中華警政研究學會

警政與警察法相關圓桌論壇(第 61 場)

【〈打擊詐騙〉系列座談(一)】紀錄

日期：2024 年 3 月 15 日 14:00

地點：網路視訊

主持人：中央警察大學 楊源明校長

鄭理事長、朱前院長、廖教授、線上的各位老師、朋友大家好，歡迎大家今天來參加「打擊詐騙」系列座談。本場座談也是中華警政研究學會舉辦的第 61 場論壇，今天很榮幸來擔任主持人。中華警政研究學會在林德華榮譽理事長及鄭善印理事長的帶領下，每個月均舉辦警政與警察法學圓桌論壇，這對我國的警政治安發展扮演相當重要的角色。

近年來詐騙集團利用資通訊科技作為犯案的工具，不斷衍生新型態犯罪手法，並藉由金融網路科技的便利性迅速轉帳、匯兌，隱匿贓款流向，規避檢警的偵查，這儼然已對全球人民財產造成高度危害，是當前社會治安關注的重點議題。

政府為展現打擊詐欺犯罪決心，配合當前施政要點，由行政院整合各相關部會，於民國 111 年 7 月 15 日頒訂「新世代打擊詐欺策略行動綱領」及成立「打詐國家隊」，跨部會合作共同打擊詐欺。另因應詐欺犯罪演進趨勢，在 112 年上半年重新盤點打詐國家隊相關策略、人力、物力及經費，精進推動「新世代打擊詐欺策略行動綱領 1.5 版」， 針對打詐相關作為分為：「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 4 大面向進行管考，並也於去年完成「打詐五法」修法工程。

以臺灣詐欺犯罪趨勢來看，112 年發生 37,984 件及 88.87 億元財損，相較 111 年 29,509 件及 73.28 億元財損，其發生數增加近 3 成；全國地方法院判決詐欺罪的有罪人數更是達到了 14,651 人，比前一年增加了 7.41%，且詐騙的方式也漸趨多元，包括網路詐欺、電信詐欺等各類型都呈現增加的趨勢。

有鑑於此，行政院打詐辦公室表示，今年度會將「打詐專法」草案送立法院審議。行政院陳院長與內政部林部長更在本月 12 日立法院院會質詢時表示，目前各機關「打詐專法」草案已經回到內政部彙整，行政院也已指示本會期提到立法院審查。專法內容的方向是健全電信金融機構，數位精進管理，並提高詐欺刑責，盡快完成送立法院審議。因此，期待中華警政研究學會藉由此系列「打擊詐騙」座談，分享心得、集思廣益，提供具體建言，協助政府在打擊詐騙的路上持續推進。

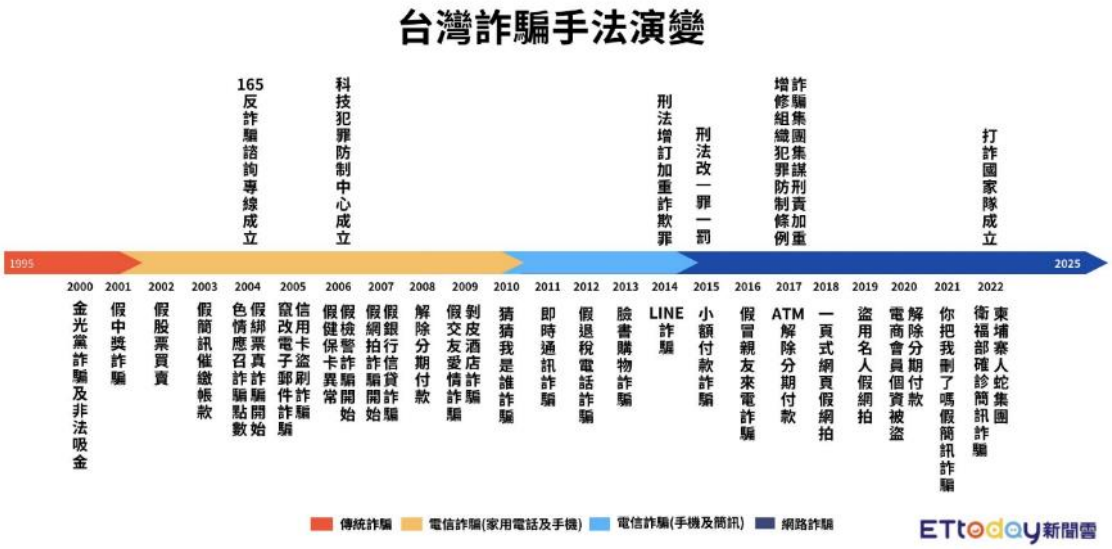
引言人1：中華警政研究學會 鄭善印理事長

〈主題：電信人頭門號問題〉

壹、詐欺案件現況

我國的詐欺案件近十年來逐年增加，依刑事警察局統計，2023 年近 4 萬件，受騙金額近 89 億元，令人怵目驚心。相信有許多國人都曾接獲疑似詐騙電話或看過以假亂真的廣告，即便警政署的 165 專線也曾被自媒體利用為二次詐騙的行頭，詐騙案件的橫行已達影響國人日常生活的程度。

這些詐騙案件可以分門別類，以尋求其手法及推敲出防制的方法。我認為這些詐騙至少可以分為：一、屬於銀行法之吸金案，例如 IMB 案。二、屬於刑法或洗錢防制法之詐欺案，例如衛生福利部確診簡訊詐騙案。在刑法或洗錢防制法之詐欺案，依其利用之工具，又可分為：(一) 早期利用電信詐騙之案件，例如猜猜我是誰案。(二) 近期利用網路廣告詐騙之案件，例如各類詐騙投資案。(三) 無論何種詐欺均需利用之人頭帳戶案，例如柬埔寨人蛇集團拘禁人頭案。這些詐騙案件，ETTODAY 新聞雲層曾製作「台灣詐騙手法演變圖」，明顯標示出詐欺時間與手法的演變。茲即依上述演變圖之分類，略述各種詐欺手法及法制規範於後。



貳、各類詐欺防制法規

一、吸金案：2024 年 3 月 8 日 yahoo 報導：「基泰建設前董事長陳 00、前副董事長兼總經理馮 00 等人對外招攬投資基泰大陸地區不動產，涉嫌不法吸金新台幣逾 5 億元，台北地檢署今天偵查終結，依違反銀行法起訴基泰建設及陳 00 等 15 人」。此為典型吸金案，IMB、百富、澳豐兆富等吸金案的手法均相同。這些吸金案違反的是《銀行法》第 29 條第 1 項：「除法律另有規定者外，非銀行不得經營收受存款、受託經理信託資金、公眾財產或辦理國內外匯兌業務。」又依《銀行法》第 125 條第 1 項：「違反第 29 條第 1 項規定者，處三年以上十年以下有期徒刑，得併科新臺幣一千萬元以上二億元以下罰金。其因犯罪獲取之財物或財產上利益達新臺幣一億元以上者，處七年以上有期徒刑，得併科新臺幣二千五百萬元以上五億元以下罰金」。此外，這種經

濟犯罪案件傳統都是法務部調查局在辦，警察是不能辦的。本文對於吸金案不再贅述。

二、刑法或洗錢防制法案：一般國人所熟悉的詐騙案，都與刑法詐欺罪或洗錢防制法的一般洗錢罪相關。而依其詐騙工具，又可分成電信詐欺、網際網路詐欺、人頭帳戶詐欺三種。

（一）以電信為工具之詐欺

上述台灣詐騙手法演變圖中，「假中獎詐騙、假簡訊催繳帳款、假綁票真詐騙、竄改電子郵件詐騙、假健保卡異常、假檢警詐騙、假銀行信貸詐騙、解除分期付款、假交友詐騙、剝皮酒店詐騙、猜猜我是誰、即時通訊、假退稅電話詐騙、小額付款詐騙、假冒親友來電詐騙、ATM 解除分期付款、你把我刪了嗎、假簡訊詐騙、衛服部確診簡訊詐騙」等，應該都是以「電信的人頭門號」來詐騙，它的特色是雖然有發話人，但真正的門號所有人卻不是發話人，等警察找上門後，真正的門號所有人至多被處以幫助詐欺罪，背後的主謀仍逍遙法外。雖然，近年這種詐騙手法較為少見，但卻讓國人餘悸猶存，經常懷疑日後是否會再出現電信之新詐騙手法，故仍不能不加以防範。目前為止，主管全國電信業務的通訊傳播委員會（以下簡稱NCC），為管理人頭門號，已發佈《電信事業受理申辦電信服務風險管理機制指引》，並已草擬《電信事業用戶號碼使用管理辦法草案》公告。

