「電信網路詐欺集團犯罪之跨部門防制經驗研究」

研究成果報告

研究主持人：國立中正大學犯罪防制學系 許華孚 教授
共同主持人：國立中正大學犯罪防制學系 馬躍中 教授
東吳大學法學院暨法律學系 蕭宏宜 教授
研究員：國立中正大學犯罪防制學系 黃光甫 博士
國立中正大學犯罪防制學系 陳勁州 博士
國立中正大學犯罪防制學系 施宛妤 碩士

法務部司法官學院 委託研究

中華民國一一四年十二月

摘要

隨著通訊技術與數位支付普及，電信與網路詐欺案件在我國呈現快速上升趨勢，不僅造成大量民眾財產損失，也暴露出跨部會、跨域治理與國際合作的制度性不足。政府自 2022 年推動「新世代打擊詐欺策略」以來，陸續透過法制補強與策略升級，試圖在識詐、堵詐、阻詐、懲詐與防詐等面向建構整體體系，但實務成效與執行障礙仍待檢驗。

本研究旨在比較美國、歐盟、日本、南韓防制經驗；檢視我國自綱領 1.0 到 2.0 之政策演進與具體作為；並透過對檢警、檢察官、法官等實務者之深度訪談，彙整實務困境與提出短中長期政策建議，期望為政策設計與執行提供具體可行之參考。本研究採系統性文獻與政策文件分析，含我國相關法規、綱領與國外政策文件；半結構式深度訪談，訪談對象為檢警、檢察官、法官、金融及產業主管實務者，進行質性主題分析，並由比較研究歸納出可借鏡之要點與政策建議。

研究發現我國從打詐綱領在法源與策略面快速擴充，已涵蓋電信管制、金融 AML、科技偵查與被害保護等多元面向。實務上仍有關鍵瓶頸：法條適用與程序競合之模糊、電子證據與業者配合的時效與法律障礙、銀行與第三方支付即時阻斷標準未明、偵查與司法量能不足，以及跨境追查與國際互助回應遲緩。來自美、歐、日、韓之比較顯示：技術驗證、金融端即時阻斷與專法授權、以及長期社會化宣導/公私協作，均為有效降低被害與加強追繳的關鍵要素。

研究結論認為政策已具方向與工具，但若要由策略轉為可量化成效，必須同步補強「程序化」「資料交換平台」「業者配合與免責保障」、以及「偵查與司法專業化」；並推動國際快速司法互助與長期技術與人才投資。基於此，提出短期的建立緊急通報 SOP、被害者快速救助窗口、中期的資料交換平台、法制明確化、專責偵辦與專庭、長期的國家防詐中心、國際快速互助、人才與科技研發之具體政策路徑，以期在黃金時間內有效阻斷金流、提高追繳成效並提升被害者保護。

Abstract

With the proliferation of communication technologies and digital payments, telecommunication and online fraud cases in Taiwan have surged rapidly. These crimes have not only caused substantial financial losses among the public but also revealed institutional deficiencies in inter-agency coordination, cross-sectoral governance, and international cooperation. Since the launch of the "New Generation Anti-Fraud Strategy" in 2022, the government has sought to strengthen the legal framework and upgrade strategic measures, aiming to construct a comprehensive system across multiple dimensions—awareness, interception, prevention, punishment, and protection. Nevertheless, the actual effectiveness and implementation barriers remain to be critically assessed.

This study seeks to: (1) compare anti-fraud experiences in the United States, the European Union, Japan, and South Korea; (2) examine Taiwan's policy evolution and concrete measures from Guideline 1.0 to 2.0; and (3) analyze practical challenges through in-depth interviews with prosecutors, judges, police officers, and industry stakeholders, with the aim of providing short-, medium-, and long-term policy recommendations. Methodologically, the study adopts systematic literature and policy document analysis—including Taiwan's legal frameworks and strategic guidelines as well as foreign policy reports—combined with semi-structured in-depth interviews with practitioners from the judiciary, law enforcement, financial institutions, and related industries. Data were analyzed through qualitative thematic analysis, and comparative research was employed to identify transferable insights and policy implications.

Findings reveal that Taiwan's anti-fraud framework has rapidly expanded in both legal and strategic dimensions, encompassing telecommunications regulation, financial anti-money laundering (AML), technological investigation, and victim protection. However, critical bottlenecks persist in practice: ambiguities in legal applicability and procedural overlap, delays and legal barriers in electronic evidence collection and industry cooperation, unclear standards for real-time blocking by banks and third-party payment providers, insufficient investigative and judicial capacity, and slow responses in cross-border investigations and international cooperation. Comparative analysis of the U.S., EU, Japan, and South Korea demonstrates that effective approaches include advanced technical verification mechanisms, financial-sector real-

time blocking supported by dedicated legislation, and long-term social campaigns with strong public–private collaboration.

This study concludes that while Taiwan's policies are directionally sound and equipped with relevant tools, translating strategies into measurable outcomes requires simultaneous enhancement of procedural standardization, data-sharing platforms, industry compliance with liability safeguards, and specialization of investigative and judicial capacities. Moreover, the promotion of rapid international judicial assistance and sustained investment in technology and human capital is essential. Accordingly, the study proposes concrete policy pathways and KPIs: in the short term, establishing emergency reporting SOPs and victim assistance hotlines; in the medium term, developing cross-agency data exchange platforms, legal clarification, dedicated investigative units, and specialized courts; and in the long term, creating a National Anti-Fraud Center, institutionalizing rapid international cooperation, and advancing talent cultivation and technological innovation. Collectively, these measures are expected to improve the timely disruption of illicit financial flows, strengthen asset recovery, and enhance victim protection.

目錄

表目錄

圖目錄

第一章 研究主旨

詐欺嚴重侵害人民的財產法益，我國電信網路詐欺犯罪於近年呈現遽增現象，以警政統計為例，我國近年來詐欺犯罪的案件數量從 2012 年的 20,421 件攀升到 2024 年的 122,805 件，整體案件數量增加了六倍之多；詐欺犯罪嫌疑犯急遽的增加，從 2012 年的 17,561 人至 2024 年 58,666 人，整體犯罪嫌疑犯也增加了三倍之多；接著看詐欺犯罪被害人，從 2012 年的 27,308 人攀升到 2024 年的 132,445 人，隨著詐欺犯罪案件數量的增加，被害人也增加超過六倍，不管是案件數、被害人與嫌疑人數皆創下近年來的新高點。從圖 1 來看，所有的資料都突破以往高峰，且上升趨勢並非緩步上升，而是急遽拉高。若是往回看過去統計紀錄，詐欺犯罪嫌疑人從 2002 年的 4,707 人急遽增加至 2009 年的 31,417 人，但隨後降低至 2013 年的 14,548 人，卻在 2024 年達到 58,666 人，顯然我國在打擊詐欺犯罪上仍有相當大的進步空間，進而應該探討我國在打擊詐欺犯罪政策上實施手段是否有待改進，更顯著來講似乎刑法威懾效應無法遏制詐欺犯罪的增加。

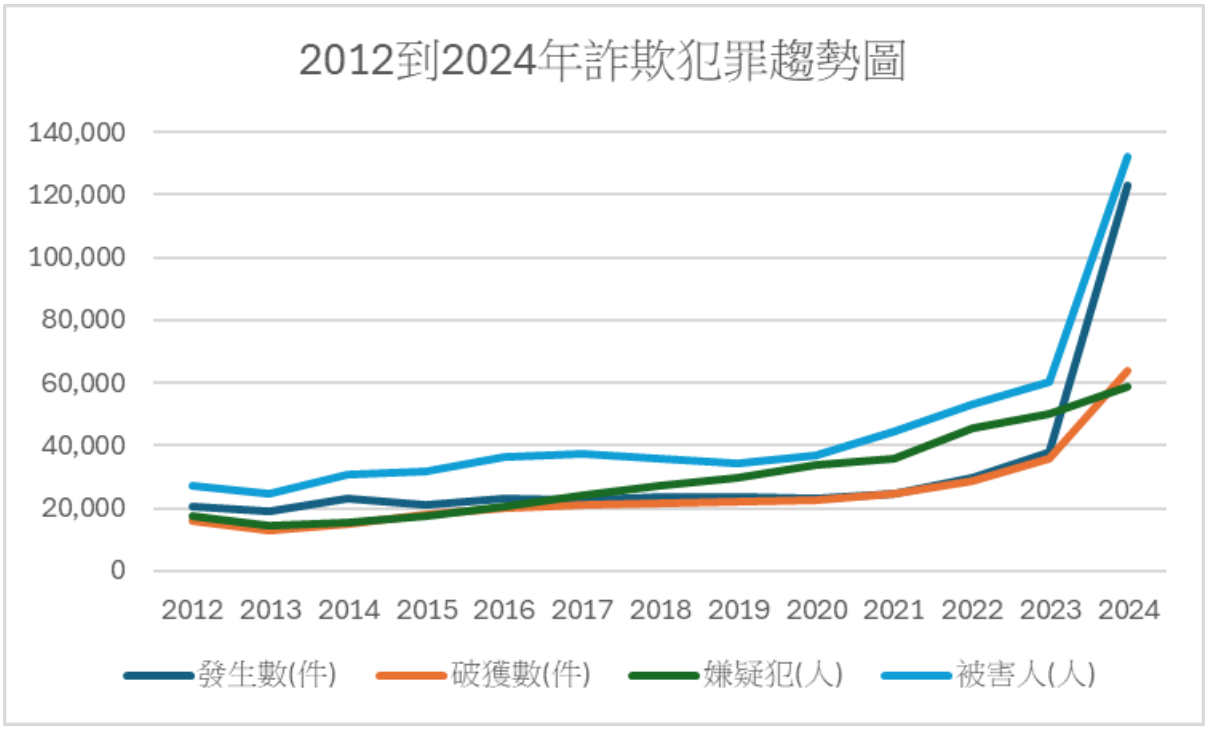


圖 1 2012 到 2024 年詐欺犯罪趨勢圖

資料來源：刑事警察局統計，本研究整理

電信詐欺案件量與犯罪者的向上趨勢，除了龐大的詐欺犯罪利益外，對國家社會所造成的金融、治安、財產安全產生了極大的威脅。我國因應電信詐欺手段的不斷演進，透過各種對策來抗制電信網路詐欺的蔓延。從 2022 年核定「新世代打擊詐欺策略行動綱領」開始，我國展現對抗電信網路詐欺的決心，整合國家各部會進行抗制詐欺，分別由內政部、國家通訊傳播委員會、金融監督管理委員會及法務部主政，教育部協辦「識詐」宣導作業。然而經過將近一年的時間，各部會協力達成許多重點工作目標，不過在電信網路詐欺犯罪上仍有許多困境等待突破。因此在 2023 年通過「新世代打擊詐欺策略行動綱領 1.5 版」，增修「打詐五法」（包括《中華民國刑法》、《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》修正草案），防堵詐欺從源頭著手，加強後端查緝。但推陳出新的詐騙犯罪型態與手法，使得抗制電信網路詐欺的政策難以落實，因此 2024 年 7 月通過「打詐四法」（詐欺犯罪危害防制條例、科技偵查及保障法、通訊保障及監察法、洗錢防制法），用來作為對抗電信網路詐欺犯罪不斷進化的政策。行政院再於 2024 年 11 月 28 日通過「新世代打擊詐欺策略行動綱領 2.0 版」，除原有「識詐、堵詐、阻詐、懲詐」4 大面向架構外，新增「防詐」，強化數位經濟產業治理，並以「運用 AI 防制、深化跨境合作、監管防詐產業、加強被害保護」為規劃亮點，希望達成「強化防詐意識、減少發生數、降低財損數」3 大目標，為國人打造更安全的生活環境。然而打詐政策的施行仍有待未來打擊成效的驗證，若能夠借鏡國外成功的電信網路詐欺犯罪成功防制經驗，對比我國打詐政策的具體措施，從政策制度、具體施行，單位整合、法律抗制、查緝專業等面向加以檢視並提出改進建議，將能有效的撲滅不斷拓展的電信網路詐欺犯罪氣焰。

本研究概以「我國與國際間跨部門的成功防制電信網路詐欺集團犯罪之經驗」議題為出發，渠引「重要先進國家抗制電信詐欺犯罪政策發展及實務經驗」為前題，輔以「我國電信詐欺犯罪防制問題與研究對策」的主軸論述，綜整提出「先進國家與我國電信詐欺抗制政策與實務的比較」及其提出「我國電信詐欺犯罪部會整合與國際合作的政策建

議、具體作為」等具體建議為研究結論。

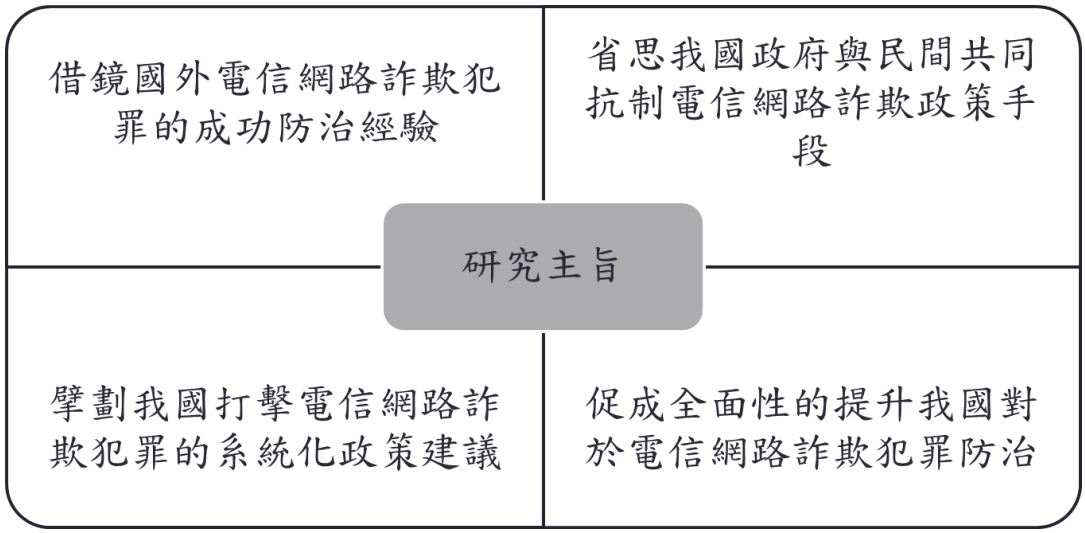


圖 2 研究主旨概要示意

因此本研究的目的有三：

一、釐清國外電信網路詐欺集團犯罪的問題與特性，與爬梳是類國家在公部門與國際、民間單位，於制度、政策及實務面向，如何相互助益與發展成功的詐欺犯罪防制經驗。

二、盤點我國電信網路詐欺集團犯罪特性、防制策略、執行實務、運作脈絡等，和前揭國家間的異同，與足以取法之處。

三、提出我國電信網路詐欺集團犯罪之跨部門、國際合作防制之政策、制度、執行面向，在法制化（含詐欺犯罪危害防制條例）、科學化、專業化、系統化等精進建議。

第二章 文獻探究

第一節 電信詐欺犯罪的背景與網絡分析

我們日常生活中使用最多的數位裝置是手機。它廣泛應用於通訊、搜尋、購物、支付、驗證身份和投資等日常活動。有些人沒有個人電腦，但現在幾乎每個人都有手機。詐騙者瞄準手機是因為它們是最廣泛、使用最多的設備。犯罪者透過詐騙手段來竊取我們的金錢、資訊和個人資料遂行犯罪。為彰顯研究議題之重要性，爰將我國對於電信網路詐欺犯罪「全面性抗制政策與作為」之原由及其背景因素，分列「電信網路詐欺的社會背景脈絡」、「我國電信網路犯罪現況與犯罪組織架構與過程」、「我國電信網路詐欺犯罪防制實務及政策面臨的困境」等三個部分詳予說明於後。

一、 電信網路詐欺的社會背景脈絡

資訊時代的來臨主宰了社會變遷的腳步，當前知識與資訊，對於科技進步有著極大的貢獻，電腦與網路已經是當前社會不可或缺的重要元素。在二十一世紀的當代社會，網路成為大家共同的話題，也帶來了全球化、消費與數位世界的關注，網路詐欺也就在這樣的社會變遷下蓬勃發展，本節從幾個面向來說明網路詐欺與被害的社會脈絡(鄭祖邦等，2015)。

(一)全球化

1980 年代全球化議題成為主流，然全球化卻猶如雙面刃，帶來了便利卻也成就了負面效應，儼然成了各國複雜且難以掌控的議題。全球化首先帶動且活絡商品和服務市場的市場經濟，各國的市場透過日新月異的科技技術，進而將全球市場融合成單一模式。然而電腦網際網絡跟通訊技術的革新、交通運輸普及，更重要的是電子消費金融的便利與即時性，反而助長犯罪活動擴展到世界各角落。各國因全球化產生了鏈結，低發展國家充斥著高失業率、高犯罪率的情形；高度發展的國家，則因社會結構的轉變、貧富差

距擴大等剝奪感受的影響，貧窮使得犯罪不斷發生(許華孚、吳宗穎、劉育偉，2018)。

全球化以市場與經濟為圭臬，通過資本、資訊和市場來衝擊傳統國家主義思維，市場與經濟的整合下，使得多數國家都能夠在過程中享受長遠的利益，各種事物存有共享的機制。全球化是各國相互依存的社會過程，因為地理因素限制不再，使得行為模式、價值觀、先進科技以及各種產品，透過不同的工具向世界各地擴散。然而轉換過程中，產生跨越空間、人際互動的一系列過程建構出流動空間(Space of flow)的概念，現今的資訊、電信、網路傳輸的科技，和流動空間交互纏繞，形成了一種「時空的壓縮」(Time-space Compression)，言簡扼要來說，交通工具、運輸航運和通訊科技的進步，縮短了原本跨越空間所耗的時間，跨過了空間所造成的阻礙。時空壓縮的全球化趨勢，讓經濟、社會、文化及政治上，跨越疆界發展依存關係，犯罪活動在這場全球化浪潮下沒有缺席，擴散的快且廣(Albrow, 1996; Harvey, 1989; Manuel Castells,1997; 陳志賢，2007)。

Giddens(1990)將全球化解釋為時空解離（time-space distanciation）下的結果。是世界各地的社會關係經過科技進步後而連結，緊密連結下進而相互增強彼此的連結效果，導致在地事件被遠在他鄉的事件所深刻影響。因全球化而形成的網絡社會，使得原本受困於國界內的金融、犯罪、消費開始交流，當中犯罪成為最不受控制的洪水猛獸，即便政府的枷鎖不斷加嚴加深，卻肆無忌憚地流竄於世界各地。尤以虛擬貨幣的流通，跳脫以往國家貨幣的概念，「金融秩序」在虛擬貨幣面前，似乎成為其笑柄，尤以後 COVID-19 時代，擴散的網路依賴現象，我們深刻的瞭解到，犯罪活動將因為全球化持續並且擴大。最明顯的例子就是第三方支付與貨幣都是全球化趨勢下所發展出的多元交易模式。像是全球金融機構、電信網絡等皆透過專業認證機構，讓全球信息交流無國界。除了讓全球各地的個體能夠快速地接受到貨品、服務與訊息，卻也在同時間使得疾病、犯罪隨著全球化擴散到全球，產生了「全球化偏差」(deviant globalization)。

隨著全球市場與經濟的高強度競爭，隨即加速了個人、企業與國家之間壓力與緊張產生的關鍵因素，個人間的貧富差距擴大，產生相對剝奪感，社會結構的變化會連帶家庭結構不健全、家庭功能裂解、升學的教育制度、社群傳播與網路的重度依賴等，反成

為犯罪的溫床，升高犯罪活動的機會(Scott, 1976；蔡德輝、楊士隆，2019)。全球化帶來重度網路依賴的生活模式，跳脫出與傳統的階級、性別、種族因素，自成新的社會風格，一種嶄新的生活「框架網絡」騰空出世，挑戰傳統觀念與價值觀。現有的政策是否能夠有效的遏止全球化犯罪的擴散，成為目前各國打擊跨境犯罪的重點目標。

犯罪因為進步的交通以及便捷的通訊技術，透過便捷交通將人才以及犯罪技術跨越疆界並擴展，近年更因為網路有隱密性、快速流通性、金融即刻性等，讓跨境詐欺集團成為各國法律的漏網之魚，讓各國疲於奔命，無不絞盡腦汁極力防堵詐欺犯罪的發生，同時因為國際間司法管轄權爭議、我國特殊主權地位問題以及領土疆界的認定，讓跨境犯罪顯得更加棘手難以處理。

(二)消費

1950 年代後，從美國為主的已開發國家開啟了另一種社會變遷，從原本生產與工作為主的社會模式，轉而投入消費(consumption)的面向。以現今社會來說，消費是所有人生活中無法忽視的一種相當重要的社會活動，當中也帶動了相當大的社會變遷。工業革命的時代，生產與工作是當時的重要過程，在資本主義的經濟體不斷成長下，消費(consumption)逐漸取代了生產與工作的社會過程。消費和全球化緊密的連結，而網路讓消費的便利性更加活躍，即便再遠的距離，都無法阻擋消費力道的不斷強大。尤其是線上購物這類型的消費，更是幾乎主宰著各種社會變遷的關鍵角色。從演變史來看，信用卡是加速消費的首要工具，信用卡使得人們在各式購物中心與賣場、街邊商店與萌芽的網路購物，成為人們加速消費力道的重要工具。隨著網路的普及，購物不再侷限於實體消費，使得人們能夠不出門即可消費，更加大信用卡消費力道，同時衍伸出各種不同的付款方式，信用卡、線上支付、分期付款等，都是因應網路購物而蓬勃發展的消費型態。

然而網際網路早期只能透過電腦與筆電來與世界接軌，隨著電信通訊網絡與網際網路的結合，智慧型手機的橫空出世，讓消費拓展到各個社會層面，從文化、經濟、政治與生活，都透過電信網路來強大消費的力道。過去社會學家專注在生產、工作、工廠與

工人的研究，目前更致力於消費與社會的變遷關聯，像是消費所帶來的負債、犯罪、價值觀等，都與過往傳統社會出現極大的差異(鄭祖邦等，2015)。不過近年來因為 COVID-19 的全球肆虐下，後消費時代再度出現革新的機會，多數人因疫情因素而依賴網路來取得與世界的連結，長達兩年的的時間，讓所有人開始透過電信網路與社會連結，人際間的互動從面對面的模式轉而剩下影像與聲音，加上疫情間的消費急遽削減，對於消費型態改變，到後疫情時代的消費爆發，大量不斷的網路資訊從原本的電腦與筆電轉而從手機來取得，讓人們更加依賴電信網路，此舉使得犯罪機會從電信網路與消費之間油然而生，加上個人資料透過電信網路的非法取得與傳遞，也促發了電信網路詐欺犯罪的誘因。

消費是現代化社會的象徵，從過去的生產時代轉型到消費型時代，顯見消費已成為整個社會的主軸。消費初期是為了滿足個體需求，根據 Baudrillard 所提出的觀點來看，當滿足需求後消費應隨之停止，然而當基本生活需求透過消費滿足之後，便會出現新的需求，人類就在不斷的需求與消費之間出現了差異性，這些差異性不斷創造出新的需求，消費也就成為永不停止的動態過程。那麼在消費過程中，超消費(hyperconsumption)這種超出個人所能負擔的消費便出現在這個動態的過程中，也出現了超負債(hyperdebt)現象，超負債現象使得個體汲汲營營的追求個人財富的增長，進而出現投資的需求。投資是在確認可獲得一定擔保後，將資金存放、或投入於具有安全性的組織的一種承諾(李顯儀，2022)。而投資的方法相當多元，如定存儲蓄、外匯、股票、基金、期貨、ETF(Exchange Traded Fund)等，由於網際網路的進步，投資工具的多元，各種投資管道透過網際網路加以宣傳，也使得具有犯罪動機的人利用網際網路來傳播虛假訊息，藉投資機會來遂行電信網路犯罪。

(三)數位世界與總體金融

當代社會變遷源於科技的進步，從工業革命開始的機械、工具、技能等生產線模式，一直到現代化的電腦、網路、手機與通訊設備的普及，數位科技的生活逐漸主宰著這個社會生活的模式。透過數位科技，我們身處在數位世界當中，資訊的流通讓人際間的互

動模式有了極大的改變，網路社群媒體佔據了我們生活中的每個小細節，更值得注意的是人際間的互動跨越了時空，讓時間與空間不再成為互動與活動的阻礙。透過手機與網路的媒介，讓生活、學業、消費，甚至是犯罪，都是透過手機、網路與電腦設備來進行，由於資訊的普及與分享，讓犯罪更快速的擴散到全球。網路詐欺犯罪也是如此，過去傳統詐欺犯罪模式從面對面的犯罪行為，因為電話的普及而有了電信詐欺，直到現代，網路電話、社群媒體、消費購物、求職謀生等各種我們習以為常的日常活動，也成為犯罪的溫床。在全球化年代、消費主宰的活動，加上數位科技無所不在的情況之下，無形中讓電信網路犯罪悄悄的成為新興犯罪樣態，後面將透過各種官方資料來彰顯出電信網路詐欺的嚴重性。

消費與數位世界的互動下，與經濟極度相關的總體金融也開始出現變化，貨幣與金融與國家主權息息相關，過去的貨幣的轉換上須要到當地進行轉換，而改成多國使用的轉帳卡即可實踐貨幣流通。然在正式貨幣轉換制度下，地下貨幣經濟則成為另類的金融系統，直至現今電子貨幣的盛行，使得總體金融秩序出現變化，電子貨幣不但與傳統貨幣一樣，可實現面對面支付最終性，而且具備了高度的匿名性(anonymity)及可移轉性(transferability)。當中最重要的莫過於創新支付方式以及虛擬貨幣的出現，從傳統的面交支付手段，到磁條晶片卡片的支付手法，線上轉帳到目前的電子支付，使得金融制度面向多元，也顯示金融管理與控制的重要性，也正因貨幣制度的改變隨著科技進步也變化多端，政府若無法快速地跟上金融制度的變化，非法的犯罪行為就會透過這些地下貨幣經濟來加速犯罪的擴散。

二、 台灣電信網路詐欺的演進歷程

全球在 1980 年代末期開始，犯罪型態從傳統的個人犯罪手法，逐漸演變成組織集團化犯罪。為了讓犯罪利益擴大，集團組織除了遠端遙控犯罪集團外、更廣泛利用國際法的管轄權的缺陷來進行電信網路詐欺犯罪，由於「跨境電信詐欺罪」的「犯罪行為人」、「犯罪行為地」、「犯罪結果地」以及「犯罪被害人」的不同國度，致使檢警在查緝的

困難度增加。電信網路詐欺相對於一般傳統的犯罪類型，主要歸因於科技發展與普及化，連帶受惠犯罪者，讓犯罪高度科技化，不僅有利於犯罪過程的進行，同時也增加犯罪偵查的困難度。詐欺犯罪遍及全球，包括中國大陸、日韓或東南亞地區國家、甚至美國與歐盟有組織性的電信網路詐欺集團。由於詐欺組織集團分工專業化、金融便利、交通革新等，讓跨境犯罪跨越疆界之侷限，構築成各國之司法人員的一座嚴峻的高牆(許華孚、黃光甫，2020)。

臺灣電信網路詐欺犯罪盛行，電信網路詐欺手法及規模因時代與科技的進步而不斷演進，統整詐欺犯罪的過往相關研究，初步能夠區分為幾個階段：(汪子錫、葉毓蘭，2013；蔡田木，2010；許華孚、黃光甫，2020)

1. 1950 年至 1970 年，以個人或小型聚眾的犯罪手法進行，多以賭博、假冒身分、金光黨、宗教或巫術迷信、不實廣告、虛設商標或行號、倒會、票據為主。

2. 1971 年至 1990 年，開始加入些許工具與劇本，讓詐欺犯罪的金額越來越大，此時電腦科技與電信尚未純熟，手法仍以報明牌的六合彩賭博詐欺、偽造身分詐欺、刮刮樂詐欺、金光黨、互助會詐財、保險詐欺、虛設行號詐欺、巫術宗教詐欺、票據詐欺為主。

3. 電信詐欺盛行始於 1997 年的電信自由化政策的施行，2002 年的詐欺案件開始向上竄升，集團式運作開始大量出現，電信詐欺犯罪結合人頭電話與帳戶、金融電子轉匯等手法，讓詐欺得手贓款在極短的時間內將大筆金錢，快速地將得手的詐欺款項小額轉匯至大量的人頭帳戶，透過越來越便利的網路銀行服務來完成電信網路詐欺犯罪作業。

4. 2004 年到 2009 年，境外的竄改叫話手段開始出現，犯罪移轉的現象逐漸嶄露，當時解除分期付款（ATM）、假投資求職、假冒公務機構等劇本不斷更新。

5. 從 2010 年至 2019 年近十年的期間，在第三地設立機房的模式成為各國犯罪偵防的盲點，集團以組織的方式到東南亞、非洲、歐美等國家進行第三地甚至

第四地的電信網路轉接的方式進行電信網路詐欺，包括 ATM 解除分期付款、假冒名義、偽稱買賣與假冒機構公務員，集團組織日漸龐大。

6. 2019 年底 2022 年，COVID-19 的全球大流行，跨境電信的規模逐漸縮小成為機動式樣態，加上封城管制的策略不斷擴大，多數人的生活與網路緊密結合，從一頁式廣告、網路購物、假冒名義、投資詐欺成為主流，而行動機房取代海外設立機房的主要手段。

2022 年至今，全球經濟大解放的階段，我國經濟成長率亮眼，股市也屢創新高，在投資氛圍濃厚的狀況下，電信網路詐欺集團透過社群、臉書、IG、LINE 等網路媒體加以渲染投資致富的訊息，誘使許多投資人誤以為能夠透過各種投資管道來賺取利益。加上網路使用率大幅增加，人們改變購物習慣與支付手法，使得詐團利用電信網路遂行詐欺犯罪。

三、 我國電信網路詐欺犯罪現況與犯罪組織架構及犯罪過程

(一)我國電信網路詐欺犯罪現況

根據內政部刑事警察局的官方資料統計，我國詐欺犯罪的案件數量從 2014 年的 23,053 件緩步上升至 2021 年的 24,724 件，而疫情過後逐步上升到 2023 年的 37,823 件，然而在 2024 年底，我國的詐欺案件突然暴增至過往從未達到的案件高峰 122,805 件，足足比 2014 年的案件量增加了近六倍之多；續從犯罪人數來看，詐欺犯罪的嫌疑犯卻急遽的增加，從 2014 年的 15,518 人急遽增加至 2024 年的 58,666 人，成長了三倍之多，顯然越來越多人投入詐欺犯罪的行列，根據 James Q. Wilson 的嚇阻理論(Deterrence Theory)的核心概念，人是理性的動物，犯罪人計畫犯罪，會因害怕懲罰而有所考量，並且應為其惡行接受懲罰。其中犯罪人會因為刑法的迅速性(Swiftness)，確定性(Certanity)以及嚴厲性(Severtiy)而考慮是否進行犯罪。但根據表 1 的資料來看，詐欺犯罪案件到了 2024 年破天荒的增長到 122,805 件，犯罪嫌疑人數也來到近年來新高點，顯然刑法威懾

效應無法遏制詐欺犯罪的增加[1]。

電信網路詐欺犯罪係為了龐大犯罪利益而遂行之犯罪類別，根據警政統計 112 年報資料，少年嫌疑犯(12 歲以上未滿 18 歲)涉入詐欺犯罪從 2019 年的 17.24%，到了 2023 年增加到了 20.30%；青年嫌疑犯(18 歲以上未滿 24 歲) 涉入詐欺犯罪從 2019 年的 22.09%，到了 2023 年增加到了 31.53%；成年嫌疑犯(24 歲以上) 涉入詐欺犯罪從 2019 年的 8.61%，到了 2023 年增加到了 14.85%[2]；顯然各年齡層對於詐欺犯罪趨之若鶩，值得一提的是涉入詐欺犯罪的外籍人士有增加的趨勢，從 2014 年的 100 人，到了 2022 年來到了 921 人，增加了九倍之多，可見詐欺犯罪組織為了製造更多的查緝斷點，從國外鼓勵外籍人士到台灣進行詐欺犯罪。

[1] 自 113 年 9 月 1 日起刑紀系統將與 e 化系統介接整合，員警於受理民眾報案後 30 分鐘，系統自動產出刑案紀錄表，以資訊技術將 e 化系統填輸資料自動匯入刑紀系統。為與 e 化系統數據統計標準一致，並符合民眾認知，刑紀系統將案件數認定原則從「1 案 1 件」改為「1 被害人 1 件」。警政署公共關係室(2024 年 8 月 30 日)，刑案統計制度革新，迎向大數據時代。內政部警政署。https://www.npa.gov.tw/ch/app/news/view?module=headnews&id=2136&serno=d9eb552b-4eb2-43f4-bd5f-137f975d3fa0

[2] 內政部警政署(2024)，《警政統計年報，資料時間：2023》，8-11 頁

表 1 台灣近十年犯罪現況統計表

	竊盜犯罪		暴力犯罪		詐欺犯罪		毒品犯罪		全般刑案
	案件數	嫌疑人	案件數	嫌疑人	案件數	嫌疑人	案件數	嫌疑人	案件數
2014	76,330	34,574	2,289	2,825	23,053	15,518	38,369	41,265	306,300
2015	66,255	33,913	1,956	2,522	21,172	17,283	49,576	53,622	297,800
2016	57,606	31,543	1,627	2,208	23,175	20,321	54,873	58,707	294,831
2017	52,025	32,204	1,260	1,910	22,689	24,330	58,515	62,644	293,453
2018	47,591	32,028	993	1,666	23,470	27,237	55,480	59,106	284,538
2019	42,272	31,398	859	1,464	23,647	29,581	47,035	49,131	268,349
2020	37,016	29,128	707	1,195	23,054	33,631	45,489	47,779	259,713
2021	35,067	27,929	598	1,073	24,724	36,002	38,644	40,987	243,082
2022	37,670	31,139	499	761	29,509	45,540	38,088	39,964	265,518
2023	38,339	31,920	442	819	37,823	50,276	36,435	38,292	251,485
2024	54,608	35,331	378	600	122,805	58,666	36,511	38,095	384,877

資料來源：內政部警政署，本研究整理

表 2 地檢署辦理電信網路詐欺案件統計表

項目	偵查終結件數	偵查終結人數						執行裁判確定人數			定罪率
		計	起訴	起訴比率	緩起訴處分	不起訴處分	其他	有罪	無罪	其他	
		A	B	B/A ×100				C	D		C/(C+D) ×100
別	件	人	人	%	人	人	人	人	人	人	%
108年	42,448	60,586	21,525	35.5	303	18,557	20,201	10,949	826	474	93.0
109年	56,927	84,263	24,746	29.4	337	29,432	29,748	13,272	979	635	93.1
110年	90,974	115,558	38,478	33.3	420	46,443	30,217	12,604	861	645	93.6
111年	156,904	187,183	60,769	32.5	294	68,355	57,765	19,729	1,083	1,095	94.8
112年	231,400	265,377	76,482	28.8	345	108,379	80,171	26,700	1,446	1,383	94.9

說明：1.電信網路詐欺案件包括以網路、電話、簡訊等方式進行詐欺、恐嚇之犯罪行為。
2.起訴包含通常程序提起公訴及聲請簡易判決處刑。

資料來源：法務部統計年報，112 年，法務部，頁 4-5

根據法務部 2023 年統計年報資料，2023 年地方檢察署終結電信網路詐欺案件計 23 萬 1,400 件，較 2022 年增加 7 萬 4,496 件，約莫 47.5%。偵查終結 26 萬 5,377 人，

其中起訴 7 萬 6,482 人，較上年增加 25.9%，起訴人數占終結人數比率為 28.8%。112 年法院裁判確定移送檢察機關執行有罪 2 萬 6,700 人，定罪率 94.9%。以上述起訴率來看，只有三分之一的人遭到起訴，最後裁判確定移送檢察機關的人數更只有 10%。查扣犯罪所得部分，以詐欺罪 3 億 1,670 萬元占 22.2%最多，對比 2023 年的詐欺財損 89.4 億來說，幾乎沒有任何嚇阻作用可言，更遑論 2024 年的財損突破的 500 億元，可見台灣目前的電信網路詐欺犯罪相當嚴重。

再從表 3 來看，發現詐欺罪偵查起訴的人數逐年增加，從 2019 年開始的 16,822 人，到了 2023 年時變成 38,362 人，整體來說已經增長了 2.5 倍，相較其他類型犯罪起訴人數來看，唯有和詐欺有關聯的洗錢防制法，期增長倍數驚人，2023 年共 43,386 人，比起 2019 年的 3,134 人足足 14 倍之多，顯然我國因修訂了打詐相關法律後，對於詐欺犯罪的相關統計資料都同步上揚，不過這也顯示我國詐欺犯罪相當嚴重，政府也努力朝向打擊詐欺犯罪的方向前進。

表 3 地方檢察署偵查終結起訴主要罪名

項目別	總計	洗錢防制法	詐欺罪	公共危險罪	竊盜罪	傷害罪	毒品危害防制條例	妨害自由罪	賭博罪	偽造印文文書罪	妨害秩序罪
108年	232,563	3,134	16,822	52,384	27,015	27,487	48,214	4,183	5,523	4,680	101
109年	227,507	2,972	24,696	50,171	28,533	29,903	36,784	4,327	6,277	4,785	788
110年	203,524	12,873	29,334	37,827	27,609	28,771	16,732	4,625	3,760	4,538	2,492
111年	248,439	32,091	33,959	39,653	31,565	30,488	21,164	5,557	4,498	4,744	4,603
112年	273,057	43,386	38,362	36,545	36,075	32,359	26,319	5,557	4,891	4,737	3,935

資料來源：法務部統計年報，112 年，法務部，頁 4-13

再以經法院判決確定應沒收犯罪所得的表 4 來看，涉入詐欺犯罪經法院判決確定後應沒收犯罪所得的統計資料，2019 年 266,485 萬元，到了 2023 年則來到了 512,064 萬元，足足提高了一倍之多，除了顯示國內詐欺犯罪之嚴重程度外，對於國內打詐的決心

可見一番，企圖透過嚴法以及沒收制度，嚇阻退散從事詐欺犯罪者的動機，降低可能的犯罪風險。

表 4 地方檢察署執行經法院判決確定應沒收犯罪所得主要罪名統計

單位：新臺幣萬元

項目別	總計	銀行法	詐欺罪	證券交易法	侵占罪	偽造印文文書罪	偽造證券有價罪	廢清棄物法	賭博罪
108年	1,641,409	432,773	266,485	404,991	72,725	81,880	28,800	3,543	28,793
109年	2,156,845	212,095	404,958	106,737	71,361	93,008	62,673	6,337	36,262
110年	5,259,644	3,057,981	331,542	383,891	125,839	116,042	17,292	24,619	82,427
111年	3,007,568	1,101,033	294,656	670,065	68,283	90,466	23,696	23,525	29,764
112年	2,506,249	1,299,690	512,064	163,169	154,440	101,833	32,694	29,320	28,485
結構比(%)	100.0	51.9	20.4	6.5	6.2	4.1	1.3	1.2	1.1
被告	1,976,432	1,030,757	275,571	156,085	150,444	101,693	30,359	23,629	28,485
第三人	529,817	268,933	236,493	7,084	3,996	141	2,335	5,691	-

說明：1.金額係指執行法院判決確定全部案件犯罪所得沒收及追徵金額總計。
2.金額單位為新臺幣萬元，因尾數採四捨五入計算，故細項之和與其總數間偶有些微差異。

資料來源：法務部統計年報，112 年，法務部，頁 4-22

再從監獄新入監受刑人罪名統計表來看，表 5 所顯示的資料從事詐欺罪當年度新入監人數，2019 年時 2,940 人，到了 2023 年有 3,301 人，增加幅度相當低，然當我們比較當年度起訴的有三萬八千人，裁判確定的也有兩萬六千多人，因詐欺犯罪入獄服刑的卻只有三千多人，如此低比例的判決確定數量，對於嚇阻詐欺犯罪人的效果似乎難以符合嚇阻犯罪的確定性、迅速性及嚴厲性，不禁讓我們思考，要徹底嚇阻詐欺犯罪或降低涉入詐欺犯罪人的再犯風險，應該要在司法系統上提出更加解決辦法。

表 5 監獄新入監受刑人罪名

單位：人

項目別	總計	公共危險罪	毒品危害防制條例	竊盜罪	詐欺罪	洗錢防制法	傷害罪	槍砲彈藥刀械管制條例	其他
108年	34,771	9,417	10,598	4,190	2,940	38	1,137	962	5,489
109年	32,547	8,603	8,957	4,058	3,262	71	1,239	930	5,427
110年	25,221	6,665	4,748	3,523	3,094	237	1,107	875	4,972
111年	30,196	9,356	4,390	4,248	3,300	1,421	1,344	841	5,296
112年	31,763	8,444	5,113	4,142	3,301	3,159	1,440	748	5,416
較上年增減%	5.2	-9.7	16.5	-2.5	0.0	122.3	7.1	-11.1	2.3

說明：毒品危害防制條例含87年5月20日修正施行前之肅清煙毒條例及麻醉藥品管理條例。

資料來源：法務部統計年報，112 年，法務部，頁 4-36

總觀上述有關國內詐欺犯罪統計資料來看，日漸嚴峻的詐欺犯罪已經造成國內司法系統的負擔加劇，綜觀國內檢察官在職人數來看，2014 年有 1,398 人，2023 年則有 1,420 人，然而詐欺犯罪案件數量卻是以往的倍數增加，顯然基層法官或檢察官每月的新收案件量相當大，再者面對社會輿論與限時結案的壓力，因為人力、資源不足，使得部分案件調查或審理未能完善，對於第一線的警政人員以及後端的司法系統人員都形成莫大的壓力，唯有降低從事詐欺犯罪的比例，才能徹底解決因為日益嚴重的詐欺犯罪所帶來的各種困境。

(二)電信網路詐欺犯罪組織架構

根據許華孚、黃光甫(2020)的研究，跨境電信詐欺集團的可分為四個子集團，包括電信機房、系統商、水房集團與車手集團，每個子集團當中又包含各種不同的運作角色，透過強連結的方式進行集團內部的運作，透過弱連結來進行橫向集團的聯繫，藉此創造出集團的斷點來躲避查緝。近年來雖然電信網路詐欺手法推陳出新，但其基本組織架構

仍以這四個集團進行詐欺犯罪，以下說明四個集團的組織角色與工作。

1、 電信機房

在電信機房當中，由於有小型電信機房或是大型電信機房，運行核心關鍵角色包括金主、外務親信、總務會計、機房管理、一二三線幹部、電腦手等。金主是電信機房最大的股東，也可以說是整個電信網路詐欺犯罪當中主要發起者。多數的金主會指派一名相當親近的人擔任外務接洽的角色，由該外務親信來成立電信機房與金主之間的聯繫工作。總務會計在電信機房當中的角色多數是金主與外務親信當中會有所接觸，此角色根據機房規模的大小而定，有時候會是由外務親信擔任，有時候也會是金主身旁的重要的人物。電信機房管理者，通常都是之前有豐富的電信機房經驗，同時間已和其他合作組織有廣闊的人脈。機房內部包括一二三線幹部、電腦手、一二三線話務手。

以電信機房來說，目前我國詐欺罪言中的類型為投資型詐騙，電信機房多半以小型機房為主，過往大型海外設立電信機房式微，取而代之的是不易被查緝且移動方便的小型機房。電信機房的角色規模也縮小許多，過去動輒數十位以上的機房，目前多已改成十人以下的機動性機房存在，而一二三線的話務手也因應詐騙劇本的改變，各線的話務手也朝向開設假投資群組當中的成員或投顧老師，以投資獲利為誘惑，群組慫恿的方式來蠱惑被害者相信投資致富手法。不過仍有許多電信機房採用電信網路詐欺手法，向海外華人圈進行詐騙，可謂相當多元的發展，值得透過研究來揭開各種詐欺犯罪手法。

2、 系統商

系統商的角色因為是提供電信機房所需要的節費網路、跨國跳板以及虛假網頁的設計，屬於後勤設備的支援系統，其角色相對來說也比較單純。系統商的負責人與內部工程師為主要角色，負責人多半與外界聯繫與接洽，同時間與多個電信機房配合，將犯罪利益極大化，同時分散被查緝的風險。隨著投資型詐騙的猖獗，許多系統商除了兼顧原本群發系統的業務之外，開始著手製作假網頁以及假投資平台，更擔負起各種網站平台的教學與維修，無疑是拓展詐欺犯罪的範疇，藉由近年來台灣股市投資的熱潮，以投資

名義來遂行詐欺犯罪之實。

3、 水房集團

水房主要工作就是將犯罪所得透過各種不同的匯兌手法來實現犯罪利益。水房集團負責人有的透過合法的金融相關業務公司行號作為掩護，擁有大量的資金可以運用，有的則是熟悉車手與機房業務的經驗老手成立。其成員包括負責人、內部操作、外務交付以及收簿管理等，而有些大型的水房集團也有自己的提款車手，為了不與車手集團混淆，因此本研究的水房集團指著限在金錢匯兌轉帳的部分。內部操作幹部負責與電信機房聯繫與對帳，外務款項交付人員負責與車手交付犯罪所得，同時也與電信機房外務人員交付款項。過去人頭帳戶收購容易，但近年來人頭帳戶耗損率以及警示效率加強，詐團必須以高價收購，而許多人頭帳戶也出現黑吃黑的狀態，進而衍生收簿管理者的角色。

4、 車手集團

車手集團在整個電信網路詐欺犯罪集團當中屬於犯罪利益兌現的重要角色，包括車手頭、幹部(收水、收簿)與提款車手。車手集團除了提款交付外，幹部也包括收購大量的人頭帳戶與轉交犯罪利益的收水幹部，每個重要幹部下面都有自己的車手，而且多半互不認識，也沒有向系統商、水房與機房有固定的位置作為犯罪基地，彼此之間透過社群軟體進行通訊與聯絡，目的就是要降低被查緝的風險。

整體來說電信網路詐欺犯罪是具有結構性、牟利性與持續性的犯罪行為，以組織形式來遂行犯罪，並非所有詐欺犯罪都由這四個子集團共同組成，有些分工仔細的大型詐欺犯罪集團包括四個子集團，有些則是為了躲避查緝或是資金不足的情況下，透過彼此合作而形成的任務型編組，進而衍生出各種不同型態的電信網路詐欺犯罪集團。

然而電信網路詐欺犯罪革新速度快，網際網路快速發展下，電信網路資訊工具的進步與優化，上述四種跨境詐欺組織犯罪群組過於龐大，疫情過後相關詐欺犯罪組織逐漸轉型，從大型的單一組織逐漸轉型成小型組織的型態。以臺北地檢署 2025 年的法律宣導文案中，針對詐欺犯罪組織成員進行說明，犯罪組織的首腦，也是常見的金主，顧名

思義，指的是整個詐騙集團的領導者，負責詐騙工作的策劃及分工。由於首腦通常隱身幕後，因此往往也是最難抓到的詐騙集團成員。其次是行騙者，是詐欺機房成員，是實際與被害人互動並騙取被害人匯款的人，方式可能包含電話、簡訊、通訊軟體等等。再者為取簿手，以前往超商、置物櫃等方式，收受人頭帳戶之人。第四為車手，負責將贓款提領出來，或是向被害人面交詐欺贓款的人。最後為收水手，負責收受車手提領出來的贓款，再把錢交給上手或透過各式管道，輾轉將錢交回給集團的人。收水手的功能在於透過輾轉交付金錢的過程，增加金流上的斷點、造成警方查緝困難。由於取簿手、車手、收水手的工作內容需要在外拋頭露面，因而也是整個詐騙集團中最容易遭查獲、取代性也最高的成員，所以也是詐欺集團成員最有可能利用圈套誘使民眾前往擔任的角色。

(三)電信網路詐欺犯罪過程

根據許華孚、黃光甫(2020)的研究，利用犯罪腳本技術來分析整體電信網路詐欺犯罪過程，將電信網路詐欺犯罪過程分為三大階段，分述如下：

1. 犯罪施行準備階段

以犯罪施行準備階段來看，主要犯罪活動分為前置作業、腳本演練、被害個 資取得。前置作業包含了網路及通訊設備購置與架設、境外聯繫作業、橫向組織聯繫、話務手招募，前置作業的完備有利後續犯罪施行階段，詐欺犯罪啟動需要有首腦成立話務機房，透過境外聯繫作業來完成地點選擇、設備網路的建置，同時與系統商與金流商做好橫向聯繫，接著在台灣或大陸招募第一階段話務手，用大量的第一階段話務手來提高整個受騙率。話務手大多是第一次參加詐欺犯罪，流程與技巧上都有待加強，因此職前訓練的部分則顯得重要，多數的話務機房會在台灣先進行職前訓練，以利到國外機房時便能夠馬上進行，也有些集團採用邊做邊學習的策略，先從旁觀察學習後再上機操作，縮短職前訓練的時間,配合集團運作時程前往國外。此階段尚有一個關鍵的主要犯罪活動，就是被害個資的取得，受害者的個資取得方式第一種是向兜售個資的集團購買，另一種則是群發系統，透過語音文字簡訊的大量發送，讓被害者回撥再進行詐欺，第三種是隨

機撥號的方式找尋被害者，猶如大海撈針的方式進行。

2. 犯罪施行階段

此階段主要犯罪活動包含了被害對象發話以及電信機房一二三階段的腳本詐騙。由於犯罪施行準備階段對於被害個資取得已經完成，接下來則透過逐一撥打、地區撥號系統、語音簡訊群發、社群軟體帳號聯繫、參與交友網站、假網站等，都是與被害者接觸的方式，由於購買個資與群發系統為主流，而社群軟體、交友網站與假網站的方式取得與被害人接觸的方式多半為愛情詐欺的方式較多，有些話務機房為了能夠發揮被害個資的最大效應，在一般假冒公務機關的劇本失敗後，同樣的個資也沿用愛情詐欺的腳本繼續進行犯罪活動。第一階段詐欺犯罪先讓被害者誤認為自己的權益受損或者違反相關規定的情形，經過深入詢問後懷疑被害者有個資外洩的情況，因此協助被害者進行報案的動作。第二階段的詐欺犯罪，讓被害著警戒的心態降低，恐懼的狀態提高，半信半疑的情境下讓被害者信以為真。第三階段話務手則是最後關鍵階段，利用被害人的不穩定心理情緒狀態，以恐嚇與協助雙管齊下讓被害者將自身帳戶內的財物轉匯至特定人頭帳戶，來進行財產來源調查，三階段的話務手多為獨立空間作業。犯罪施行階段的系統商、話務手、電腦手扮演著重要的關鍵角色，沒有這些關鍵角色的扮演與開展，是無法讓電信網路詐欺犯罪成功。

3. 犯罪後續處理階段

犯罪後續處理階段的主要犯罪活動為犯罪所得轉匯與提取、犯罪利益分配，當被害者已經將自己帳戶內款項轉到特定帳戶後，透過同步轉匯、車手取款、地下匯兌、有價金融商品、外務交付款項等步驟將款項轉到集團首腦手中，電腦手、第三階段話務手以及洗錢機房三方在同時間核對帳戶內款項後，以層層轉匯的方式打散到車手集團的人頭帳戶，在由車手集團提領款項進行交付的動作。整體電信網路詐欺犯罪就是為了讓犯罪所得最後能夠回到首腦手中，因此必須有萬全的準備才能夠降低風險。

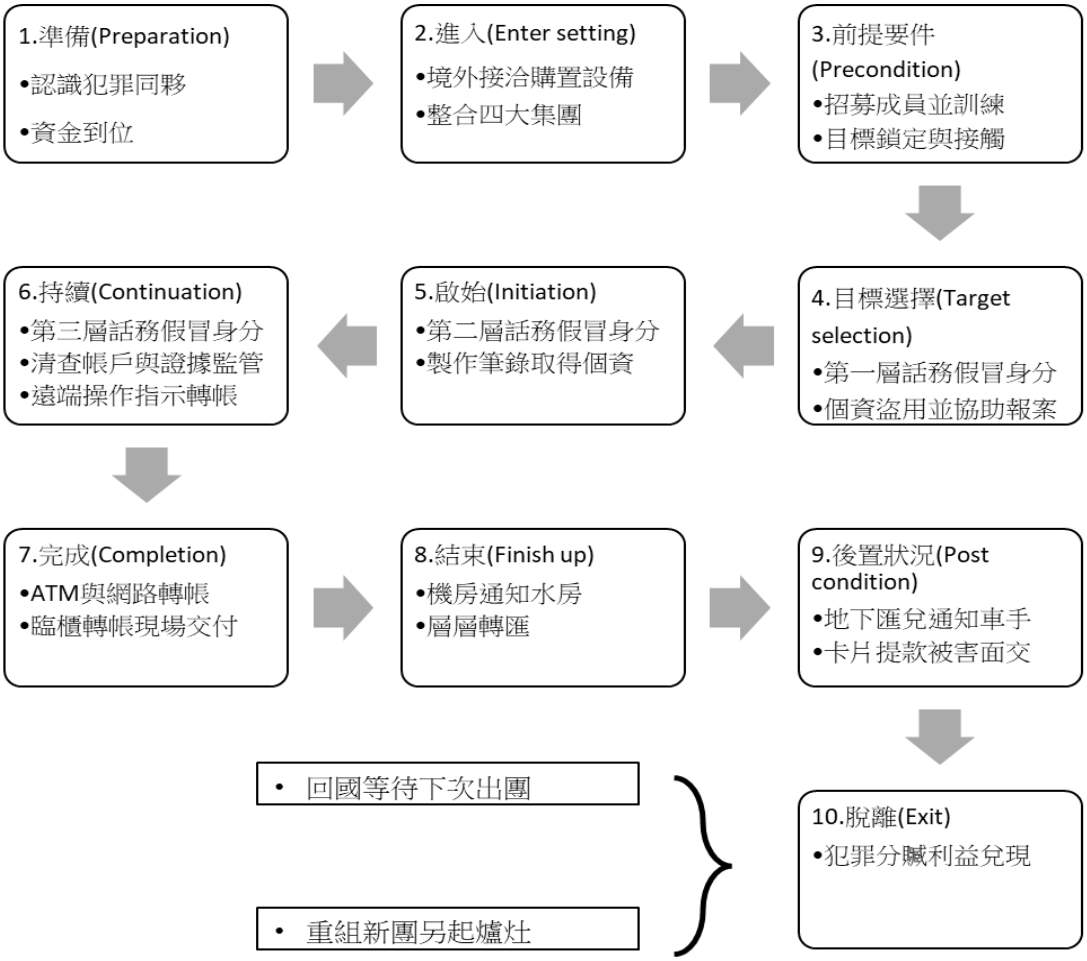


圖 3 電信網路詐欺犯罪過程，資料來源：許華孚、黃光甫(2020)

透過圖 3 的詐欺犯罪腳本，可清楚地了解詐欺犯罪集團的運作過程，也能夠知道詐欺犯罪過程中，每個子集團會在哪個階段負責那些工作，了解電信網路詐欺犯罪的特性，將能夠有效的針對每個犯罪過程施以具體的犯罪介入與偵查，能夠提出更具體的詐欺犯罪抗制具體政策與作為。

詐欺犯罪腳本的分析係以過往犯罪過程進行解構，當詐欺犯罪集團發現此類腳本已無法滿足或者是成功率驟降，便開始轉換不同的犯罪腳本。然根據內政部警政統計通報(2025)第 14 周資料，2024 年 9 月至 12 月詐欺案件被害人計 94,757 人，其中女性占 54.67%；被害方式以「投資詐欺」占 35.87%最多。由於投資詐欺金額龐大，犯罪利益相當可觀，近年來詐欺手法已經慢慢朝向投資詐欺。投資詐欺的手法有其模式，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，後續再以洗碼量不足、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。投資詐欺手法層出不窮，常見的投資詐欺手法包括以下幾種：

1、 龐氏騙局，是一種以後來投資者的資金支付給早期投資者的詐騙模式。詐騙者承諾高回報，但實際上並未進行任何真正的投資，整個計劃依賴於不斷吸引新的投資者來維持資金流動。當新資金無法跟上支付需求時，詐騙就會崩潰。

2、 金字塔騙局，俗稱老鼠會，與龐氏騙局相似，金字塔騙局依賴於不斷招募新成員來獲取收益。參與者需繳納初期投資或費用，並被承諾通過推薦他人加入賺取回報。這種模式無法長期持續，因為新加入者最終會耗盡，導致金字塔崩潰。

3、 虛假證券投資，這類詐騙通常會偽造股票、債券或其他金融工具，或在未經許可的市場上販售這些虛假的投資產品。詐騙者可能通過偽造的文件、網頁和名人背書來提升其可信度。此外，為了增加受害者受騙的可能性，詐騙集團往往會利用限時限量的口號，讓民眾的思考時間受壓縮而做出不理性的選擇。

4、 外匯和虛擬貨幣詐騙，外匯和加密貨幣市場相對較新，詐騙者常以這些高風險、高回報的市場為名設計詐騙，利用投資者對市場運作的陌生。詐騙者可能會以虛假的平台或保證獲利為誘餌，吸引投資者投入資金。除此之外，有些詐騙者會謊稱只需要提供帳戶，投資者就會將錢匯給受害者，並且要求受害者註冊虛

擬貨幣交易平台後將收到的錢購買虛擬貨幣後轉入指定帳戶，剩下的錢會成為傭金，受害者在未熟慮的情況下依指示進行就會觸犯洗錢防制法。

5、 APP 投資詐騙，詐騙者會要求受害者依指示下載特定 APP 並註冊會員，謊稱該 APP 為投資用，但實際上為詐騙集團在後台中操弄數據，目的是為了要讓受害者相信該 APP 是真的投資軟體，且詐騙者說的項目確實能獲利，進而依指示將錢匯入，後續被害者才發現無法將錢領出。

6、 繳納保證金詐騙，在受害者依詐騙者指示進行投資後，受害者發現無法領出錢時，詐騙者會佯稱只要受害者再投入保證金，就可將之前投資賺到的錢領出，而實際上卻只是再被騙一次錢。

7、 「合夥投資」詐騙，詐騙者假裝提供合法的商業合作或投資機會，通常利用人們對某一行業的興趣或信任，聲稱合夥投資會帶來豐厚回報。事實上，這些投資要就是不存在，或是被嚴重誇大。此外，有時詐騙者會將被害者拉入群組，然而群組成員實際上皆為詐騙集團成員，並透過一搭一唱的方式使受害者相信真的能投資賺到錢。

上述的投資詐騙手法是常見的投資詐欺類型，根據表 6 統計表內容，我國詐欺犯罪型態前五名從 2015 年依序排名為假冒名義、解除分期付款詐欺(ATM)、假網路拍賣(購物)、假冒機構(公務員)、偽稱買賣，其占比為 16.34%、13.67%、11.05%、9.84%、9.34%，2016 與 2017 年開始解除分期付款爬升到第一名，比例提高至 23.46%，隨後 2019 與 2020 年開始，網路購物與一般購物詐欺竄升至第一名，疫情期間，2021 年與 2022 年開始，投資詐欺取代網路與一般購物詐欺成為第一名，比例多為 24%左右，隨即到了 2023 年開始，疫情趨緩後，台灣恢復正常生活模式，投資詐欺仍位居第一名，比例卻提升至 31.13%，已高達三分之一強。若以 2025 年 3 月的打詐儀表板統計資料來看，前五名依序為假投資詐騙、網路購物詐騙、假買家騙賣家詐騙、假中獎通知詐騙以及假交友(投資詐騙)詐騙，從統計資料來看台灣目前詐騙主流就是以投資為主的詐騙手法，然仔細分析，

這五大詐騙手法，受害者獲得相關訊息都是藉由社群媒體 LINE、抖音、臉書、簡訊、交友軟體、網路購物等網站上獲得，隨即陷入詐騙集團的話術與手法，進而遭到詐騙集團的犯罪模式當中。而上述的相關社群媒體、網站購物、APP 等手法，皆是透過電信網路來遂行犯罪，多數人生活忙碌下，獲得相關資訊都是從手機或筆電來取得，可見電信網路詐欺犯罪深入每個人的生活當中，一不小心將落入詐欺犯罪集團的陷阱中。

從 165 打詐儀表版的最新案例分析來看，以下將近來各種電信網路詐欺犯罪過程進行初步說明：

1、 投資詐騙：先透過獲利飆升或者快速獲利等吸睛廣告來吸引被害人注意，接著誘使被害人連結其他 APP 進而加入虛假群組中，第三步驟則是利用話術讓被害者以小額充值投資，透過後臺顯示虛假的獲利數字，營造或綠的假象並取信被害人加大投資力道，當被害人投入大筆資金後，想獲利了結發現投資金錢無法領回，被害人被踢出群組或者帳號消失等，才驚覺自己遭受到投資詐騙。

2、 網路購物詐騙：由於網路購物商品多樣化，犯罪人先以低價商品以及限時限量的口號來吸引被害者的注意，接著要求私下交易能夠提供更便宜的價格來優惠客戶，加上以貨到付款的方式宣稱比起網路轉帳，或者是第三方支付平台交易更有保障，被害人不疑有他的情況下下單購買，當貨到付款後，才發現購買的貨品與廣告宣稱的不同，聯繫對方要求退款，但對方一直找藉口拖延，甚至開始已讀不回。

3、 假交友(徵婚詐財與投資詐騙)詐騙：透過時下流行的交友軟體或者是社群軟體來大量發送交友訊息，聊工作、分享經驗，並對我噓寒問暖，拉近彼此距離。隨後分享自己成功故事，塑造專業形象，接著分享自己賺錢的截圖，誘導被害人投入資金，最後想獲利了解必須再度投入保證金方能出金，最後發現無法獲利了結。徵婚詐財則也是先透過交友軟體來建立信任後，假借自己遭遇困境急需協助，匯款後仍持續以多種不同藉口要持續匯款索取金錢，待提出質疑後便

切斷聯繫。

4、 假買家騙賣家詐騙：在網路購物上佯裝買家對賣家所販售物品有極高興趣，藉口提出常見的交易方式後，再佯稱交易時遇到匯款轉帳之問題，藉由賣家想賣出商品之心態，提供偽造之客服網址、金流驗證或實名制認證等藉口，套取賣家的個資與帳號，假借驗證之名將帳號與相關轉帳密碼輸入驗證後，盜取金錢後迅速消失。

5、 釣魚簡訊(惡意連結)詐騙：假借官方名義發送各種不同簡訊通知，簡訊中表示相關未繳納費用逾期可能涉及之刑事責任，誘使被害者點選虛假訊息中的連結網址，在虛假網址中輸入個人資訊與信用卡資料，當詐騙集團收集到相關資料後，便將信用卡盜刷套取現金。

6、 假中獎通知詐騙：透過社群軟體或者網路簡訊得知抽獎訊息，填入個資後收到中獎訊息，緊接著佯稱領獎須繳交相關費用之藉口，要求被害人匯款，並表示多次匯款錯誤訊息，誘使被害人多次操作匯款動作而遭到詐騙。

目前台灣最常見的詐欺犯罪，除了上述六種詐騙手法外，尚有假求職、假借銀行貸款、假檢警、騙取金融帳戶、假廣告、色情應召詐財、虛擬遊戲與猜猜我是誰等詐騙手法。然經犯罪過程分析後，發現上述所有的詐騙類別多與電信網路相關。所有的詐騙與被害人第一次接觸都是藉由電信網路所發出之虛假簡訊、社群媒體網站虛假廣告、交友軟體互動等，多半透過手機或平板筆電上網的機會進行首次接觸，隨著台灣經濟股市大好的繁榮前景下，利用多數人想要投資致富的心態，逐漸陷入詐騙集團的陷阱。

表 6 台灣近十年詐欺型態分析統計表

	第一名	件數 百分比	第二名	件數 百分比	第三名	件數 百分比	第四名	件數 百分比	第五名	件數 百分比
2015	假冒名義	2824 16.34%	解除分期付款詐欺(ATM)	2363 13.67%	假網路拍賣(購物)	1909 11.05%	假冒機構(公務員)	1700 9.84%	偽稱買賣	1615 、
2016	解除分期付款詐欺(ATM)	4156 20.45%	假冒名義	3452 16.99%	假網路拍賣(購物)	2578 12.69%	假冒機構(公務員)	2105 10.36%	拒付款項(賴帳)	1807 8.89%
2017	解除分期付款詐欺(ATM)	5707 23.46%	假冒名義	4697 19.31%	假網路拍賣(購物)	2987 12.28%	假冒機構(公務員)	1885 7.75%	拒付款項(賴帳)	1873 7.70%
2018	假冒名義	6052 22.22%	解除分期付款詐欺(ATM)	4648 17.07%	假網路拍賣(購物)	4011 14.73%	假冒機構(公務員)	2035 7.47%	假冒機構(公務員)	1933 7.10%
2019	假網路拍賣(購物)	3720 15.72%	一般購物詐欺(偽稱買賣)	3060 12.93%	解除分期付款詐欺(ATM)	2846 12.02%	投資詐欺	1871 7.90%	猜猜我是誰	1852 7.82%
2020	一般購物詐欺(偽稱買賣)	3,044 13.27%	解除分期付款詐欺(ATM)	2,905 12.66%	投資詐欺	2,845 12.40%	假網路拍賣(購物)	2,790 12.16%	猜猜我是誰	2,068 9.01%
2021	投資詐欺	8,743 24.28%	解除分期付款詐欺(ATM)	6,949 19.30%	一般購物詐欺(偽稱買賣)	3,065 8.51%	假網路拍賣(購物)	2,939 8.16%	猜猜我是誰	2,816 7.82%
2022	投資詐欺	6,542 22.16%	解除分期付款詐欺(ATM)	5,084 17.22%	一般購物詐欺(偽稱買賣)	3,496 11.84%	假網路拍賣(購物)	3,295 11.16%	假愛情交友	1,442 4.88%
2023	投資詐欺	11,775 31.13%	解除分期付款詐欺(ATM)	7,351 19.44%	假網路拍賣(購物)	4,667 12.34%	一般購物詐欺(偽稱買賣)	3,579 9.46%	假愛情交友	1,368 3.62%

資料來源：內政部警政署刑事統計資料，本研究整理。

根據 165 打詐儀表版統計資料所示(如表 7)，從 2024 年 8 月開始上路後，八月份的詐騙案件數 21,244 件，財損金額達 138 億，近八個月的詐騙案件數有下降趨勢，財損也降低至 70 億。整體來說我國從打詐 2.0 政策開始後，短期似乎有明顯的成效，然從前五種詐欺手法來看，多為假投資詐騙、網路購物詐騙、假買家騙賣家詐騙、假交友(投資)

詐騙、假中獎通知詐騙等，都是藉由電信網路的手法來接觸被害者，對於打擊電信網路詐欺顯得更為重要。

表 7 台灣詐騙案件數與財損金額與手法統計表

	詐騙案件數	財損金額	第一名手法	第二名手法	第三名手法	第四名手法	第五名手法
2024/8	21,244	138 億	假投資詐騙	網路購物詐騙	假買家騙賣家	假交友(投資)	色情應召詐財
2024/9	18,015	119 億	假投資詐騙	網路購物詐騙	假買家騙賣家	假交友(投資)	假中獎通知
2024/10	18,150	120 億	假投資詐騙	網路購物詐騙	假買家騙賣家	假交友(投資)	假中獎通知
2024/11	18,204	126 億	假投資詐騙	網路購物詐騙	假買家騙賣家	假中獎通知	假交友(投資)
2024/12	17,766	124 億	假投資詐騙	網路購物詐騙	假買家騙賣家	假中獎通知	假交友(投資)
2025/1	13,120	95 億	假投資詐騙	網路購物詐騙	假買家騙賣家	假交友(投資)	假中獎通知
2025/2	10,773	60 億	假投資詐騙	網路購物詐騙	假買家騙賣家	假交友(投資)	假中獎通知
2025/3	16,643	70 億	假投資詐騙	網路購物詐騙	假買家騙賣家	假中獎通知	假交友(投資)

資料來源：165 打詐儀表板，本研究整理。

四、 我國電信網路詐欺犯罪演進及政策面臨的困境

(一)電信網路詐欺定義

電信網路犯罪是新興犯罪型態，許多犯罪學家都針對網路犯罪提出定義。學者林山田(2012)提出廣義的「網路犯罪」，是指所有與電腦相關的犯罪行為，簡單來說就是「與電腦有關的犯罪」。黃富源、張平吾、范國勇(2012)也針對網路犯罪提出廣義與狹義定義，認為網路犯罪是與電腦有關的犯罪，與電子資料處理有關而違法的財產破壞行為。多數的國外學者認為網路犯罪從早期跟電腦資訊設備有關的犯罪，因為網路科技進步的關係，慢慢將網路犯罪的定義拓展到一切和電腦與網路相關的違法行為，都可以稱之為

網路犯罪 (Alshammari & Singh, 2018; Amarullah, Runturambi & Widiawan, 2021; Sharma & Kaur, 2019)。

網路犯罪通常結合電信科技，主要是因為近年來手機成為大眾生活不可或缺的生活用品，根據我國電信法的定義：是指利用有線、無線，以光、電磁系統或其他科技產品發送、傳輸或接收符號、信號、文字、影像、聲音或其他性質之訊息。電信所提供的重要服務之一就是網際網路，隨著智慧型手機的普及，便宜的資費以及電信通訊設備的進步，民眾生活中的大大小小事項都可以透過電信網路來完成，從通訊、上網到各種消費金融服務，都在智慧型手機上便可完成，也因此詐欺犯罪利用這樣的生活模式，透過電信網路為媒介遂行詐欺犯罪。

Smith & Grabosky (2017)認為網路犯罪包括竊取通訊服務、散播色情圖片資料、網路粗魯恐怖行為、電腦通訊著作權侵害、犯罪集團使用通訊技術犯罪、網路資訊非法竊聽、通訊銷售詐欺行為、洗錢、轉移資金等。由於過往能夠使用網路的設備多為電腦，但是隨著手機、電視、平板等各種裝置都具備上網功能，網路電話與社群媒體已成為目前主流的溝通工具之一，不再局限於電腦設備的犯罪行為。因此「電信網路詐欺犯罪」是行為人透過各種電子資訊通信設備，藉由網路為媒介來遂行犯罪行為。

(二)我國電信網路詐欺犯罪防制困境

根據內政部 165 全民防騙網的資料，在 2023 年所公布的常見詐騙手法及防範方法當中，最常見的方法有「一頁式廣告」、「三方詐欺」、「假網拍詐騙」、「假投資詐騙」、「解除分期詐騙」、「人頭帳戶詐騙」、「假檢警詐騙」、「假愛情交友詐騙」等，都是目前詐欺犯罪方法的主流模式。這些模式都有一個共同點，首先不會有被害者與加害者見面的機會，再來會透過網路工具來進行聯繫，緊接著會指示被害者透過 ATM、線上付款或臨櫃轉帳等多種方式將款項匯至人頭帳戶，之後便銷聲匿跡。這樣的手法如出一轍，都是透過不同的劇本編排，以及網路來進行詐欺犯罪。網路世界無遠弗屆，卻也存在著犯罪者可能分布在各個不同國度的問題，再加上網路本身的開放性質，普羅大

眾都能夠使用，透過網路可以將不同區域、工具相互連結，產生了互通性，但即使如此的便捷之下，卻也因為虛擬化的存在，使得整個網路充滿了隱密性，最重要的是因為網路科技的發達，許多透過網路來行使的活動，都能在短時間內完成，橫跨了空間與時間，能夠有立即性的效果。這也使得犯罪者趨之若鶩的使用網路來當作犯罪的工具。

目前行政院新世代打擊詐欺策略存有以下幾點困境：1.識詐層面存在未能分齡分眾宣傳防詐、教育訓練未能擴及第一線執法人員之專業與精進以及實務上已存在重複被害之情形；2.堵詐層面存在 165 反詐專線之任務編組位階過低、未能廣泛運用高科技如 AI 技術於偵辦網路詐欺犯罪、法官的審判與量刑較為保守以及社群平臺規避審查責任等，讓當前堵詐成效受限；3.阻詐層面則是政府與產業界合作仍然不足、偵查部門對於區塊鍊、加密貨幣進行交易與資產移轉，能力不足以及金融機構與警方合作偵辦網路詐欺犯罪尚有努力空間；4.懲詐層面存在司法互助曠日廢時、派駐他國聯絡官人力不足、數位專家鑑定機制尚未成立、懲詐之刑度與量刑過短以及政府與民間橫向連結與情資互通，仍嫌不足(賴擁連、蔡田木、陳玉書，2024)。

政府自 2022 年 6 月起實施「新世代打擊詐欺策略行動綱領」，2023 年進升至 1.5 版，並於 2024 年 7 月三讀通過「打詐新 4 法」包括制定「詐欺犯罪危害防制條例」、「通訊保障及監察法」、「刑事訴訟法特殊強制處分專章」、「洗錢防制法」，我國打詐綱領已進化至 2.0 版，也從金融機構與虛擬資產事業與人員、電信事業以及數位經濟產業三方面著手，結合過往的 1.0 版到 1.5 版的打詐作為，制定更完整的打擊詐騙整體政策。2.0 版政策已經上路半年，打詐成果上面難以看到顯著之成效，除了將過往的困境羅列之外，本研究團隊嘗試從我國官方資料來進行剖析並進行說明。以警政署 2024 年的詐欺案件統計數來看，2024 年詐欺案件數量達 122,805 件，案件量的暴增是統計基準的改變所導致，我們從 2025 年的法務部統計月報資料來細看(表 8)，台灣電信詐欺網路詐欺的犯罪類型以提供人頭帳戶為主，結構比高達 61.6%，車手為 12.6%，一般電信網路詐欺則為 25.8%，只有人頭帳戶比例降低，其餘皆有增長的趨勢。顯見多數人知悉帳戶不能提供他用，也顯示詐騙集團人頭帳戶的取得越來越困難，才會有台版柬埔寨案件

[3]的出現。車手的部分則是約略 12.6%，顯見電信網路詐欺的犯罪利益實現，逐漸轉由數位金融的部分來取代。

全球詐欺犯罪日益猖獗，台灣近年詐欺案數量與金額居高不下，對於打擊電信網路詐欺犯罪所遭遇的困境，法律層面上來說，台灣當前反詐欺困境在於現行《刑法》第 339 條規範詐欺罪，最高可處 5 年有期徒刑，併科罰金。雖然打詐 2.0 有「詐欺犯罪危害防制條例」的出現，過去司法實務上量刑較輕、緩刑居多，甚至部分詐欺集團幕後主謀難以追查，使得詐欺犯罪的成本極低，誘使更多人鋌而走險，尤其目前詐騙集團使用各種手段來招募或拐騙被害者擔任車手，使得國內檢警疲於抓車手的情形越來越多，使得檢警人力也開始出現吃緊的狀態。此外，打詐雖然政策與面向相當全面，然而公部門的協同作戰與私部門的配合又是另外一個亟待解決的困境之一。公部門的本位主義運作下，設立再多的打詐辦公室或者是統籌中心，若沒有實際的協調者或者發號施令與落實執行的效率，這些任務型的辦公室可能又是曇花一現的亮點政策。私部門的配合又是另外一個重點，私部門諸如金融機構、電信與社群媒體等企業，皆以營利為主，保護顧客隱私為優先。而電信網路詐欺犯罪又是隱密性極高的犯罪型態，從個人資料到金融匯兌轉帳等業務，業者在營利優先的情況下，且沒有法規的強制規範下，似乎很難有效成為打詐的得力助手。再者，詐欺案件的受害人往往難以追回損失，僅能無奈承受痛苦，這讓大眾對司法制度產生失望，甚至影響社會信任基礎。在打詐 2.0 政策上路後，相關的規範是否能夠奏效，則有待時間的考驗。

再從表 9 的統計資料來看，電信網路詐欺的新收案件數從 2020 年的 58,508 件，佔 11.7%，到了 2023 年增加到 229,711 件，佔 31.3%，為歷年新高，2024 年則降為 167,932 件，佔 25%，仍處於高檔中。從起訴率來看，2024 年電信網路詐欺犯罪的起訴率來到 37.3%，而已 2025 年最新四月統計資料來看，前四個月的起訴率來到 46.5%，有顯著的增長，已是近年新高，顯見我國對於打詐成效有顯著的增長。由於打詐 2.0 剛上路半年，

[3] 王宏舜(2025 年 5 月 15 日)。台版柬埔寨案詐 3.9 億還凌虐 3 男女致死 「藍道」杜承哲上訴仍判無期。聯合新聞網。https://udn.com/news/story/7321/8740962

目前困境尚未顯著出現，因此本研究將收集各國可能出現的困境再加以探討。

表 8 近五年電信網路詐欺案件偵查終結人數表

地方檢察署辦理電信網路詐欺案件偵查終結人數─按犯罪類型分

單位：人、%

項目別	總計	單純車手	起訴	起訴比率	單純提供人頭帳戶	起訴	起訴比率	一般電信詐欺	起訴	起訴比率
		A	B	B/A ×100	C	D	D/C ×100	E	F	F/E ×100
109年	84,366	12,054	7,250	60.1	49,164	8,566	17.4	23,148	8,934	38.6
110年	115,637	13,176	8,276	62.8	75,253	17,802	23.7	27,208	12,410	45.6
111年	187,193	12,067	8,040	66.6	134,794	32,742	24.3	40,332	19,988	49.6
112年	265,379	12,172	8,522	70.0	202,073	40,958	20.3	51,134	27,004	52.8
113年	207,485	26,144	20,001	76.5	127,754	28,732	22.5	53,587	28,603	53.4
結構比(%)	*100.0*	*12.6*	*9.6*		*61.6*	*13.8*		*25.8*	*13.8*	
較上年增減%	*-21.8*	*114.8*	*134.7*	*{6.5}*	*-36.8*	*-29.9*	*{2.2}*	*4.8*	*5.9*	*{0.6}*

說明：1.電信網路詐欺案件包括以網路、電話、簡訊等方式進行詐欺、恐嚇之犯罪行為。
2.單純車手：為詐騙集團中負責領取被害人交付款項者。
3.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。
4.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。

資料來源：法務部統計月報，2024 年 12 月

表 9 近五年電信網路詐欺犯罪偵查案件收結統計表

地方檢察署辦理偵查案件收結情形

單位：件、人、%

項目別	偵查新收件數 A	電信網路詐欺 B	百分比 B/A ×100	偵查終結人數 C	電信網路詐欺						
					計 D	百分比 D/C ×100	起訴 E	起訴比率 E/D ×100	緩起訴處分	不起訴處分	其他
109年	499,607	58,508	11.7	619,134	84,366	13.6	24,750	29.3	339	29,455	29,822
110年	533,569	98,256	18.4	628,135	115,637	18.4	38,488	33.3	420	46,457	30,272
111年	639,301	160,803	25.2	779,851	187,193	24.0	60,770	32.5	294	68,357	57,772
112年	733,505	229,711	31.3	869,530	265,379	30.5	76,484	28.8	345	108,380	80,170
113年	670,574	167,932	25.0	808,249	207,485	25.7	77,336	37.3	317	77,121	52,711
較上年增減%	*-8.6*	*-26.9*	*{-6.3}*	*-7.0*	*-21.8*	*{-4.8}*	*1.1*	*{8.5}*	*-8.1*	*-28.8*	*-34.3*

說明：1.電信網路詐欺案件包括以網路、電話、簡訊等方式進行詐欺、恐嚇之犯罪行為。
2.「其他」包括移送調解、通緝、移轉管轄、移送法院併案審理及其他簽結等。
3.括弧{}內數字係指增減百分點。

資料來源：法務部統計月報，2024 年 12 月

第二節 先進國家電信網路詐欺犯罪政策及防制經驗

一、 美國

(一)美國電信網路詐欺犯罪現況

美國對於網路犯罪打擊始於 2000 年，當年成立了網路犯罪通報中心(Internet Crime Complaint Center, IC3)[4]，美國成立 IC3 以打擊網路犯罪的專責單位，其目的的為了可與民間部門以及地方、州、聯邦和國際相關機構合作，透過 www.ic3.gov 網站，專責受理被害人報案，辦理關鍵角色來提醒民眾注意網路犯罪與威脅、蒐集資料、執行分析、轉介報案和追回資產，更重要的是透過 FBI 的執法企業門戶網站(Law Enforcement Enterprise Portal, LEEP)，介接遠端查詢數據庫(FBI, 2024)。

根據美國聯邦調查局中的網路犯罪通報中心資料顯示，美國在 2023 年總共接收到 880,418 件網路犯罪通報案件，潛在的網路犯罪財損超過了 125 億美元，比起 2022 年的通報案件上漲了 10%，財損增了 22%。投資詐騙成為 2023 年財損最高的網路犯罪手法。投資詐騙造成的損失從 2022 年的 33.1 億美元增至 2023 年的 45.7 億美元，增幅達 38%。其中 30 至 49 歲的個體是最有可能遭到投資詐騙的族群，而老年人則有超過半數的損失是來自投資詐騙。從上面調查報告得知，美國的網路犯罪最大宗的犯罪類型就是詐欺犯罪，顯然美國對於打擊電信網路詐欺的政策與作為，值得我們台灣做為借鏡。

根據 FBI 的 IC3 對於詐欺犯罪的類型來說，包括收養詐欺(Adoption Fraud)、商業和投資詐欺(Business and Investment Fraud)、電子郵件詐欺(Business and Investment Fraud)、慈善與災難詐欺(Business and Investment Fraud)、消費購物詐欺(Consumer Fraud Schemes)、加密貨幣投資詐欺(Cryptocurrency Investment Fraud)、求職詐欺(Cryptocurrency Job Fraud)、

[4] IC3 成立於 2000 年 5 月，負責受理各種網路事務的投訴，包括各種形式的網路詐欺，包括智慧財產權（IPR)、電腦入侵、經濟間諜（竊取商業機密)、線上勒索、國際貨幣洗錢、身份盜用，以及各種網際網路促成的犯罪。

老人詐欺(Elder Fraud)、醫療保險詐欺(Health Care Fraud)、節慶網購詐欺(Holiday Scams)、轉帳洗錢 (Money Mules)、勒索郵件(Ransomware)、愛情交友(Romance Scams)、網路釣魚簡訊詐欺(Spoofing and Phishing)、假客服詐欺(Tech Support Scams)、分時度假詐欺(Timeshare Fraud)。根據 IC3 的統計，近六年的所受理的網路報案案件，未付款未交貨、個人資料外洩、釣魚詐欺、勒索、假冒身分、假客服、愛情交友詐欺、投資詐欺等，這幾個項目的詐欺類別排名順序有所不同，過去美國最常見的是未付款未交貨的詐欺犯罪，高達 81,029 件，比起第二名的個人資料外洩足足有三倍之多；然而到了 2019 年開始，釣魚簡訊類詐欺犯罪異軍突起，從 2019 年的 114,702 件，到 2021 年來到了 323,972 件，隨後降至 2024 年的 193,407 件。綜觀當時時空背景，是新冠肺炎肆虐全球的期間，多數人封城在家而開始依賴電信網路工具來獲得資訊並與外界取得聯繫，明顯的看出美國的電信網路詐欺犯罪相當嚴峻。

表 10 2018-2024 美國網路報案中心前五名的網路犯罪類型

	第一名	第二名	第三名	第四名	第五名
2018	未付款未交貨 65,116	勒索 51,146	個人資料外洩 50,642	釣魚詐欺 26,379	假冒身分 16,128
2019	釣魚詐欺 114,702	未付款未交貨 61,832	勒索 43,101	個人資料外洩 38,218	假冒身分 16,053
2020	釣魚詐欺 241,342	未付款未交貨 108,869	勒索 76,741	個人資料外洩 45,330	愛情交友詐欺 23,751
2021	釣魚詐欺 323,972	未付款未交貨 82,478	個人資料外洩 51,829	勒索 39,360	愛情交友詐欺 24,299
2022	釣魚詐欺 300,497	個人資料外洩 58,859	未付款未交貨 51,679	勒索 39,416	假客服 32,538
2023	釣魚詐欺 298,878	個人資料外洩 55,851	未付款未交貨 50,523	勒索 48,223	投資詐欺 39,570
2024	釣魚詐欺 193,407	勒索 86,415	個人資料外洩 64,882	未付款未交貨 49,572	投資詐欺 47,919

資料來源：FBI(2023)，2022 Internet Crime Report; FBI(2024)，2023 Internet Crime Report. FBI(2025)，2024 Internet Crime Report.賴擁連、蔡田木、陳玉書(2023)，我國網路

詐欺被害調查與防制研究，頁 36。

此外 IC3 的年度報導也針對網路詐欺犯罪類型對於美國民眾之威脅與現況，進行分析。

1. 商業電子詐欺[5](Business Email Compromise, BEC)

2023 年，商業郵件妥協(BEC)共有 21,489 投訴，其財損超過 29 億美元。商業電子郵件詐欺是針對大量企業以及個人的資金轉帳的詐欺手法，其犯罪手法是由透過程式或電腦駭客入侵的方式，對於合法企業的電子郵件帳戶進行未經授權的資金轉帳。透過駭客的方式取得各大企業的電子郵件，假借企業名義去針對其他廠商或個人下訂單，或者要求大量貨品的偽需求交易。利用金融機構的託管帳戶為加密貨幣交易或第三方支付平台，或讓個體戶將資金直接發送至這些平台，而資金在這些平台上迅速做轉帳打散。由於交易所或第三方支付平台強調必須經過多重驗證來做為金融安全性。由於犯罪過程需要透過驗證來付款，因此除了電子郵件往來溝通外，也包括直接撥打電話來取得驗證碼等方式，由於電子郵件為企業彼此商業往來的重要關鍵，使得被害者不疑有他而陷入被詐欺的風險中。

2. 投資詐欺[6](Investment)

在 2023 年統計資料中，投資詐騙造成的財損是所有網路犯罪中最多的。從 2022 年的 33.1 億美元增加到 2023 年的 45.7 億美元，增幅為 38%。當中加密貨幣的投資詐騙從 2022 年的 25.7 億美元上升到 2023 年的 39.6 億美元，增幅為 53%。投資詐騙是誘使被害人信以為能夠有豐厚的投資回報為真。以投資詐欺來看，20 歲以下的報案數有 387 件，20 到 29 歲的有 3,363 件，30 到 39 歲的有 6,654 件，40 到 49 歲的有 6,680 件，50 到 59 歲的有 5,608 件，60 歲以上的有 6,404 件，顯然投資詐欺都針對有一定存

[5] FBI(2024)，2023 Internet Crime Report. P11. Retrieved from: https://www.ic3.gov/annualreport/reports/2023_ic3report.pd 最後瀏覽日：2025 年 3 月 25。

[6] 同註 5。頁 12。

款或者財富的個體進行詐騙。以 2022 年的報告內容來看，同樣也是投資詐欺為主，其手法有以下五種：

(1) 流動資金挖礦(Liquidity mining)，是將被害人透過其他管道被引誘而將加密貨幣錢包鏈接到挖礦的 App 中，然後犯罪者則在未經被害人許可的情況下轉移被害人的資金。

(2) 駭入社群媒體詐欺 (Hacked social media)，由犯罪者透過科技駭入被害人之社群媒體帳號，再大肆宣傳虛假加密貨幣投資機會，引誘被害人將加密貨幣轉入詐欺帳戶進行虛假投資，此類手法多半是假冒社群軟體上的好友，或是宣揚虛假投資訊息等方式。

(3) 假冒名人詐欺(Celebrity impersonation)：犯罪者假冒社會知名賢達，藉由網路社群媒體與被害人帳號進行互動，再以虛假投資訊息讓被害人了解投資加密貨幣或其他可能的投資機會，藉此信任而陷入虛假投資詐欺。

