本論文獲得法務部司法官學院115年傑出碩博士犯罪防治研究論文獎

中央警察大學警察政策研究所

博士論文

指導教授：黃翠紋 教授

警察防制電信網路詐欺犯罪策略之研究：以假投資詐欺為中心

A Study on Police Crime Prevention Strategies for Telecom-Related Online Fraud: A Focus on Online Investment Fraud

研 究 生：蘇信雄

中華民國 115 年 1 月

謝誌

歲月流轉，重返母校攻讀博士學位的學習旅程，即將畫下句點。回首來時路，最初僅是希望充實工作所需之專業學養與論述能力，也為自己保留一份持續精進、不輕言放棄的信念，於接近知天命之際，再度踏入校園。回顧七年三個月的求學歲月，每週一次的課堂時光，始終是我最為珍惜與期待的日子，不僅成為調適心境、紓解繁重工作壓力的重要時刻，更讓我得以重新沉澱思緒，回到閱讀與思考之中，在師長的引導下汲取新知、拓展視野。縱然歷程艱辛、步履不易，但此刻回望，心中滿懷感謝，並對完成這段階段性的求學之路，深感踏實，並心存感恩。

本論文得以順利完成，首先必須衷心感謝恩師黃教授翠紋，研究歷程中，無論是在研究方向的釐清、研究方法的選擇、研究架構的建構，或訪談資料的整理與論文撰寫的反覆修訂，您始終耐心提點、細心指引，並於繁忙行程中撥冗指導，使本研究得以逐步深化並趨於完善。您長期的提攜與栽培，不僅是學術上的引領，更是治學態度與研究精神的重要示範，謹致以由衷的敬意與感謝。

同時，誠摯感謝論文審查委員鄭教授善印、朱教授金池、洪教授文玲、許福教授福生撥冗指導，於審查與口試過程中，提出多項兼具理論深度與實務觀點的寶貴建議，使本論文在內容完整性與論述嚴謹性上均獲得實質提升，亦促使本人重新審視研究觀點，深化學術思維與研究視野。

此外，亦要感謝所有參與本研究之警界長官與實務界先進，在公務繁忙之際，仍慨然分享防制電信網路詐欺犯罪的第一線經驗與專業見解，使本研究得以貼近實務現場，增添豐富而真實的研究內涵，各位的協助與信任，皆銘記於心。

求學期間，亦感謝進益及坤寶同學在課業與研究歷程中的相互扶持與鼓勵。能與具備豐富實務經驗、來自不同領域的同學共學互勉，不僅拓展專業視野，更豐富人生閱歷，這段相互砥礪的學習時光，將成為我人生珍貴而難忘的記憶。

最後，謹向我的雙親致上最深的感謝，感謝您們賦予我樂觀、勤奮與刻苦的性格，使我在從警生涯中，得以不畏艱難、持續前行。本論文亦謹獻給我最摯愛的妻子，感謝妳三十餘年來無怨無悔的支持與陪伴，於低潮時給予安慰與鼓勵，於順遂時適時提醒，使我得以穩健前行。因為有妳，才有今日的我；因為有妳，我們才擁有三個可愛的孩子。妳不僅是家庭最堅定的支柱，更是我最親密的戰友與伴侶。未來，仍願攜手同行，共創幸福的人生。最後，也想再次對孩子們說，老爸能做到的，你們一定也行，加油！。

蘇信雄謹誌

中華民國 115 年 1 月

摘要

隨著電信通訊、社群媒體與數位金融服務之快速發展，電信網路假投資詐欺犯罪逐漸展現高度組織化與具階段性之犯罪運作模式，其運作方式不僅變化迅速，亦持續暴露出現行防制制度架構之限制。於防制實務上，警察機關除須因應跨境性、匿名性與科技化所帶來之挑戰外，亦面臨犯罪成因日益複雜化與防制資源分散等結構性困境。基此，本研究旨在從犯罪成因、理論解釋、防制策略與執行成效等層面，系統性探討臺灣電信網路假投資詐欺犯罪之運作樣態，並重新審視警察防制犯罪策略之角色定位與強化方向。

本研究採用文獻探討法與質性研究方法，蒐集環境犯罪學相關理論、官方統計資料、政策文件與實務訪談資料，結合理性選擇理論、日常活動理論、犯罪腳本分析、情境犯罪預防與問題導向警政等觀點，建構電信網路假投資詐欺犯罪之整體分析架構，並據以解析犯罪流程、制度斷點與警察防制作為之互動關係。

研究發現，電信網路假投資詐欺已由零散事件發展為具高度模組化與可複製性的詐欺犯罪產業鏈，其運作橫跨犯罪前準備、主要犯罪行為與犯罪後行為等多個階段。犯罪者藉由組織分工、技術工具與人頭資源配置，形成多重斷點與時間差設計，使犯罪流程具高度封閉性。警察防制面向上，打詐五面向雖已形成政策架構，然在制度整合、資訊共享、科技應用與跨境合作等層面仍存在落差，影響整體防制效能。

綜合研究結果，本研究建議警察防制電信網路假投資詐欺犯罪，應回到犯罪腳本之整體視野，於犯罪早、中、晚期同步配置打詐五面向之防制措施，並透過制度統整、科技強化與組織合作，系統性提高犯罪風險、增加犯罪成本並降低犯罪報酬，以促使詐欺犯罪由高報酬、低風險結構，逐步轉向高風險、低報酬之不利運作環境，作為建構長期穩定防制體系之基礎。

關鍵詞：警察防制犯罪策略、電信網路詐欺犯罪、假投資詐欺

Abstract

With the rapid development of telecommunications, social media, and digital financial services, telecom-related online investment fraud has increasingly demonstrated highly organized and stage-based criminal operational patterns. These modes of operation not only evolve rapidly but also continuously expose the limitations of existing crime prevention and regulatory frameworks. In crime prevention practice, police agencies are required to address challenges arising from cross-border operations, anonymity, and technological sophistication, while simultaneously confronting structural difficulties such as increasingly complex crime causation and fragmented prevention resources. Accordingly, this study aims to systematically examine the operational patterns of telecom-related online investment fraud in Taiwan from the perspectives of crime causation, theoretical interpretation, prevention strategies, and enforcement outcomes, and to reassess the role positioning and enhancement directions of police crime prevention strategies.

This study adopts a literature review approach and qualitative research methods, drawing upon environmental criminology theories, official statistical data, policy documents, and in-depth interviews with practitioners. By integrating rational choice theory, routine activity theory, crime script analysis, situational crime prevention, and problem-oriented policing, this research constructs a comprehensive analytical framework for telecom-related online investment fraud, which is used to examine criminal processes, institutional breakpoints, and the interactions between criminal operations and police prevention practices.

The findings indicate that telecom-related online investment fraud has evolved from isolated incidents into a highly modular and replicable fraud industry. Its operations span multiple stages, including pre-crime preparation, core criminal activities, and post-crime processes. Through organizational division of labor, the use of technological tools, and the deployment of nominee accounts, offenders create multiple breakpoints and time-delay mechanisms, resulting in a highly closed and resilient crime process. From the perspective of police prevention, although Taiwan's five-pillar anti-fraud framework has been established as a policy structure, gaps remain in institutional integration, information sharing, technological application, and cross-border cooperation, thereby undermining overall prevention effectiveness.

Based on these findings, this study recommends that police strategies for preventing telecom-related online investment fraud should return to a holistic crime script perspective, with coordinated deployment of the five anti-fraud measures across the early, middle, and late stages of the criminal process. Through institutional integration, technological

enhancement, and strengthened organizational cooperation, prevention strategies can systematically increase criminal risks, raise criminal costs, and reduce expected criminal rewards. Such an approach may gradually transform online investment fraud from a high-reward, low-risk activity into a high-risk, low-reward operating environment, thereby forming the foundation for a stable and sustainable long-term crime prevention system.

Keywords: police crime prevention strategies; telecom-related online fraud; online investment fraud

目錄

謝誌.....I
摘要.....III
Abstract.....V
第一章 緒論.....1
第一節 研究背景與動機.....1
第二節 研究問題與目的.....4
第三節 重要名詞詮釋.....5
第二章 理論基礎與相關文獻探討.....9
第一節 解釋電信網路詐欺犯罪之理論與防制策略.....9
第二節 臺灣電信網路詐欺犯罪現況及防制策略.....44
第三節 主要國家電信網路詐欺犯罪現況及防制策略.....64
第四節 臺灣與主要國家防制電信網路詐欺策略比較.....119
第三章 研究設計與實施.....125
第一節 研究步驟與架構.....125
第二節 資料蒐集方法.....128
第三節 研究工具.....129
第四節 抽樣方法與樣本來源.....129
第五節 資料處理與分析.....130
第六節 研究倫理.....130
第四章 深度訪談資料分析與討論.....133
第一節 電信網路假投資犯罪的成因與現況.....133
第二節 電信網路假投資詐欺犯罪的犯罪腳本.....152
第三節 防制電信網路假投資詐欺犯罪面臨的困境與對策.....164
第五章 結論與建議.....187
第一節 主要研究發現.....187
第二節 未來政策推動建議.....199

第三節 後續研究建議 205
第四節 研究限制 207
參考文獻 209
附錄一 電信網路假投資詐欺犯罪案例 223
附錄二之一 刑事警察人員訪談大綱 257
附錄二之二 金融監督管理委員會人員訪談大綱 259
附錄二之三 國家通訊傳播委員會人員訪談大綱 261
附錄二之四 數位發展部人員及民間業者訪談大綱 263
附錄三 訪談同意書 265

表目錄

表 1-1 2015 年至 2024 年臺灣刑案破獲數及嫌疑犯數統計 2
表 1-2 2022 年至 2024 年臺灣假投資詐欺案件統計表 3
表 2-1 影響深遠的環境犯罪學方法年表 11
表 2-2 犯罪腳本的分析與應用 25
表 2-3 過程評估與影響評估之區別 37
表 2-4 現今的 25 項情境犯罪預防技術 40
表 2-5 2020 年至 2024 年臺灣詐欺案件發生數前 5 名 46
表 2-6 2020 年至 2024 年臺灣詐欺案件財損數前 5 名 46
表 2-7 2020 至 2024 年臺灣警察機關查獲詐欺犯罪案件年齡分布表 47
表 2-8 臺灣電信網路詐欺集團機房蔓延過程分析 50
表 2-9 2000 年至 2024 年臺灣全般詐欺犯罪發生數及財損數 52
表 2-10 2024 年 8 月至 2025 年 7 月臺灣全般詐欺犯罪發生數及財損數 61
表 2-11 2021 年日本詐欺案件發生數前 5 名 66
表 2-12 2021 年日本詐欺案件財損數前 5 名 67
表 2-13 2021 年日本欺案件使用犯罪工具前 3 名 67
表 2-14 2022 年日本詐欺案件發生數前 5 名 68
表 2-15 2022 年日本詐欺案件財損數前 5 名 68
表 2-16 2022 年日本詐欺案件使用犯罪工具前 3 名 68
表 2-17 2023 年日本詐欺案件發生數前 5 名 69
表 2-18 2023 年日本詐欺案件財損數前 5 名 69
表 2-19 2023 年日本詐欺案件使用犯罪工具前 4 名 70
表 2-20 2024 年日本詐欺案件發生數前 5 名 70
表 2-21 2024 年日本詐欺案件財損數前 5 名 71
表 2-22 2024 年日本詐欺案件使用犯罪工具前 4 名 71
表 2-23 2021 年新加坡詐欺案件發生數前 5 名（含財損） 81
表 2-24 2021 年新加坡詐欺案件使用犯罪工具前 5 名 82
表 2-25 2022 年新加坡詐欺案件發生數前 5 名（含財損） 82
表 2-26 2022 年新加坡詐欺案件使用犯罪工具前 5 名 83
表 2-27 2023 年新加坡詐欺案件發生數前 5 名（含財損） 83
表 2-28 2023 年新加坡詐欺案件使用犯罪工具前 5 名 84
表 2-29 2024 年新加坡詐欺案件發生數前 5 名（含財損） 84
表 2-30 2024 年新加坡詐欺案件使用犯罪工具前 5 名 85
表 2-31 2021 年澳洲詐欺案件發生數前 5 名 91
表 2-32 2021 年澳洲詐欺案件財損數前 5 名 92
表 2-33 2021 年澳洲詐欺案件使用犯罪工具前 5 名 92
表 2-34 2022 年澳洲詐欺案件發生數前 5 名 93

表 2-35 2022 年澳洲詐欺案件財損數前 5 名 93
表 2-36 2022 年澳洲詐欺案件使用犯罪工具前 5 名 93
表 2-37 2023 年澳洲詐欺案件發生數前 5 名 94
表 2-38 2023 年澳洲詐欺案件財損數前 5 名 94
表 2-39 2023 年澳洲詐欺案件使用犯罪工具前 5 名 95
表 2-40 2024 年澳洲詐欺案件發生數前 5 名 95
表 2-41 2024 年澳洲詐欺案件財損數前 5 名 96
表 2-42 2024 年澳洲詐欺案件使用犯罪工具前 5 名 96
表 2-43 英國詐欺案件發生數 2021 年與 2020 年比較表 104
表 2-44 英國預付費詐欺與金融投資詐欺案件發生數 2021 年與 2022 年比較表 104
表 2-45 2021 年英國詐欺案件發生數前 5 名 105
表 2-46 英國詐欺案件發生數 2022 年與 2021 年比較表 105
表 2-47 英國其他詐欺與零售詐欺案件發生數 2021 年與 2022 年比較表 106
表 2-48 2022 年英國詐欺案件發生數前 5 名 106
表 2-49 英國詐欺案件發生數 2023 年與 2022 年比較表 107
表 2-50 2023 年英國詐欺案件發生數前 5 名 107
表 2-51 英國詐欺案件發生數 2024 年與 2023 年比較表 108
表 2-52 2024 年英國詐欺案件發生數前 5 名 109
表 2-53 主要國家識詐面向作法與政策特徵 121
表 2-54 主要國家堵詐面向作法與政策特徵 121
表 2-55 主要國家防詐面向作法與政策特徵 122
表 2-56 主要國家阻詐面向作法與政策特徵 123
表 2-57 主要國家懲詐面向作法與政策特徵 123
表 3-1 深度訪談對象分配表 129

圖目錄

圖 1-1 2015 年至 2024 年臺灣詐欺案件發生數及財損金額 3
圖 2-1 電信網路假投資詐欺犯罪活動模型 17
圖 2-2 參與電信網路假投資詐欺的開始階段 18
圖 2-3 習慣參與電信網路假投資詐欺的階段 19
圖 2-4 終止參與電信網路假投資詐欺的階段 20
圖 2-5 日常活動理論概念圖 21
圖 2-6 電信網路假投資詐欺犯罪流程 27
圖 2-7 SARA 流程模型 32
圖 2-8 治安問題分析三角 33
圖 2-9 SARA 流程及評估 36
圖 2-10 2020 年至 2024 年臺灣全般詐欺與投資詐欺發生數比較 45
圖 2-11 2020 年至 2024 年臺灣全般詐欺與投資詐欺財損金額數比較 45
圖 2-12 臺灣電信網路假投資詐欺集團組織架構圖 48
圖 2-13 臺灣電信網路詐欺犯罪流程圖 54
圖 2-14 臺灣防制詐欺犯罪工作四大面向圖 55
圖 2-15 臺灣防制詐欺犯罪工作 3 減策略圖 56
圖 2-16 臺灣政府防制詐欺組織架構 56
圖 2-17 臺灣政府防制詐欺四大面向策略 57
圖 2-18 臺灣防制詐欺四大面向分項指標 57
圖 2-19 臺灣詐欺犯罪危害防制條例架構圖 58
圖 2-20 臺灣打詐綱領 2.0 核心概念 59
圖 2-21 臺灣打詐綱領 2.0 組織架構 60
圖 3-1 本研究流程示意圖 125
圖 3-2 本研究工作進度甘特圖 126
圖 3-3 本研究架構圖 127
圖 4-1 電信網路假投資詐欺犯罪腳本流程 163

第一章 緒論

本章分三節，第一節為研究背景與動機，針對本研究緣起加以敘述，並說明本研究關注議題之背景與研究之動機；第二節為研究問題與目的，藉以提出具體可供探究之研究問題並釐清相關主要研究目的；第三節為重要名詞詮釋。

第一節 研究背景與動機

2024 年 2 月 16 日中正大學犯罪研究中心及犯罪防治學系，針對 2023 年全年度臺灣民眾對司法與犯罪防制滿意度調查研究報告指出（楊士隆、鄭瑞隆、許華孚、馬躍中，2024）：

民眾對「警察維護治安工作」的滿意程度持續顯著上升；對政府詐欺防制滿意度下滑，創歷年新低…，今年度的調查顯示，民眾對於「政府防制詐欺犯罪」的滿意度為 37.62%，為近十年來的新低。在 2023 年間，柬埔寨等地利用錯誤資訊引誘國人出境的事件以及近期投資詐欺之猖獗，可能促使民眾對政府防制詐欺的信心造成重大影響。…。

根據內政部警政署統計資料顯示，近 10 年（2015 年至 2024 年）全般刑案（不含過失駕駛）查獲數，除 2020 年至 2022 年，COVID-19[1]疫情期間降至 22 萬至 23 萬餘件外，都穩定維持在 24 萬至 26 萬餘件，犯罪嫌疑人則維持在 24 萬至 27 萬餘人。但竊盜犯罪從 2015 年的 55,055 件，降到 2024 年的 38,024 件（-30.09%），犯罪嫌疑人總數近十年亦減少 530 人。暴力犯罪從 2015 年的 2,008 件，降到 2024 年的 368 件（-81.67%），犯罪嫌疑人從 2,522 人，降到 2024 年的 597 人（-76.32%）；毒品犯罪則從 2015 年的 49,576 件，逐年上升到 2017 年最高點的 58,515 件（+18.03%），隨後再逐年下降到 2024 年的 36,364 件（與 2017 年最高點比較-37.85%，與 2015 年比較-26.64%），犯罪嫌疑人則是從 2015 年的 53,622 人，上升到 2017 年的 62,644 人（+16.82%），隨後降到 2024 年的 37,854 人（與 2017 年最高點比較-39.57%，與 2015 年比較-29.4%）。然而，詐欺犯罪卻從 2015 年的 17,958 件，占當年全般刑案（不含過失駕駛）查獲總數 260,178 件的 6.9%，增加到 2024 年的 59,074 件，占當年全般刑案（不含過失駕駛）查獲總數 257,914 的 22.9%，較十年前增加 41,116 件（詐欺犯罪+228.95%；全般刑案（不含過失駕駛）+16%）。犯罪嫌疑人也從 2015 年的 17,283 人，增加 2024 年的 53,783 人（+211.19%），詐欺犯罪破獲數及犯罪嫌疑人數雙雙達到近十年的新高點（如表 1-1）。

[1]係「*Coronavirus Disease 2019*」之縮寫，中文正式名稱為「2019 冠狀病毒疾病」。

表 1-1 2015 年至 2024 年臺灣刑案破獲數及嫌疑犯數統計

統計期	全般刑案(不含駕駛過失)		竊盜		暴力犯罪		毒品		詐欺	
	破獲數	嫌犯數	破獲數	嫌疑犯	破獲數	嫌犯數	查獲數	嫌犯數	破獲數	嫌犯數
2015	260,178	256,001	55,055	33,913	2,008	2,522	49,576	53,622	17,958	17,283
2016	260,443	259,094	48,898	31,543	1,656	2,208	54,873	58,707	19,812	20,321
2017	263,795	273,111	46,022	32,204	1,293	1,910	58,515	62,644	20,833	24,330
2018	255,913	276,086	43,262	32,028	995	1,666	55,480	59,106	21,678	27,237
2019	242,280	260,776	40,406	31,398	898	1,464	47,035	49,131	21,936	29,581
2020	237,372	264,292	36,597	29,128	737	1,195	45,489	47,779	22,647	33,631
2021	221,454	245,458	34,826	27,929	597	1,073	38,644	40,987	24,484	36,002
2022	236,254	270,377	36,603	31,139	497	761	38,088	39,964	28,718	45,540
2023	245,264	273,152	38,092	32,245	458	826	36,554	38,581	36,280	50,698
2024	257,914	263,026	38,024	33,383	368	597	36,364	37,854	59,074	53,783

資料來源：內政部警政署(2025a)。警政統計查詢網。取自：https://ba.npa.gov.tw/statis/webMain.aspx?k=defjsp，最後瀏覽日期：2025 年 4 月 18 日。

為遏止電信網路詐欺犯罪持續高發，行政院於 2022 年 7 月 15 日訂頒《新世代打擊詐欺策略行動綱領》（以下簡稱打詐綱領），結合法務部、內政部、國家通訊傳播委員會、金融監督管理委員會等機關成立『打詐國家隊』，以「識詐、堵詐、阻詐、懲詐」4 大面向破解詐欺手法，建立國內「防詐欺、毀工具、擋金流、清集團」終極目標。惟實施後詐欺案件發生數及財損金額仍持續高發，再於 2023 年 6 月 9 日訂頒《新世代打擊詐欺策略行動綱領 1.5 版》（以下簡稱打詐綱領 1.5）(行政院，2023)，新增 4 項策略及 17 項行動方案及相關預算編列，俾賡續透過「宣導教育」、「犯罪通路」、「贓款流向」及「偵查打擊」等四大面向，整合各部會力量，並透過公私部門協力，從法律面和技術面減少通信流及加重詐欺刑責，希冀發揮「前端阻卻」及「後端查緝」之效用，以減少受害者，掃除詐欺集團，達到有效抑制詐欺犯罪，保障人民財產安全的目標(行政院，2022；內政部警政署，2022a;b)。

惟政府在採行相關防制措施後，詐欺集團犯罪模式與手法亦隨之改變，致發生法令不完備情形。為落實打詐綱領，強化源頭管理，立法院於 2024 年 7 月陸續三讀通過《詐欺犯罪危害防制條例》（以下稱詐防條例）、《通訊保障及監察法》、《刑事訴訟法特殊強制處分專章》及《洗錢防制法》等修正草案(法務部，2024)，其中，詐防條例採取「就源」及「溯源」之「雙源齊清」方向，以「強化防詐作為、打擊詐欺集團、保護犯罪被害」三大重點為主軸，從金融、電信及數位經濟相關產業等三面向著手。行政院為即時應處詐欺犯罪手法之演進，並與上述「打詐新 4 法」相輔相成，進一步於 2025 年 1 月 1 日開始實施《新世代打擊詐欺策略行動綱領 2.0》（以下簡稱打詐綱領 2.0）（行政院，2024），並新增「防詐」面向，由數位發展部擔任統籌機關，強化數位經濟產業管理。設立「強化防詐意識、減少發生數、降低財損數」3 項目標，從「識詐、堵詐、防詐、阻詐、懲詐」5 大面向（以下簡稱打詐五面向）著手，跨部會推動「厚植防詐知能、落實電信、網路、金融源頭管理、刨根溯源查緝」等相關工作，並與金融機構、虛擬資產服務提供、電信事業、網路廣告平臺、第三方支付服務、電商及網路連線遊戲等 7 大防詐關鍵產業公私協力，以收抑制詐欺犯罪危害之效，保障民眾財產安全(行政院，2024)。

多年來臺灣警察機關防制電信網路詐欺犯罪雖一向採取打防並舉策略，但犯罪危害情形不但未見消聲匿跡，近幾年還日見猖獗。觀察臺灣近 10 年（2015 年至 2024 年）詐欺案件發生數總計達 293,073 件，財損金額達 871 億餘元，並自 2020 年開始急速上升至 2024 年止，5 年間案件發生數成長 432.68%，財損金額更成長 1080.96%[2]（如圖 1-1）。

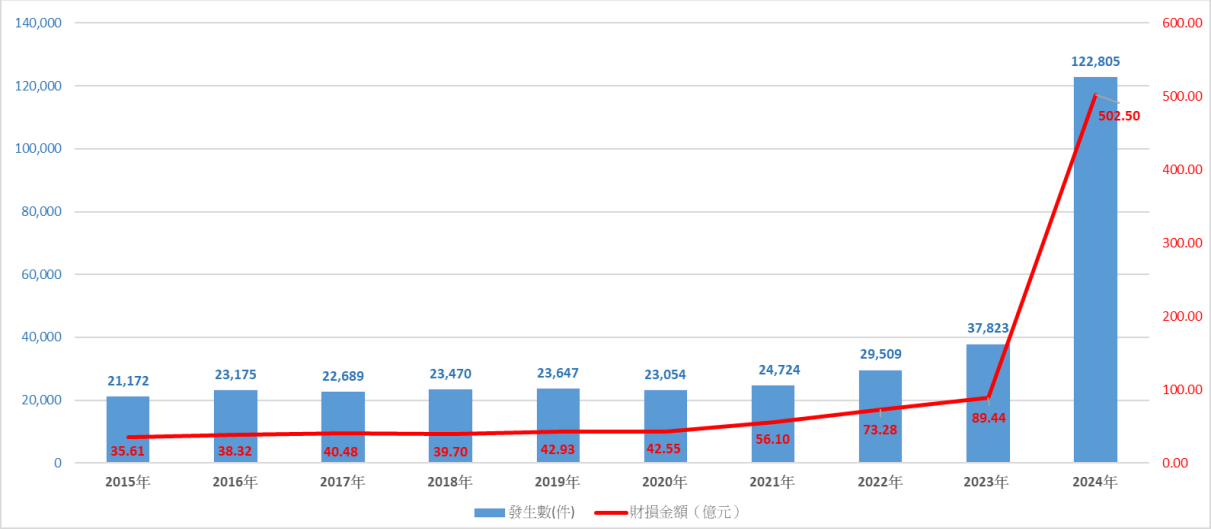


圖 1-1 2015 年至 2024 年臺灣詐欺案件發生數及財損金額

資料來源：整理自內政部警政署刑事警察局（2015－2024）。刑案紀錄表。

其中，假投資詐欺更是從 2022 年發生 6,542 件，到 2024 年增長至 43,015 件，增加 36,473 件（+557.52%），假投資詐欺發生數在 2022 年佔全般詐欺 22.17%，但到 2024 年佔比已上升至 35.03%。損數亦從 2022 年的 37 億元，到 2024 年 372.2 億元，增加 335.2 億元（+增加 905.94%），假投資詐欺的財損在 2022 年佔全般詐欺 50.55%，到 2024 年佔比已高達 74.07%（如表 1-2）。

表 1-2 2022 年至 2024 年臺灣假投資詐欺案件統計表

年度/項目		2022年		2023年		2024年	
		數值	占全般比	數值	占全般比	數值	占全般比
假投資詐欺	發生（件）	6,542	22.17%	11,775	31.13%	43,015	35.03%
	破獲（件）	6,404	22.30%	11,212	31.16%	26,453	41.57%
	財損（億元）	37	50.55%	53.7	60.01%	372.2	74.07%

資料來源：整理自內政部警政署刑事警察局（2022－2024）。刑案紀錄表。

由上觀之，電信網路詐欺犯罪已成為當前臺灣最嚴重的治安問題之一。其中，假投資

2.2024 年 9 月起，內政部警政署進行刑案紀錄系統改革，變更統計方式，使刑案統計數據貼近治安現況，內政部網站「刑案統計制度革新 迎向大數據時代」，網址 https://www.moi.gov.tw/News_Content.aspx?n=9&s=320311 最後瀏覽日 2024 年 11 月 8 日）。爰呈現件數、財損大幅增加情形，並於於同年 11 月發生件數及財損數趨於平緩。

詐欺犯罪更是電信網路詐欺犯罪的主流，對民眾財產安全造成莫大的危害，常使被害人傾家蕩產，畢生積蓄遭詐一空、造成民眾恐慌，減損社會互信，更衝擊人民對政府施政能力的信心，（鄧煌發 2010；汪子錫、葉毓蘭，2013；蘇信雄，2022；賴鼎銘、范巽綠、趙永清、葉宜津、林文程、賴振昌、王麗珍；2024），臺灣對於電信網路詐欺犯罪的學術著作雖然繁多，但對於研究假投資詐欺犯罪類型相對稀少，因此本研究聚焦探討警察機關防制電信網路假投資詐欺策略。

第二節 研究問題與目的

一、研究問題

隨著電信通訊、社群媒體與數位金融服務的普及，電信網路假投資詐欺犯罪逐漸展現出高度組織化與流程化特徵，其運作模式不僅快速變化，亦持續突破既有防制措施之限制。實務上，警察機關在偵辦與防制過程中，除面臨跨境性、匿名性與科技化等挑戰外，亦須回應犯罪成因複雜化與防制資源分散等結構性困境。基此，實有必要從犯罪成因、理論解釋、防制策略與執行成效等層面回答以下問題，以釐清電信網路假投資詐欺犯罪之全貌，並作為後續策略研擬之基礎。