（二）以網際網路為工具之詐騙

電信詐騙之外的新近詐騙手法，例如投資詐欺，大多是以「網際網路為工具的方式」來詐騙。2023 年的詐騙投資案已佔全體詐欺案的 51%，其勢頭不容小視，尤其許多名人名社均被濫用為行頭，最堪注意。例如自由時報 2020 年 3 月 23 日即曾報導：「165 在線反詐騙聯盟可『追回被騙資金』？刑事局：新詐騙手法！」，其內容為歹徒利用 165 名義，博取民眾信任，欺騙民眾可以追回交友網站被騙資金，以再次騙取佣金，可謂是二次詐騙。有關於網路投資詐騙，金融監督管理委員會（以下簡稱金管會）曾在 2023 年 5 月 30 日，修訂《證券投資信託及顧問法》增訂第 70 條之 1 及第 113 條之 1 條文，其修正重點如下：

1. 增訂非屬證券投資信託事業及證券投資顧問事業者不得從事之廣告行為類型；另網際網路平臺提供者等網路傳播媒體業者刊登或播送廣告應載明委託刊播者及出資者相關資訊，且不得刊登或播送違反規定之廣告，如於刊播後始知該廣告有違規情事，應主動或於司法警察機關通知期限內移除廣告、限制瀏覽、停止播送或為其他必要之處置，並明定網際網路平臺提供者等網路傳播媒體業者與委託刊播者、出資者之連帶損害賠償責任。
2. 明定網際網路平臺提供者等網路傳播媒體業者未於通知期限內移除、限制瀏覽、停止播送或為其他必要之處置者，由通知廣告下架之司法警察機關處以罰鍰，並責令限期改善。

警政署嗣後也根據該規定，訂頒了《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》。

（三）以人頭帳戶為工具之詐騙

無論是電信詐欺或網路詐欺，無不利用人頭帳戶以為接受、移轉贓款之工具。故亞洲各國如日、韓、中、台很早就有買賣銀行帳戶之產業，買者甚至在報章雜誌刊登廣告

收購帳戶，例如日本就是。我國在十五年前購買帳戶的廣告也甚囂塵上，當時一個帳戶約 2 千新台幣，要看銀行的分支機構多寡，分支機構多者價格貴，如郵局，反之則少，聽說近期一個帳戶要價至少 3 萬元，可見人頭帳戶的市場供給面也稍有抑制。但日本早在 15 年前已出現收購人頭帳戶者，處一年以下有期徒刑之法規，我國則至 2023 年才對收購者處刑。

洗錢防制法 2023 年 6 月 14 日由法務部主導修正，增訂了兩個重要條文。

第 15-1 條：「無正當理由收集他人向金融機構申請開立之帳戶、向虛擬通貨平台及交易業務之事業或第三方支付服務業申請之帳號，而有下列情形之一者，處五年以下有期徒刑、拘役或科或併科新臺幣三千萬元以下罰金：

一、冒用政府機關或公務員名義犯之。

二、以廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散布而犯之。

三、以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄之方法犯之。

四、以期約或交付對價使他人交付或提供而犯之。

五、以強暴、脅迫、詐術、監視、控制、引誘或其他不正方法而犯之。

前項之未遂犯罰之。」

第 15-2 條：「任何人不得將自己或他人向金融機構申請開立之帳戶、向虛擬通貨平台及交易業務之事業或第三方支付服務業申請之帳號交付、提供予他人使用。但符合一般商業、金融交易習慣，或基於親友間信賴關係或其他正當理由者，不在此限。

違反前項規定者，由直轄市、縣（市）政府警察機關裁處告誡。經裁處告誡後逾五年再違反前項規定者，亦同。

違反第一項規定而有下列情形之一者，處三年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金：

一、期約或收受對價而犯之。

二、交付、提供之帳戶或帳號合計三個以上。

三、經直轄市、縣（市）政府警察機關依前項或第四項規定裁處後，五年以內再犯。

前項第一款或第二款情形，應依第二項規定，由該管機關併予裁處之。

違反第一項規定者，金融機構、虛擬通貨平台及交易業務之事業及第三方支付服務業者，得對其已開立之帳戶、帳號，或欲開立之新帳戶、帳號，於一定期間內，暫停或限制該帳戶、帳號之全部或部分功能，或逕予關閉。

前項帳戶、帳號之認定基準，暫停、限制功能或逕予關閉之期間、範圍、程序、方式、作業程序之辦法，由法務部會同中央目的事業主管機關定之。

警政主管機關應會同社會福利主管機關，建立個案通報機制，於依第二項規定為告誡處分時，倘知悉有社會救助需要之個人或家庭，應通報直轄市、縣（市）社會福利主管機關，協助其獲得社會救助法所定社會救助。」。

除此之外，金管會也公布了《金融機構防制洗錢辦法》、《洗錢防制法第十五條之二第六項帳戶帳號暫停限制功能或逕予關閉管理辦法》。

另外針對第三方支付產業的帳戶問題，金管會也在 2023 年 1 月 19 日制定《電子支付機構管理條例》，並陸續頒訂《電子支付機構身分確認機制及交易限額管理辦法》、《電子支付機構管理條例第五條第二項授權規定事項辦法》等。

參、現行防制三種工具詐欺法規的缺漏

雖然訂有許多防制詐欺的法規，但仍有許多缺漏，以至於出現下述的批評。

一、人頭門號部分

例如 Yahoo 奇摩新聞 2024 年 3 月 6 日報導：「立法委員徐巧芯、黃健豪和葛如鈞今（6）日踢爆，中華電信的合作業者，將未實名的『軟號』賣給其他詐騙集團，更利用電信後台漏洞竊取國人個資，國營事業竟成詐騙集團的工具。黃健豪指出，『魔方移動公司』在 2020 年是 NCC 核准的虛擬行動網路服務經營業者，屬於第 2 類電信業者可以承攬行動轉售、加值等服務，但到 2021 年 NCC 審查時，已經廢止其許可。他說，直到昨晚，在魔方移動的網站，仍寫著為中華電信合作業者，為什麼執照被撤銷還會繼續合作？」。

其所以如此，本文以為肇因於電信業者並沒有落實「確認客戶」及「不定時抽查」制度，老字號的中華電信都這樣了，其他四家電信業者，恐怕更有缺漏。

二、網際網路廣告部分

雖然，警政署緊接在《證券投資信託及顧問法及》增訂之後，訂頒了取締規則，但事情好像沒有進行得那麼順利，我們只要觀察自由時報 2024 年 2 月 19 日的報導即知：「詐騙集團假冒財經名人及政商人士，透過網路平台大量投放假投資廣告，刑事警察局為此成立專責小組執行每日蒐報，去年下半年共移請業者下架近五萬則假投資廣告，其中最大戶是臉書（Meta）逾四萬六千則，占比逾九成，警方強調，網路平台業者須擔負企業社會責任，未來將定期公告，降低民眾遭詐機率」。

聯合報在 2024 年 2 月 19 日也報導說：「經查發現曾通報下架相同內容廣告仍持續出現，顯見網路平台業者未落實源頭管理；遏止違法廣告不能單憑警方通報下架，需業者擔負企業社會責任配合，發現違法主動移除、限制瀏覽等」。據聞，警察雖欲進行取締，卻連行政處分調查通知書都寄不出去，原因在於國際媒體大廠的總部都在境外，其國內代理人根本不理警察的要求。