(4) 房地產詐欺(Real estate professionals)：犯罪者聯繫房地產仲介，提出以現金或加密貨幣或其他方式來購買房產。仲介人員一旦受騙，犯罪者再以虛假投資機會轉知給房產仲介，號稱這些投資帳號以及機會價值高達數百萬美金，以引誘這些房產仲介或者其他被害人參與投資活動。

(5) 求職詐騙(Employment)：被害人在網上申請企業的虛假職位。然而被害人得到的不是工作，而是投資建議。該投資具有詐欺性，旨在向被害人詐取盡可能多的資金。

3. 假客服詐欺[7](Tech support)

IC3 受理假客服詐欺案件主要有兩種型態，在 2022 年時總共受理 44,092 件，其中技術/客戶服務詐欺計 32,534 件，而冒充政府之詐欺（11,554 件），造成被害人之財

[7] 同註 5。頁 15。

損超過 10 億美金，目前仍呈現增加的趨勢。根據 IC3 分析，20 歲以下僅占 0.3%；20-29 歲占 4%；30-39 歲占 4%；40-49 歲占 5%；50-59 歲占 9%；60 歲以上占 69%；遺漏值占 8%。換言之，假客服絕大多數以老年人為目標，造成毀滅性的影響。幾乎一半的被害人年齡超過 60 歲（占 46%），遭受 69%的損失（超過 7.24 億美金）。而這些詐欺行為主要來自南亞（尤其是印度）的假客服。為因應日益增加的被害情況，美國司法部(Department of Justice)和 FBI 正在與新德里中央調查局和印度當地各邦等印度執法部門合作，打擊網路金融犯罪和跨國假客服詐欺。此次合作已交換美國假客服詐欺被害人的筆錄，用於針對犯罪嫌疑人的執法程序。2022 年，在美國執法部門的協助下，印度執法部門對涉嫌參與該網路金融犯罪和全球假客服詐欺的個人進行多次搜索、查緝、扣押和逮捕。

4. 勒索軟體[8](Ransomware)

在 2023 年，IC3 收到 2,825 件勒索軟體的詐欺案件報案，整體財損超過 5,960 萬美元。勒索軟體是一種惡意軟體，勒索軟體多半透過網路釣魚電子郵件、遠端桌面協定(Remote Desktop Protocol,RDP)，當該軟體被下載至電腦，或者藉由遠端遙控來操作被害人電腦，網路犯罪者將電腦上的資料予以加密，沒有密碼解鎖將無法讀取相關檔案。該軟體除了針對網路進行加密之外，會從電腦系統中竊取重要資料並加密扣押，若不支付贖金，電腦中重要檔案將無法使用。其中值得注意的是有 1,193 件報案，來自重要公務基礎建設部門單位，受到勒索軟體攻擊的影響。約莫有 16 個公務基礎建設部門受到勒索軟體攻擊，當中 14 個部門至少有 1 名成員受到贖金軟體攻擊。

5. 假冒身分詐欺[9] (Identity Theft)

根據美國身份盜竊研究中心（Identity Theft Research Center, ITRC）年度報告，2024

[8] 同註 5。頁 13。

[9] ITRC 2024 Annual Report. Retrieved from: https://www.idtheftcenter.org/publication/2024-itrc-annual-report/ 最後瀏覽日：2025 年 3 月 25 日。

年的所發生身分盜竊的報案數是自 2005 年 ITRC 開始統計以來的最高數量，比 2023 年的記錄僅下降了一個百分點，其中包括 1.35 兆次的通報量。聯邦貿易委員會（The Federal Trade Commission, FTC）消費吹哨者網站在 2024 年共收到了 647 萬次報案，其中 40％是詐欺類別，而身份盜竊的占 18％。盜刷信用卡的 43.9％，最常見的就是網路購物和付款帳戶的詐欺行為，還有透過電子郵件和社交媒體盜用身分的詐欺行為。ITRC 2024 的年度報告中指出，身分盜竊詐欺多以商業銀行和保險業遭受不明網路攻擊最嚴重的產業，緊隨其後的是醫療保健、專業服務、製造業和科技，這些大型企業擁有最多的個人資料，透過駭入這些企業來取得個人資料，進而奪取他人個資，再假冒他人身分進行詐欺犯罪。

(二)美國聯邦打擊電信網路詐欺政策

由於美國目前電信網路詐欺犯罪在近年來躍升成為嚴重的犯罪樣態之一，因此美國政府在面對電信網路詐欺的打擊與預防上，制定了相當多的政策與實務手段。從打擊電信網路詐欺犯罪的政策架構談起，從法律面來著手進行全面性的電信詐欺犯罪法律制定與修法。從表 9 來看，美國對於打擊電信網路詐欺的相關法案有六個，針對電信網路詐欺類型而逐一修訂，企圖將新型的電信通訊與網路的詐欺手法納入法律監管範圍，提供偵查權限，鼓勵公私部門合作，強化各種可能的資源來共同打擊電信網路詐欺犯罪。

表 11 美國打擊電信網路詐欺相關法案表

法案	防詐欺重點內容	所屬機構單位
通信法案（Communications Act）	禁止自動撥號、預錄語音；禁止來電顯示偽冒；建立 Do Not Call 機制	聯邦通信委員會（FCC）
	禁止未經授權更換電信服務提供商（Slamming）	
	限制電信業者濫用用戶資料（如 CPNI），防止身份盜用或釣魚詐騙	
TRACED Act	要求實施 SHAKEN/STIR；強化對 Robocalls 的罰則與執法時效	FCC、司法部、電信業者
電話消費者保護法（TCPA）	限制廣告電話、傳真；擴展 §227 執行效力；允許消費者提告	FCC、法院系統
電腦詐欺與濫用法（CFAA）	處罰未經授權存取電腦系統（網釣、假冒網站、社交工程攻擊等）	FBI、司法部
身份盜竊與假冒法（ITADA）	禁止使用他人身份資料進行詐欺（含 SIM 卡詐騙、社會工程詐騙等）	FBI、司法部
RAY BAUM'S Act（補充通信法案）	要求即時處理詐騙電話投訴；加強緊急通訊定位技術	FCC、緊急應變系統

資料來源：本研究整理

1. 相關法律的制定與歷程

① 《通信法》（Communications Act）

通信法的立法起源於 1930 年代，當時無線通訊的普及率以及使用率快速成長下，造成無電線的頻譜混亂與干擾，缺乏統一管理與混亂，當時雖然建立《Radio Act》法案來解決頻道干擾與混亂問題，但卻沒有針對當時的廣播，與興起的電信有線通訊。當時美國的新政（New Deal）認為政府需要一個能整合「無線廣播」、「電話」、「電報」等各種通訊形式的綜合法案，因此在 1934 年通過《通信法》（Communications Act）。也因為該法案的通過而成立成立聯邦通訊委員會(Federal Communications Commission, FCC)，統一監管電信、電報、無線廣播等通訊方法，讓 FCC 能夠依據當時通訊技術制定技術標準、核發使用執照，而這部法案的基本架構至今仍是美國通信法律與政策的基

石(Winseck, 2017)。

從美國的法律來看對抗電信網路詐欺犯罪，1934 年的《通信法》（Communications Act）結合了電話，電報和無線電通信的聯邦法規。透過聯邦通信委員會（FCC）來監督和規範這些行業。該項法案會定期更新，以添加管理新通信技術的規定，例如廣播，有線電視和衛星電視(Grabosky & Smith, 2003)。《通信法》雖然是一部規範美國電話，電報，電視和無線電通信的法案，更重要的是政府授權聯邦通信委員會（FCC）來監管電信產業，同時對通信系統的使用規範了更詳細的法規和監督。然《通信法案》本身並非「刑法性質」的法律，但卻能夠提供政府對於電信業務的監管架構。

當中對於打擊電信網路詐欺最關鍵的就是，防止不當使用通信設備，像是機器人 robocalls 與詐騙電話相關的犯罪行為。第 227 條（Section 227）當中規範，禁止未經同意使用自動撥號系統或預錄語音向住宅或手機撥打商業性質的電話。還有禁止用來電顯示欺騙（Caller ID spoofing）的詐欺行為。並且建立「全國拒絕來電登記系統」（Do Not Call Registry）。其次是第 258 條（Section 258），明文禁止在未經消費者授權下，不能隨意更改其長途或本地電信服務商。第 222 條（Section 222）立法用意在保護用戶個人資料、通訊記錄不被濫用或詐騙集團所利用。上述兩個法條皆為防止業者濫用客戶資料而讓詐騙集團有機可乘來進行電信商的轉換而難以追查。

② 《電話機器人濫用刑事執行與威懾法案》（Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, TRACED Act/2019）

第二個與打擊電信網路詐欺犯罪的法律為《電話機器人濫用刑事執行與威懾法案》（TRACED Act）。該法案要求電信公司實施 SHAKEN 和 STIR 呼叫驗證技術(Tiwari & Singh, 2020)，SHAKEN 和 STIR 是增強電話通訊安全性的技術，特別是針對防範電話詐騙和假冒來電的問題。SHAKEN 是一種標記驗證技術，確保來電者的身份是經過認證的。當電話訊號發送時，電信業者會生成一個包含撥號者身份資訊和其他相關數據的數位簽名，收話者的電信業者可以利用這個簽名來驗證撥號者的身份，確保該來電的真實

性。STIR 是 SHAKEN 技術的基礎，用來建立管理撥號者身份的安全性，確保通話過程中的身份信息不會被篡改。這兩項技術的結合增強了電話通訊安全性，有效地識別並攔截偽裝來電，減少電話詐騙的風險，同時提高電信用戶對來電的信任度。

其次，TRACED Act 增加執法者的權限，聯邦通信委員會（FCC）能夠擁有更大的權力來追查並懲罰那些從事電話詐騙的個人與企業。首先是刑事處分[10]，對於從事電話詐騙的個人或企業，將會面臨刑事起訴。違法者可能會因為詐欺行為而被判處重罪，處以高額罰金，甚至監禁。第二是民事罰款，聯邦通信委員會對違反規定的詐騙者裁罰民事罰金，罰款的金額可根據違法行為的嚴重程度而定。第三則是加強執法權限，FCC 將擁有更大的權力來追查和懲罰從事電話詐騙的行為者，並提高執法效率，特別是在涉及跨州或國際的詐騙行為中。第四則是受害者賠償，受害者能夠得到法律支持並對犯罪者進行賠償(Hunsinger & Sen, 2020)。

③ 電話消費者保護法（Telephone Consumer Protection Act）

電話消費者保護法(TCPA)是美國國會在 1991 年通過的電信消費者相關法案。1980 年代末，自動撥號與預錄語音技術（robocalls）開始被廣泛運用，讓企業能在短時間內大量撥打廣告電話進行市場銷售。然而當時美國民眾抱怨來電頻繁且無法拒接，使得家庭電話被長時間佔線而錯失重要來電，且相關廣告電話消費者卻無法退出或選擇「不被打擾」的選項，當時傳真機還會收到未經同意的傳真廣告（junk faxes）。後續在 2003 年成立全國「Do Not Call」名單，讓消費者可主動登記，避免接到行銷來電。2012 年新增「書面同意」規定，使用自動撥號器與預錄語音向手機撥打行銷電話，必須取得受話者書面同意。在 2015 年時，FCC 進一步明確「autodialer」定義與責任，對於消費者應主動封鎖可疑號碼，擴大消費者保護範圍(U.S. Congress, 1991)。

[10] Federal Trade Commission. (2020). **Robocalls and Telemarketing Scams.** Retrieved from https://www.consumer.ftc.gov/articles/what-know-about-robocalls 最後瀏覽日：2025 年 2 月 19 日

第 227 條的條文內容，催生了《電話消費者保護法》[11]（Telephone Consumer Protection Act, TCPA, 1991），此法案立法目的是為了保護消費者免於詐騙電話的騷擾，立法之初係針對透過電信的廣告與行銷行為，然而該法案對於打擊電信詐欺起了關鍵作用。第一個是保護消費者隱私，法案內容限制企業與個人透過自動化系統濫發未經請求的來電或傳真。第二個是建立消費者同意制度（Prior Consent），法案要求電信業者或個人取得明確同意，才能撥打廣告性質或自動撥號的電話。第三個則是抑制騷擾與詐騙性來電，立法限制相關技術的濫用以及賦予消費者對於違法的電信業者擁有民事求償權，此舉將讓電信業者對於詐騙電話的過濾更加注意，減少電信網路詐欺與被害人接觸，對於自動撥號系統和錄音語音的使用有相當程度的限制，進一步對未經同意撥打廣告電話者可施以罰金(Shiyang, 2023)。由於電信網路詐欺犯罪集團常利用自動系統進行大量詐騙電話撥打（robocall），TCPA 限制這類來電對於技術面防堵有所助益。此外，電信詐騙經常透過錄音方式(Robovoice)來假冒政府或銀行，作為與受害者的第一類接觸，因此 TCPA 禁止這類未經同意的通話。再者許多受害者係藉由電信簡訊(SMS)收到相關虛假訊息，像是假冒送貨通知、獎金領取或中獎通知等連結，TCPA 將這類商業簡訊納入限制，亦即未經同意，不得讓消費者接到此類訊息。以下是與打擊電信詐欺相關法條的說明。

§ 227(b)(1)(A)：禁止未經同意使用自動電話撥號系統（ATDS）或預錄語音來電至行動電話、尋呼機或其他類似設備。這條是 TCPA 的核心條文之一，直接禁止企業或個人未經允許使用機器自動撥號或錄音來電。許多詐騙集團會使用自動撥號機大量撥打詐騙語音。可有效防止詐騙集團用自動語音冒充銀行、政府、醫療單位進行恐嚇或詐騙。§ 227(b)(1)(B)：禁止未經明確同意，使用預錄語音撥打住宅電話。限制企業以機器語音撥打廣告或通知到家用電話，除非事先取得明確同意。可防止詐騙電話冒充如 IRS、社保機構等政府單位對家庭成員進行誘騙。§ 227(b)(1)(C)：禁止未經許可的商業傳真訊息。

[11] Telephone Consumer Protection Act 47 U.S.C. § 227. Retrieve from: https://www.govinfo.gov/app/details/USCODE-2023-title47/USCODE-2023-title47-chap5-subchapII-partI-sec227/summary 最後瀏覽日：2025 年 2 月 19 日

..

防止利用傳真向企業或個人傳送未經請求的廣告或詐騙性文件。過去詐騙手法包括偽造「付款催款單」、「假合約」，透過傳真詐騙中小企業。§227(c)(1)-(4)：授權 FCC 建立「Do Not Call Registry」（拒接來電名單）制度。建立國家級的拒接名單，消費者可登記，禁止企業行銷或促銷來電。提供法律依據讓民眾能防範未經請求的來電，也可作為辨識詐騙來源的依據。§227(c)(5)：賦予消費者民事訴訟權，針對違規來電求償。消費者若接到違反 TCPA 的來電（如自動撥號未經許可），可對主體提告並索賠每通來電 $500（故意者為$1,500）。提供受害者法律武器對詐騙主體或相關企業提起訴訟，形成威嚇作用。§227(d)：規範電話設備須顯示正確來電資訊，並禁止匿名自動撥號。要求通訊設備具備來電識別功能，並限制設備未經授權撥號功能。可避免「未知號碼」或「空號」詐騙的來電進入用戶系統。

④ 《電腦詐欺與濫用法》（Computer Fraud and Abuse Act, CFAA）

第三個是《電腦詐欺與濫用法》（CFAA）。是美國於 1986 年通過的一項法案，最主要目的是打擊電腦和網路犯罪。雖然 CFAA 多微電腦相關的犯罪行為，然而目前電腦已進入電信與網路的年代，因此法案的相關規範對於電信網路詐欺具有重大指標意義。首先是第 1030 條(a)(1)明確規定針對未授權方式存取或操控電腦系統的行為係屬違法行為，可適用於網路釣魚與假網站詐騙手法，如果詐騙行為涉及這些特定類型的系統，則所面臨的懲罰會更加嚴厲。第 1030 條(a)(2) 涵蓋了對網站上的各種資料的非法盜竊行為之規範，用於詐騙集團試圖以駭客或其他方式竊取或讀取受保護的個人資料，盜竊後遂行犯罪，如果詐欺行為對個人或企業造成了經濟損失，會加重其刑。第 1030 條(a)(4)則針對使用電腦來進行詐欺的行為加以規範。此條款明文規定，任何使用電腦或網路進行的非法獲取金錢或財產詐騙行為，都屬於犯罪之範疇，倘若詐騙金額超過 5,000 美元，則會被視為加重情節，將面臨最高 5 年的監禁和最高$250,000 美元的罰金。。第 1030 條(a)(5)則是涉及對電腦系統或資料的損害行為係屬違法犯罪，此法條係涵蓋因詐欺犯罪行為故意對電腦系統造成資料或硬體損害之行為，做嚴格禁止。更重要的是第 1030 條(b)，該法條為檢警執法調查中提供了查緝犯罪時所需的權限，包括執行搜索令和逮捕令，

這對打擊電信網路詐欺至關重要，同時更規範若重複涉入違法詐欺犯罪行為，將面臨更長的監禁和更高的罰金。

⑤ 《身份盜竊與假冒法》（Identity Theft and Assumption Deterrence Act）

《身份盜竊與假冒法》(ITADA）於 1998 年通過，旨在打擊身份盜竊及相關的詐騙行為，對於假冒身份進行詐欺犯罪行為罰予刑事責任，對於目前電信網路詐欺常見的社交軟體或交友詐騙、SIM 卡詐騙等，起了關鍵作用。首先此法案對於身分盜竊建立明確性的定義：「將任何非法使用他人身份信息以獲取財務利益的行為視為犯罪[12]。」這一點對於打擊利用電信網路進行的詐騙行為至關重要，因為很多電信詐騙都涉及身份的濫用。第二，此法案明訂對身份盜竊的刑事責任，§1028(a)明定盜竊他人身分者將面臨最高 5 年的監禁和高額罰金。這為執法機構提供了強有力的法律工具，以追訴從事電信網路詐騙的犯罪行為者，給予相當程度的嚇阻作用。第三，§1028(b)：對於多次身份盜竊或涉及大量受害者的案件施加更重的刑罰。由於詐欺犯罪所得巨大，許多犯罪者會重複涉入詐欺犯罪，難有嚇阻作用，該條款允許施加更嚴重的刑罰，包括更長的監禁期限和更高的罰金。第四，ITADA 也強調了保護消費者的必要性，要求金融機構和商業實體在處理個人信息時採取適當的安全措施。這有助於減少因身份盜竊而導致的電信網路詐騙情況。§1028(c)正是對於上述保護受害者身分資料之必要性所訂定之法條，包括提供法律救濟和補救措施。第五，§1028(d)則是對於聯合查緝給予重大的法律支持，該法案促進了聯邦、州和地方執法機構之間的協作，這有助於更有效地打擊身份盜竊和電信詐騙。透過信息共享和聯合調查，執法機構能夠更快速地定位和追捕犯罪嫌疑人。

具體來說，聯合查緝的具體作為有幾個面向，首先是犯罪相關的資訊共享，聯邦與州之間的執法機構建立訊息共享的機制，以便在調查身份盜竊案件時能夠快速獲取相關數據和證據。包括分享有關可疑活動的報告、受害者資訊以及犯罪嫌疑人的資料。其次

[12] U.S. Code. (n.d.). *18 U.S.C. § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information.* Retrieved from https://www.law.cornell.edu/uscode/text/18/1028

是聯合調查，聯邦、州和地方警察這些不同層級的執法機構，依法組成聯合調查小組，集中所有打擊犯罪資源，提升調查效率才能有效打擊電信網路詐欺。接著是州政府間的協同運作，電信網路詐欺多半為跨州犯罪，雖然非強制協作偵查，但鼓勵不同州的執法機構之間擴大聯合查緝力道，使得追查可疑的犯罪分子能愈加順利。再者是打擊詐欺策略與技術的專業培訓。電信網路詐欺是高科技的犯罪手法，打詐需要專業技能，此法案能確保並強化執法人員具備打詐所需的技能和知識。包括可疑的身份盜竊詐欺的資訊、證據採集的策略以及與其他機構合作的具體方法。最後則是公私部門的合作，金融機構多為私營企業，唯有公務執法機構與私立金融機構合作，分享信息和共享資源，才能提高防詐能力。像是金融機構對於可疑交易跡象的預警制度，後續金流的追蹤與流向，對於打詐與防詐具有相當大的助益。

⑥ 《RAY BAUM’S Act》

《RAY BAUM’S Act》是美國於 2018 年通過的重要電信法案，其全名為《Repack Airwaves Yielding Better Access for Users of Modern Services Act》。該法案的第 503 條款對打擊電信網路詐欺，特別是針對「來電顯示更改號碼（caller ID spoofing）」的詐騙電話，納入法律的監管範圍。RAY BAUM’S Act 為日益猖獗的電信網路詐欺犯罪，提供了相當堅毅地的法律後盾。聯邦通信委員會(FCC)透過 RAY BAUM’S Act 來強化國際打詐合作、同時推動電信相關技術驗證機制以及提升公眾防詐意識，將保護消費者、維護通訊網路的安全性和信任度納入法律所保護的範圍(FCC, 2019)。

首先是擴大「竄改來電顯示」的適用範圍擴大。RAY BAUM’S Act 修訂了《Truth in Caller ID Act of 2009》，當中第 503 條 Truth in Caller ID Modernization，明確禁止美國境內或境外者使用語音或簡訊服務，傳送誤導性來電資訊（Caller ID spoofing），包含所有 VoIP 服務與 SMS/MMS 簡訊等非傳統通訊工具。倘若其目的是詐騙或非法獲取利益，美國聯邦通信委員會（FCC）能夠根據此法案對來自海外的詐騙行為進行管制和執法。接著是立法將 SMS/MMS 訊息和非傳統語音服務，如一對多的 VoIP 服務納入監管範圍，填補了原有法律在這些通訊形式上的漏洞。第三是厚植國際合作與執法能力。第

601 條— Enforcement Jurisdiction Over Communications Fraud，給予聯邦通信委員會(FCC)與加拿大廣播電視暨電信委員會（CRTC）簽署了合作備忘錄的依據，並參與了「非請求通訊執法網絡（UCENet[13]）」等國際組織，透過各種可能的國際資源合作，打擊跨國電信詐欺行為。最後是加強消費者教育與防詐意識。根據第 502 條— Improving Coordination and Enforcement 法案規定，聯邦通信委員會(FCC)需與聯邦貿易委員會（FTC）合作，制定並定期更新消費者教育資料，幫助公眾識別和防範利用來電顯示偽冒進行的詐騙行為。

2. 執法機構角色與具體打詐手段

根據這麼多的法案來進行打擊電信網路詐欺犯罪，且法案範圍相當廣泛，整體來說美國打擊電信網路詐欺有幾個重要的執法機構，以下分別說明。

① 聯邦通信委員會(Federal Communications Commission)

聯邦通信委員會（FCC）規範電信業者與呼叫驗證技術的實施。對違規業者處以重罰（如大量傳送 robocalls）。對於打擊電信網路詐欺的有以下幾種重要作為，首先由 FCC 是主要規範電信的技術標準單位，因此由 FCC 來制定電信防詐規則，像是推動 STIR/SHAKEN 來電驗證技術，便是其中一項針對電信網路詐欺來電的規範技術。其次是建立自動撥號防範資料庫(Robocall Mitigation Database,RMD)，FCC 要求所有語音服務提供者提交其防範非法自動撥號的計劃，並在 RMD 中進行認證。提供者必須描述其採取的具體措施，包括務必實施 STIR/SHAKEN 或其他來電驗證技術，監控和封鎖可疑的來電流量，更重要的是根據法律的修正並於 10 天內更新資料且定期更新防詐策略，違者將可能面臨高達 10,000 美元的罰款(FCC, 2024)。

此外還有加強對第三方驗證的規範，授權電信業者主動封鎖可疑來電。為確保

[13] UCENet（Unsolicited Communications Enforcement Network）是一個國際合作網絡，致力於打擊垃圾訊息、詐騙電話、網路釣魚和其他形式的未經請求的電子通訊。該組織的目標是透過促進跨國執法合作、資訊共享和協調行動，增強全球消費者保護。資料來源：https://www.ucenet.org/who-we-are/

STIR/SHAKEN 驗證技術的的有效性，FCC 要求即使語音服務提供者委託第三方進行來電驗證，確保來電驗證的完整性，若沒有盡到完全責任，仍需對驗證結果負責。另外有鑑於 AI 的盛行，開始有詐騙集團利用 AI 生成技術來進行詐欺犯罪，因此 FCC 在 2024 年發布禁止在未經同意的情況下，使用人工智慧（AI）生成的語音進行自動撥號之命令。此舉是為了防止詐騙者利用 AI 技術模仿知名人士的聲音，進行詐騙或干擾選舉等行為。違反者可能面臨高額罰款。

最後為了能夠加大法律的嚇阻效果，《TRACED Act》給了 FCC 更大的法律權限，可與其他執法機構合作，追查跨境詐騙行為，亦可開罰騷擾電話與來電竄改號碼的電信業者，要求企業遵守 TCPA 之相關規範，尤其是與電信網路詐欺相關的電信業務，像是違法的行銷電話，若經查核確實，將依法罰款。也設立「消費者投訴中心」，讓民眾舉報詐騙來電與簡訊，能夠即使獲得詐騙來電簡訊的第一手消息，同時更新 RMD 資料庫並且對於該類相關的來電撥號予以禁止。

② 聯邦貿易委員會(Federal Trade Commission, FTC) 聯邦貿易委員會（FTC）

首先是執行「National Do Not Call Registry」拒接名單制度，該制度從 2003 年正式啟動，主要是允許消費者能夠登記不希望接到行銷來電的電話號碼，電信業者與民間企業必須遵守相關規定，不得主動撥打促銷電話給名單上的用戶，倘若違反該規定，FTC 有權可對公司提起行政執法與民事罰款。FTC 能夠對於假冒電話銷售與身份盜用詐騙進行調查，《FTC 法》當中 15 U.S.C. §§ 41–58 規定，對欺騙性廣告、不當促銷、網路釣魚等違法行為可協助提起訴訟來要求企業繳納罰金，並擔負起被害人賠償的責任。FTC 為 UCENet 國際組織的會員，透過該組織能夠參與國際間打擊垃圾郵件、詐騙電話、簡訊詐騙的合作行動，目前 FTC 也與加拿大與英國簽訂合作備忘錄(MOU)，共同調查跨境詐騙案件，同時協助凍結海外詐騙犯罪收益，打擊跨國詐騙行為(FTC, 2023)。

FTC 也與美國商業改善局（Better Business Bureau, BBB）合作，由 BBB 管理 Scam Tracker 平台，該平台能讓美國民眾第一時間內舉報詐欺行為，舉報內容包括遇到的詐騙

情境、詐騙者的聯絡方式、詐騙手法、損失金錢、發生的日期與地點。該平台也建立詐騙犯罪熱點地圖(View Scam Tracker Map) ，用互動地圖模式，查看最近在哪些地區出現哪些詐騙。也能夠分享個人遭詐的經歷，相關資料能讓美國大眾查詢最新的詐騙活動趨勢，相關資料將整理年度或季度趨勢報告，亦能幫助執法機構與政府來制定追蹤詐騙模式。

③ 美國司法部(Department of Justice, DOJ)

美國司法部對於打詐相當重視，多以刑事起訴重大電信與網路詐欺案件。像是根據美國聯邦法典 18 U.S.C. § 1343 電信詐欺，便是針對電信詐欺的相關刑事法條，此條款針對利用電子通訊，如利用電信、網路進行詐騙的行為，最高可處 20 年徒刑。18 U.S.C. § 1341 是郵件詐欺，係針對利用郵寄系統進行詐騙的行為，最高可處 20 年徒刑。18 U.S.C. § 1029 是與存取裝置相關的詐欺行為，涵蓋未經授權使用信用卡、電信設備等進行詐騙的行為。18 U.S.C. § 1030 則是與電腦相關的詐欺行為，是針對未經授權存取保護電腦系統以進行詐騙的行為。

而為了加大法律的威懾程度，可以凍結詐騙資金、沒收犯罪所得。18 U.S.C. § 982 是刑事沒收制度（Criminal Forfeiture），法院可命令被定罪者沒收與犯罪有關的財產，這當然包括因為詐騙而獲取的犯罪所得。18 U.S.C. § 1956 是針對洗錢所訂的法律（Money Laundering），該法條針對將非法獲取的犯罪所得，透過多元的洗錢的行為來進行起訴，並可沒收相關財產。比較特別的是司法部制定了資產沒收政策手冊（Asset Forfeiture Policy Manual），提供檢察官和執法人員關於資產沒收的政策和程序指導。該手冊由 DOJ 的洗錢與資產回收科（Money Laundering and Asset Recovery Section, MLARS）所編撰，旨在為聯邦檢察官、執法人員及相關專業人士提供資產沒收程序的政策指南。該手冊的指導原則促進聯邦、州、地方、部落及國際執法機構之間的合作，在聯邦法律允許的情況下，回收資產以補償受害者。當中的第二章是查封與限制措施（Seizure and Restraint），規範行政沒收程序中，當有人對資產提出主張時，政府需在 90 天內採取行動，如取得刑事或雙重用途的查封令、根據 21 U.S.C. § 853(e) 的限制令，或其他授權保留資產的

命令。第 14 章的內容提到受害者詐騙案件中的建構信託(Constructive Trusts in Multiple-Victim Fraud Cases），目的是希望能在涉及多名受害者的詐騙案件中，如何透過建構信託的方式，確保受害者能夠從沒收的資產中獲得補償。當中資產沒收應在法律授權的範圍內進行，根據 21 U.S.C. § 853(g)，在法院發出沒收命令後，檢察總長有權查封所有被命令沒收的財產。

司法部也會和各州檢察總長辦公室(State Attorneys General, AGs)共同合作打擊電信網路詐欺。美國各州檢察總長（AGs）在打擊電話詐騙與網路釣魚方面，可根據各自州內的消費者保護法（Unfair and Deceptive Acts and Practices, UDAP）起訴，像是馬里蘭州檢察總長辦公室的刑事調查部門，就包含負責調查和起訴白領犯罪、網路詐騙等多種犯罪行為[14]。此外 AGs 也會與聯邦機構協作，根據 2021 年所通過的《FTC 協作法案》（FTC Collaboration Act），聯邦貿易委員會（FTC）與各州檢察總長合作，分享詐騙資訊、共同執法打擊詐騙和不公平商業行為。最著名的應當就屬 Avid Telecom 公司的起訴案件，該案件是由 48 個州與哥倫比亞特區的檢察總長組成的「反自動撥號多州訴訟任務編排小組」(Anti-Robocall Multistate Litigation Task Force)，對位於亞利桑那州的 VoIP 服務供應商 Avid Telecom 及其負責人 Michael D. Lansky 和副總裁 Stacey S. Reeves 提起聯邦訴訟，指控其協助傳送超過 245 億通非法自動撥號電話，其中約 75 億通撥打至「全國拒接來電名單」（National Do Not Call Registry）上的號碼[15]。

④ 美國郵政稽查局(United States Postal Inspection Service, USPIS)

美國郵政稽查局（USPIS）是專責保護郵政系統避免遭受非法之危害，尤其近年來電信網路詐欺犯罪，經常透過購物詐騙與身分盜竊的詐欺方式橫行，因此加入打擊詐欺

[14] Office of the Maryland Attorney General. *About the Office of the Maryland Attorney General*. https://www.marylandattorneygeneral.gov/Pages/About.aspx 最後瀏覽日：2025 年 3 月 19 日

[15] Office of the Attorney General of Arizona. (2024, May 9). *Court Rejects Avid Telecom's Attempts to Dismiss Illegal Robocalls Case*. https://www.azag.gov/press-release/court-rejects-avid-telecoms-attempts-dismiss-illegal-robocalls-case 最後瀏覽日：2025 年 3 月 20 日

的行列。根據聯邦法典 18 U.S.C. § 1341 的郵件詐欺、§ 1343 的電信詐欺、18 U.S.C. § 1028 身份盜竊詐欺以及 18 U.S.C. § 1029 的存取裝置詐騙，USPIS 有權進行調查、逮捕並起訴這些涉及郵政系統的詐欺行為。尤其是網路購物、網路犯罪與身分盜竊的詐騙容易結合郵政系統為之[16]。當然郵政稽查局因應跨國詐欺案件增加而開始與其他國際機構合作，美國郵政調查局（USPIS）曾與加拿大皇家騎警（RCMP）成立打擊跨境詐騙的聯合工作小組，從 2000 年開始便進行合作，從雙方信息共享，確保能快速獲取關於可疑活動、犯罪嫌疑人及其手法的最新信息。進一部能夠合作跨境調查，追踪和打擊在兩國之間進行的詐騙活動，彼此也能夠提供專業培訓資源，以提高執法官員在識別和調查跨境詐騙方面的能力(Smith, 2022) 。

⑤ 聯邦調查局網路犯罪中心(FBI–Internet Crime Complaint Center, IC3)

聯邦調查局（FBI）轄下之「網路犯罪投訴中心」（IC3），負責網路犯罪相關訊息之接收和分析，協調對跨國網路詐騙集團的調查與打擊。最快速能夠獲得相關詐欺犯罪資訊是由被害人報案得知，因此 IC3 建立線上網路舉報平台供民眾舉報各類網路犯罪，當中包含詐欺類型的犯罪，包括網路釣魚、商業電郵詐騙、投資詐騙、身份盜用等。IC3 亦每年會針對相關資訊進行分析並製作成年度犯罪報告《Internet Crime Report》，分析當年度的網路犯罪趨勢。

IC3 對於打擊電信網路詐騙有其一套完整且系統性的重要策略模式，從犯罪預防、嫌疑資訊偵測、犯罪活動追蹤與偵查、犯罪者資產凍結、跨部門合作等。首先獲得犯罪資訊是從處理網路犯罪舉報開始，除了舉報平台讓美國大眾能隨時舉報各類網路詐騙，接著將這些資訊加以收集，並進一步根據犯罪類型、金額損失、手法細節、犯罪來源 IP、支付工具等資訊進行分類統計。接著將相關舉辦案件根據案件嚴重程度進行即刻分流，像是金額龐大的詐騙屬於嚴重案件，將優先轉交 FBI Cyber Division 及地方執法單位跟

[16] United States Postal Inspection Service. *Report a crime*. Retrieved from https://www.uspis.gov/report 最後瀏覽日：2025 年 3 月 20 日

進。接著會進行龐大資料分析與詐騙模式追蹤（Data Analysis and Fraud Pattern Identification），大量的舉報案件將建立資料庫進行收集，並且將舉報資料標準化、結構化建檔，建立大型網路詐騙案件資料庫。緊接著著手進行資金追蹤與凍結行動，由資產追回小組(Recovery Asset Team, RAT)執法小組將因詐騙、洗錢及其他金融犯罪所獲得的非法資產進行追蹤，當詐騙案件涉及國際資金轉移且數量高於 50,000 美元，會趁著這些犯罪所得尚未移轉取出時，啟動追蹤與凍結程序，快速聯繫銀行與國際金融機構要求凍結款項。根據 2024 與 2025 年度報告，2023 年 IC3 啟動超過 3,000 件 FFKC 案件，凍結追回金額超過 5.38 億美元，成功率約 71%。2024 年則是啟動了 3,020 件資金凍結行動，涉及潛在損失金額達 8.484 億美元。其中，成功凍結的資金總額為 5.615 億美元，整體成功率約為 66%。

在部門合作部分，在美國境內與聯邦機構合作，如 FTC、FCC、USPIS 等協作分享情報。IC3 會與 FTC 透過其「消費者哨兵網絡」（Consumer Sentinel Network）收集的詐騙舉報，將類似的詐欺被害報案資訊，轉介給 IC3 的資產追回小組（RAT）來啟動資金追回凍結程序，以協助受害者追回詐騙資金。此外彼此分享可能的防詐手段以及教育宣導，將相關資訊共同在 FTC 與 IC3 的網頁上，發布防詐騙指南與警示，提升公眾對詐騙手法的認識。IC3 與與聯邦通信委員會（FCC）亦會共同合作，從打擊非法自動撥號電話著手，追蹤非法自動撥號電話系統來源和來電顯示竄改等詐欺行為，向上溯源來查緝。同時也會與美國郵政稽查局（USPIS）合作，對郵寄詐騙相關詐騙案件資訊了解後並進行調查。在國際合作上，與歐洲刑警組織(Europol)合作，最著名的像是 2015 年的聯合行動「Operation Shrouded Horizon」，FBI 與 Europol 合作，聯合 20 個國家的執法機構，成功瓦解了大型網路犯罪論壇 Darkode，逮捕了 70 名嫌疑人，起訴 12 人，打擊了跨國網路犯罪活動。另外與國際刑警組織（INTERPOL）的合作，則是針對資金流追蹤與凍結為主，INTERPOL 多協助 IC3 追蹤跨國詐騙資金流向，並協調各國執法機構凍結詐騙所得資金。2023 年的聯合行動「Operation HAECHI III」，NTERPOL 協調 31 個國家的執法機構，成功攔截了價值 1.3 億美元的詐騙資金，逮捕了 975 人，關閉了 2,800 個銀

行和虛擬資產帳戶，打擊了跨國網路詐騙活動(FBI,2025)。

最後 IC3 為了達到犯罪預防成效，積極的針對電信網路詐欺進行預警發布與相關預防的教育推廣。像是對於最新的詐欺犯罪手法進行揭露，像是新興詐騙手法的深偽技術詐騙，還有金額數量龐大的加密貨幣投資詐騙，都會定期在網站上發布安全警示。亦會在網路上提供防詐教育資源，包括企業詐騙防範指南、個人資料保護建議。為了擴大打擊量能，期望學界共同合作，會定期舉辦防詐網路研討會，並且深入社區推廣電信網路安全的議題講座。

3. 公私跨部門與國際合作

一、國內與國外的多元合作

聯邦貿易委員會（FTC）與聯邦通信委員會（FCC）於 2024 年簽署的合作備忘錄（MOU）主要是針對美國國內的合作，並未與其他國家共同簽署。該備忘錄旨在加強兩機構在消費者保護、網路詐騙及非法電信行為等方面的協作，特別是在非共同運營商活動上的執法權限，以及對 VoIP 服務提供商的監管。合作備忘錄雖然僅限於國內機構，不過 FTC 和 FCC 也跟許多國家的機構簽署了合作協議，以促進跨境執法合作和資訊共享，將合作的範圍擴大到了國際。包括與加拿大隱私專員辦公室（Office of the Privacy Commissioner of Canada）、英國資訊專員辦公室（Information Commissioner's Office）、新加坡資訊通信媒體發展局（Info-Communications Media Development Authority）、巴西國家電信局（Anatel）、羅馬尼亞國家通訊管理和規範局（ANCOM）、智利、哥倫比亞、墨西哥、秘魯、哥斯大黎加、多明尼加共和國和巴拿馬的消費者保護機構簽署了合作協議，致力於在隱私保護和資料安全執法方面的合作(FTC, 2024)。

二、資訊共享與執法協調

由於電信網路詐欺橫跨多部會之職責，因此部門間會共同推動打詐策略，像是從 2023 年開始的「打擊詐騙電話行動」（Operation Stop Scam Calls）是美國聯邦貿易委員會（FTC）與聯邦通信委員會（FCC） 共同發起的大規模執法行動，針對非法自動撥號

電話的打詐行動。這個活動的主要打擊對象是名單提供商（Lead Generators），這些公司透過虛假或模糊的方式收集消費者的聯絡資訊，並聲稱獲得了消費者的同意，將這些資訊出售給詐騙電話業者。第二個是 VoIP 服務提供商，這些提供網際網路語音通訊服務的公司，允許詐騙者利用其網路傳送大量非法電話。第三是非法電話行銷業者，直接進行詐騙電話行銷的個人或公司。FTC 針對涉嫌非法電話行銷的公司提起訴訟，指控這些公司違反《電話行銷銷售規則》（Telemarketing Sales Rule），非法收集並出售消費者資訊，協助詐騙電話行銷活動。FCC 則是同時間對 VoIP 服務提供商進行更嚴格的監管，強烈要求所有服務提供商應實施 STIR/SHAKEN 來電驗證技術，降地來電顯示竄改的詐欺案件量。

三、私營企業的參與與協作

美國無線通信與互聯網協會（CTIA）的成員企業在打擊電信詐騙方面，與 FCC 共同合作並積極部署多層次的防詐機制[17]。CTIA 成員的相關企業會採取多種措施來阻擋非法簡訊和詐騙電話，首先是網路上的封鎖，在網路進行識別並阻擋可疑的簡訊和來電。第二是提供用戶端下載應用程式來設定可疑來電與簡訊。第三則是與政府執法機構合作，與聯邦通信委員會（FCC）和聯邦貿易委員會（FTC）合作，將客戶所提供可疑的來電與簡訊分享。由於根據 FCC 的規定，所有電信業者若有提供語音服務，那麼電信業者必須繳交自動撥號的認證[18] (Robocall Mitigation Certification)，證明其已實施 STIR/SHAKEN 認證機制或其他詐騙防範措施。並且加入自動撥號的數據資料庫，若未在該資料庫中註冊的電信業者，其來電可能會被阻擋而無法發話。

---

[17] CTIA. *Fighting Robocalls*. Retrieved from https://www.ctia.org/fighting-robocalls 最後瀏覽日：2025 年 3 月 20 日。

[18] FCC 要求所有語音服務提供商必須向 FCC 證明自己已採取措施，來防止非法自動撥號透過他們的網路傳送。這個制度是《TRACED Act》法規中要求，目的是從源頭切斷詐騙電話的傳播。資料來源：*Robocall Mitigation Database and Certification*. Retrieved from https://www.fcc.gov/robocall-mitigation-database 最後瀏覽日：2025 年 3 月 20 日

(三)美國打擊電信網路詐欺困境

電信網路詐欺是透過電信服務與網路來誘騙受害者損失金錢、個人或機密資訊或造成其他損害。不管是案件量或是財損金額，都呈現上漲的趨勢。美國對於日趨嚴重的電信網路詐欺犯罪，FTC 、FCC 與全國多個聯邦和州執法合作夥伴一起展開“制止詐騙電話行動”，針對非法電信進行大規模的打擊，對人工智慧的新詐欺形式加以警告。同時加強反垃圾郵件執法，盡量涵蓋每個社區，降低詐騙訊息與被害者的接觸機會。美國政府整合政府部門與、非營利組織和學術機構，希望能夠全面將網路詐欺威脅消除殆盡。由於網路犯罪相當多元，因此網路空間與數位政策是美國政府首要提出的政策。由於網路世界自由、開放特性，因此安全的環境下使用數位技術滿足生活所需，網路安全、資料安全的前提下同時獲得教育和經濟機會，以推動包容性經濟成長，是美國政府極力推動的數位安全生活政策 (Cole, 2023; FTC, 2025)。為了推動網路空間的責任制度，美國建立網路安全與基礎設施安全局(Cybersecurity and Infrastructure Security Agency)來打擊網路釣魚和社群媒體詐欺，以互補式的網路安全和執法能力兩方面來著手。執法部門強化調查能量，查緝並逮捕和起訴犯罪人，國土安全部 (DHS) 與其他聯邦機構合作進行刑事調查，招募和培訓網路安全技術專家，瓦解網路詐欺犯罪分子的活動。美國特勤局設有電子犯罪特別工作小組，專注於識別和定位與詐欺相關犯罪的國際網路犯罪集團。特勤局網路情報部門直接協助逮捕跨國網路犯罪組織分子，更重要的是特勤局的國家電腦取證研究所，為執法人員、檢察官和法官提供網路培訓和訊息，以打擊網路詐欺(Fonseca, Moreira, & Guedes, 2023)。

這麼多的打擊電信詐欺犯罪的政策與手段，仍然遭遇到許多困境而有待解決。首先是技術演進與詐騙手法的快速變化，詐騙者持續利用先進技術，如 AI 語音合成與來電顯示竄改技術，使得傳統的防詐機制難以有效辨識與阻擋(Wang et al., 2023)。AI 生成語音的自然度極高，尤其透過深度學習（deep learning）訓練的語音合成技術，可以生成幾乎無差別的真實人聲，使得詐騙集團能模仿特定人物語氣、口音甚至講話風格，讓受害者更容易相信。此外 AI 不只能產生單一語音，而是能批量自動生成成千上萬通詐騙通

話。此時若搭配自動撥號系統，可以極短時間內攻擊大量目標，更可怕的是 AI 語音合成技術可以根據受害者的反應即時調整說話內容與語氣，此時搭配竄改來電顯示手法，被害者難以防範。(Hao, Wang & Smith, 2023)。

接著是執法與罰款執行的困難，雖然 FCC 對違法者開出高額罰款，但實際收回的金額極少，削弱了法律的嚇阻效果。主要還是因為違法者，在罰款裁定前就會將資產轉移、隱藏或洗錢到境外帳戶。再者許多非法自動撥號業者是空殼公司或以人頭名義登記，帳上幾乎無資產可扣押。其次就是跨境問題的難以追溯，很多非法自動撥號電話的來源在美國以外地區，美國法院的判決無法在他國執行，尚須經過複雜的國際司法互助程序，才有可能進行裁罰。而且這類罰款屬於行政裁罰（civil forfeiture），係屬「民事性質」，執行優先度低於刑事案件，且執行資產扣押時，通常排在刑事罰金、稅務債務、優先擔保債權之後。許多詐騙集團為了躲避法律的嚴格規範，設立的公司行號常用虛假身份或是人頭來申請，不然就是把公司結構複雜化，像是多層控股公司、境外公司等，使得政府查緝實際負責人相當困難，即使判決生效，也無法對金主執行扣押(Lyons, 2021)。

再來是法律修訂與技術革新難以整合，隨著數位社會的發展，電信詐欺呈現出智能化、跨境化和隱蔽化的特點，現行刑法跟不上犯罪腳步。Zhang(2024)研究指出，僅依靠法律手段難以有效遏制此類犯罪，建議加強法律框架與類似大數據和人工智慧的技術手段整合，以提高調查和預防能力。不過即使法律跟上技術的革新，另一個挑戰隨即而來。政府機關之間的協調問題要先解決，不同政府機關，像是 FCC、FTC、DOJ、FBI 等都有打擊電信詐騙的權責，但它們的管轄範圍、優先事項、資源配置各不相同，本位主義的作祟下，形成多頭馬車各自為政。即便規範公私部門的協調合作，但並非所有業者都願意與政府合作，除了大型電信公司有技術部門，小型電信話務提供商根本沒有技術能力來配合，即便引進認證系統，常常為了節省成本或害怕得罪客戶而不願遵守，有些 VoIP 業者明知道流量來源可疑，但仍提供服務。

最後是跨國執法協調問題難以解決，美國境內大量詐騙電話來自國外，尤其是使用低價 VoIP 服務，這些電信話務提供商都來自加勒比海、東南亞等較落後的國家，美國

對境外犯罪者沒有直接執法權，即使簽訂合作協議，跨國調查與資產凍結程序冗長、繁瑣，常常錯失最佳追查時機。

二、 歐盟

(一)歐盟電信網路詐欺現況

歐盟目前並未對「電信網路詐欺」建立一致性的官方定義。然而，歐盟在相關領域的立法中，對於「詐欺」（fraud）有廣泛的定義，涵蓋了多種形式的詐欺行為，包括與電信和網路相關的詐欺。根據 1995 年所制定的《保護歐洲共同體財政利益公約》（PFI Convention）第 1 條(b)，其中提到：「任何與使用或提供虛假、不正確或不完整的陳述或文件有關的故意行為，或違反特定義務而不披露資訊，或將資金用於原本未授權的目的，從而導致歐洲共同體的預算或由其管理的預算遭受損失的行為。」此定義強調行為的「故意性」和對歐盟財政利益的損害，可視為是歐盟對詐欺犯罪的定義(EU, 1995)。

雖然歐盟未對「電信網路詐欺」進行明確定義，但歐盟 2019 年之 713 號指令當中提到打擊非現金支付手段的詐欺和偽造行為，其中涵蓋了透過網路或電信手段進行的詐欺行為。第二版的支付服務指令（PSD2），PSD2 要求支付服務提供者必須回報詐欺事件，並強化了對電子支付安全性的要求，間接涉及了與電信和網路相關的詐欺行為。而 2023 年所通過的第三版支付服務指令(PSD3)，PSD3 強化歐盟電子、數位支付和金融服務規範，加強現有的法律框架，擴大金融資料的存取範圍，建立更適合歐盟的支付架構，保護消費者權益和個資，建立更好的金融支付環境(European Commission, 2023)。

歐盟許多國家也對電信網路詐欺提出明確的定義，如下表所示：

表 12 歐洲各國對電信網路詐欺的定義

國家	電信網路詐欺定義
法國	法國刑法第 313-1 條將詐欺定義為:「以欺騙手段使他人交付財物、提供服務或放棄合法權利的行為」。此定義涵蓋了透過電信手段(如

	電話、電子郵件、簡訊等）進行的詐欺行為[19]。
德國	德國刑法第 263 條將詐欺定義為：「故意以欺騙手段使他人產生錯誤認知，從而導致財產損失的行為」。此定義適用於透過電信方式進行的詐欺，例如電話詐騙、網路釣魚等[20]。
義大利	義大利刑法第 640 條將詐欺定義為：「以欺騙手段使他人產生錯誤認知，從而導致財產損失的行為」。此定義涵蓋了透過電信手段進行的詐欺，如電話詐騙、簡訊詐騙等[21]。
西班牙	西班牙刑法第 248 條將詐欺定義為：「以欺騙手段使他人交付財物、提供服務或放棄合法權利的行為」。此定義適用於透過電信方式進行的詐欺，例如電話詐騙、網路詐騙等[22]。

[19]L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Retrieved from: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418192 最後瀏覽：2025 年 3 月 25 日。

[20] Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. Retrieved from: https://www.gesetze-im-internet.de/stgb/__263.html 最後瀏覽日：2025 年 3 月 25 日。

[21]Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549:

1. se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare;
2. se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità; 2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5). Retrieved from: https://www.gazzettaufficiale.it/ 最後瀏覽日：2025 年 3 月 25 日。

[22] 1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación

荷蘭	荷蘭刑法第 326 條將詐欺定義為：「以欺騙手段使他人交付財物或提供服務的行為」。此定義涵蓋了透過電信手段進行的詐欺，如電

informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que, utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realizaren operaciones de cualquier clase en perjuicio de su titular o de un tercero. Retrieved from: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444 最後瀏覽日：2025 年 3 月 25 日。

	話詐騙、網路詐騙等[23]。

資料來源：本研究整理

[23] Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het verlenen van een dienst, tot het ter beschikking stellen van gegevens, tot het aangaan van een schuld of tot het teniet doen van een inschuld, wordt, als schuldig aan oplichting, gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie. Retrieved from: https://wetten.overheid.nl/BWBR0001854/2024-01-01 最後瀏覽日：2025 年 3 月 25 日。

歐盟反詐欺局[24](European Anti-Fraud Office, OLAF) 指出，歐盟詐欺犯罪有多種模式(表 11)，包括共謀、操縱採購程序、虛報 帳務、逃稅、走私和偽造。雖然 OLAF 沒有專門針對「電信網路詐騙」的分類，但上述詐騙類型中，許多行為涉及使用電信和網路技術進行詐騙。像是透過電子郵件、電話或網路平台進行虛假申請或提供虛假資訊，利用網路進行虛假交易或設立虛構公司，透過網路銷售假冒或不合格商品等，這些其實都與電信及網路相關(OLAF,2022)。從 2022 年的調查報告來看，詐騙調查有結案的共 256 件，整體追回犯罪金額有 4.268 億歐元，即使阻止詐騙的有 1.979 億歐元，整體涉嫌刑事案件有向 EPPO 通報的共計 71 件。當時主要的詐騙案件類行為 COVID-19 恢復基金的資金濫用、公共採購案的違法操控與利益獲取、逃避關稅與走私活動以及假冒商品與非法貿易。而 2023 年的調查報告出爐，詐騙調查結案的有 265 件，微幅增加，但追回的詐騙犯罪所得高達 10.4 億歐元增加了 1.5 倍左右。即使阻止被害人匯出的有 2.09 億歐元，也是比 2022 年增加。顯然詐騙案件在歐盟地區也是逐漸上升中。從 OLAF 的報告中發現利用數位技術來進行詐騙的案件有增加趨勢，詐騙越來越多地在網路上進行，跨境詐騙案件也日益增加。比較值得注意的是新興詐騙手法開始出現，尤其是 AI 人工智慧的橫空出世，使得詐騙集團利用人工智慧生成的內容進行詐騙，對傳統的防詐機制構成挑戰(OLAF, 2023)。

表 13 OLAF 調查的主要詐騙類型

類型	定義
補助金詐騙[25]	通過虛假聲明申請歐盟補貼關於特定的資金要求，例如資格和排

[24] 歐盟常設性機構-反詐欺局（OLAF），為歐盟授權的保護歐盟金融利益的機構，於 1999 年 4 月 28 日根據歐盟委員會第 1999/352 號決議成立，任務為打擊影響 歐盟預算的詐欺行為、制定反詐欺立法和政策。資料來源：立法院詐欺議題研析第 2461 號。

[25] EPPO Annual Report 2023. Claiming EU subsidies with false declarationsregarding specific funding requirements (such as eligibility and exclusion criteria – e.g. by concealing a previous criminal conviction, which would disqualify the applicant from receiving EU funds), or by creating artificial circumstances in order to meet eligibility conditions (e.g. by over-declaring the size or quality of eligible agricultural land) 資料來源：European Anti-Fraud Office. 最後瀏覽日：2025 年 10 月 9 日。

	除標準，像是通過隱瞞以前的刑事犯罪，這將使申請人失去接受歐盟資金的資格，或通過製造人為的情況來滿足資格條件。
公共採購詐騙[26]	在歐盟資助的公共採購程序中，透過操縱投標、提供虛假資訊或行賄等手段，非法獲取合同。
海關詐騙[27]	進口商透過虛報商品原產地、低報商品價值、錯誤分類商品或走私等手段，逃避關稅和反傾銷稅，對歐盟財政造成損失。
虛假企業詐取雙重資助[28]	同一項目透過欺騙手段，從不同的資助機構獲得多筆資金，導致資金重複發放。或者設立虛構公司或使用空殼公司，進行虛假交易或申請資金，非法獲取歐盟資金。
內部貪污與不當行為[29]	歐盟機構內部人員濫用職權，涉及薪資、差旅費、社會保障和健康福利等方面的詐騙行為。
假冒與偽造商品[30]	進口假冒或不合格商品，危害消費者健康和安全，並對歐盟市場造成不正當競爭。

資料來源：本研究整理

進一步從歐盟各國來比較其詐欺犯罪的統計，從表 12 來看，2024 年歐盟各國中，

https://www.eppo.europa.eu/sites/default/files/2024-03/EPPO_Annual_Report_2023.pdf

[26] From OLAF's investigation to EPPO conviction: Joint Efforts Deliver Results in Croatia. 資料來源：European Anti-Fraud Office. 最後瀏覽日：2025 年 10 月 9 日。 https://anti-fraud.ec.europa.eu/media-corner/news/olafs-investigation-eppo-conviction-joint-efforts-deliver-results-croatia-2025-09-24_en

[27] Customs fraud. 資料來源：European Anti-Fraud Office. 最後瀏覽日：2025 年 10 月 9 日。 https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud/customs-fraud_en

[28] Special report 22/2024: Double funding from the EU budget – Control systems lack essential elements to mitigate the increased risk resulting from the RRF model of financing not linked to costs. 資料來源：EUROPEAN COURT OF AUDITORS. 最後瀏覽日：2025 年 10 月 9 日。 https://www.eca.europa.eu/en/publications/SR-2024-22

[29] Fraud or other serious irregularities with a potentially negative impact for EU public funds, whether EU revenue, expenditure or assets held by the EU institutions. serious misconduct by Members or staff of EU Institutions and bodies. 資料來源：European Anti-Fraud Office. 最後瀏覽日：2025 年 10 月 9 日。 https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en#olaf-can-investigate-allegations-of

[30] Investment scammers slip through cracks in EU Big Tech law. 資料來源：Investigate Europe. 最後瀏覽日：2025 年 10 月 9 日。 https://www.investigate-europe.eu/posts/investment-scammers-slip-through-cracks-in-eu-big-tech-law

以德國的詐欺犯罪最嚴重，犯罪件數高達 89,742 件，涉入詐欺犯罪人數高達 42,156 人，且主要的詐欺犯罪類型為網路詐欺、身份盜竊，前五名的詐欺犯罪較嚴重的國家，犯罪件數都在四萬五千件以上，參與犯罪人數也都在兩萬人以上，主要的犯罪類型包括網路詐欺、投資詐欺、電信詐欺等。即便歐盟沒有針對電信網路詐欺進行統計，然歐盟各國對於詐欺類型與手法統計中看出，多數的嚴重的詐欺犯罪也都是透過電信與網路來接觸被害者。從歐洲委員會 EPPO (2025)的 2024 年報告來看，德國以網路詐欺犯罪增幅最大，達 45%，年度財損約 42 億歐元；法國由於是旅遊旺盛國家，在信用卡詐欺部分最多，不過投資詐欺與社交軟體的詐欺也有上升的趨勢，年度財損約 38 億歐元；西班牙的詐欺犯罪則是以電信、網路與跨境三種類型的詐欺案件為榜首，年度財損約 28 億歐元；荷蘭的詐欺犯罪問題則是以投資詐欺為主，加密貨幣的手法與運用網路遂行詐欺的案件層出不窮，年度財損約 21 億歐元。很顯然各國目前的詐欺財損金額都相當高，對比以往傳統詐欺犯罪手法的犯罪財損，增長幅度驚人。

表 14　2024 年歐盟詐欺犯罪前五名國家統計表

國家	詐欺犯罪件數	詐欺犯罪人數	主要詐欺類型
德國	89,742	42,156	網路詐欺、身份盜竊
法國	76,534	38,921	信用卡詐欺、投資詐欺
義大利	65,823	31,456	商業詐欺、稅務詐欺
西班牙	58,967	27,834	電信詐欺、網路詐欺
荷蘭	45,321	21,567	網路詐欺、投資詐欺

資料來源：Annual report 2024. (EPPO, 2025; Eurostat, 2025). 本研究整理

(一) 歐盟電信網路詐欺相關法律

近年來歐洲的電信網路詐欺犯罪也相當嚴重，因此，大多數刑事調查都開始朝向數位化。歐盟希望透過法律與行動來加強網路詐欺犯罪預防，從調查和起訴、加強執法和法案的完備、與業界合作，賦權並保護公民免於網路詐欺犯罪的恐懼。以下分別敘述：

1. 網路團結法案(Cyber Solidarity Act)[31]

網路安全法案從 2023 年中開始，歐盟委員會針對日益嚴重的網路安全問題提出初步提案，尤其是疫情過後，人們依賴電腦與網路的程度加深，使得電信網路詐欺愈趨嚴重，歐盟各成員國對於如何解決網路犯罪問題進行初步討論，同時也召開多場次的專家會議，提案完成後送至歐洲議會審議，終於在 2024 年由歐洲議會投票通過網路安全法案並正式公布正式生效日期為 2025 年 2 月 4 日，使得歐洲抗制電信網路犯罪進入另一個階段(ISC2, 2025; European Commission, 2025)。

當中對於與打擊電信網路詐欺相關的主要條款有幾個比較關鍵的條款(EUR-Lex. ,2024)，首先是第 3 條(Article 3, Establishment of the European Cybersecurity Alert System)有關歐洲網路安全警報系統的規範，法條內容規定須建立安全運營中心網絡，對於新興的 AI 技術，應用於偵測網路上的各種威脅，包含電信網路詐欺犯罪的可疑資訊，該法條規定，透過這個安全營運中心可將即時資訊共享給歐盟會員國。第 5 條（Article 5, Cross-Border Cyber Hubs）是跨境網路安全營運中心的建立，由至少三個成員國組成的跨境網路安全營運中心，這些中心將協調其國家網路安全營運中心（National Cyber Hubs），進行網路威脅的監控、偵測和分析，並透過共享工具和資訊來增強防禦能力。第 6 條(Article 6, Cooperation and information sharing within and between Cross-Border Cyber Hubs)則是規範跨境網路安全營運中心之間的合作與資訊共享，透過警報系統來及時通報會員國有關網路安全的資訊，對於網路威脅、漏洞或特定可疑資訊給予網路安全警報和建議，這可以幫助及早識別和應對詐欺行為。第 7 條(Article 7, Cooperation and information sharing with Union-level networks)則是建立歐盟層級網路的合作與資訊共享機制，跨境網路安全營運中心應與歐盟網路安全事件應對小組（CSIRTs Network）和歐盟網路危機聯絡組織網絡（EU-CyCLONe）密切合作，特別是在發現潛在或正在發生的大規模網路安全事件時，應及時提供相關資訊和預警，以防止可能的犯罪事件發生。第

[31] European Parliament & Council. (2024). Regulation (EU) 2025/38 on the Cyber Solidarity Act. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng

8 條（Article 8, Security）的網路安全緊急機制，該條款規定在發生重大網路安全事件時，歐盟會員國可以請求歐盟的支援，這將有助於應對電信網路詐騙的事件。

接著是第三章(CHAPTER III, Cybersecurity Emergency Mechanism)的網絡安全緊急應變機制，條文規範應建立網絡安全緊急機制，用以監控並針對大型的網路事件，第 10 條(Article 10, Establishment of the Cybersecurity Emergency Mechanism)強調歐盟會員國之間的合作，包括資源的共享和信息的交流，有助於打擊跨國詐欺犯罪。第 12 條[32]提到歐盟網路安全局(ENISA)的建立，該隊伍能夠在成員國或歐盟機構的請求下，協助應對重大或大規模的網路安全事件。這個條文主要還是針對網路被駭客攻擊等大型事件而訂定，然而規範中的歐盟各國跨境合作框架與各項資源調配方案，也能夠提供各國在電信網路詐欺犯罪的資訊共享的法規依據。再者第四章(CHAPTER IV, European Cybersecurity Incident Review Mechanism)的歐洲網絡安全事件審查機制，歐盟各國對於網路安全的重大事件有調查權力，第 18 條(Article 18, Incident Reporting)與第 20 條(Article 20, Review of Incidents)就是針對網路安全事件進行相關成因分析，找出該事件的源頭才能針對網路遭受攻擊的地方，提出修正建議，才能達到預防效果。第 23 條(Article 23, Public Awareness and Communication)強調需要向大眾宣導的重要性，將電信網路詐欺相關過程與可能的結果向民眾宣導，提高公眾對網路詐騙的警覺性，減少潛在受害者。雖然整個法案對於電信詐欺的部分雖然並未明確提及，然而當歐盟各國中對於電信詐欺有最新的打擊偵查與預防的政策執行，都可藉由本法條與其他各國共享，建立起龐大的打擊電信網路詐欺的網絡。

2. 通用數據保護條例 (General Data Protection Regulation)

通用資料保護條例（GDPR）雖然主要聚焦於個人資料的保護，但其中多項條文與打擊電信詐欺密切相關。首先是第 5 條(Article 5, Principles relating to processing of personal data) 個人資料處理的原則規範，規定個人數據必須以合法、公正和透明的方式進行處

[32] Article 12, Coordinated preparedness testing of entities. 同註 25。

理，這對於防範詐欺行為至關重要。若數據處理不符合這些原則，將增加詐欺的風險。第 6 條(Article 6, Lawfulness of processing)提到的合法性、公開性與透明性（Lawfulness, Fairness and Transparency）。根據第 6 條內容，所有與個人資料處理需有法源依據。企業在防詐的情況下可依「合法利益」（Legitimate Interests）為基礎進行資料處理，防止未經授權的數據使用。第 32 條(Article 32, Security of processing)有提到個人資料處理的安全性（Security of Processing），條文要求企業在資料管控和處理上必須採取合適的技術和措施，這對於電信業者和防詐平台而言，意味著需建立強大的資安防護機制，以防止詐欺犯罪。第 33 條與第 34 條是有關個人資料洩漏的通報機制(Notification of a Personal Data Breach），第 33 條(Article 33, Notification of a personal data breach to the supervisory authority)規定，若發生個人資料洩漏事件，業者需在 72 小時內通報監管機關。第 34 條(Article 34, Communication of a personal data breach to the data subject)則要求，若該洩漏可能對資料主體造成高風險，則需通知受影響的消費者，提早告知消費者或顧客，其資料已經外洩，請消費者應注意可疑來電以利於及早發現和應對可能的詐欺犯罪接觸(EUR-Lex, 2016)。

3. 網路與資訊安全指令第二版（NIS2 Directive，Directive (EU)）

NIS 1.0 版於 2016 年修訂，當時修訂僅適用於少許部門適用，NIS2 則修訂後預計於 2025 年生效並實施，將網路與資訊安全指令的適用範圍擴大，涵蓋電信業者、雲端運算供應商、資料中心營運商、網域名稱系統（DNS）管理者、電子商務平台、社群媒體平台、醫療設備、公共管理單位等，或者 50 人以上或年營收超過 1000 萬歐元中型以上企業適用之，目的希望能夠涵蓋更多可能成為網路詐欺攻擊對象的產業與平台。因此本次最大的法條修正在於，明確規定通報時限與流程，當發現重大資安事件 24 小時內，必須初步通報主管機關。72 小時內提交正式初步報告。一個月內提交最終調查與回應報告。通報的範圍擴大到資料外洩、服務中斷、勒索攻擊、詐欺事件等，上述的相關事件都必須通報。若是沒有通報，可能被罰款最高至公司全球年營收的 2%。(López & Schweitzer, 2023)。

網路與資訊安全指令第二版（NIS2）是歐盟為提升整體網路安全水平所制定的重要法規，特別針對電信與網路詐欺等問題，提出了多項相關條文。首先是第 4 條(Article 4, Security of network and information systems)，要求歐盟成員國和企業採取措施來保障整體網路和信息系統的安全，強化企業的防詐責任。第 14 條(Article 14, Incident reporting)規定在發生重大安全事件時，需在 24 小時內通報主管機關，有助於及時識別並應對電信網路詐欺事件，提升企業與機關的警覺意識。有關資安風險管理措施的第 21 條(Article 21, Supervisory authorities)，此條文規範成員國必須設立獨立的監管機構，負責執行和監督 NIS2 指令的實施。這些監管機構擁有調查、干預和執行的權力。像是要求電信業者、VoIP 服務提供商、數位平台等與電信網路相關之業者，應採取適當的技術作為，像是建立事件預防、偵測與應對機制並且能夠提供安全的資訊作業環境，負責管理網路與資訊系統的安全責任。第 23 條(Article 23, Reporting obligations)則是強調業者應負起資安事件通報義務，當發生重大影響的資安事件時，業者必須在在 24 小時內向主管機關或 CSIRT 提交初步通報，並在 72 小時內提供詳細報告，最後需在一個月內提交最終報告。

第五章(CHAPTER V, JURISDICTION AND REGISTRATION)是管轄權與登記，第 26 條到 28 條明定規定了不同類型機構管轄權歸屬，即使非歐盟境內的服務提供者也需遵守歐盟的網路安全規範，以便於監管和應對可能的資通安全事件。這些規範包括網域名稱註冊機構需提供準確完整的登記資料，並有提供特定資料的義務，有助於追蹤和防範詐騙網站。第六章的(CHAPTER VI, INFORMATION EXCHANGE) 資訊共享篇章，未強制但鼓勵機構之間建立資訊共享機制，對於網路威脅、漏洞等資訊能夠相互交流，以提高整體防禦能力。第七章的(CHAPTER VII, SUPERVISION AND LAW ENFORCEMENT) 監督與執法，第 31 條(Article 31, Key aspects regarding supervision and enforcement)監管與執法關鍵中，賦予主管機關對企業或機構進行監督和執法的權力，包括審查其網路安全措施和應對能力。第 32 條(Article 32, Supervisory and enforcement measures regarding significant entities)是相關的行政裁罰，主管機關可採取一般警告措施，包括書面警告、公開譴責等；進一步可採取限制性措施，像是限制相關業務的拓展、暫

停已發出的許可證明文件或撤銷其已經認證的相關系統或技術；最後可採取強制措施，對業者實施強制性的人員專業培訓或技術升級。最重要的最要的是提出對違規行為實施罰款或其他制裁，裁罰金額可從 1000 萬歐元到 2000 萬歐元或是年營業額的 2%~4% (EUR-Lex, 2022)。

4. 非現金支付詐欺指令（Directive (EU) 2019/713）

《非現金支付詐欺指令》（Directive (EU) 2019/713）於 2019 年 4 月 17 日由歐洲議會與理事會通過，目的在加強對非現金支付手段詐欺與偽造行為的刑事打擊，特別針對數位支付、虛擬貨幣與網路詐騙等新興犯罪形式。當中第 3 條(Article 3, Fraudulent Use of Non-Cash Payment Instruments)是針對非現金支付工具用來作為詐欺工具的法律規範，屬於刑事犯罪的範疇，故意使用被盜或非法取得的非現金支付工具，是必須受到刑事起訴處分的，此條文幾乎涵蓋了所有電信網路詐欺犯罪的樣態。非現金支付的工作又分為有形支付以及無形的支付工具，分別由第 4 條(Article 4, Offenses Related to the Acquisition of Payment Instruments)與第 5 條(Article 5, Counterfeiting of Non-Cash Payment Instruments)加以規範如信用卡就是有形的非現金支付，電子錢包、虛擬貨幣就屬於無形的非現金支付。

接著第 6 條(Article 6, Possession and Distribution of Tools for Committing Offenses)是與資訊系統相關的詐欺規範，若是使用未經授權干擾或操控資訊系統，以非法轉移資金或虛擬貨幣，或者是未經授權修改、刪除或傳輸電腦資料，以進行詐騙。都屬於刑事犯罪的一種，該條文係針對網路釣魚、木馬程式等手段進行的詐騙活動而訂定。為了徹底打擊電信詐欺，第 7 條(Article 7, Handling of Illegally Obtained Non-Cash Payment Instruments)則是用來規範用於詐欺犯罪的工具，相關製造、取得或提供專門用於實施電信網路詐欺犯罪的工具，如偽造信用卡的設備、惡意軟體等，除了使用者涉及刑事犯罪外，若明知犯罪而提供或製造者也視為刑事犯罪。第 7 條第 2 項還有具體的刑罰規定，違反第 3~5 條的犯罪行為，處 1 年以上 8 年以下有期徒刑，可易科罰金，某些特定的重大電信網路犯罪則可判處 3 年以上 15 年以下有期徒刑，若是組織型態犯罪，則加重二

分之一，最高可到二十年。由於詐欺犯罪多為組織型犯罪，因此第 8 條(Article 8, Incitement, Aiding, and Attempt) 將刑事責任擴大到煽動、協助或意圖號令的個人。此舉將問責範圍擴大，確保電信欺詐計劃的所有參與者，包括促進或鼓勵此類活動的人，都可以被起訴。

比較特別的是因為歐盟是多個國家所組成的會員制度，因此司法管轄權責相當重要。第十二條中針對管轄權(Jurisdiction)有詳細的規範，該法條係屬地原則，犯罪行為中包括犯罪行為地、行為開始地、行為完成地、結果發生地多為優先管轄權，其餘的準備行為地、共謀地點、工具準備地、規劃地點之國家的管轄權其次；當然電信網路詐欺樣態多元，也有被害人原則、犯罪者國籍原則、境外管轄原則。不過條文中有說明管轄權的主要考量因素，從犯罪行為主要實施地、最大損害發生地、主要證據所在地、嫌犯人身自由限制地為最主要考量；次要考量因素則由被害人數量分布、調查取證便利性、追贓可能性、司法資源效率等；特殊考量因素則包括案件複雜程度、國際合作需求、被告權利保障、訴訟經濟原則等。繁複的管轄權考量除了一般簡單的詐欺案件外，較困難的還是跨境的電信網路詐欺，多半各成員國仍須召開協調會議來完成，確認主導機關，分配工作任務以及合作機制(Eurojust, 2024)。

5. 支付服務指令第三版（Payment Services Directive 3, PSD3）

歐盟於 2023 年提出《支付服務指令第三版》（Payment Services Directive 3, PSD3），旨在加強對支付服務的監管，特別是針對電信與網路詐欺的防範。相較於 PSD2 第二版的支付服務指令，第三版有許多修正，對於消費者保護更全面，尤其是未經授權交易之保護，提出詐欺之賠償方案，可減少消費者潛在損失。還有推動開放銀行發展，加強第三方支付業者（Third party payment provider）提供更標準化與更安全的應用程式介面。並也強化支付系統安全性，引進客戶身分認證機制（Strong Customer Authentication,），使支付過程更加透明與安全。推動歐盟市場一體化，讓跨境支付能夠降低成本與提升安全性。更重要的是監管機制的完備，制定更明確的法規，加強各方監管，確保市場公平與穩定。以下從幾點來說明第二版與第三版之間的差異與修正不同之處(EBA, 2024)。

(1) 身分認證機制：PSD2 的認證採雙因素認證、基本生物特徵、靜態密碼、一次性密碼等方式,而到了 PSD3 則採取強化式的認證改成三因素以上的動態認證、進階生物識別、AI 行為分析、持續性認證機制、情境風險評估等方式，其目的都是希望透過不同的身分認證，防止詐騙集團輕易地進行金融方面的詐欺。

(2) 預防詐欺的監控與回報架構：PSD2 原本的只有基本監控架構僅有異常交易監控與偵測、通報機制與基本的風險評估，但是到了 PSD3 則是因應新型態詐欺而增加即時 AI 偵測、跨機構資訊共享、自動阻斷系統等，讓金融支付必須透過更嚴謹的方式才能進行轉帳。

(3) 支付服務業者的義務：PSD2 對於支付提供的業者只要求一般資安標準、資安事故報告、初級風險管理、基本的客戶保護，而 PSD3 則要求業者負起主動防護、即時通報機制、擔負賠償責任、配合並技術升級。

(4) 開放銀行[33]規範：PSD2 對於開放銀行採取標準 API 平台，客戶的資料能跨機構共享，存取控制機制則採取一般化的安全標準。然而到了 PSD3 的支付服務命令則是擴展 API 服務的範圍，資料交換不需等待，即時能夠進行共享，適用於跨國金融的使用，強調的是資料主權保護機制，客戶能夠依照個人的需求進行客製化，將限制級小化。

(5) 資安的提升與監管制度的強化：PSD2 對於資安要求只需要加密、稽核以及事故進行通報，然電信網路詐欺的盛行下，PSD3 要求一律進行認證的零信任架構，由於量子電腦的出現，因此要求業者必須以「量子加密通訊」技術，讓使用者可以利用建制在各處的量子網路，透過「量子密鑰分發」的方式進行安全的通訊。PSD2 的監管制度原本在一般的架構下執行，像是定期報告與基本檢

[33] 開放銀行（Open Banking）是金融科技的具體運用，係由銀行透過與第三方平台合作，以開放應用程式介面（Application Programming Interface；以下簡稱 API）之方式共享金融數據資料，並將金融數據主導權回歸消費者，使消費者從中獲取更多元的金融服務。資料來源：立法院議題研析，編號：R00876

查，PSD3 則是要求做到即時監控，利用 AI 輔助稽核作業，建立相關的預警機制，發生問題的則視需要進行跨境協調，更重要的是進行動態風險評估，隨著風險的動態評估進行改善。

6. 數位服務法（Digital Services Act, DSA）

數位服務法案於 2022 年 10 月 19 日由歐洲議會與理事會通過，2024 年 2 月 17 日生效，為了建立更安全、透明的線上環境，特別針對電信與網路詐欺等非法內容，提出多項規範。第三條的(Article 3, Definitions)定義則是明確了 DSA 適用的服務範圍，包括所有提供數位服務的企業機構。因此所有網路線上平台和相關金融與網路服務提供者都必須遵守該法規，以確保網路安全，杜絕可能的詐欺犯罪行為。從第 9 條(Article 9, Orders to take action against illegal content)的業者負有違法內容處理之義務，除了建構 24 小時快速通報系統外，對於相關違法內容必須採優先順序進行分類，對於犯罪通訊應立即下架，對於違法證據要進行保存，提供給檢調單位查察，同時企業需要進行定期的風險評估，特別是針對可能導致詐騙的風險的威脅。第 16 條(Article 16, Notification and action mechanisms)針對業者必須建立通知和採取行動的機制，要求線上通報檢舉平台建立易於操作的通報機制，讓用戶能夠快速立即舉報詐騙資訊。平台在接獲通報後，能夠迅速評估並採取適當行動。第 18 條(Article 18, Reporting suspected crimes)通報可疑犯罪義務，企業一旦發現可能的刑事犯罪，應立即通知成員國執法機構或司法當局，或通知歐洲刑警組織，並提供所有可用資訊。第 19 條(Article 19, Exclusion of micro and small enterprises)則是針對大型話務業者（VLOPs）定期進行系統性風險評估，尤其當發現這些業者進行詐欺相關的電信網路訊息傳播，業者應採取有效的預防措施。第 24 條(Article 24, Transparent reporting obligations for online platform providers) 網路平台供應商的透明報告義務，第 3 項規定平台業者對於數位服務協調員和委員會要求提出相關資訊時，應立即提供，但對於個人資料部分則以予排除。第 30 條(Article 30, Trader traceability)商家的可溯源性，目的是針對眾多線上購物系統的店家進行身分資訊的驗證，慎防線上購物的店家對消費者進行詐欺犯罪。最後在第 34 與 35 條的風險評估與緩解對策中，規定對網

路詐欺進行預防措施，包括對疑似詐欺行為進行偵測、識別與預警，同時對消費者建立保護機制，透過用戶驗證技術，對每筆交易進行監管控制，了解資金的流向，一經舉報，能夠將資金進行凍結，以防被詐騙集團轉走。

7. 人工智慧法案（AI Act）

歐盟人工智慧法案》（EU Artificial Intelligence Act, Regulation (EU) 2024/1689）於 2024 年 6 月 13 日通過，並將於 2025 年 2 月 2 日開始分階段實施。該法案採取風險為本的監管架構，對於打擊電信與網路詐欺具有重要意義。當中第 6 條規定對於詐欺預防利用 AI 系統進行分類，針對網路上可能利用 AI 來進行詐騙的疑似電話與訊息，進行評估預測與提出警告，該系統應即時進行監控，一有異常，則利用原本的預警機制來進行警告(Williams & Johnson, 2024)。

(二)歐盟打擊電信網路詐欺的執法機構

歐洲刑警組織關於網路詐欺的重點報告(Europol's spotlight report on online fraud)指出，網路詐欺是歐盟及其他地區的主要犯罪威脅，因為網路詐欺每年造成數十億美元的損害，2023 年網路詐欺犯罪多以網路支付為主，加上烏俄戰爭導致慈善詐騙增加，利用網路 ATM 進行的詐欺也相當嚴重。由於電信網路成為日常生活所需的工具，虛擬貨幣成為歐盟電信網路詐欺的主要犯罪工具，因此歐盟為了打擊電信網路詐欺犯罪，以幾個面向來強化打擊力道(Ilbiz & Kaunert, 2023)。歐盟在打擊電信與網路詐欺犯罪，並非單一執法機構便能執行，必須透過多個專責機構進行協調與執法。

1. 歐洲刑警組織(European Union Agency for Law Enforcement Cooperation, Europol）

1999 年在荷蘭海牙設立總部，一開始是為了因應跨境犯罪、恐怖主義及網路犯罪在歐盟內部迅速增加的趨勢。然而在 2016 年，歐洲議會與歐盟理事會通過新規範（Regulation (EU) 2016/794），將 Europol 重新組織再造，使其成為歐盟內部的正式機構。Europol 的主要工作內容包括促進各成員國警察部門的情報交流，同時支援各國執

法機構偵查跨國犯罪與恐怖主義活動。對各種犯罪情報進行收集分析並分享。目前 Europol 主要針對網路犯罪（Cybercrime）、恐怖主義（Terrorism）、販毒（Drug Trafficking）、人口販運與非法移民（Human Trafficking & Illegal Immigration）、洗錢與金融詐欺（Money Laundering & Financial Fraud）、電信詐欺與網路詐欺（Telecommunications and Online Fraud）。

對於打擊電信網路詐欺犯罪，Europol 本身內部設有「歐洲網路犯罪中心」（European Cybercrime Centre, EC3），EC3 本身 24 小時監控電信網路詐欺犯罪可疑資訊，對於疑似詐欺犯罪有快速反應機制，本身技術能夠進行網路威脅偵測，可提供各種情報分析，再者透過數位鑑識的技術，專門處理網路詐騙、勒索病毒、網路釣魚等案件。Europol 設有聯合網路行動小組（J-CAT），專門處理網路詐欺、勒索軟體、網路洗錢、身份盜竊等電信網路詐欺犯罪事件，利用本身資料分析中心，透過內部大數據平台的資訊，藉由新興的 AI 分析工具，對於電信網路詐騙犯罪進行預測分析，整合所有詐欺資訊來進行模式識別，將每個詐欺犯罪進行關聯性分析，最後做成風險評估報告，提供有效的犯罪預防手段。Europol 在合作機制方面，除了官方的執法機構相互合作之外，也會與私營部門合作，尤其是跨機構偕同必須先進行情報共享，查緝行動必須聯合整個行動的框架，為了加快查察效率，彼此的技術交流顯得格外重要。與私部門的話，要從資訊安全公司取得相關第一手詐欺犯罪情報，電信業者也應與其配合，這些合作關係擴展到金融機構還有網路業者等，像是 Google、Meta 等資訊的共享，持續追蹤詐騙電話與詐騙網頁。推動跨國聯合行動，例如「Operation First Light」，打擊跨境詐騙電話中心。(Wilson & Anderson, 2024; Brown & Wang, 2024)。

EC3 隸屬於歐洲刑警組織（Europol）， 因應歐盟內網路犯罪而在 2013 年成立。尤其是跨境網路詐欺、金融詐騙、網路攻擊的犯罪案件快速增長，有必要成立一個專責、專業的網路犯罪偵查與支援中心。中心的工作內容主要支援各成員國並提供必要的技術協助，疑似犯罪資訊與情報的交換，對於相關資訊進行分析。尤其是電信網路詐欺多為跨境犯罪，因此 EC3 必須整合不同國家的查緝人力。定期也會發表犯罪預測與風險評

估，揭露最新的犯罪手法，避免詐欺橫行歐洲。同時查緝案件時透過不管策略與私營部門合作，除收集資訊提供情報外，亦能從銀行、電信、社交媒體、加密貨幣交易平台獲取必要資料，並提供可能的疑似犯罪情報，以利金融與各業者提早準備。

打擊電信網路詐欺方面，尤其是網路詐欺（Cyber-enabled Fraud），打擊透過網路進行的銀行詐欺、商業電子郵件詐騙(BEC)、假冒網站詐騙、電信詐騙。合作展開「EMPACT Fraud Week」，針對跨國詐騙集團行動。虛擬資產犯罪也是新興犯罪型態，也結合電信網路詐欺進行犯罪所得的轉移(Bures & Carrapico, 2022)。

2. 歐洲反詐欺辦公室（European Anti-Fraud Office, OLAF）

OLAF 成立於 1999 年，接替了當時負責內部調查的「內部調查組織單位」(UCLAF)。主要原因是歐盟機構需要一個更獨立且有權調查自己機構貪污和詐欺案件的單位。OLAF 調查單位分為金融詐欺組、網路犯罪組、結構基金組、海關詐欺組，四個組都擁有獨立調查權力，從行政調查到現場檢查，對於證據還能調取相關資料，最重要的能夠在歐盟進行跨境合作，當中電信網路詐欺相關的跨國騙案屬於重大案件，因此 OLAF 能夠進行調查。OLAF 對於重大詐欺案件的調查，其案件來源相當多元，有的是平台舉報、成員國資訊共享、歐盟機構內部發覺或者經由風險分析部門分析後的可疑情資。面對眾多的可疑資訊，OLAF 會進行初步評估是否符合 OLAF 的調查範疇。若是符合則展開正式調查，透過其調查權力進行偵察與取證。由於 OLAF 非檢察機關，因此在調查完之後會產出調查結果與建議，建議的部分可以提出追繳資金、刑事起訴、行政處分，或者轉交歐盟機構或成員國執法機構執行。OLAF 對於打擊電信網路詐欺具有重要的關鍵貢獻，尤其是歐盟為多個國家所組成的聯盟，跨境調查自然有主權上的疑慮，因此透過歐盟的官方單位來進行調查跨境詐欺是最好的主導機關。同時間也能夠擁有調查權力，去本位主義的共同合作查辦電信詐騙案件，也能夠和歐洲刑警組織（Europol）、歐洲檢察官辦公室（EPPO）共同合作，處理電信詐騙資金流與洗錢路徑。最重要的是能夠共享相關詐欺犯罪資訊，第一時間向成員國傳送詐欺趨勢警報（Fraud Alerts），幫助電信業者提前防範新型網路詐騙(Lee & Chen, 2024)。

3. 歐洲網路與資訊安全局（European Union Agency for Cybersecurity, ENISA）

ENISA 在 2004 年成立，當時因為網路時代的來臨，為了能夠加強歐盟整體網路與資訊安全，同時希望整個歐洲唯一體，對各類網路威脅能夠提早偵測與預警，由於近年來電信網路詐欺相當嚴重，因此目前也電信與網路詐欺提出相關作為。ENISA 的角色類似預防犯罪的機構，對於電信網路詐欺進行技術性預防工作，包過系統防護與身分認證，系統防護部分致力於網路監控與入侵偵測系統的建置，對於身分認證制認證標準，對於網路安全加密都有嚴格的規範。尤其針對目前主流的電信網路詐欺類型發布《電子通信安全報告》（Electronic Communications Security Report），針對虛偽基地台（IMSI Catchers）、VoIP 詐騙、SIM 卡詐騙（SIM swapping）等。此外 ENISA 的預警系統能夠即早發現大規模的電信詐騙攻擊，如大規模 Smishing 簡訊詐騙，一有疑慮便可以跨境發布警告。ENISA 對於歐盟各國的國家級電信業者具有強制力，所有電信業者應該建立資安事件通報機制，對於可疑情報必須進行偵測與標準的回應作業流程，同時必須定期進行資安風險評估與系統滲透測試，確保歐盟各國的資安能夠統一(Lisi & Stefanizzi, 2022)。

4. 歐洲電子犯罪工作小組（European Electronic Crime Task Force, EECTF）

歐洲電子犯罪工作小組（EECTF）是一個集合電信技術、調查、情報分析的單位，2009 年的時候成立，總部位於義大利羅馬。是一個公私部門合作平台，集結了國家執法單位、金融業、電信業以及相關資安負責的機構，對於打擊網路詐欺犯罪而組成的工作小組，現今電信網路詐欺嚴重，尤其是涉及電子支付與電信網路的詐欺行為，目前 EECTF 致力於該領域的犯罪預防工作。這個工作小組與其他機構的任務大同小異，從詐欺犯罪可疑情資共享，會將最新的電信詐騙的手法、如何接觸被害者、甚至是偽造的基地站（IMSI Catchers），只要一知悉就會即時通報到各成員國進行預警動作。加上許多技術專家的加入，也會協助進行技術培訓與相關標準制定。EECTF 雖然是公私部門合作的單位，也沒有正式的法律強制力，但在實務上有其「影響力」與「協作壓力」。由於 EECTF 組成有相關專業人士，因此該單位會針對電子錢包、行動支付、加密貨幣交易中詐欺提出具體的防護作為。尤其金流的部分都與電信網路手段來進行詐欺，他們對於犯罪集團

模式相當了解。加上非正式的官方單位，其資訊的共享並不需要冗長煩悶的公文程序，能夠快速且即時的傳遞犯罪資訊，這當然對於政府執法單位有莫大的破案壓力存在(EECTF, 2025)。