(一)電信網路假投資詐欺犯罪的成因及現況？

(二)解釋電信網路假投資詐欺犯罪的理論？

(三)目前主要國家防制電信網路假投資詐欺犯罪的主要策略，有那些可供臺灣參考？

(四)目前警察機關防制電信網路假投資詐欺犯罪的主要策略？

(五)目前警察機關防制電信網路假投資詐欺犯罪的成效與面臨的困境？

二、研究目的

基於前述研究問題，本研究旨在透過系統化的文獻探討與質性研究方法，全面分析臺灣電信網路假投資詐欺犯罪之成因、運作特性與警察防制實務現況，並進一步比較主要國家之防制策略與執行經驗。藉由導入犯罪腳本分析與環境犯罪學相關理論，本研究期望重新審視警察機關在防制電信網路假投資詐欺犯罪中的策略角色與介入重點，進而提出有助於提升整體防制效能之政策與實務建議，具體而言本研究期望達成以下研究目的。

(一)探討臺灣電信網路假投資詐欺犯罪之成因與現況，並分析警察機關防制困境與對策。

(二)了解電信網路假投資詐欺犯罪實施過程的所有階段，藉以建構犯罪腳本，再導入情境犯罪預防技術阻斷或減少犯罪機會。

(三)比較主要國家防制電信網路假投資詐欺犯罪的策略及成效。

(四)研擬臺灣警察防制電信網路假投資詐欺犯罪策略，以提昇政府治理效能。

第三節 重要名詞詮釋

一、警察防制犯罪策略

「防制」一詞常被用以指涉超越單純刑事制裁之犯罪治理概念。相關研究指出，犯罪防制不僅在於犯罪發生後之查緝與處罰，更重要者，係透過制度、環境與組織安排，降低犯罪發生之可能性與誘因。Clarke（1995a；1995b；1997a）指出，犯罪防制的核心在於改變犯罪發生的情境條件，使潛在犯罪行為人感知到犯罪成本提高、成功機率降低，進而抑制其犯罪決策，此一觀點亦構成情境犯罪預防理論的重要基礎。此外，環境犯罪學進一步強調，犯罪防制係一種需持續調整與回饋的連續性過程，而非僅於特定時間點進行之單一介入行為（Clarke, 1995b；Felson & Clarke, 1998）。

Felson 和 Clarke（1998）及 Felson（2002）之日常活動理論指出，犯罪的發生係犯罪者、合適目標與缺乏有監控能力者在場三者同時存在之結果；因此，犯罪防制工作在於透過制度與組織設計，使「有監控能力者」得以有效進入犯罪情境，從而破壞犯罪成立之結構條件。

另在公共政策層次上，犯罪防制亦被視為一種策略性治理行動。相關研究指出，面對現代高度複雜與多元的犯罪問題，由警察單獨承擔之執法導向手段往往難以奏效，必須結合法制、行政、產業監理與社會參與等多元政策工具，方能形成具整體性與持續性的防制架構（Tonry 和 Farrington, 1995）。此一論述凸顯犯罪防制工作的跨部門特性，亦為現代國家犯罪治理的重要發展方向。

在此學理基礎下，行政院自 2025 年 1 月起執行之打詐綱領 2.0，即將防制電信網路詐欺犯罪定位為涵蓋打詐五面向之整體治理工程，並透過跨部會分工與公私協力，將防制作為一項持續運作且可動態調整之國家行動。因此，本研究所稱之「防制」，係指在學理與政策雙重脈絡下，透過制度建構、科技應用與組織合作，於犯罪發生前、進行中及發生後各階段，系統性降低電信網路詐欺犯罪發生機會，並減輕其社會危害之整體治理作為。

而「策略」一詞則源自組織理論與政策分析領域，強調行動並非零散措施之集合，而係經深思熟慮後形成之整體規劃。Mintzberg（1987；1994）指出，策略係組織在特定環境條件下，為達成長期目標所形成之行動模式，其重點不在於單一決策，而在於整體行動邏輯的一致性。在犯罪防制研究中，策略概念亦被廣泛運用。

Goldstein（1979；1990）於問題導向警政理論中即指出，警察策略應建立在對犯罪問題成因與脈絡之深入分析基礎上，透過整合多元手段與外部資源，針對問題本身進行回應，而非僅重複傳統執法作為。進一步而言，策略亦具有動態調整之特性。政策研究指出，面對快速變動的犯罪手法與科技環境，策略若無法隨情境變化而修正，易流於形式化或績效導向，難以產生實質防制效果。

在此理論脈絡下，打詐綱領 2.0 所呈現之策略，係以中央統籌、分工執行為原則，透

過打詐指揮中心之設置，整合內政部、國家通訊傳播委員會、數位發展部、金融監督管理委員會與法務部等機關之權責，並結合關鍵產業共同參與，形成具層次性與互補性之防制體系（行政院，2024）。因此，本研究所稱之「策略」，係指警察機關在國家整體打詐政策架構下，基於對電信網路詐欺犯罪成因、犯罪腳本與情境特徵之系統性理解，所形成之整體行動構想與資源配置安排，其目的在於提升防制作為之整體效能與持續性。

綜合上述，本研究所稱之「警察防制犯罪策略」，係指警察機關在學理引導與國家政策框架下，結合跨部會分工與公私協力機制，依據對詐欺犯罪成因與犯罪腳本之審思與分析，所建構之整體防制行動規劃；其核心在於透過策略性整合，降低詐欺犯罪發生機會，並強化社會整體防護能力。

二、電信網路詐欺犯罪

學者孟維德認為「電信詐欺犯罪模式即為，假借各項虛構之身分及名義，利用資訊、通訊及大眾傳播媒介等管道，傳遞不正訊息給社會大眾，再進一步操弄、掌握及誘騙，並透過金融服務管道，將被害者的金錢迅速移轉至人頭帳戶，甚至直接以假冒的身分，親自向被害者索取款項」(孟維德，2010)。學者汪子錫等認為「欺騙者利用電信通話或者網路連絡，有時加上假證件、假公函佐證，再配合所掌握的個人資料，就有機會使他人信以為真，誘人入彀。如果接收者無法偵測到欺騙意圖，就可能成為受害者」（汪子錫、葉毓蘭，2013）。

犯罪者利用資通訊匯流技術及金融科技快速發展，民眾通訊方式普遍由電訊轉向網路聯繫機會，藉由加密通訊 APP、VPN 跳板及跨境寬頻網路(xDSL、Cable、FTTB 等)、新型態電信服務 (4G、5G、DMT、VoWiFi)或 Skype、ISR 等國際話務服務上網連結網路電話(VoIP)，配合群呼系統(I.V.R)[3]發話給民眾，以隱匿真實身分同時竄改境外來電顯示，輔以駭客盜取的民眾個資及非法取得之人頭金融帳戶，再透過社交（交友）軟體（Instagram、Tinder、派愛族等）、手機通訊軟體（Line、WeChat、Telegram 等）等遠程非接觸式工具，發送海量虛假訊息；以利益誘惑、虛構危險、虛假恐嚇，或利用民眾一時疏忽等心理因素，以假中獎、假冒公署（假冒警察、檢察官、法院等政府官員）、假簡訊催繳費用、假綁架（恐嚇）、猜猜我是誰、假網路拍賣、假援交、假交友（誘使被害人裸聊或參與博弈、投資）、假投資、解除 ATM 分期付款、混合型結合臨櫃匯款等作為犯罪手法，誘騙或盜取被害人資金或虛擬貨幣匯（存）入其控制的實體或數位銀行人頭帳戶或電子錢包之犯罪行為，甚至直接以假冒的身分，親自向被害者索取款項，且隨著資通訊科技的進步，犯罪手法的演變，治安機關查緝能力的強化，犯罪者基於犯罪理性選擇，逐漸將實施電信網路詐

[3](1)寬頻網路:指 xDSL(數位用戶線路)、Cable(有線電視)、FTTB(光纖)等網際網路提供上網服務，也稱為電信最後一哩路。(2)VoWiFi(Voice over Wi-Fi)網路電話：在境外使用國內門號，可透過當地 WiFi 無線網路連入國內電信業者交換機發話，無須支付漫遊及高額國際通話費用。(3)DMT(Digital Mobile Trunk)行動節費設備：一種網路電話語音與傳統行動電話轉換的中繼傳輸裝置(VoIP Gateway)，詐騙集團在境外以網路電話軟體連入國內機房 DMT 設備，即可使用 SIM 卡進行發話及受話，藉此營造門號持有人在國內假象。(4)IVR(Interactive Voice Response)互動式語音應答：詐騙集團常用來自動(循序/清單方式)撥號給民眾的設備，可以接通 之後播放語音或導引進行互動通話。

欺犯罪的機房，從臺灣往世界各國蔓延(陳玉書、曾百川，2007；何招凡，2010；李堅志，2010；內政部警政署，2024；塗凱竣，2020；蘇信雄，2022)。

此外，臺灣《刑法》第 339 條規定「普通詐欺罪」為：「意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處五年以下有期徒刑、拘役或科或併科五十萬元以下罰金。以前項方法得財產上不法之利益或使第三人得之者，亦同。前二項之未遂犯罰之。」；同法第 339-4 條規定「加重詐欺罪」為：「犯第三百三十九條詐欺罪而有下列情形之一者，處一年以上七年以下有期徒刑，得併科一百萬元以下罰金：一、冒用政府機關或公務員名義犯之。二、三人以上共同犯之。三、以廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散布而犯之。前項之未遂犯罰之」。綜上所述，本文所探討之「電信網路詐欺犯罪」係指：犯罪者利用資通訊匯流技術及金融科技以隱匿真實身分及洗錢管道，運用精心編造配合社會時事或利用被害人貪心、恐懼或疏忽等心理的騙術，再以廣播電視、電子通訊、網際網路或其他媒體等傳播工具對公眾散布，致被害人將自己或第三人之金錢交付或使犯罪者得金錢上不法之利益或使第三人得之者之犯罪行為。

三、假投資詐欺

假投資詐欺係指電信網路詐欺犯罪手法之一，犯罪者先在影音、社群平台(FB、IG、YouTube、交友軟體、簡訊等)大量散播虛假投資訊息，以輕鬆賺錢貼文或假冒名人代言廣告，宣稱保證獲利、穩賺不賠且利潤豐厚為幌子，吸引民眾加入通訊軟體（Line、WeChat等）投資體驗群組，參加由自稱「老師、分析師」等教學投資，且群組內不斷有其他學員獲利貼文藉以博取被害人信任，接著再介紹被害人加入詐欺集團架設的假投資網站，先誆騙被害人小額投資，初期有小額獲利，再引誘投入大筆資金；待要獲利出金時，即以各種理由拒絕出金，或是凍結帳號、關閉網站失去聯繫(內政部警政署，2025b；內政部警政署刑事警察局，2025) 。

第二章 理論基礎與相關文獻探討

臺灣詐欺犯罪在上世紀 90 年代脫離以 3 至 5 人組成「金光黨」，利用人性貪小便宜的弱點，使用人際接觸方式，採取「扮豬吃老虎」手法，以假鈔或假金飾詐欺被害人現金的傳統手法，轉變成犯罪人數動輒數十人，以利用郵寄刮刮樂中獎通知及手機簡訊中獎等非接觸式的犯罪手法行騙的電信詐欺犯罪集團。根據臺灣司法機關判決書顯示，電信詐欺犯罪集團早於 1999 年 8 月即已蔓延至中國大陸廈門地區[4]，而隨著詐欺犯罪往中國大陸地區蔓延，臺灣官方統計資料亦顯示，詐欺案件受理數自 2000 年起逐年增加，並於 2005 年達到 4 萬 3,023 件，財損金額於 2006 年達到 185.88 億餘元（蔡田木，2009；林德華，2010；曾雅芬，2016；蘇信雄，2022)

近 20 餘年來在全球化（globalization）的風潮引領下，資通訊科技高度發展，促使各國通訊和金融都朝向網路化及全球化的同時，亦提供詐欺犯罪趁勢快速往世界各地蔓延的有利犯罪環境，使得利用電信實施詐欺的犯罪集團，轉變為利用電信網路施實施跨境詐欺的犯罪集團，而犯罪統計資料也顯示，網路及電信通訊等新興科技雖帶給人們生活便利，卻也可能淪為犯罪者的犯案工具與媒介(孟維德，2015)。犯罪集團利用各國尚未建立密切合作共同打擊犯罪機制之漏洞，共同犯罪施行遠端遙控跨境犯罪，已蔓延至兩岸、亞洲、非洲、歐洲等 34 個國家地區（曾雅芬，2016；何招凡，2018；蘇信雄，2022；李雅村，2024)。詐欺犯罪被害人亦由臺灣蔓延至中國大陸等地區。跨境電信網路詐欺犯罪危害人民財產安全，使被害人蒙受鉅額財產損失；減損政府威信及社會互信，導致民眾人人自危，嚴重影響日常工作和生活，嚴重破壞國家形象（鄧煌發 2010；汪子錫、葉毓蘭，2013；蘇信雄，2020；賴鼎銘、范巽綠、趙永清、葉宜津、林文程、賴振昌、王麗珍；2024）

本章首先藉由犯罪學理論探討犯罪成因的環境因素，再以環境犯罪學的角度詮釋犯罪者的理性，以日常活動理論瞭解犯罪者與被害人的日常生活，以犯罪腳本的角度進行文獻回顧，剖析電信網路假投資詐欺犯罪歷程，將所有犯罪的細節詳細羅列；再以問題導向警政綜合分析防制困境，最後以情境犯罪預防思考防制政策，以建構本研究之理論基礎；接續運用警政署及法務部的官方次級統計資料分析電信網路詐欺犯罪之特性及趨勢，據以瞭解臺灣詐欺犯罪現況與發展趨勢；再賡續研析臺灣有關電信網路詐欺之防制策略；最後分析主要國家防制電信網路詐欺犯罪的相關政策，並進行研究架構構思，完成警察防制電信網路假投資詐欺犯罪的研究設計。

第一節 解釋電信網路詐欺犯罪之理論與防制策略

為觀察電信網路假投資詐欺犯罪歷程，本研究以七個犯罪學理論為基礎進行討論，包括：分別以犯罪原因論(Etiology of Crime)及環境犯罪學(Environmental Criminology)說明學界探究犯罪成因理論的分類，來探討犯罪者避免痛苦、追求快樂及滿足自我利益的特性及環境對犯罪的影響；以理性選擇觀點，觀察犯罪「機會」和「選擇」對詐欺犯罪者，在決定犯罪時扮演重要的角色的有限理性；運用日常活動理論分析有動機的犯罪者、合適的標的物及缺乏有能力的監控者等三種因素同時存在時空的聚合；犯罪腳本解構犯罪歷程；問題導向警政分析防制犯罪問題；及以情境犯罪預防整合上述理論為基礎進行研究。

[4] 參照臺灣高等法院臺中分院 2003 年 1 月 14 日 91 年上重訴字第 10 號刑事判決判決。

一、犯罪成因

(一)理論介紹

探究犯罪成因之目的在於衡量犯罪行為（Measurement of Criminal Behavior）、了解犯罪行為（nderstanding Criminal Behavior）、控制犯罪行為（Controlling Criminal Behavior）（蔡德輝、楊士隆，2019)。而有關探究犯罪成因的理論，大致可為分二類，第一類為犯罪原因論(Etiology of Crime)此類理論聚焦於「人」的探討，即研究人為何會犯罪?；第二類為環境犯罪學(Environmental Criminology)此類理論聚焦於犯罪事件的探討，即研究犯罪為何會發生？

1.犯罪原因論(Etiology of Crime)

長久以來，研究犯罪人的理論一直是犯罪學發展的主流，而此類研究大多把焦點集中在，為什麼某些特定類型的人會犯罪，以及應該如何處理這些人之上(黃翠紋、孟維德，2017)在遠古時期，人們相信所有的犯罪行為都有一個共同的根源，即超自然的惡魔力量，這一觀點代表著「人們對犯罪行為最古老的觀點」（Pfohl,1994）。人們藉由宗教思想或超自然力的魔鬼說解釋犯罪，認為一個人會犯罪乃因邪魔力量作用的結果，刑罰充斥宗教觀點，人們相信許多家庭具有卑劣的血統。

十八世紀中葉貝加利亞（Cesare Beccaria）邊沁（Jeremy Bentham）為代表的「古典犯罪學派」，提出人的行為是「趨樂避苦」的，人是有自由意志(free will)，可理性選擇犯罪或守法，學者們認為對於犯罪的反應及懲罰愈迅速、確定、嚴厲，愈可控制犯罪行為；當時之研究著重法律之執行，所以又稱「法律犯罪學」。十九世紀後，受社會學創始者法國實證主義(Positivism)哲學家和社會學家孔德（Auguste Comte）以科學方法研究社會的影響；龍布羅梭（Cesare Lombroso）等犯罪學家們開始以講求證據，強調觀察、歸納等邏輯方法的科學方法研究犯罪，將犯罪學研究導向犯罪學實證學派(positivist school)，該學派認為人之所以犯罪是因生理、心理等個體特質的外在因素所決定，分別提出了犯罪生物學理論、犯罪心理學理論及犯罪社會學理論，強調每個犯罪的原因都是不同的，有其個別差別，重視犯罪處遇的個別化。上世紀六十年代末，批判犯罪學（Critical Criminology）風行，犯罪學者們反對傳統實證研究的思考路線，認為性別、種族與階級歧視，權力概念及權力的不平等是造成犯罪的主因。八十年代以後，犯罪學家們發現，複雜的犯罪現象很難以一元性的理論解釋清楚。因此，有不少的犯罪學家嘗試以「整合理論」(intergrated theory)研究不同層面的犯罪現象（許福生，2018)。

晚近犯罪學者們的研究逐漸重視犯罪生涯（Criminal Career）的發展與形成歷程（progression），此即為發展性犯罪理論（Developmental Theory），該理論認為反社會及犯罪行為是逐步發展而成，犯罪之開始（On Set）與持續 （Continuation）並非基於單一因素，而強調用許多的發展因素（developmental factors）的相關聯性來解釋複雜的人類行為，同時認爲早期家庭生活的品質對於一個人反社會行為的發展是很重要的，他們亦主張，早期家庭的缺陷教養或忽略是犯罪的主要因素（許春金，2007）。

美國犯罪學家 Siegel(2007)以生活週期理論（Life Course Theory）及潛伏特質理論（Latent Trait Theory）兩大主軸探討發展性犯罪理論，生活週期理論（Life Course Theory）認為，人類的犯罪因素會隨著個體的成長及社會、個人、經濟等因素的變化，而導致其偏差行為與犯罪行為跟隨著改變。因為，人的犯罪性會受到個體的特質和社會經驗影響。所以，其犯罪生涯是趨向惡化或中止是無法預測的。代表性理論包括 Thornberry 所提出之

互動性犯罪理論（Interactional Theory），主張犯罪行為係個體特質與社會控制因素交互作用下的動態結果（Thornberry, 1987）；Loeber 所進行之少年犯罪路徑研究（Developmental Pathways），指出少年偏差與犯罪行為具有由輕至重、循序發展之多重路徑（Loeber, 1990）；以及 Sampson 與 Laub 所提出之逐級年齡非正式社會控制理論，強調家庭、學校、工作與婚姻等非正式社會連結，會隨生命歷程變化而影響犯罪行為的持續或中斷（Sampson & Laub, 1993）。

相對地，潛伏特質理論（Latent Trait Theory）認為，個體自出生或幼年時期即具有相對穩定之犯罪傾向，且該特質隨時間推移而持續存在，最終肇致犯罪行為。此一觀點中，Aichhorn（1935）即提出潛伏性偏差行為之概念，認為部分個體早期即展現深層偏差傾向；Wilson 與 Herrnstein（1985），以及 Gottfredson 與 Hirschi（1990），亦主張犯罪者普遍具有我行我素、衝動性高及低度自我控制等人格特質。相關代表性研究尚包括 Glueck 夫婦針對少年人格特質所進行之長期追蹤研究（Glueck & Glueck, 1950）、Wolfgang、Figlio 與 Sellin（1972）對慢性犯罪人的實證分析，以及 Gottfredson 與 Hirschi（1990）所提出之一般性犯罪理論與 Colvin（2000）的差別壓迫理論，皆強調穩定人格特質或結構性壓迫對犯罪行為之關鍵影響。

2.環境犯罪學(Environmental Criminology)

環境犯罪學的誕生可以追溯到 1971 年美國犯罪學家 C. Ray Jeffery 提出《透過環境設計預防犯罪》一文，Jeffery 研究當下環境在犯罪中所扮演的角色，提出改變當下環境來減少犯罪的措施，開啟學界運用環境設計的思維，採取犯罪預防措施的策略，同時創造了環境犯罪學這個術語。此後 15 年內，大部分的環境犯罪學與犯罪分析的方法論已經確立(如表 2-1)，而後來的發展主要建立在這些基礎上，環境犯罪學與犯罪分析是由許多相互關聯的方法組成，這些方法或多或少是相互協同發展的。

表 2-1 影響深遠的環境犯罪學方法年表

年份	概念	主要提出人	開創性論文名稱
1971	環境設計預防犯罪	*C. Ray Jeffery*	*Crime revention Through Environmental Design (Jeffery, 1971)*
1972	可防禦空間	*Oscar Newman*	*Defensible Space: Crime Prevention Through Urban Design (Newman, 1972)*
1976	情境犯罪預防	*Ronald Clarke*	*Crime as Opportunity (Mayhew, Clarke, Sturman and Hough, 1976)*
1979	日常活動方法	*Marcus Felson*	*Social Change and Crime Rate Trends: A Routine Activity Approach (Cohen and Felson, 1979)*
1979	問題導向警務	*Herman Goldstein*	*Problem-oriented policing(Goldstein, 1979)*
1981	犯罪模式理論	*Patricia and Paul Brantingham*	*Environmental Criminology (*Brantingham, P.J. & Brantingham, P.L. (eds)*, 1981)*
1982	破窗理論	*James Q. Wilson and George Kelling*	*Broken Windows: The Police and Neighborhood Safety (Wilson and Kelling, 1982)*
1985	理性選擇觀點	*Derek Cornish and Ronald Clarke*	*Modeling Offenders' Decisions: A Framework for Research and Policy (Clarke and Cornish, 1985)*

資料來源：Wortley & M.Townsley, M.(2016).Environmental criminology and crime analysis:Situating the theory, analytic approach and application.In R. Wortley & M.Townsley, M. (Eds.),*Environmental Criminology and Crime Analysis (2 nd ed)*（p8）.London:Routledge.

換言之，環境犯罪學家關注並分析促進犯罪發生當下的時空環境因素，並以改變目標環境為手段來預防犯罪發生。Brantingham 和 Brantingham 認為，犯罪事件的發生是犯罪者、受害者或犯罪目標與法律在特定時間和地點的特定環境中的匯合（Brantingham & Brantingham,1991)。刑事司法及犯罪學者普遍認為，針對犯罪問題進行廣泛且清楚的分析是預防犯罪的關鍵基礎（黃翠紋、孟維德，2017），因此，環境犯罪學必須以犯罪分析為研究工具，所謂犯罪分析即指：「一套系統性的分析過程，提供有關犯罪模式和犯罪趨勢相關性的及時、相關的資訊」（Emig et al ,1980），利用犯罪數據與警察的犯罪報告來研究犯罪問題，這些資料內容應包括犯罪者、受害者和犯罪目標。換言之，環境犯罪學家的任務是發展並提供犯罪分析人員所需理論，犯罪分析人員則在環境犯罪學理論的指導下利用犯罪數據與警察的犯罪報告分析犯罪模式，以支持環境犯罪學家的理論。

環境犯罪學與犯罪分析研究的重點於促成犯罪發生的環境因素，關注的目標是當前的犯罪動態，即犯罪發生在哪裡？何時發生？何人參與？犯罪者做了什麼？為什麼這樣做？以及他們是如何做的？環境犯罪學的目的是預防犯罪，而不是治癒罪犯或改革社會。因此，環境犯罪學與犯罪分析的研究是基於以下三個命題（Wortley & Townsley,2016）：

(1) 環境結構對犯罪人行為有決定性的影響

環境犯罪學的觀點認為所有的犯罪行為都是人與情境互動的結果。環境結構不僅是犯罪人行為的背景，更扮演犯罪人開始和發展犯罪過程中決定性的角色。因此，犯罪事件不僅是由犯罪人造成的，它們同樣是由犯罪現場的環境因素造成的。環境犯罪學的目的即在解釋環境因素如何影響犯罪行為，以及為什麼某些特殊的環境因素會導致犯罪。

(2) 發生犯罪的時間和空間不是隨機分布的

由於犯罪行為取決於情境因素，因此犯罪模式是根據犯罪環境的位置而決定的，犯罪將集中在犯罪機會和其他有利於犯罪活動的特殊時空環境。因此，每一個地區的犯罪率都不盡相同，每一個都市或鄉村，在不同時空環境下就會有不同犯罪情況，而犯罪分析的目的是識別和描述這些犯罪模式。

(3) 了解犯罪環境和犯罪模式是調查、控制和預防犯罪的關鍵因素

這些觀點可以使警察和犯罪預防組織團體，能夠將資源集中在特定地點發生的特定犯罪問題上，經由環境犯罪學和犯罪分析的結合，藉以改變目標環境的犯罪因素，減少該地點的犯罪發生率，為解決犯罪問題提供實用的方案。環境犯罪學與犯罪分析橫跨理論、分析和實踐三個領域，其立論基礎是多學科的，其方法是實證的，其使命是功利主義的。同時參考了社會學家、心理學家、地理學家、建築師、城市規劃師、工業設計師、電腦科學家、人口統計學家、政治學家和經濟學家的想法和專業知識。它包含測量和科學方法，致力於建立理論並提供根植於現有數據的嚴格分析與建議。最後，環境犯罪學家和犯罪分析師積極與執法人員和犯罪預防組織團體合作，幫助減少犯罪（Wortley & Townsley,2016）。

環境犯罪學係透過宏觀、中觀、微觀等三個層次分析犯罪與環境之間的關係（Brantingham & Brantingham,1991)。

(1) 宏觀層次分析

指涉國家之間、特定國家內的州或省或城市之間、或州內的縣或城市之間的犯罪分佈研究。

(2) 中觀層次分析

指涉城市或大都市的各區間的犯罪研究，這些區域代表中觀層次的空間聚合，範圍包括從郊區和各分局到每條街道和地點。

(3) 微觀層次分析

指涉對特定犯罪現場的研究分析，聚焦於建築類型及其佈局、景觀美化和照明、內部設施和安全硬體的研究。與生態方法相比，微觀層面的分析反映日益簡化的哲學，即整體被分解為較小的組成部分，其研究分析重點是當下環境的特定因素，對個人的特定決策和行為的影響，在此層面犯罪分析路線發展的關鍵是心理學界對於個體行為原因發展的軌跡的爭論。心理學家認為人格、態度、信念等心理結構特徵是驅使人類作出不同行為和區分不同人格的方法，在特質理論中，每個人的心理結構都包含不同的面向，而在每個面向上，個體都可能位於這個面向的某一個位置。此一理論對個體性格的詮釋與人類直觀地解釋事件的方式相似，使我們自然傾向於認為每個人都要對自己的行為負完全責任。心理學家將這種認知偏差稱為基本心理歸因錯誤（Jones,1979；Ross,1977）。雖然，這種理論模型在心理學界占有主導地位，但它在心理學中從未被普遍應用，與此同時，學界對行為是受當下環境影響的理論和研究開始感到興趣。Mischel (1968)指出，個體的行為方式，受當下不同環境的影響，可能會有很大差異，例如：我們對待朋友的態度與對待家人的態度即有明顯的不同。行為特異性原則應用於解釋犯罪行為具有重要意義，犯罪者只在相對有利的條件下才會實施犯罪，了解觸發犯罪的環境，對於全面分析犯罪行為有著關鍵作用，從環境犯罪學的角度觀之，微觀層面的分析對於預防犯罪策略的發展有特別重要的影響力。