本文以為，對於國際網路大廠，各國都有與之交手的經驗，各國也都以不同方法獲得國際大廠的尊重與合作，若能在商言商而不要太多其他顧慮，對國際大廠應仍可從各國實踐中學到方法。

三、人頭帳戶部分

2024 年 3 月 11 日三立新聞網報導：「由基層檢察官組成的『劍青檢改』認為，許多人甘願販賣帳戶或交出提款卡、密碼，協助詐騙集團收款，事後又以被害人之姿，於司法案件結案後，繼續助長詐團。而銀行行員即便察覺有異，在『普惠金融』大旗下，得自行承擔遭申訴的壓力，只能無奈屈服、道歉，使得詐騙集團更加無法無天。呼籲金融主管機關應堅定立場，力挺基層，才能真正有效落實金融監理及洗錢防制。

劍青檢改認為，各類人頭帳戶橫行氾濫，是詐騙集團持續猖獗的禍首。不少人甘願販賣帳戶，輕率交出提款卡及密碼，協助詐騙集團收款，事後卻又以被害人之姿，辯稱遭網路騙走帳戶，再利用司法案件結案後，仍能大開新帳戶之便，持續輸送新帳戶給詐團，等於如入無管制之境」。

本文以為，人帳戶問題與人頭門號同，都肇因於未落實確認客戶及不定時抽查，尤其在「普惠金融」與「普惠電信」的大旗下，人頭帳戶與人頭門號的充斥，當然會增加業者一部分的利潤，故業者當然缺乏打詐誘因。

肆、日本法制比較

相對於我國打詐法制，日本另有一套作法。今即以電信為例說明之。

日本的《手機非法使用防止法》可謂與我國 NCC 打算頒訂的《電信事業用戶號碼使用管理辦法草案》非常類似，例如兩者同有「契約締結時之本人確認義務」、「過戶時之本人確認義務等」、「中介業者之本人確認義務等」、「過戶時需得手機事業者的同意」，並且在確認時區分自然人與法人，而有不同之確認項目。

不同者在於日本在該法的罰則部分，臚列出許多處罰條款，並且均以「刑罰」，如有期徒刑或罰金為名目，而非以行政處罰為名目。我國電信事業用戶號碼使用管理辦法草案，則無罰則規定。其母法的電信管理法第七章罰則，則對於相關違法行為，多以「罰鍰或限期改善、停止使用、廢止登記」等，作為處罰名目。其所以如此，乃因日本在二次戰後改走美國路線，二次戰前的行政處罰，大多以刑罰名目取代。但我國在最近 20 年，卻全面採取德國法制，而將國家對違反法律者的處罰，採二元處罰體系，亦即刑罰與行政罰併行。然而，卻對處以行政罰的「預防犯罪行為」，究竟應由哪個機關管轄，卻未曾定性。反觀日本，雖處罰大多改採刑罰名目，但一樣用刑罰罪名威嚇的犯罪預防，卻清楚地交給警察來執行。

例如，日本《手機非法使用防止法》的第 8 條即規定：

「為防止手機通訊的非法使用，警察局長認為有必要時，可以要求已簽署與涉及下列條款之一罪行的手機等通訊提供契約的手機業者，根據國家公安委員會的規定，對該契約用戶進行第九條所規定的確認事項。

一、當有足夠理由相信已發生本法規定的罪行時；

二、當認為手機通訊符合刑法第 246（詐欺罪）、249（恐嚇罪）條之罪，或有足夠理由認為手機通訊被濫用於可能導致損害或公共危險，且屬於政令所定的罪行，而有高度防止之必要時」。

第九條（契約者的確認）

依前條第一項規定受到確認要求的手機業者，得依總務部的規定，對該契約用戶進行確認，以確保其具有手機通訊契約用戶身份所需的相關事項」。

由此可知，日本警察仍然負起「犯罪預防」責任，並且在執行此項責任前，可以對目的事業主管機關用某種協商方法，要求再次本人確認。其餘兩種管道的犯罪預防，因業篇幅所限，即不再贅述。

伍、是否宜以專法方式訂定「打詐專法」？

本文以為，現行打詐五法均為實體法上的犯罪處罰法，亦即對於犯罪者應以何種處罰來面對的法律。但犯罪尚有「預防與制止」[1]兩個面相，犯罪的制止，最淺顯的就是警察對於街頭鬥毆的制止，犯罪預防則是所謂消彌犯罪於無形，這是至今為止警察較少從事的工作，若欲以打詐專法作為詐欺犯罪的預防專法，則本文認為十分洽當。

行政院於 2023 年 5 月 4 日通過的「新世代打擊詐欺策略行動綱領 1.5 版」，意圖精進「識詐、堵詐、阻詐、懲詐」4 大面向，並運用公私協力推動各項防詐作為，達到「減少接觸、減少誤信、減少損害」的 3 減目標，以全面降低詐騙受害事件，本文認為仍然是打詐的

[1] 犯罪的「預防、制止與偵查」三個面相，本文受教於李謀旺副局長。

基本綱領。在此基本綱領下，本文認為，「打詐專法應與實體處罰法區隔，僅對違反者處以罰鍰而不應有刑罰名目的處罰;打詐專法除以目的事業主管機關作為處罰名義人外，仍得以處理犯罪預防的機關，作為背後支持、協力及監督的力量;打詐專法也無須規定過多，只要將預防詐欺犯罪的幾個重要概念與工具清楚規定，並對違反者如何處以罰鍰即可。

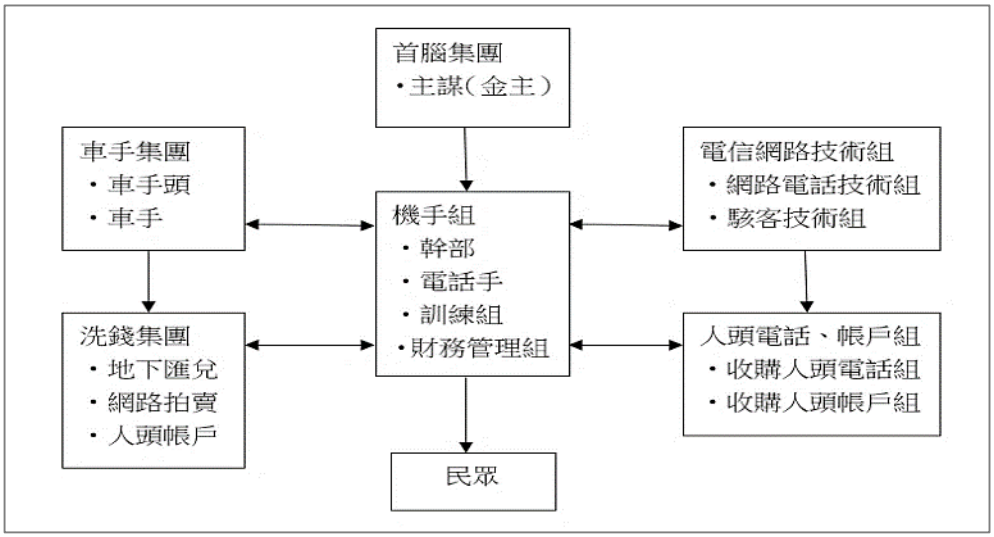
引言人2：中央警察大學刑事警察學系 廖有祿教授

〈主題：二類電信在詐欺上的作用及其治理方法〉

電信詐欺犯罪

- 利用傳統市話、行動電話、網路電話或衛星電話等通訊工具，以微波、衛星通訊系統、電腦或網路等作為工具從事詐欺行為。
- 電信流為承載發送詐騙話術的話務，由以下三者組成，分別為提供話務平台的系統商，與共犯及被害人間聯繫的人頭卡，以及電信詐欺機房內的電腦手與機手。
- 在通訊與網路匯流下，電信詐欺機房是跨境電信詐欺犯罪成功的關鍵，詐騙話務路由隨著匯流後呈現 IP(Internet Protocol)化、雲端虛擬化、跳台層轉化、委外分工細膩化與通訊多元化等情形，且有逐漸出現智慧型手機通訊軟體詐騙的新手法。