5. 國際刑警組織（Interpol）

國際刑警組織（Interpol）是世界最大規模的跨國執法合作組織，目前有 195 個成員國。成立於 1923 年，當時名稱是國際刑事警察委員會，1989 年時總部遷至法國里昂，為了能夠達到國際刑警辦案與偵查的目標，2015 年建立了全球詐騙數據庫（Interpol Global Rapid Intervention Platform, I-GRIP），建立全球各國上報的詐騙模式、IP 地址、可疑電話號碼資料庫。近年來為了偵辦電信網路詐欺犯罪，透過數位鑑識與情報分析，成為打擊電信網路詐欺的最強後盾。國際刑警組織擁有全球取證實驗室以及網路追蹤系統，對於相關詐欺的情資與情報都能夠快速取得，再進行數據中心中進行加密分析，再制定聯合行動計畫並即時協調衝突部分，最後進行跨境打詐行動。

由於 Interpol 有建立財務詐欺行動小組（FF-ISAC），讓銀行、電信業者、第三方支付平台等與詐欺犯罪相關的機構共同分享金融詐欺情報，有利於資金凍結與攔截。由於電信網路詐欺伴隨各種不同金融的匯款工具，國際刑警組織為了加大打擊加密貨幣詐騙與洗錢犯罪，成立專門追蹤虛擬貨幣詐騙與資金流向的特別小組（Virtual Asset Crime Units），這個小組能夠追查跨境轉帳的虛擬貨幣以及金流蹤跡，可協助各國警方凍結加密貨幣錢包，尤其是與電信詐騙資金流動有關的犯罪，更是目前國際刑警組織的重點工作。Interpol (2024)的報告中顯示，於 2024 年 7 月到 11 月所執行的 Operation Haechi V 行動當中，總共逮捕涉及電信網路詐欺超過 5,500 人，同時追回並攔截超過 4 億美元，包含最難追查的虛擬貨幣，當中多數詐欺類型為語音釣魚詐騙、感情交友詐騙、投資詐欺等，成果輝煌。另外 2024 年所進行 First Light 行動，成功追回 2.57 億美元中，其中約莫 30%資金是透過追蹤虛擬貨幣而成功攔截並凍結帳戶所追回的(INTERPOL, 2024)。

(三)歐盟打擊電信網路詐欺的整體策略

由於歐盟非單一國家而是由歐洲國家所共同組成的聯盟，在打擊電信網路詐欺犯罪上有其優點及缺點。從優點來看，統一的主導機構能夠制定一致的政策與目標，同時對所有會員國都能夠建立資訊共享以及預警機制，同時整合各成員國的打詐力道，不管在查緝犯罪人或者是隱匿蹤跡的金流，都能快速取得相關證據。但也不是沒缺點，對於歐盟來說，各國發展程度不一，從電信網路的技術到橫向的機構聯繫，雖然歐盟能夠發布統一的政策與作為，但當各國要落實相關政策時，若資金不到位、人才跟不上、機關執行力不一，對於整體的打詐策略是相當大的挑戰。歐盟整體打擊電信網路詐欺的策略可從法律框架、執法合作、技術防護及公民教育，以下從這四個方面來加以說明。

1. 法律框架

政策的具體作為必須有法律的支持，才能順利地執行。因此探討整體打擊詐欺策略應從法律的框架開始著手。法律框架類似同心圓的概念，從最核心的法律為主，外圍的則是屬於補充核心法案的不足。以歐盟的電信網路詐欺犯罪來說，應該包含一般性資料保護規範(GDPR)、網路安全法(NIS Directive 2.0)、反詐欺刑事制裁指令(Anti-Fraud Criminal Sanctions Directive)、電子支付服務指令(PSD2)。而補充的法案則包括網路犯罪公約執行法(Convention on Cybercrime Implementation Act)、數位市場法(Digital Markets Act)、數位服務法(Digital Services Act)等。其實眾多與電信網路相關的法案，立法的思維朝向風險掌控與技術導向、跨部門協調與合作以及強化執法與監管機制。

由於歐盟非屬單一主權國家，因此歐盟的法律架構必須以風險掌控為原則，根據不同的風險等級制定相應的規範，並保持技術導向為主，才能夠適應快速變化的科技環境。其次是跨部門協調與合作，歐盟國家與機構相當多，若採取本位主義，則容易形成多頭馬車，因此部門間的協調與合作顯得格外重要，像是上面提到的歐洲反詐騙辦公室（OLAF），就負責主導的反詐策略的發想與制定，最後督促所有成員國能夠建立資訊共享、提前預警以及協同打詐的默契。然而法律制定並非束之高閣，應當落實執法以及

後續的監督管理，執法方面則是成立歐洲公共檢察官辦公室（EPPO）等機構，加強對跨國詐騙活動的調查與起訴能力，提升法律的嚇阻效果(European Commission, 2025)。下面要特別介紹反詐欺的刑事制裁命令(Anti-Fraud Criminal Sanctions Directive)，該命令是完全針對詐欺所訂定的，具有相當指標性。

歐盟於 2024 年 4 月 24 日通過了《反詐欺刑事制裁命令》(Directive (EU) 2024/1226)，旨在統一成員國對違反歐盟制裁措施的刑事處罰標準，強化對制裁違規行為的執法力度。該指令於 2024 年 5 月 19 日生效，歐盟成員國需在 2025 年 5 月 20 日之前將其轉化為國內法律。該指令規定成員國必須將以下行為視為刑事犯罪[34]：

① 將資金或經濟資源提供給受制裁的個人或實體。

② 未能凍結受制裁對象的資產。

③ 提供被禁止的金融服務或其他受限制的服務。

④ 允許受制裁對象進入或過境歐盟成員國。

⑤ 與第三國或其控制的實體進行被禁止的交易。

⑥ 從事被禁止的商品或服務的貿易活動。

⑦ 規避歐盟制裁措施。

⑧ 違反成員國授權機構頒發的許可條件。

而裁罰的部分也明定若涉及詐欺犯罪事實，自然人與法人都有明確的裁罰標準，以自然人來說，第 5 條(Article 5, Penalties for natural persons)規定，成員國應確保對自然人違反歐盟限制性措施的刑罰具有有效性、威懾力和罪刑法定性。詐欺犯罪行為是嚴重程度或者財損金額多寡來判定，若是達 10 萬歐元以上，可判處 1 年以上有期徒刑，嚴重者可判 5 年以上有期徒刑，罪刑可說是相當嚴重，個人來說還可以暫時禁止競選公職。

---

[34] Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures. Official Journal of the European Union. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024L1226 最後瀏覽日：2025 年 3 月 28 日

第 6(Article 6, Liability of legal persons)與 7 條(Article 7, Penalties for legal persons)則是針對法人，可裁罰的金額從全球年營業額的 1%至 5%，或採固定金額的罰鍰，金額多寡可由成員國法律來決定。更嚴重的可以禁止參與公共招標、撤銷營業許可、強制解散等行政懲處。

2. 通力執法合作

歐盟在打擊電信網路詐欺犯罪方面，建立了多層次的執法合作機制，涵蓋專責部門、跨境偵查、成員國警政合作平台以及國際執法單位協作。單打獨鬥的時代已經無法因應科技日新月異的快速變化，打擊犯罪需要多方面的協調與合作，對於打擊電信網路詐欺犯罪，歐盟最常見的就是以下組織的合作辦案。根據圖 4 的架構圖來看，最高層級的決策機構為歐洲理事會(European Council)、歐盟理事會(Council of the European Union)、歐洲議會(European Parliament)。主要透過這三個單位制定打擊跨境犯罪的戰略方針，與歐洲議會共同立法並審議預算分配，三位一體成為最高決策中心。接著由歐盟執行委員會擔任實際的政策執行機構，負責將最高決策中心的相關決議與政策輔導歐盟各國遵守，而打擊電信網路詐欺部分的執法工作就交由四個單位去合作執行。

首先是歐洲刑警組織（Europol）轄下的歐洲網路犯罪中心（European Cybercrime Centre，簡稱 EC3），專門應對網路犯罪，包括電信詐騙、網路詐騙、勒索軟體攻擊等。EC3 最重要的是從可疑情報進行分析與共享機制，歐盟擁有較高層次的電信網路技術，為成員國提供高階數位鑑識、惡意軟體分析等支援；一旦發現可疑犯罪蹤跡，並確認相關詐欺犯罪已有被害人，聯合網路犯罪行動工作組(J-CAT)馬上進行偵辦查察的行動開展，從協調主導與權責分配之外，專案任務編組以及後勤的技術支援分配，更是不能忽略，透過多層次的協調與計畫，才能以舉偵破猖獗的電信網路詐欺犯罪行動。不過 EC3 強調單以公部門之力量已無法順利完成打詐行動，必須公部門與私營部門協同合作，共同開發防範網路犯罪的策略和工具。

歐洲檢察署(EPPO)[35]跨境偵查則擔負重責大任，歐盟中央檢察系統負責建立標準化案件分案處理流程，制定統一起訴標準，對於各種電信網路詐欺犯罪制定起訴指南，倘若遇到跨國事務，則由國際法務組負責處理跨境法律事務，更重要的是透過證據管理中心來確保跨境證據效力。而區域檢察網絡則是各國檢察官，由各成員國指派專業檢察官來進行辦案偵查事務，若是跨國案件則需加速跨境司法程序，同時對跨國資產凍結、攔截與追討。跨境辦案需要成員國警政合作，成員國之間透過情報交換系統來實踐資訊共享目標。成員國之間透過加密網絡來確保打詐情資能夠安全傳輸，進一步將資料庫進行整合，突破語言與文化之間的隔閡，將各國犯罪資料庫共同集合在大數據資料庫，透過AI 技術處理大數據運算並進行預測分析。待一切時機成熟後，展開聯合行動，由歐洲檢察署擔任指揮調度中心來統籌跨國行動，成立聯合調查小組（Joint Investigation Teams，JITs），該組是由兩個或多個歐盟成員國的執法和司法機關組成的臨時合作機構，指揮各國成員的警力進行優勢部署行動，整體打詐行動應動態分析與檢討，作為下次出動之優化依據(Florea, Aivaz & Vancea, 2022)。

接著是跨國執法合作網絡，全球合作架構下透過國際刑警組織（INTERPOL）協助整合，來強化跨境打擊詐欺犯罪力道，由於會員國之間仍屬國與國的合作，因此透過雙邊協議來深化彼此間的合作同時跨國的偵查技術共享，才能有效打擊詐欺犯罪。此外除了官方機構的合作外，電信網路詐欺通常伴隨著私營企業的金融機構，因此歐盟強調公私部門合作機制，金融機構、電信業者都視為合作夥伴，方能全面的瓦解詐欺犯罪組織(Wilson & Davis, 2025)。

[35] European Public Prosecutor's Office. (2025, April 14). *Investigation Cuba: EPPO secures another conviction in €100 million VAT fraud involving Voice over IP*. Retrieved from https://www.eppo.europa.eu/en/media/news/investigation-cuba-eppo-secures-another-conviction-eu100-million-vat-fraud-involving 最後瀏覽日：2025 年 4 月 20 日

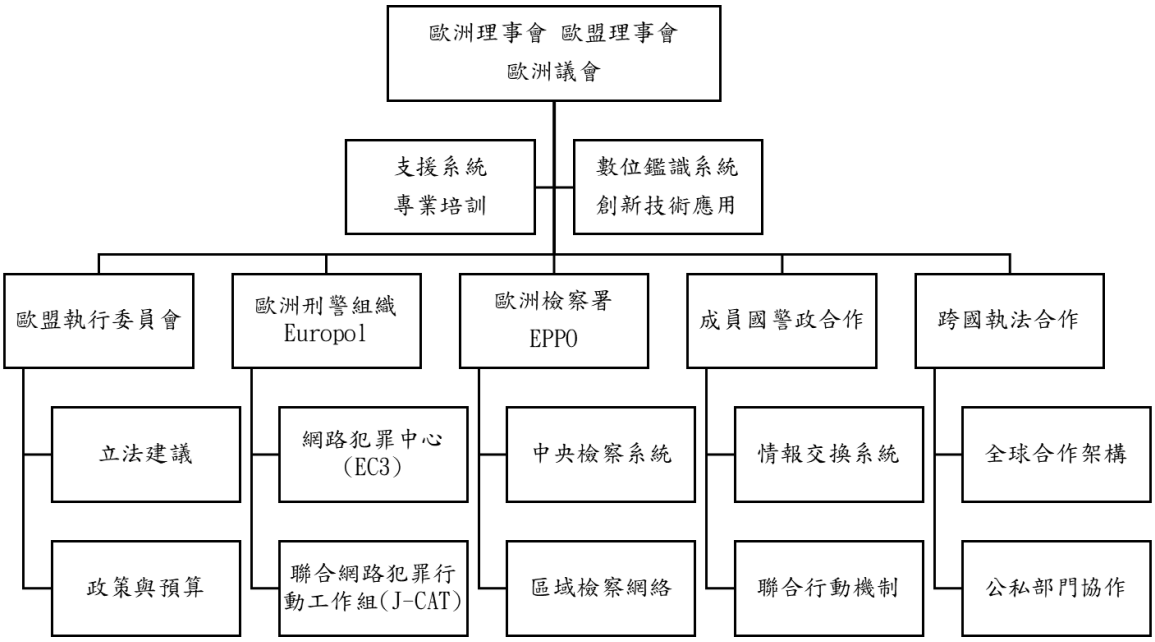


圖 4 歐盟打擊電信網路詐欺架構圖，本研究整理

3. 透過技術升級來進行防護措施

即便有強大且完整的打擊電信網路詐欺犯罪的執法網絡，然而最佳的打詐應該是提前預警讓詐欺犯罪無法得逞，詐欺犯罪集團透過各種不同的犯罪手法來遂行詐欺犯罪，從各種電信通訊工具來接觸被害人，透過網路來傳遞各種虛假以及社交軟體的互動，使得被害人一步一步地踏入已經設計好的劇本圈套，被害人一個不小心便會陷入，大量財損造成個人、家庭、社會以及國家的危害，使得國家付出極大的成本來進行打詐行動，然透過高階技術的各種防護措施，減少或降低各種可能接觸被害人的渠道，多種不同的驗證技術等，能夠增加犯罪阻力，有助於達到犯罪預防的目的。

(1) 提前預警系統建置

EUROPOL 的預警系統是新冠肺炎之後所建立的全方位即時監控系統架構，定期發布針對新型詐騙手法的預警報告，讓成員國的執法機構能夠及時獲取最新的詐騙信息，提前做好防範準備。而 Cyber Crime Centre (EC3)定期收集來自成員國的網路犯罪數據，包括身份盜竊、勒索病毒等詐欺犯罪的資訊，包括可疑 IP 位址、惡意程式、社交媒體等詐騙，並對這些數據進行深入分析，識別主要的網路犯罪趨勢和模式(Europol, 2024)。

(2) 先進人工智慧輔助偵測

大數據整合與近一步分析是未來的趨勢，歐盟鼓勵金融機構和在線平台整合來自不同來源的數據，如交易記錄、用戶行為數據和社交媒體信息，以建立全面的用戶檔案。進行統合式分析後，將正常交易的模式與異常行為進行比對，對於潛在的詐騙即時發出警報。而未來人工智慧將運用在交易監控，即時分析交易數據，快速識別可疑交易。一旦檢測可疑詐欺犯罪，系統可以自動執行預定的應對措施，如暫停交易、通知用戶或要求額外的身份驗證，從而降低損失風險(Europol, 2024)。

(3) 全面性通報機制

歐盟刑警組織中的 Report Cybercrime online 的系統，能夠簡化通報可疑詐騙行為的過程。被害者可以通過平台迅速提交詐騙訊息，系統會自動分類收到的報告，並根據其緊急程度和重要性，將資訊轉發給相應的執法機構或部門，迅速對於相關詐欺犯罪做出應有應對作為。再者根據反洗錢指令（AML Directive）和支付服務指令（PSD2）規範，業者發現可疑交易時必須立即通報相關機構。此法規也意味著企業內部監控系統的建置，才能及時檢測和報告可疑活動(Europol, 2024)。

(4) 新世代支付系統安全強化

交易安全機制是防止詐騙集團快速將犯罪所得轉走的重要手段。除了上述的多重身份驗證系統之外，動態密碼認證也能夠適時阻擋，包括一次性密碼(OTP)、動態安全碼、簡訊驗證等都是多重驗證程序。其次是金融交易限額管理，對於交易的額度進行分級限額。對於日常交易限額，一般消費限額上每日累計限額為 3,000 歐元，每月累計限額為 15,000 歐元。當客戶有需求時，會根據個人信用評級來放寬每日限額，A 級是基本額度的兩倍，B 級是 1.5 倍，C 級額度不變，D 級的則是減少 50%。對於從商的個人，則採取大額交易限制，該限制有分層審核機制，第一層是 10,000-50,000 歐元，除了線上身分認證，還必須提供資金來源證明，經由 24 小時審核期後才會通過；第二層是 50,001-100,000 歐元，除了雙重認證外，還必須透過視訊面談確認，要等 48 小時審核期；第三

層是 100,000 歐元以上，除了客戶要到實體銀行辦理，資金的轉匯需多重主管審核，審核期是 72 小時。如果是跨境交易控管，每日的一般限額約為 50,000 歐元。至於高風險交易限制，將虛擬貨幣、博彩業、貴金屬、藝術品視為高風險的交易類別(IMF, 2023)。

緊急凍結程序的落實，能夠讓財損降到最低。首先是金融機構的快速反應機制，一旦發生可從行動銀行 APP、網路銀行平台或是專用通報網站舉報已發生的詐騙案件，在第一時間凍結資金管道後，即刻進入歐盟銀行聯防系統進行協調，此時除了即時回報詐騙集團的相關資訊外，同步凍結可疑帳戶與資金以及進行已轉出的資金進行追蹤，同時保全相關證據，與此同時與司法聯繫窗口進行報案，期望能在第一時間快速反應(WEF, 2023)。

由於電信網路詐欺犯罪伴隨各種金融匯兌手段，因此建立進階生物識別技術相對重要，阻擋犯罪所得的入手，也能夠有效地降低被害者的損失。可透過多重生物特徵整合系統來加強轉帳的身分認證，像是臉部辨識系統、指紋識別技術、虹膜掃描功能、聲紋分析能力都是屬於多重的生物特徵來進行身分驗證。或者是採用行為生物識別技術，像是個人打字模式深度分析、操作習慣辨識、使用行為模式的驗證、持續性身份驗證都是金融機構可採用的身分驗證手段。除了身分認證外，交易過程也是可以著手的地方，高科技智能交易監控能夠掌控金流去向，將原本的風險評估系統轉為即時回報模式，對於交易模式進行分析，了解炸團在金流匯兌轉帳的模式，進一步建構風險預測模型，一旦發現類似情況的金融轉帳，即可啟動自動干預機制，即時凍結與攔截犯罪所得的轉匯。此外匯款交易的同時，採用進階加密保護機制以及動態金鑰管理手段，多層防護與風險管控，延長詐團對於金流的匯兌與轉帳，爭取更多的時間來阻止被害者金錢被快速匯出(Anderson & Smith, 2024)。

4. 預防機制與宣導落實

(1) 公眾意識的提升

歐洲網路與資訊安全局（ENISA）致力於提升公民對網路安全的認識，然而普羅大

眾鮮少對於犯罪資訊有所瞭解，為了提升所有民眾對於電信網路詐欺的認識，歐盟推出網路安全月活動 (European Cybersecurity Month)，所有成員國同步執行打擊電信網路詐欺主題宣導活動，各國可根據當地文化與民情來進行在地化的活動設計，活動設計與教學應採年齡分層策略，針對青少年推行數位素養計畫，成年人則推動成年人防詐意識宣導，對於長者執行銀髮族保護專案，至於兒童則從小奠定兒童網路安全教育。由於防詐是全民共同責任，建立知識傳播平台，透過防詐的互動式教材讓民眾了解最新詐騙的手法，同時擴充案例資料庫，讓最新的詐騙手法無所遁形，該平台應設置即時諮詢服務，共同投入全民防詐意識的培養(Costea, Putină & Brie, 2024)。

(2) 企業資安訓練要求

NIS2 指令強制要求下，尤其是金融服務業的銀行、證券交易所、保險公司以及支付服務提供商，除了技術層面的評估與改進之外，更希望能夠從人員訓練著手，對於資安意識還有詐欺事件通報流程要熟悉，方能在第一時間發覺異狀。另外就是認證制度建置，從企業人員的專業認證開始，詐欺手法識別訓練，以及人員遇到詐騙案件時的反應能力，包括緊急處置程序是否熟知、資金凍結機制是否快速反應、證據保全方法能否完成、整體通報協調流程是否順暢，都是企業人員在資安訓練上應當加強的。企業人才的培訓目的是要建立標準化防制能力，企業本身對於詐騙犯罪本應負起相當責任，因此內部人員的專業培訓是打擊電信網路詐欺的重要一環(ENISA, 2023)。

(3) 媒體宣導策略

打擊電信網路詐欺犯罪除了執法機構外，還有公眾意識的提升，然而如何讓防詐相關認知讓更多人知道，歐盟認為應該利用媒體進行宣導。尤其是目前是社群網路年代，透過媒體來宣傳防詐的相關資訊是最佳管道(EUROPEAN COMMISSION, 2023)。

① 社群媒體多平台宣導：整合時下最多人使用的社群軟體為目標，包括 Facebook、Instagram、Twitter、LinkedIn、TikTok 等社群媒體，進行電信網路詐欺的預警資訊傳遞，還有影音圖像宣導、即時通報資訊以及相關短影音來分享專業資訊。

整體來說內容的規畫朝向詐欺預警、週期性教育課程、互動式宣導活動、受害案例宣導。

② 傳統媒體的合作：傳統媒體包括電視廣播以及平面報章雜誌等，考量不同族群有不同媒體的使用率，因此在電視廣播上可專注在新聞專題報導、公益廣告投放、專家訪談節目、案例重建劇集等。而平面報章雜誌則可強調報紙專欄報導、雜誌深度分析、公共場所海報、交通運輸廣告等。

③ 不同族群應規畫不同宣導策略：年長者目前成為電信網路詐欺的對象，因此對於年長者的宣導朝向大字體宣導品、簡明易懂圖解、實體講座活動、社區宣導會等，更重要的是年長者應強化家庭支援網絡，避免成為待宰肥羊；青少年族群則從校園出發，配合數位管道的散播，透過各種 APP 以及遊戲的廣告，強力播送相關防詐知識，期許能夠將相關防詐知識內化。

④ 深入社區組織聯盟：社區是大家生活的地方，因此和社區組織整合，在地化的宣導、志工培訓後建立起關懷的社區網絡，遇到緊急或者重大的詐欺事件時，能夠即時協助通報，深入社區才能夠將防詐意識全面化。

(四)歐盟打擊電信網路詐欺的困境

1. 跨境執法困境與國際合作障礙

政策的制定多半由上往下，由上位的思考來訂定相關政策，多數都是執行過程中才發現有極大的困難之處。首先打擊電信網路詐欺犯罪最怕遇到司法管轄權衝突，法律適用問題、各國法規差異、域外管轄爭議、證據採認標準不一、處罰規定不同步，執法權限限制、跨境搜查受限、資產凍結困難、犯罪者引渡複雜、調查權限不明確。行政程序延遲、互助請求耗時、文書送達困難、程序標準不一、回應時效過長。情報共享限制、資訊安全顧慮、隱私保護衝突、系統整合不足、分享機制不完善(EC, 2023; SOCTA, 2023)。

2. 技術層面困境

由於新型詐欺手法層出不窮，目前除了電信網路之外，更是利用 AI 技術來進行深偽應用，將影像、聲音等進行仿造，使得被害人輕易地上當；而詐騙集團利用加密通訊作為彼此之間溝通聯絡的管道，使得查緝更加不易。目前詐欺犯罪所得除了傳統的提領之外，目前開始使用電子錢包與虛擬貨幣來逃匿追蹤，使得被害人的財損無法即使攔截，造成更大的經濟損失。在執法過程當中，尤其目前多半為跨境電信詐欺，查緝工作也需要跨境合作，然而蒐證過程常因司法權爭議而出現證據難以保全的困境，加上目前多以行動裝置進行詐騙，這些數位證據容易毀損且還原，加密的雲端資料也因加密而難以取得，即便取得要將加密資料解析時業者的消極以對，使得即時性證據流失，而錯失瓦解詐騙集團的契機(EC, 2023; SOCTA, 2023)。

3. 制度不完善使資源配置出現問題

打擊電信網路詐欺是重中之重，然而法律更新遠比新型犯罪模式以及科技發展速度來的落後，若無法即時跟上國際的變化，勢必對於打擊電信網路詐欺犯罪潑了一盆冷水，未來將會遭遇到更大的挑戰。此外，歐盟是多個會員國的聯合組織，因此歐盟機構對會員國來說，是否有絕對的強制力還有待觀察，常見的機構內部協調問題，多個機構轄下部門的工作內容似乎有重疊，會造成工作推託的情形，加上空有相當強大的資源，卻因本位主義而整合不易，也導致訊息傳遞延遲進而導致決策拖延，錯失最佳打詐機會。另外歐盟機構外部合作實際操作上有其困境，尤其法令雖規範私營企業應該與公營企業互相合作，然私營企業以獲利為優先，對於法律的遵守以最低標準為之，也使得公私協作不足，更嚴重的是資訊共享若只是最低限制的配合，將難以達到打擊詐欺的目標(EC, 2023; SOCTA, 2023)。

4. 社會環境因素且新興手法不斷

由於電信網路詐欺犯罪儼然成為組織型態犯罪，透過跨國網絡形成，且多項資源整合下，詐欺犯罪的專業分工，造成許多查緝上的斷點，甚至以合法掩護非法來進行犯罪。而此時民眾防詐意識的不足情況下，警覺性不高加上投機心理影響，過度信任詐欺犯罪

人的說詞，且本身若資安觀念薄弱，一旦落入詐騙集團所設下的陷阱，多的是傾家蕩產的案例。更有些受害者深怕自己的陋行曝光，常自認倒楣而報案意願低落，加上目前對於受害者損失的金錢難以追回，使得犯罪黑數難以察覺。

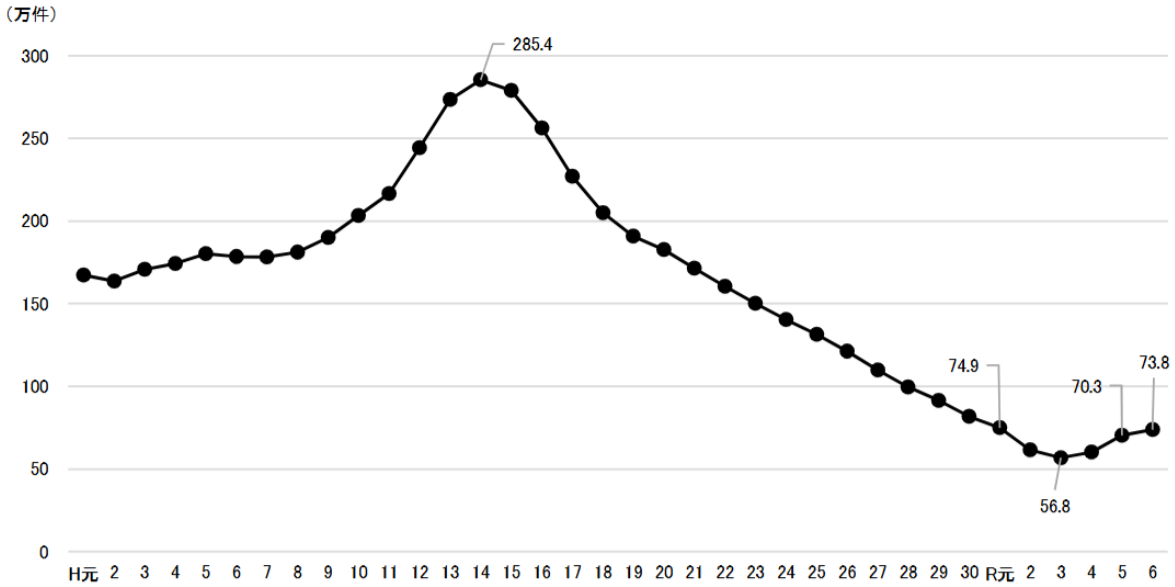
三、 日本

(一)日本電信網路詐欺現況分析

全球反詐騙聯盟 (GASA)的《2024 年日本詐騙狀況報告》，報告指出犯罪者與被害者多半使用 Instagram、Facebook、訊息應用程式 LINE 或約會應用程式進行第一次的接觸。日本警察廳公佈的 2023 年特殊詐騙統計，特殊詐騙是一種犯罪行為的總稱，指通過給受害人打電話等方式，在不見面的情況下取得對方信任，之後讓其給指定活期帳戶匯款，從而騙取現金或其他資產。此類案件多集中在大都市圈，主要的犯罪手法包括謊稱返還醫療費或保險費、退費詐騙、冒充家屬、哄騙老年人的「現金卡詐騙盜竊」、網路電子貨幣詐騙等，尤其是透過網路銀行進行行為激增(Ando, Hieu, Haoqian, Liu, & Takefuji, 2025)。日本傳統的犯罪多數是組織犯罪，在 1991 年的時候，犯罪組織人口高達 91,000 人(NPA,2024)，儘管組織犯罪集團保持低調活動，但近年來影響力持續下降，從 2005 年以降，日本全國有效實施策略打擊下，加上社會上多數民眾對組織犯罪集團有排除等因素下，其影響程度越來越低。隨著組織犯罪集團影響力的減弱，結構化的組織犯罪集團多半會考量法律規範與社會文化，而許多沒有明確的結構的犯罪集團，由於鬆散的結構，便成為警方積極的打擊對象。然而犯罪移轉的情形下，日本出現了新的組織犯罪團體，「匿名流動犯罪集團」(anonymous and fluid criminal groups)。匿名和流動性犯罪集團的一個特點是更難識別他們的組織和成員，除了集團核心部分，多數成員是匿名的、鬆散的成員，更喜好僱用新的最低級別成員作為“一次性”特工來讓他們犯罪，最顯著的犯罪型態就是電信網路詐欺犯罪。

從圖 5 來看，日本從 2003 年至 2021 年，犯罪通報總數持續減少，但 2024 年犯罪總數有 737,679 起，是自 2021 年以來連續第三年上揚，增加 4.9%。續從 2024 年的犯罪

情勢報告來看，當中詐欺犯罪的部分，財產犯罪的損失金額比前一年增加了 59.6%，達到約 4021 億日圓，大大超過了 2002 年的水平，是 1989 年以來的最高值（圖 6）。從具



體數字來看，詐欺造成的損失約為 3,075 億日圓，比前一年大幅增加（增加了 89.1%）。從圖 7 來看，日本的詐欺犯罪總數 2019 年時 32,207 件，到了 2024 年來到了 57,324 件，比起 2023 年的詐騙案件數量比前一年增加了 24.6%，詐欺犯罪總數的增加，對比圖 5 的財損統計表，財損金額也是急速增加中，顯示日本的詐欺犯罪也是相當的嚴重。再從表 9 的涉入詐欺犯罪的因素來看，最常見的詐騙動機是「生活困頓」，2019 年有 34.8%，到了 2024 年來到了 39.9%，排名第二的因素是「遊樂費用」需求，介於 20%至 27%之間，排名第三的是「擁有和消費」的需求，大約一成左右。

圖 5 日本近二十年來犯罪趨勢圖。資料來源：令和六年犯罪趨勢報告(NPA, 2025)

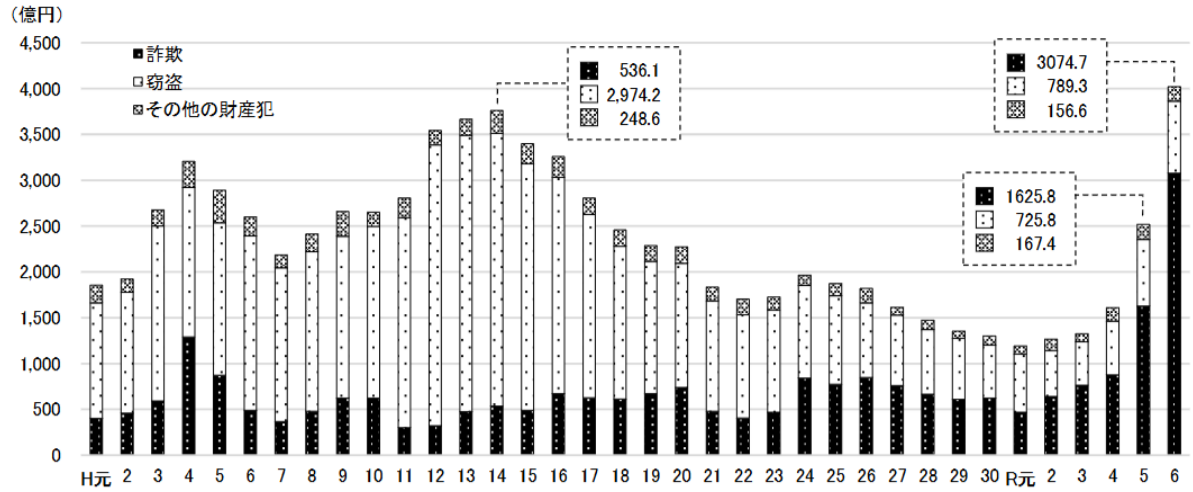


圖 6 日本近二十年來財產犯罪損失金額趨勢圖。

資料來源：令和六年犯罪趨勢報告，(NPA, 2025)

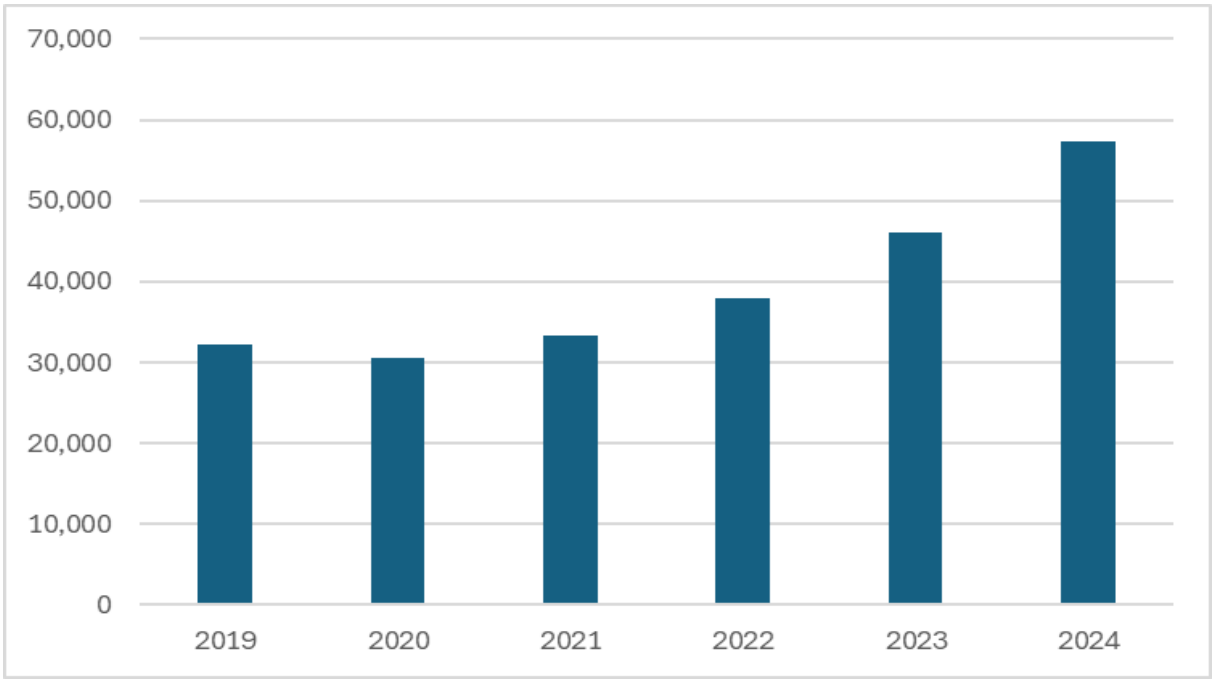


圖 7 日本 2019-2024 年詐欺犯罪統計趨勢圖。

資料來源：令和六年犯罪趨勢報告，(NPA, 2025)

表 15 日本近六年來從事詐欺犯罪之因素統計

	生活困頓	遊樂費用	擁有和消費	債務返還	動機不明	其他
2019	34.80%	26.60%	10.30%	5.80%	3.40%	19.10%
2020	37.90%	25.40%	10.30%	6.90%	3.60%	15.90%
2021	36.70%	27.10%	9.50%	6.50%	3.60%	16.50%
2022	37.70%	25.70%	10.00%	6.20%	3.50%	17.00%
2023	39.20%	22.90%	9.10%	6.40%	4.30%	18.10%
2024	39.90%	20.90%	9.30%	7.00%	6.40%	16.60%

資料來源：令和六年犯罪趨勢報告，(NPA, 2025)

日本詐欺統計當中有一項「特殊詐欺」，日本特殊詐欺是指在未與被害人見面的情況下，透過電話、網路、傳真、電子郵件等非面對面的方式，騙取他人的金錢。特殊詐欺的被害人多為需要前往金融機構匯款，匯款至指定人頭帳戶，詐欺犯罪型態像是猜猜我是誰（Ore ore）、假檢警詐欺，其手段多半為欺騙被害人帳戶被用於犯罪、低利貸款、假帳單、投資詐欺、ATM 卡盜刷等，這類的詐欺都鎖定老年人以及社會弱勢群體。從日本《刑法》第 246 條第 1 項：「詐欺而使其交付財物者，處 10 年以下有期徒刑」、第 2 項：「透過前項方法取得非法財產利益或使他人取得非法財產利益，亦同」。本條文即清楚規範以「財物」與「財產上的利益」為主體的詐欺罪，只要構成侵害各個財物與財產上利益持有的犯罪即可認定屬於詐欺。

從日本警察廳資料來看[36]，2024 年，特殊詐欺案件數為 20,987 件，比起去年增加 1,949 件，增長 10.2%，受害金額為 721.5 億日圓，比起去年增加 269.0 億日圓，增加 5.99%。從地區來看，特殊詐欺都主要集中在大都會區，其中東京都 3,494 件、大阪府 2,658 件、神奈川縣 2,000 件、埼玉縣 1,589 件、愛知縣 1,461 件、兵庫縣 1,442 件、千葉縣 944 件。上述 7 個通報案件數占總數的 64.7%。每日受害金額為約莫 1 億 9,714 萬

[36] 日本警察庁網站，令和５年における特殊詐欺の認知・検挙状況等について，網址：https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2024.pdf ，最後瀏覽 日期：2025 年 4 月 13 日。

日圓。此外，利用網路資訊來從事投資詐欺和利用社群媒體的戀愛詐欺的受害者數量急劇增加。2024 年發生 10,164 起，損失金額約 1,268 億日圓，分別比前一年增加了 164.3% 和 178.6%。再從特殊詐欺的樣態來看，以下分別敘述：

1. 是我啦詐欺(オレオレ詐欺)[37]：包括「是我啦」、存款及儲蓄詐騙、現金卡竊盜三種，這三類案件數為 10,413 件，比起 2023 年增加 1,487 件，15.4%，損失金額為 502.2 億日圓。其中「是我啦」件數為 6,752 件，比 2023 年增加 70.7%，損失金額為 458.4 億日圓。存款儲蓄詐欺件數為 2,276 件，年減 17.4%，損失金額為 25.5 億日圓。現金卡詐欺案件量為 1,385 起，年減 37.5%。

2. 虛假收費詐欺(架空料金請求詐欺)[38]：假帳單詐欺件數為 5,716 件，年增 10%，損失金額為 133.8 億日圓，檢舉案件數增加，損失金額減少。「假客服詐欺」是指詐騙分子以幫助受害者清除電腦病毒為藉口，誘騙受害者交出電子貨幣和其他金錢的詐欺類型。假客服共發生 1,524 起，年減 29.7%，損失金額達 10 億日圓。「求職詐欺」的案件增加至 2,342 件，年增 142.2%，增加幅度相當大。

3. 退款詐欺(還付金詐欺)：退款詐欺意旨假借退還款項而取得帳戶資料，進而騙取被害人將金錢轉入特定帳戶，案件數為 4,070 起，年減 2.7%，損失金額為 63.7 億日圓。案件數雖然減少，但損失金額增加。

4. 社群媒體投資詐欺：另外日本正興起的社群媒體(social networking service，SNS)投資和戀愛詐欺，其增長速度可謂電信網路詐欺之冠。從圖 8 的統計圖來看，2024 年利用 SNS 進行的投資及戀愛詐欺的舉報案件數為 10,237 件，比起 2023 年增加 6,391 件，增幅達 166.2%，財損金額為 1,271.9 億日圓，也增加了 816.8

[37] 日本警察庁網站，令和６年における特殊詐欺及びＳＮＳ型投資・ロマンス詐欺の認知・検挙状況等について（確定値版）頁 2，網址：https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2024.pdf ，最後瀏覽日期：2025 年 10 月 9 日。

[38] 頁 2，同註 37。

億日圓，增幅達 179.4%。其中 49.2%集中在大都會區[39]，反而其他非電信網路詐欺案件相比，並不集中在大都會地區由於大都會地區的電信網路分布較密集。從兩個年度來比較，投資詐欺的增加幅度驚人，顯示日本電信網路詐欺仍是以電信詐欺為最大宗，其次則是以網路為主的社群軟體交友。日本警察廳更進一步調查，統計社群媒體投資詐欺犯罪者所用的工具，由於社群媒體投資詐欺案件數在 2024 年總數 6,413 件[40]，犯罪者與被害者最初開始接觸的社群媒體中，以 Instagram 為最多有 1,481 件，占 23.1%，使用 LINE 的為 1,120 件，占 17.5%，使用 Facebook 為 997 件，有 15.5%，上述三種社群軟體就佔比超過一半。值得注意的是使用 TikTok 的案件呈上升趨勢。不管是透過何種社群媒體來進行初始的接觸，高達 90%，有 5,829 起的犯罪者在施行詐欺時，使用的通訊工具為 LINE，與台灣的詐欺犯罪模式雷同。再進一步看被害人是如何獲得訊息的方式，最多的方式是看到廣告而被吸引的有 2,901 件，占 45.2%，收到網路訊息的有 2,133 件，占 33.3%[41]，這兩種就已經接近八成。配合 Instagram、Facebook 以及 LINE 的大量冒充投資者或名人的“虛假廣告”，使得日本的社群軟體投資詐騙案件居高不下。

以戀愛詐欺來看，2024 年 SNS 戀愛詐欺舉報件數為 3,824 件，增幅 142.8%，損失金額為 400.9 億日圓，增幅 126.1%，舉報件數和損失金額均比 2023 年大幅增加為兩倍。尤其在愛情的劇本中，要求被害者加碼「投資」的案件數為 2,797 件，占 73.1%，損失金額為 344.1 億日圓，占 85.8%[42]。社群媒體戀愛詐欺的初始接觸工具也都是利用 Instagram、Facebook 居多，1,637 起占 42.8%，另外就是使用配對應用 APP 的約會軟體有 1,311 例，占 34.3%，當開始接觸後，隨即

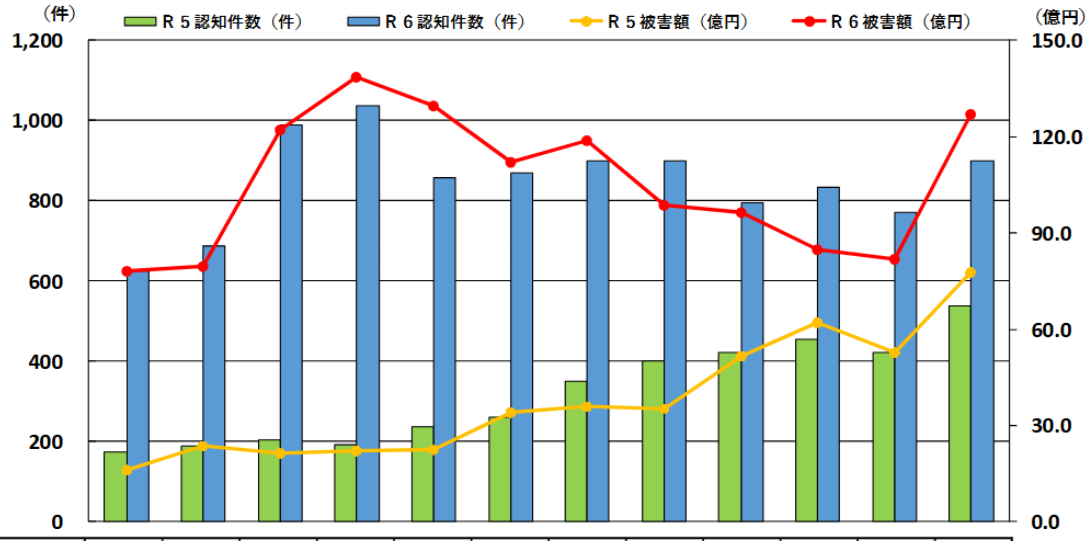
[39] 頁 5，同註 37。

[40] 頁 6，同註 37。

[41] 頁 9，同註 37。

[42] 頁 10，同註 37。

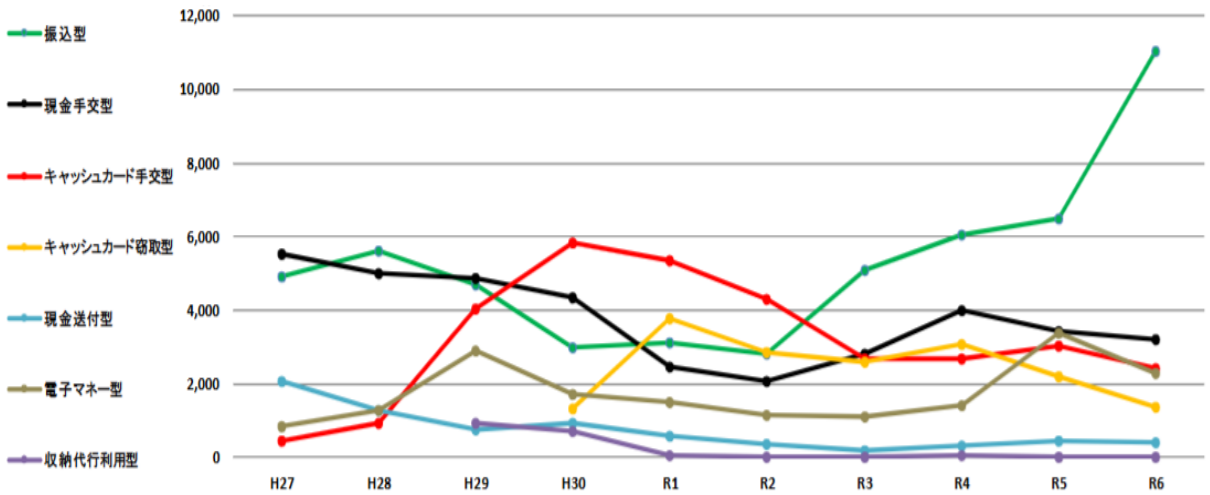
轉用 LINE 來當作主要犯罪工具，3,609 件占 94.9%[43]。日本詐欺犯罪集團多半利用社群媒體的留言與簡訊功能來接觸被害者，許多被害者在不知情的情況下，誤入愛情詐欺的陷阱中。



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
R５認知件数（件）	173	188	205	193	237	261	350	401	422	454	423	539
R５被害額（億円）	16.1	23.8	21.4	22.1	22.6	33.9	36.1	35.1	51.5	62.0	52.9	77.6
R６認知件数（件）	626	688	989	1,037	857	871	899	901	794	833	770	899
R６被害額（億円）	78.1	79.6	122.1	138.6	129.7	112.0	119.0	98.8	96.4	84.7	82.0	127.0

圖 8 日本 2023 年至 2024 年社群媒體投資與愛情詐欺趨勢圖。
資料來源：令和六年犯罪趨勢報告，(NPA, 2025)

從被害者交付被詐欺款項的方式來看(圖 9)，包括銀行轉帳、現金交付、現金卡交



[43] 頁 12，同註 37。

接、現金卡盜取、電子貨幣以及 ATM 轉帳等。銀行轉帳類案件 11,048 件，增加了七成，損失金額達 431.4 億日圓，佔總比例為 59.8%。報告顯示，其中利用網路銀行進行轉帳金額在 500 萬日圓以上的案件共 1,023 起。電子貨幣詐欺為 2,279 件，年減 32.4%），損失金額為 18.4 億日圓。

圖 9 特殊詐欺被害人財物交付手法趨勢圖。資料來源：令和六年犯罪趨勢報告，(NPA, 2025)

在日本的詐欺犯罪中，欺騙被害人最常使用的工具是電話，約莫 79.1%，其次是電子郵件與簡訊通知，佔有 9.7%、網頁彈跳視窗廣告有 8.9%、明信片詐欺有 2.3%，其中電話詐騙佔比接近 80%。當中「是我啦」特殊詐欺、退款詐欺 99%以上都是透過電話來接觸被害人。在假帳單詐欺中，37.4% 是電話詐騙，31.7% 是彈出視窗，25.9% 是電子郵件詐騙。透過電話詐欺的方式多半以詢問來電者地址、姓名、資產、金融機構等的理由，配合各種虛假劇本的應用，取得被害人信任後再加以詐騙。根據日本警察廳統計資料，涉嫌特殊詐欺的電話高達 192,686 通，一個月平均增加至 16,057 通，年增率高達 46.1%。

(二)日本打擊電信網路詐欺的相關法律

數位科技與經濟和人們日常生活具有緊密的相關性，日新月異的包括無現金支付方式、數位醫療服務和遠距工作等領域，這使得網路犯罪成為日本的重要議題。網路詐騙和網路釣魚詐騙在世界各地迅速增長，2022 年網路和電話詐騙案件通報數為 17,570 件，年增加 21.2%，損失金額為 371 億日圓(NPA, 2023)。2023 年網路和電話詐騙數量增加了 8.3%，達到 19,033 起案件，為 10 年來最多，而與海外犯罪團夥有關的人數也創歷史新高週四。其中 2,271 件為投資詐騙案件，損失總額約為 278 億日圓，主要針對 50 多歲和 60 多歲的男性以及 40 多歲和 50 多歲的女性(NPA, 2024)。由於電信網路詐欺犯罪隱密性高，科技日新月異下，兼顧法律與人權的考量，打擊電信網路犯罪可說是整合各方面而為之。為了有效打擊電信網路詐欺犯罪，日本政府加強網路使用的相關法律的修訂，強化公私合作的重要性。

日本《刑法》第 37 章[44](Chapter XXXVII Crimes of Fraud and Extortion)談到詐欺犯罪，當中第 246 條第 1 項(Article 246-1)：「詐欺而使其交付財物者，處 10 年以下有期徒刑」、第 2 項：「透過前項方法取得非法 財產利益或使他人取得非法財產利益，亦同」。本條文即清楚規範以 「財物」與「財產上的利益」為主體的詐欺罪，只要構成侵害各個財 物與財產上利益持有的犯罪即可認定屬於詐欺。而第 246 之 2 條[45](Article 246-2) 則是電腦詐欺罪(Computer Fraud)：「除前條所規定者外，凡以虛偽資訊輸入或非法指令輸入，作用於他人進行事務處理所使用之電腦，製作與財產權之取得、喪失或變更有關之不實電子或磁性記錄，或將此類不實電子或磁性記錄用於他人之事務處理，從而獲取自己或使他人獲取財產上的不法利益者，處以十年以下有期徒刑。」刑法中的規範是日本詐欺罪的法源依據。此條文針對的是「以虛偽資料操作他人電腦系統進行財產詐欺」的行為，強調「電磁記錄」的造假使用。涉及「他人事務處理」通常指的是公司、金融機構等的正常業務流程。

1、 未經授權使用電腦詐欺罪法 [46](不正アクセス行為の禁止等に関する法律,Act on Punishment of Unauthorized Computer Access)

該法案在 1999 年提出，由於資訊科技的發展和網路的普及化，連帶網路犯罪也層出不窮，特別是電信網路詐欺案件已經嚴重影響社會安全和經濟。日本內閣提出了針對網路犯罪的法律草案來打擊相關犯罪行為。該法案中的第 2 條[47]針對電腦詐欺犯罪做出

---

[44] 第二百四十六条人を欺いて財物を交付させた者は、十年以下の懲役に処する。 Japanese Law Translation. (2023). *Penal Code*. Retrieved from https://www.japaneselawtranslation.go.jp/en/laws/view/3581 ，最後瀏覽日：2025 年 3 月 5 日。

[45] 第二百四十六条の二前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、十年以下の懲役に処する。同註 31。

[46] Japanese Law Translation. (2023). *Act on Punishment of Unauthorized Computer Access*. Retrieved from: https://www.japaneselawtranslation.go.jp/ja/laws/view/3933 ，最後瀏覽日：2025 年 3 月 5 日。

[47] 第二条この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利

明確的定義，尤其是「未經授權的計算機使用」和「計算機系統」，確定法律適用的範圍與對象。檢察與執法機關提供了法律依據。第 3 條[48]是禁止未經授權的計算機使用，從第 4 條開始，對於未經授權的電腦使用加以規範，包括不得假冒資訊管理人員或著其他非正當理由來取得使用他人電腦的權限。第 8 條[49]則是規範電腦系統的管理人員應盡力且妥善管理電腦系統資訊的存取權，同時要驗證這些管理手段的有效性，做出及時改善與相對應的緊急措施，此條文規範了系統服務提供者的責任與義務。第 9 條[50]則針對發生疑似的非法電腦詐欺行為時，都道府縣公共安全委員會或者警察機關要求提供相關資訊時，應及時給與，做為未來緊急應變措施的參考依據。第 10 條[51]則規範國家安全委員會應至少每年定期公告相關的電腦詐欺犯罪資訊以及應對措施。從 11 條之後，則是對違反相關規定應判定的懲處，包括涉及詐欺犯罪者處以三年以下有期徒刑或一百萬日圓以下罰款，而應提供相關風險管理與有效策略的服務提供商若是違反相關規定，則處

用」という。）につき当該特定電子計算機の動作を管理する者をいう。同註 33。

[48] 第三条何人も、不正アクセス行為をしてはならない。同註 33。

[49] 第八条アクセス制御機能を特定電子計算機に付加したアクセス管理者は、当該アクセス制御機能に係る識別符号又はこれを当該アクセス制御機能により確認するために用いる符号の適正な管理に努めるとともに、常に当該アクセス制御機能の有効性を検証し、必要があると認めるときは速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする。同註 33。

[50] 第九条都道府県公安委員会（道警察本部の所在地を包括する方面（警察法（昭和二十九年法律第百六十二号）第五十一条第一項本文に規定する方面をいう。以下この項において同じ。）を除く方面にあっては、方面公安委員会。以下この条において同じ。）は、不正アクセス行為が行われたと認められる場合において、当該不正アクセス行為に係る特定電子計算機に係るアクセス管理者から、その再発を防止するため、当該不正アクセス行為が行われた際の当該特定電子計算機の作動状況及び管理状況その他の参考となるべき事項に関する書類その他の物件を添えて、援助を受けたい旨の申出があり、その申出を相当と認めるときは、当該アクセス管理者に対し、当該不正アクセス行為の手口又はこれが行われた原因に応じ当該特定電子計算機を不正アクセス行為から防御するため必要な応急の措置が的確に講じられるよう、必要な資料の提供、助言、指導その他の援助を行うものとする。同註 33。

[51] 第十条国家公安委員会、総務大臣及び経済産業大臣は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、毎年少なくとも一回、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表するものとする。同註 33。

以一年以下有期徒刑或五十萬日圓以下罰款。

2、 高度情報資訊通信基本法[52] (高度情報通信ネットワーク社会形成基本法，Basic Act on the Formation of an Advanced Information and Telecommunications Network Society)

日本政府在 2000 年提出了《高度情報資訊通信基本法》的初步草案，鑒於資訊通信技術的應用而在全球範圍內發生的社會經濟結構的快速而重大的變化，迫切需要妥善應對，為了制定資訊通信網路社會的基本原則和措施，明確國家和地方政府的責任，希望建立一個全面的法律框架以促進資訊通信技術的發展和保障安全。在立法過程中，著重於網路科技技術發展所伴隨的消費者保護，更重要的是如何確保網路安全的議題去探究，最終在 2001 年通過，並在同年生效。此法案所稱的「高度資訊通信網路社會」是指通過網際網路和其他資訊通信網路，在全球範圍內自由、安全地獲取、共用或傳播各種資訊或知識。本法案的第 25 條規範內閣必須成立高度資訊網路社會推進戰略本部(高度情報通信ネットワーク社会推進戦略本部)，掌管網路基本法以及執行相關業務。

第 7 條[53]與強調政府應採取措施保障資訊通信系統的安全，防範網路犯罪。這一條文直接針對保障資訊安全的措施，促使政府制定相應的政策和技術標準，以減少電信網路詐欺的發生。第 10 條[54]到 13 條強調國家中央與地方政府應該通力合作與必要的立法，來促進先進網路的資訊社會責任，同時政府也應該將高度資訊通信網路社會的統計資料，

---

[52] Japanese Law Translation. (2023). *Basic Act on the Formation of an Advanced Information and Telecommunications Network Society*. Retrieved from https://www.japaneselawtranslation.go.jp/laws/view/6021，最後瀏覽日：2025 年 3 月 5 日。

[53] 第七条高度情報通信ネットワーク社会の形成に当たっては、民間が主導的役割を担うことを原則とし、国及び地方公共団体は、公正な競争の促進、規制の見直し等高度情報通信ネットワーク社会の形成を阻害する要因の解消その他の民間の活力が十分に発揮されるための環境整備等を中心とした施策を行うものとする。同註 39。

[54] 第十条国は、第三条から前条までに定める高度情報通信ネットワーク社会の形成についての基本理念（以下「基本理念」という。）にのっとり、高度情報通信ネットワーク社会の形成に関する施策を策定し、及び実施する責務を有する。同註 39。

透過網路來公佈，強調透明化[55]。為了擴及資訊社會的對象，第 19 條強調政府做為應包括審查法規、制定新的規章制度、妥善保護和運用智慧財產權、保護消費者權益、以及促進電子商務所需的其他措施等，顯見該法案已經考慮到利用網路進行詐欺犯罪的可能範疇。

3、 數位交易平台消費者權益保護法[56](取引デジタルプラットフォームを利用する消費者の利益の保護に関する法律，Act on the Protection of Consumers Who Use Digital Platforms for Shopping)

鑑於資訊通信技術的進步，數位交易平台已成為日本國民主要的消費生活方式，由於詐欺犯罪透過網路數位平台來的遂行，犯罪者使用數位交易平台作為非法取得他人財物的資訊工具，該法案能夠保護使用數位交易平台的消費者的利益，減少網路詐欺犯罪的可能風險。法案的第 2 條開始便對於數位交易平台做明確的定義規範，從個人到企業，只要是透過網際網路進行交易的行為，都受到本法案的規範。第 5 條[57]中規範消費者為行使請求權所必需的賣方等的姓名或名稱、地址等資訊，可向提供該數位交易平台的數位交易平台提供者請求披露其持有的賣方等的賣方資訊，顯見是為了數位交易平台的實名制，便於查緝相關犯罪。不過本法案僅限於對於交易上的糾紛有所解決的依據，對於電信網路詐欺犯罪的多樣性能稍嫌不足。

4、 支付服務法[58] (資金決済に関する法律，Payment Services Act)

電信網路資訊年代的來臨，交易手法不再侷限於實體貨幣，日本政府對於預付支付工具、電子支付工具、加密貨幣、兌換交易以及銀行交易等手法，確保與貨幣與金融秩

---

[55] 第 14 條。同註 39。

[56] Japanese Law Translation. (2023). *Act on the Protection of Consumers Who Use Digital Platforms for Shopping*. Retrieved from https://www.japaneselawtranslation.go.jp/ja/laws/view/4310，最後瀏覽日：2025 年 3 月 5 日。

[57] 同註 43。

[58] Japanese Law Translation. (2023). *Payment Services Act*. Retrieved from https://www.japaneselawtranslation.go.jp/ja/laws/view/4477 ，最後瀏覽日：2025 年 3 月 5 日。

序能平穩，因此於 2009 年制定了此法案。該法案也對於相關的支付工具規定了交易的安全義務，對於金融服務提供者在防範詐騙方面的責任設有要求，違反者將面臨法律後果。從第 2 條[59]開始便明定本法的適用範圍，第 3 條[60]則針對數位支付工具做出定義，更重要的是從第 22 條[61]開始，預付或支付工具發行者必須依照內閣的規定，準備並保存與有關的帳簿和文件並且定期繳交業務部告，必要時內閣府可命令金融服務業者提供報告資料，或派官員進入了解或檢查其賬簿、文件和其他物品，經發現有所缺失，可命令其改善[62]，若情節重大則可以命令其全部或部分停止發行業務[63]。更值得注意的是第 36 條[64]規定，在外國從事預付支付工具發行業務的人不得向日本國內的人推銷該外國發行的預付支付工具，此舉避免海外支付工具的濫用以及成為網路詐欺犯罪匯兌的溫床。

此法案的第三節(Section 3 Supervision)談到了如何進行支付工具的監督。電子支付工具業務經營者必須依照內閣府條例的規定，準備和保存與其電子支付工具業務有關的帳簿和文件[65]，每個營業年度編制電子支付手段業務報告並向上提交[66]，同樣也允許政府機關單位視情節嚴重與否來進入發行機構中進行偵察工作。在第三章(暗号資産，Chapter III-3 Cryptoassets)的部分則是針對加密貨幣進行規範。對於營運加密貨幣的業者，必須實名登記[67]。加密貨幣的兌換具有高度隱密性，因此加密貨幣兌換服務提供者必須依據內閣府令採取必要措施，防止與其加密貨幣兌換業務相關的資訊的洩漏、遺失或毀損，

---

[59] 同註 45。

[60] 同註 45。

[61] 第二十二条前払式支払手段発行者は、内閣府令で定めるところにより、その前払式支払手段の発行の業務に関する帳簿書類を作成し、これを保存しなければならない。同註 45。

[62] 第 25 條，同註 45。

[63] 第 26 條，同註 45。

[64] 第三十六条外国において前払式支払手段の発行の業務を行う者は、国内にある者に対して、その外国において発行する前払式支払手段の勧誘をしてはならない。同註 45。

[65] 第 62-18 條，同註 45。

[66] 第 62-19 條，同註 45。

[67] 第 63-2 條，同註 45。

並確保此類資訊的全面性管理[68]。為了強制加密貨幣業者執行力，必須遵守政府的相關規定，提供必要的保護措施來確保加密貨幣的可靠性。第四章則是外匯交易規範(為替取引分析，Chapter IV Funds Transfer Transaction Analysis)，包括提供相關金融服務的業者必須公開透明，負起保護使用客戶的交易安全，全程資料的保存與提供的義務等，目的是將現行多樣化的支付工具納入政府法規的管理中，進而降低電信網路詐欺犯罪利用這類支付工具作為犯罪用途。第八章則是違反相關規定後的罰則，第 107 條規定違反該法的規定，最重可處 3 年以下有期徒刑、300 萬日圓以下罰金。

5、 金融商品交易法[69] (金融商品取引法，Financial Instruments and Exchange Act)

日本的《金融商品交易法》（Financial Instruments and Exchange Act）是打擊電信與網路詐欺犯罪的核心法律之一，特別針對金融詐欺、虛假資訊、操縱市場等行為，提供了明確的法律依據與處罰機制。最近的修法是 2022 年的修訂，首先是加強投資者保護與資訊揭露，修法明確禁止在金融商品銷售過程中進行虛假陳述或欺詐行為，並加重對違法行為的處罰，以保護投資者免受不實資訊的誤導[70]。除此之外更要求金融機構在銷售金融商品時，提供更全面且易於理解的資訊，特別是對於風險較高的商品，如衍生性金融商品，需詳細說明其風險特性[71]。第二是數位化與金融科技的法規調整，針對網路平台銷售金融商品的業者，明確其需遵守的法規範圍[72]，並強化對其業務行為的監督，以防止詐騙行為的發生。為了強化金融交易的安全性，法條規定要求金融機構在開立帳戶或進行交易時，採取更嚴格的身份驗證措施，如多因素認證，以防止他人冒用身份進行詐騙[73]。由於金融秩序需要維持，因此需建立更完善的交易監控系統，及時發現並報

---

[68] 第 63-8 條，同註 45。

[69] Japanese Law Translation. (2023). *Financial Instruments and Exchange Act.* Retrieved from https://www.japaneselawtranslation.go.jp/ja/laws/view/4633 ，最後瀏覽日：2025 年 3 月 5 日。

[70] 第 37 條，同註 56。

[71] 第 27 條，同註 56。

[72] 第 29 條，同註 56。

[73] 第 38 條，同註 56。

告可疑的交易活動，特別是涉及大額資金轉移或異常交易模式的情況[74]。第八章的罰則則是針對違反金融商品交易法可能有相對應的懲處，依據各種不同的違法程度，最重可處以處 10 年以下有期徒刑、1000 萬日圓以下罰金[75]，或者沒收財產。進一部為了強化偵查力道，在第九章(犯則事件の調査，Chapter IX Investigations in Criminal Cases)的部分則是賦予查緝的法源依據。證券交易監督委員會可以要求犯罪嫌疑人或證人，檢查犯罪嫌疑人等持有或遺留的任何財產，或扣押犯罪嫌疑人等主動提交或遺留的任何財產[76]。

(三)日本打擊電信網路詐欺犯罪的機構

電信網路詐欺犯罪是近年來新興的犯罪手法，其犯罪樣態與組織規模相當複雜。對於第一線打擊電信網路詐欺犯罪的機構來說，充滿著相當多嚴酷的挑戰。從 1990 年代開始，隨著網際網路的普及和手機使用的增加，電信詐欺活動開始出現。最初的詐騙形式主要是電話詐騙。然而隨著電信與網路的結合，兩者密不可分，加上金融工具與手機的整合後，連帶詐欺犯罪的工具也簡化，被害者透過手機便能夠完成轉帳匯款等，使得詐欺犯罪愈來愈嚴重。內閣府（Cabinet Office）為日本最高行政機關，透過政策制定和協調，期望能夠促進各部門之間的合作，提升對電信詐欺的防範能力，特別在與網路安全和消費者保護相關的議題上。由於分工明確，內閣府必須扛起全責，通過跨部門合作，推動整體的防範政策和措施(Saeki, Kitayama, Koga, Shimizu & Oida, 2022)。

日本法務省（Ministry of Justice）則是負責刑事法律的制定和執行，包括與詐欺相關的法律的提案與制定。打擊電信網路詐欺犯罪需要法源的支持，因此法務省提供打詐法律框架，協助警方和檢察官進行詐騙案件的調查和起訴，確保詐騙案件的法律程序正當且無違法之虞，完備整體的刑事政策。在法律架構完備後，刑事司法的部分日本政府先行規劃，隨後總務省（Ministry of Internal Affairs and Communications）為了抗制電信

[74] 第 39 條，同註 56。

[75] 第 197 條，同註 56。

[76] 第 210 條，同註 56。

網路詐欺犯罪的高科技演進，必須提升打詐的科技層次。因此對於日本的電信業務的管理和資訊技術的監督，都需要總務省的協助，將涉及網路安全的政策和規範加以完備。尤其電信網路為民營公司，多數民營私立機構多以營利為目的，唯有透過電信與科技業的監管政策與法規，才能確保電信公司遵守相關規範，將防範詐欺犯罪視為營運的責任與義務，才能電信詐欺犯罪有更全面的監控和防範措施(Ayumu, Hiroyuki, Kosuke, Tetsuya, Taichi & Takahiro, 2024)。

1、 警察廳（National Police Agency, NPA）

日本警察廳（National Police Agency, NPA）成立於 1948 年，負責全國的警察業務及公共安全。其工作主要負責調查和打擊各類犯罪，當然包括電信詐欺。設有專門的網路犯罪對策部（Cyber Crime Division），負責調查和打擊包括電信詐欺在內的各類網路犯罪，作為電信網路詐欺犯罪的指揮中心並協調全國各地方警察機關。對於打擊電信詐欺犯罪從可疑情資的收集開始，將大量可疑資訊與犯罪資訊進行分析，了解可疑詐欺活動的特點，確認後開始進行專案調查，查緝過程中需要與其他機構的合作，整體打擊電信網路詐欺的模式相當全面(NPA, 2024)。

從令和 6 年警察廳白皮書可知，警察廳對於電信網路詐欺犯罪預防方面，從三方面著手。首先是大眾宣導教育，警察廳定期舉辦研討會和宣傳活動，向民眾普及電信詐欺的識別技巧和防範措施，提升大眾的防範意識。其宣導的內容主要是以防詐騙資訊的手冊和海報，特別針對高風險群體，如老年人，提供針對性的教育資源。其次是深入社區進行合作，透過與地方社區和非政府組織合作，進行社區宣導活動，增強社區居民的警覺性，從預防做起，讓大眾辨識詐欺的虛假資訊，進而降低成為詐欺受害的風險。接著是查緝行動，由於警察廳設有網路犯罪安全部，因此能夠針對特定型態的詐騙案件進行深入調查。由於電信網路詐欺屬科技犯罪，因此針對對電子郵件、通話記錄和金融交易進行取證，確保證據的完整性和合法性。在檢調協作上，聽從檢察官指揮，定期向檢察機關報告，確保調查過程中的法律合規性，並準備起訴所需的證據。然而電信網路詐欺多為跨境類型的案件，警察廳也會透過與國際執法機構合作，追查跨國詐騙集團，打擊

國際電信詐欺行為。更重要的是能夠跨機構的資訊共享，與其他執法機構、金融機構及電信公司進行密切合作，形成聯合行動小組，提升查緝效率(NPA, 2025)。

2、 消費廳[77]（Consumer Affairs Agency）

隨著經濟發展和市場多樣化，消費者所面臨商品安全、詐騙行為以及不公平交易等問題，因此日本政府根據《消費者基本法》於 2009 年設立消費者廳。由於近來電信網路詐欺犯罪與消費行為息息相關，消費者廳開始加強對詐騙防範的工作，提供專門的資訊和支援，與警察廳及檢調合作，共同組成防詐網絡。消費廳主要是以消費行為的主管機關，因此首重消費者教育，近來電信網路詐欺與消費行為以及支付相關，因此定期舉辦講座、研討會和展覽會，主題圍繞電信詐欺的識別和防範，以提高公眾的認識。進一步與網站和社群媒體配合，提供有關電信詐欺的最新信息、受害者故事和防範技巧。對於較少上網的老年人來說，也會製作相關的消費者行為教育手冊來發放，提供易於理解的防範指導(Consumer Affairs Agency, 2024)。

當被害者或一般民眾無法得知相關訊息時，消費廳有設立專門的熱線[78]，為電信詐欺的受害者提供諮詢與支援，幫助他們了解如何報案和尋求法律援助。另外消費廳也成立了資訊中心，該中心定期發佈有關詐騙的報告、防詐指南和警示消息，透過網站、社交媒體和其他渠道向公眾提供最新的防範資訊，增強消費者的自我保護能力。此外更將所有收到的報案資訊以及相關的內容收集、整理，包括定期收集受害者的案例，記錄詐騙手法和事件的詳細信息，以便分析詐騙行為的趨勢和模式。接著會利用數據分析技術，該中心能夠識別出高風險的詐騙手法，並將這些信息用於提升公眾的防範意識。該資訊中心也會主動提供分析後的數據資料，幫助改善和制定針對電信詐欺的法律和保護措施(Consumer Affairs Agency, 2024)。

---

[77] Outline of the Consumer Affairs Agency. Retrieved from: https://www.caa.go.jp/en/ 最後瀏覽日：2025 年 3 月 5 日。

[78] 日本消費廳的受害者支援熱線號碼是 03-5449-0906。Retrieved from: 台北駐日經濟文化代表處 https://www.roc-taiwan.org/jp/post/331.html 最後瀏覽日：2025 年 3 月 5 日。

此外消費廳會及時發佈針對新出現的詐騙手法的警示，提醒消費者提高警覺。定期編制防詐指導手冊[79]，介紹如何識別常見的詐騙手法，例如假冒電話、網路釣魚等，並提供應對建議。更重要的是消費廳與警察廳共同合作來打擊電信網路詐欺犯罪，消費廳所收集的資訊與警察廳共享，分享受害者的案例和詐騙手法的分析結果，促進跨機構的合作。更在警方調查過程中，協助收集受害者的信息，分析詐騙行為的趨勢，並提供專業意見。消費廳雖然從犯罪預防的角度與被害者保護的議題為主，然而這些寶貴的資料與資訊，都將促進政府對於法律和規範的改進，以加強對消費者的保護(Consumer Affairs Agency, 2024)。

3、 日本金融廳(Financial Services Agency)

1990 年代末，日本經歷了金融危機，促使日本政府進行金融體系的全面改革。2000 年，為了加強對金融機構的監管和改善消費者保護，成立了日本金融廳（Financial Services Agency, FSA）。對於金融秩序的維持有巨大的影響力，尤其在電信網路詐欺盛行的今日，詐團利用現代化金融的隱密性與便捷性，對國家金融秩序造成巨大的損害。因此金融廳強化監管體系，對銀行、證券、保險等金融機構的全面監督[80]。

金融廳管轄的範圍為銀行、證券、保險等金融機構，在電信詐欺犯罪過程中，屬於犯罪利益實現的階段。因此監管金融機構則成為首要任務。根據金融商品交易法、銀行法等規範，金融廳要求所有金融機構必須實施客戶身份驗證程序，以防止詐騙行為的發生。金融廳也根據相關法律定期對金融機構進行監管，確保其在反詐騙措施上的有效性，並要求機構報告任何可疑的交易活動。由於金融機構是一般人最常接觸的機構，因此大眾教育宣導顯得格外重要，日本金融廳會通過媒體、社交平台等方式，發起多項宣傳活動，提高一般民眾對電信網路詐欺的認知。同時也針對多種詐欺犯罪的樣態，如虛假投

[79] 日本消費廳當中有消費者教育項目可參閱。Retrieved from: https://www.caa.go.jp/en/policy/consumer_safety 最後瀏覽日：2025 年 3 月 5 日。

[80]金融廳(2018 年 6 月)。金融検査・監督の考え方と進め方（検査・監督基本方針）p28-36。Retrieved from: https://www.fsa.go.jp/frtc/kikou/2024/20240528.pdf 最後瀏覽日：2025 年 3 月 5 日。

資、網路釣魚等，製作成教育材料來幫助識別各類詐騙手法[81]。

日本金融相關法律制定的相當完整，根據金融商品交易法規定，對可疑交易進行監控和報告，並設立必要的內部控制系統以防範詐騙行為。目前許多金融機構已經開始部署實時監控系統，這些系統能夠即時分析交易並識別可疑行為，從而快速採取行動。銀行法則規定金融機構必須建立完善的風險管理和報告系統，以便於及時識別和應對可疑活動。有鑑於此，金融廳便能夠利用金融機構所提供的數據進行分析，針對可疑的金融交易進行識別並採取行動，相關金融資訊也能提供檢調單位進行後續調查。打擊電信網路詐欺需跨部會合作，日本金融廳與警察廳、消費者廳及其他政府機構合作，共同打擊電信網路詐欺，分享情報和資料，以加強對詐騙行為的識別和應對。面對未來科技的變化，金融廳也將人工智能（AI）和機器學習（ML）技術來分析交易數據，識別潛在的詐騙行為。這些技術能夠通過模式識別和預測分析，及時發現異常交易，並自動生成警報，從而提高反詐騙的效率[82]。

4、 檢察廳（Public Prosecutors Office）

日本檢察廳的組織結構包括中央檢察署和地方檢察署，中央檢察署負責全國性的重大案件，而地方檢察署則處理地方範圍內的案件。檢察院的運作受到《檢察官法》和《刑事訴訟法》等法律的規範，以確保其公正性和獨立性。眾所皆知檢察廳的工作包括對涉嫌犯罪的個人或組織提起公訴，並在法庭上代表國家進行指控。然起訴前必須對犯罪案件進行收集證據、詢問證人和進行現場調查，對於警方的偵查活動進行指揮與監督，確保其在法律範圍內行使權力，並保護被告的法律權益。也應當負起公眾教育的責任，提高公眾對法律的認識，推廣法治觀念，並對詐騙、暴力犯罪等議題進行宣傳和教育(UNAFEI,2019)。

---

[81] 金融廳(2018 年 10 月)。コンプライアンス・リスク管理基本方針。Retrieved from: https://www.fsa.go.jp/news/30/dp/compliance_revised.pdf 最後瀏覽日：2025 年 3 月 5 日。

[82] 金融廳(2024 年 5 月 28 日)。金融機関における AI 利用の促進に向けた論点整理。Retrieved from: https://www.fsa.go.jp/frtc/kikou/2024/20240528.pdf 最後瀏覽日：2025 年 3 月 5 日。

日本檢察廳對於打擊電信網路詐欺犯罪，從犯罪資訊的獲得開始，檢察廳對於電信詐欺犯罪的資訊多數與日本警察廳合作，定期接收有關電信網路詐欺案件的報告和調查結果[83]。第二種則是透過受害者直接舉報的方式，檢察院能夠獲得第一手的犯罪資料，包括詐騙手法和受害情況。接著是當金融機構發現可疑交易或詐騙行為時，會依據法律要求向檢察院報告，提供相關的交易數據和客戶信息。最後則是利用內部和外部的數據庫，經過資料整合和分析，對於犯罪趨勢進行剖析。由於檢察院為司法機構，相關資訊必須藉由其他部門的協助，形成多機構的聯合行動，與警察廳、金融廳、消費者廳進行跨機構的聯合行動，從證據蒐集到犯罪活動介入，反詐騙行動的整體效能能夠提升(UNAFEI,2019) 。

嚇阻犯罪其中重要的一個關鍵因素是迅速性，日本檢察院設立專門的電信網路詐欺偵查單位，由具備法律、技術和調查專業知識的檢察官和偵查官組成，電信網路詐欺屬於科技犯罪，因此檢察院多數採用數位取證技術，對涉案的手機、電腦進行檢查，提取潛在的證據，包括通訊記錄、文件和網絡活動資料，而採證的過程遵循嚴格的紀錄程序，以確保其在法庭上的有效性和可接受性。能夠在正當程序下完成偵查、採證與起訴，以最短的時間內完成起訴過程，才能有效的嚇阻犯罪(UNAFEI,2019)。

(四)日本打擊電信網路詐欺犯罪的策略

根據內閣府(2025)的保護公民免於詐欺的綜合措施 2.0 政策，談到 2024 年財產犯罪造成的損失超過 4000 億日圓，尤其是詐欺犯罪造成的損失急劇增加，單 2024 年就超過了 3000 億日圓。詐欺犯罪是利用人們的信任遂行的犯罪行為，動搖支撐安全穩定社會的基礎，尤其是「民眾之間的信任」更是社會安定的關鍵。因此日本政府於 2024 年 6 月制定了首部專門針對詐欺犯罪行為的綜合性措施—《保護國民免受詐騙侵害的綜合性措

[83] 警察廳(2023 年 3 月 28 日)。特集：日常生活を脅かす犯罪への取組み，P22-37。Retrieved from: https://www.npa.go.jp/hakusyo/h21/honbun/pdf/21p00100.pdf 最後瀏覽日：2025 年 3 月 5 日。

施 2.0[84](国民を詐欺から守るための総合対策 2.0)》。該綜合性措施總體來說有七大面向，從法規的強化著手，將打擊電信網路詐欺的法源依據修訂完備，才能有效打擊電信網路詐欺。接著為了能夠應付日漸嚴重的詐欺犯罪，檢察院設立專門機構來應對，專注於該類犯罪的調查和起訴。由於電信網路詐欺為跨國組織犯罪型態，因此加強警察廳、金融機構、消費者保護機構和電信公司等的合作，建立信息共享機制，促進不同機構之間的聯合行動。然而最佳的犯罪預防是公眾教育的宣導以及即時的監控策略，透過各種不同的宣傳管道來提升國民對於詐騙手法的認知，避免落入詐騙陷阱當中。金融機構以及電信公司參與，能夠即時監控可疑的詐欺犯罪活動，第一時間能夠阻止並通報，避免損失擴大。對於被害者來說，提供法律和心理支持，能快速地協助復歸正常生活。以下就電信網路詐欺犯罪的具體抗制作為進行說明。

① 電信網路詐欺的對策

(1) SNS 型投資詐欺的對策（ＳＮＳ型投資・ロマンス詐欺対策）

① 公眾教育與宣傳

多數的 SNS 型投資和愛情詐欺多為未經金融商品登記的業者所進行的詐欺行為，為防止此類受害，政府將實施各相關省廳聯合的政府宣傳活動，並加強與業者團體等的聯繫，利用數位空間等各種媒體，提高網路安全素養的宣傳機會等，進行有效的宣傳。

② 電信業者的監控

SNS 型投資和愛情詐欺中，多利用社群交友軟體，因此對各服務的使用者進行個別且適時的注意提醒。此外，開設使用者專用的諮詢窗口，對於 SNS 上可能違反金融商品的廣告和信息積極主動給予提醒。日本政府也要求對 SNS 業者的廣告進行審查，避免民眾因為 SNS 上的偽廣告而導致投資詐騙的受害。具體來說，廣告發布前階段，對於封閉

[84] 警察廳(2025 年 6 月 9 日)。「国民を詐欺から守るための総合対策 2.0」の決定。Retrieved from: https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/250609/01.html 最後瀏覽日：2025 年 10 月 9 日。

型聊天的廣告原則上不予採用，並同時置入 SNS 型投資詐騙的資訊。對電信業者要求其加強對廣告預審，以及廣告業主的身分核實。對於發布後的廣告，必須設立請求刪除廣告的窗口，建立回報機制並公開相關資訊。

③ 廣告平台的監管

根據《金融商品交易法》，未經他人同意的情況下發布虛假廣告將遭到裁罰。同時對於虛假廣告嚴加審查與下架，假借名人肖像以投資詐騙為目的的廣告，企業經營者有義務查證，並要求其在收到用戶舉報或自行檢測時發現可疑情形時，迅速採取刪除廣告和凍結賬戶等措施。依據《特定電子通信所引起的資訊流通侵權等處理法》[85]，要求大型平台營運商加快刪除虛假廣告，並且明確哪些資訊屬於非法資訊，同時能夠針對這些非法資訊立即做出應對[86]。

④ 投資詐騙網站的抗制

對於眾多的投資網站的用戶，日本政府將收集各種虛假網站訊息並公告。根據《金融商品交易法》，金融廳將收集未註冊許可經營者的資訊，發出警告信並向法院提交禁止或暫停命令的申請，並且在網站上公佈此類經營者的名稱。

(2) 社群媒體和交友 APP 的防範措施(ソーシャルメディア／出会い系アプリを利用した詐欺)

① 預警與加強身分驗證機制

社群媒體是最初接觸被害者的聯繫工具。多數情況下，這些詐騙分子都是在 SNS 上被陌生人引誘加入 SNS 群組，在與這些群組不斷交流的過程中，被捲入利用 SNS 進行投資詐騙。因此日本政府要求 SNS 業者在未知帳戶添加為好友時，必須顯示警告、獲得

[85] 特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律。Retrieved from: https://laws.e-gov.go.jp/law/413AC0000000137 最後瀏覽日：2025 年 3 月 15 日。

[86] 第 26 條。同註 71。

同意等機制，防止 SNS 的投資和戀愛詐騙造成的損害。目前日本盛行的社群媒體的投資與愛情詐欺犯罪，多為冒充名人在社群媒體上鼓勵被害者進行投資，也有人利用官方社群媒體帳號獲取用戶信任，從而落入詐騙陷阱。因此，日本政府要求社群媒體業者在開設官方帳號時進行身分驗證。

② 立即暫停涉入犯罪的社群媒體帳號

當發現犯罪嫌疑人濫用社群媒體帳號和配對應用程式聯繫受害者時，一旦經舉報並確認為犯罪行為的帳號，立即暫停使用。此措施也同樣運用在儲蓄帳戶、加密貨幣交易帳戶，一經舉報立即停用或凍結該帳戶，方能有效降低 SNS 型投資詐騙並阻止犯罪持續，同時警察廳將被凍結儲蓄和銀行帳戶名單，回報給日本銀行協會。

③ 詐欺犯罪預防的金融教育計畫

《國家投資安全法》係針對公眾對資產管理的規範，2024 年 4 月成立的金融經濟教育推進機構將與相關部委和機構合作，在學校、工作場所以及社區中心和圖書館等當地社區等各種場所，向各年齡段的廣泛人群提供金融經濟教育，包括如何應對投資詐欺和財務困境等。特別是針對 10～20 歲的年輕人，透過課程指南等方式，鼓勵學校推廣金融經濟教育，向他們提供有關投資風險和財務困境應對方法的正確知識，同時提供有關社交媒體投資詐騙的案例。

(3) 網路釣魚詐欺(フィッシング詐欺)的應對措施

① 推動身份驗證與認證金鑰技術（DMARC[87] 等）：

鑑於語音釣魚郵件的詐欺犯罪造成金融機構匯款詐欺和信用卡盜刷的財損，日本總務省要求電信網路業者在電子郵件接收與發送電子郵件時，引進發信者身分認證機制

[87] Domain-based Message Authentication, Reporting and Conformance 的縮寫。收到的郵件的網域名稱與寄件者的網域名稱（Header From）一致時，視為認證成功，投遞到信箱的收件匣，若與寄件者的網域名稱不一致時，視為認證失敗，存放在垃圾郵件資料夾（隔離區）或不存放在信箱（拒絕區）的技術。

（DMARC5 等），進而減少可能的語音釣魚郵件與大眾的接觸。日本政府將推動下一代身分驗證技術 Passkey[88] ，鼓勵金融機構、電子商務聯盟採用該身分驗證機制，主動納入該技術而負起企業的防詐責任。

② 強制關閉釣魚網站

目前日本政府正積極修法要針對網路釣魚網站強制關閉，寄望電信業者與網路服務提供商能夠主動提出關閉請求，同時加強與相關組織的合作，能即時收到請求，一旦犯罪屬實主管機關能夠予以關閉。

③ 強化金融機構金流間的認證

強化電商與警方的合作關係，在保護個人資訊和防範財損措施之間取得平衡，並推動詐欺交易資訊的共享。為了更迅速、有效地打擊信用卡盜用行為，鼓勵各商家經調查而出現疑似可能的詐欺犯罪配合的信用卡，將疑似情資提供給各個信用卡發行機構等。由於加密貨幣是近年電信網路詐欺新寵兒，因此未經授權的加密貨幣交易所轉賬予以禁止。日本政府要求金融機構定期查核加密貨幣，並將檢查結果報告通知政府單位，防止加密貨幣成為詐欺犯罪的工具。隨著電子支付的使用範圍不斷擴大，電子支付帳戶被盜用的情況相當嚴重，因此日本政府要求業者公開類似詐欺手法的訊息，並要求業者強化身分認證機制。

④ AI 技術的運用

除了透過報案和檢舉等方式識別出釣魚網站外，對於尚未現蹤的釣魚網站，使用人工智慧生成等技術來檢測並發掘釣魚網站，目前由警察廳和都道府縣警察分別對網站是否為釣魚網站進行檢查判斷，未來希望透過 AI 生成式人工智慧來協助，將能有效的打擊釣魚詐欺。

[88] 由 FIDO 聯盟和萬維網聯盟標準化的無密碼身份驗證技術。據稱，由於身份驗證在釣魚網站等非合法網站上不起作用，因此可以有效降低身份驗證資訊外洩的風險。

2、 通話電信的預防作為

(1) 來電攔截機制

由於日本屬於高齡化社會，老人也成為電信詐欺的主要對象，為了防止接到犯罪者的電話，在老年人家中安裝具有騷擾電話攔截功能的裝置、家中的座機上停止撥打國際電話、拒絕接收隱藏號碼的電話、家中設置座機自動回覆留言等措施。目前推動的「優秀騷擾電話防盜設備推薦計畫」係由公益財團法人全國犯罪預防協會合作，推動具有騷擾電話防盜功能設備的普及。

