裁罰等)
聯○商業銀行	110.3.2	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。	依銀行法第61條之1第1項規定予以糾正。
台○國際商業銀行	110.12.28	該行辦理他行行員開立於該行存款帳戶之交易持續監控作業缺失，顯示該行未能有效執行洗錢表徵交易之審核與通報機制，對於自動化交易監控態樣及參數設定亦未盡周全。	依銀行法第61條之1第1項規定，予以糾正。
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」專案檢查報告及一般業務檢查報告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。	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。	核處600萬元罰鍰。
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。	該行海外分行辦理防制洗錢作業所涉缺失一案，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200萬元罰鍰。
聯○商業銀行	112.3.31	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	核處150萬元罰緩。

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(如予以糾正、裁罰等)
		制法第7條第1項，同條第4項授權訂定金融機構防制洗錢辦法第5條及第9條規定。	
聯○商業銀行	112.9.15	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，有礙健全經營之虞。	依銀行法第61條之1規定，核處糾正。
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，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。
臺灣新○商業銀行	112.3.31	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。	核處1,000萬元罰鍰。

資料來源：金管會於113年6月3日座談提供書面資料。

(五)跨境詐欺犯罪辦理成效:

1、深化國際司法互助交流方面，法務部陸續派員參加包括APEC(亞太經濟合作會議,Asia-Pacific Ecnomic Cooperation, APEC)、EUROJUST(歐洲司法合作組織,European Union Agency for Criminal Justice Cooperation)、ARIN-AP(亞太追討犯罪所得機構網路，Asset Revocery Interagency Network-Asia Pacific)、APG(亞太防制洗錢組織,Asia/Pacific Group on Money

Laundering)及台越民事司法互助諮商會議等。

2、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，為我方與各國警政單位聯繫合作之第一線，有利於我方與駐在國執法單位之間進行即時情資交流。

3、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。

4、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，近期派遣案例有108年派員前往蒙特內哥羅與當地警方合作偵辦跨國電信詐欺案，以及在111年8月份派遣任務型聯絡官，前往柬埔寨協助人口販運專案，與當地政府聯繫救援我國國人返國。

5、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。

6、生效起至112年11月30日止，兩岸合作共同查獲跨境詐欺犯罪共118件、7407人；其中108年至111年查獲11件、112年迄今合作查獲32件(包含共同交換犯罪情資破獲1件)。

7、自100年迄112年11月30日止，大陸警方協助我方查獲遣返潛逃大陸刑事(通緝)犯381人次，其中112年已自陸方遣返犯嫌4人(臺南88槍擊案通緝犯2人、利用教師職權涉犯數起妨害性自主案通緝犯1人、槍砲及殺人等罪通緝犯1人)；大陸警方請求我方協緝遣返大陸籍刑事(通緝)犯共20人次，我方協助執行遣送陸方共7人次。在困境部分與前項兩岸共同打擊各類犯罪之困境相同，合作遣返人犯亦受政治大環境影響，惟法務部仍強化與陸方各項層面之交流，維持彼此互信關係，深化合作機制，配合民間協會參訪、學術研討會及定期業務性會議之民間交流，持續推動案件研商等各項合作事項，期能回復以往合作模式。

四、防制措施所遭遇之挑戰及困境:在政府推動一連串政策及修法後，電信網路詐欺仍持續高發，調查研究透過綜整防制措施所遭遇之挑戰及困境如下，以進一步發現目前政府防制措施所可能存有不完備或落後之處：

(一)詐欺犯罪由傳統面對面接觸轉為透過資通訊匯流隱匿身分：

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[33]、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。

(二)後疫情時代詐欺型態轉變：

1、假網路拍賣購物[34]、投資詐欺[35]及解除分期付款詐欺[36]案件持續高發：

109年起COVID-19疫情爆發迄111年後疫情時代,除衝擊國內各項產業獲利,致營利銳減民眾急迫尋求投資機會，且疫情期間民眾大幅減少戶外活動,居家上網宅經濟普及,致增進犯嫌藉由網路交友遂行詐欺契機。檢視111年間全般詐欺案件發生數前3名，依序為假網路拍賣購物(含一般購物詐欺)6,791件、投資詐欺6,542件及解除分期付款詐欺5,084件,其中相較110年發生數增加者,以投資詐欺增加33.4%最多、解除分期付款詐欺增加24.18%次之、假網路拍賣購物增加19.83%再次之。

2、投資詐欺於社群網站及網路廣告等管道密集投資：

投資詐欺藉由金融證券、境外基金、虛擬貨幣或博奕等名義在社群網站如Meta、臉書、交友軟體網站、通訊軟體(如LINE)或網路廣告等管道散布

[33] VPN Virtual Private Network ，虛擬私人網路:可透過已加密之網路協定將私人訊息在公用網路中傳送對方。

[34] 透過購物網站販售商品過程進行詐騙，常見可區分為買空賣空付款完未出貨、三方詐欺及團購詐騙前期正常出貨，俟取信大額匯款後未出貨等類型。

[35] 假借投資名義或任何以小搏大換取金錢方式，吸引被害人投入資金含虛擬通貨之詐欺手法。

[36] 詐欺集團假冒商家或金融機構人員，佯稱被害人購物付款方式誤選或遭誤植為分期付款，將按月扣繳商品之原價，誆騙被害人至ATM提款機依指示操作可解除分期付款設定，致被害人遭騙匯款。

投資資訊，吸引民眾加入特定理財群組後，復鼓吹至假投資網站、虛擬通貨交易平臺進行投資或博奕網站操作，藉被害人投入大量金錢欲出金時，即要求再匯入保證金、關閉網站或不再聯繫。

3、假求職結合囚禁人頭帳戶當事人：

歷年假求職[37]案件僅以騙取當事人證件或金融帳戶後施行濫用，於去年間復以施加囚禁當事人，犯嫌以簽約或給付報酬為由，引導被害人至旅館或租屋處，集中拘禁私宅管理、控制測試存摺帳號，以提升金融帳戶之存活時間及匯入贓款額度，並利用被害人兼作車手提款，減少犯罪集團之成本。

(三)詐騙集團組織分工結構層級分明，不易一網打盡，影響偵查能量：

1、詐騙集團採行層級管理、分工細密，組織結構一般劃分為金主及幕後首腦、核心管理幹部、話務機房、系統商、轉帳水房、車手集團、組織結構完整，且因加入管理要素，使該犯罪組織更具效率。各節點間彼此均透過通訊軟體代號方式聯繫，亟難掌握成員間真實身分，易致警方查緝溯源中遭遇層層斷點，鮮少查獲幕後首腦偵破整團犯罪組織。

2、針對躲避境外之詐騙集團，檢警調調閱金融機構金流交易明細回復時間冗長，且回復資料格式不一，彙整作業亦須花費大量人力及時間，形成查緝斷點，影響案件偵辦效能。

3、人頭帳戶及網路銀行約定轉帳，以及VPN國外IP層層轉出，檢警追查不及（包括外籍移工帳戶、獨資

[37] 假求職:於報章雜誌或網路訊息刊登求職訊息誘騙被害人，再以設定薪資轉帳等名義騙取被害人之金融帳戶及密碼等，用作詐騙集團人頭帳戶之用。

商號或人頭公司帳戶、網路銀行難以KYC等)。

4、經由第三方支付業者提供之信用卡、虛擬帳號、超商代碼繳費等方式取得詐欺款項(包括非特許行業、無資本額限制及無需登記)。

5、「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(包括法院做出對被告有利之認定,以及管理虛擬資產平臺及交易業務事業VASP指導原則未臻完善。)

6、傳統通訊監察無法有效監控通訊軟體之通訊。

7、透過台灣網路資訊中心DNS RPZ等限制接取方式雖得暫時達成即時防止個案災害擴大之目的,惟網路無國界,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,爰現況實難僅由國內單以DNS RPZ之技術手段達成遏止效果。

(四)有關現行詐欺查緝實務上,詐欺集團使用之犯罪工具(例如:網路服務、人頭電話、人頭帳戶、虛擬通貨等),基於電信、網路自由化與全球金融便利性,難以對使用者予以管制,致使前揭工具可輕易獲取利用於詐欺犯罪。

(五)人頭帳戶未能有效下降:

1、金融機構(銀行、中華郵政、信合社)警示帳戶[38]總數由108年27,970戶逐年成長至112年118,356戶,5年至少增加[39]90,386戶,增加3倍以上,詳表10。

[38]「存款帳戶及其疑似不法或顯屬異常交易管理辦法」第3條及第5條規定,法院、檢察署或司法警察機關為偵辦刑事案件需要,可通報銀行將存款帳戶列為警示帳戶,銀行應即通知財團法人金融聯合徵信中心,並暫停該帳戶全部交易功能。

[39]依據疑似不法管理辦法第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,如有必要,可再延長1年,故單一存款帳戶警示期間最長可延續3年,是以,前1年之警示帳戶,於次年會因為超過有效期限等原因而減少,故實際淨增加數會較統計數為高。

表10　金融機構警示帳戶變動情形

單位：戶數；%

	銀行	信合社	合計	較前1年增加	
				戶數	比率
106年	32,960	174	33,134	5,494	19.88%
107年	29,000	150	29,150	-3,984	-12.02%
108年	27,850	120	27,970	-1,180	-4.05%
109年	40,478	165	40,643	12,673	45.31%
110年	64,407	271	64,678	24,035	59.14%
111年	90,467	346	90,813	26,135	40.41%
112年	117,830	526	118,356	27,543	30.33%
113年3月31日	125,756	579	126,335	7,979	6.74%

資料來源：本院依據「金管會銀行及信合社警示帳戶辦理情形」整理。

2、各金融機構警示帳戶情形：

（1）警示帳戶前2大金融機構累計數均超過2萬戶，約占全部金融機構(39家)之4成，詳表11。

（2）中○郵政警示帳戶由111年17,058戶成長至113年第1季26,379戶，仍持續增加中。

（3）中○信託警示帳戶由111年20,213戶成長至113年第1季22,066戶，雖113年第1季較112年底略有減少，然仍占全部金融機構近2成。

（4）警示帳戶前5大金融機構，約占全部金融機構之5成5，詳表12。

表11　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○地銀行	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
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

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
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
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日座談提提供書面資料。

表12　前5大金融機構警示帳戶情形表

單位：戶數

金融機構	111年第4季	112年第4季	113年第1季
中○郵政	17,058	23,799	26,379
第○銀行	4,308	6,191	6,728
國○世華銀行	6,171	7,004	7,335
台○銀行	5,262	6,316	6,723
中○信託銀行	20,213	22,192	22,066
合計	53,012	65,502	69,231
全部金融機構總計	90,343	117,830	125,756

資料來源：金管會。

(六)打擊跨境詐欺面臨之困境：

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：

（1）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,情資交流僅能透過日本東京中央局的居間傳遞，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。

（2）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、跨境詐欺犯遣送主要爭議分為：

（1）國際部分：

警政署統計自105年起迄112年11月20日止，兩岸跨第三地詐欺集團案主動破獲49案，查獲臺嫌837人及陸嫌372人。困境部分如下：

（2）我國與多數國家無簽訂引渡條約，且各國法律制度及執法機關態度不一，因我國於國際地位敏感，與多數國家無簽定引渡條約，故跨境詐欺犯無法以引渡之方式回我國受審。遣返跨境詐欺犯目前以個案合作模式為主，需耗費龐大資源及人力，且需視詐欺犯出境國之政府執法及移民機關之態度，決定是否協助我國遣返詐欺犯。

（3）跨境詐欺犯之護照或旅行文件未失效，增添遣返難度，現行制度為遣返代替引渡，然跨境詐欺犯之護照仍可持有效之護照跨國移動，更增添追緝困難。

（4）兩岸部分面臨之困境：兩岸共同打擊各類犯罪及警政交流之默契，因近3年疫情及兩岸政治大環境低迷影響，致使兩岸共同打擊犯罪的合作與執行難循往例，即時與陸方進行案件研商、合作辦案及人犯遣返等。惟法務部持續向陸方傳達珍惜並維護雙方交流及共同打擊犯罪所累積之現狀與成果，以及合作偵辦案件之必要性，因此雖互動不如以往，仍有務實之合作案件進行中。

五、專家諮詢、研討會及出國交流所得建議：本調查研究除蒐整政府單方面之說明及公開資料外，於客觀之第三方見解方面，已透過專家諮詢、研討會及出國交流所得建議如下，發現政府防制電信網路詐欺相關措施之可能盲點，以資作為後續具體指出盲點所在之重要佐證。

(一)本院於2024台灣-英國『傳播媒體與新聞產製』雙邊交流」之研究分析發現如下：

1、英國在2023年10月通過了「Online Safety Act」，該法是源於【Molly Russell案】[40]而立法，其治理概念與歐盟「數位服務法」(Digital Services Act,下稱DSA，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，我們初步將歐盟及英國法令比較分析如表13，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，雖然這個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、「Online Safety Act」是由英國的數位文化媒體暨體育部(Department for Digital, Culture, Media & Sport, DCMS，相當於數發部)所推動立法，但執行單位是英國通訊管理局(Office of

[40] Adam Satariano.2022.10.1.British Ruling Pins Blame on Social Media for Teenager's Suicide.*The NewYork Time*.

Communications, 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)作為最終解決方式來解決數位平臺的所有問題，而是必須搭配「數位市場法」(Digital Markets Acr, DMA)、「人工智慧法」(EU AI Act)及「一般資料保護規則」(General Data Protection Regulation, 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。本次交流對於協助本院調查研究，指出政府目前的治理盲點確實有其參考價值。

表13　歐盟DSA及英國Online Safety Act初步比較分析

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

面向/法令	歐盟/DSA(Digital Services Act)	英國/Online Safety Act
		機制略有差異。
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

1. 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）
2. 英國成文法資料庫。(2023)https://www.legislation.gov.uk/ukpga/2023/50/enacted
3. 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。
4. 歐盟官方網站。https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package。

(二)調查研究共計辦理三場次專家諮詢會議，分別邀請識詐(事實查核與傳媒)、堵詐(資訊流及數位平臺治理)、阻詐(金流)及懲詐(詐欺集團研究、檢方及犯罪學學者)計10位專家學者針對客觀意見，摘述如下，完整記錄詳附錄A。

1、識詐面(事實查核與傳媒)：

(1) 國立中正大學傳播學系羅世宏教授:

〈1〉我覺得臺灣也許從傳播的角應該是要去蒐集案例普為傳播，就像我們反擊假訊息，不可能去查每一則，而且通常是事後，所以最好預先告訴民眾這次選舉可能會有哪些類型的假新聞，我們會預擬劇本，讓這些東西讓更多人知道。

〈2〉別人被騙之後，他願意公開出來，讓大家知道說這麼聰明的人也是會被騙。我最近看了韓國有一部電影非常好看，叫做金派特攻隊，這樣的一個故事，他把它戲劇化，收視效果很好，那看過之後會幫助民眾知道說會有這樣的事情發生。

〈3〉尤其現在新聞疲勞，現在讓重要事情讓全國人知道是一件困難的事情，但我們要用一些有創意的方法，包括戲劇化，包括跟網紅合作，去打造宣傳。傳統的政令宣導的這種短片，其實點擊率應該很低吧!

(2) 台灣事實查核中心邱家宜執行長：

〈1〉教育部到底在媒體素養這個事情上做了多少事？他當然已經成立了媒體素養推動會，有產生什麼具體的結果？當然我們其實NGO其實有在做，Google也有給我們funding做media literacy，可是系統性的、結構性的，

我覺得整個學校體系，教育部如果能夠多做一點，例如公私協力，那會更有幫助。

（3）社團法人全球反詐騙組織台灣分會理事長：中年婦女是他們很常去針對的一個群體，在某一套劇本裡面。家庭代工話術很多是以中年婦女為核心，然後還有另外一個的，他們殺豬盤也會是以中年女性為族群，那原因也很簡單，就是如果他想要騙錢的話，這群人是有儲蓄習慣的人，如果我的劇本是假交友，假投資的話，那這群人通常也是生活比較單純，而且可能在婚內是缺乏陪伴的，有感情上面的需求，所以對這群人要騙感情或是騙錢都是相對比較好處理，所以說官方統計跟我這邊統計可能會不一樣，我覺得是通報率太低，所以才產生了這個落差。就我自己統計大概七成的對象是女性，然後裡面大概有四成左右都被騙。他們很愛下這種廣告，就是什麼如何兼顧工作跟育兒和家庭，又照顧小孩，又同時有收入，他們有一陣子很常下這個廣告類型。

2、堵詐面（資訊流及數位平臺治理）：

（1）國立中正大學傳播學系羅世宏教授:

〈1〉我覺得平臺是一個關鍵，從預防角度，平臺成為詐騙集團更加容易去取信或是找尋受害者的工具。其實平臺就是在賣數據，平臺就是讓詐騙集團可以容易地找到特定族群的人，對某種訊息有感的人，然後會有反應，然後你發出交友邀請建立信任關係。很多人容易被詐，然後通常都透過臉書交友，之後變成轉到LINE更私密的聯絡管道當中，透過各種方式去經營信任關係。沒有人一開始就會受騙，但

是他如果能成功建立某種信任關係，那就有機會，只是大騙還是小騙而已。

〈2〉我覺得預防的這個部分就是我們有缺幾個法律上的東西，第一個就是我們對數位平臺的監管，目前其實是沒有法律。歐盟跟英國現在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它採取有有效措施，或者是這個notice and take down(通知/下架)的這個運作會比較有效。而且平臺要採取預防性的、有系統的一些措施，不是那麼純粹被動的，因為notice and take down現在其實就有在運作，只是如果涉及到沒有法律禁止的內容，要期待平臺可以有效的收到notice馬上take down，它可能不會照辦，因為沒有法律的的依據。所以我們必須要補這一塊，也就是數位服務法。

〈3〉「數位中介服務法」的一致性跟很多應該要配套的沒有考慮清楚，最後那個版本沒有通過。可惜的是這件事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一個機會。可能短期內都不太容易有重啟這個討論的機會。

〈4〉落地還是重要的，只是落地不能解決問題，所以你落地沒有法是不行的，也就是作用法的部分，所以數發部也是要加加油，還有防詐的法律現在草案作用法的部分都還沒有送出來。

〈5〉另外歐洲的公民的個資被保護的很好，至少

在目前的GDPR包括跨境傳輸都有規範，我們可以努力的去學習歐洲還有英國的這個線上安全法，他們都是民主國家，而且從民主的排名上面，他們比美國還前面，如果學這些國家的作法，我們就可以去defense說，我們立這些法不會違反民主的問題，是透明公開，而且是公正的，也有很好的立法諮詢跟公共聽證的過程。而且我們不是第一個，因為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。

〈6〉比方說，通傳會的數位中介服務法，他就是抄了歐盟的這個數位服務法在平臺規模方面的規定，如果你的平臺用戶超過人口數的十分之一的話，你就叫超大平臺(Very Large Online Platforms, VLOPs)，你就要要受到很嚴格的法遵監管；結果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。事實上200萬在全世界是很小的平臺，所以我就說，為什麼那麼的草率倉促，沒有做好研究，直接抄就抄出問題，連我們本土的小平臺都反對，那 Meta 跟 Google 都還不用出來反對，我們的網民、在野黨、各種小平臺都跳出來了，所以這個是他們很大的一個失誤。要不然的話，其實歐洲和英國已經示範過要怎麼立法，然後Meta跟Google也會願意善盡他們的法遵責任。