電信詐欺集團組織



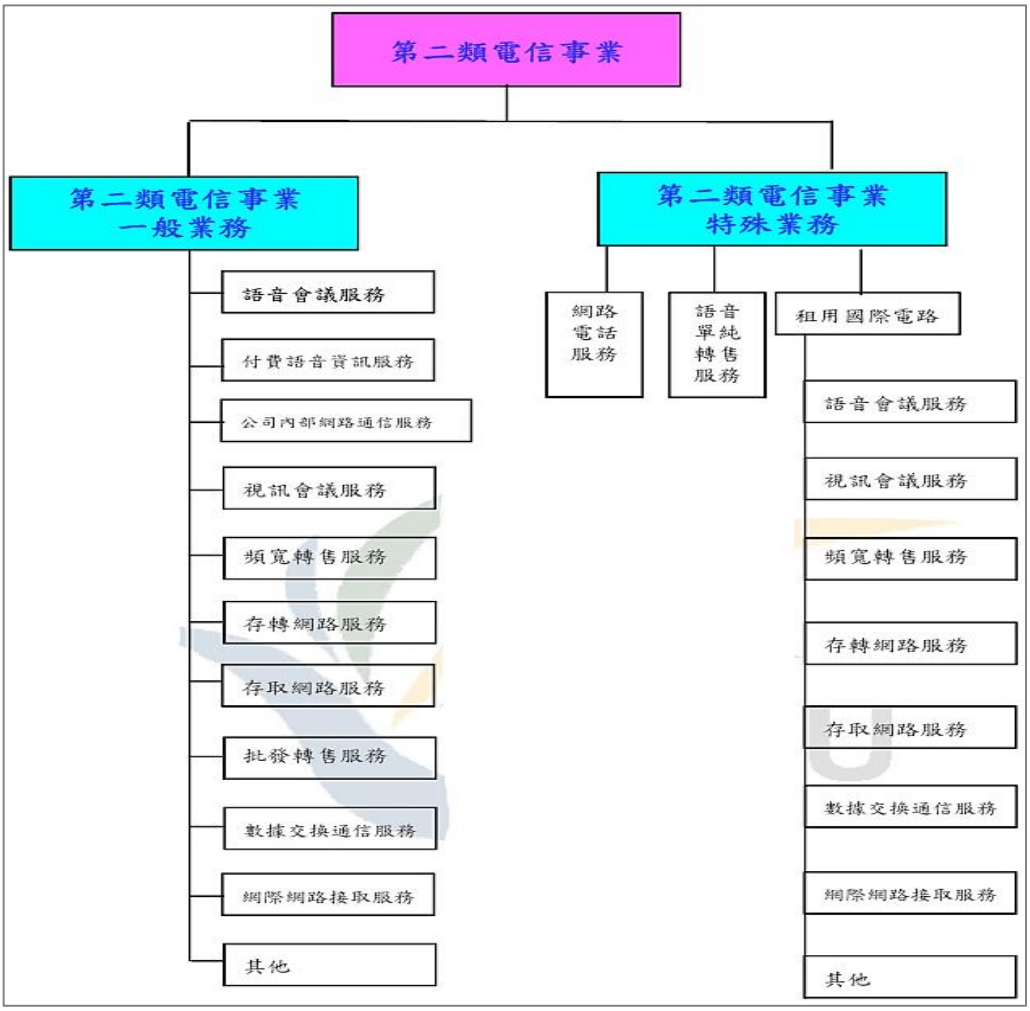
相關名詞

- 第一類電信：自行建設其提供電信服務所需的基礎架構、網路、機房等設備，以經營有線、無線電話語音及網際網路業務等電信服務的業者。
- 第二類電信：沒有架設實體線路固網或實體無線基地台，而是以向第一類電信業者承租固網或無線基地台一定數量的門號或頻寬來經營其電話或網際網路業務的業者。
- 第二類電信事業特殊業務：指經營語音單純轉售服務、E.164 用戶號碼網路電話服務、

非 E.164 用戶號碼網路電話服務、租用國際電路提供不特定用戶國際間之通信服務或其他經主管機關公告之營業項目者。

- 第二類電信事業一般業務：指特殊業務以外之第二類電信事業業務。

第二類電信事業業務分類圖



為什麼要分成第一類和第二類？

- 電信業進入門檻高：大多數國家將電信分為第一類與第二類，第一類行動電信業需要投入大量資金，建設端對端完整的電信基礎網路，以確保全區電信服務品質的良好。而第二類行動電信業者則是承租第一類行動電信業者的電信機線設備，以提供電信服務予大眾。
- 頻譜資源有限：二類行動電信業者營業模式相對一類行動電信業者有彈性，因其租用一類行動電信設備來提供電話服務、寬頻轉售及行動轉售和加值服務等，其網路品質不僅和一類行動電信完全一樣外，二類行動電信服務商『小而美』的經營模式，反而能提供給用戶更好、更便利的服務品質，因此這也是二類行動電信業者的優勢。

詐騙機房

- 機房一般來說泛指配有許多電腦、機械機台的數據中心；然若用於詐騙集團則是指專門僱人打電話或利用網路進行詐騙的場所，於機房工作成員可依階級分為一線、二線、三

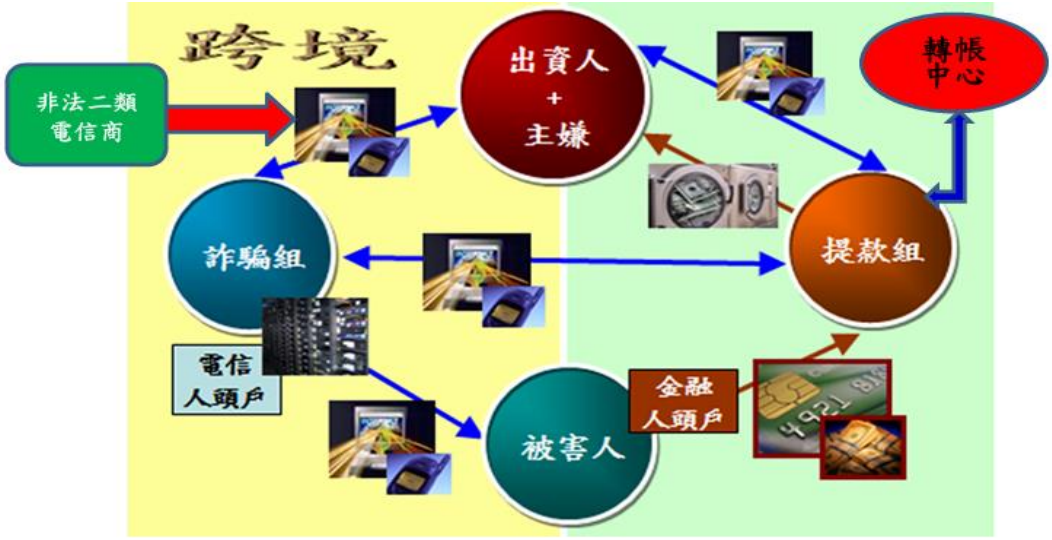
線，如同電話推銷業務概念，若詐騙所得高、業績好或詐騙成功率高，則可能晉升管理幹部。