(2) 強化高齡人口家中來電顯示與拒接國際電話

要求電信業者顯示來電號碼的服務，可強制雙向發話者顯示來電號碼之請求，推廣安裝自動檢測疑似特殊詐欺呼叫設備。尤其 70 歲以上的用戶免費提供各種服務的措施，進一步可設定未顯示來電拒接之電信服務。此外跨境來電詐欺有增加之趨勢，可申請中止國際電話服務。

(3) 打擊不當簡訊傳遞與立即發送預警訊息機制

因應利用簡訊進行網路釣魚詐騙（smishing）蔓延，日本政府要求電信業者預設的簡訊過濾功能，同時加強公眾意識教育，開放客戶檢舉釣魚簡訊。向上溯源追查發送釣魚簡訊的發話基地台，規範電信業者建立實名制發送短訊息認證服務，來阻絕惡意發送釣魚簡訊。另外要求業者建立自動攔截特殊詐騙等預警電話的號碼、設定了攔截來電通知的號碼、涉及海外通訊服務的電話號碼等措施。

3、 金融機構合作打擊與預防詐欺犯罪

(1) 建立金流監控與檢測機制

因為轉帳詐騙金額財損巨大，以及以企業經營模式來進行詐欺犯罪，針對這種情況，日本政府要求金融機構建立監測和發現取款、匯款和其他涉嫌詐欺交易的金流工具，包括預付支付工具和電子貨幣，加強其檢測能力，包括企業帳戶在內的詐欺帳戶訊息，將

利用可疑交易報告系統，與警方迅速分享資訊。日本政府欲建立一套系統，讓預付支付工具發行機構在發現使用詐欺性電子貨幣時，及時向警方提供資訊。

(2) 打擊惡意犯罪工具提供者

電信網路詐欺犯罪透過金融業務來做為犯罪工具，根據《防止犯罪收益轉移法》[89]的要求，加強使用儲蓄帳戶時的交易確認機制，防範儲蓄帳戶被利用。日本近年發現許多外國居民非法轉移的儲蓄帳戶被用於詐欺犯罪，以及冒充外國人盜用儲蓄帳戶，因此推動依居留期限管理儲蓄帳戶等措施。對於人頭帳戶凍結也是推行策略之一，一旦發現帳號被作為詐欺犯罪使用，即刻要求金融機構凍結該帳戶。警察廳編制已被凍結的儲蓄存款帳戶持有人名單，並將該名單提供給日本銀行家協會和其他組織，以促進防止開設詐欺帳戶。近來盛行的加密貨幣，也列入限制的範圍。日本金融廳要求金融機構強化監控措施，定期檢查並將檢查結果報告，同時對於違法的加密資產進行沒收和保管，引入執法和保全程序。

(3) 關懷問候與宣導

為了防止被害人遭詐而臨櫃大額提款轉匯，除了櫃檯與客戶交談外，還將根據各金融機構設定的客戶年齡、提款金額標準，主動積極關懷，經查有異立即向警方報告。老年人家中存放現金的「現金移交」詐騙案件日益增加，透過社區警政向老年人示警，告知家中存放大量現金的危險性，並建議他們採取利用金融機構存款和儲蓄等預防措施。透過巡邏等方式保持警惕，透過有效進行日常盤查和宣導，預防犯罪發生。

(4) ATM 機制的限制措施

加強對金融機構存款和儲蓄帳戶的監控，收集相關帳戶提領資料來進行預警。要求金融機構推動對未進行過任何 ATM 轉帳的老年人設定 ATM 轉帳限額，ATM 取款小

[89] 犯罪による収益の移転防止に関する法律。e-gov 法令検索。 Retrieved from: https://laws.e-gov.go.jp/law/419AC0000000022 最後瀏覽日：2025 年 3 月 15 日。

額等措施。積極宣導 ATM 與手機不共同操作的行動，推動「不在 ATM 上撥打手機，也不允許他人撥打手機」的標語，並在 ATM 機器旁呈現醒目的警告標誌。

(5) 電子貨幣發行機構的合作犯罪預防

與日本支付服務協會、電子貨幣發行機構、收款代理商等各方合作，推行預警與監管機制，向客戶發出警告、加強監控並有限度暫停使用電子貨幣之行動。過往超商使用電子支付相當頻繁，而詐欺被害者也經常使用電子支付來進行付款，因此推動超商預警機制，有相關疑似犯罪存在，立即通報。因網路購物詐欺而使快遞業者成為被利用之工具，要求快遞公司利用過去受害者付款接收者名單，向上溯源去挖掘可疑快遞並向警方舉報等工作。

(6) 反洗錢機制

許多大型電信網路詐欺集團透過虛構公司來掩蓋詐欺等犯罪收益的現實，政府將確保公司實際所有權資訊的驗證制度全面運行，根據《防止犯罪收益轉移相關法律》要求在交易時進行確認，同時加強邊境管控，與相關機構密切合作，對非法現金等物品流出海外實施邊境管制。

4、 瓦解並懲戒犯罪組織之措施

(1) 揭開求職詐騙資訊與淨化青少年生活環境

由於「非法打工」[90]等資訊在社群媒體上廣泛傳播，為防止此類資訊被用於招募犯罪分子，透過網路巡邏推動調查，並與電信或平台業者合作刪除此類資訊。網路巡查中心引進了人工智慧搜尋系統，精確地掌握「非法打工」的訊息，進一步透過網路熱線中

[90] 指以「非法打工」、「地下打工」等字眼，或以支付極高報酬的方式招募人員從事違法犯罪活動，但未透露具體工作內容的貼文及相關資訊。有人指出，這種語言讓人們更容易隨意參與犯罪。該計劃繼續使用廣為人知的術語「不正當打工等資訊」。但是，正如《針對利用社交媒體招募犯罪者的方法的搶劫及特殊詐騙的緊急應對計劃》（2023 年 3 月 17 日預防犯罪及對策部長會議決定）中所使用的那樣，在向年輕人等進行宣傳和提高認識時，也將繼續適當使用“有關招募犯罪者的信息”等術語。

心和網路巡查中心的強制下架「非法打工」等資訊。國家、地方政府、相關組織等將相互合作，提高公眾對青少年參與詐欺犯罪的危險性的認識。學校則是透過輔導員、社會工作者和警察等相關機構宣導電信網路的正確使用以及勿信虛假訊息，並揭露「非法打工」等犯罪活動，以免學生成為犯罪的同謀。

(2) 保全證據與精密分析

因應資訊通信技術犯罪，政府將提高分析最新電子設備和應用程式的技術能力，強化和改進分析未知密碼智慧型手機設備的分析設備，與外國調查機構和研究機構等相關組織協調和共享信息，並加強檢察官和調查人員的培訓，從而加強 IT 分析能力。

(3) 嚴懲電信網路詐騙犯罪

鑑於近期透過社群媒體招募犯罪者以及專業詐騙案持續嚴重的現狀，為了確保犯罪者得到應有的懲罰，警方將在調查中積極追訴其他罪行，並適用 2022 年 12 月加重了法定處罰的《有組織犯罪處罰及犯罪收益管制法》。加強對未成年人犯罪預防教育，與未成年人監獄等相關機構合作舉辦預防未成年人犯罪訓練班等，以防止未成年人再次犯罪。

(4) 強化身分驗證機制並加強未經授權手機之使用

依據《防止犯罪收益轉移法》和《防止手機非法使用法》規範之身份驗證，不管何種認證，必須讀取個人身分證上之 IC 晶片中的信息以進行身份驗證。用於實施詐騙等犯罪的手機，將依據《防止手機非法使用法》要求用戶確認，一經確認立即暫停該手機相關服務。此外對於販售非法手機等助長詐騙的犯罪行為，修法予以嚴懲。對於利用固定電話號碼向犯罪集團等提供電信服務的不法運營商，採取暫停使用犯罪中使用的固定電話號碼、拒絕提供新號碼、暫停使用所有庫存號碼等措施。為了杜絕人頭公司，成立總務省、警察廳和相關企業之間的合作與協商平台，禁止不法企業的擁有電信服務證照。

(5) 實現公正量刑：

為了給予電信網路詐欺犯罪者公平量刑，除了日本刑法第 246 條詐欺罪[91]、第 247 條[92]的詐欺未遂以及第 248 條加重處罰之外，根據《關於組織犯罪處罰及犯罪收益控制法律》[93]，從第 3 條第 1 項第 13 款就提到組織性詐欺的加重處罰，最低刑期為 1 年有期徒刑。第 10 條的犯罪收益隱匿[94]，談到隱匿犯罪收益或處分犯罪收益者，處以 10 年以下有期徒刑或 500 萬日圓以下罰金。若犯罪者明知該款項為電信網路詐欺犯罪所得，仍試圖隱藏或處分這些資產的行為，將會遭受嚴厲的刑罰。第 11 條是犯罪收益的收受[95]，明知是犯罪收益而收受者，處以 7 年以下有期徒刑或 300 萬日圓以下罰金，這有助於追究那些協助詐騙者處理非法資金的共犯責任。第 13 條則是犯罪收益的沒收[96]，對於犯罪收益及其衍生資產，得予以沒收，此條文允許對犯罪所得進行沒收，能夠切斷詐騙集團的資金鏈，有效遏止詐團的不斷擴大。這幾個條文都希望藉由嚴懲來嚇阻詐欺犯罪

5、 建立犯罪預警機制與國際合作

(1) 大數據資料庫的建立

警察廳和都道府縣警察廳將建立資訊收集體制，有效掌握匿名、流動犯罪團伙的實際情況，並加強對匿名、流動犯罪團伙的戰略打擊力度。同時將專業知識和技術的調查

---

[91] 第二百四十六条の二　前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、十年以下の拘禁刑に処する。Retrieved from: https://laws.e-gov.go.jp/law/140AC0000000045 最後瀏覽日：2025 年 3 月 15 日。

[92] 第二百四十七条　他人のためにその事務を処理する者が、自己若しくは第三者の利益を図り又は本人に損害を加える目的で、その任務に背く行為をし、本人に財産上の損害を加えたときは、五年以下の拘禁刑又は五十万円以下の罰金に処する。Retrieved from: https://laws.e-gov.go.jp/law/140AC0000000045 最後瀏覽日：2025 年 3 月 15 日。

[93] 組織的な犯罪の処罰及び犯罪収益の規制等に関する法律。 Retrieved from: https://laws.e-gov.go.jp/law/411AC0000000136 最後瀏覽日：2025 年 3 月 15 日。

[94] 第 10 條。同註 79。

[95] 第 11 條。同註 79。

[96] 第 13 條。同註 79。

體系，例如追蹤包括加密貨幣在內的犯罪收益、分析高度匿名的通訊方式等納入數據庫內。對已獲得資訊進行彙整和全國範圍內的橫斷面綜合分析體系，推動查明匿名和流動犯罪團伙的真實狀況。

(2) 建構 SNS 業者的資訊共享機制

根據《刑事訴訟法》處理調查機構的調查，要求 SNS 業者立即在日本國內設立事務所，並迅速建立能夠快速回應調查的系統。對於已經設立此類問詢窗口的社群媒體營運商，要求擴大問詢窗口的架構，簡化詢問方法，以便能夠更快地回應，從而比以往更快地推進刑事調查。此外，為了比以往更快地推進刑事調查，對封閉聊天室的社交媒體業者收集證據，根據《刑事訴訟法》與業者共同協商，並明確各自的意見。

(3) 跨境合作

對於主謀或指揮者位於海外的案件，需要與外國調查機構迅速交換信息，提供調查所需的證據，查明事件全貌。日本政府透過國際調查協助組織（ICPO）等組織推動調查合作，並利用外交管道和條約協定進行國際調查。進一步深化與外國政府和偵查機構的合作，確保在海外犯罪嫌疑人的引渡、驅逐出境等方面的協調更加順暢。加強對海外基地的打擊力度，透過駐外使領館加強與外國當局的合作，促進證據的順利移交等。

(五)日本打擊電信網路詐欺犯罪的困境

雖然日本也提出了相當多具體的打擊電信網路詐欺犯罪政策，然而政策制定與實際執行仍有一定的落差，對於目前的電信網路詐欺犯罪仍有許多困境有待突破。

1. 法律與監管挑戰

日本現行刑法規範不足問題浮上檯面，由於傳統刑法框架限制，詐欺罪條文過於傳統且沒有大舉修法，網路犯罪特徵並未納入修法內容，且該類型的犯罪多為組織型犯罪，因此電信網路詐欺犯罪的法律構成要件不符現況，像是集團犯罪認定困難，這些都使得法律看起來種種抬起卻輕七放下，即便抓到所謂的預備犯，卻因為法律規定使得預備犯

處罰範圍受限。目前電信網路詐欺犯罪屬於新型態犯罪模式，像是虛擬資產詐騙、投資詐欺創新手法、身分冒用新型態、社交工程演進模式多變，使得法律認定違法相當困難(Takahashi, 2023)。

接著是數位證據採認問題，法律是看證據能力來認定違法與否，因此證據完整性要求較高，然而電信網路詐欺屬於數位證據，加上數位足跡容易消失，本身證據取得就難，若沒有完整的保全程序，加上時效性重要，使得取得證據後，嫌疑犯都逃之夭夭。就算取得證據，另一大挑戰隨即而來，就是證據的真實度，由於電信網路詐欺是數位電子產品下的犯罪行為，加上現在偽造技術進步，網路隱匿性高，證據來源認證困難，若沒有高超的專業鑑定技術，根本無法成為證據來指控犯罪者。

回到法律程序面來看，雖然刑事程序有法律規範，但面對調查權限範圍有限的情況下，使得搜索扣押限制過多，且雲端資料取得困難，若是境外資料，其存取限制更多，若是加密資料，更是束手無策。由於跨境電信網路犯罪涉及管轄權，因此國際間合作相當重要，只是國與國之間的回應時效拖延，兩國間的司法程序標準有落差，技術支援不足又資源配置限制下，跨境合作下究竟是誰主導，似乎也起不了作用。

2. 技術與基礎設施限制

首先是專業人力不足問題，日本並非沒有專業人才，只是在警界中技術人才缺乏，尤其是數位鑑識專家短缺，若是招募高階鑑識人才，因薪資問題而招募困難，與私部門搶人才多半因為薪資競爭壓力不足而敗下陣來，也導致認證鑑識人員數量不足，拖垮了整體案件的承辦順序。因應跨境電信網路詐欺，需要的資安分析人員出現缺口，南以滿足檢調單位專業能力需求，也因此造成線上的即時監控人力不足，也促使情資威脅分析無法立即反應、在惡性循環下，使得打擊電信網路詐欺愈加困難。談到技術層面限制，國際合作人才短缺也屬於技術層面一環，除了原本的語言能力限制所造成的外語溝通障礙，當到達其他國家欲進行聯合打詐，根本就是難以溝通。國際實務經驗人才缺乏，加上缺乏國際實務經驗，根本沒有處理過跨境案件，對於國際合作程序也不熟悉，建立國

際打詐偵查網絡實屬困難。第一線的執法警力地方警力負擔，尤其地方警察並非只有詐欺案件，五花八門的案件所帶來處理壓力是相當龐大，加上目前基層人力不足，專業訓練不足的情下又設備資源有限，使得警察超時工作負荷過重，加上日本城鄉差距相當明顯，預算排擠之下，設備更新困難，更是難以負荷日益增多的詐欺案件(Jun, 2023)。

3. 國際合作與跨境執法困難

由於目前電信網路詐欺犯罪集團使用的犯罪工具相當多元，從 AI 技術應用深偽學習技術，由 AI 執行自動化詐騙系統，這類型的身分偽裝技術讓被害者難以分辨，詐欺犯罪為多層詐騙手法，加上犯罪者彼此透過加密通訊平台聯繫，根本無法追蹤。目前多數為跨境組織，成員非單一國籍，加上高薪聘請高階技術人才協助，如魚得水的情況讓詐欺更容易上手。詐欺犯罪伴隨金融多層轉帳系統，高明的資金分散技術，利用小額分散轉帳，再把多重帳戶重新串接，為了逃避資金流的查緝，透過跨行跨國轉移，抑或是虛擬貨幣轉換、數位支付混洗，甚至以合法商業掩護，這些都使得跨境執法越來越難。

國際合作是個大挑戰，由於跨境電信網路詐欺多為跨國合作，但是因為各國之間的法規差異問題，難以落實資訊共享機制，若是資金在國外流竄，對於資金的凍結時效將會延遲。若是兩國有簽訂司法互助還好，日本並非所有國家都有簽訂司法互助，此時管轄權爭議便浮上檯面，若案件涉及多國那麼整體行動相當複雜而協調無果，若是當地技術不到位而無法及時進行數位證據的採集，不僅蒐證成本飆高，更可能因權限範圍爭議而難以合作(Takahashi, 2023)。

4. 社會文化因素

首先日本的高齡化社會，老年被害者逐年增加，不僅造成個人財損之外，國家必須多付出更多的社會福利。由於老年人多半防範意識不足，加上對於新興科技應用能力不足，多半在家裡足不出戶，容易有社交孤立風險，加上沒有穩定的工作收入，一旦被詐騙，將使期的財務造成相當大的影響。由於新世代與老年世代存有根本性的差異，從文化價值觀念到各種社會學習能力，落差相當大，老年人若是真的遭到詐騙，多半通報意

願低落，加上與社會沒有頻繁接觸，對於求助管道知識嚴重不足，是日本詐欺犯罪困境之一。

即便日本推動各種宣導與教育政策，然而老年人的科技應用能力仍是最大問題，除了操作介面不熟悉之外，手機新技術適應困難，即便手機設有安全性設定選項，但老年人的緊急處理能力不足也是隱憂之一。目前老年人普遍都有學習意願不高的情形，獨居老人居多的情況下支援系統缺乏，導致持續學習困難，因而放棄繼續學習。

四、 南韓

(一)南韓電信詐欺定義與犯罪類型

南韓政府對於電信詐欺犯罪有其官方定義，根據南韓《電信基本法》第 2 條第 1 項規定，利用電信手段欺騙或勒索他人，獲取財務或財產利益，或使第三人獲取財務或財產利益的下列行為[97]。南韓政府對於電信詐欺犯罪的類型有明確的說明，除了表 16 所列出電信通訊詐欺犯罪外，尚有一些透過電信網路來遂行犯罪的行為，像是電子商務合約詐欺、線上遊戲、網路購物、網路股票以及虛假買賣等。電信通訊詐欺常見的手法來說，係假扮檢察官辦案、假冒金融機構的低利貸款詐騙、假冒家人、惡意連結等，都是透過電信通訊的科技來遂行詐欺犯罪。

表 16 南韓電信通訊詐欺犯罪類型與定義

類型	定義
語音式網路釣魚 (Voice phishing)	是一種結合「語音」、「私人資料」和「釣魚」的複合詞，係指透過電話竊取個人資訊、財務資訊或侵吞財產的犯罪行為。
簡訊網路釣魚 (Smishing)	是將簡訊（SMS）與網路釣魚詐騙整合，透過簡訊（SMS）誘騙受害者點擊包含「免費優惠券」、「週歲生日派對邀請函」、「手機結婚邀請

[97] Korean National Police Agency. What is Telecommunications Financial Fraud? http://https://www.counterscam112.go.kr/board/CONTENT_000000000001.do 最後瀏覽日 2025 年 4 月 25 日

	函」等內容的網址，誘使受害人點擊連結，隨後在被害人的智慧型手機上植入惡意程式碼，最後在受害者不知情的情況下遭受小額支付損失或購買個人資訊或財務資訊的犯罪行為。
釣魚網站 (Phishing site)	試圖透過建立與原始主頁畫面相似但網域名稱、IP 不同的虛假主頁來竊取用戶個人資訊的犯罪行為。
聊天室網路釣魚 (Messenger phishing)	透過駭客攻擊等手段取得他人網路聊天軟體（例如南韓最流行的 KakaoTalk 等）的 ID 和密碼，登入後透過 1 對 1 對話或簡訊等方式向已登入的熟人借貸緊急資金，侵占其資產的犯罪行為。
網址嫁接詐欺 (Pharming)	網址嫁接（Pharming）是由「網絡釣魚（phishing）」和「農業（farming）」這兩個詞組合而成，是一種類似於網絡釣魚的網上詐騙，使用用戶的電腦感染惡意軟體，並連接到虛假網站，從而誘導用戶輸入居民身份證號碼、帳戶號碼和信用卡號等信息，竊取信息的犯罪行為。
裸聊詐欺 (Body camping)	犯罪者透過智慧型手機聊天應用程式或隨機應用程式接近受害者，進行淫穢視訊聊天（body cam phishing），記錄對方的淫穢行為，然後在受害者的智慧型手機上植入惡意程式碼，竊取受害者熟人的聯繫方式，然後威脅將錄製的影片（照片）分發給熟人以勒索錢財的犯罪行為。
貸款詐騙 (Loan fraud)	犯罪者冒充金融機構等，以手機發送非法垃圾簡訊來接近受害人，提供貸款諮詢或貸款安排，然後以調整信用等級、貸款費用或償還現有貸款等理由索要金錢，然後將錢轉入虛假帳戶進行詐騙的犯罪行為。
投資誘導式詐欺	利用各種手段欺騙受害者並騙取錢財的犯罪行為，透過電話、簡訊（SMS）或社交網路（SNS）與被害者接觸，承諾保證本金和高收益；誘導被害者加入社群聊天室；使用虛假身份來發佈加入投資將能獲得高收益的虛假資訊。

資料來源：Ministry of Government Legislation[98],法制處.本研究整理

電信網路詐欺的形式多種多樣，但最具代表性的是語音釣魚。「語音釣魚」是一個複合詞，由「voice」（語音）、「private data」（個人資訊）和「phishing」（釣魚）組成。字面解釋就是利用語音來竊取個人資訊的行為。然而，它通常是透過語音或文字等媒體竊取受害者的個人或財務訊息，直接向受害者勒索金錢的一種方法。早期的語音釣魚詐騙大多冒充檢察機關、金融監督院等機關或金融機構，謊稱出現需要調查帳戶非法使用或其他刑事案件的緊急情況。在這個過程中，他們製造一種恐懼感或緊迫感，使受害者難以做出理性的決定，然後竊取他們的經濟利潤。隨著司法、金融等部門對語音釣魚的因應力度不斷加強，利用新科技的語音釣魚手法也日益複雜、多元。目前南韓常見的有冒充官方機構人員、金融貸款詐欺、簡訊網路釣魚、投資詐欺。

南韓警察廳投資引領室專案整治現況及防範方法指南[99](투자사기 예방 및 단속 백서)指出，2024 年財損嚴重的詐欺是投資誘導式詐欺，投資誘導式詐欺是指利用各種手段欺騙受害者並騙取錢財的犯罪行為，透過電話、簡訊（SMS）或社交網路（SNS）與被害者接觸，承諾保證本金和高收益；誘導被害者加入社群聊天室；使用虛假身份來發佈加入投資將能獲得高收益的虛假資訊，詐欺犯罪結構如下。

首先就是社群網路服務入口處投放簡訊誘餌。這種的犯罪手法結構是提供免費投資資訊，這些資訊都是針對即將上市或上漲的股票、加密貨幣進行投資，給予虛假的資訊來吸引他人的注意。時常出現在社群媒體廣告，有時在 YouTube、Facebook 等平台上冒充投資專家或名人招攬相關生意，有時以網路交友詐騙為開端，在網路上發展戀愛關係，然後誘導投資。第二步是與潛在被害者接觸。此時詐騙集團會鼓勵這些潛在被害者

[98] Ministry of Government Legislation, Electronic financial crime. Retrieved from: https://www.moleg.go.kr/legnl/legnlInfo.mo?leg_nl_pst_seq=765&mid=a10403000000 最後瀏覽日 2025 年 4 月 25 日

[99] 南韓警察廳(2025 年 2 月 27 日)，投資領導室專案打擊行動現況及防制方法指南。 最後瀏覽日 2025 年 4 月 25 日

參與 KakaoTalk 社群的聊天室，這些聊天室裡看似有數十名所謂的追隨者(바람잡이)，但實際上這些都是少數人利用數十個虛假帳號來欺騙這些潛在的被害者。等到取得信任時，透過電話和社群網路聯繫被害者，並推薦他們投資非上市股票和虛擬資產。第三步則是提供虛假訊息。犯罪組織製作的網站、部落格和上發布與股票和虛擬資產相關的虛假訊息，並誘導受害者閱讀。此時這些詐騙集團已經讓被害者誤信自己所連結的是官方正式網頁進行投資，殊不知是連接到犯罪組織製作的虛假交易系統網頁，並在螢幕上顯示其推薦的股票正在飆升。這些虛假交易所透過與南韓綜合股價指數等即時數據鏈接，精心設計之下使其看起來像真正的交易所，並在進行小額投資時支付部分利潤，以安撫受害者。最後一步就是被害者投資資金。此一步驟是詐欺犯罪者認為他們所詐欺的資金足夠時，他們就會立刻消失於相關網路社群。

投資誘導式詐欺警察廳國家搜查本部(경찰청 국가수사본부에서는)自 2022 年底來發現投資誘導型詐欺受害情況增加，發起「侵害民生金融犯罪特別打擊行動」。由於受害情況持續，打擊行動在 2024 年兩度延長，目前將持續到 2025 年 10 月 31 日。從 2023 年 9 月至今，共破案 7232 起，逮捕 3,300 人。

(二)南韓電信網路詐欺現況

根據南南韓家警察廳最新的 2023 年的犯罪統計[100](National Police Agency Crime Statistics)資料，全年詐欺案件高達 347,901 件，以低於 100 萬韓元為大宗，為 136,070 件，然 1000 萬韓元有 73,012 件，一億韓元的有 72,260 件，連超過台幣一千萬以上的詐欺騙也有近兩萬件，顯見南韓的詐欺相當嚴重(表 15)。當中利用電信網路所進行的語音調查詐欺 34,101 件、金融貸款詐騙有 5,695 件、網路購物詐騙有 74,361 件、投資詐欺有 26,219 件；比較特別的南韓警察廳有調查詐欺犯罪的時間多半是落在凌晨

[100]National Police Agency. National Police Agency Crime Statistics 2023. https://www.police.go.kr/user/bbs/BD_selectBbsList.do?q_bbsCode=1115&estnColumn2=%EB%85%84%EB%8F%84 最後瀏覽日：2025 年 4 月 25 日

12 點到三點之間，高達 208,604 件，其次是中午 12 點到下午三點有 31,698 件，接著是下午三點到下午六點，有 31,342 件，顯然凌晨與下午時段，最容易被詐騙。以犯罪工具來說，電腦、智慧型手機以及其他電子設備，也是詐欺犯罪的主要犯罪工具，上述手法與我國類似，且金額都相當龐大。

表 17 南韓 2023 年詐欺財損金額與件數統計表

損害金額	案件數	比率
低於100萬韓元 (約莫台幣22,000元)	136,070	39.1
低於1000萬韓元 (約莫台幣220,000元)	73,012	21.0
低於1億韓元 (約莫台幣2,200,000元)	72,260	20.8
低於5億韓元 (約莫台幣11,000,000元)	18,095	5.2
超過5億韓元 (約莫台幣11,000,000元)	4,536	1.3
未知	43,928	12.6
總計	347,901	100.0

資料來源：南南韓家警察廳，2023 年犯罪統計資料

南韓政府一直在推行包容性金融和創新數位技術的運用，隨著電信網路數位技術的進步與發展，也導致電信網路詐欺犯罪的蔓延。加上南韓智慧型手機的廣泛使用，電信網路詐欺在這幾年成為網路佔罪的主要類型。根據南韓警察機構 2023 年的網路犯罪統計資料，2018 年共有 149,604 件，上升至 2022 年的 230,355 件，網路犯罪事件總數增加了 5.8%，其中網路詐欺 155,715 件佔所有網路犯罪事件的 67.6%。電信網路詐欺分為

直接交易詐欺(又稱二手交易咖啡館詐騙)、購物中心詐欺、遊戲詐欺，以及其他四個類別，從過去離線方式到目前都是線上來進行詐欺犯罪(Na, 2023)。

儘管數位可及性和文化存在差異，手機簡訊 (SMS) 是最常用的三大詐騙管道之一，簡訊是第二常用的詐騙管道 (58%)，僅次於電話 (61%)。南韓 2023 年最常使用的詐騙方式是工作詐欺（61.2%），第二個最普遍的類型是信用卡詐欺（17.6%），詐欺犯罪者都是透過簡訊或郵件誘使受害者撥打這些號碼，冒充公共機構、家人和朋友遂行詐欺。詐欺犯罪者多透過 Instagram 和 Facebook 等 SNS 平台以及線上購物商場等 APP 程式，由於網路犯罪的特性，利用外國公司、外國虛擬資產、交易所逃避調查的案件越來越多。由於網路犯罪案件不斷增加，警方已形成各類型的國際網路，例如國際刑警組織、國外執法機關和全球 IT 公司直接形成各類國際網路。透過海外公司進行的網路詐騙增加，但清洗犯罪所得的手段和犯罪類型有所改變，從海外禮品卡變為當地貨幣、國內禮券、大炮存摺、虛擬貨幣交換等(Park, Lim, Kim, Yu & Koo, 2023)。

Lee(2024)的研究報告中指出 2023 年，由於政府不斷改善語音釣魚相關制度和防範措施，受害金額和受害者人數雖然有所減少，但人均受害金額反而增加了。 2023 年語音釣魚詐騙總損失為 1965 億韓元，較四年前減少約 70.8%，受害者人數也減少了 77.2%至 11503 人，但人均損失金額實際上較四年前增加了 28%，達到 1708 萬韓元。從各年齡層受害金額趨勢來看，截至 2023 年，50 多歲族群的語音釣魚受害金額比例逐年減少，而 20 歲以下族群的受害金額比例則每年增加約 2 倍。從 2024 年金融詐騙的受害情況來看，受害件數方面，語音釣魚以 11,734 件佔據絕對優勢，其次是投資引導室 6,143 件，戀愛詐騙 920 件。從受害金額來看，投資引導室的受害金額為 5340 億韓元，超過了電話釣魚的 3909 億韓元。2024 年，冒充機構的語音釣魚案件數量較前一年減少，但貸款詐騙的語音釣魚案件數量增加，導致語音釣魚案件總數較前一年增加。貸款詐騙語音釣魚案件總數較前一年增加 61%，其中 20 歲以下和 30 多歲受害者的案件數分別增加 109%和 111%，導致貸款詐騙語音釣魚案件總數增加。值得一提的是深偽技術的詐騙悄悄的在詐欺犯罪中流行，利用深度偽造技術進行金融詐騙最近被用於金融詐騙的 Deepfake 技

術，主要是指製作著名政客或明星的視頻或聲音，利用其對不特定人數進行投資詐騙，或者接近家人、熟人、同事等親近的人，進行各種詐騙手段。

從 2024 年重大金融詐騙的受害情況來看，語音釣魚最為常見，共發生 11,734 起，其次是投資閱覽室詐騙，共發生 6,143 起，再次是戀愛詐騙，共發生 920 起。但從受害金額來看，投資龍頭房受害金額達 5340 億韓元，超過語音釣魚受害金額 3909 億韓元。因此，投資引導室每月平均受害金額為 668 億韓元，比電話詐騙的 558 億韓元高出約 110 億韓元。

(三)打擊電信網路詐欺的具體作為

隨著技術的進步，尤其是在語音網絡釣魚等數位技術，各種形式的電信金融詐欺變得更加複雜。在當今社會中，手機不僅可以用作通信設備，還用作存儲和處理信息的私人工具。除了語音網絡釣魚之外，各種形式的電信財務詐欺，例如網絡釣魚，smishing，藥品和記憶黑客，利用電子通訊網絡(KNPA, 2024)。以下針對南韓在打擊電信網路詐欺層面上加以說明。

1. 法規修訂強化法制面

根據南韓刑法[101] 第 347 條【詐欺】（사기）提到以欺騙手段使人產生錯誤，從而取得財物或財產上不法利益者，處 10 年以下有期徒刑或 2 千萬韓元以下罰金。第 348 條第 2 款（Unlawful Use of Facilities for Convenience）任何人使用自動售貨機、公共電話或其他付費自動設備以不正當方式獲得任何財產或財產利益，而不支付費用，應處三年以下有期徒刑或五百萬韓元以下罰金，拘留或輕微罰款。第 351 條則是針對慣習犯的加重二分之一量刑。這也是南韓對於詐欺犯罪的基本法律架構。

---

[101] Criminal Law, Korean Law Information Center. Retrieved from: https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=%ED%98%95%EB%B2%95&x=0&y=0#liBgcolor0 最後瀏覽日：2025 年 4 月 25 日。

由於法律是打擊電信網路詐欺的根本，唯有檢視法律是否足以應付詐欺犯罪，才能制訂有效的打擊策略。打擊電信網路詐欺最難的就是執法過程，調查與偵查都需要法律規範的支持，因此南韓為了打擊電信網路詐欺，讓執法機構能夠有法律支持來進行查緝犯罪，因此在幾個法律中進行修訂。南韓《電信事業法》在打擊電信網路詐欺方面，透過多次修訂與政策調整，建立了較為完整的法律架構。

(1) 資訊通信網路法[102]（ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION）

資訊通信網路法在 1986 年最初為《電算網法》，1999 年後正式更名為《資訊通信網路法》，該法犯隨著電信網路技術的革新，法律條文的修訂內容也從加強個人資訊保護開始，納入網路安全相關條款，明文規定相關處罰規定，近年來對網路服務提供者負起相關責任。由於電信網路詐欺是利用網際網路來遂行詐欺犯罪，因此網路安全格外重要，第 45 條第 2 項[103]是規範業者必須盡到網路安全義務，要求服務提供者採取高技術性以及完善管理的相關網路安全措施。第 46 條[104]則是規範業者應負起網路保安責任，透過定期安全檢查和漏洞評估，對於網路設備安全必須要有認證制度。對於這些系統與認證制度必須能夠有效的保護個人資訊，對於特殊案件的資訊必須有管理制度來應對。更重要的第 48 條[105]規定任何禁止侵入資訊通訊網路的行為，此條規範任何人不得無正

---

[102] 정보통신망 이용촉진 및 정보보호 등에 관한 법률, Korean Law Information Center. Retrieved from: https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D+%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84+%EB%B0%8F+%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8+%EB%93%B1%EC%97%90+%EA%B4%80%ED%95%9C+%EB%B2%95%EB%A5%A0&x=0&y=0#liBgcolor0 最後瀏覽日：2025 年 4 月 20 日。

[103] 第 45 條。同註 88。

[104] 第 46 條。同註 88。

[105] 第 48 條。其中的惡意程式，任何人不得透過發送大量訊號或資料、讓網路處理非法命令或採取類似行動，對資訊通訊網路造成乾擾，幹擾資訊通訊網路的穩定運作。同註 88。

當理由損壞、破壞、竄改或偽造資訊通訊系統、資料、程式等，也不得傳送或傳播「惡意程式」。同時強調資料的保護機制，尤其是對個人資訊的保護更為重要。第 22 條第 2 項強調存取權的同意機制，對於提供資訊通訊服務業者，需要取得「存取權限」時，必須向使用者告知，取得使用者的同意方能存取其個人資料。第 23 條第 6 項規範提供服務的業者對於相關個人資訊必須提供安全保護措施的義務。該法案的第 70 條開始就是違反相關法令的懲戒，第 70-2 條[106]規定，傳送或傳播惡意程序的人，處以 7 年以下有期徒刑或 7000 萬韓元以下罰款。損害他人訊息，或侵犯、竊取、洩漏他人秘密，處以 5 年以下有期徒刑或 5000 萬韓元以下罰款[107]。整體來說，此法案是南韓第一部專門規範網路空間的綜合性法律，成為數位網路時代的法律基礎框架，從技術、安全與個資的保護都有著墨，且持續的因應最新的網路規範而進行修正。

(2) 電信事業法[108]（Telecommunications Business Act）

首先是修法加重詐欺犯罪刑責，為了提高對電信詐騙行為的威懾力，《電信事業法》對於違法行為給予嚴格的刑罰。違法經營處罰可以依照第 95 條[109]處以最高 3 年徒刑或 1 億 5000 萬韓元罰金。播送虛假簡訊與竄改來電顯示號碼的行為，可處以最高 3 年徒刑或 1 億 5000 萬韓元罰金[110]。對於未定期檢視風險管控機制與提交報告者，可處以最高 2 年徒刑或 1 億韓元罰金[111]。對電信業者加重處罰無非是希望業者能夠自律且有義務去打擊電信網路詐欺犯罪，若是能夠建立起良好的風險管控機制以及回報制度，將能夠有效地降低詐欺犯罪數量。

---

106 第 70-2 條。同註 88。

107 第 71 條。同註 88。

108 전기통신사업법， Korean Law Information Center. Retrieved from: https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=Telecommunications+Business+Act&x=0&y=0#liBgcolor1 最後瀏覽日：2025 年 4 月 25 日。

109 第 95 條。同註 94。

110 第 95-2 條。同註 94。

111 第 96 條。同註 94。

此法案針對消費者保護作出了相當大的規範，第 32 條是透過服務契約規範來保護用戶的權益，第 43 條進一步規範業者禁止將資訊用於其原定目的以外的目的，不得濫用或提供給第三方。同時加強用戶身份驗證與防止冒名開戶，為了防止詐騙分子利用他人身份開設通信帳戶，要求電信業者在用戶開戶時進行嚴格的身份驗證。此外，業者必須提供防止非法使用他人名義的服務，並在發現可疑活動時，立即採取措施防止詐騙行為的發生。

(3) 特定金融訊息報告和使用法[112](ACT ON REPORTING AND USING SPECIFIED FINANCIAL TRANSACTION INFORMATION)

該法是為了建立了更完善的金融體系的監控機制，由於詐欺是為了實現犯罪利益，因此該法的修訂能夠為打擊電信網路詐欺給予有效的法規支持。該法案在 2024 年作最新的修訂，主要是希望及時發現並阻止可疑資金流動，加強執法機關對電信詐騙的調查能力，促進國際間的資訊交流與合作，共同打擊跨國詐騙行為。

首先金融監控機制的強化方面，第 4 條[113]是金融機構應對可疑交易進行報告，內容包括金融機構、虛擬資產服務提供業者（VASP）等，若發現客戶交易與其身份不符、有異常頻繁交易或涉及高風險國家，應向金融情報分析院[114]（KoFIU）通報。第 7 條是金融機構對顧客身分有確認之義務，規定金融機構應對於客戶開戶時，必須完成客戶身份驗證並持續監控其交易行為。第 5-3 條則是交易記錄的保存，規範所有客戶識別資料與交易記錄應保存 5 年以上，供未來調查及審查使用。帳戶凍結機制方面，第 5-4 條主要

---

[112] 특정 금융거래정보의 보고 및 이용 등에 관한 법률. Korean Law Information Center. Retrieved from: https://www.law.go.kr/lsInfoP.do?lsiSeq=195313&urlMode=engLsInfoR&viewCls=engLsInfoR#0000 最後瀏覽日：2025 年 4 月 20 日。

[113] 第 4 條。同註 98。

[114] KoFIU 是金融服務委員會下屬的南韓金融情報部門，旨在防止此類洗錢和恐怖主義融資，並有助於提高金融交易的透明度。KoFIU 負責分析金融機構和其他機構提交的金融資訊，並在被認為與犯罪收益或洗錢有關時向執法機構傳播相關信息。https://www.kofiu.go.kr/eng/intro/about.do 最後瀏覽日：2025 年 4 月 25 日。

是針對可疑帳戶的暫停交易與凍結。若經 KoFIU 分析認為某帳戶涉及洗錢或詐騙活動，得通知主管機關凍結相關帳戶或中止交易，金融監管機關凍結可疑資金，可防止資金外流與持續詐騙行為。

跨境資金監控方面，金融機構針對大額現金或跨境交易申報必須進行報告。達 1 萬美元以上的現金存取或出入境資金都需向 KoFIU 報告。由於電信網路詐欺金流多為跨境，KoFIU 可以與國外反洗錢機構交換可疑交易資訊[115]，特別針對跨國詐欺資金流動。除了跨境資金的情報，打擊詐欺需要跨機構的合作，條文也規範金融機構能將金融情報提供給警察、檢察廳、國稅廳、海關等機關，利用於調查詐欺與洗錢的金融犯罪[116]。因應新興支付工具的發展，2021 年就增訂了電子支付與虛擬資產納入規範。要求支付服務提供商建立風險評估系統，並實施交易限額管理。目前南韓金融情報分析院（KoFIU）實務上已應用 AI 與大數據分析來監控交易模式，並與 FinTech 公司合作發展監理科技（RegTech），透過 API 介接取得金融機構之交易資訊流，實施即時監控。

(4) 電子金融交易法[117]（ELECTRONIC FINANCIAL TRANSACTIONS ACT）

2006 年南韓為了確立基本制度架構以及規範電子金融業務，因此制定了本法案。主要是為了強化用戶保護以及完善安全規定，要求金融機構要加強資安要求，並且增加監管手段，才能夠保護消費者。《電子金融交易法》的修訂是朝向建立金融領域語音釣魚詐騙資訊共享系統、暗網威脅資訊收集與應對等方向進行修法，大力支持創新金融服務相關安全審查，以及非面對面身份驗證等新興金融技術的實施，創造數位金融創新的安全環境。第 2 條[118]先針對電子金融的範疇做出明確的定義，金融公司或電子金融經營機

115 第 8 條。同註 98。

116 第 7 條。同註 98。

117 전자금융거래법，Korean Law Information Center. Retrieved from: https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B1%B0%EB%9E%98%EB%B2%95&x=0&y=0#liBgcolor0 最後瀏覽日：2025 年 4 月 20 日。

118 第 2 條。同註 103。

構透過電子設備提供金融產品和服務，使用者以非面對面、自動化的方式使用，無需與金融公司或電子金融經營機構的工作人員直接接觸的交易，其支付的方式包括電子資金轉帳、電子借記支付手段、電子預付手段、電子貨幣、信用卡、電子債券或其他以電子方式進行的支付方式都納入電子金融業務。第三章開始規範電子金融的保護措施，第 21 條(Duty to Ensure Safety)內容為確保電子金融交易的安全性和可靠性，金融公司對於子傳輸或處理所需的人力資源、設施、電子設備和費用，以及電子金融業務，要求建立安全管理系統，強制身份認證要求以及交易程序必須經過驗證。為了交易透明化，電子金融交易要求實名制[119]，驗證記錄保存必須完整，才能在未來資料調取程序能夠配合相關單位。

值得注意的是第 27 條的爭議的解決與調解。事業體對於用戶就電子金融交易提出的合理意見或投訴，並補償用戶在進行電子金融交易過程中遭受的損失。該項規定讓金融機構負起賠償的責任，也相對的讓電子金融事業體必須善盡自己打擊電信網路詐欺的責任。

(5) 預防電信金融詐欺損失及損失補償特別法[120](Special Act on the Prevention of Loss Caused by Telecommunications-Based Financial Fraud and Refund for Loss)

南韓政府針對日益猖獗的電信與金融詐欺犯罪，許多民眾因誤信假冒來電、簡訊、平台，而轉帳遭詐，尤其在 2020 年疫情之後，虛擬貨幣詐欺與社群投資詐欺大量出現，傳統法律規範又難以因應新型詐騙手法，政府認知受害者保護機制不足，因此針對電信金融詐欺犯罪制定此法律。尤其打擊電信網路詐欺犯罪上，檢警單位只能苦追詐團的犯罪行為之後，因此希望藉由金融機構能夠共同擔負打詐責任，快速凍結帳戶讓犯罪利益延後兌現，建立受害者補償申請制度，期許將打擊電信網路詐欺犯罪之風險降至最低。

---

[119] 第 22 條。同註 103。

[120] 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법，Korean Law Information Center. Retrieved from: https://elaw.klri.re.kr/kor_mobile/viewer.do?hseq=39681&type=part&key=23 最後瀏覽日：2025 年 4 月 20 日。

2020 年 11 月 20 日起施行本法案，整體朝向防止預付費電話等通訊手段被不法利用的綜合應對體制、建立冒充公共機構或金融公司電話號碼的虛假提示的過濾系統、建構刪除語音釣魚電話號碼的機制、利用大數據和人工智慧開發新型語音釣魚防範技術、成立金融聯合體推進金融公司詐欺檢測系統（FDS）等。

第二章是建立防止及阻斷機制，從金融機構的定義[121]著手，涵蓋銀行、農水產合作社、保險、郵政以及其他各種金融業務的機構。法條將電子金融交易進行明確的定義，系指金融公司通過電子設備向使用者提供金融產品或服務，通過自動化方式或服務的交易行為。為了讓金融機構能夠負起打詐的責任，第 2-2 條[122]的電信金融詐欺應對措施規定當中，金融服務委員會收集和發布電信金融詐欺資訊，並且進行預測和預警電信金融詐欺，為確保金融公司進行電子金融交易業務的安全性和可靠性，業者應建構必要的人員、電腦化設施、電子設備等。第 2-5 條[123]使用者帳戶的臨時措施中規定，若發現疑似詐欺交易，金融機構可立即申請臨時凍結帳戶，以遏止資金外流。第 2-7 條[124]明文規定電信金融詐欺綜合舉報應對中心的設立，其主要工作包括接收有關電信金融詐欺的報告和諮詢，將有關電信金融詐欺的資訊，彙整後發布電信金融詐欺預測和警報，要求暫停支付用於電信金融詐欺的帳戶，並要求暫停向用於電信金融詐欺的電話號碼提供電信服務，將這些資料分析後作為犯罪相關資訊，並向相關行政機關和相關機構、企業和組織

---

[121] 第 2 條，同註 106。

[122] Article 2-2 (Response to Telecommunications-Based Financial Fraud) (1) To prepare for telecommunications-based financial fraud and minimize any loss, the Financial Services Commission shall conduct the following duties:1. Collection and distribution of information on telecommunications-based financial fraud;2. Forecasting and warning on telecommunications-based financial fraud，同註 106。

[123] Article 2-5 (Interim Measures for Accounts of Users) (1) In any of the following cases, a finance company shall take measures to delay or temporarily suspend the transfer, remittance, or withdrawal of all or part of the relevant user's account (hereinafter referred to as "interim measures")，同註 106。

[124] Article 2-7 (Establishment of Integrated Reporting and Response Center for Telecommunications-Based Financial Fraud) (1) The Integrated Reporting and Response Center for Telecommunications-Based Financial Fraud (hereinafter referred to as the "Center") shall be established under the Korean National Police Agency to efficiently conduct affairs, such as reporting and receiving information on telecommunications-based financial fraud. ，同註 106。

發布犯罪相關資訊；第 13-3 條則是檢察總長、警察廳長官或社會保障部省長確認某個電話號碼被用於電信金融詐騙時，可向資訊通信技術部請求停止提供該電話號碼的電信服務。

2. 打擊電信網路詐欺機構

(1) 警察廳（경찰청）

警察廳已將電信詐欺與網路詐欺列為侵害民生之罪(민생침해범죄)，因此對於打擊此類犯罪的核心作為，列為「2024 年民生犯罪重點對策」之一，透過集中資源與專案小組進行詐欺犯罪的打擊(KNPA,2024)。南韓警察廳扛起打擊電信網路詐欺犯罪的第一線工作，其重要性不可同日而語。警察廳組成了 T/F 小組(惡意詐欺根除工作組)，從左邊開始的調查主任負責任務推進與考核工作，刑事局局長的重點打擊工作推行，計畫的協調者擔任通緝及未破案件管理，發言人則負責詐欺預防的策劃和公共關係，最後的國際合作辦公室，與國際刑警組織配合來進行打擊詐騙的國際合作與遣返。此外，還與金融服務委員會（金融監督院）、科學技術資訊通信部、國土交通部等相關機構及相關行業簽訂了業務協議，特別是向國土交通部派遣了應對傳諂詐騙的合作官，為完善法律制度、有效打擊建立起了有機合作關係。

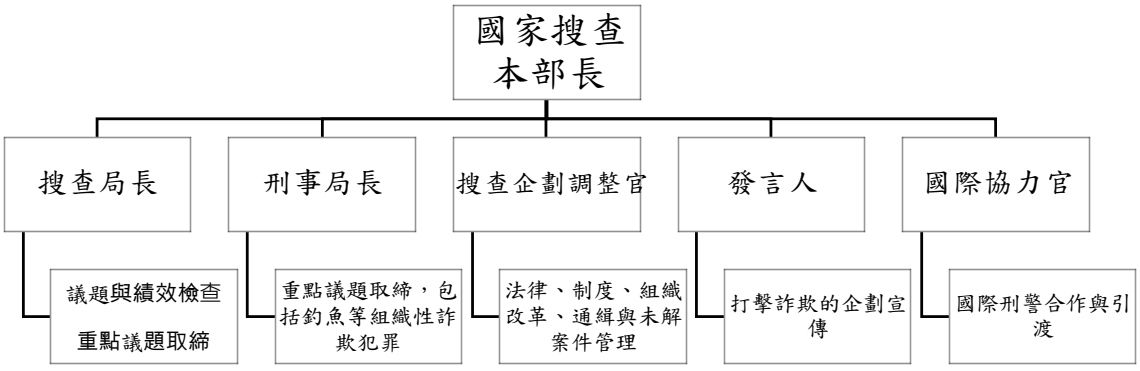


圖 10 惡意詐欺根除工作組組織結構圖，資料來源：KNPA 2024 警政白皮書，32 頁

南韓警察廳在打擊電信網路詐欺方面，首先應用 AI 語音分析哪些可能是詐團的詐

騙用語，透過 AI 來協助偵測並防堵。接著針對疑似犯罪可能的 APP 進行封鎖，將建構的通報資料庫比對後再與 KISA[125]配合，將舉報的可疑號碼、帳戶、連結與惡意行為紀錄提供警察與電信公司進行快速比對與阻斷。警察廳也對於第一時間的詐團接觸進行策略建構，與電信公司合作，將可能的詐欺電話標示，提示詐騙來電可能造成被詐騙的可能，整體來說警察廳要強化對詐騙集團的即時應變能力(KNPA,2024)。

在預防層面，南韓警察廳 2023 年 9 月 26 日設立電信及金融詐欺綜合檢舉與因應中心(전기통신금융사기 통합신고대응 시스템)，整合民眾通報、簡訊舉報、可疑帳戶查詢與自動化阻斷處理，並與南韓主要銀行、通訊業者建構即時連動平台[126]。該平台涵蓋語音詐騙（보이스피싱）、短信詐騙（스미싱）、號碼偽冒等多種詐欺手法，相關的資料也可做為警方進行犯罪分析的大數據資料庫。詐欺犯罪的預防從宣導做起，警察廳警察廳結合金融機構，在地鐵、戶外、大眾媒體發起防詐宣導活動，在 ATM 張貼高風險轉帳警示，種種的作為目的就是為了提升群眾防詐意識，能夠識別詐欺犯罪手法，遠離可能的詐欺受害風險[127]。

KNPA(2024)有針對電信網路金融詐欺的相關政策進行說明，首先是宣傳品的部分，由於電信網路結合金融手法，起初從簡單的電話詐騙，演變為冒充金融公司和政府機構

---

[125] Korea Internet & Security Agency 是南韓網路安全局，主要工作是促進網路廣泛使用、保障資訊安全、防範網路犯罪，該機構與警察廳合作建置黑名單資料庫，協助封鎖詐騙連結、釣魚網站與假冒政府頁面。Retrieved from: https://www.kisa.or.kr/EN 最後瀏覽日：2025 年 4 月 27 日。

[126] Korean National Police Agency(2023, Sep 26). Voice phishing, now report it by calling '112'. [Press release] Retrieved from: https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20230926174554153&q_currPage=1&q_rowPerPage=10&q_searchKeyTy=&q_searchVal=&q_sortName=&q_sortOrder=&q_tab=&utm 最後瀏覽日：2025 年 4 月 27 日。

[127] Korea National Police Agency. (2024, May 14). 200 days since the launch of the Integrated Telecommunications and Financial Fraud Reporting and Response Center, prevention through integrated reporting and reporting of phishing crimes [Press release]. Retrieved from: https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20240514075709783&utm 最後瀏覽日：2025 年 4 月 27 日。

發送誘餌短信，以及讓受害者在手機上安裝惡意應用程式。因此警察廳建構了「預防-逮捕-連結」的電話金融詐騙綜合根除措施(전화금융사기 종합 근절대책)。警方與知名YouTuber合作加大宣傳力道，並與國防部和南韓國民銀行簽署了業務協議，製作一系列的防詐影片。同時展開打擊詐欺行動，從詐團的主要核心成員進行追捕與查緝[128]。此外，警察廳與南韓網路安全局及各電信公司合作，建立阻斷電信犯罪手段的機制，並利用企業公益計畫募集的資金，為電信金融詐騙受害者提供生活補助和心理諮詢等支持。

(2) 金融監督院（금융감독원）金融情報分析院（금융정보분석원）

在南韓打擊電信與網路詐欺犯罪的體系中，金融監督院（Financial Supervisory Service, FSS）與金融情報分析院（Financial Intelligence Unit, FIU）扮演著關鍵的金融側協作角色。兩者分別負責監理、執行與金融交易情報的蒐整與分析，與警察廳、通訊業者及相關政府單位密切合作，共同強化防詐機制與跨部門應變系統。

首先，金融監督院作為南韓主要的金融監理執行機構，依據《預防電信金融詐欺損失及損失補償特別法》第一條的規定，金融機構應負起詐欺預防的責任與採取相關的應變措施。條文中規定金融機構應協助實施包括帳戶凍結[129]、異常交易識別、預防機制建置[130]等。對於目前最流行的第三方支付，推動建立內部風控機制，以攔截異常匯款、阻斷快速洗錢鏈條[131]。金融監督院本身除了與警察廳合作來分享可疑帳戶清單外，透過與

[128]忠南道廳逮捕在中國杭州設立呼叫中心，冒充檢察機關及金融監督院，詐騙1,891名受害人，金額達1,491億韓元的犯罪集團44名成員。首爾道廳逮捕以小額貸款或預付SIM卡開卡為名招募人員，透過網路平台等管道向網路釣魚組織分發1,706張非法開立的假SIM卡的主謀等138人（7人）。大田道廳逮捕設立8家假公司，從支付機構取得6萬個虛擬帳戶，並將其分發給網路釣魚、賭博等犯罪組織的主謀等23人。資料來源：KNPA 2024 南韓警政白皮書，p35.

[129] 第4條第1款，同註106。

[130] 第2條之6，同註106。

[131]Financial Services Commission Inquir.(2024, Aug 19) [Press release] It has become possible to quickly block damage from voice phishing that exploits simple remittance. - The revision of the “Enforcement Decree of the Telecommunication Fraud Damage Refund Act” passed the State Council. Retrieved from: https://www.fsc.go.kr/po010101/82912 最後瀏覽日：2025年5月17日。

電信公司及南韓網路振興院（KISA）協作，FSS 亦參與詐騙電話攔阻技術與惡意應用程式辨識系統的整合。金融情報分析院（FIU）則負責對國內所有可疑金融交易資料進行彙整、分析與通報。當民眾或金融機構舉報潛在詐騙案件時，FIU 會即時透過其金融情報分析系統進行風險建模與行為模式分析[132]，並將可疑資料提供給警方、檢方或其他權責單位進行後續調查。FIU 同時與國際金融情報合作組織保持密切合作，針對跨國電信詐騙與洗錢組織共享帳戶線索與身份資料，成為南韓跨境詐欺打擊的重要後勤單位[133]。FSS 與 FIU 為南韓金融運作安全的核心機構，對於電信網路詐欺的偵查與預防相當重要。無論從金融機構的管理到詐欺犯罪的情報提供，都是打擊詐欺的重要支柱。

(3) 通信傳播委員會（방송통신위원회）與網路安全局（한국인터넷진흥원）

通信傳播委員會（Korea Communications Commission，KCC）的成立是因為行動手機及網際網路快速普及下，對於網路的監管與相關的政策制定都需要專業機構，以前由多部會分別負責監督，然隨著通信與網路的結合後，因此設立通信傳播委員會來負責相關的政策與法規建議。通信傳播委員會（KCC）為了配合打擊電信網路詐欺犯罪，因此推動了《電信事業法》、《資訊通信網法》等與詐欺相關的法案，提供電信業者攔阻詐騙來電與惡意簡訊的法律依據。同時推動來電顯示的真實性驗證機制[134]，要求業者標示可疑國際來電，協助使用者辨識號碼偽冒行為。此外，該機構積極策畫大眾宣導活動，如舉辦「User Week」資安週與針對青少年與長者的反詐騙教育活動，發行語音詐騙防制手冊，並推出多語言短片與社群推廣素材。未來將積極推動開發 AI 辨識模型與「緊急封鎖機制（Circuit Breaker）[135]」，以即時中斷大量詐騙簡訊或來電的傳輸流程，提升系

---

[132] Definition of Suspicious Transaction Report. KoFIU. Retrieved from: https://www.kofiu.go.kr/eng/policy/amls03.do 最後瀏覽日：2025 年 5 月 17 日。

[133] International standards and international organizations. KoFIU. Retrieved from: https://www.kofiu.go.kr/kor/policy/iois01_3.do 最後瀏覽日：2025 年 5 月 17 日。

[134] 根據第 84 條之 2 所設立, Telecommunications Business Act. Retrieved from: https://lawnb.com/Info/ContentView?sid=L000001733_84X2_20200609 最後瀏覽日：2025 年 5 月 17 日。

[135] KCC, Annual Report 2023, p. 230–231.

統反應效能與民眾防詐能力(KCC, 2023)。

網路安全局則是南韓的資安與網際網路服務主要推動機構，主要是針對網路資訊安全的政策規劃與建議。南韓網路安全局在打擊電信網路詐欺犯罪的上，主要負責惡意應用程式（malicious apps）與釣魚網站的識別與封鎖。KISA 能夠透過分析可疑網域、IP 與惡意程式碼，主動提供資訊給警察廳與金融監督機構(KCC, 2023)。為了能夠提高即時應變能力，推出「Illegal Spam Easy Reporting App」[136]，讓民眾可透過該 App 迅速舉報詐騙簡訊與電話，提高攔阻時效。

(4) 檢察廳（검찰청）

根據南韓檢察廳 2024 年檢察年鑑中資料，南韓檢察廳架構從中央到地方分為三級，最高層級為最高檢察廳(대검찰청)，是由檢察總長領導，負責全國司法與偵查綱要，第二層為高等檢察廳，作為處理大規模、跨區案件與抗訴，第三層則是地方檢察廳，是執行一線偵查與起訴工作。由於犯罪類型多元，當中以科技犯罪調查部、金融犯罪部作為打擊電信網路詐欺的主要部門，專責處理電信金融詐欺案件，掌握高科技詐騙手法並協調警察與金管機構執行聯合偵查[137]。南韓檢察廳設置多個專責單位來打擊電信網路詐欺，金融犯罪與資金追蹤組（Financial Crimes and Asset Tracing Unit）專門負責分析詐騙資金流向，並與金融監督院（FSS）、金融情報分析院（KoFIU）等監理單位合作，推動可疑帳戶凍結、非法資金追查與受害者資金返還等作業。該組亦負責指揮警方調取帳戶資料與比對異常匯款模式，作為起訴依據[138]。其次，科技犯罪調查部（Cyber & Technology Crime Division）則專責處理新興詐騙手法，如偽冒來電、惡意應用程式、釣魚網站及利用 AI 變聲的「聲音詐欺」。檢方透過數位鑑識技術、IP 與網域分析、通訊紀錄比對等

[136] KCC, Annual Report 2023, p. 90.

[137] Prosecutors' Office. (2025). *2024 년 검찰연감 [2024 Prosecutor's Yearbook]*. 서울: 대검찰청. Retrieved from: https://spo.go.kr/site/spo/ex/board/View.do 最後瀏覽日：2025 年 5 月 27 日。

[138] p. 282，同註 123。

手段蒐集證據，並結合網路安全機構如 KISA 的威脅情報，提高精準打擊力道[139]。當案件規模擴大、涉及跨國詐欺或需整合多機關調查時，檢察廳會啟動跨部門聯合偵查小組，由地方法院檢察署或高等檢察廳主導，協調警察廳、科學技術情報通信部、通訊公司、金融單位與 KISA 等共同調查。檢察官擔任協調角色，統籌調度蒐證、法律程序與國際司法互助事宜，確保案件處理具時效性與合法性[140]。比較特別的是南韓檢察總長能夠根據《預防電信金融詐欺損失及損失補償特別法》第 13 條之 3[141]向主管機關提出「停止詐騙電話號碼服務」的權限，可在詐騙活動進行時即時阻斷通訊鏈，防止更多被害發生。此制度顯示檢察體系在電信詐欺防制工作中的核心角色，不僅止於起訴階段，更涵蓋從偵查、資金攔截到通訊阻斷的全流程。

3. 跨部門合作

南韓打擊電信網路詐欺犯罪的政策，最早可回溯到 2018 年金融委員會所發布的「預防電信和金融詐欺綜合措施」[142](전기통신금융사기 방지 종합대책)，包括虛假簡訊的辨識系統、可疑交易發生時凍結帳戶資金、「人頭帳戶」（대포통장）之處罰範圍、國際合作情報交換與司法互助、透過宣導建立社會防詐意識。同時，針對青少年與高齡者等詐騙高風險群體，進行反詐宣導，擴大識詐觸及率與社會參與度(Choi & Lee, 2021)。隨著年代不斷增加，電信結合網路與金融，使得電信網路詐欺犯罪更加猖獗。打擊電信網路詐欺不再是警察廳、檢察廳這些司法系統下的機構責任，必須透過跨部門的合作才能有效打擊。從打擊犯罪開始，案件受理與初步調查是由警察廳負責，民眾透過 112、

---

[139] p. 284，同註 123。

[140] p. 285-286，同註 123。

[141] When the Prosecutor General, the Commissioner General of the National Police Agency, or the Governor of the Financial Supervisory Service ascertains a telephone number exploited for telecommunications-based financial fraud, he/she may request the Minister of Science, Information and Communications Technology to cease provision of telecommunications service for the relevant telephone number. 同註 106。

[142] FSC(2018). Announcement of "Comprehensive Measures to Prevent Telecommunication Financial Fraud. Retrieved from: https://www.korea.kr/docViewer/skin/doc.html 最後瀏覽日：2025 年 5 月 27 日。

詐騙舉報平台[143]或向金融機構提出電信詐欺檢舉，警察廳即會受理，並啟動初步調查，蒐集帳戶流向、手機號碼、IP、SIM 卡、聊天紀錄等數位證據。檢察官接手後，主導證據整合與法律適用方向，進入司法程序。

上述的過程絕大多數國家都相同，接著是證據的共享才能體現跨部門合作的精神。一旦發現疑似電信網路詐欺犯罪，可向警察廳所建立的網路犯罪舉報系統[144]舉報，並在接獲舉報後立即合併案件進行調查。系統中的「Cybercop」的服務，可檢查電話、電子郵件和電話、帳號和電子郵件地址在過去三個月內是否有無被舉報為疑似詐欺犯罪使用，以防止詐騙交易。針對這些透過報案或網路舉報的疑似帳戶資訊，便能依據預防電信金融詐欺損失及損失補償特別法第 3 條之 2，來進行凍結資金查核帳戶真實性。然而金流相關資訊是證據之一，因此根據電子金融交易法第 22 條，要求金融監督院（FSS）與金融情報分析院（KoFIU）協助比對可疑交易，一旦發現便能對涉案帳戶啟動暫停交易與資金凍結的強制作為。而在電信流的部分，根據《預防電信金融詐欺損失及損失補償特別法》第 13 條之 3，檢察總長可請求電信公司立即中止詐騙電話號碼服務。

對於金融機構阻止詐欺，具體的策略包括凍結詐騙帳戶，依據《預防電信金融詐欺損失及損失補償特別法》，在現場逮捕嫌犯後，可請求金融機構停止可疑帳戶的支付功能，防止資金外流。還有調降無卡 ATM 入金與提領限額，將 ATM 入金限額由 1,000,000 韓元降至 500,000 韓元，並將每日此類交易總額限制為 3,000,000 韓元。此外強化開戶驗證與開放式銀行風險管控，強制金融機構在開戶與交易時執行驗證，若交易異常，要求銀行主動設限或凍結帳戶。

總歸來說，在前線偵查與緝捕行動方面，由警察廳專責打擊電信與金融詐騙案件，負責現場查緝、追查帳戶來源與通聯記錄等。而檢察廳則發揮核心領導作用，擔任案件

---

[143] Korean National Police Agency, 詐騙舉報平台. 取自： https://www.counterscam112.go.kr/ 最後瀏覽日：2025 年 5 月 27 日。

[144] Electronic Cybercrime Report & Management system(ECRM), Retrieved from: https://ecrm.police.go.kr/minwon/main

協調中樞，更能有權請求電信業者立即中止可疑電話號碼之服務，並可針對涉案帳戶啟動凍結資金的緊急程序。資金流的部分則是金融監督院與金融情報分析院，藉由帳戶異常活動及凍結措施來減少被害損失外，也與警檢系統共享疑似詐欺帳戶資料，推動跨機關資金攔截合作。在電信流方面，以韓國網路安全局為首，攔阻釣魚網站、惡意應用程式及可疑 IP 來源，並協助警方與檢方執行通訊來源封鎖、域名凍結等行動。

4. 公私部門的合作

南韓政府為有效因應日益複雜的電信與金融詐騙犯罪，單純只有公部門的打擊詐欺犯罪是不足的，從 2013 年推動的跨部會全流程防詐對策(Comprehensive countermeasures against new and variant telecom financial fraud)，並與通訊業者、金融機構、科技平台、資訊安全公司密切合作，形成高度公私協力體系。近年才由成立 T/F 小組(惡意詐欺根除工作組)來進行整合的工作，定期召開會議，統整預防、查緝、執行、司法程序與國際合作策略。此統籌制度確保資訊共享不中斷、政策滾動式修正，並提升決策反應效率。將最新技術運用於攔截、通訊的即時封鎖，一直到受害者救濟的整體協作策略，考慮相當周全。然而沒有私部門共同合作的話，難以有效的打擊詐欺犯罪，因此南韓政府先與電信業者合作，由通信傳播委員會（KCC）主導，與 SK Telecom、KT、LG U+ 等主要電信公司合作推動「來電顯示真實驗證（Call Authentication System）」、「國際號碼識別封鎖」與「可疑號碼自動攔阻」等手段。當警方或檢察機關確認可疑號碼後，可即時依法請求業者停止該號碼的通訊服務(Choi & Lee, , 2022)。

對於未來將導入 AI 技術來進行防詐，SK Telecom 開發了 Scam Vanguard，這是一種高級人工智能系統。 Scam Vanguard 在 CES 2025 年獲得了網絡安全最佳創新獎，它使用最先進的 AI 來保護用戶免受假訊息的干擾。此一人工智慧系統跨語音呼叫，短信和社交媒體平台這三個領域，Scam Vanguard 檢測到可疑活動時，客戶會在手機上收到警告，並帶有“語音網絡釣魚可疑”等警告。當簡訊詐騙訊息接收時，AI 識別出文字是詐欺訊息時，系統會立即通知客戶。更厲害的是 Scam Vanguard 能透過臥底機器人與詐騙者互動，藉此收集 URL 的相關資訊，在打擊欺詐方面更進一步。Scam Vanguard 也用於

金融領域的工具，其影響力也已擴展到金融領域。通過與韓國興業銀行合作，該技術為名為“Surpass”的解決方案提供支援，旨在保護客戶免受詐欺，自 2024 年下半年推出以來，Scam Vanguard 每月封鎖了 130 萬次騙局和電話，展示了 Scam Vanguard 應對詐欺犯罪預防的潛力[145]。

除了電信公司之外就是金融機構，透過金融監督院（FSS）與金融情報分析院（KoFIU）為主的公部門，配合各大金融機構與銀行，協助司法機關共享可疑交易資料、比對異常匯款模式，快速鎖定詐騙資金流向，並實施暫停帳戶與凍結措施[146]。然而科技日新月異不斷進步下，資訊科技勢必要跟上詐騙的趨勢，因此網路安全局與 NAVER、Kakao、Google Korea 等主要數位平台合作，能夠快速下架與封鎖釣魚網站（phishing）、惡意應用程式（malicious apps）與假冒網頁，避免詐欺犯罪被害範圍的擴大。未來也將推動開發 AI 即時辨識詐騙風險。更重要的是透過大眾宣導與教育來建立正確的防詐意識，透過公私部門的共同合作，推動防詐教育課程、發行簡訊詐騙手冊，舉辦「資安週（User Week）」活動，針對長者、青少年、外籍移工的高風險族群，提供多語言宣導與應對教戰手冊(KISA, 2024)。

5. 國際合作強化

南韓《採取電信金融詐欺防止及受害退款特別法》第 2-3 條[147]明定：「政府應與其他國家或國際組織合作，以預防因電信金融詐欺可能造成的損失。」該條款自 2014 年修訂以來，一直作為跨國協調的法律依據。而電信網路詐欺多為跨境犯罪，因此南韓政府

---

[145] Laurent Garrigues(2025, Jan 20). SK Telecom ScamVanguard: Transforming mobile scam prevention with AI. Retrieved from: https://thereadable.co/sk-telecom-scamvanguard-transforming-mobile-scam-prevention-with-ai/ 最後瀏覽日：2025 年 5 月 27 日。

[146] Financial Services Commission. (2014, December 4). Do you know about the “Safe Savings Account” to prevent financial fraud? [Press release]. Retrieved from: https://www.fsc.go.kr/po010105/71369 最後瀏覽日：2025 年 5 月 27 日。

[147] Article 2-3 (International Cooperation)The Government shall cooperate with other nations or international organizations to prevent loss that may be caused by telecommunications-based financial fraud. [This Article Added by Act No. 12384, Jan. 28, 2014], 同註 106。

必須和多個國際執法機構進行合作，包括 INTERPOL、歐盟刑警組織等，更透過 MLAT 司法互助程序與國外檢察系統合作辦案，也透過簽訂 MOU 合作備忘錄的方式來強化打擊力道。

南韓政府曾經參與過 INTERPOL 聯合行動調查，HAECHI V 行動從 2024 年 7 月至 11 月，超過 40 個國家和地區執法部門的全球合作打詐行動，共逮捕了 5,500 多名嫌疑人，超過 4 億美元的虛擬資產和貨幣。HAECHI V 行動是韓國與中國共同合作，成功破獲語音網路釣魚集團，該集團施行多種電信網路詐欺手法，包括語音網路釣魚、愛情詐騙、性勒索、投資詐欺、非法博弈、商業電郵詐騙和電子商務詐騙等。該集團造成了總計 15110 億韓元的經濟損失，高達 1,900 多名受害者。國際刑警組織還在 HAECHI V 行動期間發佈了紫色通緝令，警告各國注意 USDT 詐欺的警報。該手法首先使用浪漫誘餌技術引誘受害者，指示他們通過合法平台購買流行的 Tether 穩定幣（USDT 代幣）。受害者點入網路釣魚連結，該連結是虛假網頁的投資帳戶，被害者在不知情的情況下從他們的錢包中轉出資金[148]。

全球化導致跨國犯罪、罪犯逃往海外和犯罪所得外流迅速增加，應對犯罪的國際合作已成為一種必要，而不是一種選擇。韓國檢察廳(Korean Prosecution Service, KPS)的國際合作是由最高檢察廳國際合作科(International Cooperation Division at Supreme Prosecutors' Office)的領導下，積極與外國執法機構合作，專責遣返逃往海外的罪犯、追蹤和追回海外犯罪所得、收集海外資料的證據、重大刑事案件的國際合作偵查[149]。韓國檢察廳的國際合作網絡(International Cooperation Network)相當廣泛，韓國檢察廳擔任亞太資產追回跨機構網路 (ARIN-AP) 的秘書處，該網路旨在為亞太地區執法機構交流犯

[148] INTERPOL(2024, Nov 27). NTERPOL financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million. Retrieved from: https://www.interpol.int/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million 最後瀏覽日：2025 年 6 月 2 日。

[149] Korean Prosecution Service. International Cooperation of Korean Prosecution Service(KPS). Retrieved from: https://www.spo.go.kr/site/eng/03/10305010000000202101050 2.jsp 最後瀏覽日：2025 年 6 月 2 日。

罪所得資訊而設立。韓國檢察廳透過處理行政事務和組織各種會議，與海外執法機構在犯罪所得追回領域保持合作。第二是國際檢察官協會(IAP)，韓國檢察廳參加 IAP 組織的各種會議，加強與海外檢察官的直接合作。第三是韓國檢察官協會(KPA)，促進世界各地的韓國檢察官之間的交流與合作。檢警一體的辦案模式，韓國警察廳除了解檢察工作的國際趨勢外，更積極建立與世界各地韓國檢察官與外國執法機構直接合作。目前韓國警察廳已與包括美國和中國在內的 26 個國家的 30 個執法機構簽署了備忘錄，奠定與海外執法機構在調查、審判和執行刑罰方面的合作基礎[150]。

南韓在打擊電信網路詐欺犯罪不遺餘力，從推動法律法規完善開始，對於電信網路詐欺相關的法案進行修訂，從犯罪偵查、電信阻斷、資金凍結、資訊共享、被害支持等面向進行全方面的修訂。警方以「預防-逮捕-連結」為核心，建立綜合電信和金融詐欺報告和應對中心，建立起公私部門協作的泛政府綜合應對體系。從打擊詐欺，凍結帳戶資金與延遲轉帳等，到大眾教育宣傳，有系統地建立統一的防範電信網路詐欺的政府和民間應對體系。

在打擊犯罪方面，分析網路犯罪的類型，並檢查最新的犯罪趨勢，以隨時做好準備。擴展網路國際合作共同打擊電信網路詐欺犯罪，為了預防犯罪損害，也由專門研究網路犯罪的講師提供預防教育。透過網路犯罪舉報系統 (ECRM6，ecrm.police.go.kr）舉報，並在接獲舉報後立即合併案件進行調查。國家警察廳提供一項名為「Cybercop」的服務，可檢查電話、電子郵件和電話、帳號和電子郵件地址在過去三個月內向網路犯罪舉報系統舉報三次。交易前您可以在 Cybercop 上查詢對方的資料，以防止詐騙交易。對於網路詐欺犯罪採取臥底調查和密集打擊

對於加密貨幣成為電信網路詐欺的主要工具，南韓政府持續擴大並推出虛擬資產追蹤計畫，以因應使用虛擬資產的犯罪行為。推出了追蹤南韓加密貨幣交易所的計劃，國際大型幣商交易所和警方建立了直接的聯繫，在 2022 年 10 月 13 日，簽訂了「合作

[150] Korean Prosecution Service. International Cooperation Network. 同註 133。

調查和預防虛擬資產相關犯罪的業務協議」，與國際交易所協調和損害預防進行合作，交換有關犯罪趨勢、犯罪所得追回和洗錢預防等方面的資訊。

Kwon, Borrion & Wortley (2024)說明南韓政府內整合財政、部門溝通和犯罪調查，目標放在詐欺犯罪預防、科技偵查到司法懲戒、援助受害者和提高公眾意識等方面的預防措施。從幾個方向制定政策，第一、建立綜合防制體系，從預防做起，藉由法律與各種網路規範，防止各種虛假訊息藉由手機網路讓民眾接觸網路釣魚詐騙。再來要求金融公司採用詐欺偵測系統（FDS），密切監控與網路釣魚相關的可疑交易，並利用大數據和人工智慧與相關公共機構共享資訊。接著透過法規來問責金融公司和電信服務供應商，強化各種措施來預防網路釣魚詐騙。制定個人認證和身分驗證系統完善計劃，讓金融交易能夠在便利性與認證中取得平衡，最後致力於開發於預防網路釣魚的新數位技術。

第二是加強打擊犯罪和司法懲戒。首先朝向電信網路為主的金融類詐欺犯罪，以司法互助的方式來建立與海外調查機構的合作網絡，完備詐欺犯罪的各種法律制定，尤其是增加對不斷出現的新形態網路釣魚詐欺和其他詐欺犯罪的懲戒力度，強化嚇阻力道來阻卻犯罪發生的風險。第三是要求金融公司擔負賠償責任，金融秩序的穩定是國家社會進步的關鍵，金融公司除了社會道德責任外，也應擔負取法律賠償責任。透過立法確認立金融公司在電信網路詐欺犯罪的責任，只要消費者無故意或過失，金融公司就負賠償責任。另外要求金融公司開發各種針對電信網路詐欺犯罪賠償的保險產品，減少犯罪被害的損失。

第四是維持強而有力的部際合作。由於電信網路詐欺是組織犯罪，透過各種犯罪工具橫跨各領域所完成的犯罪行為，因此要求金融公司與電信服務商合作，對於境外來電、變更號碼提供攔截服務或更多的認證機制。政府對於電信網路詐欺相關部門，南韓互聯網振興院、金融監督院、調查機關和電信公司之間設立熱線電話，分享即使資訊才能有效應對新型網路詐欺，除了行政機關與民間企業的合作，更將透過執法部門和金融公司之間的密切合作，發現並即使防止電信網路詐欺犯罪。

最後則是提高公眾意識著手，不管是辨識詐欺手法還是組卻成為電信網路詐欺的幫手，著手在公共交通、電信供應商和銀行，透過電視廣播和 YouTube 頻道製作更多公共服務廣告進行撥放，越多民眾接觸電信網路詐欺的辨識知能，越能夠降低該犯罪所帶來的損害。要求各金融公司在網路銀行、APP 程式中公佈其防釣魚措施，政府應主動利用各種訊息公布方法，定期發送公共警報訊息，隨時提供如何精準辨識電信網絡詐欺的虛假訊息資料，提高公眾對電信網絡詐欺犯罪的認知。

南韓政府對於根除電信網路詐欺犯罪的政策，政策方向有助於建立一個更負責任和基於信任的數位經濟，讓個人能夠在更安全、更便利的環境中使用金融和通訊服務。而公眾應謹慎對待私人數據，強化自己辨識電信網路詐欺的金融詐騙，更應謹慎使用智慧型手機，不讓個人身份遭到冒用而受到威脅。

(四)南韓打擊電信網路詐欺的困境

南韓的電信網路詐欺破案率不高，這主要是由於兩個原因。首先，新型互聯網和電信詐騙犯罪領域對風險因素的定義不全面，導致問題沒有得到明確的定義。其次，網路詐騙犯罪資訊大多使用自然語言記錄，數量龐大，缺乏自動化、智慧化的方式來深入分析和提取風險因素。南韓在打擊電信與網路詐欺方面投入大量資源，制定多項法律並加強執法，但仍面臨重大困難。詐欺手法不斷進化、跨國犯罪、法律與技術應對不足，是主要困境。首先是詐欺手法快速演變，從早期的語音詐騙（Voice Phishing），發展到 Pharming、Smishing、記憶體駭客、Qshing、色情視頻勒索等，犯罪集團持續創新手法，規避現有防範措施，使得打詐政策與法律男以跟上這些手法的更新速度。其次是法律框架與執行落差，現行《電信金融詐騙防制法》主要針對傳統語音釣魚（보이스피싱），但新型詐騙如「預約不履行詐騙」（노쇼 사기）與「虛擬貨幣投資詐騙」無法適用帳戶凍結措施。單純偽造社交媒體帳號冒用他人身份若未涉及直接金錢詐取，依現行法僅能適用輕微的《資訊通信網法》第 44 條，最高處 500 萬韓元罰款，缺乏刑事威懾力。法律與技術應對有限，雖有多部法律，但因犯罪手法多變，現行法規與技術防線難以全面

防堵(Park & Yoon, 2018; Kang, 2021; Jeong, 2025)。

接著是技術對抗與取證挑戰,目前電信網路詐欺開始使用 AI 合成語音(Deepvoice)模仿金融機構客服,儘管南韓開發「ChainTracker」區塊鏈分析工具,但混幣服務屬於涉案加密資產,多數的跨境交易所配合度低,平均需 14 天回應凍結請求。這也顯示出南韓在跨境犯罪與司法協作有許多難以解決的困境,像是從境外遣送回來的犯罪者,也因為證據的保存無法符合目前法院的規範,定罪率不高,凸顯出跨國犯罪與執法困難,證據蒐集、引渡機制不足,導致執法成效有限,也使得詐騙集團常設據點於海外。然而為了能夠強化力道,公私部門協調必須更緊密,但《電信金融詐騙防制法》雖要求銀行承擔「冷靜期」攔截義務,但仍有些許異常轉帳因而未被凍結。許多電信服務業者以「用戶隱私」為由,拒絕向警方提供即時通話元數據。世界各地的員警組織都面臨著前所未有的新挑戰。這主要是由於資訊和通信技術的進步以及長期的 COVID-19 大流行,這兩者都正在重塑社會關係的性質。特別是電信網路詐欺的普遍性和頻率急劇增加,導致社會危害也預計會增加,如果不採取積極的預防措施,在第一時間阻止,將讓更多潛在受害者變成實際的受害者(Chung, 2008; Ju, Cho, Lee & Ahn, 2021; Jang & Suh, 2024)。

第三節 相關電信網路詐欺犯罪研究與各國政策的比較

一、 相關電信網詐欺犯罪研究

(一)犯罪組織型態研究

電信網路詐欺犯罪多半透過組織之間進行跨國合作，Cross(2020)指出當前的電信網路詐欺是由某國家的犯罪者針對第二個國家進行電信詐欺，迫使該受害者將大筆金錢匯款到第三或第四個國家。從社會符號學的角度，發現電信網路詐欺利用話語各項資源來製造假信息，虛假身份，獲得被害人信任進而欺騙和操縱被害人提供機密信息和資金。有些研究則著重在跟機房相關的電信網絡、數位網絡、行動網絡、VoIP 的語音網絡協定以及第三方發話等資訊流，了解電信網路詐欺的電信手法。Carroll (2018) 對 VoIP 的主要特性、優點和缺點以及已知的漏洞和安全風險進行研究。包括對已知漏洞和安全風險的詳細分析，企圖建構檢測系統、數據過濾、監控警報系統來解決電信詐欺犯罪的氾濫(Anbarasi & Radha, 2021)。

(二)犯罪偵查與策略研究

國外許多研究開始針對詐欺技術發展閾值規則 (threshold rule)檢測方法，當超過一定數值將觸發警報，進一步進行詐欺犯罪風險評估。 (Mawgoud & I. Ali, 2020)。為了提高打擊詐欺的有效性，企圖建構一套 AI 智能電信管理系統，藉由圖像處理技術、語音識別系統、垃圾郵件檢測等方式，以 SIM Box 以及對話紀錄來分辨出正常用戶與詐欺集團，找出所有詐欺犯罪意圖並及時阻止。

Geng (2017)認為詐欺犯罪的預防基於了解各種犯罪的要件，從了解犯罪的關鍵要素方能夠對症下藥。中國的跨境電信詐欺面臨諸多困境，價值觀分歧、法律規範不完備、輿論的壓力和人性的弱點都是讓詐欺犯罪越顯猖獗的原因。Jauhar R. S. (2020)以情境犯罪預防的觀念來制定印尼相關的詐欺犯罪政策。透過社會網絡分析方法，把印尼國內機

構與其他國家監管機構相關的網絡關係加以分析。建構出跨國網絡的架構，整合所有可能的資源，企圖透過機構內部的結構和協調方式強化跨境犯罪預防的力道，將公共行政領域的監管治理予以理論化，奠定電信網路詐欺犯罪的預防基礎(Heijden, 2020)。

(三)法律與司法互助研究

司法互助的框架下提出了快速共享概念體系，節省高昂成本並提高跨境協作效率。Yu, Cong, & Li(2024)指出國際司法機構合作機制不明，犯罪蒐證與偵查不易，以及刑事司法系統的腐敗，對於電信網路詐欺預防政策束手無策。要克服電信網絡詐騙的困境，只有結合司法互助具體實踐並提出對策，使得電信網路詐欺犯罪偵查在案件線索交換、刑事情報、協助調查取證、引渡、遣返、追回犯罪所得等的合作才能夠有效遏止電信網路詐欺犯罪(Hua，2020)。由於各國主權獨立，在不侵犯主權的前提下，提出透過聯合國整合並強化國際上的司法互助，共享犯罪偵查資訊，才能有利於遏止跨國犯罪的蔓延。聯合國垂直及橫向的整合，針對特定的跨國犯罪組織解決犯罪問題，包括洗錢、毒品、走私、網絡、詐欺犯罪 (Gless, 2019)。

電信網路詐欺已經漫佈全球各地，目前最棘手的問題在於國際間的司法互助。鑒於我國特殊的國際地位，凸顯出我國在國際司法互助的困境，許多研學者開始針對我國目前執行司法互助的現況，國際間之刑事司法互助原則，寄望能夠提出有效且全面的司法互助合作模式(吳秋宜，2015；蔡佳穎，2017)。另外有些研究從司法實際運作、偵查蒐證困境、境外關係以及國際警政合作等相關議題著手(呂鴻進，2017)，運用國際關係「層次分析」理論以及「（3+1）i 決策模型」、「政策社群」、「策略規劃」進行研究，從政策及組織架構來探討我國在司法互助上的效能 （李華欣，2011；蘇信雄，2012)。針對電信網路詐欺犯罪所進行的法律及國際司法互助的研究，量多且質精，每位學者都提出獨到的見解與後續的政策建議。

二、 各國政策的比較

(一)法制規範

面對日益猖獗的電信網路詐欺問題，美國、歐盟、日本與南韓均建立了多層次的法律與制度體系以因應此一挑戰。整體而言，四者皆重視跨部門協力與技術導入，惟其法律架構與執行重點因法制體系與社會需求而呈現差異。

美國早於 1991 年制定《電話消費者保護法》（Telephone Consumer Protection Act, TCPA），透過限制自動撥號與偽冒號碼行為，為全球首波防制詐騙立法。2018 年《RAY BAUM's Act》進一步要求通訊業者提供精準位置資訊以強化應變能力，並由聯邦通訊委員會（FCC）主導實施 STIR/SHAKEN 通話驗證架構（FCC, 2024）。歐盟則於 2022 年實施《數位服務法》（Digital Services Act, DSA）與更新《電子隱私指令》（ePrivacy Directive），要求大型數位平台主動篩檢與下架詐騙訊息，同時強化平台治理責任並要求透明通報機制。日本法制強調以《詐欺特別法》與《犯罪收益移轉防止法》為核心，並授權警方與金融機構即時凍結可疑帳戶，此外，日本總務省亦推動反詐來電通知系統，鼓勵地方社區安裝「反詐音聲設備」（高齡家庭警示器）來預防詐騙。南韓則建立《電信金融詐欺防止特別法》、《電信事業法》與《資訊通信網法》的整合法體系，賦予檢察官與警方在確認詐騙行為時得即時凍結帳戶、封鎖號碼與查扣資金的廣泛權限。2023 年起，南韓政府推行「新型態詐欺綜合對策」強化跨機關通報與 AI 輔助分析模型。

在電信技術法規層面，美國領先推行 STIR/SHAKEN 制度，強制業者實施通話簽章技術來驗證發話端的真實性。此外，《RAY BAUM's Act》第 506 條要求業者提供 911 系統精準定位，亦間接提升緊急應變效能。歐盟除推行 OTT 平台責任制外，也鼓勵各國監理機關建構自動化識別模型，針對詐騙短信與來電進行分析，部分成員國如德國與法國已設立防詐網關與黑名單機制。日本則透過地方警政合作推動反詐警示音系統，並與通訊業者合作導入「電話識別提示」技術，已於 2022 年針對特定高風險族群進行測試性推行。南韓的 KISA 主導建置「詐騙 API 平台」，提供即時號碼與 IP 評級資訊，並