（二）理論應用

傳統的犯罪學理論主要在關注人類的犯罪行為。該理論試圖從生物因素、個體的生命發展史及社會背景等面向，解釋個體如何成為犯罪者。該理論關注重點在犯罪者的成長過程，並認為犯罪的發生是犯罪人多年來養成的習慣性偏差行為，而這個偏差行為的果，是多年前種下的因，也就是說，一旦個體被種下犯罪因子，其犯罪行為的發生將勢不可避免；因而，該理論對於發生犯罪行為的確切地點和時間也就不再關注，其預防犯罪的觀點是透過填補犯罪者不幸的童年，消除其社會不利地位，並在犯罪後為他們提供康復計劃來改變犯罪者的基本犯罪行為。而環境犯罪學關注的重點則在於促進犯罪事件發生當下的環境因素，該理論置研究重點於當前的犯罪動態，即犯罪事件發生的時間、地點及促成犯罪者選擇犯罪標的、犯罪手段及犯罪過程的原因，環境犯罪學的目的是預防犯罪，而不是治癒罪犯或改革社會。

針對犯罪問題的解釋，儘管解釋事件發生的理論以及解釋犯罪人特性的理論偶有不一致的情況，但是如果能把犯罪人及犯罪事件的解釋整合互補，那麼對於犯罪現象的瞭解將是更有助益的（黃翠紋、孟維德，2017）。因此，在防制電信網路假投資詐欺犯罪的實務上，除非個體真的實施詐欺犯罪行為，否則解釋該個體有極高的詐欺犯罪傾向或動機對

預防犯罪的發生是無用的。同樣，對於解釋犯罪事件發生的理論，也不可忽略電信網路假投資詐欺犯罪者在面對特定環境的差異性和選擇性反應。另外，在功能上，解釋犯罪人形成的理論應該告訴我們個體如何成為詐欺犯罪者，以及在什麼情況下個體會停止詐欺犯罪。此類理論或許可作為潛在嚴重暴力犯罪者，或輕罪累犯者的犯罪預防策略，但迄今為止，有關研究犯罪者的理論並無法在犯罪預測上提供堅實的基礎，而學界對此類理論的未來發展，也幾乎沒有共識，因此，基於犯罪者理論的預防策略還遙不可及（Clarke & Weisburd, 1990）。換言之，植基於犯罪人理論的犯罪預防策略，還有許多尚未確定以及待澄清之處。（黃翠紋、孟維德，2017）。就算未來犯罪學家能夠更瞭解犯罪人的犯罪特性是如何形成的，但是否能夠讓更多具犯罪特性之人不去從事犯罪行為，恐怕仍是一個未知數（孟維德，2011a）。

綜上，目前犯罪學界對於人類犯罪行為的發展與形成等相關研究已是汗牛充棟，具有相當的解釋能力，但對於犯罪事件發生的當下的環境因素，尚缺成熟的解釋的能力。因此，本研究將運用環境犯罪學的相關理論，解釋電信網路假投資詐欺犯罪者選擇犯罪標的理由及犯罪標的吸引潛在犯罪人的原因；以及解構電信網路假投資詐欺犯罪全部過程；並分析防制電信網路假投資詐欺犯罪問題；最後再以改變目標環境為手段來預防犯罪的發生。

二、理性選擇觀點（The rational choice perspective）

(一)理論介紹

Cornish 和 Clarke（2016）認為理性選擇並非傳統的犯罪學理論，它是一種啟發式的概念或工具，其目的在於提供一個強調環境會對犯罪行為產生直接影響的觀點，而環境因素包括日常生活的方式及動機、需求與誘因等，同時也是為實現特定目標而採取工具性行動的特殊環境。本研究參考 Cornish & Clarke 所建構的理性選擇六個核心概念 Cornish 和 Clarke（2016），藉以說明解釋電信網路假投資詐欺犯罪的理性如下：

1.犯罪行為是有目的的

理性選擇觀點認為，犯罪是一種有目的、蓄意的行為，是為了使犯罪者受益。犯罪的好處包括滿足通常的人性動機，如性滿足、興奮、自主、欽佩、報復、控制、減輕緊張、物質財富等的慾望。當然，金錢可以買到許多這樣的滿足感，因此它本身就成為犯罪的一個方便而重要的目標，而電信網路假投資詐欺犯罪的目的即是在獲取金錢。

2.犯罪行為是理性的

吾人大都假設在日常生活中，人類的行為是有目的的，同時也是可理解的，而且是理性的。因此人們在動機和目標選擇上，會嘗試選擇最好方法來實現這些目標。這種理性假設支撐著我們對人類行為的解釋。正如 Herrnstein（1990）所評論的那樣，它「幾乎成為行為科學的基本原則」。然而，假定的理性並不等於完美的理性，在現實世界中，行動往往必須基於在不太完美的情況下做出的決定。電信網路假投資詐欺犯罪本質上即涵蓋被查獲或犯罪失敗的風險，犯罪的成本和可獲得的利益也很難提前估算。縱使犯罪者盡最大努力評估對自己有利與不利的因素後，採取最有利於己的行動，然而，犯罪者的掌握的資訊及犯罪能力均有其限度，因此，犯罪者最後可能只會獲得令犯罪者「滿意」的結果，而不是「最佳」的結果。

3.犯罪決策是針對特定犯罪的

犯罪人實施各犯罪均有其特殊的動機、目的和收益，例如：性侵可能滿足性需求以及支配、控制和羞辱的慾望；住宅盜竊可以滿足對現金或物品的需求，也可以滿足對「偷偷摸摸的刺激」的渴望（Katz,1988）。換句話說，在特定的動機下，實施的特定的犯罪行為，將為犯罪者帶來特定的利益。因此，不同的犯罪人及不同的犯罪類型需要考慮的因素，以及影響其決策的變數也會因犯罪性質的不同而有很大差異。這種情況在犯罪人決定犯罪行為的選擇和決定時尤其明顯。電信網路假投資詐欺犯罪在風險性質、收益，犯罪行為實施、犯罪地點的選擇，就和街頭飛車搶劫犯罪事件有著很大的不同。也就是說，每個犯罪行為之間都存著差別，無法用相同的犯罪決策理論去進行解釋，因為它們可能包括許多不同的動機，而且這些犯罪行為是由各式各樣的犯罪者，使用各種方法和不同程度的技能實施的。因此，就實際預防犯罪的目的而言，區分不同犯罪的選擇和決定是很重要的工作，它能有效幫助相關犯罪防治機關量身設計犯罪防措施。另外，許多犯罪者都是「通才」，在他們的生命史中已或可能犯下各式各樣的犯罪。事實上，經驗豐富的犯罪人可能會在任何特定的時間內參與許多不同類型的犯罪活動。

4.計畫犯罪和參與犯罪需分開研究

犯罪者和潛在犯罪者所做的犯罪決定可概分為計畫犯罪和參與犯罪兩大類，計畫犯罪決定是以犯罪為中心，主要是針對特定類型犯罪所擬定包含準備、實施和完成犯罪行時所作的選擇與決定，儘管完成計畫犯罪的時間會因為犯罪類型有所不同，但犯罪者只要在計畫時間內完成這些犯罪活動即可；因此，犯罪者考慮的因素比較有限，其主要關注重點在於當下的犯罪行為，例如選擇潛在的電信網路假投資詐欺犯罪受害者，或選擇安全的電信網路假投資詐欺犯罪機房地點。參與犯罪決定則涉及犯罪人的犯罪生涯，包括初次參與犯罪（引發）、繼續犯罪（習慣）和停止犯罪的決定，參與犯罪決定包括犯罪的決定和反應，因為關注的變數更廣泛，所以參與犯罪決定的時間長度比計畫犯罪決定的時間更長。計畫犯罪決定和參與犯罪決定一樣都是針對特定的犯罪，所以必須針對不同的犯罪單獨分開研究。例如：參與電信網路假投資詐欺犯罪和參與毒品走私犯罪，兩者犯罪過程及行動的複雜性、犯罪的目的和風險、所需的犯罪技能及成本等等都有明顯的不同，此情況也同時適用於繼續和停止特定犯罪的決定。例如：偷竊車內物品在改善犯罪人經濟能力方面可能不會發生顯著的影響，但參與電信網路假投資詐欺犯罪卻可能大大的改變犯罪人經濟能力。

5.參與犯罪的各階段需分開研究

將犯罪人參與犯罪區分為引發（Initiation）、習慣化（Habituation）與終止（Desistance）三個主要階段，目的在強調每個犯罪階段都有不同的變數影響犯罪人的決定。例如：首次參與電信網路假投資詐欺犯罪的決定，可能會受到先前實施其他類型犯罪的經驗，以及犯罪者性格與成長經歷，當前的生活方式和需求所產生的動機，潛在犯罪者可利用的犯罪機會和誘因。而繼續電信網路假投資詐欺犯罪或停止犯罪的決定，將受到繼續實施犯罪的成功機率，犯罪對犯罪人生活方式的雙重影響。在現實生活中，犯罪會受到犯罪本身節奏或外部因素的影響，例如：犯罪人身體健康狀況、婚姻、家庭重大變故等生活事件和危機，基此，從引發犯罪到停止犯罪的轉變是有可能發生的。另外，犯罪者也有可能同時參與多

種不同形式或種類的犯罪，導致犯罪者需同時作出許多不同選擇和決定，而犯罪者實施某種犯罪所獲得的經驗可能會影響實施其他形式或種類犯罪的決定。在電信網路假投資詐欺犯罪實際案例中，吾人可輕易發現如果犯罪不成功，可能會促使犯罪者減少犯罪頻率甚至停止犯罪。但是，如果犯罪者獲得電信網路假投資詐欺犯罪所需的技術和經驗，即可能在不同時間、不同國家、針對不同目標實施相同類型的犯罪；而且犯罪者伴隨犯罪成功經驗的累積，將更深入掌握電信網路假投資詐欺犯罪的關鍵技術，使犯罪者從犯罪最外圍的領款車手、電話手等次要犯罪角色，往第二線、第三線、甚或機房負責人（桶仔主）等核心犯罪角色轉變，或轉向以不同形式的犯罪手法實施詐欺。

6.犯罪過程是按照犯罪者的決策和具體行動依序展開的

識別犯罪者實施電信網路假投資詐欺犯罪的全部過程，是偵查和預防該類犯罪重要課題，但執法機關與犯罪學界的研究卻往往只關注與犯罪核心相關階段的決策，而沒有等量齊觀的關注犯罪開始和結束階段。為了更徹底地分析犯罪，Cornish 於 1994 年提出了犯罪腳本的概念（Cornish,1994a,1994b），據以說明犯罪者實施特定犯罪的所有過程。該概念可幫助研究者識別犯罪者在犯罪過程中，每個階段所必須採取的決策和行動，以及所需的犯罪資源，並提供一個通用模板，以概述所有犯罪均必須涉及的步驟，犯罪腳本可以揭示在表面上看起來「毫無意義」的犯罪合理性及簡單犯罪的複雜性，其應用範圍可以從簡單的單一犯罪活動到比較複雜的多人、多次、多地的犯罪活動，甚至由多個犯罪腳本組合成高度複雜的有組織犯罪活動，此概念有助吾人進一步證明犯罪者犯罪決策的重要性、其在犯罪活動中的普遍存在及其理性、有目的的本質。因此，本研究將參考 Cornish 所提出的犯罪腳本概念，分析電信網路假投資詐欺的全部犯罪過程使其更容易識別和理解。

（二）理論應用

本研究參考 Clarke 和 Cornish（1985）「郊區入室竊盜」犯罪者犯罪決定的四個決策模型，將電信網路假投資詐欺犯罪者犯罪歷程區分為犯罪活動(The crime even)與引發（Initiation）犯罪、習慣化（Habituation）犯罪、終止（Desistance）犯罪等四個理性選擇四個決策模型如下：

1.犯罪活動（The crime even）

經驗豐富的電信網路假投資詐欺犯罪者在擬定犯罪決策時（圖 2-1）往往只關注阻礙或促進實現犯罪目標的工具性或情境因素。由於需求、動機及道德顧慮、準備情況等問題已經解決，這些因素已不太可能介入犯罪決策過程，除非犯罪者缺乏經驗，或者犯罪行動受到意想不到的阻礙，或發現更好的犯罪機會進而需要改變犯罪計劃。

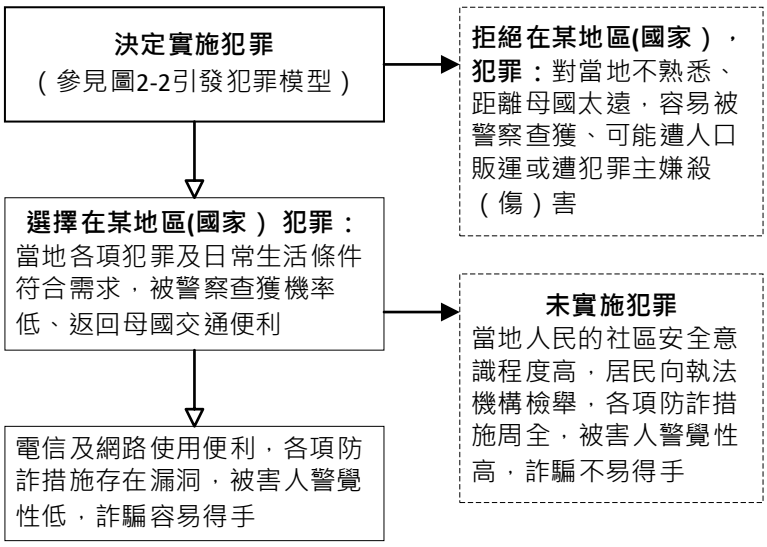


圖 2-1 電信網路假投資詐欺犯罪活動模型

資料來源：修正自 Clarke, R. V. & Cornish, D.B. (1985) Modeling Offenders' Decisions: A Framework for Research and Policy', in M. Tonry and N. Morris (eds) Crime and Justice: An Annual Review of Research, Vol. 6. （p.169)Chicago, IL: University of Chicago Press, pp. 147-185.

2.引發（Initiation）

圖 2-2 說明犯罪者的背景因素是影響最初決定參與電信網路假投資詐欺犯罪的重要原因。(1)背景因素：個體的生活背景會影響其社會價價值觀、生活態度和人格心理特質發展，從理性選擇角度觀之，這些背景因素在個體實施犯罪決策時，將產生具有關鍵性影響的判斷與認知。(2)經驗與學習：個體第一次實施電信網路假投資詐欺犯罪，深受個體犯罪經驗及技巧的學習能力，規避執法機關查緝的能力，以及對道德良心的感知能力影響。(3)當前生活狀況：個體的朋友圈、就業狀況、居住條件、婚姻狀況、生活方式等，都有助於塑造或改變個體犯罪的需求與動機。(4)需求與動機：能滿足個體這些需求的當前犯罪機會以及可能觸發或增加這些需求的犯罪誘因。(5)機會與誘因：個體依據累積的經驗和知識，識別評估採行合法或非法的行動方案。(6)對犯罪情境因素的評估：將這些需求轉化為參與電信網路假投資詐欺的犯罪情境，並評估犯罪是否比不犯罪有利。(7)準備完成：最後個體如認為參與電信網路假投資詐欺犯罪比不參與有利，即可能著手作犯罪前的準備。在本階段，背景因素對引發犯罪者是否選擇犯罪的影響最大，因為它同時決定了個體累積的知識、能力和經驗，以及目前的生活環境。

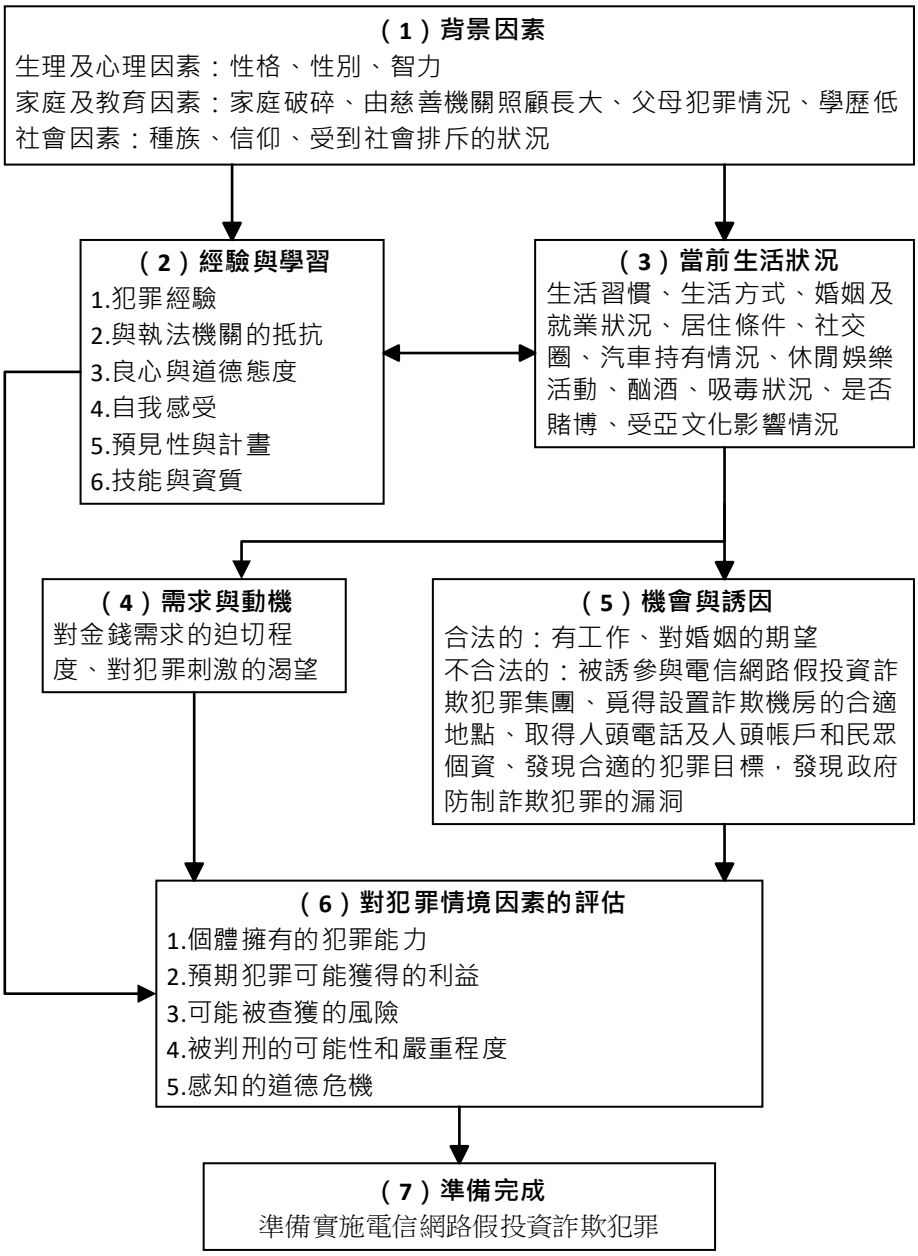


圖 2-2 參與電信網路假投資詐欺的開始階段

資料來源：修正自 Clarke, R. V. & Cornish, D.B. (1985) Modeling Offenders' Decisions: A Framework for Research and Policy', in M. Tonry and N. Morris (eds) Crime and Justice: An Annual Review of Research, Vol. 6. （p.168)Chicago, IL: University of Chicago Press, pp. 147-185.

3.習慣化（Habituation）

在電信網路假投資詐欺犯罪習慣化過程中（圖 2-3），背景因素在犯罪者實施犯罪決策過程的影響力減弱。取而代之的是，犯罪者因參與電信網路假投資詐欺犯罪所得到的不法利益和犯罪者生活環境的的變化，例如：結識共同參與電信網路假投資詐欺犯罪的新朋友、犯罪技能的提高，以及生活方式和相關價值觀的改變。

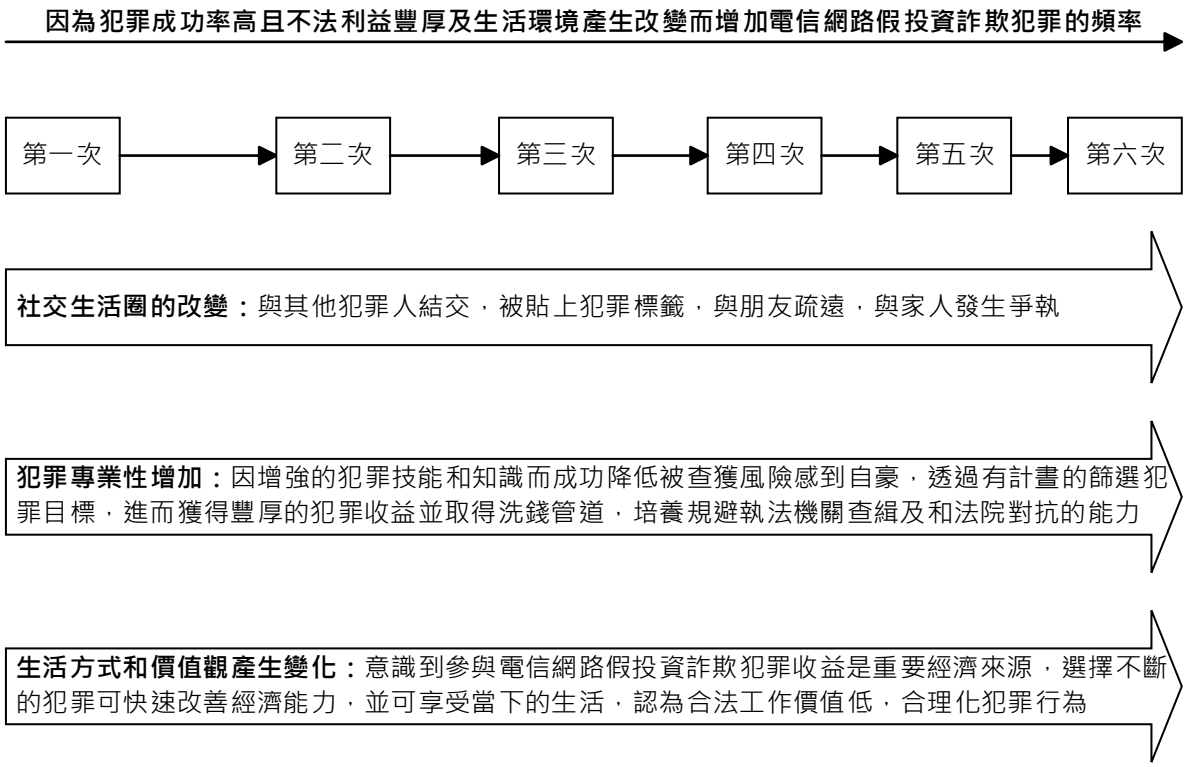


圖 2-3 習慣參與電信網路假投資詐欺的階段

資料來源：修正自 Clarke, R. V. & Cornish, D.B. (1985) Modeling Offenders' Decisions: A Framework for Research and Policy', in M. Tonry and N. Morris (eds) Crime and Justice: An Annual Review of Research, Vol. 6. （p.171)Chicago, IL: University of Chicago Press, pp. 147-185.

4.終止（Desistance）

在電信網路假投資詐欺犯罪終止階段（圖 2-4），背景因素在犯罪決策中不再扮演任何重要角色。相反的，因為犯罪者感知到遭執法機關查獲的風險日益增加，政府機關各項防詐政策措施日趨嚴密，民眾防詐意識日漸提高，使犯罪者感覺需冒更大風險及耗費更多犯罪功夫，才能達到預設的犯罪目標，使犯罪者在理性衡量犯罪成本與犯罪利益後，覺得不參與電信網路假投資詐欺犯罪比參與犯罪有利，而不敢再冒然繼續犯罪，犯罪者也可能因生活環境產生變化，例如：婚姻和家庭責任的增加，身體發生傷病，獲得合法工作，犯罪遭查獲等等生活狀況的改變，最終停止電信網路假投資詐欺犯罪而選擇合法的工作或從事其他的犯罪。

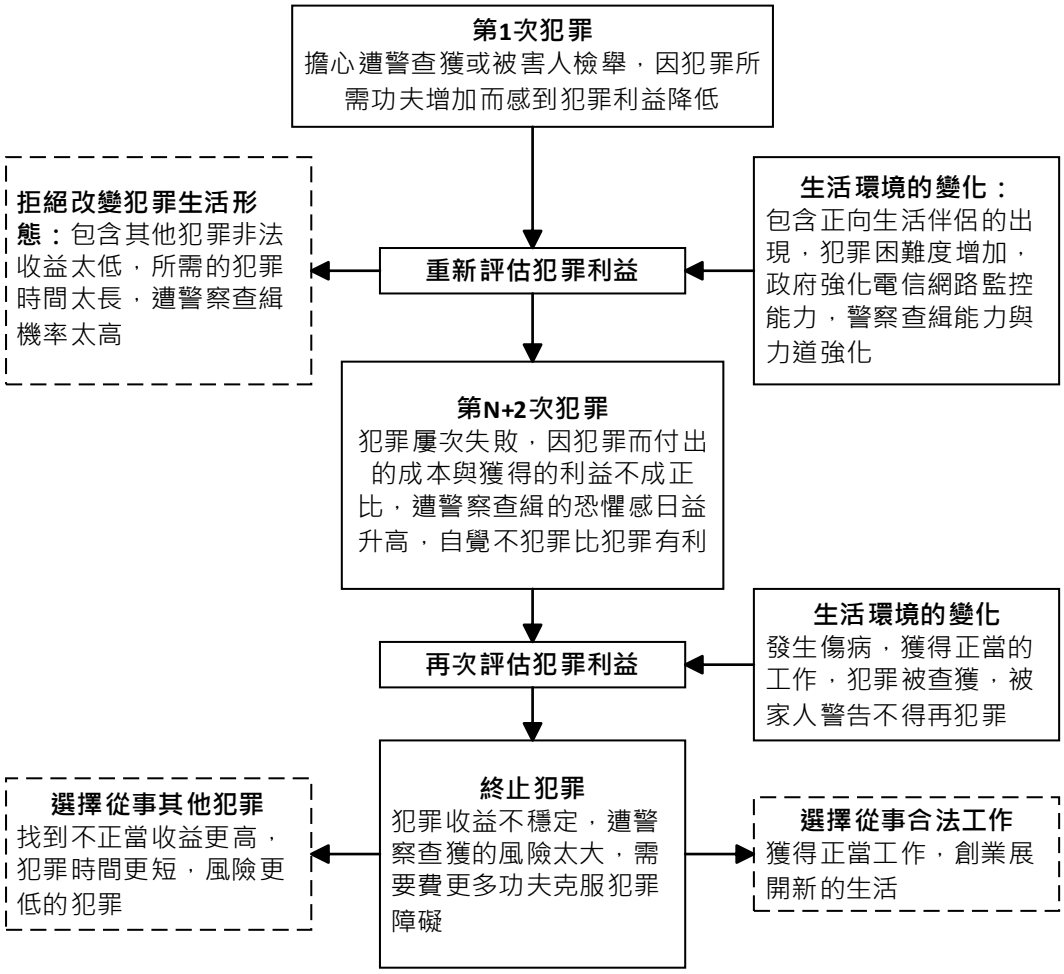


圖 2-4 終止參與電信網路假投資詐欺的階段

資料來源：修正自 Clarke, R. V. & Cornish, D.B. (1985) Modeling Offenders' Decisions: A Framework for Research and Policy',In M. Tonry and N. Morris (eds) Crime and Justice: An Annual Review of Research, Vol. 6 (pp. 147-185). Chicago, IL: University of Chicago Press, p.172.