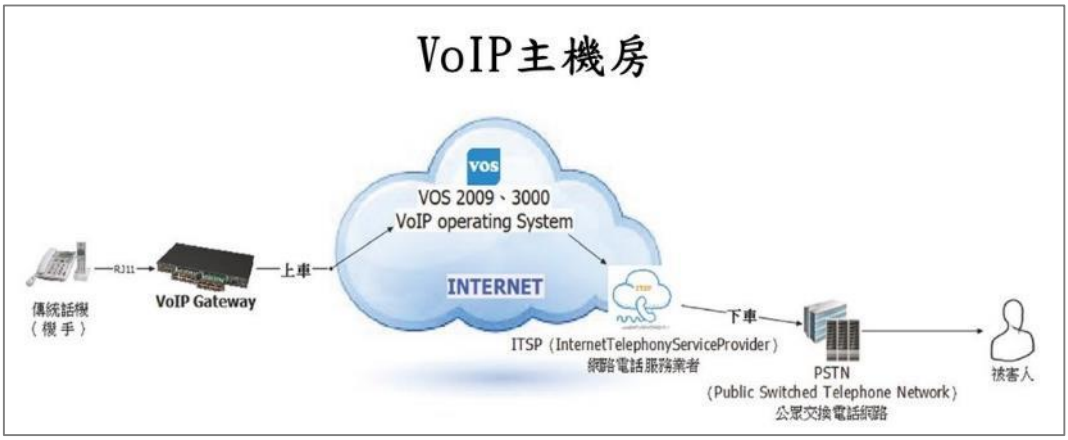
- 近年來網路資訊及交通往返普及，為了躲避追緝，有些詐騙集團轉往東南亞設立機房，而機房內也需要人力撥打電話進行詐騙，也就衍生出柬埔寨「豬仔」事件。
- 機房內往往被搜到非法數位式移動節費設備、網路數據機、分享器、遠端監視器、筆記型電腦及手機…等多樣設備，以供犯罪使用，有些詐騙集團甚至把相關器材裝進行李箱成為行動機房。

二類電信與電信詐欺犯罪之關係

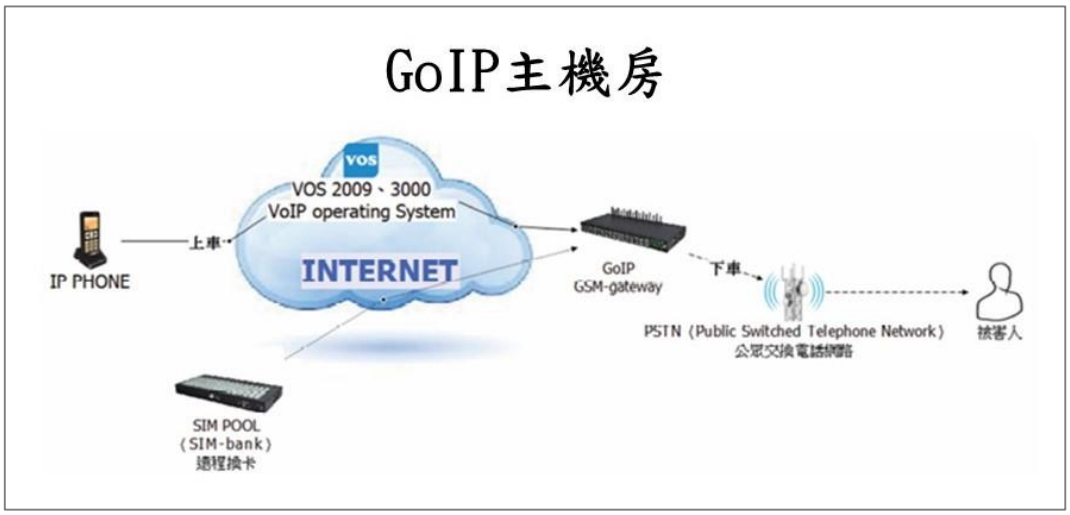
- 二類電信被利用作為詐欺工具 ，最主要之原因有二：「架設容易，不需要經過公眾之電信網路，因此不易遭到司法機關之監控」、「須花費之成本較低」。
- 對於電信詐騙集團而言，隱藏身份便是他們最重要之考量，於是便有部分合法之二類電信業者，屈服於電信詐騙集團所支付之高額報酬下，將實體機房隱藏於一般民宅內，成為所謂之非法二類電信。

跨境電信詐騙集團組織架構暨其分工模式





此類主機房在國內已為少數，由於成員過於龐大，內部管理較複雜，稍有不慎走風，即會曝露行蹤，且網路與電話都需要佈線，機手座位、話機與相關設備搬遷後再佈置新點，費時費力，靈活度不足，不過由於所需設備經費低，人員集中管理可減少開支，境外主機房仍是首選。



GoIP機房只是扮演中繼的角色，偵查時會讓人誤以為該處即是主機房所在，進入時找不到犯罪者，僅能扣得光纖網路、GoIP閘道器、基地台無線電波接收器及微型基地台強波器等相關通訊設備，此種主機房僅需少數幾個人即可維運，平時不需有人進駐，故障排除時再入內，更有以 Team Viewer 遠端連線，即可連入設定相關參數，不過重新插拔線路與開關設備還是需要人員進入處理。

轉介型主機房通常位於小套房中，犯罪者通常會在套房的門板頂部加裝抗動偵測器，以偵測入侵，並在套房內架設網眼做為遠端監控，並以紅外線 感應器做為入侵警報，在高樓層中，犯罪者有時會利用 Wi-Fi 無線電波來介接，當偵查人員攻入套房撲空，在警覺受騙後，往訊號發送的方向清查大樓時，犯罪者已掌握足夠的時間，毫無損失地全身而退。

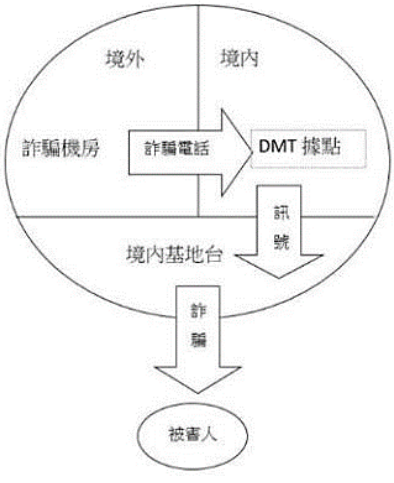
新型態主機房

當主機房遭查獲時，偵查人員會將設備切換至飛航模式，此時設備狀態會顯示為離線，當管理者發現異狀，且覺得有東窗事發之虞時，即可透過登錄 icloud 帳號，對各個連線的設備，發送清除重設的指令，此時若設備為上網連線狀態，則其於接獲清除重設指令時，會馬上抹去設備上的所有數據，將設備重置

各種詐欺機房的特徵與介接方式之比較

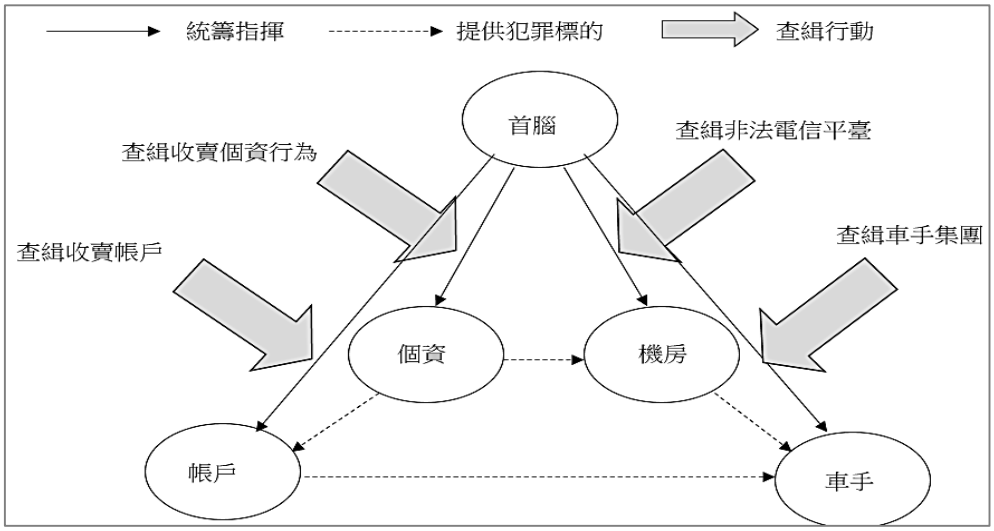
機房種類	特徵	介接方式
傳統型	動輒 10-20 人或者更多，以租賃整棟透天厝、別墅或民宿居多，亦有租用整層大坪數樓層者，人員管制進出，且生活軍事化管理。	Wi-Fi、VoIP 閘道器
中繼型	以 DMT 介接，通常由 1-2 個人管理維護，位於小坪數套房或移動式可供電的車廂內。	DMT 、IDC 、Wi-Fi 、GoIP 閘道器
轉介型	將話務從 A 處轉移至 B 處，常為小套房。	拉線、Wi-Fi
新型態	以無線分享器來共享寬頻，化整為零朝 SOHO 族邁進，組織透過雲端整合，共享資源，形成無紙化作業，成員可分散各地，藉以分散風險。	Wi-Fi、4G
水房	水房網路的頻寬不需要很大，常以人頭電話卡使用行動頻寬連結網路，成員亦不多，約 4-6 人或者更少。	Wi-Fi、4G