與金融監理機關共享警示名單。KCC 則推動來電顯示真實驗證制度，要求國際來電標示前綴號碼來提升辨識力。

金融詐騙與帳戶凍結法規上，美國實施 BSA（銀行保密法）與由 FinCEN 主導的可疑活動報告制度（SARs），銀行須主動回報異常交易行為。2023 年起也要求金融機構加強 KYC 更新頻率與客戶風險評級調整。歐盟透過第 5 與第 6 版《反洗錢指令》（5AMLD, 6AMLD）強化銀行與虛擬資產平台之間的資訊整合，設置受益人實名資料庫（UBO register）為核心。日本與南韓皆重視即時凍資制度。南韓特別建立「統一帳戶凍結平台」與「入金帳戶指定制度」，由金融監督院（FSS）、金融情報分析院（KoFIU）與韓國銀行聯合會（KFB）共同運作，確保詐騙金流在 24 小時內遭封鎖。此外，南韓自 2023 年起限制無卡與 ATM 高額存款金額上限，預防詐騙集團透過現金灌帳洗錢。

綜合來說，各國都採取了電信技術、金融限制與法律規範為主的方式應對詐騙問題。相同點包括強調跨部門資料共享、KYC 與 AML 技術應用，以及平台與金融機構的合作責任；而差異性則在於美歐較強調平台與通訊技術的制度建置，而日韓則更加強調檢警主導、快速凍資與實務封鎖的執行力道。南韓可謂在法律授權與即時執行力方面最為周延，形成具有即時防禦與追訴能力的完整法制體系。

(二)機構聯合

打擊電信網路詐欺犯罪本就非單一機構的職責，從警察、檢察、電信、金融、科技與教育等機構都負有相當的責任。以美國來說，以反詐欺架構以聯邦通訊委員會（FCC）與聯邦貿易委員會（FTC）為主軸。FCC 負責監管通訊業務，推動如 STIR/SHAKEN 等來電驗證技術；FTC 則聚焦於消費者保護與詐欺案件調查。兩者與司法部（DOJ）、國土安全部（DHS）、以及金融犯罪執法網絡（FinCEN）等機關協作，強調「通訊技術防堵＋金融追查」的雙軌制度。此外，美國設有消費者金融保護局（CFPB）與網路犯罪投訴中心（IC3），進行數據整合與民眾通報受理。

日本則以警察廳（NPA）下轄的生活安全局為主力，並設有「反特殊詐欺專責小組」，

專責處理如電話詐騙與假冒公務員詐騙等案件。配合金融廳（FSA）與地方警政單位，形成中央統籌、地方執行的雙層結構。日本亦特別強調「社區警政」與金融機構間的合作，設立「反詐櫃台」與通話預警系統，由地方銀行、郵局、便利商店共同攔阻可疑匯款。歐盟機制主要仰賴歐洲刑警組織（Europol）與歐洲委員會的數位安全部門進行跨國詐騙調查、數據共享與行動協調。尤以「EMPACT 計畫」為歐盟境內合作打擊詐欺與網路犯罪的重要平台。各成員國則須落實相關法條的規範，強化對平台與金融行為的稽核與回報機制。

南韓建立了高度協作的「跨部門聯防體系」。檢察廳擔任重大詐欺案件的統籌單位，與警察廳、金融監督院（FSS）、金融情報分析院（KoFIU）及韓國網路安全局（KISA）緊密合作。KISA 負責技術端的 API 串聯、惡意網址與 App 攔阻；而通訊傳播委員會（KCC）則負責推動「來電驗證」與「詐騙話語 AI 模型」系統。南韓並建構了「統一帳戶凍結平台」與「入金帳戶指定制度」，可即時凍結可疑資金，防堵受害擴大。

綜上所述，美國的制度設計偏向聯邦與州的分權，轄下機構負有資料報告義務與法定協作機制。歐盟則強調跨國間的資料透明與成員國協作框架。日本由內閣府、警察廳與金融廳主導，執行須仰賴地方政府，且日本並無統一的中央資料平台，而是透過區域警察與地方金融機構即時回報與配合。南韓則採取高度中央整合架構，即時串接電信、金融與警方系統，協助追查、封鎖與阻斷詐騙資金流或通訊路徑。中央統籌強化了應變效率與封鎖力道，跨部門協作制度化程度高 。

(三)查緝偵辦

在美國，查緝機制主要由聯邦執法機關主導，如聯邦調查局（FBI）、聯邦貿易委員會（FTC）及財政部屬下的金融犯罪執法網絡（FinCEN）。FBI 透過其 Internet Crime Complaint Center（IC3）彙整民眾報案與網路詐騙資料，再結合跨部門行動（如 Operation Eagle Sweep）進行打擊。而檢察體系則由各地的美國聯邦檢察官辦公室（U.S. Attorney's Offices）發起刑事起訴，司法部（DOJ）則統整全國性大型詐騙案件，且透過司法互助

機制（MLAT）與多國合作。美國的優勢在於高度制度化的偵查體系與龐大的司法資源支持。

歐盟的查緝偵辦由各會員國的司法與警政單位進行，但其跨國案件多透過歐洲刑警組織（Europol）與歐洲司法合作機構（Eurojust）協調辦理。Europol 設有專責的網路犯罪中心（EC3），可執行跨境調查、資料整合與行動部署。Eurojust 則協助成員國之間的檢察協作與證據轉移，並推動建立「歐洲調查令（EIO）」制度，加速資訊交換。歐盟的特點在於制度協調與法制整合的高效率，尤其面對跨國詐騙集團，能迅速動員多國執法資源。

日本方面，查緝工作以警察廳為核心，由都道府縣警察部門成立「特殊詐欺對策本部」負責偵辦。警政系統有良好的地域分布與社區連結，加上警察與金融機構之間有「即時帳戶凍結協議」，使得查緝與凍資作業極為迅速。檢察官在日本則通常於案件進入起訴階段才開始主導，前期偵查主要由警察系統負責。日本的特色為強調現場執行與社區警力運用，並輔以法務省推動的「被害者支援系統」。

南韓在查緝架構上，強調檢警合作與即時應變機制。警察廳設有「電信金融詐欺調查隊」與大數據分析部門，負責即時掌握可疑來電與資金流向。檢察廳則負責指揮重大案件，特別是跨境詐騙與金融整合犯罪，並具備依據《電信金融詐欺防止特別法》第 13 條之 3 對號碼中止與帳戶凍結下達命令的權限。檢察體系亦透過 MLAT 程序與他國合作，並主導高風險案件的證據整合與國際追訴。

整體比較而言，美國與歐盟制度強調跨機關資料整合與跨境合作，日本則重視警政主導與社區連動防制，南韓則展現出檢察主導、迅速反應的特點。各國雖採不同策略，但均強化數據運用與部門合作，以因應日益複雜的電信詐騙犯罪。

(四)公私協作

面對跨境、高科技化的電信網路詐欺，各國普遍認知到單靠政府力量無法全面防堵

詐騙威脅，因此紛紛強化與電信業者、金融機構、科技平台等民間企業之協作機制。此種「公私協力」（public-private partnership）模式在制度設計、資源動員、資料共享與技術研發等面向展現出顯著的異同。

美國透過《電話消費者保護法》（TCPA）與 STIR/SHAKEN 來電驗證機制，強制要求電信業者導入技術防詐。由聯邦通訊委員會(FCC)主導，民間業者如 AT&T、Verizon 與 Google Cloud 等皆須遵守「來電真實驗證技術」部署時程，否則可能遭罰。金融面則由金融犯罪執法網（FinCEN）主導，銀行須定期提交可疑活動報告（SARs），並接受洗錢與詐欺相關訓練。以「法規強制揭露與共創合作平台」為核心，公私部門間雖存在合作，但以合規性與罰則作為驅動力。歐盟則以《數位服務法》（DSA）、《網路與資訊安全法》（NIS2）與《反洗錢指令》（AMLD）構建一套跨國協作框架。強調社群平台對詐騙內容的下架與監控責任，要求金融機構進行跨境客戶審查，組建歐洲金融情報單位協調網。歐盟由歐盟委員會主導統合政策，但具體實施仍由成員國執行，公私合作程度較南韓與美國分散，需靠法律義務與資安框架落實。

南韓由國務總理室統籌「新型電信金融詐欺綜合對策」政策，設置跨部門協商機制，並由金融監督機構、電信傳播委員會、KISA 等主責單位推動。公部門與韓國銀行聯合會（KFB）、主要電信商、與金融機構密切協作，建立統一帳戶凍結平台、落實入金帳戶指定制度、Scam Vanguard AI 系統、反詐騙 API 資料共享平台等。這些機制強調即時資料交換與共同封鎖措施，民間機構須主動配合政府指令，例如依檢方指令凍結資金或封鎖特定 IP 與電話號碼。日本的公私協力模式較偏向業界自律與協助。例如「電信事業者協會」與「金融機構協會」會訂定共同防詐準則，地方政府與警察署則進行協調與教育推廣。政府提供技術補助，例如推動在 ATM 安裝「反詐語音提醒系統」，或於超商端點部署防詐警示標語。然而，由於資料共享法律較為保守，實務上銀行與電信業者之間合作仍受限。政府雖於近年推動整合平台建置，但與南韓之高度整合性仍有差距。

韓國高度整合化的公私協力架構能有效提升詐欺阻斷時效。主要是因為南韓有明確的行政與法律規範，例如檢察總長可直接要求 KISA 或銀行實施攔阻行動，因此能在詐

騙初期介入。反觀歐美日公私協力模式雖強調責任制度與業者義務，但受限於資料傳輸法規與分權制度，跨域反應速度略顯緩慢。此外，部分歐盟成員國與美國地方政府之間對於詐騙定義與執行方式仍不一致，實務上的合作仍有待觀察。

(五)國際合作

在全球面對跨境電信網路詐欺日益嚴峻的趨勢下，美國、歐盟、日本與南韓皆積極推動跨國合作，以強化資訊共享、犯罪偵防及資金追查的成效。由於電信網路詐欺多屬跨境犯罪類型，建立合作架構與國際參與機制才能有效遏止詐欺犯罪。美國透過聯邦調查局（FBI）、司法部（DOJ）與國際刑警（INTERPOL）、歐洲刑警組織（Europol）建立長期合作關係，並積極推動「全球反詐欺行動網（Global Anti-Scam Alliance, GASA）」等多邊平台，協調全球執法資源以打擊跨境詐欺。歐盟則依據《歐洲刑事司法合作條約（Eurojust）》架構，推動成員國檢警間的情報交換、同步調查與聯合行動，並與美國透過 MLAT（Mutual Legal Assistance Treaty）建立雙邊合作。日本則與亞太區各國進行多層次合作，例如與東南亞國家簽署警政協定，強化對詐騙集團遷移至第三地的追蹤與打擊；並與韓國、新加坡等國交換可疑帳戶資料與 VoIP 通話紀錄。南韓則設有跨國聯合偵查小組（Joint Investigation Taskforce），在重大詐欺案件中由檢察廳與警察廳出面協調國際合作，並在外交部與 INTERPOL 機制下請求通訊監察、凍結國外帳戶或遣返嫌疑人。

推動國際合作需要法律與政策基礎，美國依據《國際刑警合作法》、《反洗錢法》（AMLA）與 BSA（銀行保密法），授權 FinCEN 與 FBI 在特定情況下要求外國銀行提供交易資料；歐盟則依《刑事事項歐洲調查令》（EIO）及《歐洲拘捕令》作為跨國合作的法律基礎，確保各成員國能互相執行調查程序與逮捕令。日本則根據《司法共助法》與《外國判決承認法》，可主動請求與應對外國執法需求。南韓則於《電信金融詐欺防止特別法》中增設第 13 條與 13 條之 3，賦予檢察機關可對詐騙號碼進行中止請求，並結合《刑事訴訟法》第 216 條規定，允許對外國帳戶展開資金追蹤。

美國以 DOJ 主導，配合 FBI 與 ICE-HSI 進行聯合查緝，並派遣駐外法律專員協助蒐證與移送；歐盟依賴 Eurojust 與 Europol 的中心平台，促成共同調查計畫（JIT）。日本則透過警察廳（NPA）與法務省主導國際聯繫。南韓由檢察廳指揮跨國案件偵辦，與警察廳、大檢察署海外聯絡室、KISA 與金融機構共組應變小組進行海外追訴。

美國強調技術平台的開放與共享，推動與國際 CERT 組織合作進行威脅資料比對。歐盟則成立 CSIRT 網絡進行網路威脅通報與平台風險分析。日本建置跨境詐騙通報平台，並開放 API 供業者接入。南韓則以 KISA 為技術中心，透過反詐 API 串聯國內外資料來源，並建置與 INTERPOL 共用之通訊阻斷平台。

總結而言，四國在跨國合作打詐上均已發展出制度化的聯繫機制，但制度重心有所差異，美國重視檢警協作與法律先行，歐盟偏重區域整合與程序保障，日本強調實務通報效率與亞太聯防網絡，南韓則具備檢察主導、結合技術與外交的高度應變體系。

第三章 研究方法

第一節 研究架構

本研究架構如圖 11 所示，透過對電信網路詐欺犯罪的定義、類型、手法與特性進行分析，透過各國文獻以及相關研究的蒐集，從政策制度、具體執行、法律抗制與犯罪偵查等四個面向進行探究，除了針對我國目前的打詐政策加以深入探究外，並且訪談第一線的檢警調人員，了解打詐的困境以及後續的改進建議。接著蒐集美國、歐盟、南韓與日本的打擊電信網路詐欺犯罪的整體政策，從上述的四個面向進行探究，與我國的抗制政策做優劣分析，最後提出短中長期的電信網路詐欺犯罪抗制政策。

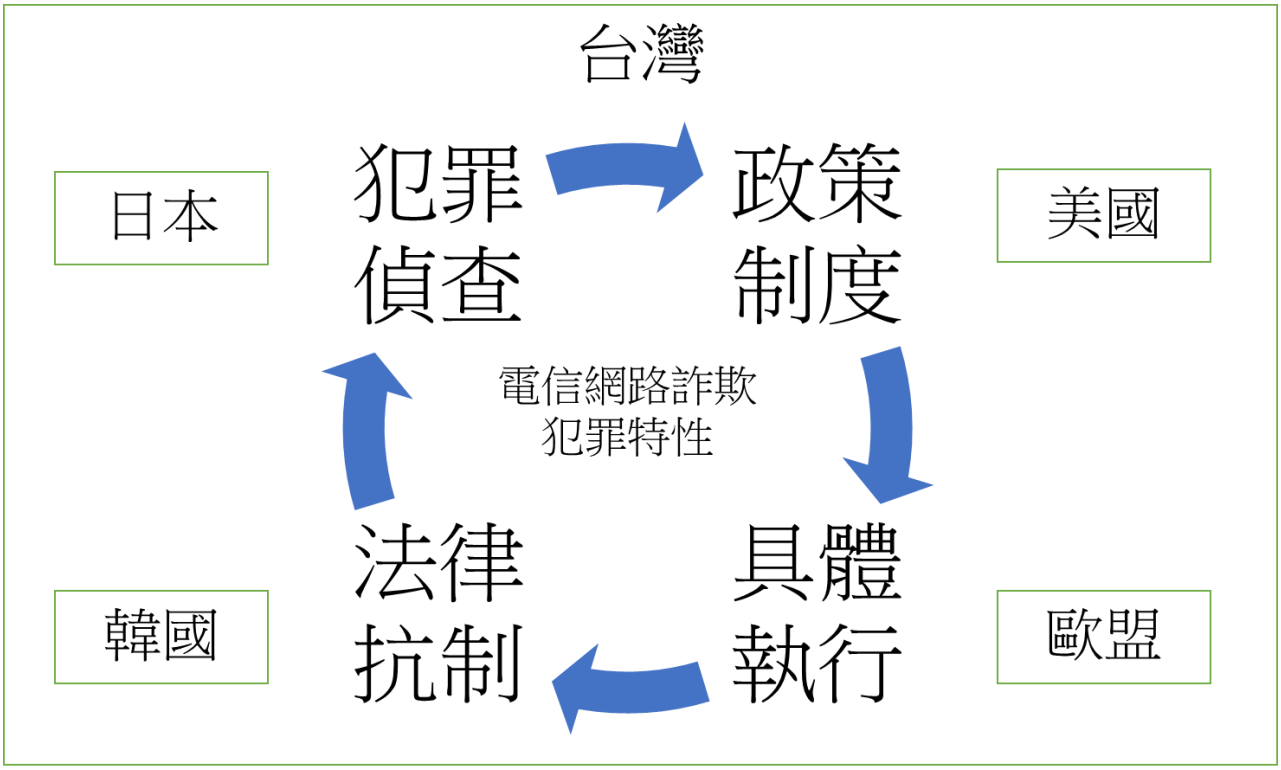


圖 11 研究架構圖

第二節 研究流程

本研究的流程如圖 12 所示，本案研根據「研究目的」研擬適合「研究方法」，引為後續資料蒐與分析之架構。由於研究目的旨在擘劃我國短中長期抗制電信網路詐欺犯罪的整體政策規劃，經分析研究主題內容及性質傾向，認為本研究適合採用「跨國比較研

究」。概以先對國內第一線打擊電信網路詐欺的檢警調專家進行深度訪談，了解我國目前打詐方向以及面臨的困境，再透過國內、外官方文獻等「次級資料」的蒐集、綜理及分析，進行國內外打詐政策與實務上的優劣比較，初步提出我國抗制詐欺的政策計劃。同時輔以一場次「專家焦點座談」，藉以深入探悉相關業務主管高層及專家學者，對於研究主題的策略性思考及具體建言，再加以檢討與改進，最後綜整歸納本研究結論與建議。

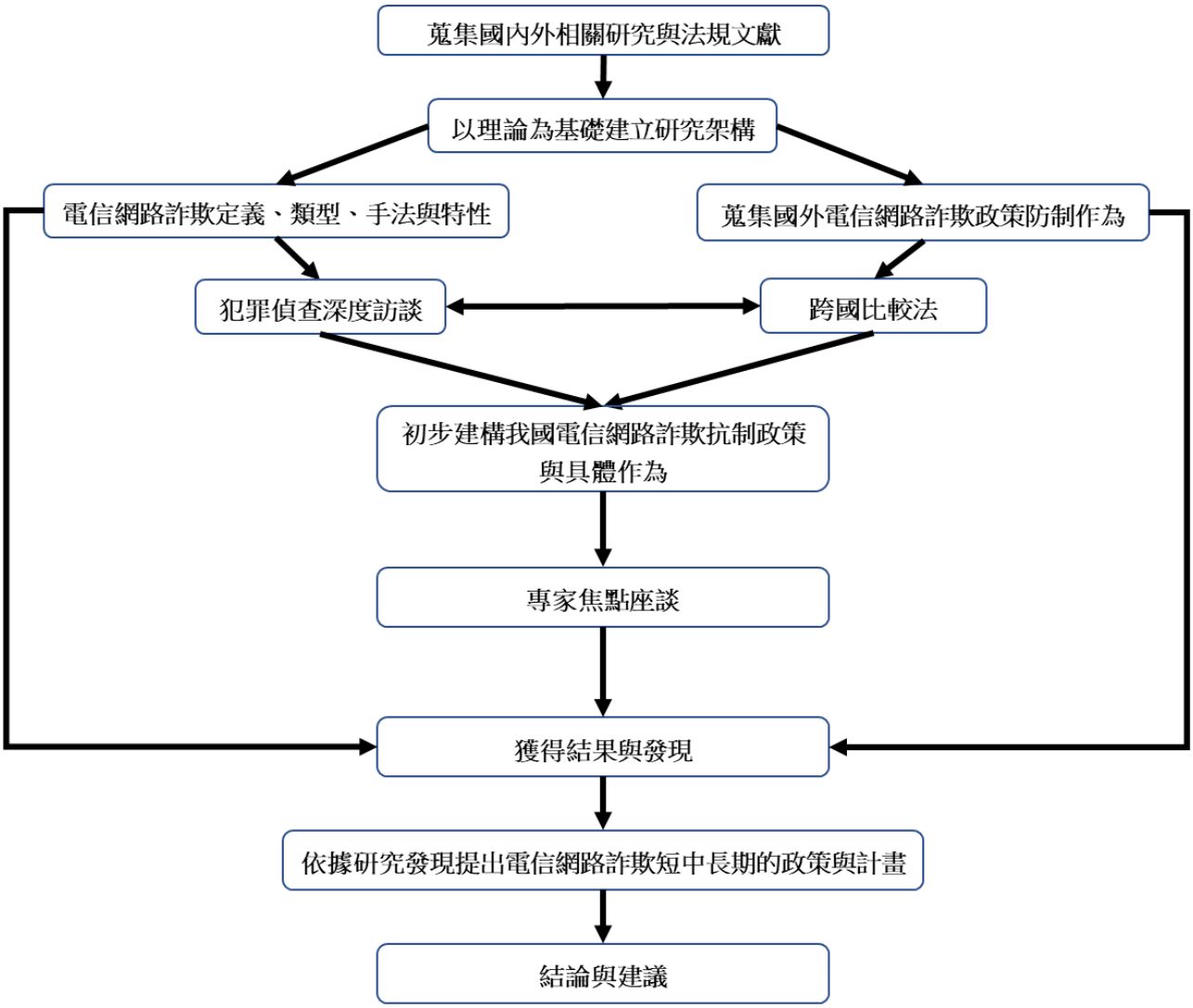


圖 12 研究流程圖，資料來源：本研究整理。

第三節 研究方法

本研究以文獻分析法為基礎，將國內網路詐欺現況進行說明，並且建立研究架構與以理論為基礎的調查問卷。接著以問卷調查以及質性訪談來獲得研究資料，蒐集網路詐欺被害的人口特性、被害樣態、內外環三角因素、社會結構限制與個人心理狀態的資料。茲分別說明如下：

一、 文獻分析比較法

本研究為了瞭解我國電信網路詐欺與其他各國抗制政策，透過文獻與資料的蒐集後，了解我國電信網路詐欺的整體抗制政策，我國電信網路詐欺集團犯罪防制之落實課題：請研究團隊從犯罪特性、制度與政策發展、實務執行狀況與調整等，盤整我國如欲發展政府、民間之跨部門防制電信網路詐欺集團犯罪模式，相較前項國家經驗，仍存在何種差異與困境。

二、 檢警調人員質性訪談

本研究為了能夠了我國電信網路詐欺定義、型態、手法與特性，除了蒐集與分析我國相關電信網路詐欺的相關研究成果之外，為了瞭解我國打詐的實務作為與困境，對第一線查緝電信網路詐欺的檢警調人員進行深度訪談，預計訪談檢察官 3 位、電信詐欺偵查警員 4 位、國際科刑警 2 位、行政院打擊詐欺指揮中心長官 1 位，共 10 位。然而目前打詐指揮中心的指揮官由由內政部次長兼任，另外有執行秘書等人，中心的相關人員，由行政院、 內政部、 法務部、數位發展部、 金融監督管理委員會及國家通訊傳播委員會等相關機關所屬人員擔任， 共同辦理業務。然本研究小組幾經開會討論後認為，政策的制定與施行，應由實務執行上所遭遇到的困難來加以修訂，由於目前打詐政策已經邁入 2.0 版本，相關政策架構已經相當完整，根據本研究主題，應以打詐實務人員為主才能了解整體政策上的執行過程，因此本研究團隊修改訪談人員組成，打詐第一線相當有經驗之偵查人員、一位主任檢察官、兩位法官，當中一位法官由檢察官轉任，兼顧打詐實務、起訴與判刑的刑事司法程序。此外由於目前詐欺犯罪案件量相當多，小組在約訪

時，許多檢察官婉拒研究小組邀約，然小組認為量刑亦為本次討論重點，因此邀約兩位法官接受訪談。透過深度訪談才能了解目前打詐政策的由上至下的抗制作為實務執行層面與困境。表述辦案實務過程與遭遇困境，對於目前抗制網路詐欺的政策給予建議，方能了解政策困境，進而提出改正建議。本次訪談的人員共計 8 位，有五位經驗豐富的偵查人員，一位檢察官與兩位法官接受訪談，針對本研究所提出的相關問題提出自身經驗與後續建議。

表 18 訪談人員表

編號	擔任職務	打詐經驗
A01	刑大偵查人員	2015 年開始至今
A02	刑大電偵人員	2019 年開始至今
A03	刑大偵查人員	2014 年到 2024 年底
A04	刑大偵查人員	2016 年開始至今
A05	偵查人員	2017 年開始至今
A06	檢察官	2018 年開始至今
A07	法官	2000 年擔任法官至今
A08	法官	前 18 年擔任檢察官，近 2 年擔任法官

三、 專家學者焦點團體座談法

焦點團體訪談法（Focus group interviews）是一種以「團體」訪問的型式，進行質性研究收集資料的方法。本研究將由研究主持人、協同主持人與熟識電信網路詐欺犯罪之實務工作者和學者專家進行焦點團體座談，針對初步對於各國電信網路詐欺政策分析比較後所提出的政策規劃，由參與的成員自由表達其經驗、看法或觀點，期能以最短時間內，獲得廣泛且詳盡的資料。為能使資料蒐集更加齊全及完備，本研究將召開專家焦點座談 1 次，該場次預計有相關專家學者共 5 位。

表 19 專家座談人員

編號	擔任職務
A01	165 中心金融股長
A02	CIB 詐防中心研究員
A03	台南地方檢察署檢察官
A04	台南少院法官
A05	助理教授

一、 文獻蒐集國家

本研究將蒐集各種文獻，建構起整個研究的架構、研究方法、研究執行流程及各篇章節撰寫重點。文獻包括我國官方的電信網路詐欺犯罪現況資料，蒐集我國電信網路詐欺犯罪研究成果，對於電信網路詐欺的定義、手法、類型與特性有全面性的認知。接著蒐集美國、歐盟、南韓與日本的電信網路詐欺犯罪政策與具體作為，將我國與各國的網路詐欺犯罪政策進行分析比較，找出政策制度、具體作為、法律抗制與犯罪偵查四面向的較佳策略，提出我國整體打詐政策的規劃藍圖。

二、 深度訪談

本研究為了解我國打擊電信網路詐欺的實務與困境，預計針對第一線犯罪偵查的檢警調人員訪談，預計訪談檢察官 3 位、電信詐欺偵查警員 4 位、國際科刑警 2 位、行政院打擊詐欺指揮中心長官 1 位，共 10 位。透過深度訪談才能了解目前打詐政策的由上至下的抗制作為實務執行層面與困境。

三、 專家座談場次

本研究預計召開一場專家焦點座談，該場次預計有法學、檢警調、獄政、行政部門、電信網路、金融機構專家學者共 5 位。會議將針對本研究文獻蒐集當中的各國網

路詐欺政策與具體防制作為進行研討，針對研究初步結果來進行討論，提出未來針對網路詐欺犯罪的全面抗制具體作為，或者是未來修法的建議。然而因本研究整體架構為檢視我國打詐政策的前提，而打詐政策中並未有針對獄政教化矯正的部分提出具體政策說明，因此亦難以對本政策進行檢討與修正，且目前獄政中並未有專為詐欺犯設計的矯正方案，像是詐欺犯的教育輔導課程、假釋條件等，若未來被獨立列為打詐政策核心之一，本議題將可納入政策的檢討與修正。

第五節 研究限制

本研究透過國內外文獻與法規的蒐集，探討電信網路詐欺犯罪，尤其該犯罪是跳脫傳統的犯罪型態,該類新型態的電信網路犯罪案件與利益損失持續攀升,讓人聞之色變。當犯罪成為社會大眾輿論焦點同時，犯罪抗制也成為重要的公共議題，除了探究新興犯罪類型與手法，從巨觀的角度來看政府面對電信網路詐欺的政策趨勢、法制完備、犯罪偵查等面向,提供政府面對電信網路詐欺政策與作為上的觀點。然而本研究進行過程中，對於各國打詐政策的資料蒐集，有鑑於各國對於打擊電信網路詐欺並非如同我國有打詐綱領的政策，雖然詐欺犯罪亦為該國之相當嚴重犯罪類型，然對打擊詐欺犯罪的資料與相關官方政策並未更新至最新年度的資料，因此在進行分析時，難以全貌的了解該國的打詐政策。

其次，本次對於質性訪談之八位實務專業人員，偵查人員因受限於其承辦的案件型態無法兼顧所有電信網路詐欺的型態，承辦案件過程與個人辦案手法廣度有限，因此其回答之內容無法與現行法令有立即性的連結，甚或是偵查人員對於法令的更新尚未全權掌握，進而對於過去承辦案件之困境進行意見表達。雖然檢察官之承辦經驗與權限較偵查人員多，其作法與經驗亦無法代表全國檢察人員之情形。而受訪之法官對於量刑角度本就有其專業考量，亦無法推論至全國法官皆有相同之看法，特此說明。

最後，本研究先從社會學角度來分析電信網路詐欺犯罪之脈絡，從全球化跨越到消費與數位經濟的時代，亦說明整體電信網路詐欺犯罪的形成，若未來計畫經費與人力許

可之下，可將社會學中的結構功能論(Functionalism)、衝突理論(Conflict Theory)、符號互動論(Symbolic Interactionism)為主軸、對於家庭、學校、經濟、法律、獄政、科技與媒體等面向加以探究，對於整個社會過程與文化進行社會學角度分析。

第四章 我國打擊詐欺政策內涵與實務

第一節 我國打擊電信網路詐欺政策之內涵與演進

電信網路詐欺犯罪是目前詐欺犯罪中的主流模式，由於新冠肺炎的爆發，封城與降低社交接觸的情形下，人與人之間對於網路的依賴愈趨嚴重，而電信與網路的結合，讓詐欺犯罪有著更多樣化的工具來實施。從五年來的詐欺類型可得知，投資詐欺、解除分期付款詐欺(ATM)、假網路拍賣、猜猜我是誰及假愛情交友等，皆是依賴電信網路便利性與隱密性而使得詐欺犯罪成功率提升。疫情結束後，電信網路詐欺犯罪相關統計資料一陸攀升至近年來新高，為了解決詐欺橫行之情況，行政院於 2022 年提出之兩年期「新世代打擊詐欺策略行動綱領」，亦稱打詐 1.0 政策。該綱領揭示「識詐」、「堵詐」、「阻詐」及「懲詐」等 4 大面向，橫向整合內政部、國家通訊傳播委員會、金融監督管理委員會、法務部及教育部。期望能夠有效打擊電信網路詐欺與減少詐欺犯罪被害的情況。該綱領以四大面向為主，從宣導教育落實來識詐，透過犯罪預防宣導工作，提升民眾防詐免疫力。接著從電信網路來防堵詐欺，使得犯罪工具難以發揮，毀斷詐欺犯嫌施詐之管道。再來是將贓款金流阻斷，從監管金融到推動防詐減損策略，讓金融與警政合作無間。最後強化偵查打擊量能來嚴懲詐欺，瓦解詐騙集團(行政院，2022)。

四大面向的具體作為相當細緻，識詐主要有兩大策略，分齡分眾主題式反詐宣導與落實金融機構關懷提問、即時攔阻。分齡分眾主題是反詐宣導來說，針對特定族群客製化宣導作為，多元管道將防詐訊息普及於大眾，邀請知名形象好之名人來作為反詐代言人，亦或是配合政府以及各機構大量進行反詐騙相關資訊的皆露，提高民眾反詐意識。更重要的是落實法治教育的執行，透過各級學校的法治教育，建立全民共同防詐的法治素養觀念，從學校的點擴大到家庭的面。金融機構關懷提問亦能及時攔阻被害者金錢的損失，結合警政共同進行及時攔阻策略。第二是堵詐作為，破獲或防堵電信網路，破壞詐欺犯罪工具的施行。包括防杜境外的竄改電話，因為詐騙集團多數透過境外轉接的方式，並竄改號碼來與被害人通話，防杜此類電話相當關鍵；其次是人頭門號的管控，由於人頭門號取得相對容易，又無實名制管控下，成為詐騙集團愛用的工具之一；第三是

惡意與虛假簡訊的攔阻，除了致電與被害人通話外，為了能夠多管道接觸被害目標，電信簡訊成為利器，對於該類簡訊應落實；第四是強化電信業者的資安防護作為，除了要求電信業者加入臺灣電腦網路危機處理暨協調中心之外，對於詐騙網頁的刊登以及涉及的 VPN 業者都應立即反應。

第三是贓款金流阻斷，首先就是人頭帳戶的管制，人頭帳戶是詐騙集團資金流動的主要工具，唯有對人頭帳戶從警示到提醒到預警，降低人頭帳戶對於詐欺的影響。對於新興的第三方支付進行管控，除了洗錢防制法的修訂外，落實第三方支付業者的主動通報義務並對相關虛擬帳號進行嚴格的審核。由於詐騙集團利用虛擬貨幣來進行犯罪利益的實踐，因此對於虛擬通貨平臺及交易相關法律進行修訂刻不容緩。另外小額詐騙的遊戲點數手法也相當氾濫，這方面則是要求實名認證以及納入洗錢防制規範的對象。而一頁式廣告與貨到付款的防制手段，要求業者對於相關付款收費機制的內控管制提高，並完善退款機制。第四為偵查打擊來嚴懲犯罪，首要任務為瓦解電信詐欺集團，加重人頭帳戶犯罪刑度，使工具難以取得，對於犯罪情資的取得管道應強化，提早介入可能犯罪的發生；對於檢警證據取得迅速性應提升，整取辦案的時效。對於偵查手法與辦案的策略精進，提升檢警辦案的專業。跨境詐欺犯罪的查緝能量提升，遏止境外犯罪的可能，檢警查緝打擊市打詐的最後一道防線，推動打擊詐欺的跨部會平臺持續運作。

然而打詐 1.0 綱領的橫空出世，為了讓打擊詐欺犯罪更細緻，2023 年 5 月通過「新世代打擊詐欺策略行動綱領 1.5 版」，增修「打詐五法」，與金融、電信及網路業者合作，從源頭防堵詐騙犯罪，同時加強後端查緝，精進「識詐、堵詐、阻詐、懲詐」4 大面向，達成「減少接觸、減少誤信、減少損害」3 減目標，全面降低詐騙受害事件。在教育宣導層面強調中央結合地方，公私協力合作，實施百工百業宣導措施，並將反詐騙觀念納入法治教育課程，建立防詐知能。第二的電信網路阻斷層面，推動數位信任科技，如建置「111 政府專屬短碼簡訊平臺」，避免民眾被偽冒政府的簡訊詐騙；推動電商業者導入物流隱碼技術、加強資安，確保個資保護與可信任的購物環境。另要求電信業者攔阻偽冒我國號碼之國際詐騙來話，從源頭降低民眾受騙風險，同時對接聽國際來話前

先撥放警示語音，提醒民眾提高警覺。此外，與 Meta 公司建立「綠色通道」下架涉詐廣告，與 LINE 公司研議建置「紅色通道」下架涉詐帳號，也與 Google 公司建立打詐聯繫管道，加速冒名投資廣告下架，從源頭攔阻詐騙資訊流。第三是贓款阻斷，加強金融機構對客戶進行臨櫃關懷提問、強化申請約定轉帳防詐措施、漸進式納管虛擬資產交易平臺業者、就源頭處理網路假投資廣告、遊戲點數防詐鎖卡及內控機制、第三方支付業者建立客戶審查機制，以及金融機構全臺宣導等，更有效攔阻非法詐欺金流。最後是偵查打擊精進，高檢署成立「查緝詐欺及資通犯罪督導中心」，來統合檢警調單位強化打詐量能。對於犯罪所得的查扣、落實罪贓返還及強化犯罪被害人關懷，同時優化境內外虛擬通貨調取、凍結及查扣機制。

然而為了能夠打詐效率的提升，2024 年 11 月 28 日通過打詐綱領 2.0 版，除原有「識詐、堵詐、阻詐、懲詐」4 大面向架構外，新增「防詐」，強化數位經濟產業治理，並以「運用 AI 防制、深化跨境合作、監管防詐產業、加強被害保護」為規劃亮點，希望達成「強化防詐意識、減少發生數、降低財損數」3 大目標，為國人打造更安全的生活環境。教育宣導的識詐應該更扎根，建立青少年正確法治觀念，加深部會合作，並結合民間團體以分齡、主題式宣導反詐、識詐；落實金融機構關懷提問，並及時攔阻。第二是電信網路的防堵，詐欺犯罪案件的激增，督導電信事業介接指定資料庫輔助核對用戶身分，限制或拒絕高風險用戶申辦電信服務，降低詐騙集團獲取人頭門號之可能；建立非本國籍預付卡用戶查詢流程，對已出境或逾期停留的用戶落實認識客戶風險管理機制（Know your customer, KYC），並於必要時停斷話，避免遭轉售不法使用；與刑事警察局 165 專線建立聯防機制，用戶被通報涉詐達一定次數即列為高風險用戶，限制其門號申辦；強化商業簡訊檢查，帶有網址連結須事前檢查及登錄。

防詐（數位經濟面）精進措施：「強化網路廣告平臺業者之實名認證」，要求業者應驗證委託刊播者及出資者之身分，並於廣告中揭露；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 5 千至 1 萬筆網路廣告，藉由公私協力機制，自動化通報加速下架作業；建置「第三方支付服務業虛擬帳號查詢

平臺」，協助檢警調單位更快速查找虛擬帳號所屬第三方支付業者，加速圈存受詐款項，降低民眾損失。阻詐（贓款流向面) 精進措施：跨機構合作，並運用 AI 科技防詐執行打詐行動，如推動建置「疑涉詐騙境內金融帳戶預警機制」，防制人頭帳戶詐騙、督導發卡機構加強信用卡交易監控機制，防制信用卡詐騙、推動虛擬資產服務提供商（VASP）相關阻詐規範及 VASP 業者自律管理、加強防制貨到付款詐騙等。懲詐（偵查打擊面）精進措施：深化公私合作，擴大追查詐欺相關共犯，並增加查緝比例；強化詐欺犯罪被害人保護，並擴大犯罪利得沒收，提高罪贓返還，有效填補被害人損害；增強執法人員及社會大眾對犯罪被害人保護規範認知，並提升民眾識詐防禦；提供被害人諮詢轉介服務、減輕民事訴訟負擔；推動國際合作管道，遏止境外犯罪。

從上述的三階段打詐綱領的演進，從教育宣導、電信防堵、金融阻斷、數位防止以及懲戒矯治等面向，我國政府相關單位不斷地從詐欺犯罪的過程、犯罪手法、犯罪工具、從被害到加害，做出相當完整的分析與建議。行政院設立打擊詐欺指揮中心，從政策及執行策略的制定，跨部會的機構單位進行整合與協調，內政部負責教育宣導的識詐工作，通傳會主導電信網路的止堵作為，數發部則針對新興數位經濟的相關作為，金管會則統管贓款金流的及時阻止與掌握流向，最後由法務部主則偵查打擊詐欺犯罪的相關策略方向。以這樣的政策思維來看，我國打擊詐欺犯罪的綱領架構相當完整，從法律面到實際執行面都有明確的指引。然而從 2022 年到 2025 年，案件量趨勢不斷增加，短短三年的時間，我國的打擊詐欺政策亦隨之進行調整，為了能夠降低詐欺犯罪率，我國透過修訂法律作為政策執行的依據，從打詐五法的修訂後，隔年為了全方面打詐，更推動打詐新四法的制定，除了加大嚇阻力道之外，更注重被害人保護與賠償的部分，也根據實務經驗來修法給予偵查作為的法律依據，企圖讓犯罪人無所遁形。然而打詐綱領與專法的訂定，雖然收到不少的成效，然而會短時間內進行修訂，顯然是詐欺犯罪的手法不斷更新，利用我國法律上的不完備部份去遂行詐欺行為，使得整體詐欺犯罪數量不斷增加，不僅危害國人的法益，更使得人民對我國法律與打詐的信心逐漸崩塌，對社會造成極大的動盪，對於我國打擊詐欺的政策實務困境，必須解構並且一一克服。

第二節 我國打擊電信網路詐欺實務之現況與困境

本研究對八位從事打擊電信網路詐欺犯罪的專業人員進行訪談，對於我國在打擊電信網路詐欺犯罪的實務面與困境進行說明

一、具體執行層面

(一) 國內電信網路詐欺犯罪現況

目前國內詐欺犯罪的主要類型仍以電信網路為主，絕大多數都是透過電信公司發送簡訊的方式來鎖定可能的犯罪目標。然而目前電信與網路的結合，目前民眾多數利用行動手機來上網，而網路的提供則是透過電信公司，因此電信網路詐欺可說是整體犯罪型態，難以將其分類為電信或是網路。由於目前手機為現代人必備的移動工具，且網路與電信的結合，過往手機單純使用的通話功能之外，增加了簡訊、上網、繳費、支付等功能，使得人們對於手機的用使愈加依賴，已經到了不可或缺的地步。而電信網路詐欺集團亦利用人們依賴手機的生活習慣，透過網路與電信的功能，藉由社群媒體為媒介，大量傳送虛假廣告、投資訊息來吸引被害人進入其設計好的圈套。

> *電信詐欺不外乎就是簡訊，...退費的簡訊詐欺，那還有猜猜我是誰的電信詐欺、打電話的電信詐欺(A01-014)。從網路，目前詐騙集團會使用 Facebook、Instagram 或 Threads 等社群媒體，藉由廣告吸引被害人，使其認為好像真的有這回事(A01-029)。*
>
> *透過電信網路、簡訊，或者是投虛假廣告，讓一般的人接觸到投資的相關訊息(A02-112)。*
>
> *大部分都已經從網路開始了(A03-443)。*
>
> *百分之九十以上的詐欺都是透過電信或網路來接觸被害人(A06-927)。*
>
> *目前的話，刑案來講，詐欺大概可能佔到 6、7 成，甚至 7、8 成(A08-012)。*
>
> *「電信詐欺」這種...可能就佔到將近 6、7 成甚至更高比例的案件數，所以他的量是很多的(A08-029)。*

整體受理報案的流程多為被害者到警局報案後，受理後將相關卷證交至業管單位進行後續程序，然時常因為人力員額的不足而必須選擇案件嚴重程度與否來展開下一步偵查作為，難以每件案件都能盡力去完成，讓基層員警心有餘而力不足。另外就是檢察官提出自訴或告發的方式，多半是發掘原本案件中有其他可以的線索以及相關犯罪資訊。第三種則是透過 165 全民防詐平臺的資料，先進行大數據分析之後，發現有偵查的線索便開始指揮警政單位進行偵辦。不過要透過偵查人員主動辦案的機會相對來講較少，主要還是因為目前人力的吃緊，原本的案件量已經難以負荷，第一線人員無暇再去進行所謂的另案偵查。

基本上第一線受理單位絕對是派出所，民眾遭詐騙也是到派出所報案，那他會將這個卷再交給業管單位(A01-016)。第二種是來自於檢方的部分，……地檢署檢察官發指揮書由警察機關做一些偵辦(A01-049)。第三種就是您剛剛所說的 165 的部分，所謂的透過 165 是說他會去分析資料，以大數據做分析(A01-054)。

有時候是我自己去洗 165。或我們那邊也是有人會來報案啊。分局一定有抓到犯嫌，所以我們要在拓展上去，基本就可以成案(A04-212)。

(二) 常見的詐騙類型

現在主流是什麼大家都知道—投資詐騙(A06-067)。

目前電信網路詐欺案件最常見的類型就是假投資詐欺，過去假檢警的詐欺案件類型目前減少中，除了我國大力的宣導之外，由於假檢警所利用的腳本多半雷同，而假投資的案件則可利用一般民眾對於投資理財與高獲利的誘因，除了較容易吸引被害人上鉤外，主要還是因為犯罪金額相當龐大，使得多數電信網路詐欺犯罪集團傾向於假投資詐欺的犯罪腳本。由於假投資需要大量資金，因此工程師與中產階級成為目標，對於年輕族群則鎖定網路購物、解除分期等手法來遂行詐欺犯罪。

實務上最多的就是假投資，...假投資不外乎就是虛擬貨幣，虛擬貨幣的假

投資是最多的(A01-024)。網路上的還有假購物。IG 則因為知道是年輕人會使用的 (A01-044)。

最常見的是假投資。然後最近有遇到假檢警的案子(A02-018)。

剛去刑事局，我是辦那個點數詐騙...猜猜我是誰...105、106，開始大量的三階段的假檢警。投資詐欺，109 年比較風行(A03-085)。

一個是「解除分期付款」，然後另外一個就是「假網拍」，「假網拍」詐騙現在也很多，然後第三個就是之前學長講的那個「假投資」(A05-071)。

2018 年以前齁，其實詐騙集團就像一個公司在經營，...，詐欺集團成員就是像公司一樣是販售商品的，那 2018 年他們主要販售的商品是販售恐懼，就是像假檢察官、假檢警，不然就是像跟你說你涉案了，你在網路上買東西，你誤設了分期付款，所以你的錢會一直扣，叫你趕快去操作 ATM，他就是販售你那種恐懼感(A06-059)。

除了被詐騙集團騙取金錢之外，目前對於人頭帳戶來取得不易的情況之下，許多詐騙集團開始透過不同手法來取得人頭帳戶，利用求職廣告、網路購物等手法來騙取他人的帳戶，利用三方或者多種手法來遂行詐欺犯罪，使得受害者除了被詐欺金錢之外，連銀行帳戶都被拿來當作是詐欺犯罪的工具。

找家庭代工就誤信詐騙集團的要買材料所以要先將金融帳戶給我，那就吸引民眾去誤信...。第二種...被騙帳戶的年輕人是中獎，假中獎的也會變你的帳戶。(A01-460)。網路上要求職，後被詐騙集團說是做一份專員的工作，就是去幫我們公司收款，可是他不知道這個款項是詐欺被害款項(A01-482)。

即便是老調重彈的假愛情交友的詐騙手法，仍會有許多人憧憬建立起親密關係，陷入關係中而不自拔，整個詐騙過程最後仍會導向投資取向的行為，以擘劃兩人共同生活的未來為藉口，使得身陷其中的被害者拿出更多的積蓄進行投資，致使詐團獲取更多的犯罪所得。

你都已經六十幾歲，怎麼還會被男女之間的感情問題騙呢(A01-614)？

假愛情交友。但是以這個名目之後，再把你拐騙進去做投資(A02-122)。

現在的現況，就是假投資的詐騙跟戀愛的詐騙(A02-073)。

現在都下 APP 廣告、Instagram 廣告，說名人教你投資。因為看起來目前詐騙案件量最多的，比如說假買家騙賣家，或者是假投資詐騙，還有猜猜我是誰，或者是假愛情交友...可是我相信，因為我看很多案件，假愛情交友回過頭來，還是回過頭來騙他去投資(A03-528)。

網路是人們目前高度依賴的工具，而人們目前多數也透過網路進行購物，除了便利性之外，能夠在手機上完成所有購物的動作，因此網路購物詐騙也成為目前電信網路詐欺的主流形式之一。包括點數購買、一頁式廣告、解除分期付款等詐騙劇本，大量充斥在網路世界中。然而畢竟網路購物屬於小額詐騙，目前也有透過假投資詐騙所衍伸出的台版地面師[151]詐騙，也是透過對於地產專業所遂行的詐欺新型態，使得被害者血本無歸，連基本的棲身之所都無法保住。

網路購物的時候，只要是一頁式的廣告（被騙的都是一頁式的廣告）(A01-234)。

這種網站非常多。因為會公告說哪些網站被封鎖，看每次都是幾十個、幾百個這樣子(A02-745)。

網路購物，還有一個解除分期付款的(A03-649)。

[151] 犯罪集團以久未辦理繼承登記的房產為案源，「偽造遺囑」將獨居長者的遺產，以「遺贈」的方式移轉給沒有親屬關係的詐騙分子，另外一種是「先以假投資名義詐騙現金」再「誘騙抵押房產貸款」，讓受害人繼續投入資金，最後受害人甚至因為還不出貸款「房產被拍賣」而「財屋兩失」的詐騙型態。資料來源：台北市政府地政局，臺版地面師破案關鍵首映 終結假遺囑詐孤獨死房產的遺憾，網址：https://land.gov.taipei/News_Content.aspx?n=0ABE9F8A3E5B75C2&sms=72544237BBE4C5F6&s=43363DB5C4343F7B 最後瀏覽 日期：2025 年 8 月 13 日。

點數詐騙。就是猜猜我是誰(A03-020)。投資詐欺，虛擬貨幣...最近我辦的那一件是，那個假代書，就是地面師(A03-085)。

假投資。假冒檢察官的吧？少。也有 ATM 分期付款，假網購那個還是有(A04-139)。

電信網路詐欺的盛行，與人頭帳戶的氾濫相關，由於人頭帳號也是詐團的金流工具之一，自然成為重要的標的。隨著目前我國對於人頭帳戶警式的落實，使得詐團取得人頭帳戶愈發困難，人頭帳戶收購價格大幅增長，逼得詐團開始用詐欺手法來騙取人頭帳戶，包括求職廣告、投資詐欺等手法取得，然而由於常常出現黑吃黑的狀況，使得詐騙集團開始控制人頭帳戶提供者,集中監禁的方式來管理,逼迫人頭帳戶提供者聽命行事。

找家庭代工就誤信詐騙集團的要買材料所以要先將金融帳戶給我，那就吸引民眾去誤信，這一種的人頭帳戶滿高的，現在移送都是這樣比較高。第二種你說以男性的話，假投資也會被騙帳戶(A01-460)。

超商店到店的方式，把自己的帳戶、印章都寄出去(A02-030)。

因為他偷偷把錢領走...為什麼之前發生豬仔，被拖去打就是因為你匯進來我偷走(A03-708)。

「辦門號換現金」誘使一些民眾...辦門號以後，...他們可能會找詐騙集團做銷售的管道(A05-038)。

這些人不聽話了，集中在一起，...進去之後我們發現這些都失蹤人口、警示帳戶，怎麼會這樣？所以就跟詐團有關，所以進去之後我們把八個人羈押之後(A06-187)。

(三) 詐團運作模式

1. 擬真變化劇本單一目標

這些電信網路詐欺犯罪有一套模式運作，許多都是要透過加入群組來進行假投資劇本，利用各種不同的角色與話術，讓被害者相信投資真的能夠賺取大量的收益，除此之外還建構擬真的 APP 手機軟體，投資收益的相關網頁都是詐騙集團委託工程師所設計，初期會了取得被害者的信任，對於投資收益都如實兌換，待被害者信任程度高的時候，利用各種話術讓被害者投入及大量的資金。第二種常見的就是假檢警的詐欺劇本，透過一般民眾對於涉入刑事司法系統的恐懼，透露自己帳戶以及各種資訊，最後將自己帳戶內的所得全數交出。不管使用何種的劇本進行詐騙，全部只有一個目標，就是讓被害者遵照詐團所預先設計好的劇本，一步一步地將金錢轉匯或交付給詐騙集團。

被害人今天在 Facebook 看到一個廣告，其顯示著穩賺不賠等話術，下面就會有個 LINE ID 請你加入，而會有詐騙集團的理財專員介紹目前有哪些投資項目，且要請你來參加。民眾就會被他們 SOP 的話術吸引，就會和其約定地點見面去簽一些投資的合約、契約或憑證(A01-030)。

假投資的 APP，他們要操作入金。一定會有現金要買幣的這個階段。通常我們在買幣的人會用比如說「幣安」比較有名的交易平台嘛。但是這個就牽扯到匯款的部分，那現在詐騙集團很聰明，他們用現金，現金就比較難追。他們叫被害人帶現金去實體門市買幣。然後員工就會教他們操作然後用他們專屬的另外一個錢包(A01-129)。

透過電信網路、簡訊，或者是投虛假廣告，讓一般的人接觸到投資的相關訊息。然後可能就把你拉進去某個 LINE 群組，或者 LINE 群組就開始說，我們去買什麼東西、或是買什麼標的物就可以大賺。那後來你可能有興趣之後，他就會可能引導你去下載可能是某個虛擬貨幣的電子錢包，然後就讓你跳進去之後，他自己本身會有個虛假網頁，可能就說你看你又賺了大概 20%、30%，甚至 100%、200%。當你要提領的時候，你會發現你提不出來，你可能要再加保證金，丟出去之後他可能用更多更多的藉口以致你提不出來。那等到你真的丟了一筆很大筆之後，他就可能踢出群組，你才

驚覺你受騙(A02-112)。

一開始是警察、檢察官，一樣前面老套路...阿嬤已經被騙了，一年半了。...那沒關係，我找一個理財公司給你...兩間房...那不然這樣子拿去抵押。阿嬤收到錢之後 10 分鐘，車手就把他的錢全部款走(A03-116)。

假檢警的話，說實在，他是利用民眾對於法律知識不足，一般民眾你突然跟我說你涉嫌什麼案件...假投資、假交友，詐騙集團就是利用人性的貪婪。...再給你騙一次。有的又把帳戶簿子交過去，到最後又變成詐騙集團共犯(A04-158)。

失去戒心的方式你知道是什麼嗎？有獲利...就是這種假出金...你要 10 萬給你 10 萬，甚至 50 萬他覺得你是個大魚他 50 萬都給你(A06-104)。

投資詐騙，投資詐騙現在最壞的他不只把你的錢騙光，還甚至把你的錢，你沒錢把你的房子抵押，抵押沒還錢幫你拍賣，拍賣完之後錢再拿走，你身無分文(A06-135)。

2. 多模手法的金流

處理金流的模式使用多種手法，除了能夠確保犯罪所得不被一網打盡之外，更重要的可以拖延檢警辦案的速度。詐騙集團常見的方式包括傳統的面交付款、臨櫃轉匯、分層打散、虛擬貨幣或第三方支付等手法，將被害人的金錢轉匯到國外或者是其他帳戶，刻意製造多層次的金流，就是為了躲避查緝與製造偵查斷點，使得犯罪所得極大化。目前較難查緝的都是使用虛擬貨幣，利用虛擬貨幣去中心化的特性來進行，加上可在國際間流通的特性，更是詐騙集團的最愛。

實務上最多的就是假投資，...，假投資不外乎就是虛擬貨幣，虛擬貨幣的假投資是最多的。我現在有分到一件詐欺的案件，被害人是個護理師，是直接騙到醫院裡的候診間跟所謂「假投資公司的專員」進行面交，做付款

的動作(A01-025)。

超過五千萬財損的案件，其實大概有三千萬以上是匯到海外帳戶，就是用外匯的方式(A02-223)。分了非常多條，就是外匯的、進去交易所的、車手臨櫃提領或 ATM 提領的(A02-274)。

被害人...點進去的時候，他就在他的後門放一個木馬，然後詐騙集團就是就會操控說用他的手機去買點數。用電信費小額付費，扣在月底的帳單裡面(A03-021)。遊戲點數買了之後，...先存到遊戲的角色裡面，這角色買了一些現實的裝備之後，再很低的價格換現金出來 (A03-033)。

他要繳保證金，那這個就是走實體金流的部分。這個車手拿到錢之後，他繳回去走金流就會走到虛擬貨幣...找個人幣商，不領錢了我直接找人換幣。最後還會歸集到一個大水庫裡面，...最後會集中到某兩個、三個(A03-582)。

現在詐騙集團的手法真是很多元，而且現在大部分都走虛擬貨幣。現在詐騙集團自己都在國外成立公司了。你在馬來西亞、柬埔寨，他們自己成立虛擬貨幣的公司。...我就再洗回去打回臺灣(A04-038)。

一種是他自己以為他這個錢包是他自己的，其實他從頭到尾都沒有這個錢包的控制權，只是他就是被洗腦，那這種詐騙集團就可以自己轉。另外一種就是這個錢包確實是他的，假如說這個 A 錢包地址是被害人的，他轉到詐騙集團的 B 錢包地址後，詐騙集團他可以再洗出 C、D、E 地址。對，因為那些不一定要跟交易所申請(A05-140)。

跟幣商接觸以後...他們就是車手嘛，他們接觸以後會把這些錢透過水商，然後把他轉出去(A05-142)。

先把它設約定轉帳，因為他要很快，所以他第一層帳戶之後，第二層、第三層就轉外面去...到國外的虛擬貨幣，去境外的虛擬交易所(A06-279)。

更多時候利用複合式的洗錢手段來進行犯罪所得的實現，將虛擬貨幣轉入國外的交易平台，或者現今轉入其他金融商品，像是線上博弈公司來洗錢，買入其他投資商品像是期貨、黃金等，都是犯罪所得實踐的手法。財力雄厚的集團，更是自己成立外國公司，設立專屬的虛擬貨幣交易平台，以正當行業掩護非法犯罪

第一個被騙的人基本上虛擬貨幣，也不怎麼熟識。第二個，他們有時候這些人用的平台，不是我們一般看的幣安，是你找不到，就是可能國外的那種(A03-563)。

詐騙集團自己都在國外成立公司了。你在馬來西亞、柬埔寨，他們自己成立虛擬貨幣的公司(A04-041)。

現在虛擬貨幣的幣商，我們講說你要經過實名制要申請。可是很多地方，他私底下本身就是詐騙集團在做(A05-444)。

如果你錢是犯罪的當然大部分是詐欺，也有很多是博弈，甚至是其他期貨，都有(A06-1028)。

面交要怎麼弄？還有人直接給三公斤黃金(A07-367)。

3. 多層斷點的設立

詐欺犯罪之所以難以查獲，除了集團是以科技為主的犯罪手法，透過電信網路來接觸潛在的被害者，利用電信網路的便捷性來縮短時間，加上網路有隱匿性，不需要面對面的接觸之外，更利用電信網路的便捷性來遂行犯罪所得。在如此繁複的犯罪過程當中，稍有不慎便會讓檢警調單位查獲並獲得判刑的證據，因此斷點的設立則成為電信網路詐欺犯罪集團首要考量。詐欺犯罪集團的斷點可設立在犯罪人、金流、電信網路等層面。以人來說，集團多數以車手為斷點，因此提款車手多數不知道集團有誰、誰為主使者，使得檢警難以向上追查。以金流來說，多層次的帳戶轉匯至國外已經難以查緝，現今第三方支付虛擬帳戶、虛擬貨幣等電子錢包，由於去中心化加上早期不須匿名，成為詐騙

集團愛用的金融工具,即便現在個人幣商的實名制,難以將金流與被害及犯罪進行連結,根本無法溯源以及證明，此舉也使得基層提款車手成為主要的判刑對象。

這種情況下我們通常會發文去跟他要資料。可是阿福錢包的系統是不會回任何回應的。所以就會變成形成一個幣流追查的斷點(A02-148)。還是有很多斷點可以用。用人頭的資料去申請就好啦(A02-583)。他會把錢丟在公園的公共廁所，然後再聯絡的人是另外一個控台，比如說用 Telegram 的一個控台。然後控台再交代另外一組人，去那個廁所拿現金(A02-665)。司法互助;像金流面也是這樣...黑莓卡的話,現在就變成不知道是誰在用的。(A02-806)。

車手的斷點它會層層...最高級的車手頭，總要有一個對水房。...只有這個人可以跟大家對(A03-728)。水房可以查得到，但是金主就會比較難。因為他們這個點就是轉手，就是斷點(A03-746)。水房斷點他可以做很多加水，他不一定只做一條詐騙集團的水。他可以做毒品的、也可以做賭博的(A03-756)。

大部分小盤提領還是有。但是他們到最後大盤,他們絕對都是打虛擬貨幣。你其實都沒辦法的(A04-053)。你要連結到犯罪事證，你找不到集團上游...斷點真的是太多了。通訊軟體講實在沒有解決的話，單靠手機鑑識，我覺得效用不高(A04-407)。

還有一些錢包連交易所都不是，所以也都調不到資料(A05-160)。目前是比較困難。國外的帳戶就...(A05-191) 可能匯到四、五層，才叫第五層車手去領出來(A05-530)...我們的工具跟不上詐騙集團，因為他們大概都是用那個飛機 Telegram(A05-738)。

主嫌永遠不會出現，出現在控房裡的永遠都是頂多到中層的而已，你下層那種小的部分,其實之前應該有成少共犯的問題,這個其實也有成少共犯,

很多都是用少年(A06-267)。他有人的斷點、錢的斷點、有資訊的斷點，完全沒辦法追(A06-270)。查到交易所，如果幣流的話你要怎麼找？查到交易所你就要停了(A06-283)。三方當然說，金融他有他的便利性，你把它當作非法用途就會變成斷點(A06-1043)。

他們就已經設好斷點了，他們就是透過這些小弟來幫他拿錢，有拿到錢就有講的，那就大家一起分；沒拿到錢，那就是你倒楣被抓。但是你也找不到我(A08-265)。

另外電信網路的斷點更是難以查緝，除了許多人頭帳號的 sim 卡之外，許多機房設在境外，利用我國國際的特殊地位，缺乏司法互助情況下，甚至透過 VPN 的轉接，讓電信網路的回溯追查更是困難，即使有明確的犯罪跡證，缺乏國際間的司法互助，使得詐騙集團更容易設立電信機房的查緝斷點。對於國內機房的查緝更是困難，由於境內的機房不會對國人進行詐欺，因此很難從被害人的報案資訊中知悉境內機房的資訊。即便當場查獲，證據的保存與調閱亦成為另外的斷點，各種不同的分工合作與集團間的聯繫，使用網路電話更難以監聽與追蹤，即便擁有多項偵辦技巧與工具，對於上述的斷點突破，仍具有相當程度的挑戰。

詐欺集團尤其是機房他會一直在移動(A01-164)。

從被害人這邊，找到的頂多車手或水房層次，沒辦法到機房層次(A02-455)。

機房設國外騙台灣人，機房設國內騙大陸人，或是設美國或其他地方，不是騙台灣就是大陸人這樣(A03-065)。

轉接的地方完全沒辦法。機房講實在，架設國外多，臺灣也有(A04-094)。

現在機房他們都設在國外的(A05-578)。我們現在實務上在 Telegram 這一塊，就是飛機這一塊，可能是卡住的，講白的是卡住的(A05-786)。

機房就是他的廠房，他就是設在境外(A06-131)。從來沒有出現過，中層幹

部只有電話聯絡過，而且電話是什麼？Telegram(A06-450)。跨境是個非常大的困境，各國都一樣，因為機房水房...(A06-875) 。

我至少兩三件卡達的。就說招待你去玩，到那邊就把你的手機收了，逼你要打電話，事實上有點像半奴隸啦...我覺得還是證明的問題(A07-090)。

由於車手的置換率高，加上國內對於車手違法的教育宣導落實，使得詐騙集團開始尋覓境外車手，透過境外徵求車手到國內旅遊，短期的提領成為查緝的斷點，不但能夠取代國內少子化的少年車手問題，更使得有源源不絕的車手可使用。更多時候利用人性想賺錢的念頭，開始鼓勵中老年人來擔任取款車手，避免讓被害者起疑。

有一個是外籍車手，有三位是本土台灣籍車手(A01-142)。

我們之前有大陸遣返的，就是在東南亞車手(A03-1037)。

現在車手年齡有趨向老年化，然後有外國籍(A04-330)。

最近那個境外車手很猖狂(A05-610)。

他要去吸收年輕人也有風險，那乾脆吸收外國人嘛。就是你那個東南亞的外籍人士，你就來台灣旅遊嘛，兩三天嘛，兩三天兼打工嘛。沒抓到，就算有賺到，就撈一筆回去。有抓到，了不起就車手嘛，就幾個月易科罰金判一判，反正你就不要把上手供出來，你就講說你不知情(A08-216)。

4. 分工細緻的企業化經營

電信網路詐欺犯罪需要機房、水房與車手等成員共同完成，不同的工作有不同的集團負責，機房負責第一線接觸潛在被害人，並透過不同劇本跟被害人接觸，以詐術讓被害人身陷其中而不懷疑，聽信其言而將自己的金錢匯入或面交；其次由水房透過各種地下匯兌、線上金融、衍生商品等手法來洗錢，配合車手集團的提領或者再度回水的方式，讓被害人的財產在瞬間遭到移轉。也因如此細膩的犯罪手法，使得整體詐欺犯罪過程細節化與分工化，為了能夠明確分工，各司其職且專責，又難以一窺全貌，同時間也將犯

罪責任平均化，難以將整個詐欺犯罪歸咎於一人，以工作分工的角度來看，沒有一定的橫向與垂直聯繫，是難以完成整個電信網路詐欺犯罪，整體來說是以企業化角度來經營電信網路詐欺犯罪。

詐欺集團就知道你現在面臨的是一個很有組織、很會跨國經營的跨國企業，我們面對的是這樣子的產業(A06-132)。我都覺得這個背後有幕後集團的可能性很高(A06-693)。

一個集團這麼多人，每個角色所負責的工作不一樣(A07-312)。

他們現在分得很負責，他們現在已經不是像以前一團包到底，他們現在已經...他們現在有些時候是分層，中間這一層發包給你，然後你又發包給誰，就是你可以想像成他就是一個企業，然後就是他已經是一個系統化的經營(A08-284)。

那這些東西，他所產生的後果可不可以全部歸罪於原本的源頭，這邊就會有問題，所以這就是為什麼到後來會變得很亂的原因。所以很多時候當事人來他會說：「法官，我這邊就不知道，因為我就做到這邊啊」「啊這邊我就不知道，因為這邊我就沒有參與啊，他那邊給誰他也不知道去...」，到底是推給業者？還是說真的不知情？就有很大的空間在(A08-296)。

二、政策制度面

政府的投資跟詐騙集團的投資真的差很多。詐騙集團如果敢，工程師、幣商、律師都可以給費用，就這樣子啊。可是問題就是我們政府資源到底投在哪裡，像數發部、NCC、金管會，給他們那麼多錢，相較於警察，一個165是自己成立的APP，點閱率多少，你們那點閱率多少，實際上到底有沒有幫助到民眾，講實在，大家都要錢，但警察做的事最多(A04-273)。

政府針對打擊詐欺犯罪不遺餘力，推行的政策與具體作為更是所有民眾的期許。然

而一個政策的制定到執行，除了相關法律的訂定之外，機構之間的責任與義務，具體作為的落實，經費的撥補與使用等，都是一個政策是否能成功的關鍵。打詐綱領三年來歷經三個版本的修訂，目的就是為了澆熄猖獗的電信網路詐欺犯罪之火焰，根據這三年來的統計資料顯示，這把罪惡之火似乎沒有停熄的跡象，更有不斷向上延燒的情況，顯然在政策綱領上仍有改進的空間。從識詐、堵詐、防詐、阻詐與懲詐五個面向來探討，在政策思維與實務運行上的困境，作為後續政策作為的修正依據。

(一)　教育宣導不夠精準

目前我國對於打擊電信網路詐欺犯罪的教育宣導面來說，多數從學校與網路影片宣導為主，實務上對於教育宣導的手段相當多元，從分齡製作、因地制宜到多元管道的接觸，其立意良善且將宣導網絡擴大到民眾一般會接觸到的場域。內政部拍攝影片與動畫，辦理大型宣導活動，法務部要求檢警下鄉宣導，教育部則深入家庭，經濟部要求轄下國營事業體亦強化宣導，更督促交通部在國家各種交通運輸上大力宣導防詐意識等，各部會能夠共同進行防詐識詐的資訊廣傳。其實面向上相當廣泛，應可擴及到士農工商各層面。警政單位推動小蜜蜂的鄰里街坊廣告車下鄉宣導，結合校園宣導毒品與詐欺等，其實都有按照打詐綱領需求去運作，然而針對網路重度使用者來說，其接觸到的機會相對較多，但對於中老年人這群網路輕度使用者卻成效有限，顯然分齡的宣導仍有一段距離。

> *積極推動了一個叫小蜜蜂，...類似我們的廣告車的概念，會每個月編排固定的場次在鄰里街坊道路去做一個廣告宣導 (A01-210)。到校園去宣導毒品跟詐欺，因為我接近的都是國中跟高中(A01-216)。到成功嶺向新兵役男宣導什麼是詐騙，跟役男們識詐，詐騙要先認識之後才能夠去阻詐，避免你去匯款或提供帳戶(A01-221)。*

> *宣傳詐騙手法這一塊，我覺得不管是政府或刑事局都已經花很多力氣了。有時候車上聽電台常常都在講這個。刑事局還有編一個預算是演八點檔，然後來告訴這些中老年人詐騙的手法。我覺得在這一塊上已經花了很多力*

氣。剩下就是可能家人間互相提醒，就是不看電視的人(A01-507)。

去宣導說，我們有做，不是都沒有做。只是在交給上面說：「我們有去做犯罪預防宣導喔(A04-325)。」

然而從詐騙財損不斷增加，發現中高年的受害者急遽增加，除了本身具有一定經濟基礎之外，多數高齡者對於網路的影音與資訊接觸較少，容易成為詐騙集團鎖定的對象，而對於中高齡的國民宣導手段，目前國內多數還是以影片與動畫為主，而網路上的相關教育宣導似乎仍然難以深入中高齡國人的生活圈，才使得目前中高齡的受害者急遽增加。另外就是教育宣導力道幾近疲乏，當文字圖片訊息千篇一律時，很多時候雖然宣導當中有重要訊息，卻因為接收疲乏而快速帶過，不僅僅是國人對於相關訊息的疲乏，基層員警與機構的宣導手段若是千篇一律，將導致執行過程不確實。

我收集到大概 200 多個被害人的資料，大概都落在 50 歲以上，而且都是第一次買虛擬貨幣的人。因為不懂所以省事請人家辦，沒有去大平台(A02-514)。

因為我們花很多力氣，去做宣傳、掛紅布條，可是大家就看看而已沒有感覺(A02-525)。

鄉下的地方，有些阿嬤說，她一輩子沒離開過屏東，你叫她去看這個文宣，或看這個影片，她可能，吸收度也沒有這麼好(A03-480)。

某一些特定的族群他其實是不太會接觸到的(A05-354)。

有沒有辦法徹底的去落實？這可能是一個問號。宣導不是掛幾個海報就叫宣導，不是找幾個警察去校園宣講就叫宣導，那是沒有用的。每天手機打開翻天覆地的照片訊息，他的量已經蓋過你正面宣導的東西了，所以你的正面宣導的東西，如果說沒有足夠強大到讓民眾能夠深刻的記在腦海裡面的話，那個宣導其實意義是零(A08-052)。

更明顯的可以從被害者的反應可得知教育宣導仍須改進之處。第一線阻詐的金融機構櫃檯人員或者是警政人員苦口婆心的規勸，遭到被害者的咆哮、生氣以對，顯然被害者深陷其中而不自知，對於詐騙手法與真實情況難以識別。尤其是假投資的被害者，幾乎要把身家財產都拱手給詐騙集團，仍對於自己的投資眼光有信心。

案子剛開始報案的有幾個人？只有 7 個人，完全不知道自己被騙，這才是問題所在(A06-521)。

這個被騙的時間很長，因為你可能先觀察嘛，失去警戒然後再匯錢給你，跟你建立關係，然後你還一直不相信被騙，我們發現警察打給你他還不相信，他還一直匯款然後匯款，之後後面沒辦法才來報案(A06-686)。

假投資的被害人是不是要有一點...股票應該去證券交易所(A07-376)。

你政府沒有大力的去宣導的話，民眾就真的誤信為真，再加上現在很多 AI 造假的東西，真真假假真真，到底是真是假也沒有人知道，你政府也不宣導。那這種東西你說民眾要怎麼去辨別(A08-086)？

教育宣導如同教育一樣重要，教育是百年大計，短時間要有成效相當困難，更難以用量化數據來呈現教育宣導的效能，唯有積極投入，如同新冠肺炎時的防疫作戰精神，讓每個人都時刻注意相關詐騙手法與資訊，方能收到成效。而且政府更應持續以最新數據與資訊來進行宣導，而非將過往的犯罪手法一而再再而三地重複宣導，必須能夠跟上詐騙集團手法更新的速度，才能突破詐騙集團的伎倆。

教育的東西他不願意投入那麼多，因為這種東西他無法及時呈現出來，所以他沒有辦法做出來這種成效的時候，大家當然就不願意去做這種吃力不討好的事情(A08-063)。

（二） 金融機構的阻詐

1. 金警合作

金融機構是詐騙集團犯罪所得實踐的媒介，為了能夠及時將被害人款項阻止轉出，我國對於金融的相關管制作為相當多。然而金融機構多數畢竟為私人企業，企業以營利為目的，若沒有明確的犯罪事實，只能視為一般的金融動作而難以阻止，此時端賴金融機構人員與警方的合作阻詐介入。對於金融從業人員的識詐敏感度提升以及金融與警政的連線，從固定巡邏到緊急到場關懷等都是基本且必要作為，此外更需要雙邊的緊密合作，包括警政通報疑似人頭帳戶是否能夠及時阻詐，金融機構對於可疑交易的即時通報警政等，都是打擊詐騙中阻止金流匯出的重要關鍵，我國七八月成功阻詐約 25 億元[152]，攔阻金額相當龐大，這也顯示我國在投入阻詐的部分相當積極。然而對比整體被詐騙金額來看，七月份為 85 億 4,100.4 萬元，八月份為 73 億 4,866.9 萬元，雖然成功攔阻，但仍有多數人辛苦財產被詐騙集團成功詐欺得逞。

金融機構阻詐是警政署目前著重阻詐的部分，我們每天都會接收到金融從業人員成功的案例，但很不幸地也是有失敗的案例，...從業人員的敏感度 (A01-248)。

我們在阻詐、識詐跟銀行或農會這一部分都有建立所謂的平台，而且之前在彰化開始就有所謂的金勤區，那台中現在也有金勤區，由派出所專責人員負責，可能一個人負責五、六間的金融機構，就是要看派出所有幾間金融機構去做區分(A01-270)。

我想金融面，就是可疑交易，就是可疑交易這個東西是，可以先讓就是偵查單位先知道的。然後再來就是剛剛講的門市是不是可以先通報我們哪些人的電話是有問題的？這些東西，好像目前都沒有特別的窗口。像我們要調可疑交易，也是知道這個是有問題的帳戶，前面有一個犯罪事實之後才會去透過我們的窗口去調。他們沒有辦法主動告訴我們(A02-866)。

警察其實人也沒有這麼多，如果銀行行員發現怪怪的，打電話請警察來，外面

[152] 打詐儀錶板，打詐成效攔阻金額。資料來源：內政部警政署，網址：https://165dashboard.tw/ 最後瀏覽 日期：2025 年 9 月 10 日。

巡邏線的...反正金融機構也要巡簽(A03-477)。

一定都是趕快報上去，報上去趕快，銀行趕快，這個警示(A04-396)。

比較常被攔阻失敗的那些分行，我們分局長跟隊長他們會再去跟他講一下(A05-370)。

預警中心有三大重要目的，第一個就是臨櫃的攔阻，第二個是對於這種重大詐欺洗錢的通報制度，第三個是建立包括金融機關(A06-791)。

警察在金融管制上需要金管會或是其他的配合(A07-428)。

銀行就是這些人，特定讓哪些帳號提領異常，那這些也都比較好追查，那就可以揪出這些人，那這個是比較有實益的(A08-531)。

2. 金融機構的內控

由於金融交易自由化的因素，且政府不應該過度干預金融市場，因此只能在極限度的範圍內進行規範與勸導。目前國內多數金融機構對於臨櫃轉帳的即刻關懷、立即聯絡轄區警力到場協助、建立內部的預警機制、利用 AI 科技偵測異常交易警示、以電話簡訊通知客戶識詐提醒、要求客戶對於可疑的帳戶情形予以回報、根據警政檢調通知凍結警示帳戶等措施。

轉到某個特定帳戶然後再轉出去...銀行端要想辦法去發現...用空殼公司然後用這種大筆交易買賣的方式去轉帳(A02-300)。

簿子的部分，我是想說能不能壓縮。因為他們簿子的成本開始高，可能一本 50 萬。告誡系統有下去，你可能得親自去提領，不能轉帳(A04-183)。

銀行他們有風控機制，至少可以擋個一兩天(A05-564)。

郵局，現在是郵局，以前最好用的是中信，因為他要快速轉帳、據點多，而且他上限要拉大，郵局不好用，郵局是現在管控的沒有那麼嚴格(A06-194)。

最近不是就會查到一些銀行可能內層通外鬼，就是銀行行員可能配合業者(A08-530)。有些銀行是可能提高一些每天轉帳的限制或次數，或是大額的可能要通報之類的，這邊比較有一個防止效果，可是如果說你透過今天所謂虛擬貨幣，或是透過其他管道去洗錢的話，其實可能影響還是有限(A08-797)。

3. 第三方支付的便利成為詐團的工具

第三方支付是指消費者與商家之間的支付平台或機構，透過中立的第三方機構代收、代付，保障交易安全。詐騙集團申請當「商家」，把第三方支付做為收款管道，第三方支付公司虛擬帳號的設立沒有限制，即便有實名認證，但人頭容易取得的情況，仍然無法有效的管控。許多詐騙集團利用電子金融便利性，讓第三方支付所收取金錢即時轉匯到其他地方，快速把款項從被害人的帳戶轉到虛擬收款帳戶，透過電子金融快速的轉匯至多個小額帳戶，最終可現金提款或轉購虛擬貨幣來躲避追查。第三方支付也是新型態的支付手法，讓詐騙集團利用其隱密性與迅速性的特性來遂行詐欺犯罪，對於提供虛擬帳號的金融機構來說，雖然目前納入防制洗錢規範以及實名查核、可疑交易等作為，然而如同受訪者所述，審核機制有無落實？如何證明該業者故意配合或知情不報，也是嚇阻程度難以提升的關鍵之一。

很明顯是個空殼公司...輕易地去申請第三方支付的公司(A01-308)？虛擬貨幣交易所跟詐騙集團掛勾，...防堵，坦白講很困難(A01-326)。

第三方服務的虛擬帳號，不是我們的虛擬貨幣的電子錢包...它這是一個大水庫(A03-623)。

第三方支付有個查詢平台，可是就算你查到了，錢也已經轉過去了(A04-357)。

第三方支付他是合法的，但四方、五方，這個現在其實很嚴重，自己就可以成立一個第三方支付的公司...只要有人給他額度就可以了(A06-1040)。

我只是個業者，我提供平台，至於你要看到什麼東西，講難聽一點，這不關我的事情，我不負審查義務啊(A08-554)。

4. 人頭帳戶氾濫與難以即時應對

所有金融都需要帳戶為主，沒有帳戶金流就難以流動，詐騙集團為了能夠快速的將犯罪所得實現，需要大量的帳戶來配合，也因此造成人頭帳戶的氾濫。也因為人頭帳戶的氾濫，使得詐騙所得能夠快速地將大筆金額小額轉匯到多數人頭帳戶，快速的將被害人財產迅速轉移並提領或轉換成虛擬貨幣。然而多數的偵查人員認為人頭帳戶不會難破獲，是後續的偵辦上有比較多的考量。尤其是人頭帳戶來源包括貧窮家庭、學生、急需用錢、或者是因為找工作而將自己的帳戶提供出來等，除了主動提供給詐騙集團使用之外，多數仍因為販賣帳戶可獲得報酬，或是本身就是被害者。加上目前我國對於人頭警示帳戶的標準流程是當發現可疑異常交易與不尋常的大額匯款時，金融機構應將疑似洗錢交易進行申報，重大或緊急案件應立即以傳真或電話通報並補辦書面資料。此舉可立即對於這些人頭帳戶進行警示，帳戶內的金錢將無法進行操作。不過詐騙集團也相當聰明，以公司名義進行開戶，假借貨品交易來掩蓋非法洗錢，令人防不勝防。

民眾提供帳戶給詐騙集團使用才會變成警示帳戶，那我民眾提供典型的兩種方式－第一種是詐騙集團請人到某個地方將他的 ATM 提款卡或金融存簿取走，這時他就會開始拿去騙；第二種是他可能寄到一個既貨櫃裡面，或者是超商，再由其他人去拿(A01-370)。外籍人士...回越南，那反正我後來不會再回台灣，就有人說不然你帳戶來賣給我，可以賺三、五萬(A01-388)。

用超商店到店的方式，把自己的帳戶、印章都寄出去(A02-031)。前端他們要警示的時候，好像公司戶會比較難被警示(A02-320)。

其實人頭帳戶不是不好抓，是抓了不好弄(A03-715)。

人頭帳戶找來其實很多都是外籍的，不然都是公司人頭戶，這樣才能大額轉帳(A04-169)。車手...新加坡啊、馬來西亞，超多的(A04-331)。

我們基層就是被害人報案以後，我們就是去抓那些車手調監視器，因為你用資料能洗出來的，其實那些犯嫌都是人頭帳戶(A05-201)。他沒有訂一個SOP，他沒有說什麼標準要警示(A05-434)。

他說找工作要提供帳戶(A07-140)。找工作時還沒有入職就要提供帳戶、密碼(A07-475)。

貪圖報酬嘛，我可能帳戶給你用，我可能可以拿幾千塊的報酬嘛。對那些弱勢的人而言，他可能賣個帳號賺幾千塊，他可能覺得也好(A08-139)。

當人頭帳戶的警示與程序縮短，詐團感受到人頭帳戶的取得開始困難時，詐騙集團為了能夠讓人頭帳戶持續使用，開始限制人頭帳戶提供者的行動自由，以便能夠延長整個人頭帳戶的使用期限，對於人頭帳戶需求增加的詐團來說，不斷出現不同的手法來持續獲得人頭帳戶，迫使第一線的警方與偵辦人員疲於奔命。

之前台版柬埔寨，你要確定裡面幾個人，不然除了大型的像人死了(A04-121)。

台版柬埔寨他是第一件有詐團拘禁、凌虐被害人致死的案件。他因為求職還是什麼交割帳戶，被詐騙之後拘禁在那邊，他一定要有一個固定、可以長期使用的，也不用太長期，至少要騙個兩三個禮拜。(A06-173)。

很多人反正我離境前，我把他賣掉，那我賣掉之後，反正你找不到我，我不會再來台灣(A08-164)。

5. 金融轉匯的即時性，難以即時阻擋

過往面對面的傳統詐欺式微，取而代之的是以電信網路為主要媒介的詐欺手法。也因為電信網路的便捷性與隱密性，金融業務也透過電信與網路而蓬勃發展，正因如此，電信網路詐欺的金流手段正朝向快速且隱密的方法進行中。過去從面對面的面交鉅款，到 ATM 轉帳，利用車手提領，現今為了逃避檢警的追緝，將各種可能的金融手段全部

混合運用，形成多樣且難以阻止的金融匯兌手段，包括分層的大小車人頭帳戶線上轉匯、第三方支付虛擬帳戶交易、虛擬貨幣電子錢包交易、線上博奕儲值變現等手法，大量的透過跨境交易或平台來進行洗錢，不斷製造查緝的斷點，使得查緝更加困難，詐團食髓知味而思考更多金融手段來兌現犯罪所得。

現在絕大部分都是假投資，假投資的就是面交，他反而是 ATM 的比較低了。因為詐騙集團現在也提升了，他現在知道帳戶和 ATM 片來不容易，因為政府一直在宣導詐騙事項，現在都騙網路銀行的帳號、密碼，這是政府需要加強的。那現在也碰到啦，民眾提供網路銀行的帳號跟密碼，款項一進來就馬上轉出去(A01-490)。

不行一定要有被害人報案、要有被害事實。可是這個時候，就已經轉帳出去了(A02-327)。

錢包直接轉一轉，就轉完了(A03-554)。

只能對境內。他們一下馬上轉，他們時間都會算得剛剛好，前一分鐘進去下一分鐘就領出來了。你攔阻不了(A04-373)。

被害人匯到第一層帳戶，他就叫車手去領出來了，他現在可能也知道我們會查，他可能匯到四、五層，才叫第五層車手去領出來(A05-528)。

專業幕後的洗車人員，他會先把帳戶做整理，把它密碼全部改掉、確定身份，確定他不會被封控，才能保有犯罪所得，轉進、轉出、轉進、轉出沒封控，ok 之後給詐團、給機房用，這帳戶可以，錢進來，一進來，他就坐在那個，開始轉、轉、轉、轉，轉 7 層(A06-336)。

第一時間他洗出去，洗出去你在後面追，追到國外第一層、第二層就斷掉了，也沒辦法阻斷(A07-357)。

直接轉帳，轉帳完之後，馬上設定完就直接轉到第二層，馬上就搞定了啊，

就解決了。這種東西有些時候就是一個政策管理面的問題(A08-238)。他們很多金流，他們都有等於說金流的公司，或金流的集團在負責，那他們負責把錢趕快再洗到各個不同的地方去(A08-652)。

6. 虛擬貨幣的查緝困境

虛擬貨幣是以數位形式存在，用來取代價值的資產或代幣，在我國並非法定貨幣，是一種投資的數位商品。而詐騙集團利用去中心化的加密型的虛擬貨幣來進行犯罪所得的價值轉換，過去虛擬貨幣難以掌握與管制，是因為即時且跨境無障礙轉移，不受傳統銀行限制，便於快速轉移贓款或分散資金。由於交易不直接顯示真實身分，對詐騙者來說風險極低。更重要的是能透過境外交易來快速換回各種等值的金融商品，成為詐騙集團相當喜愛的金流工具。也因上面這些虛擬貨幣的特質，讓第一線檢警人員難以向上溯源來查緝主謀，當虛擬貨幣一旦進入電子錢包的交易區塊鏈中，即便掌握流向，也無法得知錢包的真實擁有者。

虛擬貨幣的幣商滿街都是，且民眾無法辨識真假(A01-322)。虛擬貨幣他一定會有下車，他打了一顆USDT到你的錢包地址，詐騙集團就會從ａ錢包地址轉到ｂ，再從ｂ轉到ｃ，ｃ再轉到ｄ，一直轉了一圈到大水池之後，又轉了一圈再下車(A01-331)。

詐騙集團很聰明，他們用現金，現金就比較難追。他們叫被害人帶現金去實體門市買幣。然後員工就會教他們操作然後用他們專屬的另外一個錢包(A02-136)。

個人幣商，去跟被害人換錢那個人。「欸我就虛擬貨幣買賣，我又沒有洗錢。」(A03-797)個人幣商這個行為，到底算不算他知情犯罪？那這個就變成一個不確定故意的問題，就是說我今天去跟人家換錢，那你為什麼不做KYC，你這錢是髒的你不知道嗎(A03-800)？

我們在偵辦過程其實有一個很嚴重的問題是，虛擬貨幣洗出去，你沒辦法在追它流向，你只能往前說，可能他錢包在臺灣哪裡面交，然後直接打到哪個個人錢包下去用(A04-477)。

加密貨幣有一個錢包地址，那錢包地址就是可以拿來放那些虛擬貨幣的，現在問題就是卡在說，他這個錢包地址。假如說我們要有一個實體帳戶，我們現在是不是就要跟銀行或是一些第三方支付的業者去作申請的動作。只是今天這個錢包地址，他有那種冷熱錢包，有些是不用透過交易所，就是你 app 自己按，就可以產出無限的錢包(A05-130)。

從被害人的錢進去，我不是說進去人頭帳戶，從第二層到第三層到美金帳戶到交易所，到 FTX 或是其他交易所，他不可能直接到，可能會再轉個兩三層到藍到指定的錢包，你覺得要多久？12 分鐘(A06-322)

第一時間透過第三方支付或虛擬貨幣直接洗電子錢包到國外去(A07-366)。

虛擬貨幣他並不是我們...他雖然叫貨幣，可是他並不是我們國際間所認定的一種流通的、一種類似代表國家的貨幣，他只是一個交易的工具(A08-816)。

（三） 電信網路堵詐仍有待落實

電信網路詐欺之所以難以突破且越來越嚴重，主要還是詐欺的潛在被害人都是詐團透過電信網路來鎖定目標。對於電信方面的堵詐作為來說，電信業者對於涉詐的門號有提供路由與相關資訊的義務，強化門號的審核機制之外，建置境外門號網卡比對分析系統。對於人頭帳號的作為愈趨嚴格，檢警卻表示目前許多電信網路的詐欺多半透過境外電信業者來轉進台灣，而對於境外的電信業者，我們無法強制其配合調查，此外審查機制多為業者內控機制，並未強制，整體效率並無法追趕上詐騙的速度。然而詐團了解此類電信手法容易被反追蹤，因此開始透過網路電話來進行聯繫，利用網路電話的加密特性來逃避查緝。由於電信網路詐欺透過大量簡訊群發來接觸被害者，為了解決群發簡訊

的情況，要求電信業者進行關鍵字攔阻，雖然能夠阻擋掉許多可疑的簡訊，但簡訊內容詐團可說是一變再變，如此作為只能跟著詐團的腳步後面來做，或者透過 165 詐騙平台的詐騙門號通報來進行堵詐作為。