三、日常活動理論(The routine activity approach)

(一)理論介紹

1979 年美國犯罪學家 Cohen 和 Felson 參考 Hawley 提出的人類生態學理論（Hawley, 1950)，提出日常活動理論(The routine activity theroy) (Cohen & Felson, 1979)，用於解釋美國在二戰之後 1947 年至 1974 年美國犯罪率高成長原因。Cohen 和 Felson 認為美國借助科技的發展，研發製造大量新穎的家庭電器產品，取代了許多家務人力，改變傳統男性外出工作，女性在家操持家務的日常活動方式，令原本在家從事家務的婦女大量投入就業市場，造就雙薪家庭日趨普遍，白天無人在家看管成為常態，導致人民對住家的監控能力降低；再加上交通便利，使得有動機的犯罪者得以快速移動，造成掠奪性犯罪（predatory crimes）諸如：搶劫（奪）、擄人勒贖及入室竊盜等犯罪機會相對提高，也因為美國人民勞動參與率和家庭收入增加，導致潛在被害人及標的物數量大增。

由上述可知，Cohen 和 Felson 創建日常活動理論初期係從美國整體社會「宏觀」的角度分析犯罪的發生。之後才以「微觀」的角度關注分析被害人及犯罪者之間的互動模式，認為每個犯罪事件都需要有動機的犯罪者(motivated offender)在場、合適標的物(suitable target)的存在、有能力之監控者(capable guardian)不在場等(如圖 2-5)三要素聚合（Cohen & Felson,1979）。

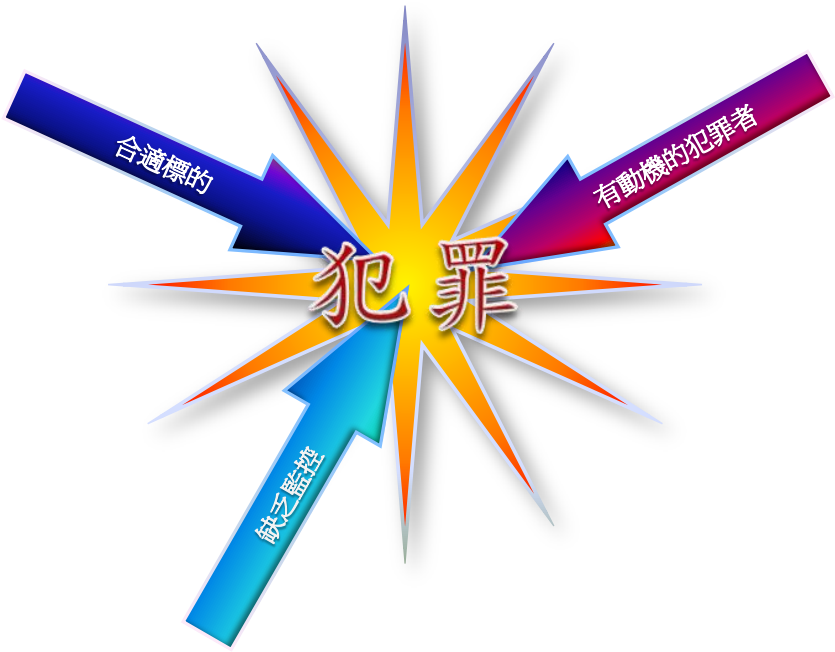


圖 2-5 日常活動理論概念圖

資料來源：黃翠紋、孟維德（2017）。警察與犯罪預防。五南圖書出版公司，頁 66。

1998 年 Felson 和 Clarke 以「VIVA」簡稱合適標的物(suitable target)，分別是有價值的(value)、可移動的(inertia)、易見的(visibility)及易於接近的(accessibility)(Felson & Clarke, 1998)。

2003 年 Felson 指出當前的日常活動理論已比理論創建初期更加注重對於犯罪人的解釋。犯罪者經常聚在一起共謀犯罪，因此共謀犯罪成為日常活動理論的一個主題。犯罪者聚集地（「閒晃」）是犯罪者們相互結識與聚集的地方，他們不僅在那裡犯罪，而且在相近的時間和地點犯罪（Felson, 2003）。

2004 年 Clarke 和 Felson 指出，有犯罪動機的人是指「任何犯罪發生之啟動者」；合適的目標是指「任何可能合適被害的人或標的物」；有能力的監控者是指「泛指足以遏止犯罪發生之人，且大多數並非指執法或保全人員，而是鄰居、朋友、路人，甚至是物品的主人」(Clarke & Felson, 2004)。

2006 年，Felson 在他的著作《Crime and nature》為日常活動理論再添加三項元素，分別是對犯罪動機者有約束力的操縱者、負責保護合適目標的監護者及負責看管物業場地的地點管理者，以上六項因素成為了犯罪者的推力及反推力(Felson, 2006)。

最初 Cohen 和 Felson 在創建日常活動理論時係聚焦於「直接接觸掠奪性」犯罪，認為犯罪之發生在時空上須與日常生活各種活動提供的機會相結合，方能導致犯罪的發生，即犯罪者透過直接接觸方式傷害被害人或侵害他人財產。雖然這已是一個非常廣泛的應用，但電信詐欺犯罪卻是非接觸型的犯罪。更重要的是，原來的日常活動理論係從「宏觀」及「微觀」的面向分析犯罪，欠缺「中觀」的角度，且並無涉及犯罪過程、受害過程的分析。再者日常活動理論雖然指出了犯罪者決策的傾向，但並未明確指出犯罪決策過程。因此，日常活動理論必須再與犯罪地理學、環境犯罪學、情境預防和犯罪人選擇模型整合才能更全面的分析及預防犯罪的發生（Felson, 2016）。

因此，Felson 認為預防犯罪的關注重點應在於犯罪問題，而不是犯罪人；犯罪的發生與人們的日常活動有密切關係，包括工作、學校和家庭生活；普通民眾在預防犯罪的功用明顯比警察和保全更重要；犯罪標的重量愈輕，價值與可見性愈高，及與犯罪人接觸的機會愈高，其受害的風險就愈高。因此，日常活動理論關注重點在於實施犯罪行為時物理性的社會環境，而不是犯罪者的特徵。所以，必須以科學方法分析犯罪，並從犯罪者的角度來思考犯罪（Felson, 2016）。

本研究歸納日常活動理論的發展，分別從「宏觀」（日常生活理論-社會結構）、「中觀」（犯罪型態理論-社區環境）及「微觀」（理性選擇理論-個體決意）等三個角度分析每個犯罪事件發生不可或缺的三要素如下：

1.需有動機之犯罪者(motivated offender)在場

指任何因社會急速之變遷，人類活動形態改變，造成犯罪機會及潛在犯罪者增加，且為犯罪被害發生之啟動者在場。

2.需合適標的物(suitable target)的存在

指任何可能合適被害的人或是有價值的(value)、可移動的(inertia)、易見的(visibility)及易於接近的(accessibility)的標的物的存在。

3.需有能力之監控者(capable guardian)不在場

泛指足以遏止犯罪發生之人，且大多數並非指執法或保全人員，而是鄰居、朋友、路人，甚至是物品的主人不在場等。

（二）理論應用

本研究將電信網路詐欺犯罪融入日常生活理論解釋則有以下發現（黃翠紋、蘇信雄，2020)：

1.合適標的物(suitable target)的存在：犯罪者事先透過駭客入侵盜用個資等不法管道蒐集準確的民眾個人真實隱私資訊，再據以為被害人「客製化」詐欺劇本實施詐欺。

2.有能力之監控者(capable guardian)不在場：犯罪者利用各國法制、司法管轄主張不一，及偵查技術及相關設備的落差，將犯罪行為分解至數個國家，再運用遠端遙控的資通訊技術，指揮犯罪組織成員騙取民眾財物，製造警察查緝斷點，造成調查取證與案件聯結困難。

3.有動機之犯罪者(motivated offender)在場：分散躲藏於數個國家的犯罪集團成員，利用新興科技工具，不斷換新犯罪手法，隱藏犯罪地點，在高報酬、低風險、低刑度的誘惑下以操作 ATM 解除分期付款、網拍詐欺、假冒公務機關、混合型結合臨櫃提款詐欺及 MSN、LINE 等犯罪手法詐欺民眾，增加警方偵辦之困難。

四、犯罪腳本(Crime scripts)

(一)理論介紹

腳本（Script）的概念起源於 Schemae「基模」，認知心理學家認為很多知識是以基模的形式儲存在人的記憶系統裏的 (Anderson, 1983; Rumelhart, 1980)。人類大腦中存在著不同形式的基模(Augoustinos, Walker & Donaghue, 2006)，它是一種認知結構，係人類基於過去的各種經驗、意識、概念等而產生對外在世界的假設和期望，人類生命歷程中會形成大量的基模，其作用是幫助人類駕馭他們的社交世界。我們每個人都會累積自己或吸收他人為實現預期目標而應遵循行動順序的經驗並作為與他人互動的指導。因此，每個人都會有不同形式的基模（例如，自我基模、他人基模、關係基模、事件基模）（Augoustinos et al., 2006; Baldwin, 1992; Fiske & Taylor, 1991）。例如，自我基模是指自己對己身的認知結構，它與本身的特質和過去的行為有關，從而為自己提供認同感。他人基模是指根據自己親自認識或透過他人聲譽瞭解的其他人的人格原型。這種結構幫助人們根據他人的主導性格特徵進行分類，然後根據自己的性格與他們互動。關係基模（稱為人際腳本）是幫助自己與他人建立相互關係的認知結構（Baldwin,1992；1995）。 事件基模（通常稱為腳本）則指是人們在特定情境中採取一系列理性的、有目的、以目標為導向的操作序列行為，尤其是在對特定領域中特定行動的具體解釋的強調(Hewstone, 1989) 特別適合在理性選擇和犯罪控制的聯合方法中發現特定的犯罪方向（Cornish, 1994a)。Schank 和 Abelson（1977）認為我們對行為程序的瞭解具有特定的性質和形式，類似於戲劇劇本，例如：「餐廳腳本」；它建構了餐廳顧客必須採取的一系列行動的知識。首先，顧客必須進入餐廳→等待入座→取得菜單→點菜→用餐→拿到帳單→支付餐費→走出餐廳。因此，腳本可以視為一組行動軌跡、變數、關係、操作、循環等，腳本常隨著時間的推移而延長事件序列，而這些關係具有明顯的因果關係，即前期事件發生的結果會促成後期事件的發生和改變，腳本可以區分為小的行為單位場景，或者實現主要目標所需的計畫。事實上，「場景」在日常用語中同時代表情節、地點、背景、行動計畫等等。腳本與其相關的角色需要道具和協助者在指定地點推動行動進行，直到發生新事件或障礙，阻止腳本的繼續執行，腳本的主要作用在使該行動過程自動化，我們不必考慮在某種情況下採取何種行動以實現目標（Leclerc, 2016）。

1994 年英國犯罪學家 Derek Cornish 套用認知心理學中「腳本」的概念並從理性選擇的假設觀點出發來解釋犯罪過程。Cornish 最初借用腳本概念是為建構一個有系統地調查和識別特定犯罪實施過程所有步驟的框架，以及每個步驟必須採取的決策和行動以及成功完成犯罪所需的資源。此範本與預防犯罪具有高度相關，因為除了與實際犯罪步驟相關的干預點之外，它還為犯罪學家提供犯罪干預點的機會(Cornish,1994a;b)。因此，使用腳本概念分析犯罪，將使犯罪過程更容易識別和理解。

由上可知，犯罪腳本運用理性選擇觀點的假設，建構犯罪者在實施特定類型犯罪前、中、後所做的選擇和決策模式。換言之，犯罪腳本是一個觀察犯罪全部過程的分析工具，它將分析擴展到犯罪行為順序的所有階段，詳細並全面的描述犯罪者實施特定犯罪行為全部過程及犯罪目的的理性決策（儘管理性是有限的）分析，以幫助強化情境犯罪預防政策，而近年來犯罪腳本在有組織犯罪方面的分析也有非常好的發展。

有組織犯罪不僅涉及大量犯罪者，亦可能牽涉多個犯罪組織或犯罪網絡，其犯罪活動往往跨越國界，遍及多個國家（Moreto & Clarke, 2013）。現在已經有許多學者透過犯罪腳本分析的技術，研究有組織犯罪並作出貢獻。例如：Morselli 和 Roy(2008) 融合犯罪腳本和社交網路分析兩次被盜車輛輸出的犯罪組織，這項研究結果顯示，去除犯罪網路中的某個特定參與者（例如經紀人）可能會導致整個犯罪網路的破壞。Savona (2010)研究歐洲和義大利犯罪組織的趨勢，並透過義大利三起有組織犯罪所涉及的公共建築產業貪腐案件進行犯罪腳本分析並據以研提創新的預防措施。Tompson 和 Chainey（2011）透過使用兩種犯罪腳本作為分析非法廢棄物處理過程的工具，對已發生的非法活動進行具體且針對性的分析，以作為調查、發現和預防該類犯罪活動的方法。Chiu,Leclerc 和 Townsley（2011）透過 25 份法庭筆錄進行分析，確定了製造毒品過程中所涉及的七個階段犯罪腳本，並運用問題分析三角的方法確定犯罪腳本干預點，最後提出對犯罪地點、化學品和設備的關注，可能對整個製造毒品腳本產生阻斷的預防效果。Savona、Giommoni 和 Mancuso（2013）透過兩份以性剝削為目的的人口販運逮捕令分析，瞭解人口販運犯罪集團和受害者之間互動的決定性資訊及犯罪各階段的犯罪腳本，以洞悉犯罪過程的弱點，並在此基礎上提出針對性的情境預防技術。

Gilmour（2014）運用犯罪腳本分析方法，針對以現金密集型交易洗錢及購買高價值可攜式商品等兩種洗錢模式進行研究，藉以重構犯罪者於洗錢過程中所採取的行動流程。研究結果顯示，犯罪者係透過一連串有限且具理性特質的決策步驟完成洗錢行為，並揭示多項過往在洗錢防制中較易被忽略的犯罪機會結構。該研究說明，犯罪腳本分析有助於辨識洗錢行為中的關鍵節點，並為後續犯罪預防策略之設計提供重要依據。

Hardy、Bell 與 Allan（2020）將犯罪腳本分析方法應用於麥道夫投資詐欺案（the Madoff investment fraud），藉以將高度複雜之詐欺犯罪程序加以概念化。該研究辨識出詐欺犯罪運作的 12 個關鍵步驟，並依其時序與功能區分為三個主要階段。研究結果進一步指出，透過強化目標管理與擴大監護範圍等犯罪預防技術，可有效降低詐欺犯罪發生之機會；同時，加強正式監控機制及協助自然監控之策略，則有助於限制行為人實施類似犯罪所需之能力。

Van Nguyen（2022）結合越南跨國電腦詐欺犯罪之官方數據與調查人員深度訪談資料，並運用犯罪腳本分析方法，發現資通訊科技得以協助犯罪集團在跨國詐欺被害人時，無需與被害者進行直接互動。研究進一步闡明，在金融卡詐欺與電話詐欺等兩類跨國電腦詐欺犯罪中，越南籍犯罪者與外國犯罪者分別扮演不同且相互分工的角色。該研究有助於深化對跨國電腦詐欺犯罪運作模式的理解，並對亞洲地區電腦詐欺犯罪之研究提供重要實證貢獻。

Morgenthaler 和 Leclerc（2023）以澳洲法院針對暗網市場毒品交易之 18 份判決筆錄為研究資料，進行系統性的內容分析，據以建構澳洲毒品走私犯罪中行為人所採取之犯罪腳本。研究辨識出犯罪行為包含準備、存取、購買、接收與儲存等五個關鍵步驟，並進一步依毒品流向與使用目的，區分為暗網銷售、線下銷售與個人使用等三種類型之犯罪腳本。研究結果同時確認各類犯罪腳本中潛在之犯罪預防介入點，顯示犯罪腳本分析有助於辨識暗網毒品犯罪之關鍵節點，並作為設計具體犯罪預防策略之基礎。

犯罪腳本分析的優點在於它能與所有參與犯罪行為的人觀點相容（Leclerc & Reynald,2015）。近年來學者們開始以不同角度使用犯罪腳本（Leclerc,2013a；b），研究者可以從被害人或監控人的角度來思考，而不是僅僅從犯罪者的角度來思考犯罪腳本，這個發展提供了被害人與監控者的角度，使得我們可以從這三個角度來瞭解犯罪事件並透過情境預防來確定目標，從而有效提高預防犯罪的效果。表 2-2 即展現三種犯罪腳本的應用方式。首先是，犯罪者的腳本，其重點在於讓研究者識別犯罪實施過程的每個階段，以便取得全面的干預點，其最終的目標是在犯罪者完成犯罪之前破壞犯罪行為的成功遂行。其次是，潛在受害者的腳本，此腳本係從潛在受害者的角度進行分析，藉以瞭解為避免受害而需採取的自衛手段。其最終目標是促進預防被害腳本的執行，以避免潛在的受害者受害。最後是，潛在監控人的腳本，其分析的重點是在識別犯罪過程中，潛在監控人可能成功干預犯罪完成的所有階段。其最終的預防目標是鼓勵和促進潛在監控人腳本的完成，以成功預防犯罪(Leclerc,2016)。

表 2-2 犯罪腳本的分析與應用

腳本名稱	犯罪者的腳本	潛在受害者的腳本	潛在監控人的腳本
犯罪活動中對應角色所追求的目標	成功實施犯罪	避免被害	干預犯罪進行
腳本分析的目標	識別犯罪實施過程的每個階段	避免受害而需採取的自衛手段	識別干預犯罪完成的所有階段
預防目標	阻斷犯罪腳本成功實現	促進預防被害腳本的實施	促進監控人干預犯罪腳本的實施

資料來源：Leclerc, B. (2013a). New developments in script analysis for situational crime preven- tion: Moving beyond offender scripts. In B. Leclerc and R. Wortley (Eds.) *Cognition and crime: Offender decision-making and script analyses* (pp.221-236). Crime Science Series, London: Routledge, p.225.

如果我們冀望採取犯罪腳本理論來設計有效的預防犯罪措施，首先必須建構經驗腳本，而經驗腳本的資料來源有犯罪嫌疑人的偵訊筆錄、被害人的被害調查筆錄、監控人自陳報告或上述三類人員的深度訪談及執法機關的偵查報告、檢察機關的起訴書、法院的判決書等。犯罪嫌疑人的偵訊筆錄或深度訪談是開發犯罪者腳本的首選資料來源，因為犯罪嫌疑人是研究者主要的分析對象。而且也只有犯罪者才能帶領研究者瞭解整個犯罪過程，被害人或許也能夠提供有關他們與犯罪者互動的過程，但無法提供有關準備或開始犯罪

等的訊息。當然，如果吾人腳本主要分析對象為被害人或監控人，其開發經驗腳本的資料來源，則以被害人的被害調查筆錄或監控人的自陳報告或渠等的深度訪談資料為佳。而執法機關的偵查報告及檢察機關的起訴書，可能因警察或檢察機關的資料主要側重於犯罪行為的法律構成要件，而漏失促成犯罪完成的關鍵節點資訊。法院判決書則是取得開發犯罪腳本來源資料最簡易的管道，因為法院判決書的資料可在網路上公開取得，在臺灣只需透過網際網路進入「司法院法學資料檢索系統」之「刑事判決書」子系統查詢，此管道除節省研究者大量的時間外，並可在短時間內蒐集大量建構犯罪腳本所需的資訊。綜上可知，取得欲開發腳本對象的筆錄、報告或對其深度訪談是獲取腳本資料最佳的途經，而執法機關的偵查報告及檢察機關的起訴書，則有漏失促成犯罪完成的關鍵節點資訊的風險，另外法院判決書則是取得開發犯罪腳本來源資料最便利的方法（Leclerc,2016）。

現今的犯罪腳本已經可用來識別過去無法透過情境犯罪預防性犯罪的手段來預防的非理性犯罪，另外犯罪腳本研究對「有組織」犯罪的理解也正在出現，這不僅有助於打擊犯罪，還有助於瓦解對這些犯罪負責的犯罪組織的活動。此外，出於情境預防目的編寫腳本現在也更常見。這項工作與 Cornish 的最終目標是一致的，即增加情景犯罪預防措施的使用以減少犯罪。最後，犯罪腳本分析的理論工作越來越受歡迎（例如：Borrion,2013；Ekblom & Gill,2016；Leclerc,2013a；b,Leclerc & Reynald,2015）。這項新的工作有一個最終目標——鼓勵和促進使用腳本分析來理解和預防犯罪。因此以犯罪腳本分析犯罪對於預防犯罪來說非常有希望（Leclerc, 2016）。

（二）理論應用

`電信網路假投資詐欺犯罪集團在獲取不法利益極大化、被捕風險最小化的理性選擇下，會反復運用最容易得手且最安全的犯罪模式實施詐欺犯罪，因此，本研究將以理性選擇的角度，運用犯罪腳本分析技術，建構電信網路假投資詐欺犯罪前、中、後所做的選擇和決策模式，並擴展到犯罪行為順序的所有階段，詳細且全面的描述犯罪者實施特定犯罪行為全部過程，以提供政府機關擬定防治及預防犯罪宣導運用，及協助執法人員全盤了解是類犯罪，掌握偵查犯罪先機、提高偵查效能，同時作為教育訓練的教材，以供新進人員或在職人員了解最新的犯罪情勢。本研究搜尋 2024 年 1 月 1 日至 9 月 24 日警政署刑事警察破獲之假投資案件新聞資料個案計 35 件，分別就新聞發布日期、查獲時間、查獲地點、查獲嫌犯、案情摘要、查獲贓證物等整理歸納分析(如附錄一)，將電信網路假投資詐欺犯罪腳本區分為犯罪前行為與準備、主要犯罪行為、犯罪後行為。

1.犯罪前行為與準備

犯罪集團（有一大部分是黑道幫派）為順利達成詐取民眾錢財目的，在實施犯罪前可能必須全部完成或部分完成以下準備工作：

(1) 糾集或召募詐欺機房電話手、提領贓款車手，不肖執法人員、銀行從業人員、律師、代書及製作假投資廣告、開發假投資 APP、提供資通訊系統架設服務等資通訊技術等廠商（人員）加入犯罪集團。

(2) 經由非法管道取得大量民眾個資、電信人頭卡，並備妥金融人頭帳戶、虛擬通貨、地下匯兌等多元洗錢管道以隱匿贓款。

2.主要犯罪行為

在實施犯罪過程中，犯罪集團可能運用以下的犯罪工具、手法，藉以引誘、取信、迷惑被害人，以騙得鉅額錢財（如圖 2-6）：

(1)利用資通訊工具投放虛假投資訊息以吸引民眾注意

犯罪集團透過行動電話、社群網站、通訊軟體、交友平臺或網路廣告等以無差別漫天撒網方式，散播高額獲利訊息，吸引民眾加入特定理財群組，或利用民眾在使用網路社群媒體，例如：臉書、IG、YOUTUBE 等觀看新聞或影片時，強制彈跳出「高獲利投資理財」等廣告，吸引民眾一時好奇點選觀看，即會因演算法的機制而提高接觸「假投資廣告、網頁」的機會。又或以美女或俊男身分利用網際網路在臉書、IG 等社群網站結識被害人。

(2) 通過通訊軟體群組，與潛在被害人建立信任

民眾在瀏覽上述廣告、網頁的過程中可能會因為信任投資老師而點選頁面的連結，而進入詐欺集團事先設置的 LINE 或 WeChat 等犯罪集團事先創建的虛假理財群組。又或誤信詐欺集團成員利用虛偽頭像（人頭照片）假扮的美女或俊男，進而以 Line 或 WeChat 等通訊軟體與歹徒互加為好友，接續歹徒對被害人發動柔情攻勢，每天噓寒問暖以取得被害人信任後，再以高報酬之誘因誘騙被害人投資境外之理財平台。

(3) 營造高獲利假象，對被害人洗腦

在被害人加入虛假理財群組或理財平台後，犯罪集團再利用預先佈置謊稱助理、老師的成員帶領操盤，並逐日貼出偽冒對帳單；另外，犯罪集團的暗樁「水軍」則在群組內不停的聲稱已經有高額的獲利，藉以吸引民眾加入假投資平臺或博奕網站。

(4)提供小額獲利，以獲得被害人信任

待被害人初步配合詐欺集團指示匯款到不同私人帳戶，即會有小額獲利匯款至被害人帳戶，營造出專業投資人的形象，以增加其信任感，並鼓吹被害人加碼投資。

(5)當被害人相信騙局之後，詐欺集團就會誘使民眾大量匯款至犯罪集團提供的人員帳戶，或要求被害人備妥鉅額現金或介紹被害人向假冒商家購買巨額虛擬通貨，犯罪集團再派出「理財專員」到府出示身分、面交收款鉅額現金或虛擬通貨。

(6)詐欺完成，犯罪集團成員全數失聯`

待民眾投入鉅額錢財，欲出金實現獲利時，客服人員即以各種理由拖延、未回訊息、謊稱駭客入侵，甚至關閉網站，致使被害人求償無門後，始知遭到詐欺。

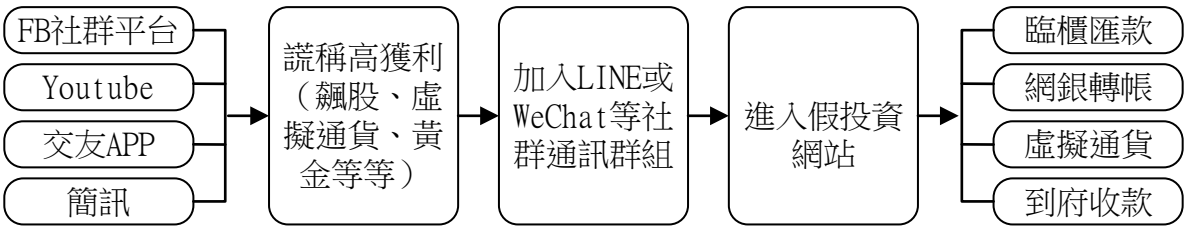


圖 2-6 電信網路假投資詐欺犯罪流程

資料來源：本研究自繪。

3.犯罪行為後

詐欺集團收取贓款後，利用金融科技(如人頭帳戶、虛擬通貨)便利性迅速轉帳，或利用地下匯兌等多元洗錢管道製造斷點以隱匿贓款，以規避執法人員的追查。

五、問題導向警政(Problem-oriented policing)

(一)理論介紹

1.基礎概念

美國犯罪學者 Herman Goldstein 於 1977 年以《Policing a Free Society》(Goldstein,1977)一書為問題導向警政的概念奠定了基礎；隨後於 1979 年在一篇名為'Improving Policing: A Problem-oriented Approach',(Goldstein,1979)的文章中詳細闡述其理念；然後在 1990 年以《Problem-oriented Policing》(Goldstein, 1990)一書中進行了擴展；最後在 2001 年於美國加州聖地牙哥舉辦的國際會議中以'Problem-oriented Policing in a Nutshell',(Goldstein, 2001)為題的演講中作歸納，本研究參考 Klingele、Scott、Dickey(2010)和 Goldstein (2016)，對 Goldstein 在這場演講摘要，並參考其他學者之論述，整理成以下概念，以作為本研究對問題導向警政理論的詮釋基礎。

(1)植根於公共管理和警察組織行為領域的理論

問題導向警政模式並不是一種特定的警務策略或犯罪控制策略，它是植根於公共管理和警察組織行為領域的理論，其目的是建構執行警察工作以及管理警察機構的思想體系、架構和原則。因此，問題導向警政對各種犯罪理論以及警察策略和戰術持開放態度，只要它們的運用方式符合其核心原則。

(2)必須建構各類獨立運作的內部業務單位

警察組織必須因應民眾所關切的各種公眾安全問題，據以建構各類獨立運作的內部業務單位，這些單位首先必須應依據業務屬性建構量化的績效考核制度；其次，必須建構該單位的工作品質、數量和效果的衡量指標，第三，必須為該單位配置足夠的人力、設備及執行特定警察業務所需的一切資源。

(3)從微觀的角度分析犯罪問題

警察組織必須將具經驗豐富處理案件的第一線警察人員、受過適當訓練的犯罪分析人員、主管人員，以及外部相關領域的專家、一般民眾等各種資源結合起來，再依社會科學的原理和方法，從「微觀」的角度更詳細、更深入地對問題進行調查、探討、分析，以充分了解發生犯罪或影響治安事件問題之間關係及原因。因為，當前的犯罪問題分析是個獨特的專業領域，如果分析人員冀望為問題導向警政工作做出重大貢獻，則必須接受專門的訓練（Boba,2003；Maguire & Hopkins,2003；Clarke & Eck,2005；Hirschfield,2005；White,2008；Boba & Santos,2011；Eck & Clarke,2013）。

(4)有效且公平的策略

問題導向警政策略以結果為導向的，故而警察機關採取問題導向警政的意義在於，能比以前更有效的控制當前特定問題，因此問題導向警政是以實務為導向，尋求對問題的澈底了解，進而採取更有效的解決方案。情境犯罪預防與問題導向警政策略都高度重視解決問題的能力，例如：問題導向警政和情境犯罪預防都不太關心犯罪人的天生惡性，也不關心犯罪人的社會、心理問題。但對犯罪案件的發生，是不是因為被害標的未受有效的保護則有高度的興趣。除了有效性外，問題導向警政另一個關注重點是公平性問題，在民主社

會中，警察對民眾施加的各項作為都必須考慮公平性，盡量避免與社會各族群產生緊張關係，減少武力的使用，以及尊重公民自由和權利。事實上，警察權威合法性的來源，很大一部分取決於公民是否認定警察執法的程序和方法是否公平，而不僅僅取決於方法是否有效（Sunshine & Tyler, 2003）。問題導向警政要求警察採取的應對措施，應公平地分配給不同族群承擔並公平地共享應對措施的好處。問題導向警政也傾向於避開警察採用強制武力，以免損害公眾對警察公平性的看法。因此認真分析問題、有效協調和實施應對措施，可以使警察擺脫高壓、脅迫甚至有時濫用強制力的做法，提高警察的合法性，減少公眾對警察的敵意。