DMT 數位式移動節費設備犯罪手法流程圖



因為國際電話費用較高，為了降低成本，境外電信詐騙集團鮮少直接以國際電話撥打給台灣之被害者，多半透過國際節費電話（購買電話節費卡），或申請國內二類電信業者（主要係特殊二類 ISR業者）之網路電話（VoIP），透過國內二類電信業者轉發給被害人

查緝詐欺集團之流程圖



電信詐欺機房之研判

- 靜態資料分析：例如租賃契約、房租付款、租賃聯絡方式、耗能指標、門禁管控、網路裝設、房屋坪數與房間格局等。
- 外部特徵觀察：例如建物位置、出入情形、後勤補給、多角度裝設多支監視器與生活起居等。
- 扣案物證解析：電信詐欺機房最重要的物證莫過於閘道器及 SIP Phone，透過閘道器及 SIP Phone 等物證的解析，我們可以進一步溯源找到 VOS 的 IP 位址，並反求其連線狀況。

電信詐欺機房之鎖定

- 靜態資料蒐集：情資布建、背景資料清查、通訊監察與 IP 查址等。
- 動態行動蒐證：配合現譯跟監與 M 化定位系統，來鎖定機房的位置。

情資布建

- 案件本身：透過人流、電信流與金融流的監控追查，常會產生案外案，藉此可擴展其它案源。
- 犯罪者：將系統商、電腦手、車手、收簿手與機手等實際從事詐騙者化敵為友，藉由拉出打入的方式，將其吸收為內線的線民。
- 社區友善通報網：電信詐欺機房常隱藏於社區大樓、透天厝或別墅等建物，輔導社區居民針對異常出入分子多加提防及通報。
- 第三方警政：與保全業的大樓管理員保持良好的通報關係，向便利超商店員宣導提款車手的特徵，由金融機構針對提領大額款項的民眾，執行關懷提問。
- 建立高風險名冊：老手於掌握資金及技術後即自立門戶，亦不乏屢遭查獲又再次回流者，利用大數據分析及情資蒐集，建立資料庫作為偵查之用。

背景資料清查

- 刑案資料：可分析犯罪者的作案手法及前案的共犯結構。

- 通信紀錄：可分析犯罪者的日常作息、出入場所及交往對象。
- 清查犯罪者名下所申請使用的電信服務：如行動電話、市內電話、網路服務、第四台服務等可查知其實際的住居所。
- 艙單比對：可清查犯罪者同行共犯的身分。
- 車輛違規紀錄：可查知犯罪者實際使用的交通工具。
- 車行紀錄：可以提供犯罪者大概的動態。

通訊監察

- 通訊監察是取得犯罪證據的利器，不過隨著通訊科技的進步，犯罪者利用通訊軟體如 Line、Facetime、Wechat、Skype、Google Hangouts 與 Facebook Messenger 等做為通訊工具時，由於通訊監察技術上的瓶頸，監聽幾乎已無實質上的功效，現譯功能也只能取得犯罪者即時的基地台位置，瞭解其大概的行蹤。

IP 查址

- 詐騙話務的電信流，移轉犯罪所得之網路交易的金融流，以及針對犯嫌所執行的通訊監察，都是取得與犯罪有關之 IP 位址的主要來源。
- 犯罪者使用的通訊軟體(Skype、Line、Wechat、Facetime)、社群帳號(Facebook、Google)、遊戲帳號、網路購物以及透過公開來源情報(Open Source Intelligence)所蒐集的犯罪者社群媒體之帳號，都可得到具有參考價值的 IP 位址。

現譯跟監

- 電信詐欺機房的成員平時集中式軍事化管理，大部分成員無法自由進出，且無法對外通訊，人員進駐與遷移亦有專車接送。成員外出採買、叫便當飲料外送以及成員進駐或退出時是跟監的最好時機。
- 針對特定對象所使用的電信編碼，執行即時監聽及快報，常配合偵查人員作現場的行動蒐證，即跟蹤與監視。

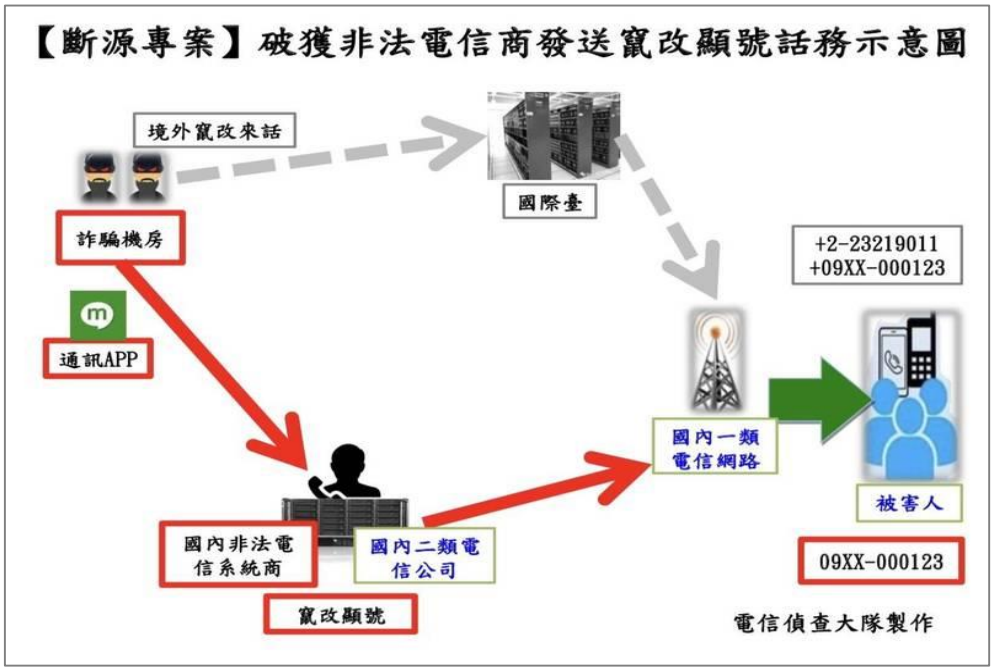
M 化定位系統

- M 化車為裝載定位設備的車輛，其運作原理為模仿基地台發射無線電波，找到目標手機後，對該手機的無線電波進行定位。
- M 化定位系統能協助偵查人員循著無線電波的來源，找到電信詐欺機房的確實位置。

詐騙新手法！國外手機門號變國內市話

- 詐騙手法層出不窮，刑事局和台中警局，聯合破獲一起「非法電信商竄改號碼」的案件。台中某間電信商和詐騙集團合作，研發手機應用程式，配合網路伺服主機，竄改來電號碼，讓被害人以為打來的是公家機關，因此受騙上當，至少有上千位受害者。
- 研發這款應用程式的林姓主嫌，在台中設立電信公司，和詐騙集團合作，做出這款程式，另外還有會計、工程師以及行政等共犯。8 個月間，透過程式，搭配伺服主機竄改來電號碼，再向詐騙集團抽取每通 0.1 到 1 元的電信費，不法獲利將近 1 億元。
- 詐團多在境外設話務機房，以境外電信服務竄改來電顯示，進線國內電信公司致電被害