我已經知道這個門號是電信詐欺了，可否直接去跟電信公司講...(A01-281)。已經有通報的暱稱、帳號，就應該馬上停止帳號(A01-285)。我覺得速度好慢。可能我這個禮拜收了五件詐欺，看到被害人提供的資料，發現這個人上禮拜某某人被同一個粉絲專頁假中獎騙了，為什麼這個禮拜還是有被騙呢？碰到國外的公司他們的配合度都不高(A01-290)。

電信斷話的部分。就是針對有報案的電話、詐騙電話，然後就會跟電信業者去做斷話。然後有些是用隱號的，就是不能強制說一定要顯示號碼(A02-531)。有人申請大量門號的時候，他們會主動來通知你們？不會...他們沒有窗口告訴警察，也沒有規定一定要強制通報(A02-555)。

公司在國內，就是專門做群發的。那是其中一個業務啦，他們還有做別的，那其中一個業務就是群發，那群發他的客戶有 Google、LINE，TOYOTA，他有接比如說印度的電信公司，或者是大陸的電信公司，他有轉包一些給他們在國內群發，他們有做這些，那其實詐騙簡訊，對他們，在他們來講是一小部分。所以那個時候我們找 NCC 跟電信業者和刑事局一起開個會，就是說要做關鍵字攔阻，這就是電信面的攔阻(A03-517)。

因為現在沒辦法通訊監察，你要怎麼賭？而且像 Telegram 或其他軟體都有及焚，也都有加密(A04-341)。

電信警察局他們就用 165 來撈(A05-101)。

電信人頭帳號的氾濫也是電信網路詐欺的幫兇。由於電信網路需要透過門號申請方能獲得網路，而為了隱匿個資的需求，電信的人頭帳號成為最佳的選擇。典型的電信人頭帳號來源為外籍移工或來台觀光旅遊的遊客取得，由於出境後不會使用該電信門號，

販售成為獲得另外報酬的最佳手段。

黑莓卡的話，現在就變成不知道是誰在用的(A02-805)。還有一種是，一接就掛的機器。測試你這支手機有沒有在用(A02-997)。

遊客或移工進來，你申辦帳戶、申辦門號需不需要那麼的浮濫？(A08-148)

現場是像機房裡面、幾十個在裡面工作，現場手機都扣到的幾十、幾百隻，更麻煩。我問你，一團爛帳。我問你哪一隻誰在使用的？他們都是出勤務的時候隨便拿一隻，然後拿一隻去用，用完就繳還，就這樣而已，共用、大家隨便用（A08-359）。

（四） 數位經濟的防不勝防

1. 各種社群廣告的上架使得詐騙訊息不斷擴散

數位經濟的興起讓電信網路詐欺手法更加複雜化。由於網路的便利性使得多數人選擇利用網路來進行各種生活所需的行為，從購物、繳費、查詢資料、掛號、外賣、付款等，生活大小事都脫不了網路，而手機及和網路，讓詐欺犯罪透過網路並經由電信來深入每個人的生活習慣，尤其是社群網站的人際互動，造就了各種生活資訊皆透過手機來接收。尤其是虛假廣告的氾濫，利用人們喜歡上網購物的習慣，以各種不同的折扣特價、名人投資或虛假訊息，引誘大重點及廣告而陷入詐團的犯罪劇本。

詐欺基本上都是以電信詐欺居多。因為你看網路上的臉書、假購物，這些都必須透過科技的偵查作為才有辦法去破案，除非是市場上那種人跟人的傳統式詐欺，不然現在基本上都是科技詐欺(A01-133)。

有很多斷點可以用。用人頭的資料去申請就好啦(A02-583)。

他們接觸到這些訊息，全部都是從網路、社群、或者是電信的部分，可能是要簡訊點進去，或者是我看到FB，或者IG(A03-440)。

民眾就算不想去點，也還是會去點到假投資、假借貸(A04-277)。

搜尋引擎或是臉書，其實廣告投放商可以接觸很多的平台(A06-948)。

廣告進來給你，你怎麼樣憑僅存的幾行字就知道他違法？那我有沒有資格去做審查？好，假設我有資格做審查。那我審查完之後，我要讓他上去、我要讓他上架，上架之後的結果一定他們負責嗎？這種東西我讓你刊登，不代表我同意你做詐騙(A08-559)

2. 實名制認證雖然有政策與法令的支持，但仍有不完善

實名制認證是保障檢警偵查時能夠有所依據，但實名制仍有需多待改進的地方。尤其是目前以人頭來進行實名認證，即便找到了，也很難向上溯源查緝，對於冒名的人頭，也只是為了賺取微薄利潤而協助登記與審查，即使現在已經多數平台與帳號申請都是實名制，如何落實查核更是困難，尤其多數社群媒體平台為私人企業，為了業績與報酬，亦很難查詢該人頭是否與詐騙集團有所勾結，亦很難去判定該廣告內容是否為虛假或是涉及詐欺。

雖然是實名認證，條件太寬廣，沒辦法去做實際上的審核他是不是有效的公司，而且是不是實際上的運作公司，還是他就究竟是人頭空殼公司？這就是需要跨部會去做協調(A01-315) 。

用人頭的資料去申請就好啦(A02-583)。

實名認證這件事情有沒有辦法百分之百，我是覺得不可能(A03-675)。

廣告是要實名制啦。但就是可能會變人頭戶，對啊(A04-279)。

它的效益有限。因為今天你廣告實名制...。應該是這樣講好了，現在詐騙集團，他不是只有這個管道可以去讓民眾接觸到詐騙。像臉書它實名制就沒那麼嚴嘛，就是你今天只要有一個門號，他不用管你這個門號到底是不是本人，你有門號可以收簡訊，我就可以讓你辦出一個帳號。那這個帳號，

詐騙集團取得太容易了，他可以...有點類似免洗筷啦(A05-404)。

有實名制，可是他如果在做違法的事情，我們還是要有等到被害人(A05-473)。

在廣告的平台要實名制，其實都是在講博士你講的那些問題，所以我覺得只要有落實，...實名制之後他會怕(A06-937)。

還是有防火牆。因為找一個人頭或是防火牆，甚至是找一個遊民(A07-266)。

這是一個大原則的思考問題，就是我常呼籲為什麼我們不能夠去做一個實名制的控管？...為什麼都要用人頭，因為我們台灣習慣用人頭來做規避法律的動作(A08-103)。

3. 執行數位經濟的相關機構雖有規範，但其查核與罰則難以落實

數位經濟是龐大的商機，然而這些龐大的商機卻暗藏著犯罪因子，我國雖然對於數位經濟的這些企業有明確法律規範，包括實名制、即時下架、配合調查與提供相關證據資料等，然而雖有法律規範，若沒有相對應的裁處或者是強制作為，私人企業對於政府要求配合義務，但時效上卻無法立即提供，失去第一時間的攔阻與防堵，這些作為與龐大的商機相較起來，罰則似乎不痛不癢，難以啟到作用。即使我國目前有綠色與紅色通道與業者串聯，然而詐騙集團只要在修正資料或是另起爐灶，仍然可利用電信網路來持續詐欺犯罪活動。

臉書跟 LINE 我們有綠色通道跟紅色通到這個緊急調撥方式，那我們可以透過 165 的系統直接通報而跟日商建立一個對等的平台或是和 META 公司，跟他們說這個帳號是詐騙的，請你馬上阻絕他的使用權，就不會有第二個人被騙了。...發現這個 LINE ID 不是誰誰誰也被騙，怎麼還繼續在騙，導致民眾一直被騙(A01-124)。

其實這個像 LINE、像 Apple，都常常遇到這個問題(A02-597)。

網路廣告因為很氾濫嘛，那我們至少要有東西可以查，那你有實名制相對來講就增加犯罪成本。我們抓他一個人頭他搞不好又想要找另外一個人頭(A03-672)。

第三方支付有個查詢平台，可是就算你查到了，錢也已經轉過去了，其實有在幫詐騙集團做事你也不知道啊(A04-357)。

不能說沒用，只是我也是覺得說它的效益有限。因為今天你廣告實名制...。應該是這樣講好了，現在詐騙集團，他不是只有這個管道可以去讓民眾接觸到詐騙。像臉書它實名制就沒那麼嚴嘛，就是你今天只要有一個門號，他不用管你這個門號到底是不是本人，你有門號可以收簡訊，我就可以讓你辦出一個帳號(A05-404)。

複審查過都只是 AI，甚至我們破的那個平台，他還會教詐團要怎麼樣去躲那個審查(A06-950)。

很多營業式的廣告，民眾被騙了之後，所以而受損害，那他現在就是強化說你發現之後，你要把他下架，你不下架造成損害的話，你要負連帶這樣子而已。到底你是主動配合給他刊登？還是說他擅自竊進來，把廣告故意塞進來，找到你們的漏洞而塞進這個廣告？還是說你們有合作關係？這可能都要去做一個認定問題(A08-549)。

假設像我是臉書，或是我是大的這些平臺業者，我不配合欸。他如果說是美商不配合，你怎麼樣？你可以處罰沒關係啊，有種我就離開你台灣市場啊，是誰受所損害？是你，不是我，我沒有你這個市場，我還是可以活下來(A08-573)。幾萬件的公文要我提供資料，我臉書公司還要混嗎？我每天光函覆給你就好了，對不對？那我臉書公司不用經營嗎？(A08-863)

（五）　編制人力的不足與機構間協調

基層人力的不足使得案件量難以負荷已成為檢警院之間的共同議題。從警政與法務部的統計資料來看，雖然警政因統計標準的不同而使得案件量大幅提升，然案件量的上升趨勢是不爭的事實，即便我國從 2022 年開始打詐 1.0 綱領開始，反而是這幾年的案件量數最大，也正因如此使得打詐綱領短時間內升級至 2.0 版，顯見詐團的犯罪手法不斷更新，政府透過立法來強化檢警院的量能尚未能滿足偵查判刑所需。當中最值得注意的是目前國內不管是警政或檢調，亦或是後端的法院與矯正機構等，詐欺犯罪已經嚴重影響上述機構的正常運作，似乎絕大多數的量能都投入在詐欺犯罪上。但是犯罪類型多樣，勢必或影響對於其他案件的進度，尤其是詐欺案件所涉及的層面眾多，包含電信相關法規、金融規範、人口販運、數位要求等，單純的詐欺之罪名，卻因為其分工細膩，不僅讓第一線打詐作戰的檢警調疲於奔命，後端的矯正較化與復歸也是焦頭爛額，尤其人力編制無法滿足案件量的時候，大大的打擊刑事司法的士氣。

很多喔。...所以就是到時候可能基本上每個人都會一件以上(A01-069)。

等於是一個人要負責一個案件？對，沒錯。而且不只一件。還可能會接到很多不同類型的犯罪的案件(A02-410)。

大家都會累啦(A03-974)。

真的全部被詐欺案壓，...，你再怎麼做警察人力有限(A04-087)。人頭帳戶就移送，會癱瘓檢察官(A04-440)。

主管機關不是只是打電話。這個問題又卡到人力的問題啦，...他沒有增加的話，他等於是你今天增加業務量(A05-499)。越來越多的工作就是要讓我們去阻詐。可是他沒有想到我們基層的人力是沒有增加的，我現在的業務量跟我四年前的業務量，多了很多(A05-761)。

檢察官那麼忙耶，如果你說每個案子判了檢察官可以上訴啊，怎麼不上訴啊(A06-414)。我們找到了匯款的金額、找到，我們還去分析，分析出來超過 100 個，有些沒報案就沒有辦法處理，分析出來大概七十幾個可能有，

但是金額很大，一個檢察官有辦法辦七十幾個人嗎(A06-861)？

我們法院是讓四個法官去當強制處分庭的法官，他們不辦一般的案件。好處是比較集中，壞處就是一樣是要臨時馬上就會來...累得要死(A07-419)。

回到整個人力的問題來講，今天你要查緝的也好，查緝本身要有人力，那主要就是檢警調的人力在處理。那你想一想，目前所有的檢警調已經被這些詐欺案件給癱瘓了，你一個月只要辦 1 件詐騙集團跟一個月要辦 10 件詐騙集團，你的人力當然會被分擔掉，更何況警方還有別的勤務要處理。那麼多勤務，你覺得他有辦法去應付那麼多詐騙集團嗎...舊案都還沒查完，新案又跑進來(A08-096)。

由於詐欺犯罪涉及的罪名多樣，其偵查過程中所需要的各種資料與證據，仰賴各部門與機構的協助，因此機構間的橫向聯繫與協調格外重要。然而我國打詐綱領的各個面向分屬於不同部門執行，雖然由行政院作為統合中心，然國家行政部門為垂直領導，上令下達的官僚體系，對於平行單位之間的聯繫與協作上來說，除非首要緊急要務之外，其他機關的行文要求下，多半對於承辦人員來說，其緊要程度不若自身機關的業務重要，加上每個部門有其法律規範，若沒有正式行文或明文規定，對於橫向部門間的合作難有助亦。正因如此，使得詐騙集團利用部門間的時效性特質來遂行詐欺，加上詐欺犯罪的各種工具與手法涉及多個部門管轄，使得詐欺犯罪能夠游刃於這些地帶。

現在大概不到一個禮拜，可能最快兩三天就會回(A02-243)。在前端他們要警示的時候，好像公司戶會比較難被警示(A02-317)。系統其實是算是滿分散的，就是你現在要查一個人的資料，你要去各個系統去查(A02-873)。

一定要我們提出需求，而且他有受信任警察機關。就是不是說隨便的機關，發文他們都會理。如果沒有的話，就要請法院申請扣押裁定(A03-385)。

我們刑事局就很傻眼，他現在說情資小組現在不要...專業化，分由各大隊去成立情資小組，好 ok，成立情資小組，又要兼所謂的說服小組...第一線

其實派出所已經在做這個動作了，他們都已經在做這個了，可是他現在要叫我們刑事局做。(A04-072)。現在就是勞工局也推、移民署也推，移民署才能控管進出，但勞工局說他們有人權，你不能擋他們開戶(A04-198)。會去點到假投資、假借貸，那你數發部怎麼不發個 APP，攔阻或管制(A04-280)。

現在這個系統的建置，可能我們警政署有些資料還是拉不到，其他行政機關他有這些資料...我們的立場就是想要趕快把人抓到破案，那其他機關的立場可能就是跟我們不一樣。(A05-316)。

我們就是綜合這個金融的情資、調查局的情資還有警方他們這個 165 報案的系統，各自有各自的資料庫，由預警中心來做整合，才能發揮到最大的作用(A06-821)。

因為警察在金融管制上需要金管會或是其他的配合，如果他們不去配合，那他也沒轍，做起來會很難做(A07-429)。

由於機構的本位主義與管轄責任及範圍，形成多頭馬車的打詐團隊，主辦偵查的第一線員警以及檢察官，難以透過其權責將所有需要的蒐證權力掌握於手中，不過政府為了解決這個問題，將所有機構可能的數據資料整合成一個系統，供第一線警員與檢調能夠獲得相關資訊，除了所知道的 165 平台外，其他縣市也會有科技偵查平台以及智慧分析平台，這些都是大數據資料庫的概念，透過各部門的整合下，提供第一手的資料，減少公文來往的時間，提升整體辦案的效率。不過即便如此，雖然對於第一線檢警辦案的便利性提升，然而像是人頭帳戶或帳號之間的管控，其他機構對於詐欺偵查相關請求與預防，並沒有如同看待防疫作戰般的謹慎，使得打擊詐欺犯罪出現漏洞可鑽。

所有的警察絕大部分是使用 165。但是以我們台中則有整合性科技偵防平台，也就是俗成台中的科偵平台，它也是屬於大數據資料庫，它這個滿厲害的，我覺得我們科偵設計的滿棒的，它會將案件都建置在這個系統裡面，

你可以輸入姓名、生日，乃至於門號或者是車牌，它就會顯示出這個人或是這個門號涉及了什麼案件(A01-171)。整合性智慧分析平台，它也可以做查詢，它也是大數據的部分。

如果是金融帳戶的話，就是用金融調閱平台(A02-239)。我們現在對 Google 有建一個平台是可以針對詐欺案類去丟廣告商的資料，假投資廣告的連結，然後告訴 Google 的平台，然後他們會回給我們當初設廣告的人的資料(A02-584)。

目前投入的資料，資訊蠻多的。比如說像一般的電商平台，投單調閱，然後還有現在跟金融業界的系統連線。不用再在發公文，發公文還要接收公文(A03-336)。

移民署那些都要管控，他們不管控啊(A04-334)。

今天查到詐騙集團，扣到犯嫌的手機，他們可能裡面哪個群組有講到哪個帳號，其實那個截圖截一截，你發個公文去給地檢署，地檢署可以用這個截圖去跟銀行要求他們警示(A05-516)。

。只是兩三天過後，如果真的沒有人報案，其實你不可能說你一直擋著不讓這個民眾領錢吧(A05-470)。

設在行政院，但主導的是內政部，像詐防條例主管機關是內政部，他只是有分好幾章，主責的單位不一樣(A06-975)。

三、偵查打擊面

電信網路犯罪偵查往往是整個打詐的最後一個環節。然而當詐欺犯罪一旦發生，被害人一旦報案，從第一線的警察、指揮辦案的檢察官、判刑確定的法官到後段矯正教育的監所等，都是民眾希望的最後一道防線。

(一) 案件來源

現況辦案的資訊來源除了有民眾報案之外，許多第一線的警察慧從內政部警政署 165 全民防騙網的數據資料，來了解多數詐欺案件的資訊。或者是檢察官受理或是案件衍伸而出的另案偵辦。這些案件除了被害人報案之外，倘若被害人的資料有限，亦難進行下一步。因此會從 165 全民防騙網的資料中獲取，開始分析提報的相關資料、比對與分析，若有明確且可疑有進展的線索，也是案件的來源之一。也有檢察官查案時發現有另案的可能性，不斷地向上溯源時所發現的，都可以成為另案的偵辦來源。

主要的來源是民眾報案，由派出所受理完後到你們這邊，還有一個就是檢察官受理自訴或告訴(A01-052)。

刑事單位有一個系統是 165 平台。裡面的話有很多資訊，我們可以去看各種案類(A02-029)。去年有協辦一個學長的機房案件。有檢舉人檢舉說他們這邊有在做機房。但是他騙的人是美國華僑。都是一些失婚婦女。他也是假愛情投資的案子。所以就是透過檢舉人才知道(A02-448)。

地下匯兌...除非是有人、又有人報案、檢舉，才會察覺到(A02-774)。

一般的電商平台，投單調閱，然後還有現在跟金融業界的系統連線。我們以前要發函嘛...我們就直接上去投單就可以了(A03-327)。我們用的是 165 的資料系統，民眾報案我裡面都看得到。主要是會是從那邊去做，因為它會一直修、增進一些詐騙手法，一些 filter 的東西(A03-404)。

不然就 165 去撈，或我們那邊也是有人會來報案啊(A04-215)。

主要還是靠民眾報案，以前是都靠民眾報案，然後再去用 165，再去那邊撈資料。現在就是警政署他們那邊，因為案件太多，他們就有比較主動積極，可能有一些潛在被害人計畫，讓我們去主動的去找這些還沒來報案的被害人聯繫(A05-085)。

詐團凌虐致死的案件，我們還破了什麼？我們還破了全台灣第一件用虛擬貨幣行收賄的案件，就是這個藍道用虛擬貨幣去行賄派出所的所長，我們還搜索大同分局把那個所長收押(A06-342)。

此外，由於目前金融機構有內控機制，一旦發現了可疑的帳戶異常提領與轉匯，金融機構會製作報告並提交調查局，甚至在第一時間與承辦的員警或派出所通知，那個地點目前有可疑的提領狀況，這些都是目前打擊電信網路詐欺的案件來源。

今天有一個台灣銀行的警示帳號，那我可以透過這個帳號去做被害人的資料分析，再透過被害人的資料分析去知道詐騙集團與他的犯罪類型是什麼，所以這種也可以得知被害的趨勢(A01-055)。

金融機構裡面，然後如果他有提領的狀況出現就馬上通知我們，然後我們就可以去抓車手(A02-650)。

這個帳戶，可能是受犯罪使用，今天有來領錢你馬上發一個即時通報給我，可能是到我的 E-mail，可能是到我的手機，幾點幾分、ATM 的哪一個號碼提領(A03-684)。

銀行趕快，這個警示(A04-396)。

有些可能銀行的風控或電信門號的風控，他們內部可能會自己去偵測，就是可能哪個門號異常或信用卡異常，那他可能就會找一些有配合過的同事，請他們去做查處(A05-096)。

郵局搞不清楚狀況，來就講一些理由，但他就有跟我們說最近發生很多這種事情，我就說好，那你們就通報給我們，通報給我們我們就開始立案偵辦，這個展金專案(A06-806)。

(二) 偵辦手段與程序

20 年前就已經存在這種東西。只是說當時的科技沒有像現在這麼方便，...，

他的詐欺的廣泛程度沒有那麼廣，他可能是打一通、騙一通、打一通、騙一通，很慢又很花成本。現在不是啊，寄發個訊息亂槍打鳥，幾萬份打出去只要中幾隻鳥可能就可以收回本了，所以他的案件數會變的這麼多的原因，就是因為科技進步所造成的結果(A08-032)。

以目前警察打擊電信網路詐欺的偵查手段來說，從接獲報案後，開始分析可能的情資，對於可疑資料的收集與偵查，埋伏或突破可能的犯罪地點，現場證物的收集與證據保全，檢方起訴的迅速性與正確性等，都是偵辦電信網路詐欺的重要關鍵過程。然而在現今詐欺手法的不斷更新，利用各種不同工具的法律規範不完備之處，使得偵辦過程中遇到許多立法前無法預知的困境，只能隨著破獲或得知新的詐騙手法來加以不斷修正應對作為。

1. 偵查辦案思維與利器

M 化車與 GPS 定位的使用確實能夠成為警方偵辦的利器之一，過往礙於法令並未完備的情況下，M 化車與 GPS 定位系統的使用有侵害人權之虞，就算要做，也得冒著違法的可能來進行犯罪偵查，然而若查緝屬實，仍有程序不正當的可能，更何況沒有法律支持之下的違法作為，反而使得第一線的犯罪偵查警政人員綁手綁腳。但在這些偵辦利器的有法源依據後，能夠為第一線警政提供更好的辦案利器。但仍有訪談者認為，使用這些器材時仍須經由檢院同意才能使用的情況下，若消息走漏或是不同意情況下，即便知道電信網路詐欺正在施行中，苦無明確證據下，無法取得檢院同意仍是紙上談兵。

基本上根據之前我跟我同學在偵辦一個案子，比方說以假投資虛擬貨幣的電信詐欺來講，要抓到機房不外乎就是去鎖門號之後，去用刑訴法修正的 158 之 3 的部分，特殊強制處分篇的 M 化車，用 M 化車去鎖，...我們去做追查一定會使用的就是 M 化車，對於電信詐欺一定要使 M 化車，因為可以用訊號波是在哪一棟建築物中去鎖，之後再去做一個蒐證的部分，這是一個作為的方式(A01-109)。

全球衛星定位系統 GPS 的部分，我覺得都是我們會去使用的(A01-107)。

在台灣境內連結到網路、需要上網的話，就是透過台灣基地台。那我們就會調的到資料，就是境外門號在台灣漫遊的資料。到這個時候，就是用基地台會直接判斷他所在的地方，然後再用 M 化車去鎖定他的位置(A02-353)。

M 化車、GPS 還有熱顯像儀。GPS 大家是常用(A04-109)。

我們現在可以用 GPS 然後 M 化車啊，可以去跟法院申請(A05-679)。

目前已經讓他賦予合法的地位，就是要讓你警方可以更無後顧之憂去做(A08-904)。

以目前我國對於電信網路詐欺犯罪的辦案過程來說，從被害人的報案、165 平台的情資分析、金融機構的警示通知、查辦案件的分案可能，都是案件的來源，然而當接獲相關資料，展開一連串的情資蒐集與分析，從監視器來調閱車手長相與動向，接著透過金融機構來追蹤金流去向。即便如此，常常因為查緝過程中的繁雜程序或斷點而難以繼續。

所有的詐騙案，我們都會盡量叫他先去派出所或分局，先去報案。然後他們會做警示賬戶，然後馬上通報金融機構。那通常派出所接到這案子之後，這個案子會再承轉到，看哪一個分局的偵查隊。那偵查隊再去調資料、就去找車手(A02-78)。可能...背後有好幾個車手集團好了。然後我們才會有把握去報檢察官(A02-97)。很明確的證據。所以基本上院檢都是會願意支持的(A02-107)。一開始接到案子應該都是先分析金流。其實我們大概會分成，金流面、資通面。資通面的話就是調網路銀行的 IP。然後 IP 的話就會調到那時候登錄網銀的使用者是誰。然後會得到一個門號這樣子。再來就是...像我去年有遇到一個案子他們登錄的 IP 都是用境外門號登錄，就是香港的黑莓卡。那在我們偵查面來講，如果用黑莓卡調的話找不到人嘛，因為它就是匿名的嘛。然後我們只能用基地台的位置去判斷他們可能在哪

裡(A02-338)。

第一個金流分析，第二個，現在你沒有聽的話，你現在要從他的這些行為模式去判斷(A03-229)。就是軟體啊，就是幣流分析軟體(A03-591)。

我們主要一開始一定就是先追金流面，那金流可能就是人頭帳戶，然後人頭帳戶再去擴出收簿手或車手，這些實務面的，調監視器調得到的(A05-120)。

雖然目前情資量大的情況下讓第一線人員人仰馬翻，但為了解決大量情資取得與分析的難題，刑事局的智慧偵測決策系統，將過往所有犯嫌的資料全部登錄，包括電話號碼、性別，或被查獲的地方，統整成大型數據資料庫，如同大海撈針般的方式來獲得切入詐騙集團方式。從被害者報案的金融帳戶溯源，或是從人頭電信帳號去查緝，甚或是將可能相同的犯罪模式進行分析，縮小整個查緝的範圍，結合科偵平台的資料，透過比對與查詢，找出蛛絲馬跡來介入。如果發現可疑的帳號與帳戶，除了透過金融機構的第一時間通知外，一有可疑的資訊，立即進行金流的阻斷，減少被害人的財損。因為詐欺犯罪集團最終目的就是要犯罪所得，如果能夠從犯罪金流去著手，方能夠斬斷犯罪集團持續運營的支撐，最終能夠瓦解集團的運作。

警政署建置的 165 其實是滿廣泛的，可以透過金融帳號進行查詢，第二還可以透過電話號碼。因為電信詐欺有可能是利用去買人頭卡的電話號碼去詐騙民眾，警政署利用電話號碼去分析這個有沒有被通報過，所以這個也可以去做查詢。第三種還有犯罪模式的，例如猜猜我是誰、假檢警、假投資、假中獎，這種的他都可以在 165 上做查詢(A01-060)。

我們局內的智慧決策系統...資訊那些都有(A03-312)。以前我們都要發文去給...有這個平台我就直接投單就好我就不用再等(A03-661)。

165 系統上面，就是可能有詐騙網址或者是一些通訊軟體的 ID 什麼的，都要打在上面。然後他們會去做這一塊的...等於他可能先請 LINE 公司還是

什麼，先把這個網站或帳號給他封掉(A05-259)。

不管是出金還是你要給金主、你要給車手、買什麼東西，全部都要透過水房，所以說你有效斬斷(A06-878)。

2. 證據取得與調閱的繁雜

許多訪談者都共同提出打擊電信網路詐欺犯罪的困境，其中之一就是證據取得與調閱，偵查過程中對於資料申請的過程，會因為不同資料的申請來自於不同的機構單位。電信相關資料要與電信業者申請，金流去向要跟金融機構與調查局申請，數位廣告需要與社群媒體索取，手機各資需要手機業者的解密機制等，由於這些絕大多數是私營企業，在個人資料保護的大傘下，沒有明確的犯罪事實或是法律依據，多數企業的配合度不高，使得證據舉得相對的困難。當中還涉及國際間的司法互助，如果今天犯罪集團在國外，或者相關金流匯往國外，由於我國特殊的國際地位，對於取得相關證據更是比登天還難。

去調META 公司一頁式廣告的申請人，或是某個臉書的帳號申請人，申請資料下來後他的 IP 基本上是在國外(A01-575)。必須要跟法院，就是地檢署檢察官先核准後由法院給搜索票，我們再拿搜索票回到我們的刑事平台去投單，和APPLE 公司調閱誰去申請這個APPLE 點數的資料，因為APPLE 賣出去的他一定帳號跟密碼。所有的資料是一組 IP，IP 前面、後面會有一串的資料，我回去用去識別化提供給您，我們調的 IP 百分之一百都在國外。檢察官就問我:「為什麼你還要再調？」我說：「主任跟您報告一下，不調不行。」因為民眾一定會質疑說為什麼警察沒作為，明知我們這個都是在國外，但還是得做(A01-592)。

我們系統其實是算是滿分散的，就是你現在要查一個人的資料，你要去各個系統去查。金融是跟金融的平台上面查。其實有整合的系統，但就還是有非常多系統要查(A01-875)。

可疑交易，是通報調查局啦。不是通報刑事局。所以我們調閱也是透過我

們窗口跟調查局拿資料回來(A02-902)。

查緝的這個點是說，我們查完車手之後，在水房要做的事情很多。那車手他有咬，或是要對一下他的手機是誰..我們就找。但是水房可能要去過濾他金流。哪筆金流是詐騙集團的？這有沒有辦法去對應到被害人？你要有被害人才有辦法去做詐騙的起訴(A03-770)。辦詐騙我們要看的資料量非常大，有時候很趕。那有些如果公司合作不是這麼好的話、他覺得他賺錢比較重要的話，他就是給你軟釘子吃(A03-911)。

手機的基本資料，他會認定說那一個是也算是個資。所以現在就是警方可以針對這部分可以調機資，要不然是不會被認為證據(A04-106)。因為你要連結到犯罪事證，你找不到集團上游，就沒辦法跟檢察官報告(A04-284)。

這樣做當然是比較好，可是因為這是不是就會扯到說你今天這個證據的合法性。我們的技術可能比不上對方，就一些法律限制的(A05-757)。

證據的錯綜複雜與數量龐大，不僅拖垮整體人力資源，更添加了整體偵查的困難度。訪談中得知由於詐騙集團人數眾多，不管是何種犯罪行為，都需要有被害人、犯罪事實、犯罪事證進行連結，多數的證據尚未有具體的連結情況下，不僅難以證明有犯罪之虞，更難以透過羈押來避免串供，加上每個犯罪人的戶籍、犯罪地、被害人都分屬不同地區，使得案件的管轄呈現多頭馬車，此時每個證據就會呈現交錯複雜的情況。

我要請搜索票去現場決勝負的時候。所以，其實這整個過程，我們可以把它理解成是一個，保全證據跟蒐證的狀態(A03-237)。管轄權也是有問題啊。我們之前有大陸遣返的，就是在東南亞車手遣返回來(A03-1037)。

我覺得有一個麻煩是，犯嫌的戶籍地很重要。到最後，車手、水房那些跑各地的，檢察官量很大，就會看戶籍地，另報指揮(A04-225)。現在量一大，大家又開始了，一直切，切到很細(A04-264)。

不只要看他匯款，你還要看他錢從哪裡來？再去追水房在哪裡，這是很簡單的邏輯，但問題是你案件被淹沒的時候你就很難這樣想，你要抽離出來去看，我發現這可以有搞頭去追查。從這個案子之後，譬如說我們去調全國的資料，一調不得了，只調七、八個月，從五月調到一月七號，掉了八個月，匯款金額超過兩萬筆，兩萬筆是什麼數字？可能匯款的金額14.5億(A06-839)。

我們申請扣押裁定的時候大部分是在我們偵查的初期，或是已經要執行的狀況之下，我根本不知道他賺多少啊(A06-702)！

為什麼說檢警很辛苦，因為他必須要從你們查扣到的手機裡面、電腦裡面去還原你們的對話紀錄、還原你們的金流，去釐清到底之間是什麼關係。那這邊就我講，他是一個很辛苦的工程，就是能夠還原多少？縱使簡訊都還原了，能不能夠比對出來這個款項指的是哪一筆款項？這邊就是很難去把他勾在一起。所以這個時候到底你參與了幾次？參與到什麼程度？這邊往往就是彼此的供詞去互相去稽核(A08-320)

按照以前我們的經驗，你縱使跟當地的警方合作查到了，證據在誰？在他們手上。你要證據是不是...不是不認真收集，而是他的難度很高(A08-424)。

3. 證據保全與時效性

除了證據的取得與調閱需要多個機關與繁雜的程序外，證據的保全與時效性又成為另一個打擊電信網路詐欺的困境。證據的保全與時效性跟跨機構的整合有莫大的關聯。檢警負責辦案的過程中需要收集證據以及調閱相關的資料，然而這些過程需要機構之間的協調，雖然目前有調閱平台與大數據資料庫，然而關鍵的資料仍有保密規定，對於一線承辦人員來說，仍需一定的程序才能取得。目前對於許多私營企業來說，由於立法的關係讓其配合檢警調的辦案須提供相關資料，然而除了公文往返的曠日廢時，許多公司的證據保存有其時效，若沒有在時間內提出，資料可能已經覆寫而不存在。目前對於手

機鑑識雖然已經能迅速的破解，然而詐騙案件的數量太多，等到真的輪到時，又已經過了好幾個工作天，期間可能已經又有許多被害人遭詐。若是發現立即可能性的證據或犯罪地，也得法院申請搜索票，雖然已經盡量縮短審核程序，但若相關事證不明確，仍有可能不核發。另外對於目前金流去向的查緝也是需要大量人力與時間，贓款金流的層層轉匯只需數分鐘的時間，然而檢調為了這短短的數分鐘的金流去向，卻需要花上百倍甚至千倍的時間才能一一釐清，即便取得確切的金流去向，這些贓款早已被詐騙集團分贓完畢而難以追回，只能作為後續懲詐判刑的證據，對於被害者最在意的金錢返還，助益不大。

LINE 目前的狀況是針對詐欺。以前的 LINE 是要搜索票。因為它是日本公司，它要搜索才會給我們通聯、然後一些片段的文字，圖片是沒有辦法給的。而且不一定是完整的資料。而且它的限制是要 90 天內提出來。LINE 現在有稍微進步一點，是針對詐騙案件可以比較快速的提供資料。還是要做公文往來這樣子(A02-611)。

我覺得案件可能很急，像機房會搬家了，可能看個卷很忙，可能看個線看個兩天三天、四天，然後又遇到連假，禮拜一才出來。那好，搬到哪裡去了...他會怪你太晚送(A03-956)。

我們現在能用的就是手機鑑識，他不講就得破解。破解完後要跑報告，還要依依看報告，你看你為了一個案件要花多少時間。我們一隊查扣到一個手機，六十個人你要排多久。因為現在只能靠手機鑑識，你其他沒有...帳戶都轉出去了啊。也可能遠端就把資料處理掉了(A04-380)。

沒辦法上線，可是可以跟法院申請搜索票，然後去請 LINE 公司提供一些資料...這個一定是都好幾天，沒辦法那麼及時(A05-242)。多久喔...在兩個禮拜到一個月吧。監視器他都有容量限制，他過了那個時間，他覆蓋過去就沒有辦法再回復了(A05-399)。

錢包只要 10 幾分鐘，我們為了這 10 幾分鐘我們花了多久？我們整整花了 158 天(A06-352)。

真的做這件事情有確切的實質證據後，我才有辦法...通常法官看到的都是這種，檢察官敢起訴的也是這種(A07-321)。

第二個是外籍身分的犯罪者與少年身分的集團成員，使得證據保全與取得更加困難。首先是外籍車手的問題讓詐欺困境加重，由於外籍車手多半使用旅遊簽證來台，期間提領多次的犯罪所得難以掌握，若期間無被害人報案，甚或是拖了很久才想要報案的情況下，車手也早已離境，根本無法掌握這個部分的證據。接著是外籍移工的帳戶問題，由於外籍移工到台灣工作都需有薪轉帳戶，而等到移工必須回國之時，帳戶不再使用情況下，轉售給詐騙集團做為人頭帳戶進行匯款，這樣的情況越來越多，也使得證據的保全與調閱愈加困難。少年車手的問題也使得打詐難以有效嚇阻，由於少年犯罪保護原則下，讓許多詐騙集團吸收少年做為車手，現行《少年事件處理法》讓查緝犯罪很難去溯源，如果不是 5 年以上重罪，多由少年法院裁定保護處分，施以感化或輔導教育，成年後又有前案紀錄塗銷機制，視同未曾犯罪，也才導致少年付出的代價過低，容易受到犯罪集團煽動，也讓青少年車手就像免洗筷一樣，用完即丟，受害者越來越多。

人都在國外，都離境了(A01-404)。觀光簽的那種，...馬來西亞籍的車手。在馬來西亞應徵工作來到台灣，從事一個商業行為。他來台灣就開始了阿，絕大部分是在北部先居住，詐騙集團在台灣的對口窗再請他去做面交、拿款項，這種是外籍車手(A01-416)。

之前臺南請票很困難，為什麼？因為法官認定的機資是必須是去地檢調的，不是警方自己調的，要不然他認為沒有證據。所以每次在請票台南就會擋(A04-101)。現在外籍勞工真的都多，有些覺得我回國我就沒差了，就帳戶一兩千塊就賣了(A04-195)。現在還越來越老，或者是說找國外的，旅遊換宿，幫他們領個錢，然後就離開(A04-328)。

最近那個境外車手很猖狂。用那種旅遊簽證，一邊玩，然後一邊照上頭的指示去領錢(A05-614)。他都是用那種旅遊簽證，而且我們最近幾個月很常有這種的，然後他就是旅遊簽證，然後他進來，他可能就是七到十天或兩個禮拜，然後他一進來以後，他就是一邊玩，然後一邊照上頭的指示去領錢(A05-612)。到期的外勞，他們就會把賬戶賣掉(A05-632)。

少年車手今天等於是很多詐騙集團會吸收這些少年的車手，讓他們去幫他從事第一線詐欺的工作，通常法官都會給他責付家長，除非他今天已經真的是被抓了好幾次了，可能才會押在收容所(A05-647)。很多都是輟學，就是學校也沒再去了。

你沒有辦法去綜觀全局，我講的你去調全國資料，他可能七個多月匯了兩千多次，然後金額是差不多一億，但他詐騙團是好幾十億，但你只是其中、單次，你看不出來，所以我們欠缺的是這一種大數據分析、資料整合的能力(A06-1128)。

整個行政院不是很同步、齊步，因為對金管會來講他覺得那不是他的重點(A07-219)。

不管是遊客或移工進來，你申辦帳戶、申辦門號需不需要那麼的浮濫？就是你當初的目的是為了便民(A08-148)。

對於早期的詐欺來說，多以傳統的電信或者面對面的詐欺手法，這些都能以監聽模式來進行辦案。然而電信通話式微的情況下，網路電話興起，詐騙集團利用網路電話無法立即監聽的特性進行溝通之外，更利用網路電話需解碼以及以代號來互動，難以辨識談話內容與人物，就算要進行通聯記錄的調閱，調閱的程序過於繁複，使得第一線承辦警員的工作負擔更重，此舉增加第一線的警察與檢察官的辦案難度。詐騙集團使用先進的通訊軟體，即便衝入犯罪現場，對於證據的保全仍有其他因素影響，這些通訊軟體都有自動銷毀的功能，即便扣押手機進行鑑識，最後也都鎩羽而歸。

網路電話就沒辦法監聽啊(A02-606)。你已經窮盡一切偵查方式，非通訊監察不能做的時候，你才能來上線(A02-890)。

那時候通訊檢查，還可以聽得到東西。現在我們都用 Line 打...通道是加密的，就算嘗試破解他們也還是會再設定。(A03-162)。現在我們要做一堆卷，然後要跑地檢署，給檢察官蓋他的章，才能回來再調(A03-883)。

Telegram，飛機。那個東西是即焚，他只要設定時間有即焚，就算我們警方扣到手機，要再做手機鑑識，那東西已經銷毀了(A04-095)。Telegram 或其他軟體都有加密(A04-341)。詐騙集團在幹麼我們其實都知道，可是現在通訊監察式微，相關的通訊軟體 APP 不能監聽的時候，我們永遠是跟在後面，只能拿手機回去鑑識，可是你都是舊的犯罪事證(A04-130)。

因為都聽不到(A05-246)。我們的工具跟不上詐騙集團，因為他們大概都是用那個飛機 Telegram，他們都有一些自焚的功能(A05-739)。我們沒有辦法在可能犯罪事件發生的時候去監控，這以往是可以的，比如說通訊監察(A05-1049)。

Telegram 你根本不知道他那是誰，閱後即焚(A06-453)。

他用微信等大陸的軟體你怎麼弄？因為不是電信公司，如果他用大陸的你也沒辦法。現在監聽也不多，因為聽不到、找不到(A07-399)。

通訊軟體他也怕你查緝，所以可能通訊軟體通聯完，他們就馬上刪除或是馬上換別的軟體嘛。今天這個軟體被抓就換下一個軟體，手機可能用完就丟了幹嘛，所以你根本也查不到相關的那些手機(A08-302)。監聽到都是文字訊息又怎麼樣，有多少人會在上面講話，沒有講話，上面訊息，而且訊息很快就刪掉了，真的意義不大啦(A08-760)。

4. 跨境犯罪查緝的困境

證據的保全的困境之一就是跨境的司法互助。由於電信網路詐欺的機房或是其他水防或車手，都橫跨其他國度。加上跨境犯罪的查緝常常因為司法之間無國與國簽訂的合作協議而告終，明顯這些詐團知道我國在國際上的特殊地位關係，便利用跨境的犯罪來躲避各國查緝。根據外交部的條約協定(司法類)的資訊來看，目前有八個國家[153]與我國有簽訂司法互助條約，在犯罪偵查的部分則有 33 個國家與我國有簽定相關的協定或備忘錄，不過詐騙集團只要避開上述有簽定的國家，仍然可以有很大的躲避查緝空間。

碰到是國外這一塊，目前還是個無解(A01-601)。我們會透過國際科或兩岸科去調資料。通常是不會有下文(A01-293)。

機房內部檢舉的會比較多。第一個機房都在國外。我們沒辦法去透過互助合作去找到這些機房、去抓這些人(A02-783)。我們的困境都是卡在司法互助這一塊。因為錢只要進得去國外，不管是交易所虛擬貨幣的錢或者是到香港、到大陸，都沒有辦法，都追不回來了(A02-938)。

外國的可能就比較沒有辦法，我們也要考慮一下國情問題(A03-606)。我們國際的地位有問題，怎麼跟人家推(A03-818)？

之前有大陸遣返的，就是在東南亞車手遣返回來。我們希望檢察官，可以幫忙我們開個拘票回來，檢察官說「犯罪事實嘞？」(A03-1039)

我覺得其實有時候是國家的問題。因為有時候對外，可能有些公司或一些政府，它不會認定你是個國家(A04-019)。台灣是個國家嗎，人家為什麼要配合你(A04-346)。

國外的帳戶就...其實我們如果轉去國外，我們都會發個公文，請那個刑事局那一邊幫我們向那個國外調資料，只是後續基本上是幾乎都沒有再回來

[153] 目前有帛琉共和國、聖文森（及格瑞那丁）、貝里斯、諾魯共和國、南非、菲律賓、越南與美國。資料來源：外交部，網址：https://www.mofa.gov.tw/cl.aspx?n=500　最後瀏覽日：2025 年 9 月 10 日。

(A05-191)。

跨境是個非常大的困境，各國都一樣，因為機房水房，你在台灣能做的就是斬斷他的，讓他沒有辦法運作，為什麼？我們目標一定放在水房(A06-875)。

我們外交的困境也是，人家不理你啊。第一個已經沒有外國的資料，剩下就是這兩個資料，但這兩個資料又不會白紙黑紙那麼清楚(A07-111)。

假設你今天是美國或中共，你去跟他要，他可能就給你。你今天去人家會理你嗎？你先跟我講一個問題，你跟我要資料，為什麼我要理你？我為什麼要理你台灣，對不對？你又不是我的誰，我公文就不回你啊，你又怎樣？(A08-437)。

5. 詐欺集團設立斷點成為偵查打擊犯罪難以突破的關鍵

電信網路詐欺犯罪偵查主要朝向犯罪人、金錢流向為主，而詐騙集團為了躲避查緝，想方設法要在可能的犯罪過程中設立斷點，讓檢警無法向上溯源。以金流追查的斷點來看，目前洗防法雖然通過，也對於虛擬貨幣的幣商加以實名認證與限制，然而要讓所有幣商都遵守相關法規，這個過程仍在持續落實當中。過去透過大量的人頭帳戶層層轉匯，讓金流難移追溯，甚至匯往國外，利用國內外金融機構上無配合提供資料之義務來遂行詐欺，還有第三方支付平台與電子錢包的匿名交易，都讓查緝詐欺犯罪徒勞無功。近來打詐相關法律的修正後，金融相關部分以實名制來對抗，然而只要第一時間金流轉至國外，又因為私人企業與國際互助的缺乏下成為查緝斷點。另外車手的高替換率也是查緝的斷點之一，除了吸收少年擔任車手外，短期的外籍車手也成為詐團愛用的手法之一。即便查緝到了車手或機房，集團間彼此的聯繫亦透過難以解碼或有自焚功能的網路電話為主，喪失第一時間保存證據的契機，難以將犯罪人與犯罪事實做連結，也成為查緝上的斷點。更困難的是境外的機房，透過 VPN 不斷地跳過各國來進行發話與被害人接觸，即便能夠知道由哪國進行發話，但被害事實若不明確，要求他國協助突破機房，亦難以

成功，各種不同的偵查困境，都可以成為詐團所設立的斷點。

然後登錄網銀的IP看到的是國外的IP。而且他還會加上VPN。他的手機是香港門號連上網了，再加VPN。所以你從網銀IP回查是查不到東西的(A02-810)。

你連被害人都沒有，就問你一個問題，你東南亞的機房那邊，詐欺有沒有被害人？*(A03-1045)*

轉接的地方完全沒辦法。機房講實在，架設國外多，臺灣也有，...，就算我們警方扣到手機，要再做手機鑑識，那東西已經銷毀了...要再追上游，斷點真的是太多了(A04-94)。

就我們基層而言，我們能抓的...因為可能現在機房他們都設在國外的(A05-578)。

機房就是他的廠房，他就是設在境外(A06-131)。

詐欺集團尤其是機房他會一直在移動(A08-164)。

查緝的時候雖然查到金流匯集的水房，然而在水房的大水庫當中，是許多詐騙集團或其他匯兌的集團，該如何證明大水庫中的那些金額是屬於詐欺犯罪的部分，變成是查緝上的斷點。況且多數的金流都轉往國外，國外的幣商也無配合之義務，根本無從查起。即便是傳統的大車轉小車，金流也都快速的打散後由車手提領或是轉到虛擬貨幣購買，對於查緝人員來說，追到第二層或第三層就無法繼續，都是詐團設立斷點的考量。

我們的經驗來講，從被害人這邊，找到的頂多車手或水房層次，沒辦法到機房層次(A01-455)。

它是一個託管錢包。它是沒有辦法去追蹤幣流...它是不會公開上鏈(A02-140)。目前剛上路，我們還在做打擊個人幣商的一個過程當中(A02-202)。現在換成另外一種模式是，有通過認證的這些公司用他們的名義去開店。

就是他們都同一家公司，比如說幣O公司好了，它開了台北分店、台中分店、台南分店，都是用同一家門市、同一個統編、同一個招牌。詐團可以去跟這些實體門市去申請一個電子錢包。然後我就假借這個方式進行洗錢(A02-223)。到外匯的地方的時候就沒有辦法查(A02-282)。

向上溯源到水房去？他們會設斷點，不一定有辦法知道。用 Telegram 的一個控台。...兩個拿錢的人是不會對接到的(A02-661)。警察抓到車手只跟你講個綽號，一定要看照片才認出來是誰，這時候就是斷點(A02-677)。

外國的可能就比較沒有辦法，我們也要考慮一下國情問題(A03-606)。

現在是很困難說，沒有辦法有一個金流去把它串連起來(A04-285)。

還有一些錢包連交易所都不是，所以也都調不到資料(A05-160)。

現狀就是很多集團的錢會匯到洗水的公司，然後他再洗出去嘛。所以他就像是一個銀行的概念，這些錢根本就是很多人的錢，很多詐騙集團的錢都放在這裡面，所以他也不會去明記說你這一團多少錢，他也不會寫，所以到後來還是你要去證明的問題啊(A08-662)。

即便抓到了車手，查扣了手機，但當車手甚麼都不說的時候，只能透過手機鑑識來進行下一步，如此拖延戰術下，耗費更多的人力與物力，更重要的是無法在第一時間向上溯源，致使愈多的被害者出現。加上現在吸收相當多的少年與境外人士擔任車手，這些都是詐騙集團善用的斷點。

現在能用的就是手機鑑識，他不講就得破解。破解完後要跑報告，還要依依看報告，你看你為了一個案件要花多少時間(A04-377)。

你今天回去越南了，你可能下次來台證件號碼不一樣，輸進去之後，我們這裡無法比對出來是同一個人。這個是國跟國的漏洞，這沒辦法，因為每個國家的護照系統不一樣，這個是漏洞(A08-177)。

(三) 司法系統的不同步

1. 檢警院不同調

刑法上對於犯罪的認定相當嚴謹，而個體是否犯罪必須依循「構成要件該當性」、「違法性」及「有責性」等三個階層審認。電信網路詐欺行為本身行為影響社會重大，且須藉刑罰制裁，才能遏止此類犯罪的發生。其行為造成的危害巨大，非社會所容許存在價值的行為，更重要的是這類違法行為應藉由法律加以責難。然而電信網路詐欺犯罪的困難點，對於檢院來說，常常因為犯罪事實的尚未發生，又該如何認定此一行為足以構成要件，因此即便警政掌握可疑資訊，也會因無確實跡證而難以成案。檢警專業能夠在偵查階段共同配合當然是最佳情況，然而在法院審理階段則可能因為事證與見解不同而可能功虧一簣，不核發相關的搜索票或同意羈押等，使得辦案落入多頭馬車的情況。更多的情況是法官的訓練與檢警民眾的預期有落差，法官對於事證的要求相對嚴謹，畢竟是人身自由的限制，若只因為可疑而無明確事證下，難與檢警同調，常見的就是抓了又放，放了又再度犯罪。

確實每位檢察官的想法是不同的...想要拜託檢察官來指揮這個案件，...他就覺得這種很單純，就是通知車手來做筆錄就好了啊，為什麼要報指揮。那我前面的兩個案子反而是檢察官會比較支持...每個檢察官的想法確實不同(A01-140)。檢察機關依照調度警察司法條例指揮我們，很多時候我們警察的實務面想做，但檢察官支不支持就另當別論。我們會有很大的方向想要做，但是有些檢察官就有他的想法，我們只能尊重(A01-626)。

他如果去領完這個人頭帳戶之後可能錢還沒進來，因為後面還有車手要提領嘛。如果沒有被害人的話，這時候就要看檢察官有沒有支持。有人報案了，...去調超商影像然後去看是不是都同一個人去領這些有簿子的包裹(A01-037)。

犯意的問題。因為檢察官的態度是很重要的。就是一個檢察官很挺的話，

他就是會願意幫助你起訴。有些檢察官就是不想辦案，就是不要抓那麼多人，或是說用一些管轄權的方式...看檢察官的態度。然後我們還有遇到比如說，要不要羈押，這件事情(A02-843)。

司法官都很嚴謹的啦，就是說溝通好不好溝通啊...你今天抓到人之後，你給A，那A他可能問完之後，他可能機會比較少幫你羈押，因為他這案子要再分出去給他同事，他只是值班的...就是在工作上協調聯繫的問題。(A03-296)。

我們之前去某個地院申請那個票，他反而今天，有時候事證不明確，他就會直接駁嘛。有時候我。們已經可能事證明確了，我們去申請，然後法院也說：「你今天事證明確了，你幹嘛還要來申請，你就直接通知他來做筆錄就好」，因為每個法官有每個法官的做法啦(A05-688)。

很多警察那些偵查的技巧都比我們厲害，但是他法律不懂，但我們比較知道哪樣的蒐證你會比較容易羈押被告、可以去突破...法院審理也是很多問題，...那麼多事證，我們可能全組投入，但法官頂多就三個。(A06-711)。

我們的訓練就是這樣，到二、三審的那些也一起訓練的，他們思維都是一樣的，二審跟三審的庭長……三審庭長更是這個想法(A07-037)。

不管五權三權我是法官、審判者，為什麼要幫你行政或檢察官背書？條文若給有一個空間時，就不會照你的想法去解釋， 最高法院從來都是這樣(A07-135)。

2. 案件量龐大下的不得已選擇

偵辦電信網路詐欺案件是相當沉重的負擔，因應逐年上升的詐欺案件，當編制人力追不上案件增加速度，當證據調閱與取得比起過往更困難，當查緝過程無法得到支持與協助，對於我國刑事司法系統的從業人員來說，只能選擇破案可能性高的案件來著墨。

這也透露出站在對抗電信網路詐欺的司法人員的無奈，當案件量龐大，在經過仔細思考與後續破案的可能性下，若案件所涉及的人數、金額龐大，勢必有優先性的考量，這也是逼不得已的選擇。

檢察官說過他哪有那個時間，給我什麼我就辦什麼(A02-383)。實際上就是警察辦到哪裡、檢察官就看有沒有到搜索拘提的地步。然後再來是搜集到證據有沒有辦法起訴，他們在意的點就是這樣(A02-390)。

一定是配合檢察官，前段偵查是我們優先，告訴檢察官後依據內容看有沒有偵查必要，...檢察官量很大(A04-224)。

50 萬的案件在地檢署來講其實很小，我們 500 萬算多嗎？...現在是你要千萬詐騙，他才會有專案小組在那邊幫你好好的查(A06-085)。我們辦案都有節奏，我們都非常有經驗，這七十幾個人你一定要排一個優先順序，比較重要的就優先處理，沒有那麼重要的就次之，慢慢慢慢處理(A06-865)。

你分身乏術啊。所以某種程度上，你也希望說：「好啦就不要查下去，因為查下去你也沒完沒了，太多要查了」(A08-443)。

3. 證據不足下難以突破

許多受訪者都指出目前打擊電信網路詐欺的困境就是證據層面。除了上面所闡述的證據蒐集與保全，更多的是因為斷點查不到足夠的證據進行犯罪行為與證據的連結。首先犯罪需有被害人，沒有被害者報案的時候，難以成案。電信詐欺犯罪包括電信流與金流，兩個方面都需要足夠的證據，而當金流面的匿名、多層轉匯、車手、虛擬貨幣、第三方支付等，詐團多半交叉使用，使得流向難以查緝，證據不足。電信流的部分則是透過境外 IP 與 VPN 的跳島轉接，網路電話的聯繫以及機房設立境外的躲避，更難以將證據與犯罪行為做連結，常常查緝到一半就難以追緝，此時若遇到其他案件的加入，讓整個查緝工作越來越複雜，最後只能查無實證而簽結。更令人第一線人員沮喪的是跨境犯罪的證據缺乏，明知有犯罪行為，也掌握確切的犯罪地點與人物，等到破獲之後，卻因

跨境蒐證辦案的標準不一下，許多關鍵證據沒有在當下保存，而難以起訴甚至定罪。

擴大沒收標的，之前就遇到詐欺犯罪所用之物不問是否屬於犯罪行為人所有，一律沒收。對查獲時無法證明，一併沒收。我們可能去搜索一個詐欺的共犯，而不一定有搜索票，其一定會請律師，那他可能會說：「你怎麼知道這個東西是我當事人的？你要怎麼去認定？」(A01-502)。

派出所都會打電話問我到底能不能抓，啊我也是打電話去問檢察官嘛，我也不能作主。其實檢察官回覆我都說：「你今天詐騙就是要有被害人」，你沒有被害人的情況下，你把案件送去他那邊，他那邊也會很難處理啦(A05-553)。

我去法律宣導我都跟大家講說，如果被騙一定要講，但是因為現在犯罪黑數，我們看大概超過二分之一以上沒有去報案(A06-152)。

高鐵下來先去嘉義面交收款五十萬，又到台南放在高鐵置物箱，再取台南這個。現場抓到時他老實地把五十萬也講出來，不過那個沒有被害者。是誰不知道阿(A07-058)？

就算他供出他上游後沒有金流佐證，有時候長官是不願意因為單一證去搜...連拘票都不一定會給(A02-471)。

印尼回來的，也是一百多個人。對，然後那時候，我們刑事局有支援去問筆錄，問完筆錄之後是不是全部放走。但是放走之後，後面扣他們手機又花時間抓回來(A02-791)。

你碰到檢察官支不支持？檢察官支持，法官支不支持？聲押，你做了...一個禮拜沒睡覺，你做了之後，結果法官用一個很瞎的理由把你駁掉(A03-939)。

檢察官就一句話，補足資料，不能證明？那看你是要通知還是到這邊結案

(A04-259)。

至少要有一個準則，...，我大概要收集到什麼樣的程度，法官是願意給他。要讓大部分的案子，它有一個一致的標準(A05-719)。我們有發現他的問題時，可能都是一大堆人，如果沒有人報案的話，我們警察其實也很難發動偵查，因為這樣可能長官也會覺得你在辦失案或什麼。我們可能也是要有一個偵查的依據(A05-451)。

有些熱心的民眾，他可能接到詐騙訊息什麼，他會很熱心的打去 165，人家說這個帳號是詐騙集團。沒有一個實體的依據，你沒有辦法去限制人民太多，就像我今天什麼犯罪事證都沒有，在銀行那邊，他不可能說無緣無故、他沒有紙本文書，他就直接說我要把你的帳號警示(A05-460)。

你就算找到人，你也需要金流去證明是這個人的，不然你要怎麼說這是他的(A06-294)。你說你要個人責任，那你舉證？你扣押裁定你好裁嗎？而且扣押裁定他要寫裁定(A06-705)。

很多法官沒看到，因為檢察官那邊就不起訴了(A07-199)。金流都沒有要如何論告？這不是讓人上法庭被律師電的嗎？而且這種案子如果在台北的話更不得了，北部的律師又更狠(A07-204)。

現在講五千算客氣，有的人說他沒拿到。就任由他說的。之後論罪時他沒有犯罪所得就減刑了(A07-540)。

刑事訴訟講的嚴格證明，就是說你證據要到沒有合理懷疑的程度，這個時候就沒辦法了啊，因為這個確實有合理的空間嘛，除非你檢察官要舉證證明說就是我幹的，不然的話法院只能判無罪，因為這邊就是證據不足(A08-326)。

是你比較難突破他欸。他只要一句話否認到底，你就會查到死欸...，他會

說：「我只有參與今天這一次而已，明天那一次、後天那次我沒有參與，你怎麼可以說他咬我，就說那兩次我有參與，我沒有參與，我就做這一次啊。這一次我認，那一次我不認啊」，又是一團爛帳(A08-368)。

在外國……無罪的機率就會變大(A07-098)。

反正我不會再來台灣。可是問題是你這樣等於債留台灣啊，你這樣等於造成很多案件癱瘓整個台灣的司法體系而已(A08-168)。

我上面的人在外國遙控，你根本就不知道我啊，所以你要找到完整的證據證明說是由我指使，我是這個詐團的主謀，這難度非常高(A08-269)。因為這邊證據門檻很難、很高，很難證明(A08-683)。

偵辦案件的過程中，大量的案件已經造成第一線檢警人員的工作量，而刑事司法的起訴程序因犯罪人的戶籍地不同，使得同一案件可能有不同地檢進行偵辦，資源的重複與浪費，更加重第一線偵查打擊詐欺犯罪的負擔。

因為依照刑事訴訟法他是被害人的戶籍、依照管轄地，除非我們知道嫌疑人住哪裡。我覺得是資源浪費啦，坦白講是資源重複性的浪費，而且會影響偵辦的程序。所以我覺得這可以協調，但還是要回歸到立法，要有法律依據，因為詐欺集團尤其是機房他會一直在移動，那要怎麼協調電信詐欺我到底報了指揮是要由 A 地檢署還是由 B 地檢署，我覺得這是要由立法者去立法、修法(A03-166)。

要再走另外一個程序，另案的又要走另外一個程序，所以其實這個很難一下子解釋完。這個我們也是常泡在這裡面(A03-418)。

緊急上線。到最後還要報，每天兩天一次這樣報，不可能啊，怎麼可能這樣用。刑事局要使用 M 化車，都會要求監票要過，通訊監察處要過，才會讓你使用(A04-114)。

我覺得有一個麻煩是，犯嫌的戶籍地很重要。到最後，車手、水房那些跑各地的，就會看戶籍地，另報指揮，...一個高雄的案件可能得跑台中、彰化，可能會到桃園大本營(A04-226)。現在量一大，...分散那麼多，要一通一通電話去要起訴書嗎(A04-264)。

懲詐方面以我來講我遇到的問題其實是跨轄的合作，你還是有轄區的限制，但詐團是全台灣都有洞，那像這個案子，像這個假出金集團，是我北檢，我願意把全台灣的案子拿起來辦，因為都有在我們管轄區被騙的，我有管轄權，但有一些你可能分散在各地的時候，你就沒有辦法凸顯這個集團，你沒有辦法還原這個詐欺集團的全貌，你可能 157 億變成一、兩億，然後淹沒在巨大的犯罪案件中(A06-1124)。

每個被害人有他們的筆錄，筆錄不只一次兩次，還有交易明細、LINE 對話紀錄、轉帳資料、報案資料或存摺等，二十幾個被害人有的有這個、有的沒那個、有的是警察沒送到(A07-467)。

即便抓到了這麼多的詐騙的犯罪事實，你要怎麼樣證明說都是我指使的？這是一個問題啊送到(A08-272)。

他只要不提供開機密碼，你就會查到天荒地老了...每支手機裡面都有幾萬筆檔案，我問你...你要怎麼去釐清哪一筆是哪一筆？所以那就是一團爛帳。他整個是一個海量數據的概念...那變數實在太多了，那個已經不是單純的犯罪，他已經是一個集團化的犯罪模式了(A08-388)。

四、法律抗制面

「治亂事用重典」恰不恰當？馬英九當部長時假釋的門檻有降低，當時有個理由是監獄關不下(A07-334) 。

所有的政策應當有法律最為最堅強的後盾，法律本就應與時俱進，然而新型態的犯罪手法不斷出現，針對我國當前法律不備的情況下來遂行犯罪，若法律難以跟上犯罪腳步，將難以有效嚇阻。當我們開始思考亂世用重典的時候，是否真的有效？而當政者的思維若真如此,其相關作為與配套是否有跟上這些政策的制定,而當政策已經開始施行,執行過程中是否有落實，其效率與效用是否如預期，這些都是檢視政策與相關作為的標準。

(一) 競合下的選擇

我國打詐相關法律從刑法的詐欺罪到最新的詐欺犯罪危害防制條例，不單單是罪名的定義，更衍伸出與電信網路詐欺相關的法律規範。然而眾多法律的適用，卻無形中造成檢察官與法官之間的見解出現差異，更讓第一線的警察人員在辦案過程中，出現法條使用的疑慮與困惑。以偵查面來看，對於電信網路的部分，需要《通訊保障及監察法》、《刑事訴訟法》的特殊強制處分專章、對於金流的部分有《洗錢防制法》、《證券投資信託及顧問法》，對於犯罪人的《人口販運防制法》、《個人資料保護法》等，近年來從打詐五法到打詐新四法，都是為了打擊電信網路詐欺而修訂或訂定，但第一線人員卻有不同的見解，有的受訪者認為給了第一線偵查人員辦案的法律依據，有些受訪者認為法條太多造成競合狀態下的適用問題，由於這些判刑的原則下，只能選擇一個較重的法條去判刑，不僅造成法官判決的負擔，使得一般民眾對於司法懲詐的滿意度不高。

> *罪名不是問題，如果看過判決，罪名都是第 339-4 條，洗錢、組織那些都吸收或者想像競合了。第二個是保安的部分，比如說沒收或是什麼。因為刑法沒有，所以比較需要專法(A07-055)。*
>
> *最後還是第 339-4 條加重詐欺，再弄 100 個法出來也是加重詐欺...下面那些想像競合或是不管什麼五花八門的講難聽一點都是虛晃一招(A07-170)。*
>
> *有洗錢就多一個洗錢想像競合；有組織就多一個組織想像競合；有偽造文書就複製貼上一個偽造文書想像競合，最後還是……加重詐欺、洗錢、組*

織犯罪、偽造文書中找一個最重的罪，以一個最重的罪擇一個最重的刑。(A07-278)。

詐欺犯罪防制條例的大概第 43 條以下，他有很多法條其實是跟刑法是有重疊的，其實法令盡量不要有競合的問題，他會造成很多適用上的困擾(A08-584)。

(二) 強制性規範不足

法律除了嚇阻犯罪之外，還包括對於打擊犯罪有幫助的強制性力道。犯罪者會逃避司法查緝是理所當然，然而法律為了顧及法益，若傾向於任何一邊，都將造成人民對司法的不信任。對於我國在打擊電信網路詐欺犯罪的規範當中，訪談中最常見的就是為什麼不要強制下去，用法律來規範民營企業強制配合偵查，企業沒有義務，反過來說，也就正是民間企業力量大，才需要民間企業的協助，若是為了社會安定，所有的受訪者都認為應該要有強制性的規範，阻止這類造成巨大社會成本危害的犯罪行為。

臉書跟 LINE 我們有綠色通道跟紅色通到這個緊急調撥方式，那我們可以透過 165 的系統直接通報而跟日商建立一個對等的平台或是和 META 公司，跟他們說這個帳號是詐騙的，請你馬上阻絕他的使用權，就不會有第二個人被騙了(A01-117)。我們受理到不少案件發現這個 LINE ID 不是誰誰誰也被騙，怎麼還繼續在騙，導致民眾一直被騙。……立法權上的問題(A01-128)。

如果他公司不配合，我們也沒辦法去突破(A03-174)。那有些如果公司合作不是這麼好的話、他覺得他賺錢比較重要的話，他就是給你軟釘子吃(A03-910)。

如果你詐欺很嚴重的時候，那有沒有必要針對特定，LINE 啦、IG 啦這些通訊軟體，去取得修法上，要強制遵守國內規定，才有辦法去解決講的這個(A04-416)。

政府的力量是有限的，但民間的力量是無限的，但是因為司法機關有時候...(A06-1160)。

政府應該可以跟臉書談，因為 LINE 以前也是不提供，法官用搜索票去調就妥協了，不然他們以前也不提供(A07-233)。

請你跟我講哪一條義務，對不對？所以你看相關立法都不敢命他提出，頂多就是說：「你要協助刪除，不刪除，我就處罰你這樣子」，他也不敢說：「你有配合調查義務」，他頂多只能夠說：「拜託你下架，你不提供我們資料就算了，但是你就幫我們下架，把傷害降到最低就好了。你不下架，就處罰你」也只敢這樣而已啦(A07-891)。

強制性規範也能夠在司法系統上略窺一二，由於司法管轄權的問題複雜，也連帶使得刑事司法的整體程序拖延。也因為於法律強制性規範的不足，迫使難以在第一時間內進行通聯監察與調閱，雖然目前對一些社群軟體公司有強制規範配合義務，但其規範並未有具體且詳細的作為，這些民營企業公司，實際上也是配合，但時效上仍無法配合我國刑事司法系統的需求。包括 LINE、臉書、google、Apple 等國際大企業，對於顧客的隱私是相當注重，倘若真的配合各國法律的需求，恐損及客戶權利而用戶數驟降。

因為詐欺集團尤其是機房他會一直在移動，那要怎麼協調電信詐欺我到底報了指揮是要由 A 地檢署還是由 B 地檢署，我覺得這是要由立法者去立法、修法(A01-165)。「要有法源」，一定要從法源去立法，去找那些外商公司去立法。因為你要在我們這裡去做使用，我們可以在合理的比例原則之下去立法(A01-295)。

像 LINE、像 Apple，都常常遇到這個問題(A02-597)。

公司也是勉強配合，那程序很麻煩，要拿搜索票，而且 LINE 公司叫你三個月後再來，不是馬上。通訊軟體這塊完全沒輒(A04-350)。

幣商，或是那些交易平台，很多也不是國內的。那問題又來了，我們的法令能不能夠約束這些人，我這些幣商在國外，在美國、在中國、在大陸、在別的地方，你的法令我需要遵守啊？我不遵守，你會怎麼樣？我不遵守，你也是透過 app 來跟我交易，你也處罰不到我，我人在外面啊(A08-831)。

通保法在我當檢察官早期還有用，因為當時他用通訊的時候，到後來有 LINE 通訊軟體出來之後，通保法幾乎已經變成一個掛在牆上的法律，因為通訊監察在 app 這種通訊軟體已經不適用了。他已經超過我們的科技範圍了，以前是因為掛線監聽還可以，所以才需要通保法，現在已經無法監聽了，既然是一個無法監聽的技術，你設這個法律幹什麼(A08-742)？

另外電信網路詐欺所涉及的犯罪行為相當多元，除了電信的人頭電話號碼與金流人頭帳戶之外，國內對於移工的逃逸與其相關衍伸的問題都無強制規範，而移工歸屬管轄並非法務部，若無法杜絕逃逸移工或非法來台的外籍人士，這些問題就無法獲得有效的解決。

就是外國的，不管移工、旅客來台越來越多，可是你相關的這些法令建置不夠嚴謹，你有沒有強制捺印指紋？或者是強制建檔？或是其他的生物特徵建檔？沒有的話，你根本找不到人，這些人一進來台灣之後可能就逃逸，變成逃逸移工(A08-195)。

個資法當然是強化公務機關或非公務機關對個資的使用，但是這邊的話，...就是你要有證據證明說他有非法洩露個資或利用個資的情形。...你要去從你的這邊去往上追個資是誰給你的？這邊可能會有一個很大的問題。那你願不願意把你的個資洩漏來源講出來？是個問題(A08-478)。

(三) 懲戒度難以嚇阻

古典犯罪學強調刑罰嚴厲性、確定性及迅速性將決定刑罰嚇阻效能，而法律其中一項的功能便是嚇阻，因此法律刑度的嚴厲性具有關鍵的嚇阻犯罪效能。目前我國法律對

於電信網路詐欺犯罪來說，包括刑法的詐欺罪、組織犯罪、洗錢防制、詐欺犯罪危害條例等，其刑度最高可判刑到十二年以下有期徒刑，得併科新臺幣三億元以下罰金，其刑責相當重。受訪者多數都指出目前我國對於打擊電信網路詐欺集團，多數只能懲罰到車手層級，多一點包括水房與設立在台灣的機房，想要追查到上游、境外機房甚至是金主，相當的困難。也因為車手被逮捕的較多，才會造成詐團處心積慮的想要找各種方式來讓車手源源不絕，當抓不到幕後主使者時，對於他們的懲戒嚇阻自然效用較低。

此外，法院量刑的標準與國人期待不同，復歸社會的想法反而使得嚇阻力降低。從檢警對於緝詐的努力可以了解詐欺對於社會的危害相當巨大，由於跨境機房成員的資料與證據難以保全，檢警認為辛苦抓回來的，常常因為證據不足而難以羈押，甚至到最後判刑的刑度相當低，對比詐欺的犯罪所得來說，似乎是相當好的一門生意。主要還是因為法官的養成培訓基本上以社會復歸為主要目標，若是一昧用重刑懲戒，除了造成監獄壅擠的情況外，矯正教化是否真能跟上仍是一個未知問題。另外量刑多寡是端看證據是否明確，由於證據取得困難與保全不易的狀況下，或是沒有直接且明確的證據來與犯罪行為連結，法官自然而然量刑只能依照證據程度。若量刑低於犯罪者的期望，相反來說就是增加下次出獄後的再犯可能。

要再往上呈現一點，主謀的部分，這個就要很大的...(A01-435)。

可能賺快錢習慣了，他們不會想要回去(A02-796)。

警察可以抓人頭帳戶，也很好抓。但現在問題是在於檢察官不好起訴，法官不好判(A03-698)。懲詐喔，懲到車手而已(A03-825)。不太奢望在辦案件用「阻攔」這件事情。犯罪還沒成功、只有犯意。可是最後他的法律沒有到這麼重大的損失的時候，反而我這最後判他罪沒有辦法定他這麼嚴重的罪，反而要等他真的有犯罪的結果出來了，他又有犯意(A03-997)。

刑度不可能判得太高。我們能抓的...因為可能現在機房他們都設在國外的。我們留在台灣抓的永遠都是車手、收簿手那些第一層的...我已經沒什麼錢

生活，...，我進去關還是有牢飯(A05-577)。他第一次犯案的話，可能通常法官都會給他責付家長，除非他今天已經真的是被抓了好幾次了，可能才會押在收容所*(A05-646)*。

他第三次犯案。前幾次有被收押，沒有用。法院的量刑也是一個很大的問題，普遍都是從低度刑開始量(A06-363)。以懲詐層面來講，司法的量刑太輕了，如果沒一個案件你都從中度刑開始量的話，你承認幫你減輕，你否認幫你加重，或是說繳回犯罪所得幫你減輕，你就不會一直都從低度刑開始量*(A06-382)*。

一直在判刑，裡面關不下有什麼用？(A07-336) 第一個已經沒有外國的資料，剩下就是這兩個資料，但這兩個資料又不會白紙黑紙那麼清楚...這時候法官判無罪的機會大增，因為他又是一團人可能三四個，一定說自己不知道、是跟著其他人來的，甚至推給還在國外的人。(A07-115)。每個禮拜都在上演：一審判無罪，二審改判有罪，三審又撤銷發回、一審判無罪，二審改判有罪，三審又撤銷發回……每個禮拜都有(A07-491)。

人口販運罪很重，要判這麼重，我有誤判的風險，只好往無罪去判(A07-128)。白紙黑紙寫的很漂亮，但是證明不出來，因為訴訟是要有證據的(A07-197)。

他真的有拿到錢的話，他當然也希望這樣可以換比較輕的刑度，可是前提是我就沒有拿到那麼多錢啊，因為就沒有辦法賠啊(A08-729)。

此外，為了打擊詐騙，我國開始對犯罪所得實現的這個部分進行防堵與嚴懲，由於金流需要帳戶，因此對於人頭帳戶提供者也視為集團成員之一。此舉應對於人頭帳戶提供者有一定程度的嚇阻，然而目前人頭帳戶提供者問題仍存在，顯示懲戒的嚇阻力道不足。不過目前洗錢防制法第 22 條經修正後，未來人頭帳戶提供者若行為嚴重且屬實則視為正犯。然而詐團開始利用其他手法，像是求職廣告、投資或購物等騙術來取得人頭

帳戶，包括外籍移工或真的是社會底層需要錢的這些人，仍然會鋌而走險來販售自己的帳戶供詐團使用。

他找家庭代工就誤信詐騙集團的要買材料所以要先將金融帳戶給我，那就吸引民眾去誤信，這一種的人頭帳戶滿高的，現在移送都是這樣比較高。第二種你說以男性的話，假投資也會被騙帳戶(A01-460)。

人頭帳戶找來其實很多都是外籍的，不然都是公司人頭戶，這樣才能大額轉帳(A04-169)。

這些人不聽話了，集中在一起，都是先把它設約定轉帳，因為他要很快，所以他第一層帳戶之後，第二層、第三層就到國外的虛擬貨幣，他這個背景大概了解了就知道他就是要搶空，進去之後我們發現這些都失蹤人口、警示帳戶(A06-187)。

貪圖報酬嘛，我可能帳戶給你用，我可能可以拿幾千塊的報酬嘛。對那些弱勢的人而言，他可能賣個帳號賺幾千塊，他可能覺得也好(A08-139)。

現行法規也沒有辦法強制，他一定要終結嘛，也沒有辦法立法說他離境就要終止、離境就要清帳戶，也沒有這樣的規定嘛。 (A08-160)。那些來台比較久的，可能越南籍或印尼籍的、他可能已經取得居留證的、他可能已經定居在台灣的,那他就會做什麼生意,就用我的名義去買很多車子或機車，然後租給這些同鄉的人，我就收租金、收錢，但是沒有過戶喔，因為他們無法過戶(A08-202)。

由於目前法律越修越嚴格的情況下，對於詐團的贓款落袋相對較困難，詐團開始對於車手的部分著墨許多,目前詐團喜歡吸收少年與外籍人士擔任車手,因為其特殊身分，常常不是抓不到人不然就是證據不足又釋放，所以嚇阻的作用有限。另外詐團為了了解辦案進度，因此目前出現有許多律師協助詐團車手，詐騙集團為了能夠了解辦案進度以及獲得更多的犯罪掩護，以高薪來吸引公務人員、律師協助了解案情。而金融機構的內

控失靈，國內雖有法律對其規範，然而卻只有相關的行政罰則，沒有刑事責任的話，強制規範力降低。

其實他們車手被抓的時候，有時候請的律師，其實都是他們上手幫他們請的...那些做車手的，他們都會要求他可能就是證件的正反面都要拍在那個...拍照上傳在那個 Telegram 群組裡面。他們就會忌諱說可能地址，詐騙集團那邊都知道。會不會被尋仇報復這樣子(A05-281)。

有些聽得下去的其實會改。聽不下去的，其實你放他出來以後，他也還是會繼續做到成年，然後成年繼續做到被抓到，也是一樣就直接進去關(A05-666)。頂多就是關幾年，然後也是家長在賠啊。如果真的要賠，對方的話，也是家長(A05-672)。

我們在衝那個水房然後他們蠻囂張的耶，弄死三條人命，你又重啟不知悔改(A06-446)。

從那個案子開始，傳統的機房、水房、系統上還有車手集團，從那個案子開始我不只發現公務員涉案，還發現律師涉案，那個案子我有抓到律師，洗錢跟洩密(A06-477)。

詐團他們覺得說這個律師可以洩密，可以幫我盯著，然後他把卷宗都影印給我，規避查緝(A06-501)。16 個律師，都是去幫詐團盯場、洩密，拍聲押書還是裁定回報給詐團，控制他的偵查進度。我洩密給你我賺 500 萬，...，我一下就撐過來了，有沒有嚇阻力？沒有(A06-582)。

有犯嫌落網了，他派律師去辯護，甚至看裡面的資料去拍給他(A06-548)。

四年的假釋執行率大概七成，大部分的案子都是關四分之三就洗白(A07-349)。

判一判，你就回去了，對不對？之後上手再把錢匯給你，對不對？他有賺錢，你也沒有吃虧，你只是來這邊關幾個月，其實你也沒有吃虧啊。所以他已經一整個是一個跨國性的問題了(A08-220)

金融機構，這個我們現在在實務上有沒有真的...因為我看的這些好像都是處罰鍰嘛，都是行政法，他沒有刑責...裁罰的動作，他只是消極的一個處罰，他沒有辦法積極的去預防。(A08-511)。

(四) 偵查犯罪的法律與專業支持

打擊電信網路詐欺犯罪，讓第一線的檢警調能夠全心全力去做，除了行政單位要全力支持之外，更要依法行政。所有的行政程序要有法律依據，雖然從打詐五法到打詐新四法，舊法修訂與新法制定，都是給予刑事司法系統強力的支持，然而修法之後如果沒有落實，缺少相關配套措施，沒有檢視實務程序上的檢視，會讓第一線的人員將該法條束之高閣。最常見的就是當要求其他企業或機構協助調查時，常遇到沒有法律規定而鎩羽而歸，也常常因為證據不足而無法核發搜索票，但反過來看，如果證據確鑿，又何須搜索，因此陷入父子騎驢的狀況。加上刑法無合理懷疑證據原則，讓法官難以重罪嚴懲，使得原本一體的檢警院，加重了彼此嫌隙程度。

我就跟他們討論說他們可不可以提供資料？他說那個依據給我(A02-568)。

我們最近的專案都會要求那個不法所得的扣押。因為說在他們為了還是錢。不法財產，就是那你要先證明，他的財產是不法所得(A02-690)。

法界在討論這些新型態犯罪的時候可能節奏要加快，不然會造成我們司法人員在前線抓人然後不知道怎麼辦(A02-925)。

其實法律歸法律的修正，其實系統的建立還是機關間去協調(A03-367)。法律的要件是你的客觀跟主觀都要有。我們客觀知道他犯罪、他是人頭帳戶。那他主觀說「我沒有犯罪啊」(A03-710)。

去取得修法上，要強制遵守國內規定，才有辦法去解決講的這個。我覺得最大的難點，就是沒有辦法即時取得相關資訊(A04-418)。

你今天你雖然有修法，只是就我們基層而言，我們能抓的...因為可能現在機房他們都設在國外的。我們留在台灣抓的永遠都是車手、收簿手那些第一層的(A05-577)。

詐騙集團是一個跨國組織的詐騙集團，你檢察官一個人有辦法嗎？所以我們現在辦案不只檢察官，主任也要去幫忙，幫忙大家才有感，甚至你整組要下去(A06-1982)。這是立法的選擇，如果沒有給我們武器，我們就沒有辦法去執行，這是一點(A06-1053)。

警政的部分跟不上，還有金管會也是(A07-213)。修法後也沒有相應的配套措施跟上去(A07-242)。有的修法是要堵三年前的、堵兩年前或是堵新的，新的不可以拿舊的來堵。有的是有偽造文書，有的沒有偽造文書；有的是有組織，有的沒組織；有的洗錢或是有未遂等交叉下來(A07-310) 。

為什麼沒有辦法判那麼重的原因，重點在於說證據的認定問題(A08-258)。

由於電信網路詐欺犯罪的工具日新月異，不管是電信技術或是金融工具等，透過各種不同策略之間的漏洞來遂行犯罪，對於檢警調的回溯偵查來說，相當繁雜的工作。訪談中也提到，檢警調對於相關新的詐騙手法與犯罪過程的回溯，所需的專業度應該同時要提升，端靠偵查隊中幾個重要成員來打詐，似乎力有未逮，若是能夠提升整體檢警調人員的查緝專業，採互助合作的方式進行，才不會讓案件負責人員士氣低落。

如果你不知道虛擬貨幣要怎麼用，你要怎麼去抓虛擬貨幣收賄？收賄其實一般來講現在都是非常私密，私密性的犯罪永遠都是最難抓的(A06-739)。案子要熟，對每一個細節要熟，其實偵訊也有一些技巧，犯罪心理學跟你掌握的事證(A06-750)。

我們在偵辦每個案子我們都想說他的策進是什麼，這不是每個檢察官都會有的概念，但因為我主任帶隊辦案，我會知道說這個案子之後要怎樣才會有用(A06-784)。我覺得譬如說現在有一些特殊強制處分過了，像是可以用科技偵查，但我覺得這都還是跟在詐團後面(A06-1046)。

你今天刑很重，可是查緝很慢，或者是查緝沒有效果的話，基本上也是沒有效果(A08-257)。

多數的受訪者也提到國內對於打詐的法律是不斷更新與修正，除了對打詐有法律支持之外，更能夠符合民眾的期待。然而新舊法之間的適用問題與重複判決情形，應加以重視。

立即的效果就是法官不行。因為光修法就要比較新舊法，三年前的要用三年前的東西;兩年前的要用兩年前的東西;一年前的新法要用新法的東西，有的未遂；有的既稅，有的一個被害人；有的十個被害人，有的是怎麼樣(A07-456)。

透過立專法來取代原本的母法，造成新法跟舊法混亂適用後，因為舊法跟新法又不是很一致的時候，這個時候法院在適用法律的時候就會產生問題(A08-587)。

因為你不明確化，每個法官在適用法律的時候會產生一些差異，因為我覺得可能法律沒有明文，「那我覺得適用舊法比較有利」「沒有我覺得可能是用新法比較有利」，因為按照法律規定要適用有利於被害者、有利於被告的法律，他就會產生判決矛盾的情形(A08-607)。

(四) 被害保護的法律保障

以詐欺被害者角度來看法律，他們只在乎自己被詐騙的錢是否能夠討回。然而根據實務上來說，贓款只要進入到金流層級，詐團透過轉匯、虛擬貨幣等手法，已經在最短

時間內將犯罪所得實踐，要回來的機會是微乎其微。目前犯罪被害補償金僅限於因「犯罪行為」被害致「死亡者之遺屬」、「致重傷者」及「性自主權遭受侵害之人」，得申請犯罪被害補償金。對於詐欺被者者的部分，也只能透過刑事附帶民事訴訟向行為人請求賠償，或與詐欺集團成員進行和解。顯然我國法律對於被害者的保障仍不足，也是民怨四起的主因。為了能夠提供更多被害者的保障，扣押與沒收制度的落實顯得格外重要，若是能夠對於詐團的財產進行扣押與沒收，納入犯罪補償金的部分，也能夠作為法律對於被害者的保障。

他們最想問就是「我被害的款項能不能夠拿回來？」(A01-526)。第一個部分，他被害人可以跟人頭帳戶求償。第二個：您剛剛所說的車手，那車手也可以去做一個求償的動作(A01-432)。我們立的這個法是為了要嚇阻詐騙集團，而且有被害人修復式司法改良主義，讓這些被害人可以做一個求償。因為我扣了這些犯罪所得，我才有東西可以還給被害人(A01-515)。

那個不法所得的扣押。因為說在他們為了還是錢(A02-690)。

被害人...其實錢也拿不回來，...當然抓到車手、抓到車手頭，我們盡量抓多少抓多少。你找他們民事求償，但是一般來講這些也沒有什麼錢(A03-1011)。

被害人也都會問我說：「我的錢到底能不能追回來」至少我們警察抓到犯嫌的時候，...你可以到時候再跟他求償」(A05-209)。

以前按照刑法，五十萬可能要發還，而打詐專法就可以把五十萬沒收。所以如果在比較保安的靈活運用上是有的，不過也是要查得到(A07-073)。

人口販運防制他修法最主要是要加強被害者保護，他加強的並不是加害者的查緝，他著重的面向是在被害者的保護(A08-393)...先賠償當然理論上可行，但是就我講的今天你抓到的永遠都是小車手，那你要他賠償多少錢...