〈7〉最後我認為這個議題永遠是跨部會的，而且我們不能只看到打詐這件事情，因為它是數位時代的問題，詐騙只是比較顯性的部分，但

是跟數位關聯的有很多問題，防詐專法或許比較能針對防詐，但是數位的、非詐騙相關的問題就無法處理。所以我們還是要去通案的去處理數位治理的時候，就是DSA跟GDPR是要有臺灣版本，然後務實的調整，符合臺灣本地的這個需要，但不要比歐盟跟英國更嚴格，要更嚴格必須有很強的defense，因為可能會有侵害言論自由的問題。我們只要學歐盟和英國，甚至學到八成，我就覺得已經是很大的進步了。

〈8〉跨部會的機制非常重要，我覺得有一個例子是需要參考的，就是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。聽起來好像就是跨部會聯繫機制的論壇而已，其實不是，它是實際的組織，有行政運作的人力，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？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)。因為像詐騙或者是這個網路購物的這些糾紛，都需要不同的部分一起來努力，臺灣如果這些部會能夠合併成為一個有固定的、

政策性的跨部會的協調機制，而且是要定期去管考的，也就是說這個DRCF是要交出成績單的，而不是今天來開會找次長，甚至有時候是一個更低階的官員來，他可能也不太敢講話，這就是我們的跨部會過去很多都沒有什麼作用，層級雖然很高，但是效果不彰，那就是因為它是一個虛的組織。我們或許還是要有一個像DRCF的實體組織，我們甚至不用去討論說遇到什麼事情到底要找什麼部會，你就直接找DRCF，就會解決。

（2）台灣事實查核中心邱家宜執行長

〈1〉然後我們最近發現一個狀況就是二次詐騙，就是有一個假訊息說我們是律師團隊，如果被騙請跟我們聯絡，可以把錢要回來。然後那個是詐騙，他用的是一個新加坡的law firm的照片，你點進去之後，他就是叫你付錢給他，然後他會幫你要錢，那個律師事務所被人家盜用照片。然後他去跟平臺講說，這個是盜用的趕快把它封鎖下架。事務所說平臺都不理他，意思就是說，本尊已經出來說有人冒用名義去做廣告詐騙，**可是平臺不理他，我記得應該是Meta吧**。

〈2〉我總結一下，我們要怎麼去設計一個平台治理的法律框架，進而重啟平台治理的社會溝通，那當然也就寄望通傳會吧，就新任的委員或者也許是數發部，未來的就是兩部會怎麼樣去協調，行政院可能要站在這個就是敦促的高度，那教育部就是要去負責使用者端。

（3）社團法人全球反詐騙組織台灣分會理事長:除了這個機房本身之外，那他們還有另外的資訊

服務，就是架設詐欺網站，是由另外的系統去處理的，並不是由機房自己去維護。以詐欺網站來說，他們更新非常快速，通常是用一個模板下去架設，所以很多詐欺網站是很雷同的，然後網域也都會事先註冊起來，比如說他們可能一次就註冊大概十幾個銷售網頁，但不會十幾個同時用，他們通常先用一個網頁二到三個月，有被通報的時候，他們會跟被害人說系統要升級了要換新的網域，所以他們都會先鋪墊好，到被BAN掉，他們就會無縫地接到第二個網域，如果再被BAN掉，再換第三個，即便他們手上的網域都BAN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

（4）Gogolook劉彥伯總監：在內容審核部份，我們雖然可以要求Facebook要做廣告審核，但詐騙集團跑第三國去做廣告，第三國審核人員對臺灣的名人根本一無所知，所以基本上他看文字、格式都對就放行了。

3、阻詐面(金流):

（1）臺灣臺北地方檢察署姜長志檢察官

〈1〉我手上案子假設80件的話，至少有40件以上是詐騙，它已經是高達五成以上，而且40件的詐騙案裡面將近有30件都是人頭帳戶。

〈2〉監察院過去曾經有針對人頭帳戶開了類似的研討會，那當時給我們的結論，我看到報告的時候，我心裡面覺得很難過，報告希望我們要注意無罪推定、罪疑惟輕；可是委員今天找我來，我一定要跟委員反映，我所有的詐騙案之所以追不下去，最重要的就是人頭帳戶。因為為什麼？詐騙集團跟其他的犯罪組織很不一

樣，詐騙集團的組織是到處充滿斷點，他們的集團內部誰都不認識誰。

〈3〉一個大斷點就在人頭帳戶，被害人第一個匯款匯到人頭帳戶，我們每次追也只能追到人頭帳戶，除非我們有情資、有上線監視、有搜索，才有辦法往上游繼續查。可是如果人頭帳戶這點不處理的狀況下，我們就沒有辦法繼續往上追。如果我們今天檢察官要很輕鬆很好下班的話，我就全部給他不起訴就好，甚至就可以得到一個什麼人權檢察官的名譽。

〈4〉各位知道人頭帳戶的價格，他跟股市一樣，是隨著檢警的努力而有價格的波動，當我們檢警越查越兇的時候，現在已經高漲到一個帳戶130,000到150,000元，當年我剛出道的時候，人頭帳戶才2、3,000元。

〈5〉如果金管會前面不把他緊縮，後面案子就留到我們手上來了嘛，我追錢追不到，追人追不到，那最後我只能簽結，那對被害人有什麼意義?錢都沒有了也抓不到，那這要怎麼判重刑?

〈6〉金管會如果認為有法律保留的問題的話，那就修法授權金管會有這個職權，能夠每年對機構做評比，而且如果警示帳戶數量降不下來，就開始限制業務嘛。

〈7〉虛擬貨幣這個東西很重要，目前沒有人管，而且第三方支付竟然分2億以下的由數發部管，2億以上由金管會管的這種方式在管。各位一定要瞭解地下匯兌對國家影響多大，因為地下匯兌洗錢的問題，會直接作為總統大選介選的資金。我們一旦放手會動搖到民主和選

舉制度。

（2）警政署曾○芬專員

〈1〉從前面金流部分，如果銀行端發現這個帳戶有問題就凍結，把錢卡住的話，他們領不到錢，就斷了他們的生路。

〈2〉金管會是不是可以課責銀行，問題帳戶不要讓他們申請，或是罰錢之類的。

〈3〉從電信流跟金融業這邊去追源頭是比較實際的，比檢警從後面追直接多了，後面檢警真的花太多心力，快被壓垮了。

（3）金流面學者專家

〈1〉前端要想的，就是詐騙集團他其實要錢，那錢在誰的手上?

〈2〉以往人流物流都管得非常好，但是整個時代因為科技的變化，現在真正的重點在金流跟資訊流，那就是金融機構跟電信業，所以人流跟物流現在其實我們都規管的沒有問題，哪裡都要身分證啊。

〈3〉但是金流跟資訊流其實是沒有規管的；就金流來講，金流的部分有二個點，一個是金融機構不覺得防詐是它的事，它的想法是我是幫忙嘛。那為什麼他這樣想，他的想法就是說這都是檢警調的事，那講來講去，他高層其實不關心，所以各位委員，如果你們去看我們現在所有金融機構的董事會都沒有討論這(反詐騙)問題，其實這(反詐騙)就是最好的ESG的社會責任，但是從來沒有任何董事會討論反詐騙，社會責任都在討論放產假、有沒有給最低工資等等，其實如果要求ESG納入反詐騙去計分，那個對金融機構來講，那個壓力就很

大，它的股價受影響。

〈4〉第二個是金流會經過的不是只有金融機構，他現在全部都轉移到外面去了，也就是第三方支付跟虛擬貨幣平臺，這二個我們政府都聽起來是有主管機關，但是如果你去問他，他是從來沒有檢查；也就是說你去問他虛擬貨幣是金管會管理，沒有金檢過，從來沒有第三方支付是經濟部管，我們的法條也規定他要檢查，但是他從來沒有檢查。洗防辦公室報告說2021年詐騙就700億，但今(2023)年光上半年就1,400億，那一定是透過金融機構大家一起幫忙洗，要洗這麼大量的錢，這三個點(銀行、虛擬貨幣、第三方支付)就沒有看到防範措施嘛。

〈5〉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，可是法律有規定他要查核，那所以我講的這幾個，都是我們國家法規其實都有點到，但就是都沒有落實。

〈6〉雖然詐騙集團金流現在一直往外，但第三方支付和地下匯兌最終還是要回到銀行來運作，原因是走地下匯兌錢會被吃掉而且出金費用很高，但是在銀行的話，錢不會被吃掉，手續費又低，兩相比較下，詐騙金流最終其實是會回來金融機構。

〈7〉既然被害人要錢，加害人也要錢，所以我們去想這個制度的時候，應該都想錢在誰身上?很簡單就在處理金流的人身上，也就是金融機構。但是現在或許洗錢防制都有金檢相關規

定，但都沒有在執行，也沒有哪一家業務受到限制。但是美國2023年7月26日，眾議院已經通過《21世紀金融創新和技術法案》與《區塊鏈監管確定性法案》

（4）臺北地檢署林達檢察官

〈1〉我直接切入，問題在虛擬貨幣，目前我們可以看到這個金管會有做了很積極的解決，去年的9月26日有發布【虛擬資產平臺及交易業務事業基礎原則】VASP，裡面第九點提到了個人幣商的問題，那其實我們檢察官發現在實務問題上最大問題就是所謂個人幣商，因為我們抓到了許多的人，被害人都是匯到他的帳戶，結果他到地檢署就說，他是個人幣商，所以他不知道匯款的是詐欺被害人，因此我們拿個人幣商沒有任何辦法，所以最後就是大量的不起訴，當初檢察官呼籲以後，金管會也受到了壓力，所以他現在用VASP把個人幣商納入。

〈2〉但如果仔細看這個個人幣商的部分，它裡面的作法是說自然人從虛擬資產業務要向金管會申請法遵聲明，他的聲明裡也要跟法人組織相同。簡單說，金管會新的作業指導原則就是把個人幣商視同為法人，看起來它就對外宣稱，說他把所有的個人幣商都納管了，但我必須說這個在實務上沒有太直接的幫助。怎麼說，其實很簡單，在金管會的正常作業準則下，法人幣商其實要去做聲明，規範其實是相當嚴格，包含他的資安、責任準備金等等，以個人幣商要達到這樣的聲明，其實都做不到，所以也就會變成說，基本上除非說你是有公

司組織，有請技術人員才能做到。但金管會只是簡單地把個人幣商等同法人，但法條是沒有幣商的明確定義的，實務上幣商概念有兩種，一種是平臺業者，它設一個平臺讓人家來存放虛擬貨幣或者進行貨幣的轉移，這個我們會理解為一個保存或者是仲介或者是經濟服務的；但是第二種，我們現在實務上大量案件的幣商不是平臺這個觀念，他們只是個人投資客，他自己買很多賣很多，買賣進出這樣每年量很大。我們修法方向會說這些人都是幣商啊，所以你應該去法遵聲明，但這都是平臺概念，因此個人幣商在地檢署就會說我又不是要經營平臺業者，我只是投資客，我幹嘛要去聲明呢?所以就金管會立法說幣商沒有聲明應該要判罪，最後檢察官應該沒辦法起訴，就算起訴好了，我相信法院可能也不會判有罪。

〈3〉我個人有幾個建議的結論，第一個就是說我們在虛擬貨幣資恐打擊、資恐辦法裡面，是不是應該把對象的定義更清楚地劃分出來，把平臺業者和投資客兩種能夠劃分出來。那我們對投資客的部分要怎麼管理?那我們建議在一定的量以下，他其實可能真的就是一個單純的玩家就是甚至是被騙的被害人他一年可能進出次數不多，但有的人他常態每天進出，這種應該是一個資深重要的玩家，甚至以這個差價為獲利的，那在一定次數以上的就應該要給予某一種聲明或管制，換句話說要到金管會去做聲明的人，恐怕有兩種幣商，一種是比較高階品牌業者，他的門檻很高就像

法人；另一種比較低階的，聲明就簡單一點，讓大家都做得到。這樣規定之後，你就不能夠免除說你只是個人在買賣，你還是必須要比照營運的事業在做繳稅。那我認為說，虛擬貨幣上面有沒有可能畫出一個界線。如果說你虛擬貨幣會變成所謂個人利得，是以這個為主業，那就去繳稅啊；這種應該要在國稅局要有一個稅籍，你去做一個聲明，然後繳一定的稅。不可能說那邊不繳稅，另一邊也不做聲明，然後來地檢署的時候說你是幣商要免刑事責任，等到要起訴的時候，又說你不是平臺性質的幣商所以無罪。簡單說，我們覺得虛擬貨幣交易每年只要超過一定數量次數或金額的人，那你就去聲明，去工業局登記一戶，然後要有一定的教育訓練。那跟人家買賣的時候，一定要有對方的本人身分證字號等等，你都要做到。如果能夠把這樣的層級化做出來，我認為對虛擬貨幣的整個觀念會比較好，不要都直接用幣商這樣一個非常混淆的概念。

〈4〉再來是第三方支付，我自己個人辦過很多案就非常的痛苦，因為以前最多的碰到匯款帳戶是虛擬帳號，譬如說玉山銀行，我們問說這個帳號是誰的？結果他就要函復我們說是虛擬帳號，這個虛擬帳號是由某某第三方支付公司發出的，我們就要發函去給那個第三方支付公司函調說這個帳號是你們發出，那請問你們是幫誰代收代付啊？然後八成的案件發過去都不會回函。我怎麼辦？我案子那麼多，只好就結案了。假設我積極一點去查那家公司負責人，然後就把他傳喚來，他要嘛就不

來，就算來了，我請他告訴我幾月幾號這一筆六十五萬，為什麼會是你在代收代付，他說檢察官我回去查一下，他回去以後呢就翻箱倒櫃，其實他們就是詐騙集團的，他就隨便拿出很多張的契約書，然後說這個是林達委託的，簽名的人是林達，那我就傳林達來，林達一來說我沒有簽過名啊，曾經遺失過，結果還是不起訴處分，後來就不查了，因為沒有意義啊。

〈5〉我覺得具體的建議，首先第一個就是所有交易所熱錢包應該要公開，他應該是一個可以被監管的內容，就是熱錢包的意思就是歸戶錢包，我舉例來說好了，比如說幣安、火幣大家比較熟知的幾個交易所，其實交易所就會是洗錢的斷點，合規的交易所的話，基本上檢警都調得到KYC資料，所以我們至少會知道說某一筆資料中間經過很多次的層轉，層轉之後，假設要從幣安的某一個用戶的錢包出金，那我就會找幣安去調那個用戶的充值錢包地址KYC是誰?我就會知道資金後面要跑去哪裡。這個做法有個前提就是熱錢包應該要被公開，那我們在做金額追蹤的時候才好去判別說現在看到這個錢包是私人的非託管錢包，還是是屬於交易所的熱錢包?那以現在臺灣水房來說，他們最常用的其實是一家在柬埔寨的交易所叫○○，但是我們管不到○○。

（5）社團法人全球反詐騙組織台灣分會理事長

〈1〉有關虛擬貨幣在產業鏈扮演的角色，有一部分金流是走反方向，用匯款或是面交現金的這種做法，但到後面七成案件都是以虛擬貨幣方式出去。也有一開始就是直接走虛擬貨

幣的，其中特別是裡面的USDT穩定幣，這一類的不法所得其實是會被在區塊鏈安全標註為黑U，這些黑U要如何去洗白?就會是一個對於洗錢方很重要事情，通常會用社群媒體去找可以做兌換的，然後慢慢把黑U消化掉，用各種平臺去做洗錢，中國那時候還弄一個斷卡行動，當時候凍結了14億的帳戶，包含留學生要去開帳戶都會變得非常困難，洗錢很難把錢匯出來，因為這個緣故，很多機房就放棄了中國盤轉做臺灣盤，現在就轉做歐美盤，對象還是在歐美的華人。

〈2〉以詐欺來說，他們真正想要的東西是財產，所以目標就應該要放在金流，去降低整個詐欺產業鏈的獲利，所以核心要處理就要變成是洗錢了，回到虛擬貨幣增強反洗錢的這個能力，應該是現行唯一可以去處理的課題。

（6）Gogolook劉彥伯總監:剛才有提到金流，因為其實詐騙有分兩塊，一塊是他透過原來的臺灣本地的金融把這些錢洗出去；另外一種是透過線上或信用卡的方式來做持續的詐騙，所以金流方面，我們過去可能會要求銀行做一些SOP來控管，但事實上，詐騙還是可以透過交易貨幣或其他方式把錢轉出去，這我們在東南亞市場都看過。

4、懲詐面(詐欺集團研究、檢方及犯罪學學者)

（1）中央警察大學外事警察學系 孟維德教授

〈1〉我也曾經分析過有派與不派駐外執法人員的國家在追緝這個跨國犯罪；有派駐執法人員的國家破案率高很多，我建議外交部可以的話，應該是可以讓我們的外館，多接受一些法

務部或內政部的執法人員，應該有助於我們偵辦跨境洗錢。

〈2〉詐騙集團的組織結構不是像幫派，而是非常的鬆垮、扁平、彈性的，他們絕對不是以詐騙集團的分子來自居，他們是以生意人的身分自居，大家是一起來做生意的，因此誰在集團裡面創造大的利益，誰講話就大聲。

〈3〉犯罪的人多半都是把坐牢當作犯罪的成本，只要不查扣到他的不法利益，他都覺得值得，假設騙800萬判3年有期徒刑，他都會去犯法。

〈4〉即使徒刑增高了，但是你擋不到他，因為當刑罰不確定時，再高的刑罰也是沒用的，所以重點在刑罰的確定性，你能不能逮到他？你能不能查扣他的犯罪不法利益？這是重點。

〈5〉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）臺灣臺北地方檢察署 姜長志檢察官

〈1〉昨天才發生一件事臺南地院的法官把那個詐騙跟吸金案的被告，全部在強制處分庭全部把他放走，我們有扣到他們的教戰守則，就教怎麼應對檢警的對話，那有教戰守則，他(法官)竟然還是認為沒有串證之虞，然後直接把人全部放走，那這個會對我們造成未來，造成政策上有多大的阻礙。

〈2〉再來第二個關於抓車手的科技偵查能量和偵查技術要怎麼提升，真的要請委員多多關心科技偵查法，有科偵法就不用派臥底，手機就可以植入木馬做臥底。沒有科偵法，我們不僅

不能滲透詐騙集團，反而被詐騙集團滲透。

（3）警政署 曾○芬專員

〈1〉受害者覺得他錢追不回來，有些人就根本不想報案，其實目前的狀況就是這樣。

〈2〉檢察官跟警察在後面苦苦的追趕，因為犯罪手法是不斷翻新的，犯罪手法會結合最新的科技，然後不斷的演變，這就是為何目前為止在斷源的部分，其實還是很難達到。

（4）國立中正大學犯罪防治學系許華孚教授

〈1〉近年暴力犯罪一直下降，但是詐欺犯罪成長了好幾倍，那我們也要學英國、日本怎麼去打詐，那我剛才說詐欺是全球化的現象，所以現在很多國家都立這種法律來打詐。

〈2〉我們可以看到一個數據，我們大概詐欺有起訴的有5萬多人，但是真正被判定入監服刑只有1萬6,000多，表示說只有三成判定有罪，其他陸陸續續交保的七成的人，交保出去還是持續在騙，像在美國有毒品法庭、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〉檢警的犯罪偵查手段是有限的，包括電信流反向追蹤偵查還有相關機關查緝的配合度很低，還有通信軟體監聽還有國際司法互助，此外證據搜查不易，尤其現在很多機房都是在國外，證據取得很困難。