(5)要具有犯罪預防性功能

警察工作始終是補救與預防併行，補救是指危害發生後的解決、糾正或懲罰措施。預防是指在危害發生前避免或盡量減少危害發生的作為。犯罪偵查逮捕犯罪者並追究其責任，此為治安的補救面，大多數受害者服務也是補救性的，而不是預防性的，它們幫助受害者在身體、情感和經濟上康復。警察巡邏則是強調預防，其目的是阻止潛在犯罪者犯罪。很少有警察活動是明確地屬於補救性或預防性的；大多數是兩者的結合。例如，逮捕罪犯既可以發揮補救的目的，讓犯罪者對自己造成的傷害負責，也可以達到預防的目的，阻止這些犯罪人及其他人將來再犯同樣的罪行。問題導向警政策略要求警方比過去更加關注對問題的應對措施，以減少或降低未來犯罪事件發生的可能性及造成傷害的嚴重程度。例如：當公眾要求警方對最近發生的嚴重犯罪事件做出強烈反應時，警察則應在民氣可用的社會氛圍下營造輿論引導敦促民眾採取新的預防措施。另外，問題導向警政與同一時期發展的情境犯罪預防理論，共同為預防犯罪策略賦予新的意義，提供警察和民眾大量預防犯罪新方法。

(6)不依賴使用刑事司法系統

儘管司法系統擁有法律賦予的絕對權威，但在處理社會上許多治安問題仍存在很多的缺陷與不足，傳統的司法系統在處理惡性故意犯罪的功能是無庸置疑的，但警察處理的許多案件並不是典型的惡性故意犯罪，犯罪人有可能是患有精神疾病或吸毒或酗酒，在這種情況下司法系統很難證明犯罪者的行為故意及惡性，即使證實其故意及惡性，監禁也可能無效或可能使情況變得更糟。研究指出，犯罪人在監獄服刑期滿或假釋出獄後再犯率都很高，此一現象已引起諸多觀察家和政策制定者質疑監禁的有效性和財政、社會，以及司法系統（尤其是警察）所付出的成本（Stuntz ,2011；Ruth & Reitz, 2003；Kennedy, 2009）。此外，本質上警察日常工作大多是在維持社會秩序，處理違秩行為及排解民眾糾紛等瑣碎事務，並不需要司法系統介入處理。而司法系統不但欠缺維護治安的能力，其人力及資源配置也相當缺乏，所以司法系統的各個部門都被迫採取變通措施以為因應，而不是全然依照法定職權行事，例如警察不可能逮捕所有的罪犯，檢察官也不可能起訴所有被逮捕的犯罪者，有部分犯罪案件可能被轉移到其他系統處理，最終法院也只能對一小部分的案件進行審判並定罪，定罪後亦可能採取緩刑、罰金、假釋、電子監控、社區服務等非監禁刑罰，以幫助舒緩擁擠的監獄空間。但矛盾的是，現在的警察仍多採用刑事逮捕策略，以作為實現其維護社會治安的手段及政策目標。此策略不僅造成刑事司法系統資源過度使用和踐行正當法律程序的壓力，況且警察工作非常仰賴人民的支持，強調以逮捕為中心的警務策

略，有可能造成警民關係的緊張和疏離，同時削弱警察的合法性。因此，問題導向警政雖然不排除使用逮捕、起訴或監禁手段處理犯罪事件，但更鼓勵警察尋找代替刑事司法系統解決問題的方案。以盡量減少逮捕、起訴或監禁等強制手段的使用，而達到降低公共成本和增強公共安全的目的（Klingele et al,2010）。

(7)要有效運用第三方警政

警察維護治安的能力是有限的，而且在民主國家普遍都會限制警察權力，無論警察有多麼重要，在整個社會中只是一股相對較小的力量。因此，問題導向警政的另一個重要挑戰，即是要求警察尋求社會其他領域的民力協助；同時鼓勵公益機關、團體、組織等第三方部門共同參與解決治安問題，所謂警力有限、民力無窮。警察需向其他公共機構、社區和私營部門徵詢治安相關問題，以獲取分析犯罪問題所需的訊息並尋求他們的幫助。鼓勵警察與第三方部門及協勤民力接觸不是為了警察本身，也不是為了增加民眾對警察的支持，而是為了更有效、更公平地解決問題。對於某些問題，可能需要高度的外部人力參與，警察究竟應該與哪些公共機構、社區和私部門接觸、合作，取決於每個問題的具體情況。對警察來說，請求與其他部門或民力合作以控制治安問題是相對容易的，但如果被請求方並無興趣時就會面臨相當大的困難。所以警察需要開發和靈活運用採用爭取、說服、施壓和強制合作等技巧，以解決治安問題（Scott & Goldstein,2005）。

(8)要實施新的行動策略

問題導向警政係採用行動研究(Action Research)模式研究警政問題，其過程是對警政實務工作情境中實際產生的問題進行思考並進行系統性、持續性的循環研究，以有效改善實務問題。換言之，行動研究即是將新的想法實際運用於警察實務工作，以改善現狀，並增進實務知識與專業。因此，問題導向警政強調將新策略付諸行動，同時必須預見實施新行動計畫的障礙，並制定相關應變措施以克服障礙。新的行動計畫除了必須糾正過去的危害之外，還要能預防未來的危害，因此在制定新行動計畫時必須考慮財務成本、執行的人力、合法性、實用性、簡單性、有效性、內部及外部的支持，而且新的行動或工作計畫應當交給有擔當的人持續的執行下去。

(9)要建構評量新策略有效性的衡量指標

問題為導向警政最重要的是衡量警察在控制犯罪和治安問題的有效性。因此必須發展具體的衡量指標以評估警察工作的有效性。但是一直以來，警察機關缺乏嚴格評估其工作的能力，故而，警察機關需要發展新的內部評估能力並導入外部專業人員（能力）參與評估。這是一種新的自我反省及接受外界批評的模式，將有利於解決警察本身對問題見樹不見林的局限性，以及接受並適應新知識的途徑，但這個構思不管在警察機構內部還是外部，都有可能不容易實現。還需要進一步發展和試驗適合警察環境特定條件的評估方法。另外，對於警察工作有效性的評估標準嚴格性程度，學者們還存在相當多的爭論。有一些學者主張採用高度嚴格的標準，例如採用隨機對照實驗來提供標準（Sherman,2013），另一些學者則認為，發生治安問題的社會環境錯綜複雜，故傾向於採用廣泛且寬鬆的方法評估警務工作的有效性。實際上，對警察解決問題的方案措施有效性評估嚴格程度，取決於每個警察機構在該領域發展的經驗與歷史。對於那些從未有過評估工作成效經驗的警察

機構，應當鼓勵他們積極發現本身最基本、最原始的問題，並在此基礎上大膽的採取策進作為。我們可以合理地預期，如果警察機構長期採取以問題為導向的警務策略，那麼警察內部各部門就會更加認真且嚴肅的看待及解決問題，同時與內部或外部合作夥伴發展更專業的分析能力。在整個警察體系，對發展評估警察工作有效性的能力還有很長的路要走。總之，問題導向警政的推動代表警察工作必須往更專業、更科學、更制度化的方向前進，並不斷尋求更有效和公平的警察工作策略。一般來說，警察工作的有效性評估通常需要一些具體的指標組合，例如：避免或減少治安事故發生的數量、降低事故危害的程度、提高民眾對警察公平性的評價，或將問題轉移給比警察更適合處理的機關團體。對任何以特定問題為導向的精準警政措施評估，都將取決於每個問題的特質及其定義。

(10)成果要與其他警察機構交流分享

推動問題導向警政的關鍵在於警察與其研究夥伴就解決問題的經驗和知識進行交流，無論是在會議上進行面對面交流，或是以書面報告方式進行交流。傳達定量和定性資訊至關重要。另外，警察還有透過互相聊天傳承經驗傳統，警察們坐在一起經常會互相分享自已辦案過程中生死交關的工作故事，這些實戰經驗是警察最重要的資產，因此，警察機構必須將這些實戰故事以文字編撰成冊或製作成影音在警察機關內外廣為流傳，同時，警察機構也必須養成搜尋和閱讀其他機構故事的習慣，再將其經驗教訓應用於當地情況。我們不可能期望任何一個警察機構能夠研究所有治安問題，因此分享經驗和知識就顯得非常重要，一個機構的經驗教訓可以幫助其他機構解決類似問題，高品質的問題導向警政報告範例包括 Goldstein 和 Susmilch(1982a,1982b)、Eck 和 Spelman (1987)、Braga、Kennedy、Waring 與 Piehl（2001）、Clarke 和 Goldstein(2002、2003)，以及 Vestfold Police District (2004)等研究報告。

(11)建立專業化的警察知識體系

每一個專門職業的行業發展，都非常依賴該行業長期累積的專門知識或技術的經驗傳承，所以每個員工從入行開始就應該努力學習，並將所習得的知識與技術充分運用於實際工作中，同時還必須不斷精進專業知能，這種不斷累積的知識體系將有助於該行業提供更優質服務並解決問題。與許多其他職業和技術行業相比，警務領域的知識體系仍然相當薄弱，外人很難系統性的學習。所以應將內部高品質的警察學術、實務研究與經驗，以及外部與警察專業相關的研究展開廣泛的學習，並運用於警察實務工作。問題導向警政也呼籲警察機構應充實警察的知識體系使其系統化、標準化並提高嚴謹性，讓從事警察實務工作人員能更容易獲得這些知識、技術與經驗。為了實現這一目標，國際上已成立了問題導向警務研究中心（POP Center）（www.popcenter.org），以開發和傳播與問題導向警務和情境犯罪預防相關的訊息，使每一個從事警務工作的人員，都能夠很輕易的獲取解決警察實務工作問題的研究成果和實際執行的經驗。

2.SARA 模式解決問題的流程

美國維吉尼亞州(Virginia)紐波特紐斯警察局(Newport News Police Department)於 1987 年與 Eck 和 Spelman 兩位顧問，共同借鑑 1982 年美國威斯康辛州(Wisconsin）麥迪遜警察局(Madison Police Department)，有關採取問題導向警政策略處理酒醉駕駛和嚴重性侵犯的研究報告（Goldstein & Susmilch 1982a,1982b,1982c）、1984 英國倫敦警察廳

（Metropolitan Police）有關問題導向警政策略試點研究報告（Hoare et al.,1984）及 1986 年美國馬裡蘭州（Maryland）巴爾的摩縣警察局（Baltimore County Police Department）有關採取問題導向警政策略成立三個問題解決小組，成功解決該州三個警察指揮區的恐懼問題的研究報告（Cordner,1986）。所開發的 SARA 流程（Eck & Spelman,1987）。SARA 過程看似簡單的線性過程，但實際上它包含許多反饋循環（如圖 2-7）。警察機構根據掃描定義和發現治安問題，並提供分析人員進行問題分析，在分析階段可能會再發現新問題，此時就必須再回到掃瞄階段重新定義問題。在回應階段可能會發現影響治安問題的新事實，進而改變分析結論、重新定義問題或重新尋找更有效或更務實的回應。評估結果可能顯示回應措施有效或無效，如果回應措施無效，將促使警察機構再次回頭檢視 SARA 流程的每一個階段。事實上，解決問題的措施可以在任何階段進行。例如，在危機中，立即採取臨時回應措施可能會啟動 SARA 流程以控制問題，首先需要定義問題，接下來分析問題階段可能會建議進一步分析並制定可持續的因應措施或回過頭來重新定義問題，評估必須從處理問題開始即應啟動並持續進行，以追蹤問題的程度並確認每個新回應的有效性。

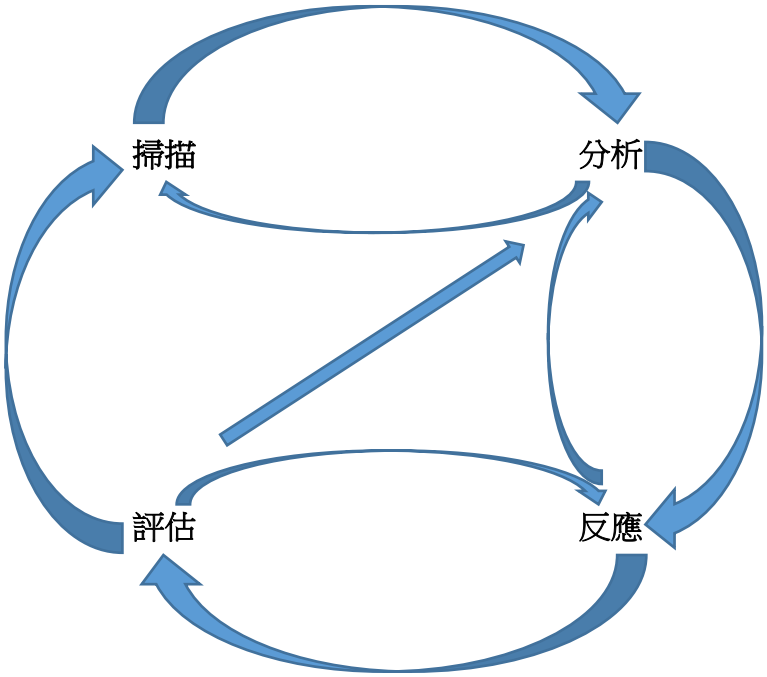


圖 2-7 SARA 流程模型

資料來源：Clarke, R., & Eck, J. (2016). *Crime analysis for problem solvers in 60 small steps.* Washington, DC: US Department of Justice, Office of Community Oriented Policing Services of Justice, p.13 .

3.治安問題的分析三角

由於問題導向警政理論並未詳細闡明如何分析問題和找到適當的回應措施等具體方法。所以需要運用問題分析三角（又稱犯罪三角）來補充問題導向警政理論（Scott, Eck, Knutsson & Goldstein, 2016）。問題分析三角來自環境犯罪學的日常生活動理論。該理論認為每個犯罪事件都需要有動機的犯罪者(motivated offender)在場、合適標的物(suitable target)的存在、有能力之監控者(capable guardian)不在場等)三要素聚合（Cohen & Felson, 1979）。換言之，有動機的犯罪者和合適標的物，在有能力的監控者不在場的時空環境下即可能發生犯罪。該理論認為人類的貪婪和自私天性，足以解釋大多數犯罪的動機，所以人類社會存在有動機的犯罪者是理所當然的，只要能滿足犯罪者的私慾，不論有生命的

（包括人類）個體或無生命物品，都可能成為犯罪標的。因此，警察機構應透過蒐集問題分析三角所有的資訊來進行犯罪分析，並據以設計至少控制三角形任何一邊的回應策略：即，防止犯罪標的和有動機的犯罪者在同一個無人看守的時空相遇。美國犯罪學者 Eck 認為此一犯罪分析模式亦共同適用於重複犯罪、重複被害和重複犯罪地點的分析。對於重複犯罪問題可以透過追究犯罪者來解決。對於重複被害問題可以透過幫助被害人來解決，對於重複犯罪地點可以透過關注該地點的物理環境和社會因素加以解決。因此，Eck 以問題分析三角為基礎，增加安保人、處置者、管理者形成雙三角形的結構(如圖 2-8)。此圖內三角形顯示了形成犯罪問題的必要條件，而外三角形則顯示有可能控制這些犯罪問題的人（Eck, 2003）。Clarke 和 Eck 指出，警察習慣從犯罪的角度來思考問題，其焦點通常是如何識別犯罪者及如何逮捕他們。而問題導向警政的目的則是在探索更廣泛的犯罪形成因素並加以防治。雙三角形的犯罪問題分析三角為三個形成犯罪問題的必要元素各添加了一個「控制器」：即，相對於被害者或犯罪標的而言，安保人（控制器）係指自己、家人、朋友或同事以及警察和私人保全。相對於犯罪者而言，處置者（控制器）係指非常了解犯罪者並且能夠對其行為施加某種控制的人，包括司法及矯正系統的警察、法官、檢察官、檢察署觀護人、父母、手足、師長、朋友和配偶。相對於犯罪區域時空而言，管理者（控制器）係指對網路虛擬空間或實體地點有管理權利（限）及義務的管理人（業者），如金融、數位、電信業者及營業場所的管理人等。（Clarke & Eck,2016)

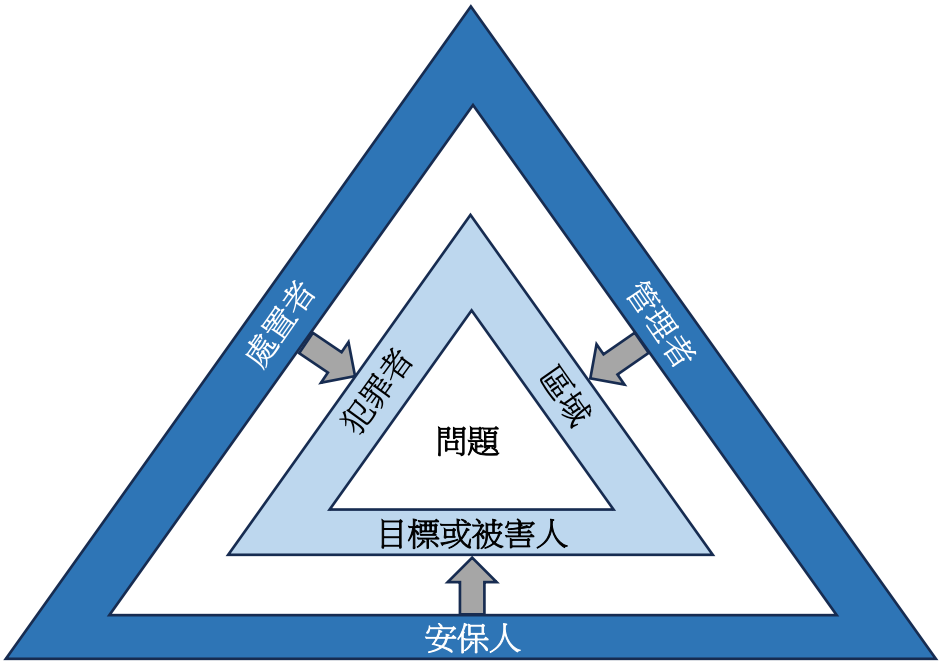


圖 2-8 治安問題分析三角

資料來源：Clarke, R., & Eck, J. (2016). *Crime analysis for problem solvers in 60 small steps.* Washington, DC: US Department of Justice, Office of Community Oriented Policing Services of Justice, p.15.

(二)理論應用

自從 1977 年 Goldstein 提出問題導向警政理論迄今已有 40 餘年，理論的最初目標是提出一種有效解決造成重複犯罪問題的警務改革，在往後數十年的發展過程中問題導向警政理論不斷的與環境犯罪學及警察工作進行研究成果與實務工作結合，期望能為警察組織打造一套量身訂作的專業知識體系，如今問題導向警政理論已蛻變為有效解決治安問題並提升警察工作效能，以滿足公眾對警察職能合理要求的綜合性警政策略，本研究將結合問題導向警政理論進展及實踐結果，運用 SARA 模式及犯罪問題分析三角以建構解決用於電信網路詐欺犯罪問題的掃瞄(Scan)、分析(Analyze)、回應(Respond)、評估(Evaluate)流程與模式。

1.掃描(Scan)確認問題的本質

問題導向警政策略的第一步驟是確認「問題」，所謂的問題係指社區（或社會）反覆出現危害公眾安全的事件，而且民眾期待警察能出面妥適處理這些事件。這個定義引出了「問題」需具備六個要素，即社區性（Community）；傷害性（Harm）；期望（Expectation）；事件（Events）；復發（Recurring）；相似性（Similarity）等（縮寫：CHEERS）（Clarke & Eck,2016)。依上述六要素定義，再透過相關犯罪數據、各式民調和新聞媒體報導觀之，電信網路詐欺是犯罪手法、工具相類似，且一再重複發生的犯罪事件，其犯罪結果造成民眾鉅額金錢損失，同時嚴重危害政府威信及國家形象，使臺灣背負詐欺王國的惡名，故此一犯罪「問題」，具備社區性（Community）及傷害性（Harm）、事件（Events）、復發（Recurring）、相似性（Similarity）等要素。再者，是類犯罪問題是民眾極為期待警察能妥善處理的犯罪問題亦符合期望（Expectation）要素。

2.分析(Analyze)問題發生的原因

此步驟是採用問題導向警政策略，防制電信網路詐欺犯罪的成敗關鍵，必須窮盡一切方法，全面分析引發問題的原因，本研究運用「犯罪腳本」分析技術，解構犯罪全部歷程，以幫助電信網路詐欺犯罪問題的資訊收集和分析，作為識別成功實施犯罪過程中的每一個重要關鍵，並提出有關問題原因和影響條件的假設，再以問題三角分析防制犯罪問題，蒐集有關解決類似問題的相關成功經驗，這些成功經驗的來源應包括國內外警察組織、社會科學研究以及與問題相關的其他機構和個人的研究或報告。藉以分析瞭解問題的根本原因並提出精準有效的解決方案，在分析完成後要再對先前的問題假設進行確認與驗證。

3.回應(Respond)問題處理的方案

在這個步驟，本研究依循「犯罪腳本」及「犯罪問題三角」的分析結果並結合當地民情及治安狀況，尋求各方資源與協助，廣泛蒐集各種可能解決問題的方案（孟維德，2011b），並從這些備選方案中，去除不利因素，選擇具有長久效益的方案（Clarke & Eck,2016)在此階段警察機關必須先確保已經徹底分析了問題並避免倉促採取行動而無法解決問題。警察應針對犯罪問題三角（受害者、犯罪者和地點）的發現，量身定制解決方案，且該回應措施方案必須與問題分析階段的結果相呼應。

其解決途徑有下列五種模式(Peak & Glensor,2008)：

(1) 徹底解決問題：使該問題衍生的事件不發生，但往往僅有少數問題有可能完全解決。

(2) 減少問題造成的事件數量：衡量解決方案有效性的主要方法。

(3) 降低危害的嚴重性：以事件危害的減輕來證明解決方案的有效性。
(4) 更好地處理問題：以提高解決事件效果及受害者滿意度和降低成本等措施來證明解決方案的有效性。
(5) 將問題交由更適合的單位處理：回頭檢視警察最初處理該問題的原因，並合理的將處理責任移交給更適合的部門或其他人來處理。

對問題的回應方式包含下列 11 個選項(Peak & Glensor,2008)：

(1) 將注意力集中在犯罪問題三角中，造成問題（犯罪者）、促成問題（控制者、管理者、監護人）或遭受問題（受害者）比例較高的個人上。
(2) 與其他政府部門或第三方合作處理。
(3) 使用調解和談判技巧。
(4) 準確傳達問題資訊並尋求民眾支持：A.幫助民眾減少焦慮和恐懼；B.促使民眾自行解決問題；C.促使民眾遵守法律規定；D 對潛在受害者提出警告並提出建議自保方法；E.讓民眾了解問題及政府能力的局限性以尋求支持。
(5) 動員社區民力以解決問題。
(6) 運用現有的社會控制力量，例如父母、老師、雇主或宗教團體的影響力以解決問題。
(7) 改變物理環境以減少問題重複發生的機會，即可藉助環境犯罪學所提供的 25 項情境犯罪預防技術運用到所有問題中。
(8) 透過現有法規或法令對導致問題的條件加強監控。
(9) 制定新的法令授以警察得在民眾行為被貼上犯罪標籤前，有限度的對行為人採取干預的權力(例如：命令離開和暫時的限制自由)，以作為正式執法措施(例如：傳喚及逮捕)的前置作為。
(10)比過去更精準的使用刑事司法系統，包括 A.直接調查、逮捕和起訴；B.有明確標準的選擇性執法；C.執行傳統上由另一機構執行的刑法；D.應透過地方法令受到刑事司法起訴或控制的行為的更具體定義；E.干預而不實施逮捕；F.為起訴目的而使用逮捕；G.緩刑或假釋附加的新條件。
(11)利用民事法令控制公共滋擾、攻擊性行為和助長犯罪的條件，包括 A.許可；B.分區相關的程序；C.適當合併；D.減少滋擾；E.禁制令救濟。

4.評估(Evaluate)問題改善的情形

Eck (2016)認為評估的主要目的在於幫助警察機構做出更好的決策，其方式係透過回答以下兩個問題來完成，首先，治安問題否有所改善？回答這個問題可以幫助警察機構決定，是否結束解決治安問題的工作，並將資源轉移到其他問題上。其次，如果治安問題確實改善了，其原因是否係回應措施促成？回答這個問題可以幫助警察機構決定，是否將相同的回應措施運用於類似問題。問題導向警政策略是否成功執行，必須運用科學的評估方法，以確認治安問題是否改善以及是否因警察的回應而促成。評估必須貫穿整個 SARA 問題解決過程，如圖 2-9 SARA 流程及評估所示。SARA 在每個階段都會提出一些待解決的問題，如果回應問題的解決策略不如預期成功，警察機構（或問題解決者）就必須回過頭來重新檢視。因此，在掃描階段，必須精準定義治安問題以便對其進行測量。在分析階段，必須收集有關治安問題性質和範圍的基礎資料。在回應階段，在制定改善治安問題的回應策略的同時，也必須制定問責機制，以確保回應中的各個參與者都依計畫行事。總之，

在遭遇問題的當下，即必須開始規劃評估。評估將提供調查結果，幫助警察機構確認是否應該重新審視問題以改善回應（如圖 2-9），評估的右側列出了進行評估時需要解決的關鍵問題。Eck (2016)指出評估類型可分為過程評估與影響評估，兩者是相輔相成的，過程評估關注：回應是否按計畫進行？所有的回應措施都有效嗎？或者，有無嚴格依據回應計畫行事？。但過程評估並無法評估回應措施成功與否，要確認治安問題改善情形及原因，則需要進行影響評估。影響評估關注：治安問題是否有所改善？及是否係回應措施促成？過程評估和影響評估分別回答及解釋不同的問題，因此，它們的綜合評估結果通常資訊都很豐富如表 2-3 過程評估與影響評估之區別，綜整兩項評估中收集到的資訊可以顯示回應措施是否促使治安問題改善。當回應按計畫（或接近計畫）實施時，結論就更容易解釋（A 欄和 B 欄）；當回應未按計畫實施時，即難以確認回應策略的有效性及下一步的策略（C 欄和 D 欄）；其中，D 欄將特別麻煩，因回應並未實施或實施方式與計畫內容完全不同，所以根本無從檢驗，C 欄的結果則值得進一步討論，治安問題的改善代表著警察機構可以結束解決問題的過程，並將資源轉移到其他問題上。但是，如果問題仍然嚴重或改善並不明顯，那麼警察機構將無法決定是否繼續或增加反應（假設回應措施正在發揮作用，但還需要更多時間或投入更多資源）。或者，可以尋求不同的回應策略（假設回應措施是無效的）。此外，也不知道回應策略是否對類似問題有用。簡而言之，當警察機構不知道回應策略為何成功時，就很難複製成功。因此，所有評估都應包含過程評估和影響評估。

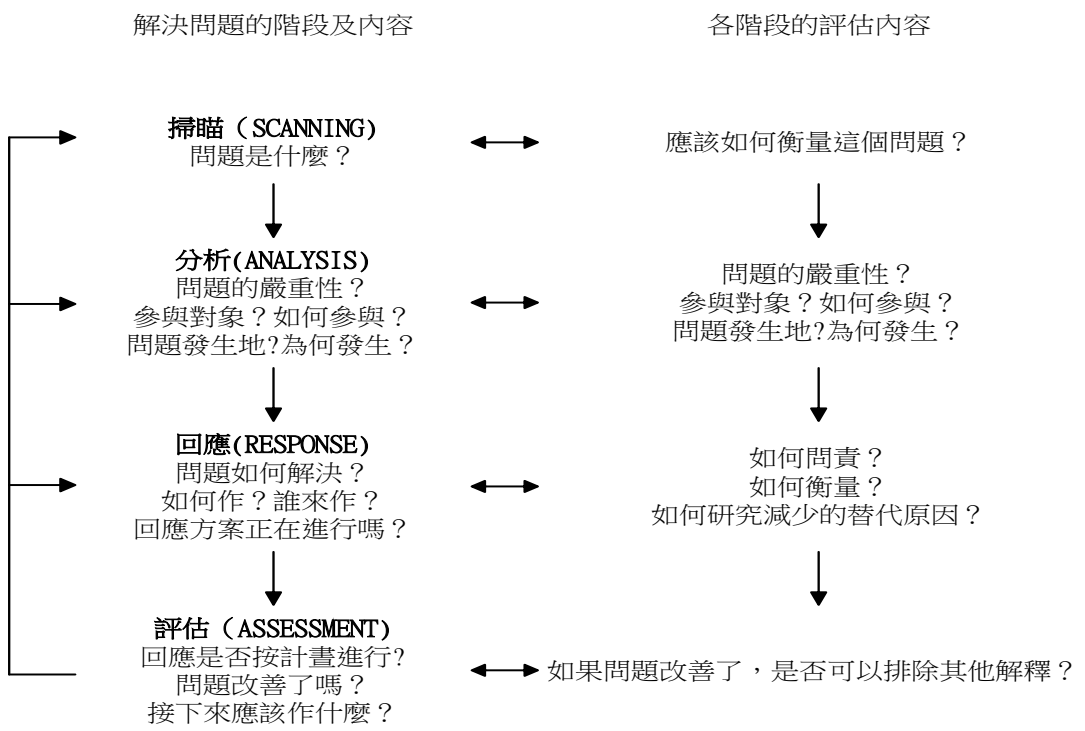


圖 2-9 SARA 流程及評估

資料來源：Eck, J. (2016). *Assessing Responses to Problems An Introductory Guide for Police-Problem Solvers*. Washington, DC: U.S. Dept. of Justice, Office of Community Oriented Policing Services, p9.