人，來電顯示前端會帶「+」碼；若透過林的設備進入國內電信公司發話，則不會顯示「+」，被害人不易辨識。



二類電信業者與詐團合作販售門號

- 桃園地檢署從去年陸續偵辦謝姓等詐騙集團成員以「數位式移動設備」(DMT)，類似移動式機房功能當作跳板，用以逃避檢警鎖定詐團實際發話位置並得將國外的詐騙門號偽裝成國內撥打的行動門號，檢方起訴謝嫌等共 7 人並求處重刑。
- 檢方同時溯源追查機房內查獲的千餘張電信門號卡來源，赫然發現謝嫌等詐團成員與桃園市「海峽電信股份有限公司」的邱姓負責人共謀，由詐騙集團成員設立空殼公司後，以法人名義陸續向海峽電信大量申辦門號，邱某並以「隨時要、隨時給」的方式，在收到詐騙集團通知後，立即委由快遞業者交付電信門號卡。
- 清查後發現，某詐騙集團以單一法人名義向海峽電信申辦的門號數量就達 2372 個，且大部分均供作實施詐騙及代收驗證碼使用。檢方於是對位於桃園市桃園區的海峽電信進行搜索，查獲許多該公司與詐騙集團勾串事證，並向法院聲押邱某獲准。
- 桃檢表示，檢察官偵辦二類電信公司疑涉詐欺案，發現涉案公司有未落實 KYC（實名認證）審核而大量發送企業卡、人頭門號給詐欺集團成員，使詐欺集團藉此逃避查緝、遂行詐欺、洗錢等犯行，並大量耗費檢警偵查能量。

二類電信成詐騙溫床 NCC 不排除開罰

- 二類電信成為詐騙溫床，桃園地檢署日前偵破海峽電信跟詐騙集團共謀販售門號，NCC 表示，除要求「源頭」中華電信收回海峽電信尚未使用門號，也不再核發新門號，現有門號要落實「客戶風險管理機制」，在釐清相關事證後，不排除開罰中華電信。
- NCC 表示，事發後已要求中華電信啟動三大措施：

1. 立即全數收回海峽電信尚未使用門號，並不再核發新門號。
2. 針對還在使用的門號再次啟動行政檢查。
3. 若經桃園地檢署認定並通知門號涉及詐騙行為，應依規定立即停斷話。

- 在接獲桃檢函文後，立即兩度行政檢查，要求海峽電信提供相關資料，若有違法事證，將依《電信法》可開罰 20 萬以上、100 萬元以下罰鍰，並通知限期改善，屆期未改善者，就能廢止海峽電信的經營許可。強調會對一類電信、二類電信業者進行相關查核，呼籲電信業者不要心存僥倖，若發現有未落實 KYC 等相關違法情形，就會依法開罰。

二類電信執照到期後仍開通門號 NCC 追究中華電信涉詐責任

- 二類電信業者「海峽電信」數千門電信門號，涉及電信詐騙案，國家通訊傳播委員會（NCC）七月對該公司裁罰 30 萬元，但由於《第二類電信事業管理規則》裁罰金額較低，NCC 在高層關切下，針對海峽電信 11 家企業客戶門號進行清查，發現「瑞O數位行銷」等七家公司之門號核配，未落實「用戶資料查核」，因此以「一行為一罰」原則，對海峽電信重罰 445 萬元，由於「海峽電信」二類電信執照，在失效後，仍透過中華電信 API 介面軟體，開通核配門號，NCC 委員會今天做成決議，將針對中華電信是否有相關行政疏失部分進行調查。
- 檢警這一波破獲的詐騙案，發現詐騙集團曾向亞太和台灣之星申辦大量門號，轉售給中國犯罪集團，最近更以一個門號 300 到 500 元的價格，向二類電信業者「海峽電信」，一口氣購買 4、5000 個門號。由於「海峽電信」在上次 NCC 裁罰時，檢調單位提供給 NCC 的涉詐門號僅不到千門，NCC 當時對該公司裁罰 30 萬元，已經被外界質疑裁罰過輕，現在又一口氣冒出這麼多涉詐門號，讓 NCC 不得不對「海峽電信」進行第二波裁罰，並通知限期改善，屆期仍未改善者，廢止其許可。

詐騙機房刑事責任

詐騙集團多半涉及組織犯罪防制條例、加重詐欺及洗錢防制法等罪名，以下詳細說明：

- 組織犯罪防制條例：詐騙集團首腦為發起、主持、操縱或指揮犯罪組織者，處 3 年以上 10 年以下有期徒刑；而電腦手、車手及水手為該組織之參與者，處 6 月以上 5 年以下有期徒刑。
- 刑法加重詐欺：無論首腦或旗下成員，彼此相互分工，共同詐騙被害民眾造成財產損失，即構成刑法第 339-4 條加重詐欺之共同正犯，處 1 年以上 7 年以下有期徒刑。
- 洗錢防制法：車手及水手提領詐騙所得，並將贓款回流到集團，掩飾或隱匿特定犯罪所得之本質、來源、去向則涉及洗錢防制法第 14 條，處 7 年以下有期徒刑。
- 詐騙集團機房可能涉及組織犯罪防制條例、刑法加重詐欺及洗錢防制法，但詐欺案件是否有獲判無罪機會須視個案狀況酌定，詐騙機房爭取無罪最重要的爭點往往在於主觀上有無詐欺犯罪故意、是否遭騙或遭強迫等，而爭取較輕刑期則須與被害人和解賠償、認罪、協助檢警釐清案情、節省司法資源甚至轉為汙點證人等。

電信監理問題

- 主管數位通訊的 NCC，因未管制電信業者浮濫出售門號，造成人頭預付卡門號、第二類電信所申辦的大量人頭企業門號橫行，讓詐騙集團能輕易通過手機門號驗證，經由電子支付等新興數位金融服務從事犯罪。
- 以漫遊門號為例，每一張濫發的黑莓卡、預付卡，都是追查的「斷點」，而在 NCC 稽查人員前往二類電信公司檢查時，根本無法見到真正犯罪用之器材；兼以其為行政稽查，

無實質調查權力，根本無法預防。

- 祇要這些非法二類電信業者被剿滅，詐騙集團對外通訊以及生財之犯罪工具旋即中斷，因此，有效打擊剷除非法之二類電信業者，才是徹底根除、有效降低電信詐騙之最佳良策。

電信法

第 17 條

經營第二類電信事業，應向電信總局申請許可，經依法辦理公司或商業登記後，發給許可執照，始得營業。

第二類電信事業營業項目、技術規範與審驗項目、許可之方式、條件與程序、許可執照有效期間、營運之監督與管理及其他應遵行事項之管理規則，由交通部訂定之。

第 64 條

違反第十七條第一項規定經營第二類電信事業者，處新臺幣二十萬元以上一百萬元以下罰鍰，並得沒入其電信器材。

違反交通部依第十七條第二項所定管理規則者，處新臺幣二十萬元以上一百萬元以下罰鍰，並通知限期改善，屆期仍未改善者，廢止其許可。

電信管理法

第 37 條

申請設置使用電信資源之公眾電信網路者應檢具申請書、營運計畫及網路設置計畫，向主管機關申請核准。經主管機關核准，始得營運及設置；其電信網路增設或變更者，亦同。

第 69 條

申請使用前條第三項規定之電信號碼者，應檢具申請書、使用規劃書及相關文件，向主管機關申請核配。

電信號碼之分類與編訂、申請者資格、條件、程序、文件、規劃書之記載事項、使用管理、限制、調整、收回及其他應遵行事項之辦法，由主管機關定之。

第二類電信事業管理規則

第 21 條

經營公司內部網路通信服務者，應向第一類電信事業租用專線，供作用戶與網路間及網路內部節點間連接之用，並不得有下列行為：

一、為其用戶提供非公司內部間之通信服務。

二、為其用戶提供受信端再轉接之通信服務。

電信號碼核配及管理辦法

第 26 條

電信事業分配用戶使用電信號碼前，應核對及登錄用戶資料。

前項規定，由國家通訊傳播委員會依相關規定辦理。

電信事業受理申辦電信服務風險管理機制指引

- 為落實 KYC，電信事業應設置獨立於業務部及通路部門外之稽核部門，並自行訂定定期及不定期稽核抽測計畫，至少每月辦理抽測，尤其針對高風險用戶應加強稽核，並定期將稽核結果及改正情形，向主管機關提出報告，知悉有不法使用情事，應立即向有關機關通報。
- 企業客戶應提出切結書，保證其使用電信門號或服務不得有違反法規情事，如經有關機關通知有違反切結書之情事，電信事業對其所申請之電信門號或服務將全部予以停、斷話。
- 曾受各有關機關停、斷話通知之自然人，向同一電信事業再度申請門號時，限制該自然人於 1 年內僅能申請 1 門電信門號。
- 倘該等用戶經有關機關通報停、斷話或服務時，得予以扣繳保證金及收取違反規定之違約金。