〈4〉刑事司法嚇阻力低，會考慮成立那個詐欺專法原因就是我們刑事司法過程非常冗長，然後犯罪的利益大於這個罰則，所以很多人交保後，又再加入犯罪集團持續犯罪。

（5）詐欺集團組織研究：社團法人全球反詐騙組織台灣分會理事長。

〈1〉機房通常是由誰去開設的呢？大多是跟臺灣幫會有關聯，比如說像○○會、○○幫，他們通常在組織裡發展27~29歲間的，鼓勵他們去境外開代理線，這個人會再帶十幾個更小的去那邊起頭，在機房裡工作。還有更大型的機房像連鎖企業，還會有另外的角色去督導不同機房的運作。緬甸的話就會落在緬北跟緬東，緬東的話就泰緬邊境那一帶，就是○○○、○○○，大家應該有聽過○○○的話，就是KK園區的所在地。然後○○○的話，就是落在水溝谷，○○○就是世界上最大的園區，規模大約三萬人。

〈2〉組織架構圖他們有一定的分工，首先是財務、客服，當一個金流進來，他們金流有走虛擬貨幣和法幣，假設做臺灣盤的話，一定要有人去收那個錢，那錢怎麼收?就要同時搭配本地的水房跟車手，就是跟車隊搭，如果他們走匯款的話，那就是跟水商、水房搭，水房就要去收人頭戶，所以水商又會再跟收簿集團搭配。人事部分是負責招募境外機房的基層工作人員，可以把它想像成HR人事的角色，那之前人口販運會變得很嚴重，就是因為境外機房那時候大缺工，所以詐騙集團開始用騙招的方式來招人，以前的話找人都用正招，通常都找一樣是找幫會，或是比較有幫會脈絡的人，說要不要去那邊作假之類的。但後來因為中國打擊，造成大缺工，那時候就開始大量騙大馬華人跟臺灣人，所以才造成臺灣人口販運的

問題。總之，本來是做正招，後來轉成騙招，騙招就跟你講說是去做博弈不會限制你自由，後來發現這個可以，他們就再編更大的謊言，比如你去那邊是賣佛牌或去當翻譯，然後就騙了一大堆人去。

(三)高檢署履勘會議紀錄

1、法務部檢察司郭司長永發:

（1）法務部刻正推動「被告總歸戶」，以減少案件，實務上一個帳戶可能有很多被害人匯款，在只有一個被告的情形下，因為被害人眾多，又分別向不同警局報案，就產生不只1件案件，案件再移送轄區地檢署，產生重複調查情形。推動「被告總歸戶」，就是把全國各地被害人報案資料集中由被告戶籍所在地警局調查，如此不會產生重複調查，並在案件調查完後移送或報告轄區地檢署偵查，也可減少案件量，檢察司也將定期召會追蹤執行成效至案件量確實降低。

（2）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，目前只能請偵查檢察官，針對被告惡性重大之案件具體求刑，公訴檢察官確實執行公訴蒞庭，若判決刑度過低時積極提起上訴；刑法已無連續犯規定，改採一罪一罰，法院針對被告犯罪行為分別判處之刑期加起來2、30年，但因為要定執行刑，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，就此法務部會持續與司法院溝通。

2、高檢署臺南分署吳主任檢察官慧蘭

（1）「窩裡反條款」一直以來都有持續在討論，「窩裡反條款」對貪瀆及毒品案件的查緝有很大的

幫助，為何在詐欺案件卻沒有積極推動立法，主要考量2個因素，首先是組成樣態不同，毒品、貪瀆犯罪集團是向上延伸，但詐欺集團是扁平化的組成，賣帳戶、車手、機房各別都是一個獨立的集團；再者是詐欺犯罪，法院的判決的刑度原本就不高，如果被告供述出介紹賣帳戶的其他人，因為有「窩裡反條款」規定，又獲得減刑讓刑度更輕，民眾是否可以接受?因此關於「窩裡反條款」還在審慎研議中。

（2）在這些廣告下架後，可能經過微調又再上架，Facebook是否可以利用AI方式清查，因為Facebook是境外公司，又涉及商業利益，在無法源依據上，檢察及行政機關要約束，確實有困難。

3、高檢署劉檢察官海倫:

（1）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，並將量刑因子納入考量以協助法官量刑，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，主要還是因為法院認為量刑是法官的裁量權。

（2）之前我曾調國兩司辦事，據我所知，因為國際情勢，「引渡」又是國與國關係，迄今臺灣沒有跟任何一個國家有成功引渡的案例，目前所採取的方式是撤銷身在國外的我國籍被告的護照，再以遣返方式將被告送回臺灣，即便如此還是很常在被告臨上飛機前，當地警方才告知要將人送到對岸而不讓被告上飛機，這部分雖然突破有難度，但仍會持續努力。

4、臺北地檢署劉主任檢察官仕國

（1）而現在司法實務，法院不分案件，幾乎全部都是從低度刑開始量，而這量刑依據判決實務，檢察官還不能干涉，除非檢察官要明確指出量刑有違法之處，否則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）而量刑最奇特的地方，還有在法院定執行刑時，更是容易產生爭議，例如，詐欺車手，犯了20次，每次都判1年，這20次合超來定一個執行刑時，只要超過1年，20年以下就是合法的，也就是20次犯罪都判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。大家看看現在有哪個幫派組織不插手詐欺行業？

（4）我們看到現在詐欺集團用1個帳戶20萬元的代價收購銀行帳戶，許多年輕人趨之若鶩，導致詐欺犯罪年齡層一直在下修，這些提供帳戶的人一旦被查獲，偵查中現在都不會說自己是賣帳戶的，反之，都會提供當初跟收購者間虛偽的LINE對語截圖，證明自己是因為求職、為了辦貸款……等各種原因被騙去提供帳戶的，最後因為證據不足，很多都是不起訴，起訴也很多判無罪。

5、新北地檢察署黃主任檢察官筵銘：詐欺案件中，絕大部分提供人頭帳戶、門號案件中的被告，在社會上往往是經濟弱勢，雖然他們犯罪是事實，但有時

候法官會認為判太重這些被告也繳不出易科罰金的錢。

(四)本院派員出席蒐整檢察官打詐實務暨修法研討會意見,會中邀請立法者、學者及基層檢察官提出政策建言，對於調查研究有重要價值，詳附錄C：

1、臺北地檢署蕭永昌檢察官

（1）大家知道詐騙一騙再騙，交保出去他接著就繼續騙,把他這個交保錢賺回來。但我們能夠不讓他交保嗎?檢察官這邊都要花很多的心力去做一些分析,甚至法律上的攻防,那現行的這個羈押規定是否夠用?

2、金門地檢署施家榮主任檢察官

（1）對於被害人來講,這樣真的算破案嗎?警方把大部分人力都投入在人頭帳戶，因為人頭帳戶好查,因為人頭帳戶直接有證據,他匯入哪個款項就抓誰，這最輕鬆嘛!可是這些人頭帳戶、車手取款等等,這些對他們來講就是工讀生、就是免洗筷,你查到這些有什麼用?他永遠都沒有被瓦解!

（2）對被害人來講,錢又沒有追回來,你沒有扣後面的詐騙錢，又沒有返還，你怎麼可以說你破案?所以老百姓的感覺就是你都沒有破案啊!宣稱破案率90幾趴，那是什麼碗糕?

（3）當人頭帳戶金管會一直沒有辦法斷絕，每年都有幾萬個人頭帳戶要辦，警方光是辦那個就飽了。當時是有一些亂象就是譬如說一個帳戶可能有10個被害人匯入,那就在10個分局報案,然後就10個地檢署受理，所以看起來案子會一下子暴增很多，都要辦的結果就是每個月分100件,你光是辦這些都爆了,所以你要期待檢方去

追查幕後的犯罪首腦或者洗錢管道?各位都有看過起訴書、不起訴書吧,如果要你坐在電腦前面，一個月要寫100份，你還有時間去做其他事嗎?可能召開專案小組要深入追查?這部分書記官可能更嚴重，我聽到已經持續5年以上，只要分發到新北或者桃檢書記官，他聽到是這2個地點他就不去報到了,所以你永遠在招考,但招考都沒用，因為他就不去報到。

3、台灣大學林鈺雄教授：

為什麼在打詐研討會討論科技偵查?因為你沒有科技偵查,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，那M化偵蒐設備(下稱M化車)這方面也是臺灣第一，因為中央一方面每年編列6、7,000萬在M化車預算，但是一方面禁用M化車，這個也是世界第一。所以我覺得我們在很多方面會有很少人有的獨創性的想法,當然也造就了我們這種畸形的現象。科技偵查比較關鍵的第3個部分就是設備端的通訊監察，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，因為我們科技偵查最後還是不會有設備端的通訊監察。

4、臺北地檢署姜長志檢察官

（1）金管會終於動起來,人頭帳戶他來處理,結果人頭帳戶處理之後，虛擬貨幣他就不管了。

（2）我們就起訴幣商，上到法院去說他也是犯罪集團一部分，法官判的都是無罪嘛，這能怪法官嘛？其實也不能怪法官，因為要怎麼證明他跟這些集團有主觀犯意聯絡？這對法官講也很困

難，雖然大家心裡心知肚明，我們是民主國家不能說關就關啊，現在只要發生問題全部把它刑事化送去判刑，送去判刑有效嗎？

（3）第一個我們強力要求金管會要開始做幣商的登記，如果你要經營幣商，你就要在金管會開始登記，登記這件事不要再甩鍋給別人，你的個人幣商沒有登記不可以營業，重點是你要修訂規則，什麼人什麼樣的條件才可以來申請幣商？你是不是有稅籍登記？是不是有公司登記？是不是商業登記都登記好再來跟我金管會登記，重點是你錢包要登記，你冷錢包、熱錢包，你的相關錢包金流就看得到。

（4）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！

5、臺北地檢署羅韋淵檢察官

（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的指引，去描述虛擬資產服務提供者應該要有所規範，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?甚至是法律依據不足?其實他們已經明確規定任何法人或自然人都應該要被定位，只要你從事這個虛擬資產的服務的話，那就應該要受到規範。

（2）我國最大的爭議是在哪裡?依據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條第2項，他所說的這個本事業，也應該依照這一個條款被規範，這個事業是已在國內設立登記者為限。也就是說，如果今天這位所謂的幣

商，他是以個人跑單幫的方式，他不去做公司登記商業登記，或其他的稅籍登記，那他就不會在這個辦法裡面被規範，那既然不在這個辦法裡面所規範，那主管機關也就沒辦法依照這個辦法去裁罰，對他做處理，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。

（3）FATF的相關指引也明確地指出，從事虛擬資產服務提供者必須取得相關證照，或者是許可，而且它強調這些虛擬資產服務提供者，應該要受到權責機關的監理或是監控，特別強調非自律組織。當然我了解金管會目前是想循序漸進的訂出業者自律規範，期待業者有所自律，不過自律依照目前的犯罪案件爆發，可能還是不夠。關於個人幣商的管制，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。

（4）我們很難期待規定每一個虛擬資產用戶都不能去使用非託管錢包，因為這涉及到人民財產權或者是隱私的問題，但如果今天這個錢包是用於商業使用，那是不是應該要課予業者要有一個呈報錢包地址的義務，不管是公司或者是個人幣商。再來一個是目前我國的洗錢防制法其實已經都施行了，但有個例外，第7條他規定的是轉帳規則，轉帳規則講的是，客戶要把虛擬資產轉給虛擬資產服務提供商的時候，那這個客戶必須要先說明資產的上一層來源是誰?什麼

姓名?以及他的基本資料，以及他轉進來的用途是什麼?轉出去的話也必須要跟虛擬資產服務提供商說明說我要轉給誰?做什麼用途?否則虛擬資產服務提供他就不應該准許這一筆交易。用這個方式來補強錢包地址可能是匿名的問題。

6、臺北地檢署洪敏超檢察官

（1）這個月初一個美國的幣流分析公司做了一個簡報，他說現在臺灣跟日本成為洗錢最終場地，原因很簡單啊，因為臺灣在國際政治上的地位比較比較沒人理啦，對有心人士而言很簡單，完成法遵聲明不如直接買下公司，就跟王牌交易所一樣也是直接換人嘛，上次我們證期局副局長說我們就禁止境外的，沒登記不准他進行招攬，但是大家看到這個招攬非常多啊!YouTube上放廣告都算招攬嗎?合約王者挑戰賽直接在臺灣辦算嗎?新加坡的MEXC抹茶交易所在臺灣辦，那這算不算招攬呢?

（2）第三方支付也是一樣，其實大家講了一大堆能量登錄，最後並沒有落實，事實上目前為止通過登錄的就是16+1家，我們原本統計的有多少家?1萬多家!代表1萬多家根本不鳥你!其實你看外勞，現在逃逸移工有大概將近8萬多人其實都是風險，我們不是有罪推定，而是他是一個風險嘛。他的帳戶怎麼使用我們無從控管，因為我們找不到人。

（3）黑莓卡這部分，我測試給大家看，我花250塊在蝦皮買的，實名制根本隨便輸入都可以過關，大家看這個IP是香港的，代表我就用這張卡之後，其實你沒有辦法掌握實際的身分。

（4）社群媒體去投放不實廣告，其實這個要處理這些網頁詐欺最快的方式就是用最短的時間、最有效率的方式、最簡易的程序去阻止，過往的方式都是向法院申請扣押，才再去TWNIC去扣，太慢了，所以最近因為創意私房，他改了一個緊急方式讓警察投單就可以，那這代表什麼?其實過往真的不需要透過檢方。

六、「打詐新四法」推動情形：在調查研究進行同時，政府仍持續強化打詐措施，近期主要以「打詐新四法」作為推動方向，截至113年7月16日，打詐新四法全數完成三讀[41]，其中科技偵查部分，於立法院審議時將由行政院版「科技偵查及保障法」草案內容改於「刑事訴訟法」增訂「特殊強制處分」，以放寬GPS及M化車之使用[42]。

(一)詐欺犯罪危害防制條例(即打詐專法)強化以下打詐面向，其中行政院草案經立法院審議後，三讀條文加重高額詐欺犯罪刑度，因詐欺獲益達新臺幣500萬元，最重可處10年有期徒刑，若獲益達1億元，最重可處12年有期徒刑，併科3億元罰金[43]：

1、各主管機關得以補助、獎勵或輔導方式推動防詐政策。並針對執行防制詐欺犯罪有功人員及檢舉人予以獎勵。

2、針對金融機構及提供虛擬資產服務之事業或人員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之相關強化措施。

3、友善被害人遭詐未被提領之款項返還程序。

[41] 行政院新聞稿。113年7月16日。行政、司法、立法三院合作 共同為國家打詐法制建立新里程碑。

[42] 聯合新聞網。113年7月16日。放寬科技偵查！GPS、M化車追犯人 刑訴法三讀通過了。

[43] 中央社。113年7月12日。打詐專法三讀通過 高額詐欺最重判12年併科3億罰金。

4、強化金融機構及提供虛擬資產服務之事業或人員違反相關義務之處罰。

5、強化電信事業管理部分：

（1）針對電信事業經通知用戶或使用電信人疑似或從事詐欺犯罪應採取之作為。

（2）電信事業受理申請電信服務、提供境外高風險電信事業漫遊服務及提供非本國籍用戶預付卡服務，應介接資料庫核對用戶身分與出入境狀態。

（3）強化簽訂國際漫遊服務協議應遵守之事項及停止服務之要件。

（4）受限制或停止電信服務之用戶再申請電信服務之限制。

（5）強化電信事業違反相關打詐義務之處罰。

6、強化網路廣告平臺業者部分：

（1）強化網路廣告平臺業者應指定法律代表之要件與該法律代表之權限及違反義務之處分。

（2）強化網路廣告平臺業者對刊登或推播廣告之義務及管理措施。

（3）強化網路廣告平臺業者揭露網路廣告資訊之義務與對涉及詐欺廣告之處理及通報。

（4）強化網路廣告平臺業者經通知刊登或播送之內容涉及詐欺犯罪嫌疑應採取之作為。

（5）強化網路廣告平臺業者違反義務之處罰、召集專家審議會議作成處分之規定及網際網路接取服務提供者或快速存取服務提供者違反義務之處罰。

7、強化第三方支付服務業者、電商業者與網路連線遊戲業者之防詐責任及對疑似涉及詐欺之事件採取相關作為之規定。

8、強化網路廣告平臺業者、電商業者與網路連線遊戲業者保存及提供資料之義務。

9、第三方支付服務業者、電商業者及網路連線遊戲業者違反義務之處罰。

10、處理詐欺犯罪防制緊急案件之處置規定。

11、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。

12、訂定詐欺犯罪被告自首或自白減輕責任之規定與假釋及不得假釋之要件。

(二)修正洗錢防制法：

1、修正洗錢行為之定義。

2、修正本法「虛擬通貨平臺及交易業務之事業」為「提供虛擬資產服務之事業或人員」;就從事交易受現金使用限制者之範圍授權法務部會同中央目的事業主管機關指定達「一定金額」者，並新增違反現金使用限制規定之法律效果。

3、增訂提供虛擬資產及第三方支付服務之事業或人員之洗錢防制登記、洗錢防制及服務能量登錄制度，就相關事項授權中央目的事業主管機關訂定辦法，並針對違反者課以刑事處罰。

4、修正指定之非金融事業或人員違反規定之罰鍰上限，並增訂「得按次處罰」之規定。

5、增訂非信託業之受託人於信託關係存續中，取得並持有信託基本資訊、實質受益權與其他受規管之信託代理人及信託服務業者基本資訊，應進行申報，資訊保存之年限，與金融機構及指定之非金融事業或人員建立業務關係或進行達一定金額之臨時性交易時應主動揭露其在信託中之地位，有關申報、更新申報之範圍、方式、程序、一定金額之範圍、揭露方式等事項授權法務部會商相關機

關以辦法定之，及違反義務之處罰。

(三)訂定科技偵查及保障法(立法院已於113年7月16日改以刑事訴訟法增訂「特殊強制處分」處理，並三讀通過)：

1、為規範偵查機關運用科技方法進行必要之科技偵查作為，以確保其合法性，切實保障人民基本權，並避免犯罪調查之手段落後於科技發展之腳步，影響國家安全及社會秩序。

2、偵查中檢察官認有必要時，得使用全球衛星定位系統或其他非以辨識個人生物特徵之科技方法追蹤位置;檢察事務官、司法警察官或司法警察因調查犯罪情形及蒐集證據認有必要時，亦同。

3、偵查中檢察官認有必要時，得使用科技方法調查行動通訊設備之位置、設備號碼或使用之卡片號碼;檢察事務官、司法警察官或司法警察因調查犯罪情形及蒐集證據認有必要時，亦同。

4、檢察官偵查或檢察事務官、司法警察官或司法警察調查最重本刑三年以上有期徒刑之罪，有相當理由認為具隱私或秘密合理期待之空間內之人或物與本案有關，得從該空間外，使用非實體侵入性之科技方法對該空間內之人或物監看及攝錄影像。

5、調查所得資料，除已供案件證據之用留存於該案卷或為後續偵查或調查目的有必要長期留存者外，由執行機關於調查結束後，保存五年，逾期予以銷燬。調查所得資料全部與調查目的無關者，執行機關應即報請檢察官許可後銷燬之。