表 2-3 過程評估與影響評估之區別

		過程評估結果	
		回應完全按照計畫或大部分按照計畫執行	未實施回應或回應方式與計畫內容完全不同
影響評估結果	問題獲得改善	A.有證據顯示回應措施可改善問題	C.可能因其他原因使問題獲得改善，或回應措施意外有效。
	問題沒有獲得改善	B.有證據顯示回應措施無效，應該嘗試採取不同的措施	D.知之甚少，也許按照回應計畫執行可改善問題

資料來源：Eck, J. (2016). *Assessing Responses to Problems An Introductory Guide for Police-Problem Solvers*..ashington, DC: U.S. Dept. of Justice, Office of Community Oriented Policing Services, p13.

六、情境犯罪預防（Situational Crime Prevention）

(一)理論介紹

1.基礎概念

情境犯罪預防與大多數犯罪學理論的基本論點截然不同，它是從分析某些特定類型犯罪的環境條件出發，繼而導入改變管理運作及環境以減少犯罪發生的機會。因此，它的研究重點是犯罪的環境，而不是實施犯罪行為的人。其目的在預防犯罪的發生，而不是偵查和逮捕犯罪者。它並不尋求透過改造社會或政府機構來消除人們的犯罪行為或犯罪傾向，而是要降低犯罪行為對犯罪者的吸引力。該理論的核心不是啟動刑事司法系統防制犯罪，而是動員公共及私人組織和機構，在日常運作或提供服務的過程中減少犯罪機會，以改變犯罪的情境決定因素，協助預防犯罪的發生。(Clarke, 1997a;黃翠紋、蘇信雄，2020)情境犯罪預防植根於日常活動理論、理性選擇觀點、犯罪模式理論等環境犯罪學理論及社會和環境心理學理論。理性選擇觀點認為，犯罪的形成是有犯罪動機的人和當前的情境互動的結果（詳如本研究前述）。與情境犯罪預防的基本假設認為犯罪是動機和情境互動的結果是相同的（Clarke, 2016），因此，情境犯罪預防係針對特定型態的犯罪，設計、操縱和管理當前的環境，讓潛在犯罪者感覺從事該犯罪較困難及較具風險，或讓潛在犯罪者感覺從事該犯罪缺乏適當利益或可饒恕的藉口（黃翠紋、蘇信雄，2020)其理論由以下四個框架組成 (Clarke, 1997a)：

(1) 以日常活動和理性選擇為理論基礎。
(2) 以行動研究作為方法論。
(3) 運用技術來減少犯罪機會。
(4) 所有的犯罪預防措施都要經過詳細的評估。

在早期的情境犯罪預防研究中機會與情境是同義的，後續的研究逐漸體認到，情境不

僅為犯罪提供「機會」也提供誘惑、引誘和挑釁（Wortley,2017），這種認知擴大了情境犯罪預防的範圍。學者 Taylor 等指出沒有人是被迫犯罪的。因此，在社會上遭受歧視和地位低下並不會驅使人們從事詐欺犯罪；相反，犯罪人選擇例如：電信網路假投資詐欺等犯罪行為的目的是為了金錢。事實上，人們犯罪是因為他們認為這會為他們帶來一些好處。這些好處並不限定於經濟上的，也可能是物質、心理、感情、精神等人類與生俱來，包括有形及無形的慾望。而人類是否選擇犯罪取決於粗略計算獲得獎勵的機會和失敗被捕、懲罰、等的風險（Taylor,Walton,Young,1973）。他們也可能是在情緒壓力下或在酒醉時做出選擇。他們也可能是一瞬間的、魯莽的、不知情的或不明智的情境下作出犯罪的選擇。換言之，如果犯罪與否是可以選擇的，那麼那些有犯罪傾向的人，在面對不利於犯罪的情境時應該也會選擇避免犯罪。因此，創造不利於犯罪機會的環境是情境犯罪預防的目標。

情境犯罪預防理論認為「機會」在犯罪中佔有有重要地位，傳統的認知理論學者，也不否認「機會」在某種程度有促進犯罪作用，同時也認為「機會」是動機的附屬品，動機是首先要解釋的也是最重要的事。另一方面，環境犯罪學者同意動機是重要，但在解釋犯罪時也同樣重視「機會」。Clarke 主張「機會」在犯罪中發揮以下的八個重要作用（Clarke,2016）：

(1) 機會在各種類型的犯罪中都存在，包括精心策劃的犯罪，例如：電信網路詐欺、銀行搶劫和恐怖主義。
(2) 機會是犯罪的重要原因。
(3) 有犯罪傾向的人，如果遇到更多的犯罪機會，就會犯下更多的罪。
(4) 經常遇到犯罪機會的人，可能會導致他們去尋求更多的犯罪機會。
(5) 在犯罪機會激增的情境下，原本沒有犯罪傾向的人，也可能而陷入犯罪。
(6) 一般來說，原本守法的公民如果經常遇到容易犯罪的機會，也極有可能會利用這些機會犯罪。
(7) 犯罪機會越多，犯罪就會越多。
(8) 減少特定形式的犯罪機會，將有助於減少總體犯罪發生數。

「減少犯罪機會」及「增加犯罪者所感知的風險」是情境犯罪預防最重要的概念，也就是說，改變當前的情境環境能使犯罪行為失去對潛在犯罪者的吸引力。情境犯罪預防假設犯罪者都是理性的，並非僅因一時衝動而犯罪，犯罪是犯罪者的自行選擇的結果，犯罪者完全可以控制自已是否實施犯罪。因此，若要嚇阻犯罪發生，就必須讓犯罪者感知到當前所處的情境環境有高度風險。而與此相反的，讓犯罪者感受到較低風險的地點、時間及潛在被害者，都將可能成為犯罪者的犯罪實施對象。而在實際運作方面，情境犯罪預防方案包括下列五個階段（黃翠紋、蘇信雄，2020)。

(1) 針對標的犯罪問題的性質及範圍，蒐集資料。
(2) 針對容許及促進標的犯罪問題發生的情境條件，進行分析。
(3) 針對阻礙標的犯罪問題發生的方法，進行系統性的研究，包括成本分析。
(4) 實施最具功能、可行性及經濟的措施。
(5) 監控結果及傳播經驗。

另外，情境犯罪預防的倡導者 Clarke（1997b）曾表示，在情境犯罪預防理論的發展過程中，雖有受到問題導向警政的部分影響，使得兩者有相似之處，但其間仍有顯著差別。

例如：問題導向警政是警察機關的運作管理方法，但卻不一定都聚焦於犯罪問題的處理，而情境犯罪預防則是一種許多機構皆可使用的犯罪控制途徑。但是，近年來的研究卻認為，情境犯罪預防與問題導向警政關係密切。首先，這兩種觀點都要求仔細分析犯罪模式和問題。其次，情境犯罪預防和問題導向警政都認為小事件可能會造成大問題，所以都同意全盤了解問題細節很重要。第三，情境犯罪預防與問題導向警政都要求解決方案必須在短期內見到效果。第四，情境犯罪預防的關注重點跟大多數警察工作一樣都在解決問題。第四，情境犯罪預防的重點是與問題密切相關的原因，就像大多數警察工作一樣。第五，有越來越多的研究結果顯示，警察和其他人的情境干預可以有效減少犯罪 Scott,Eck,Knutsson 和 Goldstein（2016）、Guerette(2009）、Clarke (1997c)、Scot 和 Goldstein (2012)以及 Eck 和 Madensen (2012)都已詳細闡述了情境犯罪預防與問題導向警務之間的關聯。

如同本研究前面所述運用犯罪腳本技術，詳細解構犯罪的連續步驟，將可發現促進犯罪成功遂行的關鍵節點，繼而採用問題導向警政的 SARA 模式及犯罪問題分析三角，針對這些節點導入多項情境犯罪防措施以阻斷犯罪的進行。

2.情境犯罪預防的技術

現在情境犯罪預防的技術仍持續在研發中，學界對於減少犯罪機會的各種情境犯罪預防措施，採取多種不同的方法進行描述和分類，從早期 Clarke（1983）揭示情境犯罪預防概念時，僅提出三項干擾犯罪發生的途徑，分別是監控（surveillance）、強化標的（target hardening）及環境管理（environmental management）。監控途徑包括自然監控、正式監控及員工監控等概念，強化標的包括使用鎖、強化玻璃及其他安全裝置，環境管理則指改變環境以減少犯罪的機會。之後，Clarke（1992）從理性選擇的觀點，將情境犯罪預防的技術具體化為三類：增加犯罪的功夫、增加犯罪的風險、減少犯罪的利益。並在每一類中建構出四項預防技術，共計 12 項情境犯罪預防技術。經過幾年的實踐經驗及研究後，Clarke 和 Homel（1997）從犯罪者為其行為辯護的觀點，認為應將犯罪行為的社會性及心理性脈絡納入情境犯罪預防中，加入了能夠激發犯罪者罪惡感或羞恥心的技術，而將情境犯罪預防的技術擴充為四類計 16 項，（Wortley,1996）認為四類的情境犯罪預防技術仍然不夠完整，尤其是「激發犯罪者罪惡感或羞恥心」這一類的技術不夠詳盡，他指出罪惡感與羞恥心並非同一件事，這兩種概念應該要分開。此外，Wortley（2001）還認為情境犯罪預防過於強調那些能夠控制或抑止犯罪發生的因素，而忽略了促使或導致犯罪發生的因素。他進一步提出四種促發因素：催促因素（有助於強化犯罪機會的事件或情境，例如敞開的門或他人犯罪）、壓力因素（引發行動的直接刺激，例如偏差同儕、隨團體行事、依指示做壞事等）、允許因素（容許犯罪行為的情境或觀念，例如每個人都會犯法的觀念或該犯罪係由被害者所引發的，繼而容許或接受犯罪的發生）、挑釁因素（讓人感到不舒服、挫折、煩躁的因素）。Wortley（2001）認為，這些因素並未納入情境犯罪預防的技術。2003 年 Clarke 和 Eck 參考 Wortley（2001）的意見，將先前的第四類技術「激發犯罪者罪惡感或羞恥心」更名為「移除犯罪的藉口」，及從社會與環境心理學理論的觀點，又增加一類技術來涵蓋犯罪的促發因素，名稱為「減少對犯罪的挑釁」。情境犯罪預防技術發展至今共有五類，每一類包含五項技術，共計 25 項減少犯罪機會技術（Clarke & Eck,2003；黃翠紋、蘇信雄，2020)參閱(表 2-4)。

表 2-4 現今的 25 項情境犯罪預防技術

增加犯罪的阻力	增加犯罪的風險	減少犯罪的利益	減少對犯罪的挑釁	移除犯罪的藉口
1.強化標的 ・方向盤鎖、防止移動的裝置 ・防搶掩蔽物 ・防損壞包裝	6.擴大監控 ・平時應採取預防措施：夜行結伴，留下有人在的跡象，攜帶手機 ・守望相助	11.隱蔽標的 ・不將車輛停放在街道上 ・性別中立的電話目錄 ・無標誌運鈔車	16.減少挫折與壓力 ・有效率的排隊與警察服務 ・擴充座位數量 ・柔和的音樂與燈光	21.訂定規範 ・租賃契約 ・騷擾規範 ・飯店住宿登記
2.管制入口 ・入口通話裝置 ・電子通行證 ・行李安檢	7.強化自然監控 ・改善街道照明 ・防衛空間的設計 ・鼓勵檢舉	12.移除標的 ・可卸式汽車音響 ・婦女庇護空間 ・付費電話的預付卡	17.避免爭端 ・隔離競爭球隊的球迷 ・舒緩酒吧內的擁擠人潮 ・訂定計程車收費標準	22.公告守則 ・「禁止停車」 ・「私人財產」 ・「熄滅營火」
3.檢查出口 ・驗票才能出去 ・出境文件 ・電子式的商品標籤	8.減少匿名 ・標示計程車司機的身分識別證 ・張貼「我的駕駛服務品質好嗎？」貼紙 ・學校制服	13.辨識財物 ・財物標記 ・車輛牌照與零件標記 ・畜養動物標記	18.減少情緒刺激 ・管控暴力色情 ・球場內鼓勵球迷的好行為 ・禁止種族毀謗	23.喚起良知 ・路旁車速顯示看板 ・海關申報簽名 ・「偷拿店內商品是犯罪行為」
4.使犯罪者轉向 ・封閉街道 ・女性浴室隔間 ・分散酒吧	9.運用地點管理者 ・雙層巴士裝設錄影監視器 ・便利商店設置兩名店員 ・獎勵警戒活動	14.分裂市場 ・監控當舖 ・管控分類廣告 ・攤販營業許可證	19.減少同儕的中立化效應 ・「白痴才會酒醉駕車」 ・「說不，是 OK 的」 ・分散學校裡的麻煩製造者	24.促進守法 ・圖書館借書簡便化 ・公共廁所使用方便化 ・垃圾桶設置普遍化
5.管制工具/武器 ・「智慧型」槍枝 ・失竊後無法盜打的行動電話 ・限制販售噴漆給少年	10.強化正式監控 ・裝設闖紅燈照相機 ・裝設防盜警鈴 ・設置保全警衛	15.拒絕給予利益 ・墨水式商品標籤 ・清除塗鴉 ・路面減速顛簸	20.防止模仿 ・立即修復毀損公物 ・電視節目過濾措施 ・檢視犯罪手法的細節	25.管制毒品及酒類 ・酒吧提供酒測器 ・侍者介入處理 ・無酒精活動

資料來源：Clarke, R.V and Eck, J. (2003). *Become a Problem-Solving Crime Analyst-In 55 Steps.* London: Jill Dando Institute of Crime Science, UCL, p63；跨境電信網路詐欺犯罪之防制，黃翠紋、蘇信雄，2020，國境執法與合作。黃文志、王寬弘主編，臺北市：五南圖書出版股份有限公司，頁 485-486。

(二)理論應用

本研究認為欲有效防制電信網路假投資詐欺犯罪，首應全力改變「現在的」犯罪情境原因，改變「現在的」情境更有可能成功減少犯罪，因果之間的連結也更加直接。因此，可參採情境犯罪預防理論，創造不利於假投資詐欺犯罪機會的環境，將是有效預防是類犯罪的目標，而其犯罪防制方案應包括下列五個面向的技術

1.增加犯罪的功夫面向

理性的假投資詐欺犯罪者，利用設於境外的詐欺機房透過影音、社群平台(FB、IG、YouTube、交友軟體、簡訊等)大量散播虛假投資訊息，吸引民眾進入其設定的詐欺情境。其防制措施應包括落實電信事業及數位經濟產業管理措施，防止犯罪集團利用電信服務發送詐欺簡訊與網路推播連結詐欺廣告，阻絕民眾接觸詐欺相關訊息及廣告，以提高犯罪的困難度。`

2.增加犯罪的風險面向

犯罪者為規避查緝，利用各國法制、司法管轄主張不一，及偵查技術與相關設備的落差，將犯罪行為分解至數個國家，再運用遠端遙控的資通訊技術，指揮犯罪組織成員騙取民眾財物，製造警察查緝斷點，造成調查取證與案件聯結困難。其防制措施應包括統合國家整體偵查犯罪能量，深化跨（國）境共同打擊詐欺犯罪與追緝境外犯罪者的合作交流，增加犯罪者在犯罪前即可感知到極高的被捕風險，促使犯罪者主動放棄犯罪的念頭，達到預防犯罪的效果。

3.減少犯罪的利益面向

假投資詐欺犯罪集團誘使被害民眾大量匯款至指定的人頭帳戶，或備妥鉅額現金或向假冒商家購買巨額虛擬通貨，再派出共犯面交收取現金或虛擬通貨，是典型的智慧型經濟犯罪。其防制措施應包括強化金融機構及虛擬資產服務提供者的監管能力，有效防制犯罪集團取得人頭帳戶，建構完善的金融防詐網，攔阻非法詐欺金流，以減少犯罪的利益並降低被害民眾的損失。

4.減少對犯罪的挑釁面向

犯罪集團利用資(通)訊科技設備及方法隱身於境外，針對人性心理弱點，編造各種一夕致富的虛假情境，使得被害人深陷詐欺情境仍不自知，政府雖長年大量宣導防詐資訊及媒體反覆報導，但部分民眾已產生麻木及過度自信心態，對宣導資訊視而不見，在心存僥倖且利令智昏情況下被詐欺；復因此類犯罪被捕風險小、刑責低，所得不法利益龐大，且犯罪模式易於複製，在成本效益考量下，造成常業犯和累犯再犯率偏高，難以嚇阻其犯行。其防制措施應包括透過政府所屬宣導通路及資源，同時結合民間團體或與企業合作，擴大宣傳途徑與範圍，採分齡分眾方式宣導，以深植內化民眾防詐意識，並透過實證方式檢驗宣導成效；另外，應謹慎揭露警察查緝詐欺之關鍵技巧，以防犯罪集團規避，並針對詐欺常業犯和累犯訂定更嚴厲的刑責以遏止犯罪模仿效應。

5.移除犯罪的藉口面向

垂涎假投資詐欺犯罪龐大不法所得的黑道幫派組織，網羅廣告投放商、APP 開發工程師、資通系統架設商、銀行從業人員、律師、代書、執法人員等各專業領域不肖人員及召募 18 至 39 歲之間互相不認識之年輕人組成的犯罪集團，組織結構完整，又採用網絡管理模式，讓整個犯罪更具效率，使其危害程度更加嚴重。其防制措施應包括加強黑道幫派組織掃蕩壓制，使其收斂犯罪氣焰，並防杜侵入校園吸收青少年加入犯罪集團；同時透過警察犯罪紀錄分析犯罪者的年齡、職業等背景，針對容易成為犯罪者之目標族群，強化跨部

會及公私協力合作等多元管道進行道德教育，加強法治觀念，以喚起良知避免成為詐欺犯罪者。

七、小結

綜合前述探討，電信網路假投資詐欺犯罪的成因與防制策略，應從犯罪學理論的演進脈絡與環境犯罪學的理論基礎加以整合分析。傳統犯罪學理論早期關注「人」的犯罪成因，從惡魔說的宗教觀點、古典犯罪學派的理性選擇、實證主義的生理與心理決定論，到二十世紀後期的批判犯罪學、整合理論與發展性犯罪理論，皆試圖從個體差異與社會結構層面解釋犯罪。古典學派強調理性人假設，主張透過確定、迅速且嚴厲的刑罰，以遏止犯罪行為；而實證主義則轉向以科學方法探究犯罪原因，認為生理、心理、社會等外在因素決定了人是否犯罪，並倡導犯罪處遇個別化。至上世紀 60 年代以降，批判犯罪學指出權力結構、階級與性別不平等乃犯罪根源。80 年代後，因犯罪現象多元複雜，遂出現整合理論，綜合多重因素以解釋不同層面的犯罪現象。晚近之發展性犯罪理論與生活週期理論則聚焦於犯罪行為的形成與演變，強調犯罪行為受個體與環境交互影響的持續過程。

然而，上述理論大多關注「為何某些人會犯罪」，卻忽略犯罪事件本身的「如何發生」。環境犯罪學正是在此理論缺口中興起，其研究重點不再是犯罪者的內在動機，而是犯罪事件在具體空間與時間中的生成條件。該理論主張，犯罪的發生並非單純個人選擇，而是環境結構、社會互動與監管機制共同作用的結果。本研究從理性選擇理論與日常活動理論出發，著重於犯罪者的決策與被害者的日常脈絡，認為犯罪行為乃特定時空下理性行動的結果，只要改變情境條件，即可改變犯罪者的行為選擇。

理性選擇理論指出，犯罪者在有限理性下，根據風險、報酬、時間與環境條件進行行為評估。假投資詐欺行為者在策畫犯罪時，會衡量犯罪成功率、被查緝可能性及贓款可得性等變數，當犯罪報酬遠高於風險成本時，即促使其行動。若能在制度設計與環境管理中提升犯罪成本、增加查緝風險或縮短犯罪獲利時間，即能有效影響其理性選擇，使其放棄行動。

日常活動理論則從受害角度出發，認為犯罪的發生需同時具備三個條件：具動機之犯罪者、有價值且易接近之標的，以及缺乏有效監護者。電信網路假投資詐欺的受害者多為具有投資需求、貪利心理或缺乏金融與數位素養之民眾，這些特性使其成為高度吸引的「合適標的」。另一方面，數位空間的匿名性與跨境性，削弱了「監護者」的存在，使犯罪者得以反覆利用相似手法行騙。因此，防制重點在於建立有效監護機制，例如：電信業者加強監測異常簡訊與假連結；社群平臺設立詐欺廣告審查機制；金融機構與警方即時共享可疑金流資料，形塑數位環境中的「警戒防護網」。

犯罪腳本理論（Cornish,1994a,b）則補足了環境犯罪學在行為過程層面的分析不足。假投資詐欺行為者通常依「招募→準備→執行→掩飾」四階段進行，從建立假投資網站、布建社群帳號、拉入潛在受害者，到最終透過人頭帳戶或虛擬貨幣洗錢。腳本化分析能揭露每一階段的行為鏈結與決策邏輯，協助警方在不同階段部署攔阻介入點，如封鎖詐欺網域、追查金流節點、監測 VPN 與跨境主機等。

問題導向警政（Problem-Oriented Policing, POP）與 SARA 模式（Scan、Analyze、Respond、Assess）進一步提供理論落實的行動架構。警察機關可透過掃描階段辨識詐欺熱區與模式，分析階段以犯罪腳本與數據分析找出成因與結構漏洞，回應階段結合跨域資源（金融監理、通訊管制、社群平臺管理）實施具體措施，評估階段再檢視政策成效與調整策略，形成動態循環的防制機制。此模式強調警察不僅為執法者，更是問題解決者與風險管理者，透過持續修正與多部門合作，將防詐工作制度化。

在防制策略層面，本研究認為情境犯罪預防理論最能提供具體可行的介入方向。Clarke（2016）指出，改變「現在的犯罪情境」比試圖改變犯罪者人格更能有效減少犯罪。電信網路假投資詐欺的防制策略可分為五個面向：

（一）增加犯罪的阻力面向

詐欺集團仰賴跨境技術與社群平臺散播假投資訊息。警方與主管機關應強化電信業與數位平臺監管機制，推動「來源封鎖與識別」制度，例如建立跨部門詐欺網址資料庫、導入 AI（Artificial Intelligence）[5]假廣告偵測系統、建立多層次通訊監控平台，以提高犯罪者操作的技術與時間成本。

（二）增加犯罪的風險面向

針對詐欺集團利用多國管轄落差分散犯罪鏈的特性，應深化兩岸及國際警察合作、金融監理與司法互助合作。透過跨境情資共享、建立境外詐欺資料交換機制、派駐境外警察聯絡官等方式，使犯罪者在行動前即感知高度被查緝風險。此外，應強化國內跨機關資料整合，例如金融、電信與警政資料連結分析，實現即時預警與追查。

（三）減少犯罪的利益面向

假投資詐欺屬於「高報酬、低風險」型犯罪，故須強化金融防詐機制以削弱犯罪誘因。包括：強化銀行 KYC 與可疑帳戶通報制度、建立跨行即時金流監控平臺、推動虛擬資產業者納管與實名制。警方應與金管會合作，導入 AI 金流分析以追蹤贓款流向，並強化犯罪所得追徵與沒收制度，使詐欺行為「無利可圖」。

（四）減少對犯罪的挑釁面向

許多被害人因宣導疲勞、過度自信或「賺快錢」心態而陷入詐局。政府應推動分齡、分眾、分層的精準宣導策略，利用社群媒體互動行銷、真實案例故事化敘事，提升民眾風險感知。同時，針對常業犯與累犯應修法加重刑責，建立累進刑制與教育矯正措施，以阻止犯罪模仿效應並強化嚇阻力。

（五）移除犯罪的藉口面向

詐欺集團常由黑道、白手套與專業技術人員組成網絡。警方除應強化掃黑與壓制外，並應防杜黑幫滲透校園與網路社群，吸收青少年為車手或電話手。另可透過犯罪資料庫分析常見犯罪者之年齡、職業背景與社群來源，針對高風險族群推展法治教育、道德教育與就業輔導，喚起其社會責任與法律意識，減少「合理化」犯罪的心理藉口。

5.指人工智慧，係由電腦系統模擬人類認知功能（如學習、推理、判斷與自我修正）之技術總稱，廣泛應用於資料分析、自動化處理、語音辨識等領域，近年亦被應用於詐騙偵測與資訊安全防護中。

進一步而言，警察機關在防制詐欺犯罪的角色，應從案件偵查轉型為風險管理。在科技發展快速與犯罪手法持續演變的今日，警方需結合 AI 資料分析、網路監控、金流偵測與社會心理研究，建構跨部會「科技偵查平台」。該平台能整合金融、電信、社群與司法資料，實現跨域即時預警，並建立民眾檢舉與企業回報機制，形成「公私協力防詐網絡」。

此外，兩岸及國際合作亦為不可或缺之要素。假投資詐欺多設境外機房，利用 VOIP 與 VPN 隱藏來源，警方應推動「跨境電信犯罪聯防機制」，透過與主要通訊服務供應商（如 Meta、Google、LINE 等）合作，建立快速封鎖假帳號與假廣告管道。

最後，從理論與實務結合觀點觀之，環境犯罪學與情境犯罪預防理論的核心意義在於「改變情境即可改變行為」。當潛在犯罪者察覺環境風險上升、犯罪報酬下降或監管強化時，犯罪動機即會自然收斂。實證研究亦顯示，情境犯罪預防不僅能有效降低犯罪率，還可能產生「利益擴散」（diffusion of benefits）效應，使鄰近區域同樣受益（Clarke, 1997；Eck, 1995；黃翠紋、蘇信雄，2020）。

綜上所述，防制電信網路假投資詐欺犯罪的根本策略，應整合理論與實務、科技與管理，從改變犯罪情境出發，建構多層次的預防網絡。警察機關應扮演「系統整合者」角色，結合環境設計、數據監理與公私協力機制，落實打詐五面向防制架構。唯有在理性選擇、日常活動與情境預防三大理論支撐下，方能形成全面、持續且具韌性的防詐體系，有效遏止新型詐欺犯罪之蔓延，並為臺灣防制電信網路假投資詐欺犯罪建立理論與實務並重之長期政策藍圖。

第二節 臺灣電信網路詐欺犯罪現況及防制策略

憑藉不斷的努力與創新，近年來臺灣在半導體、資通訊、生物科技等多個領域都有著卓越的科技實力。發達的科技產業，不僅是帶領臺灣經濟成長的動力來源，也是穩定社會的重要基石，同時也造就人民收入日益提高及民間各種投資風氣盛行，詐欺集團利用民眾急於獲利心態，以投資飆股、虛擬貨幣、期貨、外匯及基金等名義吸引民眾加入詐欺集團所架設的不實投資網站或下載 APP，初期讓被害人小額獲利，待民眾誤信為真而投入大量資金，欲實現獲利時，再以各種理由拒絕出金，俟民眾發現帳號遭凍結或網站關閉始知遭詐，造成民眾鉅額財產損失。詐欺集團掌握人性「貪心」與「不甘心」等心理因素，利用各種資通訊科技工具，編製客製化詐欺劇本，以獲取不知情民眾的信任，當被害人相信詐欺話術深陷在詐欺情境時，他人縱使費盡九牛二虎之力勸說，亦難撼動被害人對犯罪集團的信任。也有些被害人雖懷疑自己被詐欺，卻因貪於虛假的高報酬率或礙於面子而不願承認，因為沒人想承認自己是傻瓜，直到被掏光所有錢財，始驚覺遭詐欺。本節研究者將就臺灣電信網路假投資詐欺犯罪現況、犯罪特性及結構、防制策略、成效與面臨困境逐一分析，以窺得此類犯罪全貌。