法律上他們雖然說要一起賠，可是實際上他根本就沒有能力賠啊。(A08-707)。

否認的話五十萬就可以沒收了(A07-067)。

第三節 我國打擊電信網路詐欺實務之建議

台灣是法治國家，所以他必須要有立法的授權(A06-662)。

政府就是要去談，一定是有辦法談的，也許結果沒有到達預期，但是總是要去談(A07-238)。

回到一個原點就是：「不管任何犯罪，重刑化能不能夠遏止犯罪？」(A08-254)

法治國家的犯罪問題仍是要回歸法律為依據，若沒有法律的支持與保護，我們對於打擊電信網路詐欺犯罪的策略與實務作為，亦可能觸法，進而喪失其法律正當性。然而若一昧只覺得用重刑來嚇阻，是否真有效用，亦為討論與修正的考量方向之一。

一、修法上的建議

(一)　明確法律定義減少條文競合

罪與刑罰度應該分開來看，單就罪名來說本來就有詐欺犯罪，然而刑度卻因會打詐專法設立後而開始加重，不過刑度上雖然有增加，但法官養成多半希望能夠以社會復歸為最終目的，因此多半從低刑度開始判起，而且詐欺犯罪涉及多種法律規範，使得法官與檢察官在法條運用上相對複雜，徒增工作量。國家對於犯罪的治理並非一昧以亂世用重典的思維來管控，反而應該思考法律的修正與建立，應更明確為原則，過多的不確定概念會徒增解釋空間，從而無法有一致的判刑標準。

現在都是用第三三九條之四第二項，去年打詐專法出來以後才刑度拉高，所以其實罪名本來就有。如果是罪名的話刑法就夠了 (A07-026)。罪名都是第 339-4 條，洗錢、組織那些都吸收或者想像競合了(A07-055)。

*不是光是亂世用重點，還是要從行政那邊去處理才是一個現代國家。而不是覺得反正犯罪都是法院處理，法院判重刑以嚇阻，然後監獄關起來。如果沒辦法嚇阻，就繼續往上判(A07-040)。*不修的話他沒辦法交代*(A07-181)。*

你要嘛整個法令，新法部份好好的那個章節把他修完整一點也就夠了...很多法令都是疊床架屋，就是都是相同的東西，然後母法不去改，然後再另外弄個專法出來，然後專法的部分有些又跟他又有很大的重疊，就會造成很大的適用上的困擾。(A08-598)。任何刑法的加重其實都是...實際上的嚇阻意義其實都不大，就是最主要是象徵意義，給民眾宣示性意義比較大(A08-617)。

那帳戶不管他是什麼當秘書、轉帳或買虛擬貨幣，有罪的標準是在這兩個的中間。法院其實有降低標準，這時沒降的就會判無罪的多；有降的就會判有罪。 (A07-153)。修法時要訂清楚，最高法院的人都很精，訂的模糊他就不幫你背書，例如犯罪所得是不是指被騙的錢？面交五十萬但是我只有拿五千，那交出犯罪所得是指車手的五千還是五十萬？因為條文訂的不清不楚，最高法院就認為都定調了就是五千(A07-530)。

立法如果說要這樣的話，你就再加出一條比如說幾年幾月以前的行為適用舊法，幾年幾月以前行為適用這個法條。就把他明確化，因為你不明確化，每個法官在適用法律的時候會產生一些差異，因為我覺得可能法律沒有明文，「那我覺得適用舊法比較有利」「沒有我覺得可能是用新法比較有利」，因為按照法律規定要適用有利於被害者、有利於被告的法律，他就會產生判決矛盾的情形(A08-610)。

（二）　金流與電信的法律修訂外，更應強調數位經濟審查的落實

金融方面的法律修訂其實相當全面，對於電信與金融的業者內控與義務業已規範入法，然而法律雖有強調業者的配合義務與責任，但卻沒有任何施行細則或辦法來更細節的規範時效，尤其目前電信網路詐欺的年代，強調的就是在最短時間內完成犯罪行為，若偵查手段無法配合上刑事司法系統的需求，就可能在這段期間內有更多的被害者出現。因此受訪者普遍認為對於如何落實國內的打詐政策才是基本，而非一味的遇到問題就修法，即便法律修訂了，若沒有定期的稽核或有具體的罰則，多數企業能會有僥倖的心態。舉例來說實名制的規範，目前對於帳戶與帳號等都已入法，但為何仍然有這麼多人情願鋌而走險來做這些事，我們可能無法對犯罪人改變其思維，但可以從這些機構去思考做預防與介入的手段。因此對於防堵的電信公司金融機構除了立法要求負起防詐的責任外，更應該有相關罰則，甚至負起連帶賠償責任。

現在的問題在於明知道這個是有問題的，但是在阻絕他的時效上是來不及的。(A01-122)。要跟這些外商公司，比方說 META、LINE 公司即時通報，馬上停止這個帳號使用，而不會再發生後面匯錢或買點數卡被騙，這個「預警」就是從帳號使用上去即時的下架(A01-657)。

詐欺犯罪危害防制條例，因為可以在一個罪章，第三章的「溯源打詐執法」中針對外商的帳號通報、停止使用，因為第三章已經有加重刑責、窩裡反條款，也有擴大沒收，那是不是可以增加一個社群平台外商的責任、權利、義務(A01-670)？

你對一些平台業者有明定他們有社會責任，這件事情很重要，要給他課予相當的責任的罰款…適度課予一個相當的監督啊跟相當社會責任(A03-851)。

即時監聽我們才能同步並駕齊驅。你直接在帳戶被詐騙集團用的時候，你直接 165，把他攔阻。就不會出去了(A04-410)。

有沒有辦法把飛機（Telegram）設比較嚴謹，就是把飛機擋掉，公司今天要配合我們(A05-793)。

之前就說業者自律，為什麼我會說業者自律不可信？...前幾大的律師事務所，想說這所長不會騙人，後來一查下去，中了，應該收了詐團超過 3、4 千萬(A06-544)。個資的搜集者，因為他們很多個資得搜集...有阻絕好，就不會有詐騙，但問題是個資流通的太快了(A06-1185)。

這個查證的部分，你今天要處罰他，就是你要有證據證明說他有非法洩露個資或利用個資的情形(A08-465)。沒有實名制的話，後面救得起來也很困難。因為大家推來推去嘛，我給你、你給我，到底是誰給誰？弄到後來，死無對證(A08-124)。

倘若真的在實名與審核機制上已經做足，仍無法有效杜絕，那麼應該進入下一階段的防堵作為，以金融面來看，將對於人頭帳戶與公司帳戶的警示機制應預先反應，意味著第一線的金融機構與政府機關對於帳戶與公司設立審核嚴格實名與查證後，對於人頭與空殼公司警示帳戶的認定應趨於寬鬆，人頭門號也應比照辦理，一旦涉及相關電信網路詐欺犯罪，應立即給予暫停所有可能的營運及業務功能，亦能夠阻止詐團將贓款匯出。更重要的對於這些制度上無法落實的機構與單位，若是造成被害人的損失，也應負起共同的賠償責任。

雖然有實名認證，但是你的條件太寬廣，沒辦法去做實際上的審核他是不是有效的公司，而且是不是實際上的運作公司，還是他就究竟是人頭空殼公司？這就是需要跨部會去做協調，因為這是必要立法(A02-313)。

像人頭公司，經濟部真的要派人去看。不是成立了就好了(A04-336)。

這個帳號後面真的是實體公司，真的是有人的，因為如果公司的帳戶被鎖了，他們負責人一定會很緊張，一定會直接拿資料來打去銀行問，然後說哪個分局，他就直接來找我(A05-424)。

帳號的那個人負責的話，你敢亂洗錢嗎？今天假設通話記錄顯示是你的門號打出去的話，你敢說是別人打的嗎？就是假設那個人就是你的話，你敢亂來嗎？(A08-106)一離境之後這個門號立即失效或怎麼樣。就附個條件在這期間給你用，那離境之後這門號立即失效，不得轉送或轉門號給別人使用。帳號也是一樣啊(A08-154)。

用法律強制說他一定要負有什麼義務，然後要負賠償責任？這其實是一個很大的可以探討的問題(A08-579)。

（三） 正義的實現與人權之間的拉鋸

許多受訪人認為法律的訂定與修訂，應考量犯罪危害與人權之間的權衡輕重。犯罪預防與保安之間的衝突實為兩難之抉擇，犯罪預防著重於消除犯罪的社會根源與可能的犯罪機會，而保安措施則希望面對威脅防禦與做出適當的應對；不過實際應用上兩者很難取得平衡點。過度嚴格的介入手段可能影響民眾自由，但過度依賴預防，則可能對即時發生的犯罪束手無策，如何讓兩者互補達到最全面的安全，是相當困難的課題。以受訪者角度來看，多數是為了社會治安來考量，當有明確的犯罪事實存在，卻常因為證據的不足與難以連結，對於偵查過程與後續的量刑都產生了影響，以他們的角度來說，認為只要法律訂了有利於他們進行犯罪偵查與預防，相信破案時間會縮短。也有受訪者認為只要量刑足，自然有嚇阻作用的產生，亦有受訪者認為法院量刑應更貼近民情，量刑標準並非從低度刑責為起點，會降低再犯的嚇阻效能。值得思考的是，若是一昧地只考量刑事司法系統人員的觀點來立法，又如何建構出考量人權與社會治安之適當的法條呢？

預防犯罪跟防止危害這塊，再跟人民的通訊自由如何取的一個平衡，這些通訊軟體，去取得修法上，要強制遵守國內規定，才有辦法去解決(A04-415)。

如果法律能夠讓我們有適當的工具，可以去及時監看這一些，那我們就可以馬上去做後續阻止，或者是防止被害人被害、被騙嘛。這樣才能夠確實達到被防詐，而且讓被害人不要被騙以後，再來處理(A05-753)。

偵辦案件都是譬如說正義要被實現，而且要以人民看得見的方式來實現，讓人民看得見司法，來相信司法，...所以我說輕判文化要改變(A06-405)。

除非是 5 年 12 年，因為把刑拉高，刑法沒辦法處理，其他的都是還是加重詐欺(A07-175)。這樣法院判決的預測性、法律見解的預測性、事實證明的預測性不是大打折扣嗎？那司法的信任度會低是不是我們也要負一點責任？(A07-498)

可能可以談出更多東西，但我知道也許會有疑慮，就是侵害一些權利...一些行政措施上可能是有必要的。(A07-255)。

保障人權。相對的就是說，你這邊你要證明說他有犯罪的時候，你就要想辦法提出更高的證據去證明說我說謊，只是說在目前這種科技犯罪氾濫的年代，舉證門檻會變得非常非常的高(A08-331)。我用比較高科技的方式、用節省警方成本的方式，這樣也叫侵犯隱私權？我個人是覺得太 over 了啦...(A08-920)。

（四） 法律、科技與人文的妥適性考量

目前我國法律的修訂時程不斷地縮短，顯然是法律條文難以適用在新型犯罪手法上。因此受訪者皆認為法律與科技的落差是否能夠補足，在虛擬貨幣尚未納管之前，就是個三不管地帶，讓所有打詐第一線人員根本無從偵辦與預防。隨著金管會分四階段納管虛擬資產業（VASP），目前也進入最後立專法階段，此舉顯示對於詐欺可能的工具都開始立法進行管制，也更凸顯出我國立法都是因為犯罪情況嚴重後，開始進行相關修法進行規範，不過也顯示出詐團手法都處於領先地位，不過立法能夠兼顧科技創新，已經是邁出一大步了。

兩年前對於虛擬貨幣的防堵是毫無目標、目的的，因為當時還沒有所謂的打詐新四法，虛擬貨幣的幣商滿街都是，且民眾無法辨識真假(A01-320)。

科技的進步跟法律，法律能不能追得上科技進步的問題(A05-795)。

虛擬貨幣的發行、上架跟交易，或是這個VASP 業者的成立，之前都沒有規定，他募集一個東西他可以賺幾十億，沒有人管(A06-533)…你就把它想像成一個公司，他要進化，檢察官也要進化，懲詐也要去進化(A06-963)。

以前幣商金管會說不歸他管，財政部也說不歸他管，大家都不想管(A07-213)。

*他技術走在你前面啊，…看技術變得這麼高超的時候，你的舉證門檻，很難啦，很難啊(A08-780)…*法律沒有到那麼嚴格的時候，你如何去規範？這就是一個很大的問題啊*(A08-824)。法律概念思維要整個打掉，就是 AI 進步，我們很多傳統的民事、刑事的概念真的要整個要砍掉重練(A08-844)。*

台灣目前出現了許多律師協助詐團的事件，許多律師禁不起高額報酬的誘惑，為詐騙集團的車手以及成員擔任辯護律師，透過律師的專業來協助詐團了解目前檢警的辦案手段以及進度。過去詐團只對於轄下的機房、水房車手等成員進行各種斷點的設立，再對於各種新穎的電信與金融科技進行了解並利用，但萬萬沒想到現在詐團為了能夠了解檢警辦案手法與進度，開始以高額報酬來吸引專業的律師協助為旗下的犯罪成員進行辯護，甚至在替詐騙集團辯護的過程，利用職務之便接觸偵查卷證和律見被告，協助詐騙集團製造斷點和切割，阻礙檢警追查。本該保障人權、實現社會正義及維護司法尊嚴的律師，為何會選擇知法犯法？未來在修法上應該對於協助詐騙集團的相關人士，給予應負起的的法律責任與懲戒，當然絕非僅止於律師，而是在整個詐欺犯罪的過程中，未善盡責任而故意導致詐欺犯罪的各個機構與人員。

因為詐騙集團也要請律師幫車手(A01-473)。

詐騙集團如果敢，工程師、幣商、律師都可以給費用，就這樣子啊(A04-269)。

我們有遇到一個問題，就是其實他們車手被抓的時候，有時候請的律師，其實都是他們上手幫他們請的(A05-273)。

有犯嫌落網了，他派律師去辯護，甚至看裡面的資料去拍給他，然後後來還說給你一筆錢(A06-547)律師法的修正，這個要配合律師倫理規範，刑責把它加重，這是第一點。第二點就是...要加強律師懲戒的即時性、有效性。(A06-598)。各大專業人士懲戒委員會裡面沒有這種概念，所以這個叫懲戒的有效性，你要去分析他侵害的法益裡面嚴重性、重要性(A06-635)。譬如說無期徒刑，他會警覺，我破案了，那 302 條加重罰則(A06-1015)。

二、打擊犯罪應借助科技的協助

從訪談中得知，多數第一線偵查人員苦於案件資料量大而苦無效率，雖然目前有許多大數據資料庫可以運用，然而對於第一線員警與檢調來說，並非只偵辦電信網路詐欺案件，上有其他類型的犯罪案件要負責，若沒有類似助理的科技手段協助，光是下載大量的資料，仍需要進行異同性與模式分析，對於辦案效率是一大阻礙。若是能夠引進 AI 人工智能來協助進行大數據的分析工作，或是利用人工智能去判斷可能的詐騙廣告或資訊等，都能夠對於打擊與預防詐欺犯罪有莫大的助益。此外有鑑於目前電信網路詐欺偵查所需的資料能橫跨多個部會，為了能夠節省資料與證據的往返時間，跨部會的整合平台建立是必要的。然而整合的資料平台為了避免繁雜的申請程序，對於運用平台的資格也應進行審核與認定，以免造成資料外洩等情事。更重要的若能夠透過反向的逆襲作為，以詐騙集團的手法來進行反偵蒐，用魔法對付魔法，然而此一策略仍有許多爭議存在，仍需多方考量之後方式施行。

AI 目前都還沒導入警政系統(A02-1007)。

讓 AI 去學習金流判斷，或者是什麼讓 AI 去讀說哪些可能會是詐騙集團金流的行為(A05-822)。

我覺得AI是趨勢、一定要用，所以這個部分就要置建AI，但置建AI要錢，一定要封閉，這些人的AI，不管是檢察官在追查或是在後端的撰寫書類，...需要去訓練，但你要讓每個檢察官都知道，學著去善用它，學界也是一樣，其實每個單位都是一樣(A06-885)。

希望所有資料庫都串在一起，包括第一步筆錄的製作，相關的資訊把它列起來，我們檢察官就一個指令，資料庫就跑出來了，高風險名單在哪邊？然後我們很有系統地去打擊，然後我們可以去突破轄區的限制(A06-1135)。

你就把他想像成今天是一家公司，一家跨國大公司在做這種跨國業務，你覺得你把他抄掉之後，他裡面有多少帳，你有辦法分析嗎？帳多到你(A08-673)。

遠端木馬程式的植入...那個法沒有過嘛(A08-336)。

三、直向與橫向的機構協調與落實

以政府部門來說，打擊電信網路詐欺犯罪已經成為國家重要工作之一。而該犯罪型態又涉及多個政府部門的管轄範圍，從犯罪的預防歸屬各機構都應落實之外，到犯罪執行中的即時防堵屬於金融機構，延伸至後端的犯罪偵查，橫跨我國各個部會。然而直向垂直的官僚指揮系統，對於橫向聯繫的部分向來都是為之詬病之處，如何落實橫向部會的協調與聯繫，成為預防與打擊詐欺犯罪的關鍵。以實名認證來說，人頭門號現階段由國家通訊傳播委員會（NCC）管理，公司行號設立則歸屬於經濟部，金融帳戶則由金管會管理，資訊服務業務責由數位發展部負責，然而電信網路詐欺犯罪橫跨了這麼多部會，最後偵查犯罪則由內政部警政署負責，由法務部檢察部門指揮，判刑責由司法院轄下法院，教化矯正又回到法務部門，一個電信網路詐欺犯罪從預防到後端教化，幾乎所有政府機構都有涉及到，然而打擊詐欺犯罪卻由內政部警政與法務部檢察來負責，倘若各機構沒有將打詐視為本身重要業務，對於橫向部會的要求自然不會視為第一要務，時效上當然無法立即顯現，對於偵查人員與指揮辦案人員的士氣是重重的打擊。更何況立法必

須由立法院來主導,其立法前的公聽會與專家學者意見,以現階段部門的本位主義來說,若沒有法律強制性規範,只是訴諸以配合主管單位為主的法條或辦法,自然而然沒有強制力與約束力。

雖然是實名認證,但這部分我覺得就需要跨部會了,變成要和經濟部協調是否民眾可以那麼輕易地去申請第三方支付的公司?因為他們申請的精是資訊服務業,那資訊服務業營業額只有十萬塊又可以去做第三方支付(A01-305)。

金融情報機構的平台。其實就我所知刑事局應該是經濟科那邊有窗口,可是像我們在辦的這麼多案詐欺,我還沒有聽說過誰有去通報這個機構(A02-944)。

其實法律歸法律的修正,其實系統的建立還是機關間去協調(A03-367)。

所以現在就是說,各個部會有他應該要做的事情,但會覺得是不是我自己的業務(A04-203)。

如果能有一個大系統去串連各機關,這樣是最好的。就是那可能需要去協調,每個機關有每個機關的立場。因為我們的立場就是想要趕快把人抓到破案,那其他機關的立場可能就是跟我們不一樣(A05-326)。

識詐、堵詐、阻詐、防詐跟懲詐五個面向你說夠不夠用?我覺得其實非常夠用,你只要有落實就會奏效(A06-649)。目前來看這個可能還是要去落實,我講的是落實,主管機關要去落實(A06-1059)。

所以說「刑」才有用。拉高刑後因為刑太重,就要給他強制辯護的律師當配套措施。第二個是原先查到奇奇怪怪的錢按照刑法是不能夠沒收的,可是按照新的法律可以沒收。第三個是有一些修法對行政機關要做一些措施時比較有依據(A07-301)。目前能夠做的就只有這裡,檢察官要的證據就只

能蒐集到這邊。要看行政機關有沒有齊心啊...至少有立下法條...行政機關要齊心，證據要找的明確。(A07-434)。

一、多元教育宣導管道

因為不管是毒品、詐欺，或是各種犯罪防制，大家都很清楚這個查緝只是最末端的做法，如果說你從根本源頭沒有給他做一個法治教育的宣導，加害人這邊他如果說沒有守法觀念，被害者這邊沒有防止被騙的觀念的話，你後面警方再怎麼查緝其實都是亡羊補牢(A08-043)。

其實打詐綱領不管是四大面向還是五大面向，排在第一個的都是「識詐」。由於電信網路詐欺是利用網路的傳播與匿名來接觸潛在被害者，跟以往面對面的詐欺手法不同，加上目前人手都有手機，手機又都能上網，等於是利用電信的功能把網路結合起來，過去主要透過撥打電話以及群發簡訊的方式來選擇被害人，現在則是透過各種不同的虛假廣告或訊息在各大社群媒體上亂竄，也有許多網路購物分期付款的簡訊連結，線上遊戲點數的購買，更有許多假交友與假愛情社群的誘惑，讓各種不同的虛假訊息漫天飛舞，若沒有媒體識讀的知識素養，很容易就容易陷入詐騙集團所設立的圈套，一步一步地成為詐團的待宰羔羊。

打擊電信網路詐欺犯罪應視為防疫作戰般重要，原因無他，因為詐騙所造成的人民財產損失高達數百億，對於國家經濟造成莫大的震盪，若不即時阻止或預防再度發生，後果不堪設想。對於打詐，受訪者一致認為教育宣導的識詐層面為重點，不過仍有改善空間。雖然目前打詐綱領中的教育宣導涵蓋全國官方機關，然而國人手機使用習慣與接受資訊工具的落差並未完整考量，像是年輕人愛用的社群就有相當多的防詐宣導，然而中老年人對於手機的依賴度不高，觀看電視的比例仍高，但限於電視廣告的費用較高，難以全天候高頻率的宣傳。受訪者提出一些對於未來教育宣導的策進措施，從日常生活中出現的場域出現警語與標示、校園中、社區活動中心與軍隊這些政府單位能直接令達的機構著手，進而擴大到超商、金融機構、大眾交通捷運、觀光區域等，在人潮越多的

地方進行靜態的宣導，能接觸到的人群更多。網路電視上的動態宣導則透過各種情境劇本來製作短影音，透過全民防詐網上面的各種最新的詐騙手法與劇本來加以拍攝成影片，投放置電視新聞、影音平台，藉由網紅以及時下年輕人與中老年人喜好之名人作為主角，吸引大眾目光後才有繼續觀賞下去的動機。甚或是提出如同防疫期間的每天中央主管機關的相關疫情資訊彙報，讓民眾知道最新詐騙訊息並時時刻刻注意可能的詐騙手法，深植各種防詐意識。

每個月編排固定的場次在鄰里街坊道路去做一個廣告宣導...回到校園去宣導毒品跟詐欺...成功嶺向新兵役男宣導什麼是詐騙 (A01-220)。我們全台灣的宣導場次絕對是夠的，比方說我們看電視或是搭捷運都能看到警政署的一些廣告，網路上也是會有一些廣告(A01-234)。被害人發現你被騙，要馬上告訴警察機關，警察機關就要馬上通報銀行，銀行要馬上把這個帳號停掉(A01-494)。

針對這些年紀比較大的族群，針對他們的特性，去做宣導...至少先從家人朋友這邊去告訴他們。就是吃飯的時候、聊天的時候(A02-525)。政府或刑事局都已經花很多力氣了。有時候車上聽電台常常都在講這個。刑事局還有編一個預算是演八點檔，然後來告訴這些中老年人詐騙的手法我覺得在這一塊上已經花了很多力氣。剩下就是可能家人間互相提醒，就是不看電視的人(A02-508)。

請去鄉土劇直接演出來給大家看。你不用在另外花錢去拍個類似鄉土劇的東西，你就叫鄉土劇演就對了(A03-450)。民力無窮嘛，譬如說剛剛銀行那個嘛，那你說計程車可能也有廣告(A03-485)。

只是宣導說不要去當車手。那這些簿子呢，簿子交出去會涉嫌刑法，人民就會警惕(A04-435)。

我覺得應該就看那種社區座談會的時候，那種可以加強宣導，然後還有平常可能公務機關的那個 LED 燈那些，可以去放一些影片，就是可能告知民眾說如果有可疑就要撥打 165 什麼的。他們都會拍那個影片，那影片可能有些就比較有趣一點，民眾就比較願意看。然後有一些就會分享，就會增加那個觸及率，對我覺得這個是還滿有效的(A05-337)。

我去法律宣導我都跟大家講說，如果被騙一定要講，但是因為現在犯罪黑數，我們看大概超過二分之一以上沒有去報案(A06-151)。

我舉個小例子，3、4 年前當全台灣疫情大爆發的時候，各位還記不記得陳時中每天都會出來，中午 1 點多會出來開個記者會，今天染疫幾個人、隔離幾個人等等，然後教導民眾怎麼洗手、洗肥皂幹嘛的。你不是醫療專業的人，你待一陣子被洗腦久了之後，你也知道怎麼洗手、洗肥皂、怎麼樣戴口罩、怎麼樣隔離，你都懂。那相同的道理，你如果說電台每天一個頻道就跳出來，或是強制新聞裡面插播五分鐘做防詐的宣導，每天新聞一打開就有那個節目(A08-065)。

他手法在變、方式在變，你可能半年才講一次，可是半年前的方式跟現在可能不一樣啊，你說現在要什麼防止交友，他管道、方式又換了，你講的是半年前的模式，人家已經不用這一套、又換新模式，你用舊模式來宣導，沒有用啊，因為民眾被騙的是被新模式給騙的，然後等到你這個懂了之後，人家又換新模式了或是換新的管道。所以你如果說沒有辦法馬上即時的去更新你的宣導方式的話，民眾是無感的(A08-081)。

另外除了民眾防詐之外，受訪者亦提出其他的教育管道作為，首先是金融人員是防詐意識提升，目前許多假投資詐欺的許多都是透過面交收款，因此面對潛在被害人在大額提領時的警覺與提醒更為重要，雖然金融機構已經強化櫃台人員的訓練，然而仍有許多民眾遭詐，第一線面對被害人的關懷與詢問更為重要，雖然會遭到被害人的激昂以對，

時常破口大罵或者是口出惡言，然而能夠成功阻止被害人轉匯應為首要之務。第二是對於警察新興科技與查緝專業的教育培訓，目前多半警察的專業知能強化透過線上課程的學習，然而如果能夠有實體講師與實際操作的專業培訓，甚或是有查緝經驗專業的人員隨時提供專業諮詢，對於警察查緝上能有相當的助益。最後是對於相關司法專業人員的培育應給予更多的支持，近來詐團以高薪報酬吸引律師協助，不僅讓法律專業人員的養成打上問號，使得一般人對律師的印象也大打折扣，除了對協助詐團進行非法行為的律師處以刑責之外，更應從源頭進行倫理教育，讓律師持為實現社會正義的推手，而非向下沉淪的定錨。

我覺得成效是來自於金融從業人員的敏感度，要去想為什麼在同一間郵局中會有人員阻詐成功，又有人員阻詐失敗，那就是訓練及人員的精明度(A01-247)。檢察官去偵審的案件是最多的，會比警察更多，那檢察官能不能定期去跟警察機關或民間（公司協力的部分）宣導詐騙有哪些、怎麼去防範……我覺得以檢察官更高的層面來跟民眾講，會比我們警察更加有說服力(A01-627)。

《詐欺危害防制條例》其實目前來講...行政機關執行監督的部分，目前應該是還在做一個...宣導(A03-858)。

警政知識聯網系統裡面，他有線上的課程，他就會叫我們去上課。就是很多其實因為你沒有一些講師來講，你沒有辦法吸收進去。那很多基層同仁因為時間也不夠，可能有些就是又請人家來考試還是什麼，所以你可能表面上說我們那些課，我們同仁幾趴都有去上都有考過。但其實很多對我們同仁來說，都是一知半解。如果可以就是多請一些講師來上課，因為就我知道，就是我們有些同仁都還會自費，因為就不懂嘛。然後自費自己去找講師上課，那如果國家在這個資源能夠多給我們一些經費(A05-813)。

這個跟律師的制度有關，因為太多了。強化大學的法學教育還有倫理的教育(A06-337)。

二、各方協力與獎勵

政府的力量是有限的，但民間的力量是無限的(A06-1160)。

政府戮力打擊電信網路詐欺，為了能夠展現決心，從政府機關著手，除了推動各種打詐的法律之外，制定各種打詐策略並落實，然而詐團為了躲避查緝與順利達成詐欺犯罪，透過私人企業以營利為優先的原則，利用各種服務來製造斷點與尋找潛在被害人，使得詐騙目前成為國內最嚴重的犯罪型態之一。若單靠政府一臂之力，難以招架，更需要民間企業共同配合與協助，方能發揮最大的效益。

(一) 與民間機構的協力

以我國打詐綱領的實際作為，電信流以電信公司與網路服務提供者為主，金流則是以各大金融機構為大宗，數位經濟則是網路社群與大型網路公司等。這些多半是民間私人企業，且多為跨國大型企業，也因此提供相當廣泛的服務，同時為了保障用戶的隱私，其客戶隱私保密政策相當嚴謹，若不如此則會喪失許多客戶的信任與支持。從電信面的人頭門號實名制審核、大量可疑群發簡訊的阻止、境外可疑電話的攔阻、虛假訊息的傳發、強制顯示來電號碼、疑似來電提醒、可疑涉詐門號的停用等，這些做法有些已經施行中，但若能給予時效限制，方能立即阻擋；對於網路電話的落地使用必須配合實名帳號申請、未來涉詐的調查義務與時效、即時監聽與解碼技術取得譯文等配查檢警偵查義務。

以數位經濟層面來看，除了廣告帳號申請實名制之外，平台對於假廣告與假訊息的審核機制要落實並阻擋，網路購物商家的實名審核、網路購物機制的多重認證、平台個資的嚴密保護、各種付費機制的多重查核與認證、延遲付款的保障、24 小時的網站客服諮詢與查證機制、買家與賣家的實名認證等，都是面對數位經濟時代來臨的重要防詐策略。

以金融機構來看，是犯罪贓款實現的主要關鍵階段。然國營金融機構可以全權配合，私營企業雖然有法律規範的要求，若金融機構能夠配合國家打詐政策並積極協助，相信第一線的犯罪偵查人員能夠更快速的破案。除了實名制的帳戶審核機制外，不管是個人或公司都應遵守，另外轉帳次數與轉帳金額的每日限制、超商寄或購買點數的警語提醒、強化第三方支付虛擬帳戶的風險管控、虛擬貨幣的納管與專法等，目前皆已上路或正在籌畫中，受訪者皆希望未來能夠配合檢警調的偵查，迅速地提供資料或第一時間通知，讓阻詐層面能夠向上提升。

我已經知道這個門號是電信詐欺了，...去跟這些公司講，如果是已經有通報的暱稱、帳號，就應該馬上停止帳號(A01-285)。跟巡官報告的是說「要有法源」，一定要從法源去立法，去找那些外商公司去立法(A01-296)。

有些是用隱號的，就是打電話未顯示號碼的。那個被害人也沒辦法告訴我們電話號碼是什麼(A02-533)。這個像 LINE、像 Apple，都常常遇到這個問題(A02-597)。其實他們也不想管啦，因為我那時候我就跟他們討論說他們可不可以提供資料？他說那個依據給我。

電信網路通道是加密的，就算嘗試破解他們也還是會再設定(A03-166)。LINE 公司。我們政府要怎麼去，規範他們，你要進來，你就要跟我通訊監察科連線 (A03-894)。

後台一定都是可以給，有代理公司什麼的，但我不知道為什麼台灣都不做這塊，而且像之前 Telegram 被攔下來，被抓進去(A04-344)。實質背後的流程、操作業務沒辦法了解(A04-366)。LINE 啦、IG 啦這些通訊軟體，去取得修法上，要強制遵守國內規定，才有辦法去解決講的這個。我覺得最大的難點，就是沒有辦法即時取得相關資訊(A04-419)。

銀行再深入一點去追問的話，有時候那個民眾的腦筋，因為他那時候腦袋沒想那些，然後他就會突然打結，然後如果它有時候答不出來的話，就是不是可以請我們警察去到場協助說這樣子(A05-380)。

像我們有簽約的就是中信、國泰跟台新，我覺得這個制度很好的原因是因為，我們去拜會完之後，我們建立了聯繫窗口，我們的資訊可以共享，我可以把人頭帳戶名單給你，你去做自己內控、內結，讓他們銀行的這種異常金流的狀況可以減少發生(A06-1149)。

業管機關電信的方面跟這個移民署方面，如果我今天已經確定他離境了，法律就應該要規定、通知這些相關機關，要把他所有的帳號跟門號通通把他截止掉(A08-157)。現在在實務上有沒有真的...因為我看的這些好像都是處罰鍰嘛，都是行政法(A08-500)。提高一些每天轉帳的限制或次數，或是大額的可能要通報之類的，這邊比較有一個防止效果(A08-796)。民間公司，我到底有沒有義務要去配合國家去犯罪偵查？這才是最大的一個問題點(A08-866)。

(二) 獎勵與支持

第一線打詐的人員相當辛苦，除了本身的熱情支持之外，更重要的是信念的持續動力。然而受訪著都認為，當第一線正辛勤地進行打詐工作，需要的是各方的支持，不管事行動上的協助，偵查收集證據的幫忙，種種的認同並協助對他們來說就是最重要的支持動力。檢警調一體是打擊犯罪最重要的關鍵，當彼此之間有不同想法或意見時，能夠找出一個彼此都認同的規則去遵循。其次，辛勤的付出與成效有時無法同時擁有，對於這些付出相當多心力的第一線人員，希望政府能夠看到他們的努力與付出，對於這些人的獎勵應支持，除了最基本的記功嘉獎之外，不同的獎勵制度更能使的前線人員能夠更有幹勁。此外，對於提供各種不同的線索的民眾或單位、成功協助防詐或堵詐或阻詐的機構，建議也能夠有一套相關的獎勵制度，亦能夠獲得更多的辦案線索與資料，而非只

有透過法律強調應盡的義務與罰則，同時給予豐厚的獎勵與支持，才能夠有源源不絕的辦案精力。

最困難的就是這個問題，檢察機關依照調度警察司法條例指揮我們，很多時候我們警察的實務面想做，但檢察官支不支持就另當別論。我們會有很大的方向想要做，但是有些檢察官就有他的想法，我們只能尊重(A01-626)。

基本上院檢都是會願意支持的。現在的態度，我覺得院檢都滿願意支持詐欺這一塊的(A02-107)。

我們希望他們在中間是支持我們的，比如說我今天要上線通訊檢查，或是我要調通聯，調取票，然後要蓋章。那基本上我跟他報告案情、跟我給他的書類，他們可以了解我們這個脈絡(A03-253)。

今天如果去請了一、兩次都被駁的話，你可能你之後你就連請都不想請，因為我們整理那個文書也都要花很多時間。但是如果今天我們公家機關自己又站在比較嚴謹的立場，一直就是不支持我們的話，這樣慢慢的也會消磨我們警察同仁的那個(A05-723)。

你要吸引優秀人才來打詐、你要吸引資源，適度的獎勵制度是必須要啦，包括民眾的檢舉、偵辦的團隊，檢察官就不用，因為檢察官是司法官，他有身份保障，我講的都不是檢察官喔，我講的是司法警察、檢查事務官跟書記官，這一些其實很辛苦？(A06-1061)。

(三) 司法互助的突破

由於電信網路詐欺犯罪的機房有需多都設立在境外，然而境外的犯罪偵查與突破，對我國來說是欲極力突破的瓶頸。尤其是現在機房多數設在境外，即使已經知到境外 IP 位址，鑒於彼此無司法互助協定，因此無法有效的斬斷。尚須透過被害者的國家提出司

法協助，才能夠有近一步的突破。即使突破境外機房或水房，證據之間的交接也是另外一個問題，不是證據毀損就是要另外的錢，對於我國打擊詐欺實屬阻礙。

我上個月才移了十幾件的外籍人士的，全部都是通知不到啊。人都在國外，都離境了(A01-403)。

我們沒辦法去透過互助合作去找到這些機房、去抓這些人。像這次柬埔寨抓一百八十幾個人，然後都是送中國(A02-784)。

你在國外抓的所以他所有證據都在東南亞的警方那邊。都沒有，你已經先把他遣送了，那我什麼都證據都沒有，你叫我怎麼關他(A03-1049)。

轉接的地方完全沒辦法。機房講實在，架設國外多，臺灣也有...我現在臺灣不成立了，我在國外成立公司，...，被他們當地的檢察官，或什麼司法機構用到，我洗國外的我沒差(A04-045)。

國外的帳戶就...其實我們如果轉去國外，我們都會發個公文，請那個刑事局那一邊幫我們向那個國外調資料，只是後續基本上是幾乎都沒有再回來。對方國家也不願意配合(A05-194)。

跨國或是司法互助，詐欺集團都在境外，然後很多偵辦的人流、金流或是資訊的這個斷點，其實都是實際的困境(A06-1097)。

我們外交的困境也是，人家不理你啊。我們都是兩個東西－廣告在招要去柬埔寨、卡達或是哪邊做什麼，那不用錢並且提供機票；另一個是打電話叫家人匯錢，都是只有這兩種資料(A07-104)。

假設你今天是美國或中共，你去跟他要，他可能就給你。你今天去人家會理你嗎？你先跟我講一個問題，你跟我要資料，為什麼我要理你？我為什麼要理你台灣，對不對(A08-435)？

第四節 我國打詐政策的專家實務見解

本次邀請五位專家學者進行專家焦點的團體座談，從曾經從事詐欺犯罪預防與偵查事務轉戰學者、打詐中心的專業成員、檢察官、犯罪學者與法官共同探討國內打擊電信網路詐欺犯罪的政策與提出建議，本節就法律、預防、電信、數位、金流與偵查實務等面向進行探究，並提出未來可行的具體建議。

一、打擊電信網路詐欺犯罪的法規

> *從「打詐 5 法」到「打詐新 4 法」，當然我們政府在這個所謂加重刑罰的部分，這個單一事務本來是這個加重刑，那後來到了打詐，就去年年底、去年 7 月份這個總統公布施行的所謂「打詐新 4 法」，那這「新 4 法」當然就是賦予業者這個所謂管理，這個所謂就是賦予相關部會來管理這些業者的工具，把它拓展到比如說金融面、電信面、網路面，就是說課予這些業者也必須管理民間的這些網路，或是電信業者的一些明確的一個責任(E02-123)。*

從「打詐 5 法」到「打詐新 4 法」的法規增訂或修訂，多為針對整個預防或偵查電信網路詐欺犯罪所制定，從原本的「識詐」、「堵詐」、「阻詐」及「懲詐」等 4 大面向，最後針對數位經濟的部份增加了「防詐」面向，強化數位經濟產業管理，納入 AI 進行防制作為，透過各種方式進行跨境的打詐合作，對於各產業應負起防詐義務，並對這些產業進行監管，最後必須對於被害保護提出具體作為，從源頭的防詐意識做起，越多人了解詐欺犯罪型態與手法，便能夠減少被害的可能，同時讓國民的法益財損持續降低，為國人打造更安全的生活環境。

顯然我國打擊電信網路詐欺的法規層面，從嚴懲電信網路詐欺犯罪為思考出發點，發現似乎無法阻止詐欺犯罪的不斷增加趨勢，因此開始著重思考如何對於提供服務業者的層面進行管理，以及預防犯罪的發生。由於目前詐欺型態多數為電信網路，因此從電信網路業者來著手進行第一階段的防護措施。然而電信網路詐欺並非單純只有電信網路提供服務的業者，與詐欺整個犯罪過程相關的部門還有金管會、通傳會以及數發部，所以在打詐 2.0 綱要當中的防詐面向，由數發部主管相關業務，但仍然有許多業務橫跨樹發部與經濟部，甚或是其他部門，對於各部會的權責範圍仍有地方有模糊地帶，詐騙集團就是利用這些部會管轄權的真空地帶進行詐欺犯罪。

重要的是在前端這裡，包括因為現在其實是網路的時代了，當然就是說預先的阻斷是很重要的，所以等於說我們在這兩年，其實就是想辦法在不管政府高層還是立法院這邊都已經…就是說確實有跟他們做努力的溝通，我們一定要各方面的這些業者、各方面的這些部會來配合，包括金管會、還有通傳會等等這一些。(E02-132)

(一)修正後的條文嚇阻詐欺犯罪效果有限

打詐中心研究員提出目前的打擊詐欺的相關法律是否足夠，仍有待進一步地觀察，尤其是目前新法實施才剛滿一年，具體成效為何仍需透過統計數據來加以分析。顯然對於電信網路詐欺的修法，且戰且走的心態與無奈嶄露無遺，不過所有的部會與人員仍然為打擊電信網路詐欺持續努力當中。由於法律制定與修法的歷程並非立竿見影，仍有一定的法定過程，但對於第一線打詐的人員來說，似乎過於繁複與冗長，無法跟上詐欺犯罪集團的手法更新速度，更像是在詐騙集團後方苦苦追趕的樣子。像是人口販運法修訂主要為了針對詐騙集團對於他人進行剝削、奴役及利用被害人犯罪等新型態人口販運手法，將原本的犯罪態樣進行擴大，同時加重整體刑度，可以增進人權保障並嚴懲犯罪。然 2023 年 6 月 14 日總統公布修正《人口販運防制法》之後，從法院判決書中查尋人口販運與詐欺相關的數量，目前約莫 350 件與詐欺犯罪相關，對比這幾年詐欺犯罪案件來看，似乎與專家學者的看法不謀而合。此外《個資法》對於打詐犯罪的嚇阻力，也因該犯罪為告訴乃論，大大降低了嚇阻詐欺犯罪的效用。另外《證券投資與信託顧問法》的適用對象則為合法認證的投資行為，對於目前電信網路詐欺犯罪的型態來看，這些犯罪手法皆未透過主管機關審核通過，對於電信網路詐欺犯罪集團來說，似乎也是不痛不癢的存在。

這個修法的作為，到去年公布總統公布施行「打詐 4 法」以後，那當然就是說相關的法律面，你說很足夠嗎？其實也不見得啦，因為等於說也是且戰且走。(E02-141)

我們認為目前的缺點就是說立法的速度還是沒有辦法跟上這個犯罪的隱禍，因為其實我們在制定一部法律，其實歷程相當久，包括等於說三讀到整個總統公布施行，那當然這段期間可能立法、新的法可能要經過一、兩年的時間，但是事實上詐團的犯罪手法都不停的在演變當中，立法遠遠很難去跟上所謂的這個犯罪集團的速度。(E02-149)

《人口販運法》的這些規定。其實這個嚇阻我覺得效果有限，因為他主要是說要把人騙到境外去，但是問題是，台灣目前是有那種境外詐欺的犯罪，但是主要還是以境內的詐欺為主。所以他的那個 112 年 6 月 14 號修正的 30 條說：「強迫使人提供勞務」，也不過 5 年以 下，5 年以下是什麼樣的概念？跟竊盜罪一樣重。所以這個《人口販運法》的修正，我覺得對要用這個法來嚇阻那個詐欺，我覺得他的這樣的一個刑度，也沒有什麼太大的成效。(E04-936)

《個資法》是告訴乃論之罪，他全部都是告訴乃論之罪，所以你只要拿錢出來和解、撤告，就沒事了。所以這一條對詐騙也沒有什麼太大的效果。(E04-940)

《證券投資跟信託顧問法》，他雖然在第七章 105 條有規定，如果說你公眾或受益人有違反第 8 條，就是「虛偽誤信」這些罰責，可以罰 3 到 10 年。但是他第 2 條規定，本法是所謂的《證券投資跟信託顧問法》是指經過主管機關許可的《信託投資法》，那些假投資詐騙，他沒有經過主管機關的許可，所以他根本就沒有適用這個法(E04-945)

然而更重要的是刑事司法系統的效率問題，過去對於我國遭到詬病最多的就是詐欺犯罪刑度偏低的問題，由於目前詐欺犯罪數量急遽的增加，對於第一線的形事司法人員來說，是莫大沉重的負擔，意味著大量的詐欺犯罪案件對於檢警調人員來說，幾乎來到了臨界點，有鑑於刑事司法系統負擔過重，高等法院指示從九月份開始停分詐欺案 4 個月，更創設刑事「審查中心」，對詐欺案件進行預先程序審查，以嚴格控管案量，提升效率。審查庭主要工作內容是檢視上訴類型與程式是否合法，如果不符合上訴要件，即可直接駁回，在前端先篩選無須進入審理庭的案件，希冀能夠有效減少工作量。

不是只有行刑低的問題而 已，因為你判決拖太久，會產生兩個效應。第一個，檢察官、法官那邊受不了，檢察官、法官受不了之後，我 1 個月領 12 萬，結果晚上半夜做到 12 點，然後天天這樣子做，我不如一段時間之後，我轉到法官。所以你每次上法院的時候力挺的檢察官都是菜鳥檢察官，永遠都在換人，每次上來之後還要問警察，這個案件到底是怎麼回事，因為案情太多了，沒有辦法每一件下去看，所以這個就不利司法的偵辦。(E05-1104)

(二)內控管理的條文仍有侷限性

目前我國對於打詐偵查手段的精進作為不斷，由於電信網路為詐欺犯罪的主要工具，除了初期防堵外，後期偵查作為也相當重要，然而為了提升國內大詐的量能，對於能夠針對衛星定位與M化車的使用有了新的規範，讓檢警能夠利用打詐大利器來進行詐騙偵查作為。過去因缺乏法律授權，使用M化車取得的證據常被質疑其證據能力，後來為了解決此問題，特殊處分專章的修訂使該偵查手段合法化。然而實務上仍有其限制，皆需要向法院聲請核發許可書，徒增程序過程上的困擾。這也就意味著當檢警發現可疑的訊息或犯罪行為，若還要透過層層的申請，似乎已經過了最佳偵查階段。

> *《刑法》也有一條是所謂強制處分專章，特別就是那個叫做「特殊處分強制專章」，當然已經有賦予比如說我們對這個 M 化車的使用，還有衛星定位，但是事實上這個還是對我們警方偵查裡面來講，還是有他的侷限性。(E02-170)*

《詐防條例》的制定使得我國對於打詐作為有了法源依據，然雖然已經包含了多個部會，對於其他部會卻沒有納入法律規定，將可能造成管理上的漏洞。像是第三方支付部分屬於數發部，部分則屬於經濟部，人頭帳戶的運送交付部分，對於物流寄件業務的交通部，也應納入詐欺犯罪法律的規範。由於目前我國打詐最常破獲的就是車手與人頭帳戶，且該兩種犯罪成員係犯罪所得實現的關鍵人物與因素，目前雖然對於人頭帳戶的警示有積極的處理之外，若是能夠從交付工具部分來追緝，除了能夠確認販售人頭帳戶者的意圖之外，更能有效的阻絕利用物流來運送相關犯罪工具。目前最受到第一線打詐與制定政策者重視的就是企業的內控管理。這次的修法明訂了企業的責任與義務，對於金融機構、電信業者、數位經濟等面向進行修訂，不過由於法律制定所規範的範圍與時效並未具體明確，若企業對於打詐與預防作為已經盡到了企業責任，並不會對相關企業進行裁罰，不就是變相對於企業的要求只需做到基本的就好了嗎？也使得該法律對於企業的管理似乎沒有起到太大的作用。

> *《詐防條例》的部分，他現在大概是納管了 5 個部會，那其實我們觀察，其實他有漏掉一些部會，就像經濟部或交通部，經濟部他其實主要管理的是那個公司的部分跟第三方支付公司的部分。(E01-192) 交通部的部分有分兩個來講。第一個是所謂運送人頭帳戶的部分，現在人頭帳戶的部分，大部分都是透過我們所謂的空軍一號跟交貨便，那這兩個東西，一個是物*

流業者，一個是這個其實野雞車他算是沒有牌的，所以這兩個其實他的主管機關都是交通部。(E01-200)

物流寄件沒有辦法實名制？我覺得這個，不然你寄件人你有沒有辦法讓他去切結說「我絕對不是寄金融卡」，如果寄金融卡就直接推定他有詐欺取財、賣帳戶的故意啊。(E03-811) 無認證的物流啊…載車手去拿錢的人，載車手的人說「我是白牌車司機」

每次去跟遊戲公司要他們正確的身分資料，都是假的。那你至少要求遊戲公司，遊戲公司至少要要求這個當事人，他們的身分要比對、核對雙證件什麼什麼的，要再更嚴格，不然每次調這個遊戲帳號出來都是一些人頭帳戶，都是假的齁。(E04-1003)

這個害你的人是誰，這個帥哥美女是誰，弄了兩個月鑑識出來之後，給 Line 公司， Line 公司再兩個月，再經過檢察官，然後因為你沒有偵查權，那日本加上像台灣的法令，那就是要請這個合約書，所以日本的警察可以直接調閱，因為日本警察有偵查權，可是你台灣沒有，所以你要經過法官，所以也造成法官事情更多，那法官再去申請檢察官，結果跟 Line 公司要來之後，這樣過去，Line 公司又拖兩個月才給你，結果 5 個月之後給你，不知道對方是誰，因為他沒有用手機來去做，所以你都在白做。你的 Line 的部分，你要有效的來處理，這個是你社群媒體公司的責任，你有在看微信的話，你注意看微信，微信在去年已經改變了，他不再只有出現頭像跟名字而已，頭像跟名字中間他出現，唯一碼，妳的 Line IE02，所以是誰騙了我的 IE02，不用再警察局鑑識這本來就是你的企業責任，你本來就是應該要把他公布出來。(E05-1150)

(三)刑度上的爭議讓打詐效益難以彰顯

1. 刑度的提高卻難以符合公平正義

依照目前法律條文對於電信網路詐欺犯罪的懲罰來說，已經對於過往刑度過低的部分進行大幅度的提升，希冀藉由刑度的提升來增加嚇阻的效用。然而實際上實務面來說都是抓到車手與人頭帳戶提供者，對於詐騙集團的主謀與其他成員來說，這些都算是可替換的成員，只需要再招募即可，對於可能身處境外或者是藏匿在電信網路後的這些犯罪成員，透過各種層層的斷點設立，要向上溯源仍有一定的難度。尤其是刑度過低的情

況下，連帶使得國外成員都被吸引到台灣擔任車手一職，不可不重視。

這些詐欺犯行，事實上刑度都有很高，包括高額財損案件的，比如說加重他的法定刑或是說複合式的犯罪，比如說電詐集團，他所謂的複合式的犯罪就說他是三人以上，或者是利用電信網路等資通的這種手段，這一種刑度甚至法定刑都有提高到整個加重處罰大概二分之一。但是事實上，以我們實務面來講的話，事實上其實在國內做到的大部分都是車手跟人頭帳，那其實很多集團他是在海外、境外的部分，根本很難去抓得到。(E02-155)

毒品抓到之 後，是判無期徒刑、死刑等等，可是詐欺，第一個，不太容易抓到，第二個，這個即使抓到，判的刑期還是很低。(E05-1095)

因為你的刑法不夠的時候，會造成國際犯罪流動，流動到你這邊來。連你的這個外國都來你這邊當車手(E05-1251)

會造成刑度偏低的情形與《詐欺犯罪危害防制條例》的自白條款有高度相關。受訪者提到，犯罪所得的定義並不明確，成為刑度降低的判刑漏洞，由於目前對於犯罪所得的定義未明情況下，對於車手來說，只要自白說自己都沒有拿到報酬，符合自白條款又能減刑，大大降低了車手再度犯案的嚇阻力道，這些法律制定的過程中似乎沒有考慮到的層面，對於打詐第一線的檢警調人員來說，無疑是潑了一桶冷水。

《詐欺犯罪危害防制條例》的第 47 條說犯罪所得要被告真的拿到了，…所有整體車手的刑度都直接下降了，…誰知道分到多少錢啊？(E03-558)
最高法院把他解釋成說：「你只要繳回你領的，如果你沒有拿到報酬，沒辦法證明你有拿到報酬就直接減半」。(E03-561)

現在都說沒有報酬…而且還可以減刑。(E04-559) 這個法律修正下來，都是對那個行為人是有利的，這個也是一個很奇怪的一個問題。那在實際犯罪所得也是一樣，所以我們現在幾乎所有的少年，問他們報酬多少，他們都說沒報酬，現在都沒有人有報酬，他們也知道這個修法的規定。(E04-929)

這個車手在抖音裡面講，他只要騙我說我只有拿到 7 千、7 千 2 百塊，結果事實上，我騙了 26 個人，所以我拿到了 3 百萬，結果法務部也很

認真，半夜開這個假釋委員會，半夜 12 點發布撤銷他的假釋回去(E05-1078)

而刑度無法達到嚇阻的效果，主要還是法院的量刑標準不一或是過低，是許多受訪者提出的重點，尤其第一線偵辦案件的檢警好不容易將詐騙集團相關成員繩之以法，由於刑度判決不高的情況下，相較於詐騙獲利的高額報酬下卻只有少少的刑度，使得法院量刑過低成為打擊第一線偵查人員士氣的因素之一。受訪者提及法官的 KPI 績效分數，可能對判決刑度造成影響。許多法官量刑認為法條中的刑期範圍，對於主嫌才需要以長刑期來判定，然而對於集團內最容易取代的車手們，短刑期或緩刑無非讓車手們認為即便協助犯罪，犯罪所得對於刑期的相較之下，經有限的理性思考後，仍然選擇持續加入詐騙集團。雖然量刑標準在每個法官心中都有一把尺的存在，然而目前量刑偏低確實存在於目前刑事司法系統中，雖然目前我國詐防條例的出現已經將相關刑度提高，但實務上要對於相關成員課以重刑，仍需更多專業法律見解。

法院量刑過輕，這個也是一個我覺得算是會讓檢警都非常氣憤的事情，為什麼法院量刑這麼低？(E03-587) 每一個詐騙的卷宗都這麼一大疊，一到法官那裡坦承了，給你一個 1 年或是 10 個月，他案子就結掉了，他就沒事了。我們前面的人，然後還有被害人他根本拿不回，他在法官眼裡就是一個「好，我現在判緩刑了，對檢察官來說是有罪，只要這個檢察官不鬧事、不上訴，那這個案子就完美了，完美下莊」(E03-629)

最重要的這個母法的刑度，其實他沒有變。那他是 1 年以上，7 年以下，那可以併科 1 百萬罰金，那其實可以判到 7 年啊，可是那最少也是 1 年以上，至少也要判 1 年以上才對啊。可是一般法官都是從最低刑往上量，然後現在又加上你如果繳回犯罪所得，又沒有犯罪什麼，還可以減刑，就 1 年以下，我再降一下就變成 6 個月了。(E04-881)

今天這個沒有重判車手，我還是覺得是我們目前最大的遺憾，為什麼？因為如果在目前的金融環境，只要他在金融，他不管怎麼轉 帳，錢只要都在帳戶裡面，這個都可以查得到，今天之所以沒有辦法查扣是因為被車手給領現出來，領現出來彙整之後交給誰，他說不知道，當然不知道啊。(E05-1226)

2. 修訂後衍伸的可能問題

目前電信網路詐騙集團的嚴厲圍剿與偵辦，是目前我國對於犯罪政策的重點工作，也極力去瓦解整個詐騙集團。然而電信網路詐騙集團多半是跨境方式為之，目前我國較傾向於對於金流面的瓦解，主要是因為阻斷金流代表著犯罪所得無法實現，當集團無利可圖時，自然瓦解。不過目前我國多數所抓到的都是車手與人頭帳戶為主，真正的詐欺犯罪主謀似乎仍有待更積極的方式來抓捕，這也意味著無法懲罰到詐欺犯罪的主謀，顯然詐防條例與相關打詐的法律都懲罰到詐團的基層人員，包括車手與販售人頭帳戶，尤其是對於未滿 18 歲的未成年人更是難以達到嚇阻的效果，而訪談者也提到，這些車手與人頭帳戶販售者，多半也是社會上經濟較為弱勢之人，很多都是因為走投無路後鋌而走險來涉入詐欺犯罪集團，一旦這些人入獄後，高額賠償金與後續的家庭問題更衍伸出更嚴重的社會問題。

> *事實上國內這些車手跟人頭帳戶，事實上他本身就是社會的弱勢，他就是因為沒有錢找不到工作，他才會願意去當車手、當人頭帳戶。但是你用這個法，加重刑法來處罰他，甚至我們《詐防條例》在後面幾條還有說，比如說對於這個詐欺判決，比如說要課予這個所謂民事賠償的責任等等，等於說用他賠很多錢來對他的犯罪做出一個，等於說相關的一個代價，但是這些人真的能夠付得出這些高額的賠償嗎？那會不會衍生出另外一個，所謂的這個社會的問題？(E02-168)*

> *《詐防條例》第 44 條，不知道為什麼法院都不判，都不用這個加重，其實幾乎每一個詐騙都會用到，都符合啊，為什麼都不加重？(E03-572)*

> *提高法定刑，讓法官沒有辦法輕判這樣子。那為了這樣子，所以《詐欺危害防制條例》為了這樣，所以他母法沒有動，但是他後來是說，如果你同時有這個 339 之 4 的第 2 款，再加上 1、3、4 款的時候，可以加重其刑。那剛剛我們研究員講到「我不曉得為什麼不加重」，其實那是應加重，所以他是一定要加重的，但是這邊有一個漏洞，少年保護事件，他不是刑事案件，他沒有加重其刑的問題，所以少年車手，我們沒有辦法加重其刑，所以這條規定對少年來講一點影響都沒有。(E04-896)*

第二個談到的就是洗錢防制法的修正後，原本的刑度一億元洗錢額度上調至三年以上十年以下，然而其他一般洗錢的部分則從七年以下，改成六個月以上五年以下，乍看之下是提高刑責，然而實際上卻是減輕，主要是新法將協助洗錢的金額明訂下來，金額越大型度越高，然而目前我國所破獲的詐騙集團成員多為車手與人頭帳戶者，對於犯罪

過程中洗錢的金額並非集團首腦之多，顯然這樣的立法讓集團底層的車手與人頭帳戶者獲得較低的刑度判決，而低刑度的結果就是出獄後為了高額的報酬賞金，又再度涉入詐欺犯罪。更多的是，由於電信詐欺犯罪手法的多元，許多被騙的被害人相信集團出金的手法，也確實收到詐騙集團出金，然而這些偽稱「投資獲利」的出金，卻是其他受害者的贓款，如此重疊且複雜的金流，讓原本受騙的被害人不再是單純的被害人，造成更複雜的情況。

> *19 條的「一般洗錢」的規定，他是很好意的規定說，如果你洗錢達到 1 億以上，他把他加重到 3 年以上，10 年以下。問題是，一般的你要達到一億，我們在個案上並不常見，一件一件加起來是有，但是一件一件的話，很少說一次就有一億。那他的後果是怎麼樣呢？如果沒有到一億，他是罰 6 個月以上，5 年以下，但是舊法是多少？舊法是 7 年以下，換句話說，他修的是更輕，結果這個《洗錢防制法》的修正呢？我們比較新修法的結果，我們都要適用新法，因為他比較輕，他反而只要判 6 個月以上，所以為什麼判 6 個月、7 個月，即使洗錢？因為他的新法反而比較輕(E04-923)*

> *現在其實被害人是不是純粹的是被害人，我們其實在法律上有爭議，因為其實被害人他在假投資的時候，他會先收紅利，他一開始他會分到，他一定有嘗到甜頭，他才會繼續再加錢，他分的那些紅利都是贓款。(E04-1037)*

3. 修法建議

未來修法建議上，在打擊偵查犯罪的部分，都認為科技偵查是未來主要的辦案趨勢。然而號稱科技大國的台灣，空有許多科技手段可協助偵察犯罪，卻在應用上遭到許多困難。目前對於 M 化車、GPS 定位系統與熱顯像儀等科技偵查手段都已有法源依據，然而更有效的木馬程式的反向植入，卻因可能侵害人權的相關爭議而卻步。木馬程式的植入係我國的「設備端通訊監察」類似，其主要目的是在嫌犯的行動裝置上植入程式，以監控通訊軟體內容及設備其他資料。由於使用上仍需要法官裁定使用權，因此許多第一線的打詐人員在使用上仍有所保留，未來希望能夠訂出合理使用範圍與簡便的程序，因為詐欺犯罪的手法更新相當迅速，如果能夠縮短申請程序與確定範圍，似乎更能有效地對於可疑的電信網路詐欺犯罪提前預警。

木馬程式這一部分，其實還是可以做一個去研議，畢竟這對於我們偵查面來講還是一個很有用的工具。當然現在使用 M 化車跟衛星定位是法律上是沒有什麼問題的，但是木馬程式，這事實上相對的可能會對於一些人權可能會有比較大的危害，但我覺得這種工具還是可以用，但是就是說可能就是侷限在法官保留的部分，由法官來裁定(E02-179)

第二是跨境犯罪的司法互助須強化，由於電信網路詐欺犯罪屬於跨境犯罪類型，而且分散於各個不同的國家，光是資訊的取得已經困難，更何況後續的證據保全、金流過程協助等面向，亟需要跨境司法的互助。然而目前我國特殊的國際地位，只能透過「雙邊刑事司法互助條約、協定、協議」、「引渡條約」、「移交受刑人安排」、以及與代表處簽署之刑事司法互助協定等多種管道，對外請求或提供司法協助[154]，包括取得證言、提供文件、搜索扣押、資產凍結與沒收等。然而看似相互協助國家相當多，但仍需藉由外交途徑或非條約慣例處理，辦案速度與可行性受到相當多的限制，對於訊息萬變的詐欺犯罪來說，時常無法有效率地進行犯罪偵查。如何強化是相當重要的，不過在訪談中，對於司法互助的渴求是相當具體。

其實集團首腦都是躲在境外，那當然就是說，我們對於這種跨國犯罪，包括跟東南亞或杜拜這些政府如果也能夠建立更直接、有效率的情報加密司法互助協議，那我在想在偵察打擊這種詐欺集團來講的話，也是有很大的一個幫助。(E02-185)

第三個則是提到許多詐團利用開設公司帳戶來進行大額的洗錢動作，由於個人的部分有限額度，公司帳戶則能夠透過申請來進行大額的轉帳與申請第三方支付的虛擬帳號，然而經濟部維公司的主管單位，交通部則是物流業者的管理機關，這兩個部會並未在詐防條例上的主管機關，未來建議在修法部分可以將這兩個機關納入規範當中，不僅僅能夠讓主管機關有權力可進行審核與查察，更讓詐騙集團能夠利用的法律漏洞填補起來。

蠻多詐騙集團會透過公司帳戶來做洗錢，因為公司帳戶他也有一些優勢，包括他的額度比較高，那包括他可能他去銀行臨櫃匯款的時候，行員比較不會有戒心，…。那所以經濟部的部分就是，是不是有一些公司成立的要

[154] 我國與各國/地區簽署司法互助條約/協定/協議情況。資料來源：法務部。最後瀏覽日：2025 年 10 月 3 日 https://www.moj.gov.tw/2204/2205/2263/109335/109336/109341/109716/post

件，是不是要再去做提高？(E01-196) 這兩個主管機關，我們是建議是再把他放到《詐危條例》裡面。(E01-204)

第四個部分則是針對詐防條例中的自白條款。由於該條款當中的犯罪所得並未明確的定義，使得車手只要自白自己並未獲得任何報酬，成為車手減刑的條文的依據，應該明確立法必須有繳回才能減刑，而非單純只有自白即能符合相關減刑要件。

這個部分要趕快去補足啦，再重新立法把他改成、讓他…他一個車手去拿了 1 百萬，你要減輕，就是要把 1 百萬拿回來啊，他的立法目的是這樣，沒有錯啦。這個趕快補上。(E03-569)

接著是對於洗錢防制法中的修法建議，應當賦予可能的關係人的罪責，以人頭帳戶來說，大部分販賣人頭帳戶者都強調自己並未知悉戶頭被拿去犯罪使用，然而這樣的認知卻造成他人財產法益上的巨大損害，應視為重大過失，還有任何協助詐團成員的相關成員，都應納入未來修法的參考依據，從電信到金流，甚至是各種不同的工具利用等，包括物流寄送物品的 X 光機掃描、簽名具結所寄送物品非金融相關物品，只要是詐騙集團所利用的相關工具與手段，都應納入法律規範當中。

其次應針對境內外企業的防詐義務的要求與落實的方向去修訂相關法條。最主要的還是詐騙集團利用這些企業營利的前提下，透過各種不同的虛假資料、投放廣告、匿名申請、點數購買、資安要求等較為疏散之管理規範，設下重重斷點。受訪談建議未來修法時，除了將各種詐騙可能手法加以限制之外，對於各大企業的相關業務也應負起防詐的工作，更重要的是為了能夠提高打詐的效率，定期監督與審核是必要之工作，更需要明訂配合檢調單位偵查之義務，對於未配合之境內外企業，除了罰鍰之外，相關刑事責任與被害者賠償也應作為未來修法考慮的方向。

《洗錢防制法》的 22 條立法理由還是保持主觀認知，就是他事實上交出了 3 個帳戶，搞不好還有脫罪的空間。那這個部分，因為德國一直都有重大過失洗錢罪啊，就是你交出帳戶，然後你有重大過失，比方說現在很多人他們都會說我的帳號、帳戶掉了，或者是說「我也是被騙了，他說寄出去就有什麼好康，我不知道是詐騙」，那這個其實符合重大過失，因為我們花了太多時間在努力證明他有犯罪、詐欺取財故意，我覺得這真的是非常浪費時間。那我們重大過失洗錢罪法定刑可以比故意還要輕啊，但是不能沒有(E03-584)

針對幾個大公司去增加管制，或者是讓資料變得比較好調，我覺得對整個國家的社會來說是有好處的。因為現在的管制，就是那些大公司他們門號亂賣，或是點數亂賣都沒事，但是一般民眾去銀行正常領錢反而嚴重的不便。為什麼我們不把一些能量集中在一些風險比較高的地方？比方說像我去查那個點數，有五間比較大的點數，智冠、樂點、競舞、網銀那 些，這些假設點數啊 7-11 點數也好啊 Apple 點數也好，讓他們 PK 嘛，被通報詐騙的比例最多的，他就 1 年不能賣，那他們自己會不會去，我要是蘋果，我就掏錢直接跟被害人和解了，你不要去通報我，這樣子被害人還可以拿得回一點錢，你不要讓他愛賣就賣，然後一直賺錢，然後資料也不讓我們調。(E03-759)

法令的這個修正又不只是跟不上，就是在刑度上也沒有調整到有用的一個效果，所以我覺得修法上本身就有很大的問題。(E04-959)

你拿出的決心還不夠，這個本來就是你的疏失，你如果我們要比照像英國，好，你如果轉帳，他的帳戶其實他騙你是某某投資公司，可是這是個人，可是錢還是轉過去的，那對不起這個轉出的，銀行，你就賠一半，收款銀行你有沒有照會這個部分，你就賠一半，所以金融法規現在全世界要求到最強的是這個英國，這個部分可以參考。(E05-1206)

位於後端的矯正教育，更應負起教化之重擔。目前國內針對少年車手的部分，以少事法來說，保護管束到感化教育至少三年，對於少年車手再犯的可能將能有所助益。以國家親權的角度來看，少年加入車手集團，除了價值觀崩潰之外，更重要的是讓這些少年回歸校園，重建其偏頗的價值觀。更重要的是，培養相關職業技能，讓少年未來踏入社會前做好就職或者繼續接受大專教育的準備。另外就是矯正教育的詐欺犯罪課程設計也應落實。目前矯正教育對於詐欺犯罪並無相關應對的實證課程設計，為了未來長遠規劃，應該設計一套實證研究的教化課程，藉由各種課程的引導，從學理出發，針對詐欺犯罪者成因進行課程規劃，從心理與生理進行教化處遇，降低再犯的可能。

感化教育，那最輕的也是判保護管束，都是 3 年。那感化教育的很多都也是 3 年，所以少年反而會比成年的還要重。而且少年，原則上車手，我們原則上都是收容的(E04-866)

正確的一些價值觀。因為大家幾乎現在的新聞媒體大家都在比炫富，那這個也會刺激少年犯罪，我有個少年也是一犯再犯，然後我就每次收容，我都要說「我上次收容就跟你說過，你來我一定會收容你，為什麼還是再犯」，他就跟我說「法 官，我真的沒有辦法，因為我後來出去打那個，做粗工，一天就 1、2 千，我以前 1 天就有 1、2 十萬」，我說她說她很坦白，她很坦白的告訴我，她真的苦不下去了啊（台語）。他曾經滄海，他已經很難為水了。(E04-1053)

我之前去應徵超商，可是應徵超商我做了半天，不如我去幫人家提個錢，10 分鐘就可以賺的錢」，他真的曾經滄海就難為水。(E05-1086)

另外受訪者也提出一個新的思維，希冀各部會設立與警察進行犯罪偵查相等權力的部門，目前我國對於打擊犯罪由第一線的檢警調來進行，然而打擊犯罪從情資蒐集、分析情資、犯罪證據蒐集等，都由檢警單一部門進行。然而電信網路詐欺犯罪相關主責部會相當多，而檢警為了蒐集與保全相關證據，通常部會之間因為權責上的劃分與本位主義而難以全權配合，若是各部會能夠有與警察對接窗口，甚或是由檢警派駐之相關部門，未來若是有相關犯罪情況發生，能夠在第一時間進行相關資料保全與證據的蒐集，同時也能防止內部與詐團可能的連結。對於電信網路詐欺犯罪的相關法律規範，究竟是要一步到位，還是以循序漸進的方式來進行，必須審慎思考，避免落入政府要箝制言論的泥淖當中。

今天我們要解決這個問題，我們其他的部會一起加進來，比其他的部會，除了自己的監理之外，你要有自己的執法能力，不能像剛剛所講 的，我這個金管會就是我只管合法的大公司，不合法的通通這個警察來管(E05-1172)

必須要訂出你的網路偵查權，包括木馬。木馬的問題不是木馬，木馬的問題是你沒有《臥底偵查法》，你必須要先推一個網路的《臥底偵查法》，把你還有網路的這個《巡邏簽章法》，那讓警察的執法效能在網路上是有效的(E05-1347)

二、識別詐欺犯罪手法的精進策略

(一)識詐手段的宣導遭遇之困境

由於電信網路詐欺手法相當多元，雖然名為詐欺犯罪，但手法、接觸被害者、工具、劇本等都不進相同，而我國政府不斷吉利的對詐欺犯罪做大量的宣導，但仍有許多民眾上當受騙，顯然宣導並未到位。由於各年齡層國民擷取訊息的工具不同，而國內對於識別詐欺的宣導數量足夠，然而缺乏各種訊息揭露的工具的掌握以及分配，使得犯罪宣導的不夠精準。其次是資訊疲乏，由於國內相關詐騙宣導並未有統一部門進行相關文宣品的製作，每個政府部分雖然負有相關的宣導責任義務，然而宣導品的製作與經費、內容、專業、設計等面向都有關聯，有些部門只能專精於某個部份的宣導，對於其他部分相對來說較為弱勢，加上詐騙手法的不斷更新，製作的宣導品是否能跟上詐騙手法，也是另一大問題。更重要的是犯罪預防詐欺相關宣導的經費相當拮据，一個好的宣導品從企劃、腳本、分鏡、演員、道具等，都是專業度的展現，然而這些都需要經費的支持，從訪談者的角度中可得知，在有限的經費當中，只能透過各種方法來達到最佳的效果，對於預期宣導達到識詐的目標仍須加強努力。

政府就是說整個對詐欺的宣導事實上做得很多，但可能問題在於不是做得不夠多，是做的不夠準、不夠精準，當然數量是應該是沒有問題，就是不是做得不夠多，是做得不夠準。(E02-211)

我自己本身就是我大概每個月都會去做一次詐騙演講，那我的感覺就是因為有些那個…第一個，他們做的假廣告太厲害、太像真的。再來，有些我們的宣導做得不夠厲害，反而像假的。就是變成說我們有些政府的宣導，其實做起來，而且有時候看久了就會麻痺嘛。(E03-644)

我們沒有錢，零成本的同仁自己的手機的，後來就說，好那就請這個我們的數理股，這麼在做刑事鑑識的相機撥一台好一點的給我 們，我們來拍，那拍起來怎麼都死氣沉沉的？因為那個相機以前都是專門拍屍體的啊。那所以我們都是沒有錢，我們都是用沒錢的方式在做的。(E05-1396)

(二)具體建議

我覺得宣導我們真的宣導的非常完整，只是大家要不要看而已。(E03-683)

專家學者們表示我們的宣導其實相當完整，然而宣導品最重要的就是受眾願不願意接受我們所揭露的訊息，然而實際上來說，仍有相當大的空間可以努力。首先是識詐內容的分齡分眾，由於詐騙集團大量發送簡訊或影音，在各種不同的社群媒體平台上、通

訊軟體、線上遊戲、網路商店等各種接收資訊的工具中來搜尋潛在的被害者，而目前電信網路普及的緣由，不分年齡群人手一機的情況下，每個人喜好的網路世界各不同，而詐騙虛假訊息又如同病毒般的擴散，幾乎使用到手機的民眾都能接收到各種不同的詐騙訊息。從投資廣告、一頁式商品廣告、遊戲點數、電信簡訊、假買家騙賣家、ATM 分期、假檢警等各種不同的詐騙手法，透過各種網路訊息接收平台與工具，亂槍打鳥式的散播各種訊息，此時如果大眾無法第一時間辨識是否為詐騙訊息時，很容易落入詐騙集團所設計好的圈套，利用各種不同的腳本來進行詐欺。

因此，好的識詐政策與方法，從分齡分眾開始，針對各種不同年齡層的國民去分析其偏好的網路瀏覽頁面，不同行業的國民會接觸那些生活所需的頁面，百工百業皆應該去分析研究可能觸及的網路世界。此外識詐宣導的內容應不斷更新，將各種最新的犯罪手法加以剖析，結合犯罪心理的手法與專業拍攝技術，結合時下最流行的文化，先吸引受眾者的注意，才能夠讓多數的使用者點擊觀賞。另外更要結合法律制裁的效果與責任擔負，尤其是少年車手，家長對於未成年去擔任車手或販售人頭帳戶等情事，雖然少年沒有刑責，但家長有連帶賠償責任，透過學校與家庭共同來進行詐欺參與的宣導，減少未成年擔任車手的可能性。當然除了識別詐騙手法，法律責任擔負的警語為宣導內容之外，政府各部會轄下的各機構與民間私營機構，對於宣導詐騙更應相互配合，建立全民防詐的意識，提升識詐的能力。

雖然目前有打詐儀表板與 165 全民防騙網兩大詐騙宣導網站，然而這些資訊卻鮮少有全國民眾所利用，應該要想方設法讓全國民眾對於這兩個主要的識詐網站，不管透過電視新聞、社群媒體平台、甚至是國家級簡訊等，讓全國民眾能夠到這兩個網頁去瀏覽，才能將宣導品的觸擊率提升。雖然各社群媒體平台的觸擊率需要購買，然國家可以建立相關的激勵制度，讓多數社群平台主動放置相關內容，使得識詐成為全民運動，共同為打擊詐騙盡一份心力。另外更有規模的方式則是以國家演習的手段來進行詐欺犯罪宣導「全國防詐的實戰演習」，不定期地透過國家級簡訊的防詐演習，實際的讓國民了解各種可能的虛假詐騙訊息，若民眾點擊，便可以出現警語加以警示，不斷的演練讓識詐成為民眾的日常，如此便能提升全民識詐的能力。

> *詐騙宣導的內容，那針對不同的年齡，還有他的職業、心理狀態去做一個分眾化的策略。(E02-218)*

> *我們官方文宣來講，也很難說對每一個個體去做個化的宣導，那也很難，所以當然我們還是要研究一些詐團會用的犯罪手法。(E02-231)*

還要結合一些心理學家的一些建議，因為包括你被害的人可能就是…他是利用這個人的貪婪，或者是說恐懼、寂寞、權威崇拜的心理，才會演變出一種詐騙的手段。(E02-221)

百工百業這些第一線人員也有一些防詐的概念，包括超商店員，因為有一些遊戲點數詐騙的，超商店員就是第一線的、可能會接觸民眾的這些人，那我們也是多灌輸他們一些防詐的觀念，比如說這個民眾在購買點數的時候，超商店員如果說就跟銀行在攔阻那個匯款一樣，他如果有這種警覺的話，或許也可以幫忙攔阻一些被騙的案件(E02-244)

「電視沒有播啊」。我們還可以反宣傳，就是除了說詐欺本身會被騙錢之外，我們也反宣傳，因為他們都說少年犯罪沒有關係怎麼樣，其實有連帶賠償的問題，那個民事賠償是很可怕的喔，而且可能你可能要賠一輩子，所以我們可以去強化這部分的那個法律的後果跟效果。(E04-987)

比照政府這種防災演習，比如說由政府跟電信業者合作，然後定期我們發送一個模擬詐騙的簡訊或釣魚郵件給民眾，那讓這個民眾點擊以後，那我們會跳出一個「你被騙了，這是一個防詐的演習」等等，等於說讓民眾能夠持續保持這個警戒心(E02-236)

詐欺已經到了危機這個國安程度的話，有沒有可能比照這個疫情的廣告像每天都在電視上廣告，做不同類型，…比照那種防疫階段。我們防疫階段的時候，每天都有廣播。(E04-979)

三、防堵電信網路詐欺的具體政策與方法

(一)電信網路

1. 困境

電信網路的普及成為詐欺犯罪的天堂，詐騙集團透過各種網路工具來接觸被害人，由於電信網路的隱匿性與迅速性的特色，不僅被害人無法得知加害者的面容與位置，更讓人難以解決的是金融流動的迅速性與匿名性，使得各國對於電信網路詐欺無不戮力以赴。以我國目前對抗電信網路詐欺犯罪的情形來看，專家學者認為在全民識詐能力尚未普及之前，目前只能被動地防堵。從電信網路層面來看，由於電信網路是犯罪者接觸被害者的工具，加上許多犯罪集團設立在境外，使詐欺犯罪偵查過程中的逆追蹤手段受阻，

對於境外 IP 資料的取得與後續的分析，都是艱鉅的挑戰，也成為詐騙集團設立斷點的最佳考量。

> *現在的現象好像都是被動的圍堵，比如說我們發現哪一些，比如說最近有假檢警的案件，近期假檢警的案件有增加趨勢是因為那個境外未顯示來電的電話增多，那當然我們最近也在跟電信業者開會怎麼去防堵這些未顯示的電話。(E01-251)*

> *詐騙的伺服器跟他們的 IP 都是在境外，那個其實你查了也沒有用，然後再來就是他有些很多又是跟你說是浮動 IP，給你一疊資料，我得在一疊資料裡找出浮動的到底是誰，我能對到的到底是誰在用，也是個困難。(E04-993)*

> *他們都會用飛機，這個是你沒得去查，然後你去找 Line 啊，或者是用微信啊、臉書啊，你如果要去跟他調資料也很困難，他基本上也不太會給你。(E04-997)*

而例外一個電信網路查緝困境，則是人頭電信門號的浮濫不受限。專家們提出人頭電信門號的氾濫已成為最大的犯罪因素之一，主要是因為有了電信門號就能夠利用基地台網路，目前人頭電信門號的來源有外籍移工、遊客、通訊行提供、假徵才廣告[155]、辦門號換現金[156]等，更多的是有些民眾為了賺取蠅頭小利而販售自己的電信門號，而詐騙集團在網購平台大肆搜購電信門號，當詐騙集團獲得人頭電信門號後，同時申請「Voice over Wi-Fi」網路語音通訊功能，此一功能係利用電信網路傳送語音封包，詐騙集團就可利用此功能，在境外大陸東南亞地區，或者國內詐騙機房透過純網路環境撥打電話遂行詐騙，不僅用少額成本取得犯罪工具，更是躲避警方的查緝最佳利器。

---

[155] 「代辦門號賺外快」竟成詐騙幫兇　警方籲民眾慎防「人頭門號陷阱」。「假求職、真詐騙」的手法，通常以高報酬、低門檻為誘餌，吸引民眾代辦門號、提供金融帳戶或 SIM 卡，作為詐騙集團散布簡訊、洗錢或收款的工具。資料來源：GTV 八大電視。最後瀏覽日：2025 年 10 月 9 日。
https://www.gtv.com.tw/mobile/events.php?seqId=FDF021A1-FBD3-6816-F0BF-384872CB87E6

[156] 刊登「辦門號換現金」「小額信貸」等徵用廣告，吸引疫情期間無固定工作、有欠款紀錄信用不良、無法向銀行貸款民眾，利誘到電信門市申請月租門號。資料來源：高雄市政府警察局。最後瀏覽日：2025 年 10 月 9 日。
https://kcpd.kcg.gov.tw/News_Content.aspx?n=301858D950E8FB8E&sms=FC374298B757EFB3&s=19CA8882FC48BE0F

這個電信卡跟金融帳戶有一點點類似，就是移工的這一塊，因為移工他如果今天兩年期滿了，他今天要回到他的母國的時候，他會把他國內的帳戶跟這個 sim 卡一起賣給詐騙集團，這兩個一起賣的。(E01-309)

人頭門號還是比較難以根絕，因為包括這些人頭門號很多都是外籍移工，或者是一些遊民等等收購。(E02-260)

2. 具體建議

臺灣電信網路詐欺犯罪藉由科技的發展而轉為專業分工之作業模式，過去詐騙集團將所有犯罪過程一手包辦，然而當整體犯罪利益相當龐大，越來越多人加入後，不再是統包行騙、取款、洗錢一條龍作業，而是將第一階段話務手來行騙、收集人頭帳戶、車手取款、水房洗錢轉帳等工作細分，由不同子集團共同合作來完成多步驟犯罪。這蠍子集團係獨立作業，並且與其他子集團合作，錯綜複雜的合作關係，除了機動性之外，雖然都是實施相同犯罪手法，但不同劇本對應社會最新時事，靈活改變其犯罪手段，導致詐騙案件日益猖獗、難以禁絕。因此專家學者認為在電信網路層面，強調境外攔阻的重要性，整合國內電信服務業者從人頭帳戶申請的管理開始。除了實名制的落實之外，對於境外人士門號的管理更加重要，建議只要境外人士出境之後一段時間，應將該門號暫時停用，待其再度入境後另行開通。通訊行的門號申請應有一定的限制，不管是門號總量、身分審核、以及多重身分驗證方式來進行門號核發，更重要的應該整合境外與第二類電信，對於來電要有主動攔截與提醒機制，對於何種訊息或未顯示號碼等來電，應透過大數據的方式來進行分析，一有疑似的情況發生，應立即攔阻以及提示警語的功能，讓接話者能夠在接收電話或訊息之前，能夠有警語進行提醒。

台灣有一陣子就是黑莓卡非常多，黑莓卡就是 852 開頭的香港卡，然後他其實就是用黑莓卡來做上網的工具，所以我們去查完 IP 之後，會發現這個 IP 位址是在香港，所以這個確實他是一個，應該是說偵查的一個斷點。(E01-303)

這些很多都是從境外的發話，利用網路電話跟境外伺服器繞進我們的國內，所以我們是建議說要針對境外跟第二類電信做個整合，政府應該能夠加強防堵，包括境外伺服器或是說電召號，還有網路電話等等這一些，比如說要比照傳統電信一樣，要有一個攔截的一個機制，避免成為我們管理的死角。(E02-259)

建議就是不管是遊客或者是來台的移工，那其實他們只要出境，其實他們名下的電話號碼都應該要被管制…暫停服務、暫停使用這樣子，那他回來之後可能到臨櫃再來開通。(E01-314)

我們會請店面加強這一些人頭門號的控制。(E02-263) 如果不在國內，應該就把他斷卡。就不會被轉手。(E02-298)

境外入境的門市，他如果離境的話門號就要取消。(E03-741)

其次是希望透過 AI 人工智慧來協助進行可疑的電信資訊進行攔截。AI 人工智慧的盛行，當詐騙集團除了以傳統的劇本與手法來進行詐騙的同時，更有集團開始利用 AI 來設計各種新穎的劇本、影像與聲音的模仿，幾乎是假以亂真的劇本來強化其詐欺犯罪腳本的順利性。對於打擊詐欺犯罪的檢警調與企業來說，亦可引入 AI 來進行大數據的分析，找出詐欺犯罪的可能手法與特定模式，一旦有疑似的電信語音、簡訊、語音訊息、平台廣告、詐騙資訊等，可立即通知提供相關服務的業者進行攔截或是暫停服務，同時可將相關的資料保留進行證據保存。

電信業可以比照金融業，目前如果各位老師還有先進，就是說像我們國內那些銀行有建立一些所謂的 AI 模型，他們就是可以偵測一些的異常的交易帳戶，那我們建立電信業者，其實也可以建立一個電信聯合的 AI 偵測中心，他們也可以就電信的部分，就是這些涉詐電信的部分，他們也可以去建立所謂的 AI 的模型(E02-324) 短時間內向大量不同號碼發送內容相似的一個簡訊…網路的 IP 位置在短時間內，註冊大量的社群門號…境外的來電，他是在路由裝備、都是轉接，那這個也有可能是高風險的一個詐騙的訊息。(E02-332)

(二)數位經濟

1. 困境

(1) 數位廣告

數位經濟是在目前嶄新電信網路盛行時代下，以各種創新數位科技，結合各種數位平台與創新的服務模式來進行經濟活動。而數位經濟藉由電信網路盛行而生，當電信與網路結合後，對於彼此之間要有明確的界線是越來越難，也使得管理負責的單位也很難進行權責劃分。即便已經有相關法律的規範，然而許多數位經濟平台業者仍然沒有盡到

查緝的作為，反而是第一線的偵查人員為了防堵與犯罪預防，不斷的透過檢舉的方式來向數位平台業者進行通報，而專家們提到這些社群媒體平台透過演算法來讓時常檢舉的用戶，不再看到這些可能的虛假廣告與頁面，似乎有掩耳盜鈴之情況，對於企業來說，投放廣告為網站獲利來源，若是撤下廣告或是審核不通過，最直接的就是企業獲利下降，如此企業防詐的作為則難以落實。

> *在電信網路的定義上，我一直覺得很難分，以前可能電信真的是電信，網路真的是網路，可是因為現在大家都是拿著手機，然後透過網路，然後電信業者也提供網路，所以我發現他其實很難…。(E01-273)*

> *我們最近觀察，其實臉書他就是說，雖然我們《詐防條例》已經有把這些，比如說臉書這些業者納管，但是他們對於這種偵測詐騙廣告，其實他們還是不是很積極…幾乎都是我們警察在幫他們在網路上看哪些詐騙訊息，然後通報給臉書，然後臉書他們再下架。(E01-341) 事實上《詐防條例》也有賦予他們這個相關的責任，他們應該去主動去審查這些廣告有沒有涉及詐騙。(E01-350)*

> *社群媒體公司他們已經有改變了，一旦你檢舉之後，他就會讓你選擇，以後你就看不到這個廣告，這種事情就沒有了。(E05-670)*

> *目前《詐危條例》裡面，他所規定的這個網路廣告平台業者，他其實有限縮，他可能就是 Meta 、 Titok 這一些…。(E01-267)*

(2) 第三方支付

第三方支付是一種網路付款機制，由獨立於買賣雙方的第三方機構擔任中介角色，提供代收代付的服務來確保交易過程安全無虞。確認買家付款，資金會由第三方支付平台保管，直到買家確認收到貨品無誤，才會通知平台將款項支付給賣家。該支付服務是為了保障買賣雙方的權益，然而電信網路詐欺犯罪集團卻利用該支付模式來進行詐欺犯罪。傳統的第三方支付詐騙就是誘騙買家匯款給賣家，買家匯款未收到貨，賣家則被利用成為詐騙集團的人頭戶，此手段如果有多個賣家與買家，將會出現層疊交錯的第三方支付虛擬帳號金流過程，使得檢調難以追查[157]。新型的第三方支付詐騙開始有不肖業者

[157] 最狡猾的詐騙手法之一「三方詐騙」。資料來源：台中市警察局。最後瀏覽日：2025 年 10 月 9 日。https://www.police.taichung.gov.tw/precinct5/

與詐騙集團合作，透過人頭公司提供不實的營業項目及網路商店網址給第三方支付業者，提供被害人刷信用卡入金；或者是第三方支付業者向銀行申請虛擬帳號服務，讓消費者在網站選擇以銀行轉帳方式繳費。甚或是直接偽造「第三方支付介面」或發送假的付款連結來讓被害人信以為真而付款[158]。

專家們提出第三方支付的單一業務卻有不同部會管理，產生管理漏洞時的填補作為卻難以達成。首先是第三方支付公司的實名制登錄機制，但第三方支付的實名制並未徹底落實。目前經濟部登記的有上萬家公司能申請第三方支付業務，數發部則提出能量登錄制度來進行嚴格篩選。由於第三方支付的定義不明確，主管機關侷限於自身機關之權責，難以全面地進行管理與監督，有些經營代收代付業務的公司，規避「非代收代付」業務的規定，而成為第三方支付管轄的空窗期，但實際上這類公司有第三方支付業務的「類第三方支付」業者，顯然這些位於管轄權真空區的業者成為詐騙集團的最愛配合的對象。

而與詐欺集團過從甚密的博弈產業也涉及第三方支付業務，專家指出過去許多博弈公司大量申請虛擬帳戶進行代收代付業務而不需「能量登錄」，係因為官方對於運營第三方支付代收公司金錢不算在內，使得管轄公司的經濟部必須扛起管理之責，當法規沒有明確規定下，與支付業務關係密切的金融機構亦成為遭到質疑的單位。認為金融機構在沒有確定的情況下卻能提供該企業虛擬帳戶來進行第三方支付業務，然而法規的不完善，才是第三方支付業務管轄權不明的關鍵，因此必須從法律規範開始著手。

> *經濟部你在公司裡面你只要有第三方支付業務，你就可以做第三方支付，那當時我們去查大概有幾萬家的公司都有第三方支付的營登項目，那表示這幾萬家他都可以去跟銀行申請，那後來就是數發部覺得這太嚴重了，所以他們有一個制度叫做「能量登錄」，你要把你這個公司的營業額相關的一些規章制度讓我確認之後，我核准了之後，你才可以跟銀行去申請(E01-417)*
>
> *第三方支付，他可能也是會有一個破口，因為他第三方支付，KYE 並沒有做得很確實，他不像金融機構這樣做的。(E02-382) 有一些類第三方支付*