(四)修正通訊保障及監察法：

1、因應近年來利用網路遂行詐騙、盜取個資或資安駭侵犯罪不斷增加之趨勢，修正該法關於調取通

信紀錄之限制，並增訂保存及調取網路流量紀錄之規定，以分析數位足跡有效打擊網路犯罪。

2、修正要點如下：

（1）定明網路流量紀錄之定義。

（2）為有效打擊快速傳播、匿跡之網路犯罪並兼顧隱私權保障，比照調取通信紀錄之程序，增訂網路流量紀錄之調取規定，修正通訊使用者資料由檢察官、司法警察官依職權調取，刪除調取通信紀錄須偵查「最重本刑三年以上有期徒刑之罪」之限制，並增訂檢察官得依職權調取通信紀錄及網路流量紀錄之罪名。

（3）定明建置網路流量紀錄保存、調取系統相關事項與費用、電信事業與設置公眾電信網路者協力義務及違反規定之處罰。

(五)網路平臺投資廣告採認數位簽章部分：

1、強化源頭管理：

行政院院會於113年5月9日通過《詐欺犯罪危害防制條例》草案，業經立法院113年7月12日三讀通過，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。

2、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。

3、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。

4、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。

(六)強化數位平臺治理:

1、強化數位台平治理之目的

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。

2、通傳會原擬數位中介法草案之疑義:

（1）通傳會前研擬之「數位中介服務法」草案，鼓勵數位中介服務提供者針對網際網路內容，依其服務使用條款採取合法且必要的自律檢視與因應措施。草案就數位中介服務態樣與規模區分不同類型，逐級課予特別義務，以公私協力模式因應數位中介服務衍生之問題，以及線上平臺服務提供者之重大系統性風險。

（2）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。

（3）由於網際網路包羅萬象，不可能以一部法案羅列所有違法類型，故內容之違法性仍須回歸各部會的主管法規，由各部會依其專業職責認定，及針對違法內容通知業者進行不同處置作為。目前相關部會亦已陸續就其職掌針對網際網路違法內容進行規範。

3、歐盟數位服務法之立法緣由、目的及與電信網路詐騙之關聯性：

（1）隨著網路用戶數量大增，中介平臺已具備如同守門人般的強大影響力，進而衍生網路違法內容充斥與基本權利危害等風險，甚至可能阻礙創新，故備受歐盟官方關注。此外，配合歐盟數位政策規劃之目標，透過法規制定強化平臺責任，補強既有電子商務指令20餘年無法因應時

代需求之不足。

（2）歐盟「數位服務法」係針對中介服務提供者進行相關義務及作為之原則性規範，包括中介服務提供者不具一般性監督中介服務傳輸或儲存之資料義務，並且不負有主動發現違法內容事實的責任。惟應具備申訴機制，並對遭到檢舉之違法內容負擔通知即取下或封鎖的義務。此外，歐盟「數位服務法」亦訂有線上廣告資訊揭露及線上交易賣家溯源等規定，然歐盟「數位服務法」條文並未針對網路電信詐騙直接進行相關規範。

4、我國數位中介服務法草案與歐盟數位服務法之異同：

（1）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。

（2）惟考量網路治理涉及跨國性議題，因此歐盟「數位服務法」明定每個國家須指定該國的數位協調機關，這些數位服務協調機構組成歐洲數位服務委員會，負責協調歐盟境內不同國家有關「數位服務法」之相關處理措施。而「數位中介服務法」草案則設有專責機構，採財團法人型態設立，透過多方利害關係人治理模式參與討論及決策，尊重民眾言論自由，並賦予平臺業者問責之機制，同時也避免政府行政權干預。顯見因應立法層次及涉及範圍不同，而有不同的相關組織設計。

5、數位中介服務法草案擱置後，通傳會對於高涉詐風險網路平臺之管理規劃：網際網路治理不同於傳統廣電高權監理模式，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。

伍、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10)[44、45]，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

[44] 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)。
[45] 105至112年，引用警政署資料，本院繪製。

提出之報告[46]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。

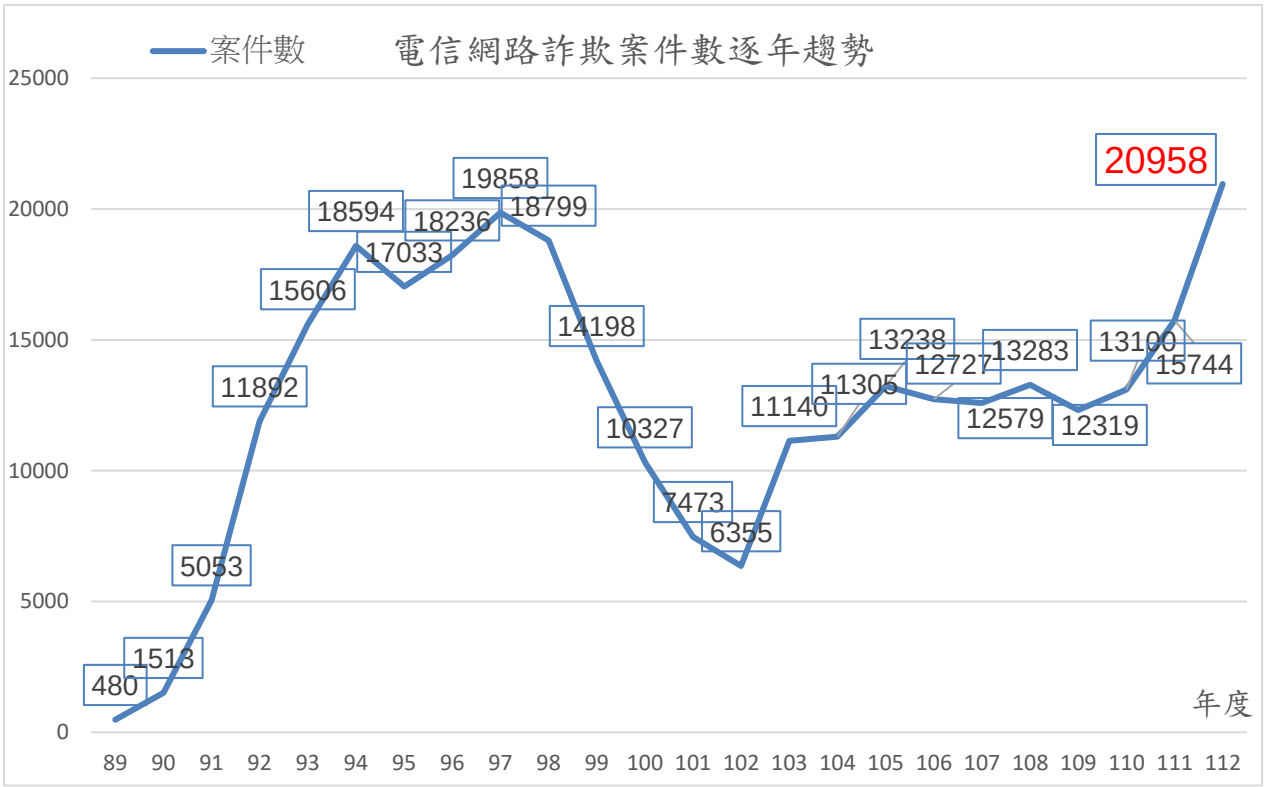

圖10　89至112年間電信網路詐欺案件之數量逐年趨勢（單位:件數）。

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[47]，本院自行整理。

[46] The Global State of Scams Report – 2022

[47] 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[48]，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[49]。

（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%[50]。

（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[51]。

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14：

[48] 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。
[49] 高檢署112年11月13日簡報資料。
[50] 高檢署112年11月13日簡報資料。
[51] 高檢署112年11月13日簡報資料。

表14　111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)[52]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，本院調查意見若依「識詐」、「堵詐」、「阻詐」及「懲詐」

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

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15，行政院及相關主管機關實宜予以正視。

表15　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[53]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

[53] 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16：

表16　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[54]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

[54] 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[55]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[56]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、標的物及監控缺**

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

[56] 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。

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」[57]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」[58]。

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[59]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

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

[58] 新世代打擊詐欺策略行動綱領1.5版，第4頁。

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

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17)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17　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）[60]，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。

[60] 「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[61]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」[62]，亦有金融機構報告[63]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、

---

[61] 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

[62] 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)

[63] 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[64]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%[65]，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**我**

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

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[66]；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『新世代打擊詐

教育部重編國語辭典修訂本[66]
https://dict.revised.moe.edu.tw/dictView.jsp?ID=18775&la=0&powerMode=0

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」[67]，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。

[67] 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）

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[68]；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「每年人頭門

[68] 「打詐綱領1.5版」關於堵詐面向，電信部分之說明。

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[69]，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[70]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

[69] 通傳會於本院113年6月3日辦理座談提供書面資料。

[70] 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」[71]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請約30萬筆門號，並自112年1月起，分成47次出

[71] 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

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[72]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18。

[72] 高檢署112年11月13日簡報資料。

表18　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11。

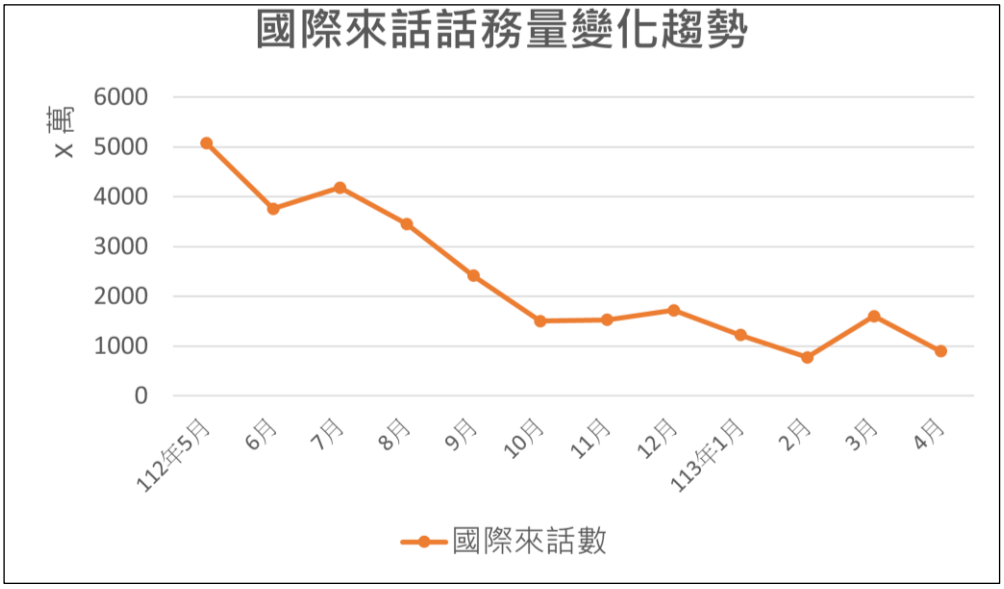

圖11　112年5月至113年4月國際來話話務量變化趨勢

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12，詐騙集團已大幅減少利用國際來話管道進行詐騙。

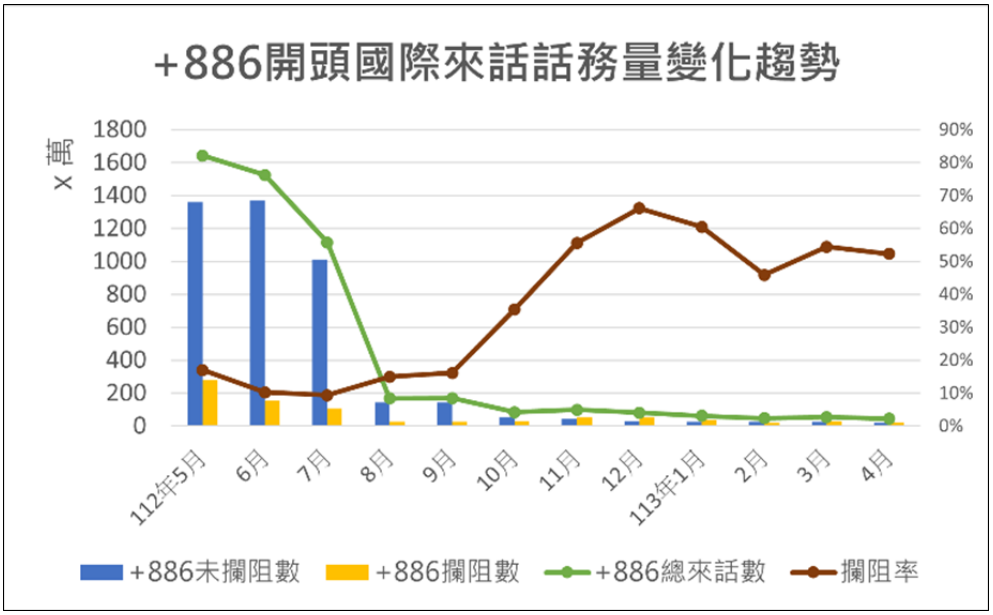

圖12　+886開頭國際來話話務量變化趨勢

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[73]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(詐欺防

[73] CU HK，香港MVNO業者名稱

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」[74]，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，包括全面禁止金融商

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

品推銷電話，以及禁用貓池[75](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，且對企業客戶幾乎毫不設防，綜合前述數據，無怪乎112年度

[75] 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)

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[76]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，或可部分解釋近年

[76] 通傳會。112年12月。112年通訊傳播市場報告。

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[77]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。

3、根據財團法人台灣網路資訊中心「2023年台灣網

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

路報告」

（1）2023年臺灣民眾的上網率[78]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[79]。

（2）美國各州敦促Meta打擊Facebook、Instagram假帳號行為[80]。

（3）韓國公正交易委員會在去年(2023)底向Meta公

[78] 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。

[79] 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

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

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[81]。

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[82])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[83]，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，惟該等措施仍有其侷限。

1、有關綠色通道及紅色通道等通報下架措施，警政

[81] 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)

[82] 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)

[83] 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。

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13：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。

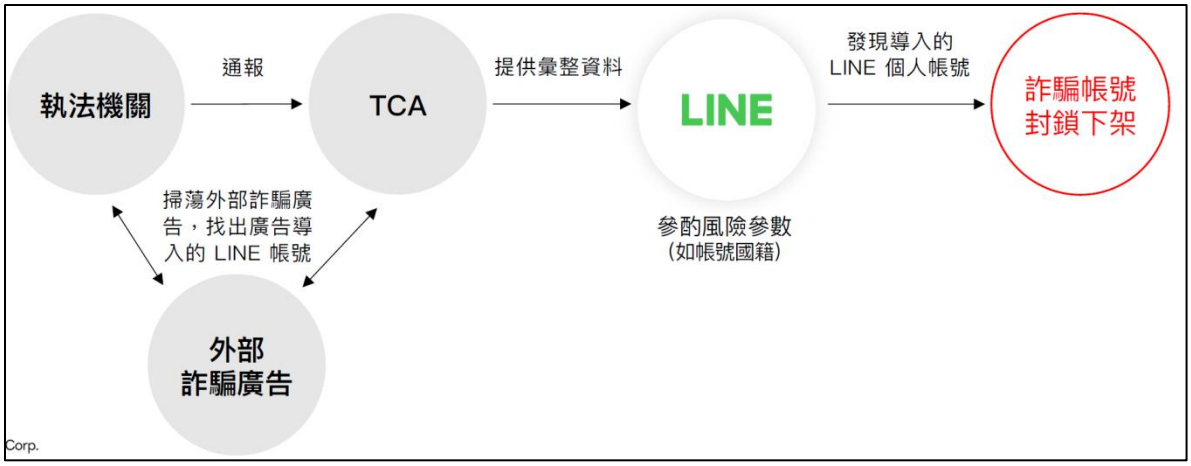

圖13　LINE公司投資詐騙高風險商業帳號檢舉下架聯防機制

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14，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。

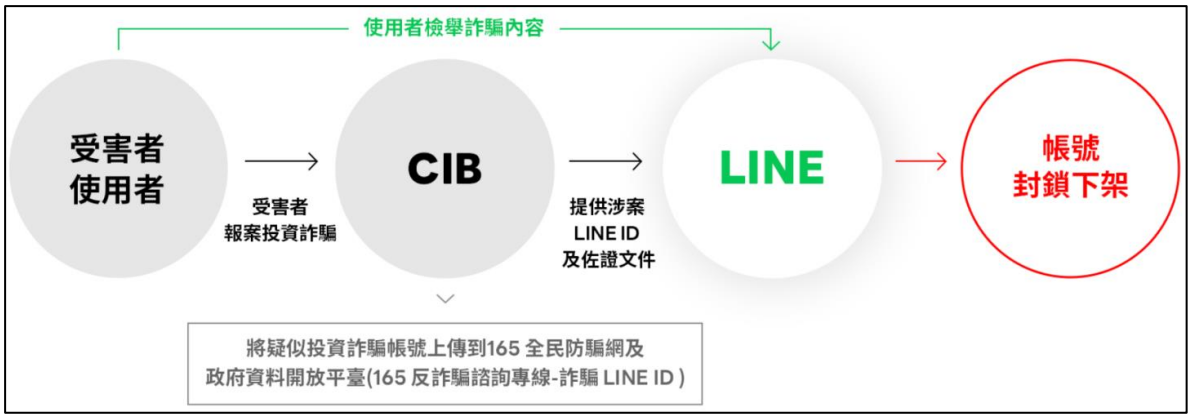

圖14　LINE公司投資詐騙刑事案件通報」下架機制

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[84]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

[84] 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。

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」[85]報導顯示，數發部所屬國家資通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

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

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15)；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15　社群平臺「假求職、真詐騙」廣告範例

資料來源：本院自行蒐整[86]

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，也引發

[86] 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)

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19。

表19　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[87]、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[88]。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。

(2) 資訊面：客戶申請約定轉入帳戶者，視客戶性質

[87] 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。

[88] 高檢署112年11月13日簡報

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[89]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，僅留下象徵性餘額者」等異常交易態樣。

[89] 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。

（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20，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20　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
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

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
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
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

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
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%[90]。

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

[90] 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。

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[91]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[92]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21，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

[91] 剔除警示帳戶未達1000戶之銀行。
[92] 剔除警示帳戶未達1000戶之銀行。

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21　110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
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	核處200萬元罰鍰

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
		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	
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150萬元罰緩
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。	核處1,000萬元罰鍰

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。[93]」。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」[94]。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[95]。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

[93] 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。
[94] 113年4月26日「檢察官打詐實務暨修法研討會」報告資料。
[95] 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[96]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。

[96]（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[97]，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?他一定要蓬勃發展嘛!