一、犯罪現況

根據臺灣警政署刑事警察局統計資料顯示，近五年（2020 年至 2024 年）全般詐欺案件自 2020 年發生 23,054 件，到 2024 年的 118,535 件，增加 95,481 件（+414.16%）；其中假投資詐欺更從 2020 年發生 2,852 件，到 2024 年增長至 44,124 件，增加 41,272 件（+增加 1447.12%），進一步分析可發現假投資詐欺發生數在 2020 年僅佔全般詐欺 12.37%，但到 2024 年佔比已上升至 37.22%(如圖 2-10)。

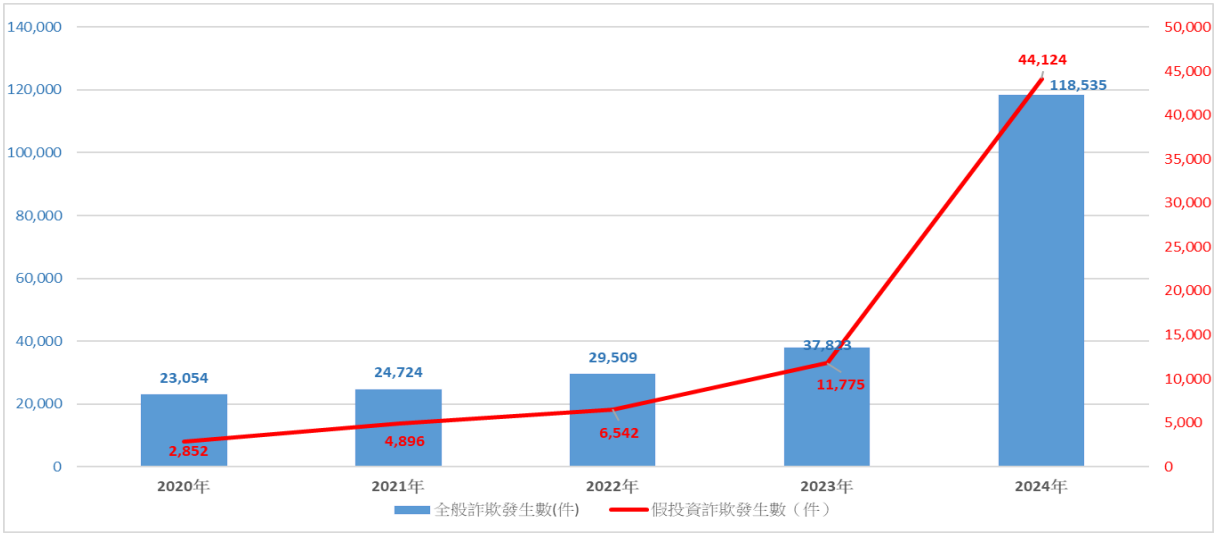


圖 2-10 2020 年至 2024 年臺灣全般詐欺與投資詐欺發生數比較

資料來源：整理自內政部警政署刑事警察局（2020－2024）。刑案紀錄表。

在財損部分，近五年（2020 年至 2024 年）全般詐欺案件自 2020 年財損 42.55 億元，到 2024 年的 487.6 億元，增加 445.05 億元（+1045.95%）；其中假投資詐欺更從 2020 年的 10.27 億元，到 2024 年 361.3 億元，增加 351.03 億元（+增加 3418.01%），進一步分析可發現假投資詐欺財損在 2020 年僅佔全般詐欺 24.14%，但到 2024 年佔比已上升至 74.10%(如圖 2-11)。

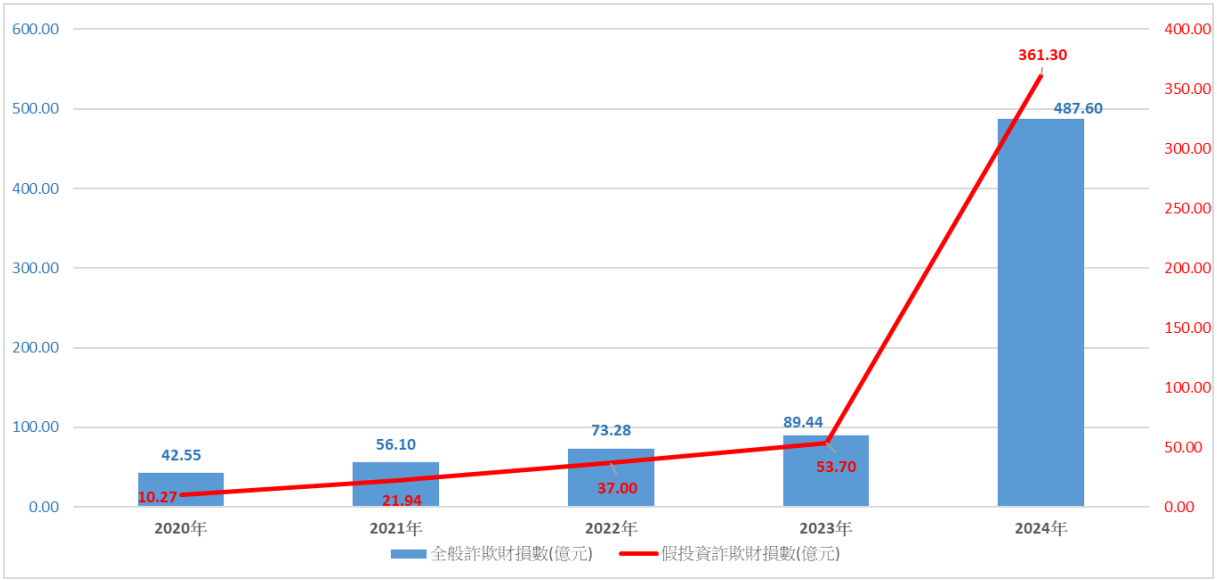


圖 2-11 2020 年至 2024 年臺灣全般詐欺與投資詐欺財損金額數比較

資料來源：整理自內政部警政署刑事警察局（2020－2024）。刑案紀錄表。

進一步分析近 5 年臺灣詐欺犯罪案件發生數，發現假投資案件發生數逐年增加，至 2023 年已竄升至第 1 名（佔全般詐欺犯罪案件發生數 30.98%）（如表 2-5）。

表 2-5 2020 年至 2024 年臺灣詐欺案件發生數前 5 名

排名＼年份	2020	2021	2022	2023	2024
第1名	假網路拍賣(購物)(含一般購物)	假網路拍賣(購物)(含一般購物)	假網路拍賣(購物)(含一般購物)	**假投資**	**假投資**
件數	5,906	5,623	6,791	**11,719**	**44,124**
第2名	解除分期付款詐騙(ATM)	**假投資**	**假投資**	假網路拍賣(購物)(含一般購物)	假網路拍賣(購物)(含一般購物)
件數	3,172	**4,896**	**6,542**	8,346	27,744
第3名	**假投資**	解除分期付款詐騙(ATM)	解除分期付款詐騙(ATM)	解除分期付款詐騙(ATM)	解除分期付款詐騙(ATM)
件數	**2,852**	4,328	5,084	6,992	9,775
第4名	猜猜我是誰	猜猜我是誰	假愛情交友	假愛情交友	假愛情交友
件數	2,135	1,758	1,442	1,352	5,649
第5名	假冒機構(公務員)	假愛情交友	猜猜我是誰	猜猜我是誰	佯稱代辦貸款
件數	1,077	1,174	1,245	1,209	3,449

資料來源：整理自內政部警政署刑事警察局（2020－2024）。刑案紀錄表。

財損金額自 2020 年起已連續 5 年排名第一，2024 年更佔詐欺犯罪案件財損金額 74.09%（如表 2-6）。

表 2-6 2020 年至 2024 年臺灣詐欺案件財損數前 5 名

排名＼年份	2020年	2021	2022	2023	2024
第1名	**假投資**	**假投資**	**假投資**	**假投資**	**假投資**
財損金額（億元）	**10.27**	**21.94**	**37.04**	**53.44**	**361.3**
第2名	假冒機構(公務員)	假冒機構(公務員)	假冒機構(公務員)	解除分期付款詐騙(ATM)	假冒機構(公務員)
財損金額（億元）	6.67	7.66	8.37	8.52	29.71
第3名	解除分期付款詐騙(ATM)	解除分期付款詐騙(ATM)	解除分期付款詐騙(ATM)	假冒機構(公務員)	假網路拍賣(購物)(含一般購物)
財損金額（億元）	5.1	6.65	7.61	5.77	21.9
第4名	猜猜我是誰	猜猜我是誰	假網路拍賣(購物)(含一般購物)	假網路拍賣(購物)(含一般購物)	假愛情交友
財損金額（億元）	5.07	4.28	4.59	5.46	17.4
第5名	假網路拍賣(購物)(含一般購物)	假愛情交友	猜猜我是誰	猜猜我是誰	解除分期付款詐騙(ATM)
財損金額（億元）	3.72	4.16	2.9	3.03	12.4

資料來源：整理自內政部警政署刑事警察局（2020－2024）。刑案紀錄表。

依據上述統計資料顯示，詐欺案類從 2020 年發生 23,054 件，到 2024 年的 118,535 件，財損金額從 2020 年的 42.55 億元新台幣，上升到 2024 年的 487.60 億。其中，假投資案件自 2020 年 2,852 件，逐年上升到 2024 年 44,124 件，高居當年臺灣詐欺類犯罪的第 1 名；財損自 10.27 億，逐年上升到 361.3 億，更是連續 5 年高居臺灣詐欺類犯罪財損第 1 名。

綜合分析上述官方統計數據可發現，近 5 年來假投資詐欺犯罪，不論發生數或財損數均呈現快速成長趨勢，在 2024 年已佔全般詐欺發生數 37.22%，財損更佔達 74.09%。

二、 犯罪特性及結構特徵分析

近年來人工智慧、區塊鏈、雲端運用、巨量資料、5G 通訊等科技陸續問世，造就電信通訊、網際網路、跨國（境）金融快速流通及虛擬通貨蓬勃發展，大幅改變人類社交及經濟活動模式，發達的科技雖為民眾生活帶來便利，成就我們跨越時空能力，但不法分子卻在犯罪理性選擇動機驅使下，經常利用資訊科技快速且隱密的特性與功能遂行犯罪並逃避執法機關的查緝（孟維德，2019）。黑道幫派高度參與的假投資詐欺集團即是運用科技的即時迅速及容易造成民眾認知錯誤的特性，使用操作簡便且易於匿名的社群通信軟體，利用民眾急於獲利心態，以謊稱各種快速致富的投資名義吸引民眾加入渠所架設的不實投資網站或下載 APP，實施假投資詐欺犯罪，使得電信網路假投資詐欺犯罪產生革命性的改變。本研究在蘇信雄 2022 年的研究基礎下（蘇信雄，2022），再參考近年學界及實務界相關研究（賴擁連、蔡田木、陳玉書、許春金、葉碧翠，2023；黃光甫，2023；張榮興，2024；林建隆，2024；黃國師，2024；李彩溱，2024；鄭嘉慶，2024）綜合分析電信網路假投資詐欺犯罪之特性及結構特徵，共有 8 項如下：

(一)黑道幫派高度參與，犯罪成員專業化及年輕化

電信網路假投資詐欺犯罪是黑道幫派組織犯罪不法獲利重要來源，犯罪集團為逃避執法機關查緝，會想方設法接近、引誘、賄賂不肖執法人員加入犯罪行列或為犯罪集團提供保護傘，並網羅廣告投放商、APP 開發工程師、資通系統架設商、銀行從業人員、律師、代書等各專業領域的不肖人員及召募 18 至 39 歲之間互相不認識之年輕人（如表 2-7），再運用細密的犯罪分工，組成關係鬆散的犯罪網絡組織，並將整個犯罪集團切割成為集團首腦、詐欺機房、召募詐欺機房電話手集團、提領贓款車手集團、提供人頭帳戶集團、竊取個資駭客集團、地下匯兌洗錢集團、提供資通訊技術集團(如圖 2-12)等，各組織均有明確任務分工，並由具有各項專業背景人員負責管理及訓練，組織結構完整，又採用網絡管理模式，讓整個犯罪組織更具效率，使其危害程度更加嚴重。

表 2-7 2020 至 2024 年臺灣警察機關查獲詐欺犯罪案件年齡分布表

統計期	12-17歲	18-23歲	24-29歲	30-39歲	40-49歲	50-59歲	60-69歲	70歲以上	年齡總計
2020	1,642	7,517	7,840	7,514	4,416	2,676	1,566	453	33,624
2021	1,633	8,383	8,159	8,459	4,920	2,679	1,410	359	36,002
2022	1,662	9,775	10,678	11,612	6,696	3,267	1,471	379	45,540
2023	2,186	10,687	11,452	12,708	7,811	3,537	1,464	431	50,276
2024	3,124	12,289	11,452	12,521	8,384	3,718	1,723	572	53,783
總數	10,247	48,651	49,581	52,814	32,227	15,877	7,634	2,194	219,225
結構比	4.67%	22.19%	22.62%	24.09%	14.70%	7.24%	3.48%	1.00%	100.00%

資料來源：內政部警政署(2025a)。警政統計查詢網。取自：https://ba.npa.gov.tw/statis/webMain.aspx?k=defjsp，最後瀏覽日期：2025 年 4 月 19 日。

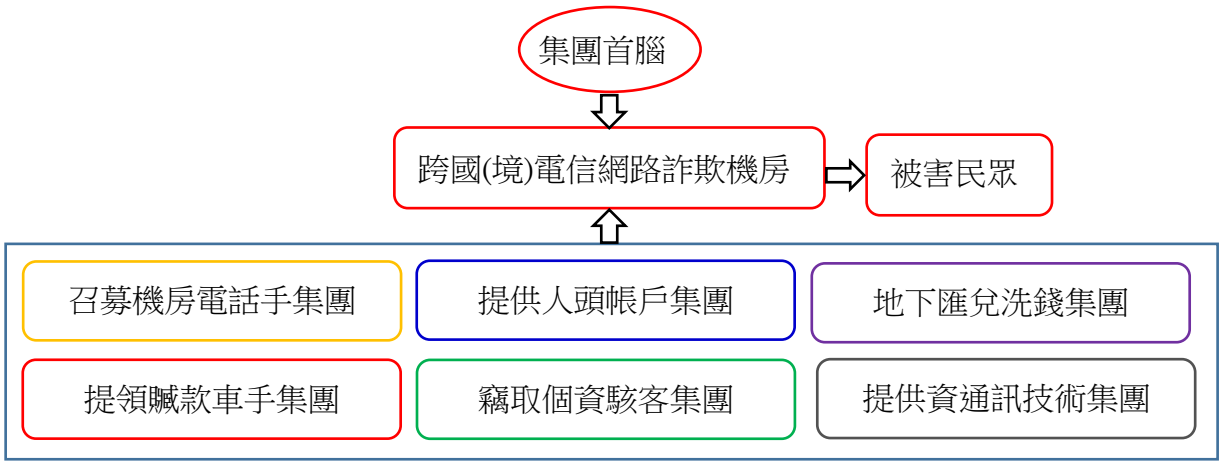


圖 2-12 臺灣電信網路假投資詐欺集團組織架構圖

資料來源：引自蘇信雄(2022)。電信網路詐欺犯罪機房跨境蔓延之研析。中央警察大學學報，第 59 期，23-52。桃園市：中央警察大學，頁 28。

(二)犯罪機房跨國蔓延，造成多國人民共同受害

電信網路假投資詐欺犯罪過程需大量仰賴資通訊技術，只要資通訊及金融網路可及地區，即可跨境實施假投資詐欺行為。因此，在執法機關強力查緝的推力因素下，犯罪集團為尋求生存的利基，逃避執法機關查緝，在理性評估各種拉力及中間障礙因素條件後，將詐欺犯罪機房遷移至犯罪資源較豐富，查緝電信網路詐欺犯罪能力尚未完備，人民之間的信任程度較低，入境證照取得較容易的鄰近國家地區，繼續針對防禦詐欺犯罪能力薄弱的民眾實施犯罪，造成詐欺機房設置地點由臺灣蔓延至中國大陸再逐漸蔓延至亞太、非洲、中東、西亞、加勒比海、歐洲等國家。被害人國籍除臺灣及中國大陸外，近年來日本、韓國、馬來西亞等亞洲國家有關民眾遭電信網路詐欺犯罪案件亦屢有所聞，當前電信網路詐欺犯罪已嚴重危害兩岸及第三地國家人民之生命財產安全，亦被臺灣媒體稱為「國恥」。

(三)犯罪集團跨境勾串，遠端遙控製造查緝斷點

電信網路詐欺犯罪集團，在評估犯罪風險及犯罪利益後，會召募不同國籍犯罪者共同組成分散在不同（地區）國家的犯罪組織，以逃避執法機關查緝，例如：最初運用通訊科技，將電話盜（轉）接至大陸沿海等地（如廈門）或利用可接收臺灣行動電話基地臺訊息或漫遊方式，演變為架設非法電信機房或透過網路電話、二類電信及各種資通訊技術進行遠端遙控，指揮車手在臺灣取款之犯罪手法， 形成「在中國大陸設立據點、詐欺臺灣民眾」或「在臺灣設立據點、詐欺中國大陸民眾」之犯罪結構，致警察機關大多僅能緝獲車手等共犯，難以追緝主嫌到案。近年來更轉型為「兩岸嫌犯結合第三國（地區）國家嫌犯共同犯罪，整體犯罪型態朝向組織化、多元化、國際化發展，利用各國尚未建立密切合作共同打擊犯罪機制之漏洞，而施行遠端遙控跨境犯罪模式，造成執法機關查緝的困境。

(四)運用各種資通訊科技工具，以隱匿真實身分

詐欺集團為逃避警察機關追查，將所施詐術與電信、網路等路徑相互結合，利用網際網路資訊互通開放，不受時間、空間、地域限制所影響的特性，輕易將大量詐欺訊息跨境傳送給不知情的民眾，特別在通訊與資訊技術結合後，利用通訊系統轉接網路再轉接通訊系統或利用通訊軟體，不但犯罪者的帳號身分隱匿，IP 位址更可以藉由虛擬私人網路 VPN（Virtual Private Network）專業技術加以隱匿，再輔以犯罪集團配合社會脈動事先精心編造各式假投資詐欺劇本，假借各種虛構之身分及名義，由多名成員分別扮演不同詐欺角色，利用資訊、通訊及大眾傳播媒介等管道，傳遞不正訊息給社會大眾，再進一步操弄、掌握及誘騙，使民眾輕易掉入犯罪集團所設陷阱，造成鉅額財產損失，最後，縱使被害人發現被詐欺報警偵辦，執法人員追查到網站的位址，亦可能在境外，或者網站早已關閉，使得偵查困難。

(五)利用被害人心理因素，精準實施客製化詐欺劇本

詐欺犯罪集團在與警察機關長期鬥智過程中，詐欺手法日益精進，犯罪集團的規模和專業程度，已可與一般中小型企業媲美。同時，犯罪者事先透過駭客入侵盜用個資等不法管道蒐集準確的民眾個人真實隱私資訊，再據以為被害人「客製化」詐欺劇本實施詐欺，提高被害人識別和預防的難度，增加遭詐欺成功之風險。電信網路假投資詐欺集團掌握利用人性貪心與急於獲利的弱點，以謊稱各種快速致富的投資名義，利用行動電話、社群網站、通訊軟體、交友平臺或網路廣告等以無差別漫天撒網方式，或利用民眾在使用網路社群媒體，例如：臉書、IG、YOUTUBE 等觀看新聞或影片時，強制彈跳出「高獲利投資理財」等廣告，吸引民眾一時好奇點選觀看，又或以美女或俊男身分利用網際網路在臉書、IG 等社群網站結識被害人，再引誘民眾加入渠所架設的不實投資網站或下載 APP 並施以小利，使被害人深陷其中，無法自拔，而遂行詐欺目的。

(六)犯罪模式易於複製，犯罪集團人員易於再犯

近年來警察機關緝獲詐欺集團，常發現重複犯案的累犯，這些資深犯罪成員在交保或服刑期滿後，常垂涎於詐欺犯罪的豐厚不法利益，而另起爐灶再度召集不法之徒，組成詐欺集團從事詐欺，並複製精進犯罪手法，以增加警察查緝困難度。另外，如果執法機關在執行查緝時，並未查獲幕後金主、機房負責人等高層關鍵成員，而僅是查獲機房電話手、取（領）款車手等低階犯罪者，將使犯罪集團召募遞補迅速且容易。且犯罪集團首要分子為降低遭執法機關查獲的風險，常會將犯罪集團切割成多個彼此不相干機房或相關小團體，分頭同時實施詐欺犯罪，即使其中一個機房或犯罪團體遭警察機關查獲，亦不影響整個犯罪集團運作，造成執法機關抓不勝抓的困境。

(七)洗錢管道隱密且多元，造成金流斷點追查困難

犯罪集團實施詐術，騙得被害人現金、黃金、遊戲點數、虛擬通貨等實體財產或虛擬通貨後，為了掩飾或隱瞞其不法所得來源，透過金融工具，將其犯罪所得漂白，使得犯罪者得以合法使用該所得（林德華，2012），電信網路假投資詐欺犯罪集團，運用金融交易數位化及支付工具多樣化的特點，利用人頭開設銀行帳戶，或藉由資通訊工具隱匿身分，使用金融科技在網路上開戶並快速轉移贓款，或利用為數眾多，提款地點便利的自動櫃員機（Automated Teller Machine,ATM）提取轉移贓款。近年來虛擬通貨在世界各國陸續掀起流行浪潮，迄今在市場上流通的種類已超過上萬種，因其具有點對點交易、去中心化、匿名性的特性，在追查不易且國際互助有限的情況下，已有愈來愈多的犯罪集團利用虛擬通貨冷錢包地址接收從被害人取得之虛擬通貨，再將資金轉到中心化交易所的地址以兌換成法定貨幣，以製造金流斷點，造成後續調查取證、贓款沒收、返還、凍結之困難性。

(八)犯罪風險小，刑責低，但所得不法利益龐大

此類犯罪風險小且詐欺金額龐大，犯罪集團結合資通訊科技，仿照企業經營方式利用電信通訊、網際網路、銀行人頭帳戶、虛擬通貨，作為犯罪工具，輔以遠端跨境非接觸式的手法透過行動通訊、社群網站、通訊軟體、交友平臺或網路廣告等大量投放高額獲利廣告及訊息，藉以吸引不知情的被害人一步步掉入犯罪集團所設騙局，因電信網路假投資詐欺犯罪集團善於利用資(通)訊科技設備及方法以分散犯罪地點並隱身境外實行犯罪，在當地國刻意保護包庇下不易為警方查獲，即便遭到查獲詐欺犯罪行為，也常因該等犯罪行為涉及跨境執法合作，完整取證相當困難，在缺乏完備犯罪事證情況下，被判之刑責通常偏低，而此類犯罪財損從 2020 年的 10.27 億元，逐年成長到 2024 年 361.3 億元，5 年來增加 351.03 億元（+3418.01%），造成被害人極大財產損失，犯罪者在成本效益考量下，此類案件之常業犯和累犯再犯率偏高，難以嚇阻其犯行，此與犯罪學理性選擇觀點（Rational Choice Perspective）亦相契合。

三、 臺灣防制電信網路詐欺犯罪策略

21 世紀伊始電信網路詐欺犯罪逐漸成為臺灣最嚴重的治安問題之一，此一源於臺灣

的特有犯罪，最初係由人與人接觸式的金光黨詐欺模式開始，再轉變成利用郵件、手機簡訊以刮刮樂中獎模式行騙，隨著資通匯流技術蓬勃發展與金融自由化等因素，犯罪集團分子利用資通訊等技術，從盜（轉）接行動（固網）電話、網路電話、境外竄改來電顯示、駭客盜取個資、人頭金融帳戶，轉變為利用、社交（交友）軟體（Instagram、Tinder、派愛族等）、手機通訊軟體（Line、WeChat、telegram 等）等作為工具；對不特定被害人施以利益誘惑、虛構危險、虛假恐嚇，或利用被害人一時疏忽等心理因素，以假中獎、假冒公署（假冒警察、檢察官、法院等政府官員）、假簡訊催繳費用、假綁架（恐嚇）、猜猜我是誰、假網路拍賣、假援交、假交友（誘使被害人裸聊或參與博弈、投資）、假投資、解除 ATM 分期付款、混合型結合臨櫃匯款等作為犯罪手法，誘騙或盜取被害人資金匯（存）入其控制的銀行人頭帳戶之犯罪行為，且隨著資通訊科技的進步，犯罪手法的演變，治安機關查緝能力的強化，犯罪集團基於犯罪理性選擇，逐漸將實施電信網路詐欺犯罪的機房，從臺灣逐漸往世界各國蔓延（蘇信雄,2022) 參閱(表 2-8)。為因應詐欺犯罪情勢，臺灣政府自 2004 年開始制定各種防制策略以為因應，本研究綜合(蔡田木、陳永鎮,2006；楊士隆等人，2007；陳玉書、曾百川，2007；盧俊光，2007；林德華，2009、2010)；柯宏宜，2010；汪子錫、葉毓蘭，2013；孟維德，2016；曾雅芬，2016；詹志文、吳柏寬，2017；黃翠紋、蘇信雄，2020；田明府、黃麒然，2020；蘇信雄，2022)等研究及警政署與法務部的官方次級統計資料，將臺灣犯罪情勢與防制策略概分為以下幾個階段：

表 2-8 臺灣電信網路詐欺集團機房蔓延過程分析

階段	萌芽期（1998 年至 2005 年）	兩岸擴散期（2006 年至 2010 年）	往世界蔓延期（2011 年至今）
機房地點	中國大陸廈門市	臺灣、中國大陸	包含亞洲、非洲、中東、西亞、加勒比海、歐洲等 34 個國家地區
被害人國籍	臺灣	臺灣、中國大陸	臺灣、中國大陸、泰國、新加坡、愛沙尼亞、香港、泰國、法國、美國、加拿大、澳大利亞、日本、新加坡、馬來西亞
嫌犯國籍	臺灣	臺灣、中國大陸	臺灣、中國大陸、泰國、韓國、越南、柬埔寨、寮國、馬來西亞、菲律賓、緬甸、紐西蘭、多明尼加、波蘭、拉脫維亞
犯罪手法	刮刮樂、假中獎、假冒公署假綁架、假恐嚇、假貸款	假中獎、假冒公署、剝皮酒店、假綁架、假恐嚇、假貸款、假退稅、假援交、假交友、解除 ATM 分期付款	假中獎、假冒公署、假綁架（恐嚇）、猜猜我是誰、假網路拍賣、假援交、假交友、假投資、解除 ATM 分期付款、混合型結合臨櫃匯款

資料來源：引自蘇信雄(2022)。電信網路詐欺犯罪機房跨境蔓延之研析。中央警察大學學報，第 59 期，23-52。桃園市：中央警察大學，頁 46。

(一)1996-2008

1.犯罪情勢

回顧臺灣詐欺手法演進過程，在 1996 年以前，詐欺犯罪多以「金光黨」3 至 5 人小規模犯罪，利用人際接觸式及人性貪小便宜的弱點，以假鈔或假金飾的方法施行詐欺的傳統手法面對面接觸方式進行，由被害人當場交付財物，施詐範圍受地域限制。1996 年後，電信業務全面開放，網路普及化，犯罪模式逐漸轉變成犯罪人數動輒數十人以電信網路為主流的犯罪集團，並發展出以下犯罪手法：

(1) 1998 年 7 月 至 2002 年(刮刮樂)，犯罪集團先經由報章雜誌廣告，購買人頭帳戶及以人頭申設市內（固網）與行動電話門號，並盜（轉）接到位於中國大陸福建省廈門市詐欺機房， 再將每刮必中大獎的刮刮樂彩券大量郵寄給不特定的臺灣民眾，藉引誘民眾回電至機房查詢，犯罪者先要求被害人提供在金融帳戶，以便將彩金匯入，以取信被害人；續以預付稅金、參加會員或以港幣差額、轉投資、轉簽賭六合彩、轉簽賭賽馬、中獎抽成、電腦 IC 維修費、支付組頭工本費及補繳會員費等名目為由，要求使害人陸續匯款至詐欺集團的人頭帳戶，再由臺灣共犯提領被害人匯入金錢，周而復始，連環詐財。