電信事業用戶號碼使用管理辦法草案

第 3 條

獲核配用戶號碼之電信事業分配用戶使用用戶號碼前，應核對及登錄用戶資料。

第 4 條

獲核配用戶號碼之電信事業，應要求企業客戶保證其使用用戶號碼或服務不得有違反法規情事。

第 5 條

獲核配用戶號碼之電信事業核對用戶資料，應確認用戶或代理人與其所持證件相符。獲核配用戶號碼之電信事業非經主管機關同意，不得在境外開通用戶號碼之使用權限。

第 13 條

有下列情形之一者，獲核配用戶號碼之電信事業應不分配用戶號碼：

四、企業客戶依第四條第一款規定檢附之使用用途說明有違反法令強 制或禁止規定之虞。

第 14 條

用戶轉讓用戶號碼予他人，應經獲核配用戶號碼之電信事業同意。

第 18 條

獲核配用戶號碼之電信事業，用戶號碼提供電信服務有下列情形之一者，應暫停或終止用戶使用用戶號碼：

一、知悉用戶有第 13 條各款情形。

二、知悉用戶違反第 14 條規定。

強化查緝能量

- 提升偵查科技能力：電信詐欺犯罪偵查為一跨領域的技術，一為犯罪偵查，另一為電信科技，通常犯罪偵查人員比較欠缺的是電信科技的知識，而電信科技知識的獲得有賴良好的電信理論基礎，並非一蹴可幾，必須經過紮實的學習與訓練。
- 盡速通過科技偵查法：警方過去曾利用 M 化定位系統破獲電信詐欺機房，起訴犯嫌，但法院認為 M 化車籍訊號探知位置資訊，干預人身自由基本權，使用上無法源依據，排除

M 化車直接取得的證據力。對於通訊監察，如今人們幾乎都使用加密的網路電話，傳統的通訊監察似乎已無用武之地，其解決辦法為在訊息被加密前或解密後，取得未經加密的資訊。以上 M 化定位系統與通訊監察面臨的困境，有賴科技偵查法的盡速通過。

- 另外 NCC 應要求電信業者核照加強 KYC 審核並強化監理，以避免大量被害人受害並耗費檢警偵查能量，以追求前端 NCC 謹慎把關而後端司法積極查緝的雙贏局面。

參考資料：

1. 詹明華、王嘉華(2021)，電信詐欺機房之分析，中央警察大學警學叢刊，第 52 卷第 1 期，第 21～40 頁
2. 張文源(2016)，臺灣非法二類電信對電信詐欺犯罪之影響，國立臺北大學犯罪學研究所碩士論文
3. 盧俊光、廖有祿(2006)，新興詐欺犯罪型態、模式及中介物之分析，2006 年刑事偵查學術研討會，中央警察大學，頁 13-32
4. 電信法第 17 條、第 64 條
5. 電信管理法第 37 條、第 69 條
6. 第二類電信事業管理規則第 21 條
7. 電信號碼核配及管理辦法第 26 條
8. 電信事業受理申辦電信服務風險管理機制指引
9. 電信事業用戶號碼使用管理辦法草案第 3 條、第 4 條、第 5 條、第 13 條、第 14 條、第 18 條

評論人：中央警察大學行政警察學系 朱金池兼任教授

壹、引言人鄭善印理事長的引言亮點

一、依據 ETTODAY 新聞雲層製作的「台灣詐騙手法演變圖」，概述各種詐欺手法及法制規範之現況。

二、明確指出現行防制三種工具詐欺法規的缺漏：包括人頭門號部分、網際網路廣告部分、人頭帳戶部分等。

三、引介日本的《手機非法使用防止法》，提供我國 NCC 訂定《電信事業用戶號碼使用管理辦法草案》的重要參考。

四、建議「打詐專法應以預防與制止電信詐騙為目的，而與現行打詐五法的實體處罰法區隔，僅對違反者處以罰鍰而不應有刑罰名目的處罰，較能強化警察機關從事預防詐欺犯罪的量能。

貳、引言人廖有祿教授的引言亮點

一、在通訊與網路匯流下，電信詐欺機房是跨境電信詐欺犯罪成功的關鍵。

二、二類電信被利用作為詐欺工具，最主要之原因有二：「架設容易，不需要經過公眾之電信網路，因此不易遭到司法機關之監控」、「須花費之成本較低」。

三、比較各種詐欺機房的特徵與介接之方式。

四、建議第三方警政作法：與保全業的大樓管理員保持良好的通報關係，向便利超商店員宣導提款車手的特徵，由金融機構針對提領大額款項的民眾，執行關懷提問等。

五、指出主管數位通訊的 NCC，因未管制電信業者浮濫出售門號，造成人頭預付卡門號、第二類電信所申辦的大量人頭企業門號橫行，讓詐騙集團能輕易通過手機門號驗證，經由電子支付等新興數位金融服務從事犯罪，建議 NCC 應要求電信業者核照加強 KYC 審核並強化監理。

六、建議提升偵查機關科技偵查的能力。

七、 建議速通過科技偵查法，解決 M 化定位系統與通訊監察面臨的困境。

參、打擊電信詐騙的策略與具體作法建議

一、公共治理的策略

(一)策略目標：由政府主導，結合企業、非營利組織及社會大眾等，構成治理電信詐騙的網絡，有效預防及打擊電信詐騙犯罪。

(二)具體作法建議

1、由行政院層級長官定期邀集內政、法務、中央目的事業主管機關(包括電信、網際網路、金融)，以及業者等檢討與策進預防及打擊電信詐騙犯罪之具體作法。此可參照美國紐約市警察局 CompStat（資訊統計管理系統）的作法，有效預防犯罪。

2、整合刑事司法系統預防及打擊電信詐騙犯罪的機制，建議訂定以預防與制止電信詐騙為目的的「打詐專法」，對違反者處以罰鍰，而與現行打詐五法的實體處罰法區隔，較能強化警察機關從事預防詐欺犯罪的量能。

二、第三造警政的策略

(一)策略目標：課責電信業者、數位中介服務提供者、網際網路服務供應商（internet Service Provider, 簡稱 ISP）等有預防電信詐騙犯罪義務的業者，負起從源頭預防的義務，減輕下游偵查部門的負擔，並規範業者在案發後有配合調查的義務。

(二)具體作法建議

1、建議NCC應要求電信業者核照加強KYC審核，並強化課責業者的監理與處罰機制。

2、建議透過外交途徑及國際相關團體的合作機制，要求國外的相關業者協助我國偵查機關從事境外電電信詐騙犯罪的預防與偵查作為。

三、科技偵查的策略

(一)策略目標：精進科技偵查的量能，並立法授權警察與偵查機關從事科技偵查的權限。

(二)具體作法建議

1、儘速通過科技偵查法，建立層級式的審核機制，授權警察機關主管、檢察官及法官審核從事科技偵查的權限，提昇偵查機關的科技偵查量能，解決 M 化定位系統與通訊監察面臨的困境。

2、推動「智慧警政」(Smart Policing)，精進警察科技偵查的設備與人才培訓。