[97] 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

〈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[98]，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，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

[98] 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

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22，高檢署亦提出兩案說明資料庫績效。

表22　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[99]《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。

4、財團法人民間司法改革基金會(下稱司改會)則於

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

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[100]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

[100] 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[101]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、起訴檢察官及

[101] 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

涉嫌協助藏錢之法官均曾為大學室友之荒謬案情[102]，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[103]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。

（2）法務部透過內部及外部監督機制，若查有不法，

[102] 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）

[103] 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

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16，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：

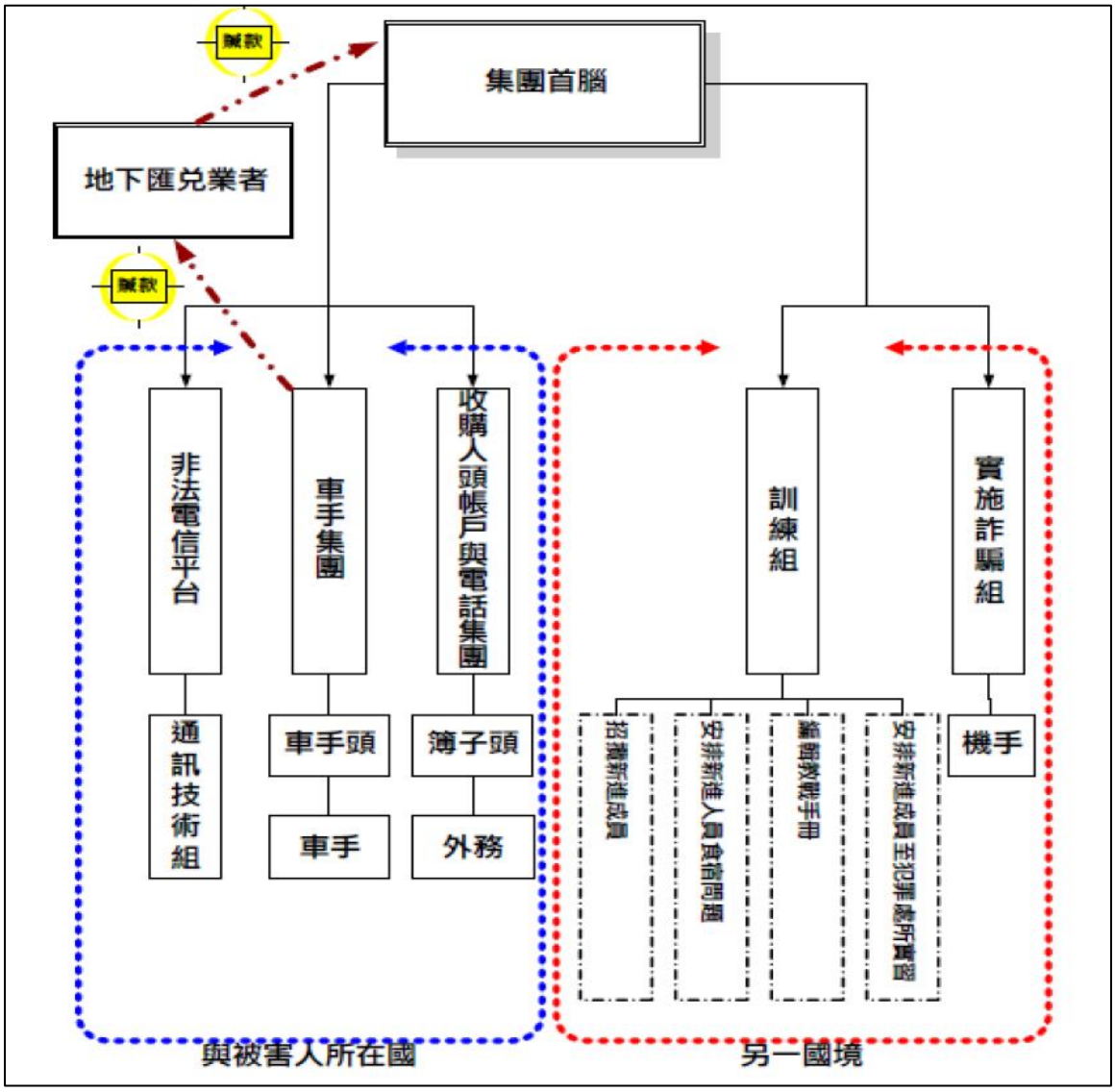

圖16　跨國電信網路詐騙集團分工圖。(資料來源：本院蒐整文獻[104])

(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[105]；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。

1、幕後首腦通常隱匿行蹤在各地流竄。

[104] 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。

[105] 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、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。

陸、處理辦法：

一、本通案性案件調查研究報告之結論與建議部分，送請行政院參處。

二、本通案性案件調查研究報告全文上網公布。

三、檢附派查函及相關附件，送請交通及採購委員會、內政及族群委員會、財政及經濟委員會、教育及文化委員會、外交及國防委員會、司法及獄政委員會聯席會議處理。

調查研究委員：賴鼎銘

范巽綠

趙永清

葉宜津

林文程

賴振昌

王麗珍

中　華　民　國　1　1　3　年　　8　　月　　1　3　　日

附件：附件:「調查案件人權性質調查回條」、本院 112 年 9 月 18 日院台調壹字第 1120800197 號派查函及相關案卷。

本案案名：政府防制電信網路詐欺之對策與檢討

本案關鍵字：電信網路詐騙、識詐、堵詐、阻詐、懲詐、打詐綱領

附錄A、本院諮詢會議摘要(依場次及姓名筆劃排列)

一、中央警察大學外事警察學系 孟維德教授

(一)當我們站在一個全球的角度看詐欺問題的時候，我們很清楚地看到是不是只有臺灣有，其實國外的損失不見得比臺灣小。

(二)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，我們在做大部分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。

(三)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，那這樣子的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。

(四)犯罪機會只會增加而不會減少。那麼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，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，而且我跟你保證，不會追上，永遠不會追上。

(五)在10年前，犯罪被害人最大量的不是詐欺，而是竊盜。詐欺是一直到最近，這兩、三年才成為臺灣犯罪樣態中最大量的被害人。

(六)被害人年齡我們再去看。18歲到39歲是詐欺的主要被害人。40歲以上的被害人詐欺就不是首位了。

(七)犯罪件數我們去年大概發生了大概19,000多件。但是呢，我們的被害人呢，竟高達了將近50,000個人，所以一件可以害很多人。

(八)我相信企業應該有不少的被害，但是企業可能顧及

到企業的形象，還有其他等等因素沒有凸顯出來。

(九)只要涉及到跨境跟跨國的這個詐欺案件，勢必一定要透過中央級的執法部門。警政部分的話要透過刑事警察局；地方的警察局對於這種跨國跨境的這種詐欺案件，在偵查上面是沒有辦法的，在組織的結構上，也是放在中央級的執法部門上。

(十)在中央級執法部門的資源，我個人覺得是短絀了。調查局大概有20幾個人派在國外，警政署大概有10幾個人派到國外，移民署大概有20幾個人派到國外，他們不見得是在做犯罪防制工作；個人是建議外館恐怕要多增設有關於執法部門的人員。

(十一)我也曾經分析過有派與不派駐外執法人員的差異；有派駐執法人員的國家破案率高很多，我建議外交部可以的話，應該是讓外館多接受一些法務部或內政部的執法人員，有助於偵辦跨境洗錢。

(十二)詐騙集團的組織結構不是像幫派，而是非常的鬆垮、扁平、彈性的，他們絕對不是以詐騙集團分子自居，他們是以生意人的身分自居，大家是一起來做生意的，因此誰在集團裡面創造大的利益，誰講話就大聲。

(十三)現在我們要做的，是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。詐騙集團他們會結交金融機構的行員或是朋友，也會結交電信業的朋友，所以他不像幫派那樣，他是非常靈活的。

(十四)各位不知道有沒有聽過地下匯兌，也就是地下金融業者，其實是非常大的洗錢管道。或許他是開飲料店、早餐店，機車行，你無法判斷這個做地下匯

兌的人平時是做什麼的，只有圈內的人找得到他。

(十五)犯罪的人多半都是把坐牢當作犯罪的成本，只要不查扣到他的不法利益，他都覺得值得，假設騙800萬判3年有期徒刑，他都會去犯法。

(十六)即使徒刑增高了，但是你擋不到他，因為當刑罰不確定時，再高的刑罰也是沒用的，所以重點在刑罰的確定性，你能不能逮到他？你能不能查扣他的犯罪不法利益？這是重點。

(十七)政府要給執法部門「科技對付科技」的資源量，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，才有辦法提高刑罰的確定性。

(十八)柬埔寨假設有我方的刑事司法人員，就可以快速處理，但是最近的在泰國，其他越南、緬甸、寮國、柬埔寨都沒有我們的人。

(十九)從研究本土的實證資料上，看不到詐騙集團的核心份子都是幫派這樣的證據。裡面可能有金融機構和電信業者，我們對於組織犯罪集團的概念已經要脫離幫派的概念。

(二十)臺灣並沒有允許臥底偵查的法。混入到犯罪集團，可能會要求他先做一些犯罪的事情，對公務人員來講是為難的，我們法律上也沒有許可。

(二十一)我補充一下，外派人員不能只是任務型的派駐，它需要培養當地的人脈，等到國內派任務給他的時候，他必須已經準備好了。

二、臺灣臺北地方檢察署 姜長志檢察官

(一)在整個詐騙犯罪裡面，最主要的兩大環節，一個是刑事機關，一個是檢察官，那如果檢察官崩潰撐不下去的時候，這個案子就是會不斷的滋長出來，那現況就是這樣。

(二)以我個人在臺北地檢署收案，我每個月收案收80到100件，意思就是這個月如果沒有減掉80到100件，我下個月還要再繼續收80到100件，那所以我們有很多學長姐現在身上背著3、4百件在轉，那各位委員可以試想，我們背著3、4百件，我們哪有能力去想說這個詐騙要追源頭。

(三)我手上案子假設80件的話，至少有40件以上是詐騙，它已經是高達五成以上，而且而且40件的詐騙案裡面將近有30件都是人頭帳戶。

(四)監察院過去曾經有針對人頭帳戶開了類似的研討會，那當時給我們的結論，我看到報告的時候，我是覺得心裡面很難過，報告希望我們要注意無罪推定、罪疑惟輕；可是委員今天找我來，我一定要跟委員反映，我所有的詐騙案之所以追不下去，最重要的就是人頭帳戶。因為為什麼?詐騙集團跟其他的犯罪組織很不一樣，詐騙集團的組織是到處充滿斷點，他們集團內部誰都不認識誰。

(五)一個大斷點就在人頭帳戶，被害人第一個匯款匯到人頭帳戶，我們每次追也只能追到人頭帳戶，除非我們有情資、有上線監視、有搜索，才有辦法往上游繼續查。可是如果人頭帳戶這點不處理的狀況下，我們就沒有辦法繼續往上追。如果我們今天檢察官要很輕鬆很好下班的話，我就全部給他不起訴就好，甚至就可以得到一個人權檢察官的名譽。

(六)各位知道人頭帳戶的價格，他跟股市一樣，是隨著檢警的努力而有價格的波動，當我們檢警越查越兇的時候，現在已經高漲到一個帳戶130,000到150,000元，當年我剛出道的時候，人頭帳戶才2、3,000塊。

(七)今天講的很多都是沒有意義的，一開始源頭就不控管他，銀行端的努力對我們來說是幫助很大。因為在人頭整個KYC做下去之後，人頭帳戶整個量有慢慢的縮減中，有被逐步的控管。

(八)如果我的心力全部都在人頭帳戶上面，就沒有精力去處理其他更重要的案件，我根本沒有時間動啊。

(九)昨天才發生一件事臺南地院的法官把詐騙跟吸金案的被告，全部在強制處分庭把他放走，我們有扣到他們的教戰守則，就教怎麼應對檢警的對話，那有教戰守則，他(法官)竟然還是認為沒有串證之虞，然後直接把人全部放走，那這個會對我們造成未來，造成偵查上有多大的阻礙。

(十)如果金管會前面不把他緊縮，後面案子就流到我們手上來了嘛，我追錢追不到，追人追不到，那最後我只能簽結，那對被害人有什麼意義？錢都沒有了也抓不到，那這要怎麼判重刑？

(十一)金管會如果認為有法律保留的問題的話，那就修法授權金管會有這個職權，能夠每年對機構做評比，而且如果警示帳戶數量降不下來，就開始限制業務嘛。

(十二)我們發現最新的趨勢，從過去的遊戲臉書詐騙，開始走蘋果的禮物卡，我們在高檢署開會發現蘋果根本不配合嘛，我們一定要開搜索票，蘋果才願意給我們ID，回復的時間都半年一年，錢早就不知道轉到哪裡去了。主管機關為什麼不跟Apple公司談說如果你不配合快速提供資料，就停止發卡？他販售這一種這種不能夠控管的商品，下架有什麼不可以？

(十三)我們現在已經把(詐騙)刑度拉高，但這刑罰有嚇

阻力嗎?為什麼現在詐騙集團不怕?因為你抓不到我啊!

(十四)委員講那個鼓勵檢舉，我覺得很重要。

(十五)一頁式詐騙的被檢舉應該立刻先把他下架嘛!你下架之後接受申訴,如果確認是合法,再回復起來。真的很需要行政機關跟立法機關配合來做快速反應，要不然我們真的跟不上他們。

(十六)韓國在很早之前提款的部分就有做，大概10年左右,他們只要去卡片提款超過三次,ATM的鐵門就關下來，車手就不敢過去韓國提款。韓國對詐騙也是從重懲罰，所以犯罪者也不太敢過去。中國一樣也是從重懲罰，是依照詐騙的金額來增加刑度。

(十七)新加坡他們會攔住簡訊，是詐騙訊息的簡訊他們就會把他攔掉。像這種作法，臺灣不知道能不能做到。

(十八)個資方面，我不知道委員有沒有聽過小白機，去年我們查緝過，你們的所有個資其實都在那個小白機上面,房仲業他們每個人手上都有一台,連總統、院長的資料都在裡面，什麼資料、身分證字號、手機號碼、住家地址全部都在裡面。我們那時候進行北臺灣的大搜索，就扣了上百臺。他們房仲業私下都在賣這些東西，你們看民眾個資都流散到到什麼程度了!

(十九)防詐我們我們也不用打高空，應該主要密集處理兩件事，一個是人頭帳戶要先降下來；第二是個資的防範要去處理。核心觀念就是，你要在臺灣做生意，你就要遵守我們國家的法律。

(二十)再來第二個關於抓車手的科技偵查能量和偵查技術要怎麼提升，真的要請委員多多關心科技偵查

法，有科偵法就不用派臥底，手機就可以植入木馬做臥底。沒有科偵法，我們不僅不能滲透詐騙集團，反而被詐騙集團滲透。

(二十一)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。

(二十二)虛擬貨幣很重要，目前沒有人管，而且第三方支付竟然分2億以下的由數發部管，2億以上由金管會這種方式在管。各位一定要瞭解地下匯兌對國家影響多大，因為地下匯兌洗錢的問題，會直接作為總統大選介選的資金。我們一旦放手會動搖到民主和選舉制度。

(二十三)據我所知美國的某些州已經要求虛擬貨幣業者必須要經過登記，之後去列冊管理，才可以做貨幣買賣。

三、警政署 曾○芬專員

(一)受害者覺得他錢追不回來，有些人就根本不想報案，其實目前的狀況就是這樣。

(二)檢察官跟警察在後面苦苦的追趕，因為犯罪手法是不斷翻新的，犯罪手法會結合最新的科技，然後不斷的演變，這就是為何目前為止在斷源的部分，其實還是很難達到

(三)從前面金流部分，如果銀行端發現這個帳戶有問題就凍結，把錢卡住的話，他們領不到錢，就斷了他們的生路。

(四)金管會是不是可以課責銀行，問題帳戶不要讓他們申請，或是罰錢之類的。

(五)從電信流跟金融業這邊去追源頭，是比較實際的，比檢警從後面追直接多了，後面檢警真的花太多心

力，快被壓垮了。

四、金流面 學者專家

(一)打詐綱領1.5版重點都放在後端，但是反詐是跟COVID-19一樣，它絕對不是大家全部去臺大加護病房，而是全面都要戴口罩。如果打詐綱領都在說要增加刑罰等等，檢察官、法官那個工作量真的壓垮。都是加班加到滿，去幫被告和犯罪集團寫一大堆附表。所以一定要整個往前推，所以這個是我認為現在的整個政策一直放在後端會產生的問題。

(二)前端要想的，就是詐騙集團他其實要錢，那錢在誰的手上?銀行嘛!

(三)以往人流物流都管得非常好，但是整個時代因為科技的變化，現在真正的重點在金流跟資訊流，那就是金融機構跟電信業，所以人流跟物流現在其實我們都規管的沒有問題，哪裡都要身分證啊。

(四)但是金流跟資訊流其實是沒有規管的;就金流來講，金流的部分有二個點，一個是金融機構不覺得防詐是它的事，它的想法是我是幫忙嘛。那為什麼他這樣想，他的想法就是說這都是檢警調的事，那講來講去，他高層其實不關心，所以各位委員，如果你們去看我們現在所有金融機構的董事會都沒有討論這(反詐騙)問題，ESG，其實這(反詐騙)就是最好的ESG的社會責任，但是從來沒有任何董事會討論反詐騙，社會責任都在討論放產假、有沒有給最低工資等等，其實如果要求ESG納入反詐騙去計分，那個對金融機構來講，那個壓力就很大，它的股價受影響。

(五)高層主要重視業績和獲利，這都反映在股價上，所以之前證交所有一個承辦人在講說，他們現在要做

模型，換算金融機構的ESG給外資做投資的考量，看要如何使防詐變成模型的一部分；我覺得這是一個比較好發展的方向，就是說你一定要讓金融機構知道這就是他的責任。

(六)第二個是金流會經過的不是只有金融機構，他現在全部都轉移到外面去了，也就是第三方支付跟虛擬貨幣平臺，這二個我們政府都聽起來是有主管機關，但是如果你去問他，他是從來沒有檢查；也就是說你去問他虛擬貨幣是金管會管理，有沒有金檢過?從來沒有。第三方支付是經濟部管，我們的法條也規定他要檢查，但是他從來沒有檢查。洗防辦公室報告說2021年詐騙就700億，但今(2023)年光上半年就1400億，那一定是透過金融機構大家一起幫忙洗，要洗這麼大量的錢，這三個點(銀行、虛擬貨幣、第三方支付)就沒有看到防範措施嘛。

(七)最後一個要講的就是，臺灣因為是以經濟立國，所以我們很重視公司的發展，我們現在有86萬的公司，但有四分之一都是假公司，所以我自己的預測，從明年開始所有的人頭帳戶，會轉到法人戶。因為現在金融機構全都在防個人戶。

(八)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，可是法律有規定他要查核，那所以我我講的這幾個，都是我們國家法規其實都有點到，但就是都沒有落實。

(九)其實主管機關是重視的，只是藥下不夠重，在洗錢防制上面，早先的時候金融機構是非常非常排斥的，洗錢防制給金融機構帶來了很多的不方便，同

時影響到他們的業績；那國外的經驗呢，那當然在洗錢的方式上面，如果金融機構不配合的話，當然就是從金融機構的商譽著手，讓他受到傷害，那麼金融機構自然會得到這樣子的教訓，像最近上海商業銀行洩漏大筆的個資，會處罰1,500萬，那我相信這個就是一個很好的一個例子。

(十)你要金融機構配合，就是棍子跟蘿蔔，金融機構他一定要賺錢，所以要用賺錢去引導他，譬如說限制他業務，那像現在總經理減薪，副總經理減薪，這個都是最近主管機關有宣示，金融機構會怕。主管機關罰他200萬他不怕，他1年賺4、5百億，他怎麼會怕200萬，但是你影響他業務、賺錢或拓展新業務，你公司治理評鑑打下去，高管要負責任，對金融機構來說就很可怕。

(十一)現在那個金融機構都是在公佈說阻詐的成績很好，還頒獎給它，其實這個都是基層行員在阻攔被害人；但國內有個名單從來沒公布過，就是金融機構內部警示帳戶的數量，也就是詐騙集團最喜歡收購哪些機構的帳戶，詐騙集團之所以喜歡收購某些機構，就是因為這些帳戶好用，機構都不控管，錢進進出出都沒在攔的，這個名單立委早就請大家提，但是從來沒有提，因為一提就影響商譽；然後再來提了，主管機關要不要罰?