[158] 近期出現假冒第三方支付平台，網購交易時請提高警覺!。資料來源：桃園市政府警察局。最後瀏覽日：2025 年 10 月 9 日。
https://www.typd.gov.tw/index.php?catid=551&cid=25&id=634&action=view&pg=0#gsc.tab=0

這些電商業者，他們認為說這個不是第三方支付，以至於說他們可以去跟銀行申請一些虛擬帳號來使用，那這個就是一個很大漏洞在這邊。(E02-397)

第三方支付他的主管機關是數發部，但是數發部對第三方支付的業者的定義他是自己訂的，他表面上界定說他有代收代付，但是事實上很多電商他也有做代收代付，他只是表面上看不出來，但實際上他是有做，但是數發部認為說這個不是他們所要納管的對象，變成說有些我講說「偽類似」的，就是所謂「類第三方支付」這些業者就沒有人在管理，就是變成他…。(E02-388)

第三方支付實在太多了。這個 1 萬多家，那反正有來能量登錄的，那我切一半，每天的營業額在 20 億以下的就數發部來管，20 億以上的大咖的就金管會來管，請問 20 億多 1 塊錢，就是這個金管會來管，少 1 塊錢，真的就是這一個數發部來管嗎？數發部也因為受到很多的這個社會的指責，所以他就是把他接下來，可是數發部到底有沒有能力去管這個第三方支付？台灣最近的第三方支付詐欺有上升，詐欺你看，金額有減少一點點，可是件數沒有減少，他從騙大轉變成騙小，他甚至會叫你去超商用點數購買的方式，1 個 QR code 2 萬塊，他一次我給你 4 個 QR code，你一次就去繳 8 萬塊。*(E05-1183)*

2. 具體建議

其實第一線的警察相當辛苦，專家談到為了能夠降低或阻止潛在被害人接觸到相關虛假資訊，許多警員以人海戰術的方式來進行虛假廣告的檢舉，目的也是為了降低這些虛假廣告的觸擊率，雖然有些社群媒體利用演算法的方式來降低這些檢舉人的觸擊率，專家也提出，社群媒體會有這樣的動作，應該是該作為出現了效用，建議我國修法或與業者共同研議，開放檢舉權限與下架權限給國內司法人員，持續透過網路警察巡邏的方式來進行檢舉與下架的動作，雖然是土法煉鋼的做法，但亦能夠對防詐目標的達成有某種程度的貢獻。

開通那個權限，讓全台灣的警察都可以去檢舉，一檢舉就直接下架…(E03-652)我們有一組專員專門在解決你說的。然後再打包給他們去下架。(E01-668)

其次在第三方支付的部份，目前第三方支付只有實名制已經不足以應付金融安全需求，更需要雙方金流提領與儲存雙方之間的認證機制，實名制除了必須落實執行之外，更重要的是即時的查核監控制度，對於可疑的第三方支付帳號或是金流，透過分析來找出可疑的模式並加以警示或停止該帳號的使用；接著是第三方支付公司年度交易報告的呈現，若是這些報告出現與公司業務不符之情況，應進行實名制地再查核，確保該支付公司並無逾越公司營運內容而成配合詐團遂行洗錢的犯罪行為，同時這些資料也應該做好保存工作，作為未來犯罪偵查的證據之一。另外則是透過修法來賦予機構內控政策的訂定，要求企業應該負起內控機制的計畫，若是要在台灣執行相關業務，應配合本地打擊詐欺犯罪需求，甚至未來如果知悉而未即時通報或阻止，亦應負責相關賠償之責任。

我們的法律規範可以要求他？可以啊。這個都已經對他們，他必須落地。在台灣受到約制(E05-355)

現在《詐防條例》就是臉書你該下架沒有下架，其實是有罰則，但是我們現在其實是建議說民眾因為你這個廣告所遭受到的財損，我應該是也可以跟你臉書求償，但是我們《詐防條例》目前並沒有這樣的規範。所以我們是建議說下一個階段的修法可以把這個納進去考量，就是說你對於這個因為收看你臉書廣告的民眾造成高額財損要負…。(E02-367)

希望金管會針對某一些特定的非第三方支付業者的公司要申請的時候，應該要提供更詳細的交易目的。然後其實應該銀行他自己也要去監控，他如果這一間公司的虛擬帳號被列警示列太多的話，其實他們在契約訂立的時候，應該也要有這樣子的訂定，就是說「你可能達到某一種幾臥的時候，那我就要跟你解約」，這個銀行可以做，所以我們這部分也是希望銀行就是進到相關的一些企業社會責任 (E01-437)

最後數位經濟最常見的就是透過各種廣告的投放來尋找潛在被害者。對於投放廣告預收保證金制度應加以考慮，虛假廣告目前雖然有實名制審查機制，然而卻難以杜絕這些虛假廣告，即便社群軟體再經由演算法的方式來篩選受眾，但廣告仍有觸及率的問題，仍然有許多潛在的被害者持續觀看此類虛假廣告，建議能夠讓更多執法機關有權力去檢舉並下架這些廣告。

如果警察有權力原則，直接讓他下架，我覺得這樣會好很多，因為幾乎所有的詐騙都是從臉書來的，然後到 Line，就是從臉書然後用 Line 來繼續騙。(E03-686)

最後你就是要立法，包括歐盟打詐的第一個就是 E03E02PR 個人資料保護法，你既然是社群媒體公司，申請你的帳號的人必須留下什麼？個人資料，既然是有投資廣告，我希望你就是先收錢，而且要預收保證金(E05-1305)
你要先給我存好，那我如果要求你的時候，你必須要告訴我，不是我告訴你，我用科學方法弄得兩個月建置出來給你(E05-1325)

(三)金流防堵

1. 目前困境

專家在訪談中指出，雖然我國對於打擊電信網路詐欺不遺餘力，尤其是最隱密的金流面，更是希望透過各種法律的制訂來保障被害人，甚至能夠將相關金流路徑保留下來成為證據。然而法條的規範不夠周全卻成為打詐的阻礙，由於法條訂定的內容不完善，使得金融機構無法對可疑帳戶進行通報或管控。尤其是《詐防條例》的第 8 條、第 9 條，對於金融機構的存款帳戶、電子支付帳戶及信用卡，以及虛擬資產帳號等應盡善良管理人之注意義務，對於異常交易可暫停或管控，相關資料須保存五年以上。看似將所有金融商品進行規範，然而通報的主體是卻是金融機構，倘若警方接獲可疑帳戶疑似為人頭帳戶，要進行通報涉詐帳號，但非「銀行自己發現的」，對於金融機構來說，擅自暫停或停止客戶之帳戶會造成營運上的困難，若是金融機構自身的警示機制不完備時，亦難以發覺可疑帳戶。

「如果今天是警方發現了一些異常的帳號，可不可以反饋給業者去做控管？」…銀行又是非常遵法的一個單位，你只要法條沒有這樣寫的話，他就不敢這樣子做(E01-451)

對於法律規範的不周全，限縮了金融機構與警方聯合打詐的效能，現金詐欺犯罪的金流已經透過各種不同的金融手段進行洗錢，然而法律雖然沒有明確定義金融機構，但法律條文在金融機構的解釋當中變成，只限縮同業之間的合作，使得同為金融機構的其他機關無法配合或藉故難以配合，像是銀行的金融、保險公司保單、證券買賣、虛擬貨幣等，各種不同的手段進行犯罪所得的實現，而我國的法律卻因字面上或實務上的困境而拖垮偵辦查緝的進度，更成為詐欺犯罪集團利用成為查緝的斷點。尤其是《詐防條例》

第 8 條第 2 項[159]當中的「照會」，意味著金融機構對於「匯入該帳號的個人資料」、「匯款的過程與行為可疑」有其內控機制，然不僅於此，因為該金流可能將錢匯入虛擬帳號來購買虛擬貨幣，一旦金流到虛擬貨幣業者交易所之後，金融機構就無法繼續追蹤金流資訊，顯然金融機構端的警示與即時阻斷極具重要性。

> *第 10 條裡面他有講到，就是金融機構或者是 VASP 業者，可以跟司法警察機關配合做相關的聯防作業，我們的所謂的警民聯防。在執法裡面就定死了同業，而且他的同業是非常的狹隘的，我銀行只能跟銀行，我保險公司只能跟保險公司。其實銀行、保險、證券他們都是金融機構(E01-462)衍生管制的範圍其實是不及所有的金融的這個，像是 VASP 的帳號，他今天交易所的帳號、交易所的加密錢包是沒有在這個範圍裡面的(E01-482)*

2. 未來建議

專家提出應透過潛在被害人的擴大追查，讓更多的警示帳戶浮出水面，斷絕電信網路詐欺犯罪的犯罪工具。此舉係因為電信網路詐欺犯罪報案的黑數不明，若被害人沒有報案，相關的人頭帳戶難以讓第一線檢警調知悉，也無法將其通報為疑似帳戶，使得詐欺犯罪持續進行而無法阻卻犯罪行為的發生。另外，金融相關業務的提供者皆應該納入詐防條例的規範責任範圍之內，避免讓金融業務的轉換過程當中，利用尚未管理的金融商品進行洗錢。而金融機構為了客戶的權益，除非真的有確切證據證明為涉及詐騙犯罪，否則多數只會暫停，事後則恢復相關功能。最佳的方式是透過法規來訂出金融帳戶的凍結與解凍之間的標準程序，考量各種可能的詐騙金流手法，對於這些金流手段來進行嚴格的檢視與規範，若能落實則能成為打擊電信網路詐欺犯罪的關鍵作為。

> *「潛在被害人的機制」，我們會從一些特定的一些目標像警示帳戶，或者是這個涉詐的加密錢包，去反查一些被害人，就是他實質上被害人，但是他沒有發現自己被害的「潛在被害人」，那目前其實按照現在專法的相關的一些條文，他也沒有授權警方可以把這些資料提供給銀行，去做相關的一些風控，或者是勸阻、攔阻等等這樣的作為(E01-457)*

> *你把他列警示帳戶之後，你要把他當陷阱，接下來再有匯錢進來這個組織帳戶的人，你銀行要趕快去通知警察，讓警察去告訴他「你為什麼要匯錢*

[159] 「金融機構及提供虛擬資產服務之事業或人員執行前項後段規定作業時得照會同業，受照會者應提供相關資訊。」資料來源：全國法規資料庫。最後瀏覽日期：2025 年 10 月 3 日

給這個帳戶，這個帳戶已經被我們封鎖了，你是不是已經被騙了」，這才是我精準要宣導的對象(E05-1266)

異業的聯防、異業的照會這都是必要的，那這部份我們也會提出修法。(E01-476)「衍生管制帳戶」，就是因為他怕你拿其他的帳號來使用，所以你的本體是警示，其他叫做衍生管制…現在就是努力要修法的方向。(E01-483)

我們的金融環境沒有在做照會，今天我如果到銀行去調這個轉帳給這個法官,那我必須要這個帳號跟名字通通都要填正確,只要名字有一個字寫錯，對不起,錢就轉不過去，可是到你的數位來的時候，你就脫鉤了,數位來，為什麼脫鉤？因為數位來的時候，我只要帳號對了，因為他說，因為你的使用者是誰，我們不知道，所以呢？電子轉帳、網路轉帳是不需要打名字的，我問他「為什麼，你這個部分就不做照會？」(E05-1199)

金融帳戶的凍結啊，實務上是要金融聯方機制通報單，雖然說有些人會覺得太慢啦，但是至少有動比沒動好，如果說詐騙電話或是那種異常簡訊，1 個小時發 5 千封，發給海量的、亂亂發的那種，如果可以去動他的門號,就是你如果是正常的門號,你來解凍嘛。異常的如果是可以去動的話，那你讓申登人去持雙證件填單申請解凍，因為如果我今天是我自己的門號，我是願意去麻煩一點，去跑一下臨櫃把他結凍的。(E03-739)

目前最常見的還是透過金融機構的 ATM、臨櫃辦理的轉匯，以 ATM 來看，車手喜歡找隱密的地點來進行，而便利商店中的提款機則成為車手的最愛。建議能夠將 ATM 機器設於櫃檯旁，讓匯款的車手能夠曝光，甚至透過人來人往的顧客與店員共同監視，達到情境犯罪預防的效果。此外銀行帳戶之間的轉匯未來是否能夠有緩衝機制，透過更嚴格的多重審核機制來確認彼此轉匯的帳號，可參考歐美國家在支付制度上的審核制度，多一層認證能夠降地詐欺犯罪的可能性。

便利商店 ATM 放在櫃檯旁邊，…有做一個十大提款熱點，我們會發現如果是在超商裡面的熱點,他都是以那個在廁所旁邊的、隱匿的。(E01-805)

銀行匯款的帳號，是從這個帳號到這個帳號中間有一個 box，那我們有沒有可能在這個 box 的部分呢？能夠加強他的審核？或是讓他能夠多一道安全的防鎖，或什麼樣的機制？就是你帳號進去的時候，他是不是能夠再

做一步確定之後，再把這個帳轉到另外一個帳號，在這個 box 能夠留意久一點，或者是能夠有什麼審核的一個機制，或者是有一個猶豫的機制、能夠確認的機制。(E04-1017)

四、電信網路詐欺犯罪的偵查實務層次

《詐防條例》是去年的 8 月 2 號施行，然後到今年，目前 8 月份應該差不多整整一年的時間，那事實上相關的成效我們也還在觀察，那誠如剛剛老師有講的，感覺好像詐騙事件也是沒有好，感覺就是趨勢下降得很慢，那這個當然我們都有在注意到。但是我想說光靠警察去打擊偵察其實是不夠的，這個也是要靠各個部會去配合。(E02-145) 檢警是打詐的最後一道防線，那當然就是前面這幾道關卡電信、金融，如果搜索不住最後，那這個被害人他就被騙，所以接下來我們必須去追緝這個詐欺集團的犯行。(E02-486)

詐欺犯罪到打擊偵查面，實際上犯罪已經發生，對於被害者來說，金錢的復得比起犯罪者是否有被嚴懲，更是被害者關心的部分。整個國家對於檢警調的辦案有個極高的期望，希望能夠徹底瓦解電信網路詐欺犯罪集團，將被害人的金錢一一尋回，伸張正義。只是新冠肺炎之後，多數民眾更加依賴電信網路的使用，此舉更助長了電信網路詐欺犯罪的氣焰，且越燒越旺，使得世界各國無不極力思考如何能夠抑制詐欺犯罪的發生。

(一)困境

由於電信網路詐欺犯罪涉及到金流面、電信面、數位經濟面等不同部會所管轄的範圍，這也意味著對於第一線打擊電信網路詐欺犯罪的檢警調人員，是一份巨大挑戰的關卡要突破。不管是金融機構的相關資料、電信帳號的通訊紀錄、數位廣告的資料來源等，全數落在這些偵查人員肩上，然而由於目前雖然法規上對於各企業配合檢警調的偵查仍不完整，往往讓第一線人員疲於奔命。主要還是因為電信網路詐欺犯罪所涉及的機構與部會層面太廣，但靠警政與檢察部門的人力來辦案，仍有相當大的改善空間，雖然目前有相關情資數據資料庫，但仍然不足以快速的破案，需要更多的機構共同將資訊匯入，方能進行詐欺犯罪模式分析，提高犯罪行為發生的預測力。

我們跟調查局檢察官在辦案的時候，其實情資還是各自獨立的，沒有辦法大家一起分享，也就是說，目前是缺乏一個能夠即時整合、交叉比對的一個大數據的情資中心，目前辦案等於說各自還是各自為政的案子，包括銀

行的資料可能也是銀行之間流通的，除非我們跟他調閱，那網路的資料也是…所謂「情資孤島效應」就是這樣，各自有各自的情資，但是不見得會拿出來分享，這是目前最大的一個問題。(E02-497)

除了資訊收集的缺乏與分析之外，由於社群軟體帳號申請的限制過於寬鬆，可申請多個帳號進行使用，此舉造成檢警在查緝過程中常常遇到的偵查斷點。主要是因為申請社群媒體帳號並未有太多的限制,個人可申請多個帳號,顯然申請帳號無實名制之需求,該情況在 line 與臉書等社群媒體上都相同,即便以正式公文行文去申請該帳號的資料,不是不給就是說查無此人。此外對於跨境的資料調閱也是相當困難，即使透過正式的外交手段與司法互助條約，也是曠日廢時，對於快速的電信網路世界來說，無疑是雪上加霜。

為什麼他們每次可以去申請十幾個門號？他們就是自導自演嘛，而且 Line 又很好申請，然後又很難查，那基本註冊資料然後要以刑事警察局為申請單位，然後要去跑申搜，反正就是非常麻煩(E03-692)

Apple 有 Apple pay、有賣點數，…只是問他說這些點數花在哪裡，都還要申請搜索票，…，這真的非常的沒有意義、浪費時間，然後出來都是境外的 IP。(E03-697)

不管跟 Line 跟 IE03、臉書、mail 啊，我們去調他們的那些身份資料，或是遊戲公司的帳號那個身份資料，那都很困難。他們幾乎都一方面敷衍你，要不然就不給你，然後跟你說查無此人。(E04-950)

其實很多東西都已經雲端化、數位化，比如說我們一些數位證據他可能是存在於海外的伺服器或雲端等等，那個調閱也會相當困難，這個除非透過外交或是司法文書手段，否則你要去另外調閱一個是境外伺服器的資料，那根本是不太可能，這是目前也是一個有關數位證據的蒐證的一個困境。(E02-502)

法院量刑的標準是否有隨著法律的修正而有所改變，而最明顯的就是車手的部分。車手時常因為量刑較輕，或者是交保候傳等方式，讓車手即便是遭到逮捕，也在出獄或交保後，仍然持續加入詐騙集團當車手來獲取高額犯罪所得，對於好不容易逮捕到這些犯罪人的檢警來說，似乎撥了一桶大大的冷水，澆熄了滿腔正義的熱血。打詐四法中對於科技偵查的部分列入特殊強制處分，當中有增訂規範

新型態科技偵查手段，既然為新型態科技偵查手段，卻比傳統的辦案手法的時間更短，既然要大破大立的針對電信網路詐欺集團進行圍剿，諸多的限制打擊了第一線的士氣。

這個新法的這些量刑的標準，對我們院的法官，他們在判斷的時候，他們運用的程度如何？因為這可能要一、兩年，有些案子可能要一審、兩審，就是說一個詐騙案件適用這個新法的判決結果，事實上我們目前也還在觀察。是不是還是會維持以往的輕判啊。(E02-508)

很多車手被抓到以後，他馬上就又放出來、被翻案。(E02-513)

特殊強制處分只允許警察有 24 小時，就是太短了，然後要許可的話，法院許可只能 30 天，這比通訊監察還短，通訊監察可以兩個月，監聽都可以兩個月那這麼難用的東西警察要怎麼用(E02-577)

更大的困境就是金流的追緝，電信網路詐欺詐欺犯罪最終目的就是要大額的犯罪利益，而這些犯罪所得都靠便利且隱密的電信網路，進行金融的轉換與流通而最後落入集團當中。目前最大的困難就是虛擬貨幣的追緝，雖然目前洗錢防制法當中增訂《提供虛擬資產服務之事業或人員防制洗錢及打擊資恐辦法》適用於虛擬資產服務事業；《詐欺犯罪危害防制條例》中明訂當虛擬貨幣被用為詐欺工具時，可適用該條例；《金融機構及提供虛擬資產服務之事業或人員防制詐欺犯罪危害應遵循事項辦法》，是針對虛擬資產服務商及金融機構之防詐條例規範。即便我國已經將虛擬貨幣納管，然而虛擬貨幣靠的是電子錢包之間的流通與轉換，詐騙集團會把資金先移到境外交易所或離岸平台或利用境外錢包完成洗淨再匯回。且一個虛擬貨幣的案件會看到數以萬計的電子錢包，加上利用混幣的模式，使得金流去向模糊化，顯著降低追蹤可能性，成為犯罪所得洗白的常用工具。

虛擬貨幣現在最大的問題就是偵查的技術門檻其實是很高的，…。(E01-526) 可能後面也有一些高人在指點，所以他們現在甚至會用到一些混幣器，我把 USE02T 變成了這個比特幣之類的，就是他們會就是有一點像是在洗錢，在虛擬貨幣的這個區塊鏈裡面在做洗錢，那你其實是非常難去追蹤，或者是個化「到底這個是誰去做的」。因為虛擬貨幣他有一個特性叫做「匿蹤性」(E01-533)

上了那個虛擬帳戶的課程，只是我坦白說我真的聽不懂，因為太複雜了。所以那個虛擬帳戶的開設、監管和控制，那個真的都很難，還有那個幣 商，尤其是虛擬貨幣的那個交易、那個錢包，真的太複雜了，真的要有專家來做。(E04-1007)

(二)具體建議

電信網路詐欺犯罪活動除了透過跨境、跨集團等手法，再利用電信網路迅速性與隱密性特質來遂行犯罪，第一線的檢警調為了向上溯源追查，最重要的是需要情資的獲得與整合，即便目前已經有了大數據資料中心，然而對於許多打擊詐欺的員警來說，面對多樣化的資料，如果沒有協助分析與整合，對於犯罪手法與模式進行預測，單靠第一線員警來說，若是該專業已經超過警員所知，等於是讓員警放棄了往下追的動力。此時若有一個具有分析統合能力的大數據資料中心，除了能夠降低員警辦案的壓力之外，藉由高科技的數據資料庫分析，能夠儘快取得預測後的犯罪模式，可能發生的地點以及結合過去可疑犯罪人的資料進行比對，或許能夠找出更有效的犯罪偵查手段，盡早瓦解詐騙集團的運作。

目前我們是感覺比較缺乏一個大數據的一個情資中心，所以這個導致可能會影響我們辦案的一個效率。(E02-496)

其次是好不容易逮捕的車手，卻因為交保或刑期較短而重複不斷的加入詐騙集團擔任車手。由於斷絕電信網路詐欺集團的金流應該要各方投注心力，不管是對金融機構的法律規範，或是第一線提領的車手進行預防性的羈押，可以有效的降低與減緩詐欺犯罪所得的實現。對於門檻較高的金流手法，政府應快速應對變化快速的詐欺手段，而目前對於虛擬貨幣的運作與金流的查緝，應屬於專業技能領域，應針對各種不同的金融手法來進行犯罪分析，因此設置金融犯罪分析師是一個未來打擊詐欺犯罪的重要關鍵。

建議說檢察官以後，我們移送這一種經常累犯的這種車手，應該是能夠落實他《刑訴法》的加重，就是所謂的預防性羈押。(E02-518)

用委外的方式做一個技術團隊，因為其實這一塊我們幾乎所有的偵查人員，在學校沒有人有上過相關的課，但是我知道坊間其實非常多厲害的一些專家，他們其實是非常會追蹤幣流的，他至少可以跟我講說這個幣，現在到

底，因為他其實是一個公開帳本的概念，所以我們是可以知道說他到底是流到哪一個錢包。(E02-541)

最後則是集團成員常用的社群媒體，由於許多詐騙都是透過虛假廣告誘騙被害人加入群組，透過不同的角色扮演以及劇本的魅惑，常使得被害人信以為真而將全部財產轉出，當發現自己受騙上當時，犯罪成員則立刻將被害人踢出群組。顯然 Line 帳號的源頭管控若得宜,相對也是降低詐欺犯罪的可能性。同時間由於手機保護個資的層級較高，目前電信鑑識警察人員雖然已有建置,然而面對大量的手機鑑識需求,仍然是供不應求，對於培訓專業電信警察人員是刻不容緩之事。

Line 的帳號太好拿了。所以我們如果不從這個源頭去管制的話，就真的無能為力啦，就真的只能抓一個，算一個啦。(E03-705)

手機鑑識需求太高了，電信警察不夠多，數位鑑識警察(E03-742)

第五節 小結

一、我國打詐政策

我國從 2022 年開始提出兩年期的「新世代打擊詐欺策略行動綱領」，亦稱打詐 1.0 政策。該綱領揭示「識詐」、「堵詐」、「阻詐」及「懲詐」等 4 大面向，橫向整合內政部、國家通訊傳播委員會、金融監督管理委員會、法務部及教育部。且針對這四大面向具體提出相關的實務作為。「識詐」為透過教育宣導來認識詐騙，其涵蓋的部分包括行政院下的各部會，各部會透過不同的宣導手段來接觸人民，從學校、公務機關、交通運輸、含括士農工商軍民，期望透過各種不同的動態與靜態的標語、影片、海報與媒體宣導等，企圖能夠將防詐意識深植民眾心中。「堵詐」則是以電信網路面為主，境外電話的過濾與防堵、人頭帳號的管制、惡意簡訊的攔阻、虛假網頁的審核、電信 VPN 服務的審核與實名制以及資安落實的個資保護等，都是堵詐的具體措施，欲將第一線接觸潛在被害人的管道封阻。「阻詐」則是將贓款金流進行即刻性防阻，從人頭帳戶的開戶規定落實、境外金融帳戶預警機制的施行、金融雙認證與延遲交易、第三方支付督導作為、虛擬貨幣管理規範、遊戲點數實名認證與稽核、貨到付款與一頁式廣告詐騙的防治等，將當時最常見的詐騙類型的金流做全面性的阻止規劃。「懲詐」的刑事司法的偵查打擊面向，人頭帳戶入罪、情資即時提供與連結、高檢署的打詐中心、推動金融調閱平台與強化偵辦能力培訓等，讓打詐進入新紀元時代。

隨後升級至 1.5 版，增修「打詐五法」，與金融、電信及網路業者合作，從源頭防堵詐騙犯罪，目標以減害為主，仍以「識詐、堵詐、阻詐、懲詐」4 大面向，但求精進作為。公私協力的百工百業宣導識詐，資安強化的網路環境，境外攔阻可疑電話，建立綠色與紅色通道，將可疑廣告與帳號立即下架，斷絕新型態的接觸手段；強化金融機構與警政結合的臨櫃關懷，研議納管虛擬貨幣與虛假廣告，進一步對於各種支付手段的實名制審查，在不影響一般金融交易情況下設置多向內控機制；罪贓返還的被害人保護，以及凍結查扣等機制來提升打詐量能。而最新的 2.0 版，「打詐新 4 法」賦予執法依據，擴大到「識詐、堵詐、阻詐、防詐、懲詐」五大面向，除了先前的百工百業外，強化青少年的法治觀念，分齡主題式的宣導，將反詐識詐的意識深耕；實名制的落實查核電信門號的發給，與刑事警察局 165 專線建立聯防機制，非本國籍的預付卡的管控機制的堵詐精進作為；數位廣告平台的實名認證機制，大數據分析與快速下架系統，第三方支付的查詢平台等新的防詐層面作為；導入 AI 科技防詐執行打詐行動，虛擬資產的專

法推動以及各種支付平台與機制的嚴控，第一時間能夠阻詐成功；最後深化公私合作，推動國際司法互助，讓詐騙無所遁形。

二、打詐困境

在打擊電信網路詐欺綱領施行的這三年，雖然綱領制定的嘎天乍響，從各個面向著手，整合政府各部會可能的作為來提升打詐量能，然而實際上卻有許多窒礙難行之處。從這三年的詐欺犯罪統計資料得知，近三年的詐欺犯罪屢創新高，似乎對於政府提出的打詐作為予以重重一擊。近三年的統計資料得知投資詐騙、假冒政府官員、假交友、網路購物、解除分期付款等仍然位於前五名，因此也連帶打詐綱領策略朝向這些犯罪手法來訂定，詐團也跟著提升各種不同的劇本來遂行詐欺，更整合不同的金融資產手段來進行贓款匯兌與轉換。扼要來說，目前我國再打擊電信網路詐欺的制度整合有待加強，雖有多部會協作，但仍缺乏跨部門即時資料交換與統一指揮機制；第二是我國司法審判與犯罪偵查之間存在著不小的落差，除了量刑遭到詬病之外，尤其是電子證據與加密貨幣追查仍有待專業人士協助；當然最關鍵的還是國際司法互助所遭遇的瓶頸難以解決，及便透過外交與法律位階的條約來說，依舊限制了打詐的量能而導致跨境追訴困難。

以詐團的金流模式來看，包括傳統的面交付款、臨櫃轉匯、分層打散、虛擬貨幣或第三方支付等手法，將被害人的金錢轉匯到國外或者是其他帳戶，刻意製造多層次的金流，更能轉換其他金融商品來躲避金流查緝，財力雄厚的甚至能夠自己成立金融公司，以合法掩護非法。如此企業化的經營模式，讓第一線的檢警調辦案時，困難重重。國內的金融機構雖建立警示帳戶機制，但仍缺乏明確的「凍結時限」與「異常通報標準」，最需要的是強化銀行與第三方支付間的自動阻斷系統與資料共享。

國內政策方向明確，但產生了幾個情形，包括教育宣導不夠精準，包括宣導品過於單調、宣導內容跟不上詐騙更新速度、工作落在基層員警與金融櫃台人員、宣導並未深入民眾認知等，由於詐騙被害人涉及各年齡層，而國家宣導力道並為精準出擊，反而使得一些有經濟基礎的中老年人成為投資詐欺受騙最嚴重的族群。其次是金融機構阻詐與內控，目前金融機構也以配合並投入相關阻詐的工作，包括臨櫃轉帳的即刻關懷、立即聯絡轄區警力到場協助、建立內部的預警機制、利用 AI 科技偵測異常交易警示、以電話簡訊通知客戶識詐提醒、要求客戶對於可疑的帳戶情形予以回報、根據警政檢調通知凍結警示帳戶等措施。雖然做這麼多，但是詐騙提團仍利用第三方支付的虛擬帳戶特性、人頭帳戶的氾濫來遂行贓款的實現，尤其一旦被害人將金錢匯入指定的帳戶或電子錢包，金融交易的即時性，在極短的時間內便將帳戶內的金錢一轉而空，想阻詐都難以及時。

現今又利用虛擬貨幣來增加查緝與阻檔的困難，過去因為虛擬貨幣處於管轄權空隙而成三不管資產，詐團如入無人之境，檢警也都束手無策，直到 2.0 版打詐綱領後，由金管會成為主管機關，幣商實名制等措施納入後，對於虛擬貨幣防堵設置了防阻牆，然而新法執行剛滿一年，單就打詐儀表板的統計資料，單月被詐金額仍高達七八十億，是否有成效仍有待時間證明。

而在電信堵詐的部分，仍然以群發訊息的蔓延，人頭預付卡門號的氾濫為主，境外來電攔阻亦存在，更令人頭痛的是通訊監察難以派上用場，過往透過電信門號撥打尚能即時監聽，目前詐團多使用網路電話來進行聯繫，該軟體又具有即時自焚功能，根本無法取得解碼譯文，無從著手，對於機房的查緝多半還是得內部自行檢舉才有辦法得知一二，對於境外的機房除非國外提供相關 IP 位址，否則對於國內檢警查緝境外機房的困境相當艱鉅。而數位經濟的防詐層面來看，由於目前電信與網路的結合，數位生活已經是大眾生活模式，而社群平台上的各種虛假廣告不斷擴散在大眾生活中，即便有實名制的審查制度，若無被害者報案或者有人持續關注該虛假廣告，常常會淹沒在大量的社群媒體訊息當中，之所以不斷有受害者的出現，意味著紅色與綠色通道的攔阻與下架，落入野火吹不息、春風吹又生的無限循環，難以全部的檢舉與下架。建議加強電信業者與平台責任，並建立即時帳號封鎖機制

讓第一線檢警調人員更崩潰的是隨著案件量不斷的增加，查緝工作越來越繁複，但人力編制卻無法負荷工作排山倒海般的侵蝕熱忱，即便擁有實現正義的那個火熱的心，卻遭到機構本位主義所造成的多頭馬車與延遲，進而澆熄那個願意為社會公平正義燃燒的鬥志。在整體偵查打擊詐欺犯罪過程中，雖然擁有 M 話車與 GPS 定位系統的利器，然而申請的程序卻成為員警使用的阻礙，情蒐分析與監視器的調閱，耗費絕大多數的辦公時間；更令人沮喪的是證據取得過程中遭到的刁難與無視，甚或因證據在境外而變成死胡同，即便掌握確切情資但因證據調閱的延遲與難以保全，無知的少年與外籍人士的帳戶與門號，成為詐騙集團的新寵，形成新的查緝斷點；而面對跨境詐欺犯罪，苦無司法互助而鎩羽而歸，都成為打詐過程中令人灰心喪志的種種。面對被害者無助的詢問：「我的錢能追回來嗎？」只能寄望透過沒收與扣押來實現被害者的正義。面對各種查緝的困境，檢警調又時常難以一致的法律觀點，使得證據認定、羈押訊問到最後的量刑判決，彼此之間都存在的一些怨言與嫌隙，同為刑事司法系統的成員，雖有共同信念，但因訓練與養成的過程不同，使得檢警調院間出現歧異。

在法律抗制層面來說，治亂世用重典的聲音再度出現，打詐新四法中的詐欺危害防制條例，一口氣將詐欺犯罪的刑度提升至最高可處 12 年有期徒刑併科三億元罰金，期望能夠透過嚴刑峻罰來嚇阻日益嚴重的電信網路詐欺犯罪。而《通訊保障及監察法》、《刑事訴訟法》的特殊強制處分專章、對於金流的部分有《洗錢防制法》、《證券投資信託及顧問法》，對於犯罪人的《人口販運防制法》、《個人資料保護法》等，然而眾多法條下因為實務上犯罪行為的競合原則，只能選擇較重的法條適用，徒增條文之間的適用問題。對於電信網路詐欺相關的條文相當多，但實務上來講多數認為強制性的規範不足，多數願意配合但缺乏積極程度，反倒讓基層辦案人員感到灰心。由於詐團多數逮捕的都是底層的車手或人頭帳戶提供者居多，當幕後金主仍逍遙法外時，對於他們的懲戒嚇阻自然效用較低。法律是執法者著最佳後盾，但無形中卻也成了一道看不見的牆敦，尤其是當代表著實現社會正義的律師也因為高額報酬而為詐團折腰，透過對法律的了解來了解辦案進度與洩密，讓同為法律代言人的執法機關更是憤恨不平。專家普遍認為「打詐五法」與後續「新四法」雖強化了刑罰與主管機關責任，卻仍欠缺跨域整合的執行平台與標準化程序（SOP）。現行修法偏重懲罰，對於防詐預防面、技術偵查及跨國合作的法律依據仍不足。

三、打詐實務建議

綜合在刑事司法系統的檢警院等人的訪談，提出了對於打擊電信網路詐欺實務的相關建議。首先是明確的法律定義，減少條文間的競合狀況。嚇阻犯罪並非一味以亂世用重典的思維來管控，反而應該思考法律的修正與建立，應更明確為原則，過多的不確定概念會徒增解釋空間，從而無法有一致的判刑標準。當我們無法改變犯罪人的認知，只能透過預防的手段來介入犯罪過程，對於一些本應負起防詐工作的企業，制定相關罰則並負起賠償之責，對於無法落實法律規範的機構與單位，若是造成被害人的損失，也應負起共同的賠償責任。

打擊詐騙犯罪的第一線為檢警調人員，其首要目標為社會秩序的維護，為了社會治安考量，執法人員多數認為法律應優先考量犯罪偵查與預防，而非人權的考量。當這些犯罪者已經危害多數人的法益，倘若考量偵查過程還在思考是否侵害其法益，那誰又來兼顧社會大眾的法益呢？孰輕孰重應重新審視法條的妥適性。由於受訪者提出數位鑑識人力不足、手機取證需求暴增，需強化專責「電信警察」或「數位鑑識中心」的量能，顯示法律與科技的落差是否能夠補足，也是打詐的重要關鍵。對於詐團不斷推陳出新的犯罪手法，除了鼓勵被害人一定要報案之外，對於整個被害的過程應進行模式分析，對

於被害的原因進行了解後，在可能進行提前介入或預防的關鍵點上，透過立法來加以規範。接著提出人工智能加入打詐的行列應該加速腳步，當編制人力追不上案件激增的速度，借用科技來協助進行大量數據資料的分析，或是提前攔截與阻擋，甚或是即時的警示等，都是可以取代人力的好方法；建議建立常設跨國資料交換平台，並引入民間區塊鏈分析專業團隊協助幣流追蹤，利用委外技術團隊強化加密貨幣追查能力；當然在整體政策執行過程中，不管是直向領導或是橫向溝通與協助，都是行政單位應戮力解決的問題，除了最高單位的領銜之外，如何讓各單位將打詐視為機構的首要任務，並積極配合才是法規與政策落實的最重要一環。最後，詐騙集團會成功，利用人性來誘惑，因此讓民眾能夠具備識詐的素養更是犯罪預防的首要任務。除了宣導的頻率與強度之外，除了原先的各部會投入，百工百業的宣導，更應深入民眾的生活，讓民眾厚植識詐的能力，才能將防詐的工作落實。

推動「新世代打擊詐欺策略行動綱領」及後續之「打詐五法」、「新四法」，顯示政府已逐步建立跨部會防詐架構，並透過法制補強、策略升級及數位工具的導入，試圖在識詐、堵詐、阻詐、懲詐與防詐等層面建構完整體系。然而，綜合訪談與專家焦點座談之實務見解可知，政策執行與現場實務間仍存在結構性落差。首先，在法制與制度整合面，雖「打詐新四法」賦予主管機關更多管理工具，將電信、網路及金融業者納入防詐責任體系，但實務者指出目前各部會之間資訊流通與職權分工仍不夠明確，導致案件處理流程及權責界線重疊。專家建議應建構統一的跨部會協調平台與標準作業程序，並建立資料即時交換機制，以落實「制度化協作」目標。其次，在偵查與技術能量面，檢警人員普遍反映，由於跨國詐欺犯罪的證據多留存於境外，司法互助與資料調取往往受限於外交與法律地位，使得案件偵辦困難重重。部分專家建議以委外方式建立專業技術追查團隊，引進民間區塊鏈分析能量，提升虛擬貨幣及金流追蹤效能。同時，應強化電信鑑識與數位取證之人力培訓，以回應行動設備取證案件暴增的實務需求。

再者，在電信與數位治理面，Line 等社群平台帳號取得容易、假投資群組橫行，導致源頭控管難以落實。實務者建議應強化平台業者義務與政府協作，建立可即時封鎖詐騙帳號之機制，以減少被害發生。最後，在跨境合作與外交面，專家普遍指出我國受限於主權地位，與他國警方或司法機關請求資料時往往遭拒或延宕，導致跨境偵查與追訴困難。因此，應在現有法制框架下，積極運用國際刑警組織(Interpol)與亞太地區警政合作機制，建立非正式但具實效的跨境情報共享通道，提升追查效率。

最後，我國打詐政策已由「策略宣示」轉向「制度化執行」階段，但若要提升整體防詐成效，仍須同步補強三大面向：一、制度面之整合與協作程序化；二、技術面之偵查專業化與數位取證強化；三、國際面之司法互助與外交協商深化。未來應以「建立跨部門資料交換中心」、「強化數位鑑識與追幣技術」、「推動區域司法互助協議」為政策主軸，逐步構築我國整合式的防詐治理體系，使打詐策略真正落實於法制、執行與跨境合作的三層次中，達到有效防詐、阻詐與懲詐之整體目標。

第五章 結論與政策建議

第一節結論

一、各國打詐政策的策略

美國的法規與制度框架，美國對於電話詐騙(robocall vishing)與支付詐欺採「技術強制結合行政執法與情資驅動」的重量級組合。聯邦通訊委員會(FCC)推動呼叫來源驗證與簽章(STIR/SHAKEN)以驗證號碼真實性、減少號碼偽冒，並持續擴大適用範圍，包含非 IP 路段或第三方簽章限制等細項規定。這項技術要求是直接針對「來電顯示可被偽造」的根本問題。而在技術與金融配套方面，透過金融機構發布可疑交易或詐欺手法的資訊，協助銀行建立風險偵測規則；同時鼓勵銀行、支付業者與執法單位共享非公開情報、進行快速風險通報。行政機關也在研究與擴充可讓銀行在接獲執法請求時加速凍結帳戶的程序。在公私協作實務上，美國的強處在於公私界線雖然受法律制約，但已有成熟的合作平臺，像是執法機構與金融機構間的相互配合、私人企業主動分享大數據資料庫，以及大量以技術為主的阻斷工具，像是呼叫驗證、AI 偵測惡意 SMS/廣告技術的防詐技術。但因為美國是聯邦制、跨州與跨國的司法程序複雜，跨境追款與跨域執法仍是挑戰。不過美國對於非 IP 電話、國際來源電話與跨境金流仍易形成漏洞，對於個人資料的隱私權與法律規範間仍有改進的空間，期望執法機構能夠監控、並獲取相關犯罪資料等。

歐盟的法規與制度框架層面上，歐盟採以「法規框架結合監理責任擴展」為主要打詐策略，將 PSD2 及後續 PSD3 落實支付層面導入強化用戶驗證、開放銀行與資訊共享機制，並鼓勵支付服務提供者在防詐、檢舉與資訊交換上扮演更主動角色。歐盟也透過數位服務法(DSA)開始要求大型平台在內容與詐欺風險上承擔更大責任。這種以法規驅動的做法強調系統性、跨國一致性。在打詐技術與整體經濟措施層面，首重支付安全面向，歐盟引入多重用戶驗證機制來減少卡片盜刷等直接盜用問題，但詐騙集團也轉向社會工程與手機 APP 的詐騙手法，利用受害者使用手機授權轉帳的功能來遂行詐欺。為此 PSD3 對於支付的跨國銀行帳戶認證機制、強化即時支付的欺詐防護與資訊共享，試圖把風險分擔機制與快速通報納入法規設計，以改善跨境快速支付造成的偵測盲點。於公私跨國協作上，歐盟優勢在於「跨國單一市場」的法規一致性，能用法規工具要求平台電信業者、APP Store 平台與其他大型社群平台，配合進行廣告實名驗證、惡意應用 APP

下架。不過歐盟對於犯罪數據保護規範限制主動監控與資料分享，且不同成員國在執法與資源上仍有落差。主要還是歐盟強調隱私保護，此舉與執法監管權限出現拉鋸，同時跨國執法實務差異，以及即時金流阻斷的實務，需各成員國協調。

日本在打詐制度層面與執法重點上，日本對警察廳(NPA)與金融監管機關金融廳長期合推全國性的防詐教育，此計畫是結合地方警察局、金融機構實施，主要是 ATM 可疑操作的偵測，以及用戶提示來降低被害。整體來說日本政府強調「預防為先、社區與家庭參與」的策略為主，希望能夠將防詐意識深耕於日常生活中。在防詐技術與金融配合面上，日本銀行與金融機構在面對高風險交易時會採取交易延遲給付與人工確認雙眾認證方式、加強臨櫃與非面對面交易之驗證，以及積極進行民眾教育，透過公眾廣告、名人宣傳、社區講座等方式進行。此外，日本也有民間與半官方的詐欺防制組織協助統整案例與教育資源，整體來說強化防詐意識為首要工作。在公私協作與社會層面上，日本的成功關鍵在於全民式的社會動員，從警察、銀行、地方政府、媒體、名人和民間團體的共同參與，使得社會整體對這類詐騙的敏感度提升，從源頭來阻斷詐騙的可能。然而透過社會宣導雖能降低詐欺被害,但面對高超技術或國際化的詐騙手法,像是跨境洗錢、假投資平台等新式詐騙，仍需更強的金融監理與國際合作。

南韓在打詐法源與執行架構上，南韓對於防止電信型金融詐欺的法律進行規範，強化對金融機構責任、被害返還與凍結程序做出具體規範，並授權司法機關與金融監理機構在發現詐欺情事時，能迅速請求銀行暫停支付或出金。這種法律授權使得銀行端即時阻斷具有較強的法源依據。南韓著重在金融層面的阻詐,近年大量推行金融層面的制度,像是新戶開通後數日內跨行出金限制、可疑收付款即時通報、臨時付款凍結、客戶申請信用交易封鎖服務等，並建立全天候的電信、金融、警察整合的快速反應中心，實現高頻度的實務攔阻。金融監管機構(FSC)亦常發佈針對詐欺防堵的金融措施與業界指引。此舉的優勢在於能在第一時間切斷資金鏈，減少被害人金錢外流，並透過法定程序加速返還或追繳；但也存在如何避免過度限制正常交易、保護無辜用戶權益與跨境資金追索的平衡難題。。

我國自 2022 年起推動「新世代打擊詐欺策略」,以跨部會整合為核心,將內政部、NCC、金管會、法務部、教育部等進行整合,建立「識詐、堵詐、阻詐、懲詐」四大面向,強調整合既有單位與建立國家級體系應對電信網路詐欺。2023 年著手進行 1.5 版與「打詐五法」的修訂，從補強法源與工具，針對刑責、個資、洗錢、證券金融等面向著手修法，使得偵查與追繳在法律上更具依據。由於詐欺犯罪手法變化快速，將相關作為法制

化成為關鍵，催生「打詐新四法」，以專法或大修方式納入法律體系，強化對通訊監管、科技偵查與金流管控的法源基礎。隨後提出 2.0 版，新增「防詐」並聚焦數位經濟產業治理，把重點擴展至運用 AI 防制、深化跨境合作、監管防詐產業、加強被害保護等新議題，並明確提出要強化數位經濟治理，針對社群網路的大型平台、第三方支付、虛擬資產等，與先進國家趨勢一致。

二、國內打詐的實務與困境

本研究訪談對象包含 5 位偵查警政（含電偵）、1 位檢察官與 2 位法官（共 8 人），受訪者多為長期處理電信網路詐欺案件的第一線或司法人員，能直接回饋實務困境與改善建議。從執法面來看，人力專業化與分工不足為關鍵。偵查案量劇增遠超人力成長，導致一線警力與檢察資源吃緊，專案化、專責分隊與快速審理機制需求強烈。基層偵查與司法審理之間在時效上存在斷層，影響凍結與追繳成效。金流阻斷需求高但即時聯繫與法制支持不足。偵查人員多數認為，當發現交易異常後，難以在短時間內通知並完成銀行支付機構的凍結，尤其面對第三方支付、小額分散、多平台匯流之情形。而全天候的金融通報與訊息提供，對於該筆交易進行即時暫停，相關金流來龍去脈能有更明確的法源支撐。金融面棘手的問題還有人頭帳戶與第三方支付。人頭帳戶收購、快速輪換與利用代付服務，讓資金追查難度大幅上升。

而打詐需要跨部門協助資料共享，但法律與實務上經常發生期望落差。警察、檢察、金管、銀行、電信等公私部門間的資料共享需求高，但受到個資法、銀行保密等法律與程序制約，造成偵辦延時。受訪者都希望能夠修訂或明確化例外授權、快速通報機制與資料共享標準化流程。打詐時常在跨境合作實務瓶頸，牽涉境外機房、系統商或金流的偵查，皆認為只要跨境後，根本難有任何機會繼續偵辦下去，因為從蒐證、合作與臨時性司法協助耗時且程序複雜，實務上需更高效率的雙邊合作機制，然本國司法互助協定上處於劣勢，因此徒增偵查困境。產業責任與執行漏洞是造成打詐困境元凶之一，訪談指出，平台與電信在門號、廣告與虛假網站管理或商業簡訊審查等面向，仍有落實不足或法令授權不明。

被害者救濟與宣導不足也是訪談者認為的改進方向。被害者往往在行政與司法程序間載浮載陳，整個刑事司法程序中，整體時效漫長，心理及法援支援不足，更只關心自己的財務是否能夠返還。尤其是詐騙手法更迭迅速，民眾識詐教育需常態化與更具針對性。期待行政單位加強即時公告、產業協作與被害者救濟流程。

人頭門號、人頭帳戶與假網站仍是詐騙集團常用的低成本工具，若產業端不主動治理，執法單位追查成效有限。透過法制或監理命令明確業者義務，包含審核、登錄、即時下架與通報等，並建立罰責與補救機制。若要有效降低詐欺發生與財損，僅立法不足，必須同步強化金融端之即時攔截能力與法制明確性。若要解決整體犯罪偵查與量刑困境，專責偵查隊伍、專門法庭或快速審理機制能顯著提升案件處理速度與沒收成效，從而提升威懾與回復被害人信心。促進辦案效率則須公私資料共享的法律框架與規範需要明確、標準化，以便在遵法情況下達到高效率偵防。被害保護與預防教育應從單次宣導升級為系統化，並將被害救濟納入常態行政業務。

總結來說，在執法資源與司法瓶頸中，案件數暴增導致檢警、檢察與法院人力壓力顯著，尤其是檢方根據犯罪事實與證據來起訴，但是在法院最後的判刑定罪結果中，存在相當大的期望落差，使刑罰嚇阻功能減弱。另外就是我國打詐在金流即時阻斷能量不足，與南韓等採用之快速銀行端凍結與大量通報機制相比，我國在銀行在第三方支付端的「即時攔截」作為仍待強化，尤其面對第三方支付與虛擬通貨的快速流動，我國目前仍是企業內部自控為主，雖有規範，但沒有罰則。人頭帳戶、第三方支付與虛擬貨幣之監管缺口，詐欺犯罪利用新型電子金流逃避偵查，現有實名制與防洗錢資訊與金融業通報互動仍有漏洞須補足。而最令人灰心的就是跨境司法與執法協作的制度性限制，即便立法快速，但跨境取證、引渡、與境外資金追索仍受制於國際程序與實務配合難度。

我國在政策快節奏、跨部會架構與科技導向上近乎追上或接軌先進國，但在執行能量上，司法與查緝人力、金融端即時阻斷、跨境互助與公私資訊協作機制上仍落後於以有銀行即時阻斷以及公私高密度合作的南韓與部份歐盟成員國。建議以強化金流即時阻擋能力、強化防制洗錢與第三方支付監理、擴充專責偵查能量、制度化跨境司法協作為優先改進方向。

三、各國打擊電信網路詐欺犯罪機制比較分析

各國的電信網路詐欺都相當嚴重，對於打擊電信網路詐欺犯罪都有制定一套該國的政策，然而透過電信網路來遂行犯罪，基本上都有類似的犯罪模式，因此各國當中對於打擊電信網路詐欺政策有其共通點，首先為阻止犯罪所得的快速移轉，因此重視金融端的「即時阻斷」是降低財損的決定因素，因此各國皆朝向多重認證、警示、攔阻與返還的規範為之;其次是防堵加害者所利用的工具,尤其目前詐欺皆利用電信與網路為媒介,因此對於電信與網路平台進行源頭驗證的實名制著手，接著對於涉及疑似詐欺犯罪的帳號或門號強制下架的機制，各國皆以該手段做為降低接觸面的第一道牆；第三，當詐欺

犯罪發生後，只能朝向偵辦的方向為之，各國對於具有隱密與迅速性的詐欺犯罪來說，皆朝向縮短處理時間的專責偵辦與協調中心為主，加快定罪與追繳的刑事司法程序；第四，由於單靠刑事司法系統難以偵破或對於科技為主的詐欺犯罪，因此各國皆強調公私協作的必要性，然而公私協作更需法律的支持，因此各國皆朝向公私合作的合乎法規與避免責任並存，才有持續資料交換的誘因；最後是最困難的一部份，尤其是電信網路詐欺多為跨境犯罪，跨境互助則是以盡量標準化程序為之，同時強調迅速姓，才能抓住黃金時間。

對於各國打詐政策的比較部分，以下表來簡易表示其主要政策的方向。美國：分工細、工具多，技術與民間能量強，但聯邦—州協同成本高。歐盟：體系法與跨境工具成熟，對大型平台的「可稽核責任」最完整。日本：特殊詐欺長期治理，高齡者保護、社區動員、地方警署細緻化明顯。南韓：源頭治理（簡訊/來電）與金融即時攔截中央集權推進速度快。臺灣：法制與政策節奏已追上，但程序化、平台化、專責化仍在強化期。

表 20 各國打擊電信網路詐欺犯罪政策比較表

	法制懲戒	金融阻斷	偵查突破	電信防堵
美國	反詐與通訊治理以部門法體系運作（通訊、金融、刑事、隱私分軌）；針對來電認證、垃圾訊息、平台責任有明確授權	即時凍結與KYC/AML協作成熟；聯邦與州層級訂定「快速阻斷／返還」程序指引	多聯邦機關分工，州檢警與總檢察長並行；專責工作組與聯合行動常態化	來電驗證（STIR/SHAKEN）、號碼可信鏈；威脅情報共享自動化
歐盟	以指令/規章「體系法」治理（數位服務、金融監管、資料保護）；跨境執法與平台合規要求強	即時凍結與KYC/AML協作成熟；聯邦與州層級訂定「快速阻斷／返還」程序指引	樞紐化協調；成員國警檢分層執行；跨境專案小組與聯合行動成熟	跨平台透明報告、風險稽核；支付與通訊資料接口標準化

韓國	專法＋總量化治理（防詐特別對策、電信與金融並軌規範）；「警察廳—金融監理—通訊」三方聯動	金融監理院系統性黑名單、可疑交易即時攔截；受害者資金追繳時效與流程明確	警察廳—檢警合署專案；專責搜查隊與聯合偵查中心；對車手網絡與機房搜查常態化	反詐中樞平台＋AI 釣魚簡訊偵測
日本	刑法與特別刑事立法並行；對「特殊詐欺」有專項規範與量刑強化；金融與電信協作具明確指引	銀行協會＋金管指引要求「疑義即暫停」；高齡者保護機制（窗口/冷卻期）	警察廳主軸，地方警察署設詐欺專班；檢察與法院對特殊詐欺有專業化分流	詐欺樣態資料庫與 AI 偵測逐步滾動
台灣	綱領 1.0→2.0 與「打詐四法」逐步到位；需整合刑、訴、通保、洗錢、電信管理等形成穩定「體系法」	銀行與第三方支付已建置警示與攔阻，但「即時阻斷 SOP、回溯追繳協作平台」仍須制度化	警政—檢方量能提升中；跨部會小組運作，但專責偵辦與專庭規模仍待擴充	科技偵查法制化啟動；需建跨域「最小必要」資料交換平台與稽核機制

美國強調刑事追訴與行政執法並行雙軌進行，有除惡務盡的精神存在。由於美國重視個人資訊，因此強化個人資料的保護作為，所以打擊電信網路詐欺從電腦與網路入侵防護為防範個資冒用來進行詐欺犯罪，若詐欺發生，最重要的要防止金錢被快速轉匯，因此要求金融機構必須通報可疑交易，對於跨州的詐欺犯罪更是以嚴懲態度為之。FCC 近年發布多項技術命令推動 STIR/SHAKEN 來電驗證框架，以阻斷號碼偽冒與自動撥號詐騙。整體來說美國的防制體系可定位為技術導向的分層治理模式，同時公私協作成熟度相當高。對於美國的打詐機制來說，台灣也有全國詐欺通報資料平台，只是通報平台的責任並未強制要求所有打詐的可能機關必須納入。目前在防詐的部分，並未制定技術防詐標準作業程序，若能夠整合出針對詐欺犯罪樣態制定標準作業程序，應能提升整體效率。最後是金融機構與執法單位即時通報與凍結帳戶的強制進行之法源基礎，由於金

融機構為營利單位，而通報與即時凍結勢必危害企業的獲利與客戶間的信任，再彼此之間取得平衡點是未來政策制定時的考慮方向之一。

第二節 政策建議

我國在政策設計與快速修法上展現出強烈意志與整合能量，但若要把政策化為減少被害與懲罰犯罪的實際成效，必須在金融端即時阻斷、司法與偵查專業化、跨部門與跨境資料共享的可操作法制上補強，並同步落實被害保護與常態化預防教育。

表 21 短中長期政策建議表

政策規劃	面向	具體建議
短期	部會整合	1. 建立常設「防詐跨部門協調中心」並落實執行，過去經常有所謂的打詐辦公室，然而卻不見實質的運作與整合，應成立協調中心來避免部會本位主義。將警政署、金管會、通傳會、數發部、經濟部、交通部與外交部納入固定成員，整合情資與執行決策，統籌統一案件指揮、金流封鎖、電信阻斷與境外資料請求程序。此中心可作為跨域整合的實體平台，補足現行打詐中心屬行政協調、缺乏法定授權之不足。然而若沒有明確績效指標的話，容易流為形式化作為，因此建議短期內建置的跨部門協調中心成立後，應明訂相關案件資訊通報應縮短至少 20%以上的時程。若要有顯著的民眾感受，對於被害人返還案件平均處理天數應下降，如此可讓短期成效更具可衡量性。 2. 「防詐跨部門協調中心」若無法定授權，易流於行政協作。建議針對該防詐跨部門協調中心給予行政命令授權依據或者明訂於法律之內。 3. 建構「跨機關通報 SOP 流程圖」，可清楚呈現警政單

		位、金融機構、電信通訊、檢方偵辦起訴的即時協作機制。 4. 單一防詐部門的協調中心難以負荷大量的案件與各種政策的執行，因此除了在中央設置協調中心外，可區分區域進行協調中心的分部設置，各協調中心的分部可整合該區域的地檢署、地方警局、金融機構、教育單位與社區，提升通報效率與落實宣導作為。
	偵查打擊專業與永續的培訓	1. 設立「數位鑑識與加密貨幣追查技術實驗室」，導入民間技術力量，成立跨部門專責單位，整合警政、檢調與學術研究機構，運用區塊鏈分析、AI 金流模型與開源情資技術追蹤虛擬資產詐欺路徑。將資料匯入國家級防詐資料交換平台。 2. 鑒於現行警調人員在電信鑑識與幣流追蹤上受限於訓練與人力不足，應建立持續培訓機制，並將數位證據保存、跨國請求程序納入檢警培訓課綱。
	被害保護與預防	1. 建置被害者「快速救助與返還」單一窗口。
	法制層面	1. 短期內要達到一定的成效，應明訂明訂部會協作義務與資訊通報程序，建立跨部門協調法源。 2. 打詐要快速與效率，對於刑事訴訟法、通訊保障法及金融監理相關條例中，對於「防詐例外」條款應充分授權金融機構、電信業者於接獲司法通報時得立即凍結或封鎖可疑帳戶與門號。 3. 證據保全的重要性與時效性，是破案的關鍵因素之一。短期可以行政命令方式先行建立跨部門資料共享規範，確保偵查、金流與通訊資料交換具合法性。

	教育宣導	1. 加強分齡、分場域之常態化識詐教育與企業責任，於平台、金融業的前端風控與風險揭露。 2. 「分齡化防詐教育教材」的設計，教育部應與內政部合作，針對不同年齡層，從學生、家長到銀髮族，設計防詐識讀教材，將媒體識讀、防詐心理學納入國民教育課程。
	金融面	1. 建議能制定「金融與執法緊急通報之標準作業程序」，收到可以交易通報後 1 小時內暫停相關金融業務等待審核、偵查重大犯罪時的責任免責條款。明確授權金融與通訊業者在接到司法警政緊急通報時之暫停凍結義務與程序。 2. 爭取與主要區塊鏈分析公司簽署資料交換 MOU，以「科技輔助執法」取代外交困境，透過第三方分析服務追蹤跨國幣流，提升我國境外偵查效率。
	電信面	1. 對電信業落實「高風險門號名單」與預付卡查詢流程，並明確規範商業簡訊登錄與審查程序。 2. 法制面上明確個資分享之例外條款與標準作業程序（SOP），以利偵辦但兼顧隱私保障。 3. 強化銀行與第三方支付之風控，包括行為分析、異常交易模型等。 4. 引入 AI 防詐與社群監測系統，參照美國、韓國經驗，發展 AI 詐騙廣告偵測、假投資群組辨識與高風險帳號封鎖機制，透過金管會與平台業者共享模型結果，實現事前預防而非事後補救。

中期	資料整合	1. 建立國家級防詐資料交換平台，在法制保護下提供給檢警、金管、銀行、電信與平台，並定期發布可疑模式與黑名單供業者採取主動阻斷。同時強化該資料交換平台的合法性，說明其法源依據、主責機關、資料保護機制，亦可參考歐盟「一般資料保護規則」（General Data Protection Regulation, GDPR）合法性原則[160]。 2. 資料治理必須架構化才能有效的供於應用，對於相關的犯罪資料來說，目前應該只能透過刑事司法系統作為犯罪偵查所用，然為了能夠讓學界與機構能夠從中進行研究與預測，對於跨域資料交換應該著重，視為中期發展目標，對於相關資料應用應給予法源依據，設置資料授權、加值、匿名化標準。
	法律抗制	1. 明確金融、電信、平台之防詐義務與配合程序，修訂或新增條文，對第三方支付、虛擬資產服務、電信門號管理、廣告平台責任做出明確義務，包含通報、保存紀錄、合作配合時限，更重要的是能夠明確規範行

[160]GDPR 強調重點為，提升個資當事人權利與強化個資專責機關權限。當中第六條有提到合法性原則(Lawfulness of processing)，若是該資料平台要讓非具有公權力單位使用的話，應當有其法源依據外，更應該這樣的原則之下，強制這些防詐單位主動阻斷可能的詐欺犯罪資訊並保留給檢警辦案使用。原文如下：Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c)processing is necessary for compliance with a legal obligation to which the controller is subject; (d)processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e)processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f)processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. 資料來源：Intersoft consulting。最後瀏覽日：2025年10月9日。https://gdpr-info.eu/art-6-gdpr/

		政罰與刑罰配套。 2. 增加刑事司法的人力編制，可考慮推動「打詐專庭」與「詐欺專責檢察官制度」，確保案件審理及追訴專業化。未來若是新興犯罪的崛起，也能作適當的人力條配，刑事司法系統需要有彈性的運作，專庭的設置若沒有搭配人力的建置，只是在舊有的人力上面給予加重的負擔，推行的可能性將大幅降低，亦只能在原地打轉，不斷抱怨案件量的增多、人力不足、效率不彰、前後線皆吃緊的狀況難以改善。 3. 透過法制化來建立標準資料管理系統，立法明定資料交換平台之主管機關、保護資料前提下需資料去識別化的相關規範、明定查詢權限層級、可提供學研究的資料範疇。進一步能以法規授權方式，導入 AI 科技，將 AI 所分析之高風險帳號、詐騙手法之分析模型結果整合進入官方預警系統,建構詐騙預防的預警制度。
	偵查打擊	1. 制定「法條適用指引」協助檢調與法院處理法條競合問題，減少實務適用之不一致性。 2. 執法機構建置或擴充專責偵辦小組，並增加檢警及司法專業人力訓練與留任誘因。 3. 制定金融、警政、檢調之全天候緊急通報與反應單位。 4. 推動標準化「情資交換整合平台」以縮短查核時間。建立虛擬貨幣交易所與跨境匯兌平台的強化 AML/KYC 與連結主動通報機制。 5. 詐欺犯罪專責法庭的設置,因應不斷增加的詐騙案件,法院設置專庭或專案審理與快速程序。

	教育宣導	1. 全民防詐學院的推廣，常態化公民教育與校園防詐課程，教育部建立分齡教材、師資培訓、年度校園防詐演練。 2. 全面審查詐騙手法中所涉及之行為，將這些行為的主管機關納入詐防條例的規範當中，成為各級學校的教材之外，推廣至全民。 3. 推動「在地防詐社群據點」，結合地方政府與社區發展協會成立「防詐輔導站」，由警察與社工合作辦理案例諮詢與預防講座，提升基層民眾警覺力。
	產業治理機制	1. 推動反詐業聯盟的構想，除了原本的法制層面外，政府政策的制定仍須考量打詐的量能，單指政府制定政策而力量趕不上的話，打詐政策將淪為口後，因此促進學術與研究單位的加入，讓與打詐相關的業者共同開發防詐科技。 2. 實名制與內控機制的法治化，業者必須具備風險管理計畫、事件通報義務、廣告上架前審查機制；建立罰責與改善令程序。 3. 公私聯防情報共享平台的設置，結合電信、銀行、支付業者，建立「警示帳戶與可疑錢包名單」即時通報機制，鼓勵業者共享匿名化的詐騙行為資料，提高防詐反應速度。 4. 數位信任認證制度的建立，對於合法平台、合法幣商頒發官方防詐標章，供民眾辨識，降低民眾遭受假投資與假交易平台詐騙風險。同時對於可疑的交易平台與商家，給予消費者與瀏覽者警語提示。 5. 對於未通過數位信任之商家與平台，未來應直接防堵或阻斷該頁面或限制相關業務的營運，直到符合國家

		安全標準方能持續運營。
長期	專業化	1. 持續人才與研究投資，長期投資於數位鑑識、虛擬貨幣鏈上分析、AI 反詐研發應用、以及跨域法學、矯正教化專業課程與資安人才培育，方能達到電信防堵、金融阻斷、犯罪偵查與再犯預防等目標。 2. 應建立「防詐案例資料庫與開放資料平台」的建置，由數發部統籌，整合 165 反詐騙專線與各部會查緝成果，去識別化後的案例、資訊與趨勢統計，提供學研界與業界進行 AI 模型訓練與風險預測。
	全民防詐與數位安全素養	1. 對於防詐的教育宣導普及化與社會化治理方針必須具體化，將防詐教育納入「終身學習」政策與企業 ESG 指標，形成社會化預防機制。 2. 建議以教育部與勞動部為主管機關，串聯科技部、金管會與 NCC。除了現有的課程融入防詐教育之外，設置可模擬真實詐騙情境的互動教材。 3. 師資培育的課程應納入「防詐教育」，由各大學之師培中心與地方教育局合辦，培育「防詐種子教師」。 4. 各企業的訓練應納入數位安全與風險管理課程，包括員工防詐訓練整體參與率，企業內部資安與社群風險演練，配合政府政策或 NGO 合作的防詐宣導成果。
	法制化	1. 建立「國家級防詐中心（National Anti-Fraud Center）」該中心能整合所有部會資源，能統一運用與指揮各部會資源，如同防疫救災等作戰等級籌設。統籌防詐資料平台、跨部會指揮、國際聯繫、研究與技術中心，包括虛擬貨幣的鏈上分析、AI 模型訓練、

		偵查演練。 2. 建立常態化的「警政作為、金流阻斷、電信防堵、平台交換」等資料交換管道，於法律保障下進行去識別化的情資交換，提高詐欺偵測即時性與可追溯性。該管道具備優先的法律位階，具有強制性作為之精神。 3. 法制長期化與預算化，除了考慮將「國家級防詐中心」納入法定常設機關之外，尚可考量編列「防詐基金」的會計項目，支應打詐費用與專責技術研發與強化國際間合作的所需經費。 4. 對於目前詐欺犯罪的法條相當分散，建議長期整合現有的法規，包括刑法、通保法、刑事訴訟法、金管規範、電信管理法、打詐條例等，形成「打詐法規體系」；能夠建立「科技執法與隱私保障」之法律架構，平衡偵查效率與基本權保護。
	司法互助	1. 強化國際交流與合作，定期分享相關打詐政策與具體作為，強調合作的重要性，並與主要詐欺來源或中轉地建立定期情報交換與執法演練。推動與重點國家之非正式司法互助「快速通道」，並在雙邊區域層級協商證據交換標準。參考歐盟美日等國在跨國平台與金融合作的法規設計經驗，採務實可行之互惠安排。 2. 竭力建構雙邊聯絡窗口與程序，考量我國獨特國際地位，應以非正式外交之管道為之，特別是與常見資金流向國家的執法單位與代表處。對於相關犯罪可疑資訊交換與證據保全與請求標準作業程序，標示緊急性並準備完整證據清單。

第六章 參考資料

中文部分

George Ritzer & Douglas Goodman(2014)。社會學理論(上下)。柯朝欽，鄭祖邦譯。巨流，新北市。。

林山田、林東茂、林燦璋(2012)。犯罪學(五版)。台北：三民。

汪子錫、葉毓蘭（2013）。跨境詐騙犯罪的類型與治理分析。展望與探索，第 11 卷，第 3 期，頁 67-90。

許華孚、黃光甫 (2020) 全球化的電信詐欺考察研究-犯罪成因與對策，台北：一品文化出版社。

黃富源、張平吾、范國勇(2012)。犯罪學新論。台北：三民。

蔡田木（2010）。詐欺被害歷程及防制策略之研究。2010 警學與安全管理學術研討會論文集。桃園：銘傳大學，P.109-126。

賴擁連、蔡田木、陳玉書(2024)。我國網路詐欺被害調查與防制研究。

賴冠允（2024）。海峽兩岸共同打擊電信詐欺犯罪之探討。發展與前瞻學報，(44)，99-115。

許春金, 謝文彥, 黃蘭媖, 呂宜芬, & 游伊君. (2021). 犯罪被害狀況及其分析-我國首次犯罪被害趨勢與服務調查報告. 刑事政策與犯罪防制研究專刊, (30), 47-91.

內閣府(2025)。国民を詐欺から守るための総合対策 2.0。犯罪対策閣僚会議 https://www.kantei.go.jp/jp/singi/hanzai/kettei/250422/honbun-1.pdf

英文部分

Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to defend against cyber crimes: An assessment with reference to anti-cyber crime law and GCI index. A*rchives*

of Business Research, 6(12).

Amarullah, A. H., Runturambi, A. J. S., & Widiawan, B. (2021). Analyzing cyber crimes during Covid-19 time in Indonesia. *In 2021 3rd International Conference on Computer Communication and the Internet (ICCCI)* (pp. 78-83). IEEE.

Carroll, P. (2018). *Investigation into VoIP Communications fraud and TDoS attacks and solutions required for the corporate environment* (Doctoral dissertation, University of Dublin).

Cole, T. (2023). How are financial institutions enabling online fraud? A developmental online financial fraud policy review. *Journal of Financial Crime*, *30*(6), 1458-1473.

Correia-Hopkins, S. (2024). A Framework for Measuring the Quality of Police Recorded Cybercrime Data, Illustrated through a UK/USA Comparison. In *The Crime Data Handbook* (pp. 260-272). Bristol University Press.

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, 20(3), 358-375.

Fonseca, C. C., Moreira, S., & Guedes, I. (2023). The prevention and control of online consumer fraud. In *Handbook on Crime and Technology* (pp. 395-410). Edward Elgar Publishing.

Federal Bureau of Investigation(2023). 2023 Internet Crime Report.

ITRC(2025). 2024 Data Breach Report

Giddens, A. (1990). The Consequences Of Modernity. Stanford, CA: Stanford University Press.

Giddens, A. (1992). The Transformation of Intimacy: Sexuality, Love and Eroticism in Modern Societies. Cambridge: Polity.

Giddens A. (2002). Runaway World: How globalization is reshaping our lives.London: Profile Books.

Giddens A. (2013). The Nation-State and Violence. Cambridge: Polity.

Gless, S. (2019). Transnational Access to Evidence, Witnesses, and Suspects. *In The Oxford Handbook of Criminal Process.*

Consumer Affairs Agency (2024). 令和 5 年度 消費者政策の実施の状況. P165-171. https://www.caa.go.jp/policies/policy/consumer_research/white_paper/assets/consumer_research_cms201_240614_31.pdf#page=5.00

World Economic Forum, WEF.(2023). Global Cybersecurity Outlook 2023. https://www.weforum.org/reports/global-cybersecurity-outlook-2023/

International Monetary Fund, IMF.(2023). Fintech Notes: Cybersecurity Risk Supervision. https://www.imf.org/en/Publications/fintech-notes/Issues/2023/

European Union Agency for Law Enforcement Cooperation. (2023). European Union Serious and Organised Crime Threat Assessment (SOCTA). https://www.europol.europa.eu/publications-events/main-reports/socta-report

European Commission. (2023). Progress Report on the EU Security Union Strategy. https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en

Junger, M., Wang, V., & Schlömer, M. (2020). Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime science*, *9*(1), 13.

INTERPOL. (2024). I-GRIP Initiative Results: Combating Digital Financial Fraud in the Asia-Pacific Region. International Criminal Police Review, 62(4), 45-58.

European Commission: European Anti-Fraud Office, *OLAF report 2023*, Publications Office of the European Union, 2024, **https://data.europa.eu/doi/10.2784/56951**

Anderson, R. J., & Smith, K. L. (2024). Advanced artificial intelligence in cybercrime detection: A comprehensive review and future directions. Journal of Cybersecurity Technology, 15(3), 234-256.

Jun, O. (2023). Direction of Japan's New Cybersecurity Policy. *Asia-Pacific Review*, *30*(3), 63-78.

Consumer Affairs Agency (2024).消費者保護ルールの在り方に関する検討会報告書 2024。Consumer Affairs Agency. https://www.soumu.go.jp/main_content/000962314.pdf

NPA (2025 年 4 月 28 日). 最近の特殊詐欺及び SNS 型投資・ロマンス詐欺の特徴について。National Police Agency https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/250428/02.html

NPA (2025). 令和６年における組織犯罪の情勢について。警察庁組織犯罪対策部.p1-2. https://www.npa.go.jp/publications/statistics/kikakubunseki/r6jyousei_digest.pdf#page=1.00

NPA (2024). 令和６年警察白書 抜粋。THE WHITE PAPER on POLICE 2024. National Police Agency. https://www.npa.go.jp/hakusyo/r06/index.html

Kwon, D., Borrion, H., & Wortley, R. (2024). Measuring cybercrime in calls for police service. *Asian Journal of Criminology*, *19*(3), 329-351.

Ilbiz, E., & Kaunert, C. (2023). Europol and cybercrime: Europol's sharing decryption platform. In *Security in Transnational Spaces* (pp. 74-87). Routledge.

Mawgoud & I. Ali, (2020) "Statistical Insights and Fraud Techniques for Telecommunications

Sector in Egypt," *2020 International Conference on Innovative Trends in Communication and Computer Engineering* (ITCE), pp. 143-150

European Union Agency for Cybersecurity (ENISA) (2023). NIS2 Directive Implementation Guidance. https://www.enisa.europa.eu/topics/nis-directive

Muhammad, S., Meerjat, F., Meerjat, A., Naz, S., & Dalal, A. (2024). Enhancing Cybersecurity Measures for Robust Fraud Detection and Prevention in US Online Banking. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 510-541.

Na, C. (2023). Proactive crime prevention through problem-oriented governance: A case study of South Korea's recent efforts to tackle new types of fraud. *Policing: A Journal of Policy and Practice*, *17*, paac080.

National Police Agency(2024).THE POLICE WHITE PAPER 2024,

Saeki, R., Kitayama, L., Koga, J., Shimizu, M., & Oida, K. (2022). Smishing strategy dynamics and evolving botnet activities in Japan. *IEEE Access*, *10*, 114869-114884.

Ayumu, Y., Hiroyuki, I., Kosuke, K., Tetsuya, K., Taichi, A., & Takahiro, K. (2024). Threat of Technical Support Scams in Japan. In *2024 IEEE Conference on Dependable and Secure Computing (DSC)* (pp. 115-122). IEEE.

Park, H., Lim, K., Kim, D., Yu, D., & Koo, H. (2023). Demystifying the regional phishing landscape in South Korea. *IEEE Access*, *11*, 130131-130143.

Saghir, W., & Kafteranis, D. (2022). The Applicable Law on Digital Fraud. In *Finance, Law, and the Crisis of COVID-19: An Interdisciplinary Perspective* (pp. 221-235). Cham: Springer International Publishing.

Smith, R., & Grabosky, P. (2017). Cybercrime. In Crime and Justice: A Guide to Criminology

(5th edition). Thomson Reuters (Professional) Australia Limited.

Ando, R., Hieu, N. M., Haoqian, P., Liu, Y., & Takefuji, Y. (2025). Characterizing Geographical Distribution of Tor Node by Local Density Comparison. *International Journal of Computer Science & Network Security*, *25*(2), 225-230.

European Commission. (2025). The EU Legal Framework Against Digital Fraud: A Comprehensive Analysis. Brussels: EU Publications Office.

U.S. Department of Justice(2025).Office of Justice Programs, *Federal Justice Statistics,2023.*

OLAF (2022). *The OLAF Report 2022: Impact of OLAF's investigations - Administrative*. Retrieved from https://ec.europa.eu/olaf-report/2022/impact-of-investigations/impacts/administrative_en.html

OLAF (2023). *The OLAF Report 2023: Anti-fraud policies*. Publications Office of the European Union. Retrieved from https://ec.europa.eu/olaf-report/2023/anti-fraud/anti-fraud_en.html

NCSC(2025).NATIONALNATIONAL CYBERCYBER SECURITYSECURITY CENTERCENTER 2024 ANNUAL REPORT.

Federal Bureau of Investigation. (2025). *FBI releases annual Internet Crime Report*. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

Federal Communications Commission. (2023). *Sixth report and order and further notice of proposed rulemaking on call authentication trust anchor* (FCC 23-18). https://docs.fcc.gov/public/attachments/FCC-23-18A1.pdf

Federal Communications Commission. (2024). *Improving the effectiveness of the robocall mitigation database* [Notice of proposed rulemaking]. https://www.federalregister.gov/documents/2024/09/12/2024-

Federal Trade Commission. (2023). *FTC joins FCC in renewing memorandum of understanding to promote cross-border law enforcement efforts to combat robocalls and spoofing* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-joins-fcc-renewing-memorandum-understanding-promote-cross-border-law-enforcement-efforts-combat

Department of Justice. (2025). *Asset Forfeiture Policy Manual*. Retrieved from https://www.justice.gov/criminal/criminal-afmls/file/839521/dl

U.S. Department of Justice. (n.d.). *Computer Fraud and Abuse Act (CFAA)*. Retrieved April 21, 2025, from https://www.justice.gov/criminal-ccips/computer-fraud-and-abuse-act

Eurojust. (2024). Jurisdiction guidelines with case examples. *European Journal of Criminal Justice Cooperation, 15*(2), 125-147.

EUR-Lex. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

EUR-Lex. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union*. Official Journal of the European Union, L 333, 80–152. Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555/oj

U.S. Department of Justice. (n.d.). *Identity Theft and Assumption Deterrence Act*. Retrieved April 21, 2025, from https://www.justice.gov/criminal-ccips/identity-theft

U.S. Department of Justice. (n.d.). *Fraud Section – International cybercrime cases*. Retrieved April 21, 2025, from https://www.justice.gov/criminal-fraud

U.S. Department of Justice (2025) Money. Laundering and Asset Recovery Section. *Asset*

Forfeiture Policy Manual. https://www.justice.gov/criminal/criminal-afmls/file/839521/dl

United States Postal Inspection Service. (n.d.). *Report a crime*. Retrieved from https://www.uspis.gov/report

Federal Trade Commission. (2024). *Operation Stop Scam Calls: Coordinated Law Enforcement Action to Combat Illegal Telemarketing*. Retrieved from https://www.justice.gov/archives/opa/pr/us-department-justice-federal-trade-commission-federal-communications-commission-and-other

Lyons, P. (2021). *Robocallers, Regulatory Challenges, and Enforcement Gaps: A Critical Analysis*. Journal of Law and Technology Policy, 2021(1), 45-78. https://illinoisjltp.com/journal/

Zhang, Y. (2024). Research on the Criminal Law Response to Telecom Fraud in the Digital Society. Economics, Law and Policy, 7(3), 33–44. https://www.researchgate.net/publication/385074770

Smith, J. (2022). U.S. and Canada team up to combat cross-border fraud. *The Washington Post*. https://www.washingtonpost.com/

Europol. (n.d.). *Cybercrime.* Retrieved April 21, 2025, from https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime

European Commission. (2024). The EU Cyber Solidarity Act. Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

European Banking Authority. (2024). *Regulatory technical standards under PSD3* (EBA/RTS/2024/XX). European Banking Authority Publications. https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-

money

EUR-Lex. (2024). *Regulation (EU) 2021/694 (Cyber Solidarity Act)*. European Union Retrieved from: https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng

European Commission. (2024). *Crime statistics - Statistics Explained*. Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime_statistics

European Commission. (2023). *Modernising payment services and opening financial services data: new opportunities for consumers and businesses*. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543

European Commission. (2025). *Report on the protection of the European Union's financial interests - Fight against fraud 2024 Annual Report*. Publications Office of the European Union. https://ec.europa.eu/anti-fraud/about-us/reports/annual-reports-protection-eus-financial-interests-pif-report_en

European Public Prosecutor's Office. (2025). *Annual report 2024: Statistical data on fraud investigations in the European Union*. Publications Office of the European Union. https://www.eppo.europa.eu/annual-report-2024

European Cybercrime Centre. (2025). *Spain Country Report: Cybercrime Trends and Threats Landscape*. Europol. https://www.europol.europa.eu/crime-areas/cybercrime

Florea, O. I., Aivaz, K. A., & Vancea, D. P. (2022). Exploratory Study on the Types of Economic Crimes at EU Level. *Ovidius University Annals: Economic Sciences Series*, *22*(2), 68-76.

Europol (2024). *Internet organised crime threat assessment (IOCTA) 2024*. European Union Agency for Law Enforcement Cooperation.p27-35. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised

%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

Costea, A. M., Putină, N., & Brie, M. (2024). Cybersecurity in the Republic of Moldova in the Context of European Integration. *Romanian Journal of European Affairs*, *24*(2).

EUROPEAN COMMISSION (2023). Commission Anti-Fraud Strategy Action Plan - 2023 revision. *EUROPEAN COMMISSION*.p.3-5. https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud/european-commission-anti-fraud-strategy_en

INTERPOL. (2024, June 27). *USD 257 million seized in global police crackdown against online scams*. Retrieved from https://www.interpol.int/en/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams

Eurostat. (2025). *Crime and criminal justice statistics 2024*. European Commission. https://ec.europa.eu/eurostat/statistics-explained/index.php/Crime_statistics

European Union. (1995). COUNCIL ACT of 26 July 1995 drawing up the Convention on the protection of the European Communities' financial interests. *Official Journal of the European Communities.* No C 316/48 Retrieved from ：https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995F1127(03)

Korean National Police Agency, KNPA. (2024). White paper on cyber crime 2024. https://www.kisa.or.kr/EN/302/form?postSeq=73

European Electronic Crime Task Force (2025, May. 23). *HOME (EECTF)*. Retrieved from https://eectf.com/

Public Prosecutors Office Japan (2025 年 3 月 28 日).Prosecution Reform Initiatives in the Past Three Years-The Principles of Prosecution and Practice. Public Prosecutors Office

Japan. https://www.kensatsu.go.jp/content/001142803.pdf

Public Prosecutors Office Japan (2025 年 3 月 28 日). *The Principles of Prosecution*. Public Prosecutors Office Japan. https://www.kensatsu.go.jp/content/000128760.pdf

UNITED NATIONS ASIA AND FAR EAST INSTITUTE FOR THE PREVENTION OF CRIME AND THE TREATMENT OF OFFENDERS, UNAFEI. (2019). *CRIMINAL JUSTICE IN JAPAN*.p2-5. https://www.unafei.or.jp/publications/pdf/CJSJ_2019/03chapter1.pdf

Grabosky, P., & Smith, R. (2003). Telecommunication fraud in the digital age: The convergence of technologies. In *Crime and the Internet* (pp. 41-55). Routledge.

Shiyang, S. (2023). Study on Telecommunication Fraud from a Student's Perspective. *International Journal of Frontiers in Sociology*, *5*(16).

Tiwari, M., & Singh, R. (2020). **A Survey on STIR/SHAKEN: An Overview of Call Authentication.** *International Journal of Computer Applications*, 176(18), 1-6.

Hunsinger, J., & Sen, A. (2020). **Understanding STIR/SHAKEN: How the New Call Authentication Framework Works.** *IEEE Communications Magazine*, 58(5), 16-21.

Wang, S., Delavar, M., Azad, M. A., Nabizadeh, F., Smith, S., & Hao, F. (2023). *Spoofing Against Spoofing: Towards Caller ID Verification In Heterogeneous Telecommunication Systems*. arXiv preprint arXiv:2306.06198. Retrieved from https://arxiv.org/abs/2306.06198

David Shepardson (2024). FCC chair asks telecoms to detail efforts to block fraudulent AI political robocalls. https://www.reuters.com/technology/artificial-intelligence/fcc-chair-asks-telecoms-detail-efforts-block-fraudulent-ai-political-robocalls-2024-06-27/

Takahashi, R. (2023). The evolution of fraud crimes in Japan: Legislative challenges and

solutions. Japanese Journal of Legal Studies, 45(2), 178-195.

Hao, F., Wang, S., & Smith, S. (2023). *Spoofing Against Spoofing: Towards Caller ID Verification in Heterogeneous Telecommunication Systems*. arXiv preprint arXiv:2306.06198. https://arxiv.org/abs/2306.06198

U.S. Code. (n.d.). *18 U.S.C. § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information.* Retrieved from https://www.law.cornell.edu/uscode/text/18/1028

Choi, Y.J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues, 24*(S5), 1-8

Choi, H.W.& Lee, S.J.(2022). Current Status of Phishing Crimes and Search for Countermeasures = Current Status of Phishing Crimes and Search for Countermeasures. *Security Policy Research*. 36(4), 105-140.

Federal Communications Commission. (2019). *FCC adopts new rules to combat caller ID spoofing.* [Press release]. https://docs.fcc.gov/public/attachments/DOC-358440A1.pdf

U.S. Congress. (1991). *Telephone Consumer Protection Act of 1991, 47 U.S. Code § 227*. https://www.law.cornell.edu/uscode/text/47/227

Winseck, D. (2017). The geopolitical economy of the global internet infrastructure. *Journal of Information Policy*, 7, 228-267.

Park, J., & Kim, S. (2023). Evolution of Voice Phishing in South Korea: A Systematic Analysis of Attack Patterns and Prevention Strategies. IEEE Access, 11, 54321-54335.

Kim, Y. J., & Park, S. H. (2023). Regulatory Responses to Telecommunications Fraud in South Korea: A Legal Analysis. Computer Law & Security Review, 48, 105689.

KISA. (2024). 2024 National Information Protection White Paper. KISA. https://www.kisa.or.kr/20303/form?postSeq=12004&page=1

Yu, L., Cong, Q., & Li, S. (2024). Study on international cooperation to address cross-border telecommunication network fraud offence. *J. Pol. & L.*, *17*, 51.

Lee, J. Y. (2022). Korea's Regulatory Framework for Virtual Assets and the Role of KoFIU. *Journal of Financial Crime and Regulation*, 19(4), 213–229.

ISC2(2025, Jan.16). *EU Cyber Solidarity Act – What You Need to Know*. ISC2. https://www.isc2.org/Insights/2025/01/EU-Cyber-Solidarity-Act

European Commission(2025, Mar.4) The EU Cyber Solidarity Act. European Commission. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

Supreme Prosecutors' Office. (2025, January 6). *2024 년 검찰연감 [2024 Prosecutor's Yearbook]*. 서울: 대검찰청. 取自 Supreme Prosecutors' Office website

Park, C.-W., & Yoon, C.-S. (2018). A study on the legal policy for the prevention of telecommunications-based financial fraud. *Han Yang Law Review*, 29(1), 113-150.

Ju, J., Cho, D., Lee, J. K., & Ahn, J.-H. (2021). Can it clean up your inbox? Evidence from South Korean anti-spam legislation. *Production and Operations Management, 30*(3), 695–713. https://doi.org/10.1111/poms.13300

Kang, W. (2021). Policing Fraud in Two Police Jurisdictions: England and Wales and South Korea. *Policing: A Journal of Policy and Practice*. https://doi.org/10.1093/police/paab036.

Chung, T.-J. (2008). Policing internet fraud: A study of the tensions between private and public models of policing fraudulent activity in cyberspace with particular focus on South Korea and special reference to the United Kingdom and the United States

[Doctoral dissertation, University of Portsmouth].

Jeong, H. (2025). Legal Response to Corporate Fraud in South Korea: A Case Study of the Samsung C&T and Cheil Industries Merger Scandal. *Law and Economy*. https://doi.org/10.56397/le.2025.01.01.

Jang, Y., & Suh, Y. (2024). Cyber Sex Crimes Targeting Children and Adolescents in South Korea: Incidents and Legal Challenges. *Social Sciences*. https://doi.org/10.3390/socsci13110596.