(十二)雖然詐騙集團金流現在一直往外，但第三方支付和地下匯兌最終還是要回到銀行來運作，原因是走地下匯兌錢會被吃掉而且出金費用很高，但是在銀行的話，錢不會被吃掉，手續費又低，兩相比較下，詐騙金流最終其實是會回來金融機構。

(十三)還有一個東西是調查局洗錢防制處，現在全部臺

灣39家機構去掉外商，就是34家的合夥銀行，它所有每天看到異常的金流，都會通報到調查局洗錢防制處，但是委員你們可以瞭解一下，調查局洗錢防制處有沒有送詐騙案出來?就我所知是沒有。為什麼沒有，就是因為案子太多了，到最後乾脆不通報，錢就在人頭帳戶流來流去。

(十四)金融機構也要增加科技的運用，現在行員就兩隻眼睛，每一次主管機關增加一種洗錢防制或者防詐態樣，內部的報表就增加十項，機構3點30分關門以後，你知道他要看的報表有多少嗎? 我們一個行員沒有科技的時候，關起門要看400多件，他3點半到晚上10點半之間怎麼可能看400多件?他會看得出來嗎?可是我們一運用科技以後，他關起門只要看兩件，差別非常大。這就是為什麼我們運用科技以後警示帳戶會一直降，每年都降20%，所以我們就是要鼓勵他用科技，否則行員只是照章辦事嘛，你主管機關一直叫我阻詐，我就叫行員做，行員做得很累，就給他頒獎，這樣子做一直循環，其實就不會有效果。

(十五)金管會是要針對這個業者來做約談，我第一次先給警告，第二次如果銀行還是不理，那就開始部分停業或業務限制。

(十六)既然被害人要錢，加害人也要錢，所以我們去想這個制度的時候，應該都想錢在誰身上?很簡單就在處理金流的人身上，也就是金融機構。但是現在洗錢防制雖然都有金檢相關規定，但都沒有在執行，也沒有哪一家業務受到限制。但是美國2023年7月26日，眾議院已經通過《21世紀金融創新和技術法案》與《區塊鏈監管確定性法案》。

五、Gogolook 劉彥伯總監

(一)年輕族群和年老族群事實上都是詐騙者主要的鎖定範圍，那以年輕的族群來說主要是購物詐騙啊，投資詐騙這種，老年人則是電話和面對面的詐騙。

(二)剛才有提到金流，因為其實詐騙有分兩塊，一塊是他透過原來的臺灣本地的金融把這些錢洗出去；另外一種是透過線上或信用卡的方式來做持續的詐騙，所以金流方面，我們過去可能會要求銀行做一些SOP來控管，但事實上，詐騙還是可以透過交易貨幣或其他方式把錢轉出去，這我們在東南亞市場都看過。

(三)我們各部會事實上都負責一個特別的domain，然後這個domain又跟其他的部會合作，舉例說，數發部把這個網購申請出來，跟通傳會、社群平臺跟廣告，又是另外一些部會；他們這幾個部會事實上並不會互相交流，而是想各自做自己的防詐系統，現在狀況是這樣，我就是常常去開會的時候看到的狀況。

(四)然後再來一件事情是目前宣導，老實講比較偏向電信的宣導，但事實上不管是臺灣還是東南亞歐美，詐騙已經大量的轉移到網路上，剛剛孟老師提到年輕人好像被詐騙比較多，原因就在這裡。

(五)各部會在討論網路詐騙經常會找資安專家，我覺得這是有一點歪樓的，詐騙集團用更多的是像社交工程，更多的時事或日期相關的，比如說現在要聖誕節了，就開始做聖誕節的詐騙，他會去做調整；但資訊安全專家事實上不會在意這個。

(六)社群平臺目前的一些困境，以目前臺灣、泰國跟日本碰到一樣的狀況，比如說在臺灣的詐騙集團最喜歡的方式，就把人先洗到LINE上面去。因為像是

LINE在各國都會說我是境外投資，並沒有直接跟你的行政層合作。

(七)在內容審核部份，我們雖然可以要求Facebook要做廣告審核，但詐騙集團跑第三國去做廣告，第三國審核人員對臺灣的名人根本一無所知，所以基本上他看文字、格式都對就放行了。

(八)馬來西亞、澳大利亞和泰國警方去年開始跟臺灣的whoscall合作，把whoscall的安裝率往上提升之後，整個泰國的電信詐騙就往下降。

(九)我在網路上看到一個量子醫學方面的廣告，很明顯是詐騙，我就通報警方說這看起來就是詐騙。可是警方碰到一個問題，警方沒辦法在一個沒有明確被害人的情況下，就判斷說這個是有問題的，也沒有足夠的專業去判斷這種醫學方面的狀況。所以警方就建議去跟食藥署檢舉，但食藥署又說有人去警方這邊做一個檢舉嗎?我又跑去跟通傳會通報說這看起來是臉書型的詐騙，但通傳會說這是藥品相關的，所以這變成我找不到一個檢舉的單位。

六、臺北地檢署林達檢察官

(一)我直接切入，問題在虛擬貨幣，目前我們可以看到這個金管會有做了很積極的解決，去年的九月二十六日有發布【虛擬資產平臺及交易業務事業基礎原則】VASP，裡面第九點提到了個人幣商的問題，那其實我們檢察官發現在實務問題上最大問題就是所謂個人幣商，因為我們抓到了許多的人，被害人都是匯到他的帳戶，結果他到地檢署就說，他是個人幣商，所以他不知道匯款的是詐欺被害人，因此我們拿個人幣商沒有任何辦法，所以最後就是大量的不起訴，當初檢察官呼籲以後，金管會也受到了

壓力，所以他現在用VASP把個人幣商納入。

(二)但如果仔細看這個個人幣商的部分，它裡面的作法是說自然人從虛擬資產業務要向金管會申請法遵聲明，他的聲明裡也要跟法人組織相同。簡單說，金管會新的作業指導原則就是把個人幣商視同為法人，看起來它就對外宣稱，說他把所有的個人幣商都納管了，但我必須說這個在實務上沒有太直接的幫助。怎麼說，其實很簡單，在金管會的正常作業準則下，法人幣商其實要去做聲明，規範其實是相當嚴格，包含他的資安、責任準備金等等，以個人幣商要達到這樣的聲明，其實都做不到，所以也就會變成說，基本上除非說你是有公司組織，有請技術人員才能做到。但金管會只是簡單地把個人幣商等同法人，但法條是沒有幣商的明確定義的，實務上幣商概念有兩種， 一種是平臺業者，它設一個平臺讓人家來存放虛擬貨幣或者進行貨幣的轉移，這個我們會理解為一個保存或者是仲介或者是經濟服務的；但是第二種，我們現在實務上大量案件的幣商不是平臺這個觀念，他們只是個人投資客，他自己買很多賣很多，買買進進出出這樣每年量很大。我們修法方向會說這些人都是幣商啊，所以你應該去法遵聲明，但這都是平臺概念，因此個人幣商在地檢署就會說我又不是要經營平臺業者，我只是投資客，我幹嘛要去聲明呢? 所以就金管會立法說幣商沒有聲明應該要判罪，最後檢察官應該沒辦法起訴，就算起訴好了，我相信法院可能也不會判有罪。

(三)我個人有幾個建議的結論，第一個就是說我們在虛擬貨幣資恐打擊、資恐辦法裡面，是不是應該把對

象的定義更清楚地劃分出來，把平臺業者和投資客兩種能夠劃分出來。那我們對投資客的部分要怎麼管理?那我們建議在一定的量以下，他其實可能真的就是一個單純的玩家就是甚至是被騙的被害人，他一年可能進出次數不多，但有的人他常態每天進出，這種應該是一個資深重要的玩家，甚至以這個差價為獲利的，那在一定次數以上的就應該要給予某一種聲明或管制，換句話說要到金管會去做聲明的人，恐怕有兩種幣商，一種是比較高階品牌業者，他的門檻很高就像法人；另一種比較低階的，聲明就簡單一點，讓大家都做得到。這樣規定之後，你就不能夠免除說你只是個人在買賣，你還是必須要比照營運的事業在繳稅。那我認為說，虛擬貨幣上面有沒有可能畫出一個界線。如果說你虛擬貨幣會變成所謂個人利得，是以這個為主業，那就去繳稅啊；這種應該要在國稅局要有一個稅籍，你去做一個聲明，然後繳一定的稅。不可能說那邊不繳稅，另一邊也不做聲明，然後來地檢署的時候說你是幣商要免刑事責任，等到要起訴的時候，又說你不是平臺性質的幣商所以無罪。簡單說，我們覺得虛擬貨幣交易每年只要超過一定數量次數或金額的人，那你就去聲明，去工商登記一戶，然後要有一定的教育訓練。那跟人家買賣的時候，一定要有對方的本人身分證字號等等，你都要做到。如果能夠把這樣的層級化做出來，我認為對虛擬貨幣的整個觀念會比較好，不要都直接用幣商這樣一個非常混淆的概念。

(四)再來是第三方支付，我自己個人辦過很多案就非常的痛苦，因為以前最多的碰到匯款帳戶是虛擬帳

號，譬如說玉山銀行，我們問說這個帳號是誰的？結果他就要函復我們說是虛擬帳號，這個虛擬帳號是由某某第三方支付公司發出的，我們就要發函去給那個第三方支付公司函調說這個帳號是你們發出，那請問你們是幫誰代收代付啊？然後八成的案件發過去都不會回函。我怎麼辦？我案子那麼多，只好就結案了。假設我積極一點去查那家公司負責人，然後就把他傳喚來，他要嘛就不來，就算來了，我請他告訴我幾月幾號這一筆65萬，為什麼會是你在代收代付，他說檢察官我回去查一下，他回去以後呢就翻箱倒櫃，其實他們就是詐騙集團的，他就隨便拿出很多張的契約書，然後說這個是林達委託的，簽名的人是林達，那我就傳林達來，林達一來說我沒有簽過名啊，曾經遺失過，結果還是不起訴處分，後來就不查了，因為沒有意義啊。

(五)除非我們直接把整個第三方支付這家公司認定是犯罪，可是我們沒有足夠的證據，因為他們都會說我們大量的代收代付，70%都是正確的，檢察官不能說我今天差一兩筆，就認定主觀上有犯意。他的問題就在於說第三方支付的管理上面沒有設許可制，它不需要責任準備金、不需要資訊安全、不需要會計師簽證，他什麼都不需要，他連會計人員都沒有，他是一群刺龍刺鳳的人自己就設立。我們橋頭地檢署先前去查的時候衝進去，發現就是一個民宅裡面都有一大堆文件。

(六)第三方支付部分去年我們在質疑數發部，我記得是20億元以下，跟20億元以上分兩個單位在管啦，20億元下是經濟部，20億元以上是屬於數發部吧，總之我們覺得當初這個業務就被他們推來推去，我們

瞭解公務人員，我們也不去追責他，我們當初提出具體的解決方案是說，第三方支付涉及到金融業務，要採許可制，許可制裡面一定要有兩大塊，一個就是資訊安全人員，第二個就是財務會計人員；而且許可制只是在最初的許可，後續應該要由會計師去簽證查核。我認為這部分目前稍微解決，為什麼？雖然我們目前政府還沒有給他採取許可制，但是有所謂能量登錄，現在就會鼓勵你們有能量登錄，然後銀行才會給你虛擬帳號。

(七)我覺得具體的建議，首先第一個就是所有交易所熱錢包應該要公開，他應該是一個可以被監管的內容，就是熱錢包的意思就是歸戶錢包，我舉例來說好了，比如說幣安、火幣大家比較熟知的幾個交易所，其實交易所就會是洗錢的斷點，合規的交易所的話，基本上檢警都調得到KYC資料，所以我們至少會知道說某一筆資料中間經過很多次的層轉，層轉之後，假設要從幣安的某一個用戶的錢包出金，那我就會找幣安去調那個用戶的充值錢包地址KYC是誰?我就會知道資金後面要跑去哪裡。這個作法有個前提就是熱錢包應該要被公開，那我們在做金額追蹤的時候才好去判別說現在看到這個錢包是私人的非託管錢包，還是屬於交易所的熱錢包?那以現在臺灣水房來說，他們最常用的其實是一家在柬埔寨的交易所叫○○，但是我們管不到○○。

(八)教育方面我不知道有沒有可能建議教育單位方面加強區塊鏈的教育，到現在很多公民教育的課程我真的覺得沒有什麼意義，我們發現大量的詐騙投資虛擬貨幣，被害人根本不知道什麼是錢包，他們以為那串數字出現了就算擁有它，其實他們根本就把錢

包的帳戶密碼都交給了詐騙集團，是他們(詐騙集團)幫他(受害者)開的戶，所以他(受害者)買了以後，人家是直接匯到別人那裡。換句話說，買虛擬貨幣的人連最基本的觀念都不知道，那他還去買，我們根本連幫他的機會都沒有。

(九)他們現在詐騙也不完全都那麼高科技，他們是用LINE，很傳統的跟你說在臺北哪一家7-11面交，我們實務上抓的案例，上禮拜值班那天晚上就抓到兩個，一個從高雄來，一個從屏東來，一個19歲，一個20歲。他們是坐夜車到臺北，然後他們到臺北以後，他們就到7-11的ibon列印一個虛擬貨幣契約書，然後去向那個被害人說投資要收錢。那種詐騙金額都在200到1,000萬之間，都是巨量的，受害人會帶200、300萬來現場，然後我們這個年輕人就會拿這個紙本契約書給他簽名，簽了以後收到現金就會告訴他，我把虛擬貨幣交給你，那不是很愚蠢嗎？虛擬貨幣再怎麼不懂也知道不會是紙本吧!然後他們叫被害人回到網頁上去看，就會看到說有200萬進來了，你這次獲利有20萬。假設知道正確的知識的話，他應該就會在臺灣那9家交易所交易，可是就因為大家都沒有這種觀念嘛，他就會亂買啊，然後就查不到，最後就完全都沒有辦法。抓到的都是這個19歲，我們向法院聲押幾乎都不准、都被駁回。說真的我們就算把他押起來，後面我們也查不到啦。我就問這個19歲、20歲的這個年輕人，他們是從高雄調人上來，臺北會調人下去，我問他什麼時候開始做這個？他們幾乎都說第一天，他就會說他昨天應徵工作，我說你怎麼應徵的？他說他在泡沫紅茶店門口，然後呢用LINE找工作找到的，然後

我說你們一定坐高鐵，他就說應徵的時候就給我2萬塊錢，工作就是跑外務，我認為我做的是合法的收錢工作，都是虛擬貨幣這個企業，我不知道後面是誰啊，他就那一天跟我有LINE，他們就會指示他拿到特定地點放在地上、拿到哪裡、交給誰，那後面我們就都查不到了啦。

七、社團法人全球反詐騙組織台灣分會理事長

(一)詐騙集團有綿密的分工,但具體怎麼分工?組織架構是什麼？我先從這邊開始說大家會比較好再進入後續的討論。今年我們人頭帳戶又創新高，我記得之前的統計是9.6萬，現在已經破10萬了。

(二)柬埔寨的○○，不知道大家有沒有聽過，○○特區就是之前人口販運很嚴重的地方，○○那邊有很大型的園區，是由房地產商去開發的，那個房地產也是早期臺灣的一個大賭場去那邊做的，後來轉型做東南亞房產，在那邊開發了○○這個園區之後呢，蓋了很多大樓，接下來轉包給物業，物業就把它理解成房東，那就是保全公司，保全公司會打點好軍隊、水電、網路這些東西，之後承租出去，大概三年前是由博弈業承租比較多，但是因為疫情的關係和中國逼著停牌的關係，就轉為做電詐，那其實電詐跟博弈本來就是一線之隔。金流技術跟後面的洗錢通路都很好跨越，他們被稱為灰產(灰色產業)啦，但一旦踏到詐欺，就變成是黑產(黑色產業)。

(三)機房通常是由誰去開設的呢？大多是跟臺灣幫會有關聯，比如說像○○會、○○幫，他們通常在組織裡發展27至29歲間的，鼓勵他們去境外開代理線，這個人會再帶十幾個更小的去那邊起頭，在機房裡工作。還有更大型的機房像連鎖企業，還會有另外

的角色去督導不同機房的運作。緬甸的話就會落在緬北跟緬東，緬東的話就泰緬邊境那一帶，就是○○○、○○○，大家應該有聽過○○○的話，就是KK園區的所在地。然後○○○的話，就是落在水溝谷，○○○就是世界上最大的園區，規模大約三萬人。

(四)組織架構圖他們有一定的分工，首先是財務、客服，當一個金流進來，他們金流有走虛擬貨幣和法幣，假設做臺灣盤的話，一定要有人去收那個錢，那錢怎麼收?就要同時搭配本地的水房跟車手，就是跟車隊搭，如果他們走匯款的話，那就是跟水商、水房搭，水房就要去收人頭戶，所以水商又會再跟收簿集團搭配。人事部分是負責招募境外機房的基層工作人員，可以把它想像成HR(人事)的角色，那之前人口販運會變得很嚴重，就是因為境外機房那時候大缺工，所以詐騙集團開始用騙招的方式來招人，以前的話找人都用正招，通常都找一樣是找幫會，或是比較有幫會脈絡的人，說要不要去那邊作假之類的。但後來因為中國打擊，造成大缺工，那時候就開始大量騙大馬華人跟臺灣人，所以才造成臺灣人口販運的問題。總之，本來是做正招，後來轉成騙招，騙招就跟你講說是去做博弈不會限制你自由，後來發現這個可以，他們就再編更大的謊言，比如你去那邊是賣佛牌或去當翻譯，然後就騙了一大堆人去。

(五)講到所謂狗推[106]，就是看公司做什麼盤口，如果是做臺灣盤，要對到的答案就是臺灣人，如果做的是

[106] 指詐騙集團中負責透過網路或電話以話術與被害人聯繫之單位。

日本盤就對日本人，就看他們是選擇什麼樣的市場。以境外來說，大概五六成都已經轉做歐美盤了，大概三成是做亞洲盤，然後兩成都是本地盤(中國盤)。

(六)除了這個機房本身之外，那他們還有另外的資訊服務，就是架設詐欺網站，是由另外的系統去處理的，並不是由機房自己去維護。以詐欺網站來說，他們更新非常快速，通常是用一個模板下去架設，所以很多詐欺網站是很雷同的，然後網域也都會事先註冊起來，比如說他們可能一次就註冊大概十幾個銷售網頁，但不會十幾個同時用，他們通常先用一個網頁二到三個月，有被通報的時候，他們會跟被害人說系統要升級了要換新的網域，所以他們都會先鋪墊好，到被BAN掉，他們就會無縫地接到第二個網域，如果再被BAN掉，再換第三個，即便他們手上的網域都BAN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。

(七)2022年的9月有一批大掃蕩，不過現在基本上都已經都回去柬埔寨了。中國國安打擊的狀況大概是2022年9月大掃蕩○○，後來半年的期間都是壓在柬埔寨○○那邊，有一段時間是機房是沒辦法運作的，就大量就挪移到緬甸。移到緬甸之後就變成了緬甸人口販運很嚴重，所以像以近期來說，大家如果追蹤新聞的話，應該就會看到中國國安大概近三個月都是在打擊○○那邊。所以○○這波清出了大概上萬人，上萬都是中國人。

(八)詐騙產業鏈的人口級別是百萬人口以上，前面講到做臺灣盤，要收錢的話，客服或是財務單位會對應到臺灣的水房車手；如果是人事的話，會跟臺灣的

人事跟中游做對接，狗頭的話會跟臺灣做對接。這種對接方式通常是讓臺灣人去處理，招募的話很多就是在偏門的地方社團PO文，PO文是以黑話的方式，只讓行內人看得懂，看不懂的人的話可能就會以為是去當臨時工，行內人看就知道是在收車手收簿。他們PO文就是在各個工作社群PO，然後要你加LINE，叫你把簿子提供出去。

(九)早期很多都是找街友直接當面收簿，後來開始因為人頭戶大量被查封之後，就處於一個不太夠用的情況，所以他們才會開始收簿，那收簿其中一個話術就是找工作，家庭代工，這也是兩個常見的話術劇本。那現在收簿的話，如果是對行內的人收的話，大概價碼，現在大概快要到30萬左右。早年他們是軟控車，控車的意思是說，我這個簿收去給水房用了之後，那水房當然就很擔心這個簿被凍結，因為卡金流對水房來說是唯一的風險，他們會很強烈地去避免帳戶在金流還在跑的時候卡錢在裡面。所以要如何去避免這件事情？就是要搭配控車，搭控車的意思就是這個人頭戶的提供者，他必須要配合做監控，然後早期他們是讓人頭住在民宿裡面，然後這段時間不能用網路，不能用電話，不能有任何聯絡，直到他的簿被凍起來，通常時間就是5到7天左右，5到7天就是他們使用這個戶頭的時間。本來是軟控，軟控的前提是這個這個人通常是內部人、是自願就會搭軟控；現在就是發展成強控，強控的意思就是被騙來的劇本是面試，一進門就把你打暈了。收簿團和控車以家庭代工為話術，說要收簿是很合理，因為要給你薪水，所以拿你的簿，這個劇本才會是合理的。這種人物設定下，那中年婦女是

他們很常去針對的一個群體，在某一套劇本裡面。家庭代工話術很多是以中年婦女為核心，然後還有另外一個的，他們殺豬盤也會是以中年女性為族群，那原因也很簡單，就是如果他想要騙錢的話，這群人是有儲蓄習慣的人，如果我的劇本是假交友，假投資的話，那這群人通常也是生活比較單純，而且可能在婚內是缺乏陪伴的，有感情上面的需求，所以對這群人要騙感情或是騙錢都是相對比較好處理，所以說官方統計跟我這邊統計可能會不一樣，我覺得是通報率太低，所以才產生了這個落差。就我自己統計大概七成的對象是女性，然後裡面大概有四成左右都被騙。他們很愛下這種廣告，就是什麼如何兼顧工作跟育兒和家庭，又照顧小孩，又同時有收入，他們有一陣子很常下這個廣告類型。

(十)資訊服務部分，他們系統商會直接支援，今天只有二十幾歲的人去那邊開機房怎麼會有相應的資源?通常都是由系統商去所謂那邊的扶持，系統商會貼文說要招代理員，他們除了系統的支援之外，還有各種好比說賣微信的、賣Facebook的、賣Instagram的，然後還有跟周邊的素材套件，就是你要執行詐欺的話首先要包裝假的人設，我要去有這些養(帳)號，養號有另外的公司或團隊處理，常用是拿小網紅的生活素材、旅遊照片打包，讓狗推第一線執行詐欺的人有素材可以跟客戶去對話，他們的素材周邊智慧系統比大家想像中齊全，受害人並不是一對一地在跟一個騙子聊天，很多人對此都誤以為說是一個狗推對一個受害者，他們的工作模式一開始是引流，好比說我在591針對房東做狙擊的，先假裝是租客然後假裝要租房，其實他只是創造接觸的話

題，說因為要工作出差，所以沒辦法去看房子，然後講到臺灣房價很貴，你是怎麼做到這個，可以讓這個房東有所好奇，轉而變成是交友，他可能會說他其實是做虛擬貨幣投資的人，今天臨時出差也是跟交易所有關，你對這個就虛擬貨幣投資有興趣嗎，慢慢地把話題引導到投資這件事情。後面的狗推通常大概是4到5個，他們會一個小team、一個小team，每個小team會有一個小組長，以一個狗頭來說，因為狗頭他們手上會有大概4到5支工作機，工作機同時會跟他十幾個被害人聊天，會在裡面去討論如何跟被害人發展關係，由小team去討論出來。比如說他們覺得關係有點卡住了，要怎麼去突破?他們其實是每一天晚上都開會討論，他們會去做客戶管理。

(十一)有關虛擬貨幣在產業鏈扮演的角色，有一部分金流是走反方向，用匯款或是面交現金的這種作法，但到後面七成案件都是以虛擬貨幣方式出去。也有一開始就是直接走虛擬貨幣的，其中特別是裡面的USDT穩定幣，這一類的不法所得其實是會被在區塊鏈安全標註為黑U，這些黑U要如何去洗白?就會是一個對於洗錢方很重要事情，通常會用社群媒體去找可以做兌換的，然後慢慢把黑U消化掉，用各種平臺去做洗錢，中國那時候還弄一個斷卡行動，當時候凍結了14億的帳戶，包含留學生要去開帳戶都會變得非常困難，洗錢很難把錢匯出來，因為這個緣故，很多機房就放棄了中國盤轉做臺灣盤，現在就轉做歐美盤，對象還是在歐美的華人。

(十二)以詐欺來說，他們真正想要的東西是財產，所以目標就應該要放在金流，去降低整個詐欺產業鏈的

獲利，所以核心要處理就要變成是洗錢了，回到虛擬貨幣增強反洗錢的這個能力，應該是現行所以唯一可以去處理的課題。

八、台灣事實查核中心邱家宜執行長

(一)我其實有在跟同事討論。我們查核中心要把詐騙highlight，我們要調整版面，把詐騙的專門就放在最上面的右上角左上角。反正我們要把詐騙放在最上面的地方，讓大家越容易看到，因為詐騙真的是民眾最有感的。

(二)然後我們最近發現一個狀況就是二次詐騙，就是有一個假訊息說我們是律師團隊。如果被騙請跟我們聯絡，可以把錢要回來。然後那個是詐騙，他用的是一個新加坡的law firm的照片，你點進去之後，他就是叫你付錢給他，然後他會幫你要錢。那個律師事務所被人家盜用照片。然後他去跟平臺講說，這個是盜用的趕快把它封鎖下架。事務所說平臺都不理他，意思就是說，本尊已經出來說有人冒用名義去做廣告詐騙。可是平臺不理他，我記得應該是META吧。

(三)監察委員的守備範圍，雖然沒有辦法去要求立法院，可是我們可以去要求行政機構，立法院要通過這個法案，可是行政院可以努力的去做一些設計，也許當然就像羅老師講的源頭管理，我們查核中心也是很下游。我們每天已經是一大堆垃圾，我們只是清垃圾，而我們能夠清的垃圾，只是讓家門口垃圾稍微掃開殘雪，我們可以走出一條路，還可以勉強走出門而已，其實還是有成堆的那種假訊息完全清理不完，我們也查核不完，我們查核中心也只能針對廣泛的詐騙議題，比如水費詐騙，可是如果是針對

你個人寄到你的 email 、LINE什麼的那種客製化的詐騙，我們比較沒有辦法處理，這種客製化我們沒有辦法去查核，因為我們不知道每個人的臉書的網頁上會出現什麼樣的詐騙的內容？而這個完全是依附在他的演算法上的，所以我們如果沒有去做源頭管理，就是說告訴這個平臺說這些東西是有責任的。我們現在的工作就是要怎麼樣讓人民相信說去管理平臺對大家是好的，平臺他賺了很多錢，那他是不是也應該要負起一點社會責任?我們各行各業都有我們自己的社會責任。律師有責任，會計師有責任，對不對，我們都有我們的倫理，那你們平臺業者應該有你們的倫理啊。

(四)我們去英國Ofcom交流,就是有點像通傳會但更獨立一些,Ofcom新成立了一個數位部門,他們現在聘了三百人在專門在做網路，主要是跟這些業者不斷地去磋商。我個人的期待就是源頭管理，打蛇打七寸才是比較有效率的，而且是從上游去做一些法律框架，我們不是說去做內容的管理，而是做一個法律框架，然後怎麼從結構面去做一個規範，就是說平臺也有他的責任，平臺也需要遵守某一種規範。

(五)另外一個就是監察院也可以去關注教育部到底在媒體素養這個事情上做了多少事？他當然已經成立了媒體素養推動會，但是我們也知道政府機關有時候有一個會之後，常常就是會而不會，就是說有一個會，可是他也不一定會開會，那他開會也不一定會有產生什麼具體的結果？當然我們其實NGO其實有在做，Google也有給我們funding做media literacy，可是系統性的結構性的，我覺得整個學校體系,教育部如果能夠多做一點,例如公私協力，

那會更有幫助。

(六)我總結一下，我們要怎麼去設計一個平台治理的法律框架，進而重啟平台治理的社會溝通，那當然也就寄望通傳會吧，就新任的委員或者是數發部，未來的就是兩部會怎麼樣去協調，行政院可能要站在這個就是敦促的高度，那教育部就是要去負責使用者端。

九、國立中正大學犯罪防治學系許華孚教授

(一)近年暴力犯罪一直下降，但是詐欺犯罪成長了好幾倍，那我們也要學英國、日本怎麼去打詐，那我剛才說詐欺是全球化的現象，所以現在很多國家都立這種法律來打詐。

(二)我們可以看到一個數據，我們大概詐欺有起訴的有五萬多人，但是真正被判定入監服刑只有1萬6,000多，表示說只有3成判定有罪，其他陸陸續續交保的7成的人，交保出去還是持續在騙，像在美國有毒品法庭、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。

(三)其實打詐綱領1.5版裡面雖然有把五個專法放進來，包括洗錢防制法、刑法，人口販運防制法、個人資料保護法，還有證券投資信託相關法律，但我要講的是限制，第一個，檢警的犯罪偵查手段是有限的，包括電信流反向追蹤偵查還有相關機關查緝的配合度很低，還有通信軟體監聽還有國際司法互助，此外證據搜查不易，尤其現在很多機房都是在國外，證據取得很困難。

(四)第二個是金融管理的不完備，虛擬貨幣電子錢包現在都非常的流行，還有人頭帳戶、金流查緝配合度、

金融機構的問責等有待加強。

(五)第三個是刑事司法嚇阻力低，會考慮成立那個詐欺專法原因就是我們刑事司法過程非常冗長，然後犯罪的利益大於這個罰則，所以很多人交保後，又再加入犯罪集團持續犯罪。

(六)第四個是識詐的資訊效能不彰。刑事局跟警察局很多單位都拍那種反詐影片，可是普及性到底高不高?有沒有分年齡層?這個我沒有看到。

(七)我們看到幾乎抓到8~9成都是車手跟水房,就是專門做洗錢的，因此破案率看起來雖然很高，可是我必須要點出來一個盲點，就是說其實抓到的都是比較下層的這些人。集團的首腦和金主其實都還蠻有社會地位的。我們在2023年大概阻詐89億，但是如果我們以犯罪學的黑數的話，大概要乘以10倍，也就是大概有700~800億，現在的詐騙都是流行小額的，雖然鉅額幾千萬也有，但是大部分的都是2、3萬這種，這種你不會去報案。

(八)其實我們數位媒體有很多的困境沒辦法突破，我們科技偵查工具的使用是沒有法源基礎，也就是說我們沒有正當程序(due process),所以會失去它的證據力，你剛剛講M化車，那我們必須在科技偵查法來完備這個部分，第二個就是人頭戶難以杜絕，那現在不是只有遊民，還有外配和外籍勞工。我們現在有75萬的外配，外籍勞工還有外配一個人都可以開好幾個戶頭，這些都是未來潛在的人頭戶，沒辦法杜絕。

十、國立中正大學傳播學系羅世宏教授

(一)我會關注這個議題，是因為這在臺灣是很嚴重、民眾很重視，然後也影響政府威信、影響社會安定的

一個很重大的課題，而且似乎是沒有辦法很短期可以見效的去處理這個複雜的議題。

(二)它是一個跨境的、全球化的，而且它廣泛的運用了非常普及的數位科技，又加上智慧型犯罪，而且犯罪集團運用了很精緻的一些心理學的操縱技術，另外我想臺灣人社會上相互信任度是高的，而且很善良，因此受詐騙的機率是高的，雖然這樣講可能有點簡化，但我覺得臺灣人是容易受騙的。

(三)我們現在要更系統性，更制度化的來看，也就是說要怎麼樣去預防，預防會比事後圍堵或是止損有用。當然發生之後還是要止損，讓民眾有管道可以尋求協助。比方說像165，當然我這樣講可能不太正確，但在很多常民的經驗當中，165沒有什麼用，也許對某些人的案例他是有發揮作用。不過就我的有限接觸當中，有人被詐了之後甚至沒有興趣打165這個電話。

(四)我覺得平臺是一個關鍵，從預防角度，平臺成為詐騙集團更加容易去取信或是找尋受害者的工具。其實平臺就是在賣數據，平臺就是讓詐騙集團可以容易地找到特定族群的人，對某種訊息有感的人，然後會有反應，然後你發出交友邀請建立信任關係，很多人容易被詐，然後通常都透過臉書交友，之後變成轉到LINE更私密的聯絡管道當中，透過各種方式去經營信任關係。沒有人一開始就會受騙，但是他如果能成功建立某種信任關係，那就有機會，只是大騙還是小騙而已。

(五)那臺灣除假冒名人和一頁式詐騙外，還有一個很嚴重的樣態不知道政府有沒有去正視，就是複委託的投資，大部分是港股，因為港股有所謂的仙股，就

是一塊錢兩塊錢，甚至不到一塊錢，臺灣的投資人聽信詐騙集團的投資建議，透過臺灣券商複委託自己下單，詐騙集團等到時機成熟之後，就會操作股價讓他從3塊錢跌成剩下3毛，而臺灣的投資人沒有辦法賣出，他其實賣不出去，因為複委託必須是現價交易，他根本不知道他會跌到0.3元。這些券商可以賺複委託手續費，但我想這個詐騙金額是非常龐大。

(六)我覺得臺灣也許從傳播的角度應該是要去蒐集案例普為傳播，因為就像我們反擊假訊息，不可能去查每一則，而且通常是事後，所以最好是預先告訴民眾說，這次選舉可能會有哪些類型的假新聞，就是基於國外或臺灣國內的選舉的經驗，我們會預擬劇本，讓這些東西讓更多人知道說，選舉快到了，你可能會看到的，跟選舉有關的一些訊息，那如果是一二三四五這五種類型呢？可能你看到的話要有警覺性，這可能是假訊息，要經過查證，有點像是打預防針，這就是我所謂的預防勝於治療。沒被騙過的人不知道，但最好不是自己親身被騙，是別人騙的經驗之後，他願意公開出來，讓大家知道說這麼聰明的人也是會被騙。我最近看了韓國有一部電影非常好看，叫做金派特攻隊，這樣的一個故事，他把它戲劇化，收視效果很好，那看過之後會幫助民眾知道說會有這樣的事情發生。尤其現在新聞疲勞，現在讓重要事情讓全國人知道是一件困難的事情，但我們要用一些有創意的方法，包括戲劇化，包括跟網紅合作，去打造宣傳。傳統的政令宣導的這種短片，其實點擊率應該很低吧!

(七)那預防來講，另外一個當然跟電信有關的就是黑莓

卡，中華電信現在似乎有做一些防堵黑莓卡這個部分，比較堵不起來是香港聯通那部分，香港聯通那邊賣的黑莓卡，不需要是臺灣人，他可以買到全世界的黑莓卡，像英國的黑莓卡是不需要實名制，日本也不需要，買了之後他就可以漫遊，你找不到他的身分。

(八)我覺得預防的這個部分就是我們有缺幾個法律上的東西，第一個就是我們對數位平臺的監管，目前其實是沒有法律。歐盟跟英國現在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他採取有有效措施，或者是這個notice and take down的這個運作會比較有效。而且平臺要採取預防性的、有系統的一些措施，不是那麼純粹被動的，因為notice and take down現在其實就有在運作，只是如果涉及到沒有法律禁止的內容，要期待平臺可以有效的收到notice馬上take down，他可能不會照辦，因為沒有法律的的依據。所以我們必須要補這一塊，也就是數位治理。

(九)數位中介服務法在法律的一致性跟很多應該要配套的沒有考慮清楚，最後那個版本沒有通過。可惜的是這件事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一個機會，可能短期內都不太容易有重啟這個討論的機會。

(十)不過，我覺得政府有責任去重啟有關數位服務法的討論，或許就不要再用數位中介服務法了。換個名字更好一點，或許就直接用國外比較通用的名字。

另外就是歐盟的GDPR其實是重要的，我們在個資保護的法律應該要做更與時俱進的修改。其實這部分不太需要學美國，因為美國即使到目前為止，沒有平臺監管的任何法律。他連要通過一個叫誠實廣告法到現在都沒通過，其實就可以用來對付詐騙。那像這一類的我們可能就防詐專法，或者是更通盤的平臺問責的這個法律，他可以降低政府的執法成本，就是說這個成本一部分平臺是要吸收的，他要採取預防性的，有系統的預防性的，以及跟公民社會以及治安機構合作的這樣的一個義務。

(十一)落地還是重要的，只是落地不能解決問題，所以你落地沒有法是不行的，也就是作用法的部分，所以數發部也是要加加油，還有防詐的法律現在草案作用法的部分都還沒有送出來。

(十二)另外歐洲的公民的個資被保護的很好，至少在目前的GDPR包括跨境傳輸都有規範，我們可以努力的去學習歐洲還有英國的這個線上安全法，他們都是民主國家，而且從民主的排名上面，他們還比美國還前面，如果學這些國家的作法，我們就可以去defense說，我們立這些法不會違反民主的問題，是透明公開，而且是公正的，也有很好的立法諮詢跟公共聽證的過程。而且我們不是第一個，因為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。

(十三)比方說，通傳會的數位中介服務法，他就是抄了歐盟的這個數位服務法在平臺規模方面的規定，如果你的平臺用戶超過人口數的十分之一的話，你就

叫超大平臺VLOPs，你就要要受到很嚴格的法遵監管；結果通傳會直接抄到臺灣，就變成兩百萬用戶的平臺就要嚴格監管。事實上兩百萬在全世界是很小的平臺，所以我就說，為什麼那麼的草率倉促，沒有做好研究，直接抄就抄出問題，連我們本土的小平臺都反對，那 Meta 跟 Google 都還不用出來反對，我們的網民、在野黨、各種小平臺都跳出來了，所以這個是是他們的很大的一個失誤。要不然的話，其實歐洲和英國已經示範過要怎麼立法，然後Meta跟Google也會願意善盡他們的法遵的責任。

(十四)最後我認為這個議題永遠是跨部會的，而且我們不能只是只看到打詐這件事情，因為它是數位時代的問題，詐騙只是比較顯性的部分，但是跟數位關聯的有很多問題，防詐專法或許比較能針對防詐，但是數位的、非詐騙相關的問題就無法處理。所以我們還是要去通案的去處理數位治理的時候，就是數位服務法跟GDPR是要有臺灣版本，然後務實的調整，符合臺灣本地的這個需要，但不要比歐盟跟英國更嚴格，要更嚴格必須有很強的defense，因為可能會有侵害言論自由的問題。我們只要學歐盟和英國，甚至學到8成，我就覺得已經是很大的進步了。

(十五)最後一個我還是要強調跨部會合作，其實過去數位的問題，大家都推來推去，最後可能都經過行政院去指定，但是這個指定也不能解決問題，所以未來應該要有一個跨部會的，不管是打詐或防制假新聞，或者是增強我們的數位民主韌性，而且這些問題有些還沒出現，會不斷的出來，我們需要不斷滾動式的，包括這些執法機構都要不斷的提升自己的

know how，才有辦法去面對新的、還沒發生的，或者正在醞釀中的這些問題。

(十六)所以跨部會的機制非常重要，我覺得有一個例子是需要參考的，就是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。聽起來好像就是跨部會聯繫機制的論壇而已，其實不是，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？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)。因為像詐騙或者是這個網路購物的這些糾紛，都需要不同的部會一起來努力，臺灣如果這些部會能夠合併成為一個有固定的、政策性的跨部會的協調機制，而且是要定期去管考的，也就是說這個DRCF是要交出成績單的，而不是今天來開會找次長，甚至有時候是一個更低階的官員來，他可能也不太敢講話，這就是我們的跨部會過去很多都沒有什麼作用，層級雖然很高，但是效果不彰，那就是因為它是一個虛的組織。我們或許還是要有一個像DRCF的實體組織，我們甚至不用去討論說遇到什麼事情到底要找什麼部會，你就直接找DRCF，

就會解決。

附錄B、高檢署履勘會議紀錄

十一、法務部檢察司郭司長永發:

(一)法務部刻正推動「被告總歸戶」,以減少案件,實務上一個帳戶可能有很多被害人匯款,在只有一個被告的情形下,因為被害人眾多,又分別向不同警局報案,就產生不只1件案件,案件再移送轄區地檢署,產生重複調查情形。推動「被告總歸戶」,就是把全國各地被害人報案資料集中由被告戶籍所在地警局調查,如此不會產生重複調查,並在案件調查完後移送或報告轄區地檢署偵查,也可減少案件量,檢察司也將定期召會追蹤執行成效至案件量確實降低。

(二)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,目前只能請偵查檢察官,針對被告惡性重大之案件具體求刑,公訴檢察官確實執行公訴蒞庭,若判決刑度過低時積極提起上訴;刑法已無連續犯規定,改採一罪一罰,法院針對被告犯罪行為分別判處之刑期加起來2、30年,但因為要定執行刑,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,就此法務部會持續與司法院溝通。

十二、高檢署臺南分署吳主任檢察官慧蘭

(一)「窩裡反條款」一直以來都有持續在討論,「窩裡反條款」對貪瀆及毒品案件的查緝有很大的幫助,為何在詐欺案件卻沒有積極推動立法,主要考量2個因素,首先是組成樣態不同,毒品、貪瀆犯罪集團是向上延伸,但詐欺集團是扁平化的組成,賣帳戶、車手、機房各別都是一個獨立的集團;再者是詐欺犯罪,法院的判決的刑度原本就不高,如果被告供

述出介紹賣帳戶的其他人，因為有「窩裡反條款」規定，又獲得減刑讓刑度更輕，民眾是否可以接受？因此關於「窩裡反條款」還在審慎研議中。(按：已於詐欺犯罪危害防制條例內訂定)

(二)在這些廣告下架後，可能經過微調又再上架，Facebook是否可以利用AI方式清查，因為Facebook是境外公司，又涉及商業利益，在無法源依據上，檢察及行政機關要約束，確實有困難。

十三、高檢署劉檢察官海倫:

(一)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，並將量刑因子納入考量以協助法官量刑，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，主要還是因為法院認為量刑是法官的裁量權。

(二)之前我曾調國兩司辦事，據我所知，因為國際情勢，「引渡」又是國與國關係，迄今臺灣沒有跟任何一個國家有成功引渡的案例，目前所採取的方式是撤銷身在國外的我國籍被告的護照，再以遣返方式將被告送回臺灣，即便如此還是很常在被告臨上飛機前，當地警方才告知要將人送到對岸而不讓被告上飛機，這部分雖然突破有難度，但仍會持續努力。

十四、臺北地檢署劉主任檢察官仕國

(一)現在司法實務，法院不分案件，幾乎全部都是從低度刑開始量刑（例如法定刑雖然是六個月以上，五年以下，但司法實務上，幾乎九成多以上都是判6個月、7個月），而這量刑依據判決實務，檢察官還不能干涉，除非檢察官要明確指出量刑有違法之處，否則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。

(二)而量刑最奇特的地方，還有在法院定執行刑時，更是容易產生爭議，例如，詐欺車手，犯了20次，每次都判1年，這20次合超來定一個執行刑時，只要超過1年，20年以下就是合法的，也就是20次犯罪都判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，人民要是知道了，大概也都無法接受。

(三)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。大家看看現在有哪個幫派組織不插手詐欺行業？

(四)我們看到現在詐欺集團用1個帳戶20萬的代價收購銀行帳戶，許多年輕人趨之若鶩，導致詐欺犯罪年齡層一直在下修，這些提供帳戶的人一旦被查獲，偵查中現在都不會說自己是賣帳戶的，反之，都會提供當初跟收購者間虛偽的LINE對語截圖，證明自己是因為求職、為了辦貸款…等各種原因被騙去提供帳戶的，最後因為證據不足，很多都是不起訴，超訴也很多判無罪。

(五)詐欺案件的被告與被害人有時其實很難區分，以近來發生的新聞事件○○大學100多位學生聲稱被騙去辦手機門號案件而言，學生都聲稱是因為受騙申辦門號，拿了業者5,000元，就把手機交給對方，以為對方會付每個月的月租費，結果只付了1、2期就沒付了，害他們要承擔被電信公司追討……未來如有被害人報案，因為收到由這批逢甲學生「被騙」

申辦的門號發送的詐騙簡訊而受騙匯錢時，這些學生究竟是被害人還是被告？

(六)新北地檢察署黃主任檢察官筵銘：詐欺案件中，絕大部分提供人頭帳戶、門號案件中的被告，在社會上往往是經濟弱勢，雖然他們犯罪是事實，但有時候法官會認為判太重這些被告也繳不出易科罰金的錢。

附錄C、檢察官打詐實務暨修法研討會

一、臺北地檢署蕭永昌檢察官

(一)我們希望增加檢察官助理來協助檢察官處理。大家可以看到一個圖表密密麻麻，這個圖表事實上是我們在這個辦詐欺案很常用的整理表，整理一些被害人的姓名、被騙經過、匯款帳號、匯款細節、地點、收款帳號、轉出細節等等，後面一大堆是所謂的第2層帳戶資訊，如果一罪一罰，全部證據要收集到非常詳細，它是非常的消耗時間，你要說這部分有需要法律專業嗎?好像也沒有。或許有人說檢事官也是協助檢察，但檢事官和助理兩者的定位是完全不一樣。

(二)大家知道詐騙一騙再騙，交保出去他接著就繼續騙，把他這個交保錢賺回來。但我們能夠不讓他交保嗎?依據刑事訴訟法第108條第2項或第5項，每次不可以超過2個月，那如果所犯的罪是重刑，是10年以下有期徒刑，一審二審只能夠延押3次，第三審只能一次。普通詐欺罪5年以下，加重其刑1年以上7年以下，組織犯罪防制條例也是10年以下的罪；換句話說你最多也是只能延押3次，檢察官這邊都要花很多的心力去做一些分析，甚至法律上的攻防，那現行的這個羈押規定是否夠用?會不會造成防逃的疑慮?我呼籲說要好好的解釋這個關於詐欺集團的這個相關規定。

二、金門地檢署施家榮主任檢察官

(一)對於被害人來講，這樣真的算破案嗎?警方把大部分人力都投入在人頭帳戶，因為人頭帳戶好查，因為人頭帳戶直接有證據，他匯入哪個款項就抓誰，這最輕鬆嘛!可是這些人頭帳戶、車手取款等等，這些

對他們來講就是工讀生、就是免洗筷，你查到這些有什麼用?他永遠都沒有被瓦解!

(二)個人幣商好像又越來越困難了，所以還是那句話，金管會要加油。對被害人來講，錢又沒有追回來，你沒有扣後面的詐騙錢，又沒有返還，你怎麼可以說你破案?所以老百姓的感覺就是你都沒有破案啊!宣稱破案率90幾趴，那是什麼碗糕?

(三)其實也不是說警方不認真,你要想警方有他的困難，比如說我們沒有科技偵查法，那個GPS爭議6年多了還沒有辦法立法，我們不知道這個刑事訴訟法主管機關司法院為什麼不能做強制處分的立法，我們也不知道立法委員、立法院有那麼多委員，每個都可以主動提案，那6年間換了多少立法委員?沒有人有辦法完成這個立法。GPS的科技含量很低，連這麼低都沒有做到，那我們現在可以做的科技監控是什麼?監聽門號的電話或者簡訊，各位你會用你的門號打電話出去嗎?大家都用APP或網路平臺，那還不用錢對不對，所以現在的科技監控是沒有效的。

(四)當人頭帳戶金管會一直沒有辦法斷絕，每年都有幾萬個人頭帳戶要辦，警方光是辦那個就飽了。當時是有一些亂象就是譬如說一個帳戶可能有10個被害人匯入，那就在10個分局報案，然後就10個地檢署受理，所以看起來案子會一下子暴增很多，都要辦的結果就是每個月分100件，你光是辦這些都爆了，所以你要期待檢方去追查幕後的犯罪首腦或者洗錢管道?各位都有看過起訴書和不起訴處分書吧，如果要你坐在電腦前面，一個月要寫100份，你還有時間去做其他事嗎?可能召開專案小組要深入追查?這部分書記官可能更嚴重，我聽到已經持續5

年以上，只要分發到新北或者桃檢書記官，他聽到是這2個地點他就不去報到了，所以你永遠在招考，但招考都沒用，因為他就不去報到。

(五)我們每年剪綵成立一個新的辦公室有沒有用?其實灰色產業，或者說違法產業，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!

(六)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、NCC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!……我們一直在召開這種研討會，不是說我們喜歡罵人或者喜歡抱怨，是因為我們還沒有打算離職，我們對這個社會還有點熱情，我們對辦案還有熱情，所以我們才要做這些呼籲。

三、臺灣大學林鈺雄教授：

(一)為什麼在打詐研討會討論科技偵查?因為你沒有科技偵查，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，那M化車喔這方面也是臺灣第一，因為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，這個也是世界第一。所以我覺得我們在很多方面會有很少人有的獨創性的想法，當然也造就了我們這種畸形的現象。科技偵查比較關鍵的第3個部分就是設備端

的通訊監察，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，因為我們科技偵查最後還是不會有設備端的通訊監察。

(二)當然就是很奇怪的臺灣現象，我講一個很簡單，從1992年開始，德國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，我們刑事訴訟法法條才500多條喔，但是我們修法次數已經破了法條的數目，但我們科技偵查到現在為止，修的是0條。今天研討會就只有一個目的，就是臺灣還要這樣下去嗎?

四、臺北地檢署姜長志檢察官

(一)我真的不知道金管會在幹什麼，去年的時候6月同一個場次，我們辦了第一場全國打詐研討會盤點了非常多詐欺的現象，第一個人頭帳戶，再來是虛擬貨幣和第三方支付，各位如果去年有參與的話都知道，所以金管會終於動起來，終於有知覺了，說好吧，人頭帳戶他來處理，結果人頭帳戶處理之後，虛擬貨幣他就不管了。

(二)我們罵這些事情、講這些事情，不是為了我們自己，我們如果查不到還不是5點半就可以下班，是不是？問題是一個詐騙案件，從被害人被騙到我手上，中間歷經至少兩三個月，甚至半年以上，錢早就不見了啦。你把人關進去又怎樣？重點是錢要拿回來啊！

(三)我們就起訴幣商，上到法院去說他也是犯罪集團一部分，法官判的都是無罪嘛，這能怪法官嘛？其實也不能怪法官，因為要怎麼證明他跟這些集團有主

觀犯意聯絡？這對法官講也很困難，雖然大家心裡心知肚明，我們是民主國家不能說關就關啊，現在只要發生問題全部把它刑事化送去判刑，送去判刑有效嗎？

(四)第一個問題就是，我要怎麼證明他跟這些詐騙集團有勾結？那什麼都不做，什麼都不管，是不是你金管會在前端先幫我們把個人幣商的這個部分先處理好，管制好。

(五)金管會被我們逼到發這種新聞稿，來各位，新聞稿說個人幣商沒有完成法遵聲明自屬違法。我接下來問，他違什麼法？我說你違法就違法，不是這樣吧！我們民主國家跟他說違法，你要跟他違什麼法嘛！我們來盤點一下他有違反洗錢防制法嗎？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。

(六)第二個他有違反公司法嗎？那金管會說什麼違反商業登記規則，沒做稅籍登記，問題是你罰得到他嗎？你是他的主管機關嗎？這全部都在甩鍋給別人對吧！

(七)你不知道怎麼改，我現在告訴你。第一個我們強力要求金管會要開始做幣商的登記，如果你要經營幣商，你就要在金管會開始登記，登記這件事不要再甩鍋給別人，你的個人幣商沒有登記不可以營業，重點是你要修訂規則，什麼人什麼樣的條件才可以來申請幣商？你是不是有稅籍登記？是不是有公司登記？是不是商業登記都登記好再來跟我金管會登記，重點是你錢包要登記，你冷錢包、熱錢包，

你的相關錢包金流就看得到。

(八)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！我們最近有看到委員希望能夠由檢察官當公益代表人，由我們當公益代理人去打訴訟，這個不是什麼大問題，問題是我要能夠追到人，追到錢嗎？要先有錢，才能求償嘛！找不到錢你要怎麼賠？

五、臺北地檢署羅韋淵檢察官

(一)法務部去年指派我到美國哈佛大學做訪問學者，研究的題目就是網路犯罪以及虛擬貨幣犯罪，首先談到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，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這個爭議?甚至是法律依據不足?其實他們已經明確規定任何法人或自然人都應該要被定位，只要你從事這個虛擬資產的服務的話，那就應該要受到規範。

(二)我國最大的爭議是在哪裡?依據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條第2項，他所說的這個本事業，也應該依照這一個條款被規範，這個事業是已在國內設立登記者為限。也就是說，如果今天這位所謂的幣商，他是以個人跑單幫的方式，他不去做公司登記商業登記，或其他的稅籍登記，那他就不會在這個辦法裡面被規範，那既然不在這個辦法裡面所規範，那主管機關也就沒辦法依照這個辦法去裁罰，對他做處理，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。

(三)FATF的相關指引也明確地指出，從事虛擬資產服務提供者必須取得相關證照，或者是許可，而且它強調這些虛擬資產服務提供者，應該要受到權責機關的監理或是監控，特別強調非自律組織。當然我了解金管會目前是想循序漸進的訂出業者自律規範，期待業者有所自律，不過自律依照目前的犯罪案件爆發，可能還是不夠。關於個人幣商的管制，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。

(四)虛擬貨幣跟我們實體的金融產業裡面有一點非常不一樣，我們去銀行開戶必須要提供我們的證件、相關文件，甚至簽名，才有辦法開一個銀行戶頭，因為銀行受到非常嚴格的監理。但虛擬貨幣不是如此，各位只要有手機Google Play或者是App Store裡面就可以任意下載一個非託管錢包，不需要經過任何實名認證，你就可以使用。非託管承包的雖然目前技術上是可以去追查到他的名字，但是這個錢包的背後到底是由誰實質掌控，我們是不知道的，或者是必須要花費很多的資源才有辦法去拼湊出來。

(五)我們很難期待規定每一個虛擬資產用戶都不能去使用非託管錢包，因為這涉及到人民財產權或者是隱私的問題，但如果今天這個錢包是用於商業使用，那是不是應該要課予業者要有一個呈報錢包地址

的義務，不管是公司或者是個人幣商。再來一個是目前我國的洗錢防制法其實已經都施行了，但有個例外，第7條他規定的是轉帳規則，轉帳規則講的是，客戶要把虛擬資產轉給虛擬資產服務提供商的時候，那這個客戶必須要先說明資產的上一層來源是誰?什麼姓名?以及他的基本資料，以及他轉進來的用途是什麼?轉出去的話也必須要跟虛擬資產服務提供商說明說我要轉給誰?做什麼用途?否則虛擬資產服務提供他就不應該准許這一筆交易。用這個方式來補強錢包地址可能是匿名的問題。

(六)我們都知道被害人去報165之後呢,銀行它有一個機制也就是它可以設定警示帳戶及時的去攔阻這一筆錢，那設定警示帳戶的法律依據是「存款帳戶及其疑似不法或顯屬異常交易管理辦法」，那如果今天這是虛擬貨幣被騙到交易所裡面，我們目前有法律依據去阻攔嗎?沒有。但我們需不需要?需要。目前這些虛擬貨幣交易所，他們覺得很困擾，當他們系統偵測到一筆異常的這個虛擬資產流進來的時候，他們覺得這個嚴重的疑似不法，可是他們沒有法律依據去凍結，往往只能靠落落長的用戶條款先暫時扣住，所以個人認為業者呢也需要有一個法律依據給他們當作他們的後盾，去凍結這些疑似不法的虛擬資產。那另外，銀行跟銀行之間如果設警示已經來不及了，錢已經流到下一層，那銀行之間有一個通報的義務，繼續一層一層的通報，及時的做阻攔。但虛擬資產服務業者目前也沒有相關法律依據可以這樣子層層通報。

六、臺北地檢署洪敏超檢察官

(一)這個月初一個美國的幣流分析公司做了一個簡報，

他說現在臺灣跟日本成為洗錢最終場地，原因很簡單啊，因為臺灣在國際政治上的地位比較比較沒人理啦，對有心人士而言很簡單，完成法遵聲明不如直接買下公司，就跟王牌交易所一樣也是直接換人嘛，上次我們證期局副局長說我們就禁止境外的，沒登記不准他進行招攬，但是大家看到這個招攬非常多啊!YouTube上放廣告都算招攬嗎?合約王者挑戰賽直接在臺灣辦算嗎?新加坡的MEXC抹茶交易所在臺灣辦，那這算不算招攬呢?

(二)第三方支付也是一樣，其實大家講了一大堆能量登錄，最後沒有並落實，事實上目前為止通過登錄的就是16+1家，我們原本統計的有多少?1萬多家!代表1萬多家根本不鳥你!其實你看移工，現在逃逸移工有大概將近8萬多人其實都是風險，我們不是有罪推定，而是他是一個風險嘛。他的帳戶怎麼使用我們無從控管，因為我們找不到人。目前解法是所有通過這個離境移工去掌握，但實際上我覺得很簡單，像玉山銀行開戶總約定書就是說，如果他沒有去更新自己的資料，導致銀行沒辦法評估做法遵的話，就只會視為不合作帳戶。我覺得很簡單的道理，你在臺灣這個土地上，你就算你不是國民，你有遵守我國法律的義務，你當逃逸移工的時候你都覺得臺灣的法律我不用管，我們為什麼要為這個普惠金融，提供到隨時隨地都可以使用你的信用卡?

(三)黑莓卡這部分，我測試給大家看，我花250塊在蝦皮買的，實名制根本隨便輸入都可以過關，大家看這個IP是香港的，代表我就用這張卡之後，其實你沒有辦法掌握實際的身分。

(四)社群媒體去投放不實廣告，其實這個要處理這些網

頁詐欺最快的方式就是用最短的時間最有效率的方式最簡易的程序去阻止，過往的方式都是向法院申請扣押，才再去TWNIC去扣，太慢了，所以最近因為創意私房，他改了一個緊急方式讓警察投單就可以，那這代表什麼?其實過往真的不需要透過檢方。