(2) 2003 年(假中獎)，除刮刮樂詐欺犯罪手法方興未艾外，犯罪集團再增加新詐術，以偽稱某國際集團公司名義大量寄送刊登有人頭電話號碼之中獎通知單等詐欺文宣，藉以取信被害人回電；當被害人回電即被轉接至中國大陸廈門機房，嫌犯即偽稱被害人抽中鉅額獎金，或具一定價值之獎項，如被害人願領獎，要先繳納稅金，或捐出一定金額之愛心捐款，而引誘被害人把佯稱之稅金或愛心捐款款項以匯款或轉帳之方式，存入該集團人頭帳戶中。

(3) 2004 年(假冒公署、假綁架)，犯罪集團再增加新詐術，利用盜接市內（固網）電話轉接至隱身於中國大陸廈門地區機房人頭行動電話後，再由機房嫌犯以假冒警察、檢察官等公署人員，以電話聯繫被害人，告知涉及犯罪，必須監管其銀行存款，要求渠前往 ATM 匯款，再利用話術使被害人陷於錯誤而將帳戶金錢轉帳至該集團所使用之人頭帳戶內。或先行蒐購國內民眾電話等個資，再由機房人員撥打被害人電話，以「唱雙簧」方式，一方面佯裝被害人親人，在電話中哭喊遭綁架，另一方面同時充任債權人或地下錢莊業者，向被害人佯稱，須於一定時間內交付贖金始放人，否則將對其親人不利等語，同時該集團其他成員並事先以電話占線、或電話騷擾等方式，迫使被害人親人關機，趁被害人接獲哭救之電話，一時心慌又聯絡不上之際，唯恐親人發生不測而心生畏懼，並因一時不察信以為真而陷入錯誤之手段誘使被害人前往 ATM 匯款。

(4)2005 年(假貸款)，除前述刮刮樂、假中獎、假冒公署、假綁架犯罪手法外，再新增利用隱身於中國大陸廈門地區機房人員以人頭行動電話，撥打被害人電話，佯稱貸款須繳交手續費，誘使被害人 ATM 匯款至犯罪集團的人頭帳戶內。

(5) 2006 年(假退稅)，犯罪集團改變假冒公署詐欺手法，搭配當年戶政機關換發國民身份證時事，以戶政事務所名義通知受害者身分證遭冒用為主要詐欺手法，同年亦發現詐欺集團利用「車輛購置稅退稅」名義，由第一線成員依據中國大陸民眾車籍資料撥打給大陸地區民眾佯稱渠等有汽車購置稅可退，並要求被害人撥打電話給第二線成員進行身分核對及確認車籍可以退稅之款項金額，最後再由第二線成員要求被害人撥打電話給第三線成員以匯款轉帳交易進行詐欺，詐欺中國大陸地區民眾，自本年度開始，詐欺案件被害人由臺灣民眾擴及中國大陸人民。

(6)2007 年，犯罪手法仍然以假中獎、假冒公署為主要。

(7) 2008 年(假援交、假交友、假網購分期重複扣款)， 除假中獎外，詐欺集團又再次變化

犯罪手法，以假藉親友出事急需用錢，或改變假冒公署詐欺手法，以金融機構帳號遭盜領、帳號內不明資金進出、欠繳電話費、身分證號碼重複等誘騙民眾回電，再假冒警察、檢察官、法官等，向被害人騙稱其等涉嫌刑事案件，須將金錢匯入指定帳戶內監管。與此同時，本年度開始出現，犯罪集團透過網際網路，在網路聊天室，以「假援交、假交友，真詐財」之方式，對不特定人佯稱：若要援交、交友，須先匯款或繳交保證金等；亦發現犯罪集團事先大量收購民眾網購個資，再撥打電話向民眾偽稱前次購物交易因作業疏失，將交易款項金額改訂為分期重複扣款，再以篡改來電顯示銀行電話，並充當行員誘騙被害人至附近超商、銀行，按歹徒指示操作 ATM 匯款至犯罪集團的人頭帳戶內。

再根據臺灣司法機關判決書顯示，詐欺犯罪集團早於 1999 年 8 月即已蔓延至中國大陸廈門地區，而隨著詐欺犯罪往中國大陸地區蔓延，臺灣官方統計資料亦顯示，詐欺案件受理數自 2000 年起逐年增加，並於 2005 年達到 4 萬 3,023 件，財損金額於 2006 年達到 185.88 億餘元（如表 2-9）。

表 2-9 2000 年至 2024 年臺灣全般詐欺犯罪發生數及財損數

年度	發生數(件)	財損金額（億元）	年度	發生數(件)	財損金額（億元）
2000 年	7,755	23.82	2013 年	18,772	37.06
2001 年	16,082	39.40	2014 年	23,053	33.80
2002 年	26,397	58.93	2015 年	21,172	35.61
2003 年	37,191	80.59	2016 年	23,175	38.32
2004 年	40,001	94.61	2017 年	22,689	40.48
2005 年	43,023	113.79	2018 年	23,470	39.70
2006 年	41,352	185.88	2019 年	23,647	42.93
2007 年	40,348	150.92	2020 年	23,054	42.55
2008 年	40,963	117.48	2021 年	24,724	56.10
2009 年	38,802	102.71	2022 年	29,509	73.28
2010 年	28,494	61.29	2023 年	37,984	88.78
2011 年	23,612	48.80	2024 年	118,535	487.60
2012 年	20,421	42.61			

資料來源：整理自內政部警政署刑事警察局（2000－2024）。刑案紀錄表。

2.防制策略

為提升全民反詐欺意識，並向詐欺集團宣戰，政府結合各部會力量遏阻詐欺案件，於 2004 年 4 月 26 日在警政署民眾服務中心設立「0800-018110 反詐欺諮詢專線」，由刑事局內外勤及該服務中心混合編組,並由 4 人輪流接聽，提供服務。主要任務係建立民眾諮詢詐欺問題之管道。為方便控管勤務運作，使服務更加專業化、效率化，於同年 7 月 1 日將工作地點遷移至刑事警察局偵防中心，另為方便民眾有效牢記，並向交通部爭取「165」特碼。惟遷移後發現民眾需求及話務量激增，遂於隔年(2005 年)4 月 1 日將駐地遷移至保安警察第一總隊石牌營區現址，並設置專責人力與擴充設備，陸續由 4 人、8 人至 24 人，最後增派警力至 53 名，線路也增為 8 線，成為單一服務窗口。同時擴充軟、硬體設備及

增建執勤機席台，亦正式更名為「165 反詐欺諮詢專線」，其功能如下(內政部警政署，2024a)。
(1) 受理民眾電話諮詢、檢舉及報案。
(2) 協調電信監理單位，有效阻斷非法話務。
(3) 聯繫金融機構，阻斷非法資金流通。
(4) 與網路業者建立聯繫窗口，即時處置網路詐欺情資。
(5) 統計相關數據、彙整相關犯罪情資配合外勤隊偵查犯罪、執行停話與復話及人頭約制審核等相關作業。
(6) 整合詐欺情資建立「165 反詐欺系統平台」，將全國警察機關有關詐欺類案件資料統一彙整，以最完整、快速與便民之方式，有效協助民眾報案與相關資料彙整。

另外，該專線成立後積極整合各方資源，於 2006 年 11 月 1 日與「金融機構」建立聯防及通報機制即時攔阻被害款項。2008 年 11 月 31 日與「電信業者」成立聯合服務平臺有效阻斷非法話務。2011 年 7 月 8 日與「網路業者」建立情資交換平臺針對異常帳號機先停權。2018 年 6 月 6 日與「遊戲點數及虛擬貨幣業者」進行聯防即時凍結遭詐點數。

(二)2009-2021

1.犯罪情勢

詐欺犯罪集團洞悉兩岸警方並無共同打擊跨境詐欺犯罪合作機制。所以，早於 1999 年 8 月即將詐欺機房轉移至中國大陸廈門地區詐欺臺灣人民，臺灣詐欺集團慣於躲在大陸對岸遠端遙控在台下游共犯犯罪，利用切割犯罪組織結構躲避警方查緝，但自 2006 年開始，犯罪集團在追求更大犯罪利益的理性選擇下，轉向同時詐欺臺灣及中國大陸人民，從以往的「大陸犯罪，臺灣受害」翻轉為「臺灣犯罪，大陸受害」及「兩岸犯罪，兩岸受害」等方式，使得詐欺案件成為跨境犯罪問題。直至 2009 年 4 月 26 日海峽兩岸在中國大陸南京簽訂《海峽兩岸共同打擊犯罪及司法互助協議》(以下稱共打協議)，並於同年 6 月 25 日生效。協議生效後，臺灣警方透過兩岸合作共同打擊犯罪機制，與大陸警務單位積極展開合作打擊跨境電信網路詐欺犯罪，多次同步執行大型查緝詐欺專案並獲致具體成效，也迫使詐欺犯罪集團將詐欺機房遷移至亞太地區國家以躲避查緝。兩岸警務單位再聯合亞太地區第三地警務單位，於 2011 年至 2012 年間共同打擊兩岸跨第三地電信網路詐欺犯罪集團，同步執行多次大規模掃蕩行動。惟嗣後雙方合作模式逐漸產生變化，自 2016 年 4 月開始，中國大陸以各自遣返己方人民之作法已造成不利偵查工作及追贓返還等理由，陸續發生臺灣人在東南亞、西亞、非洲、歐洲等地因涉嫌電信網路詐欺犯罪遭帶往中國大陸追訴等情事(蘇信雄，2020)。另外自 2011 年起，其犯罪手法雖不脫假中獎、假冒公署(警察、檢察官、法院等政府官員)、假簡訊催繳費用、假綁架(恐嚇)、猜猜我是誰、假網路拍賣、假援交、假交友(誘使被害人裸聊或參與博弈、投資)、假投資、解除 ATM 分期付款、混合型結合臨櫃匯款等模式，但犯罪集團不斷翻新犯罪手法並配合時事施行詐欺，同時，利用新興科技工具，架設虛擬私人網路(Virtual Private Network，縮寫：VPN)，以隱匿真實 IP 位址，規避執法機關追查，及事先蒐集掌握準確的民眾個人真實隱私資訊，再「客製化」詐欺劇本實施詐欺，不但提高警方偵辦難度，亦增加民眾遭詐欺之風險。

2.防制策略

2009 年 4 月 26 日與中國大陸在南京簽訂共打協議，協議生效後，臺灣警方透過兩岸共同打擊跨境犯罪合作機制，與大陸警務單位展開合作，多次與東南亞區國家同步執行大規模查緝行動並獲致良好成效(林德華,2012)；惟隨著兩岸政治大環境的變化，自 2016 年 4 月起，陸續發生中國大陸警方將在世界各地查獲的臺灣藉嫌犯遣送至中國大陸追訴；因此，警政署刑事警察局於 2016 年 8 月 24 日成立「打擊詐欺犯罪中心」，據以統整情資、建立資料庫、調整策略，希望從提升查緝國內車手量能，以量多帶動質變，有效提升偵查能量，強化打擊詐欺臺灣人民的犯罪集團(李郁薇，2017)。而在法制面部分則多次修訂詐

欺犯罪相關規範，計有刑法與刑事訴訟法、洗錢防制法及組織犯罪防制條例等（詹志文、吳柏寬，2017）。

(三)2022-2025

1.犯罪情勢

2020 至 2022 年間適逢新冠肺炎（COVID-19）疫情爆發，除衝擊國內各項產業獲利，致營利銳減民眾急迫尋求投資機會，且疫情期間民眾大幅減少戶外活動，居家上網宅經濟普及，致增進犯嫌藉由網路交友遂行詐欺契機。疫情亦同時造成就業人口失業，急欲求職的青年，在人蛇集團高薪引誘的圈套下，遭誘騙或自願前往柬埔寨、緬甸等東南地區國家，從事詐欺犯罪，待抵達國外犯罪機房後，若有不從或詐欺業績不佳，動軋加以圈禁、毆打、凌虐，甚至殺害，淪落為人口販運被害人而求助無門。後經內政部警政署刑事警察局積極彙整滯留柬埔寨之 4 千餘國人名單，積極查訪後，約有 120 名國人失聯（姚岳宏，2022），顯現出詐欺集團與人口販賣犯罪集團勾聯嚴重。然而，防制跨境犯罪需涉及臺灣與他國政治、法律、外交等協商事項，卻因臺灣國際處境艱困，造成查緝與營救之困境，加以當地政府官員曲意包庇，使得部分東南地區國家成為犯罪集團之溫床。另依據行政院洗錢防制辦公室 2021 年發表報告指出，每年詐欺犯罪平均所得高達約 700 餘億元，而近年詐欺犯罪走向又以投資、網路及電信詐欺類型最為囂張，不法金額龐大(行政院洗錢防制辦公室，2021)。觀察近 5 年（2020 年至 2024 年)全般詐欺平均發生數約 46,761 件（參考表 2-9），平均財損數約新臺幣 149.66 億元，其中 2024 年發生 118,535 件、財損 487.6 億元，詐欺案件發生數及財損數居高不下；2024 年電信網路詐欺發生數前 3 名依序為投資詐欺 44,124 件、假網路拍賣(購物)(含一般購物詐欺)27,744 件、解除分期付款詐欺(ATM)9,775 件；其中相較 2023 年發生數增加者以「投資詐欺」增加 276.4%最多。2024 年檢警雖攔阻與圈存詐欺犯罪金額達到 129.89 億元，較 2023 年增加 44.9%；偵破詐欺集團 2,815 件，相較 2023 年增加 76.37%；查扣不法利得 144.5 億元，相較 2023 年增加 268.4%(內政部警政署，2025）。惟 2024 年仍有詐欺財損金額 487.6 億，其金額已經來到歷年新高。雖然在檢、警相關單位努力查扣下，查扣金額逐年上升，攔阻成效大於被詐欺成效，然而與犯罪者不法所得相較卻不成比例，致民眾難以感受政府查緝犯罪力道。再進一步分析電信網路詐欺犯罪集團犯罪手法（如圖 2-13）(內政部警政署，2022a)如下

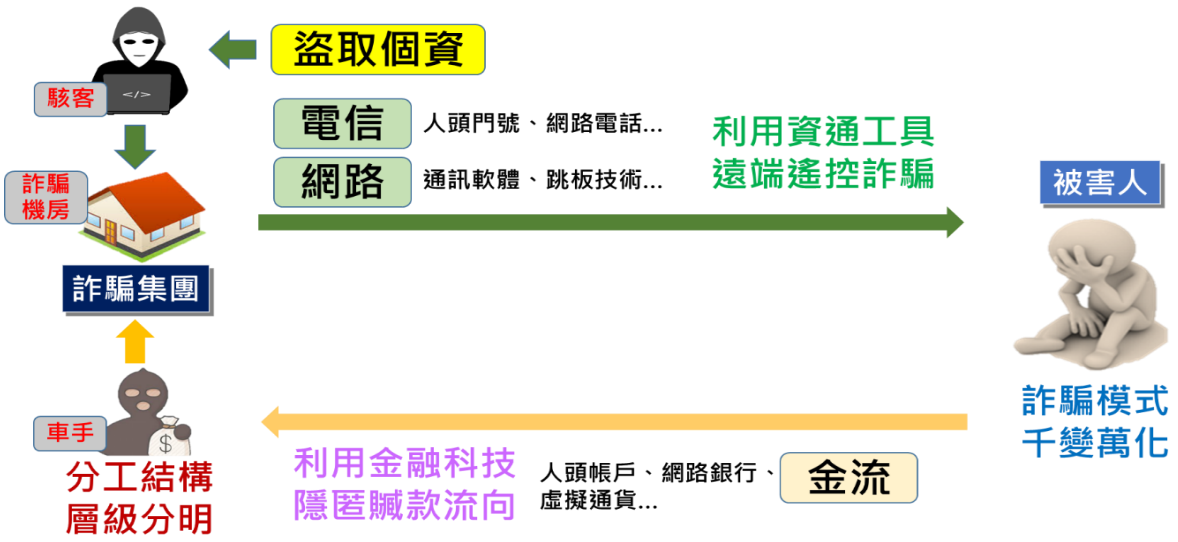


圖 2-13 臺灣電信網路詐欺犯罪流程圖

資料來源：內政部警政署(2022a)。內政部警政署署務會報。

(1)駭客藉由各式管道竊取民眾個資後，轉賣給詐欺集團使用。
(2)詐欺集團詐欺方式從行動電話轉為透過竄改來話、DMT、VoWiFi 或 VoIP 發話；網路則由線上聊天，轉為社群網站、通訊軟體傳遞訊息，在遠端利用前揭資通訊工具聯繫被害人，藉以隱匿蹤跡。
(3)詐欺手法日新月異，多數民眾防詐意識不足，容易輕信詐欺集團之話術進而受騙匯款。
(4)詐欺集團收取贓款後，由傳統之實體帳戶，轉為虛擬帳號、第三方支付或虛擬貨幣進行洗錢，再由車手提領兌現，隱匿贓款流向。

2.防制策略

臺灣政府為遏止電信網路詐欺犯罪持續高發，行政院於 2022 年 7 月 15 日訂頒打詐綱領，結合法務部、內政部、國家通訊傳播委員會、金融監督管理委員會等機關成立『打詐國家隊』，以「識詐、堵詐、阻詐、懲詐」4 大面向（如圖 2-14）破解詐欺手法，建立國內「防詐欺、毀工具、擋金流、清集團」終極目標。

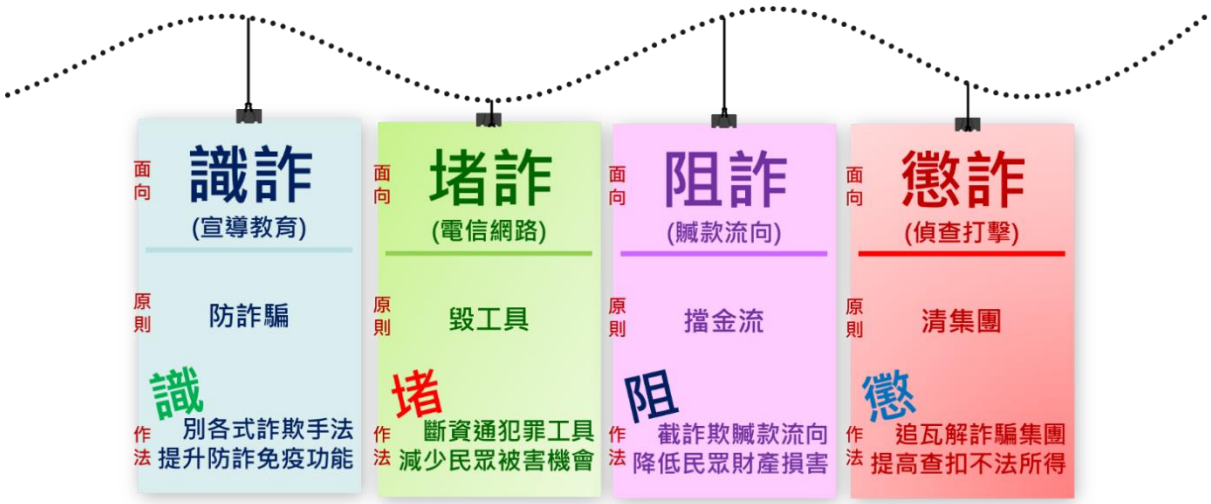


圖 2-14 臺灣防制詐欺犯罪工作四大面向圖

資料來源：行政院(2023)。新世代打擊詐欺策略行動綱領 1.5 版，頁 12。取自：https://www.moj.gov.tw/media/26683/15-%E4%BF%AE.pdf?mediaDL=true，最後瀏覽日期：2025 年 6 月 19 日。

統計 2022 年 6 月至 2023 年 1 月，在識詐面，反詐宣導資訊觸及 2084.9 萬人次、發送防詐簡訊 9,792.2 萬則；在堵詐面，攔阻詐欺簡訊 3,819.4 萬則、人頭門號停斷話 7,479 門在阻詐面，全體本國銀行設立「疑涉詐欺境外金融帳戶預警機制」及將銀行公會彙整之共通性異常交易態樣納入內部預警指標；在懲詐面，查獲電信網路詐欺集團計 1143 件、1 萬 433 人，攔阻被害款項新臺幣下同 37.4 億元(行政院，2024)。惟實施後詐欺案件發生數及財損金額仍持續高發，政府再於 2023 年 6 月 9 日訂頒打詐綱領 1.5(行政院，2023)，新增減少接觸(透過技術跟法律面阻斷措施，減少民眾接觸機會)，減少誤信(透過各種警訊及提醒，避免民眾誤信詐欺話術)，減少損害(透過銀行警示及臨櫃關懷，降低民眾財產損失)之「3 減」策略（如圖 2-15）

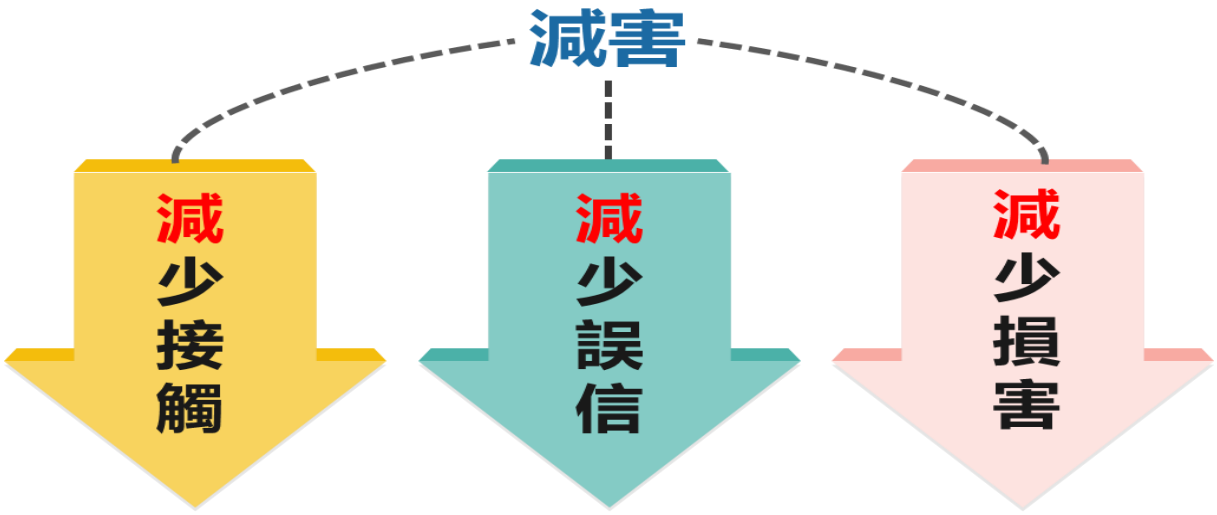


圖 2-15 臺灣防制詐欺犯罪工作 3 減策略圖

資料來源：行政院(2023)。新世代打擊詐欺策略行動綱領 1.5 版，頁 11。取自：https://www.moj.gov.tw/media/26683/15-%E4%BF%AE.pdf?mediaDL=true，最後瀏覽日期：2025 年 6 月 19 日。

及特設行政院打擊詐欺辦公室；臺灣高等檢察署成立查緝詐欺及資通犯罪中心、法務部調查局成立北、中、南部、跨境詐欺防制中心，另 6 都直轄市調查處成立打詐專案組；警政署成立專案指揮暨資料研析合作平臺(北、中、南工作站)。另中央結合各縣市政府打詐地方隊及民間團體力量，公私協力，以全力遏阻犯罪，將打詐效能極大化(如圖 2-16)。

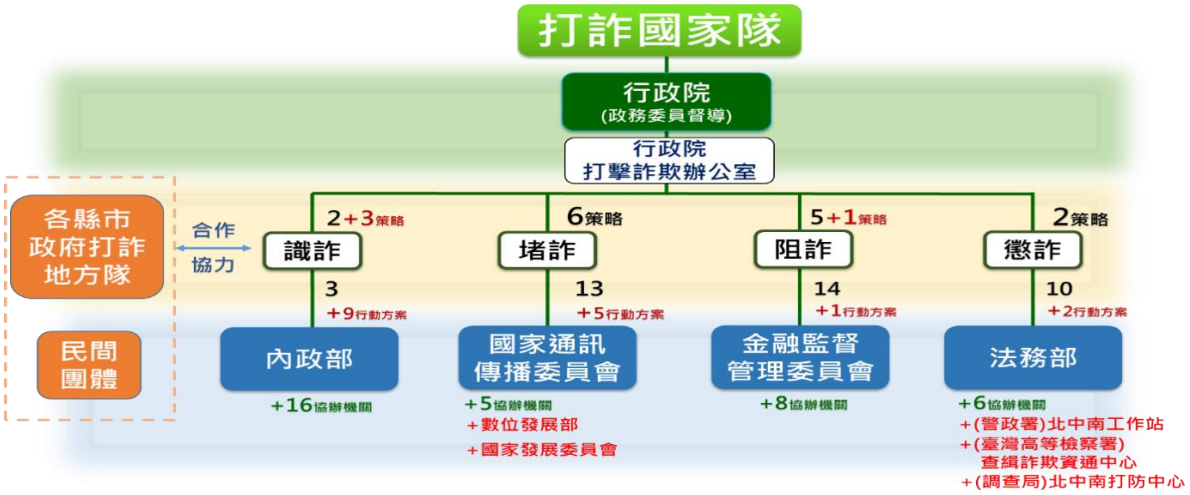


圖 2-16 臺灣政府防制詐欺組織架構

資料來源：行政院(2023)。新世代打擊詐欺策略行動綱領 1.5 版，頁 15。取自：https://www.moj.gov.tw/media/26683/15-%E4%BF%AE.pdf?mediaDL=true，最後瀏覽日期：2025 年 6 月 19 日。

另本次共研訂 4 項策略及 17 項行動方案，作為工作主軸與執行目標(如圖 2-17）



圖 2-17 臺灣政府防制詐欺四大面向策略

資料來源：行政院(2023)。新世代打擊詐欺策略行動綱領 1.5 版，頁 16。取自：https://www.moj.gov.tw/media/26683/15-%E4%BF%AE.pdf?mediaDL=true，最後瀏覽日期：2025 年 6 月 19 日。

同時由國家發展委員會會同行政院打擊詐欺辦公室(督考機關/單位)，分年度依各面向之分項指標進行管考(如圖 2-18）



圖 2-18 臺灣防制詐欺四大面向分項指標

資料來源：行政院(2023)。新世代打擊詐欺策略行動綱領 1.5 版，頁 16。取自：https://www.moj.gov.tw/media/26683/15-%E4%BF%AE.pdf?mediaDL=true，最後瀏覽日期：2025 年 6 月 19 日。

再依業務分工由各面向統籌機關督促項下各行動策略之主、協辦機關落實推動辦理。並增修「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」等「打詐五法」。同時編列相關預算，俾賡續透過「宣導教育」、「犯罪通路」、「贓款流向」及「偵查打擊」等四大面向，整合各部會力量，希冀透過公私部門協力，從法律面和技術面減少通信流及加重詐欺刑責，發揮「前端阻卻」及「後端查緝」之效用，以減少受害者，掃除詐欺集團，達到有效抑制詐欺犯罪，保障人民財產安全的目標 (行政院，2022；內政部警政署，2022a;b)。

但在相關單位採行強化防制措施後，詐欺集團犯罪模式與手法亦隨之改變，致產生法令不足情形。政府為落實打詐綱領，嚴懲詐欺犯罪，認有賦予執法機關使用科技偵查手段法律基礎之必要，且須完備相關法制面，以落實源頭管理，俾利精準打擊詐欺犯罪，續由行政院於 2024 年 5 月於院會通過「打詐新四法」，經立法院陸續於 2024 年 7 月 12 日、16 日三讀通過《詐欺危害防制條例》、《通訊保障及監察法》、《刑事訴訟法特殊強制處分專章》及《洗錢防制法》等修正草案。(法務部,2024)「打詐專法」採取「就源」及「溯源」此一「雙源齊清」方向，以「強化防詐作為、打擊詐欺集團、保護犯罪被害」三大重點為主軸，從金融(含虛擬資產)、電信及數位經濟相關產業(含網路廣告平臺、第三方支付服務、網路連線遊戲及電商業者)等三面向著手。整合行政機關與民間企業量能，共同防制詐欺犯罪；在刑事司法方面，加重犯嫌刑責與假釋門檻，也制定多項詐欺被害人保護措施，要減少詐欺犯罪對民眾造成之危害(如圖 2-19）。

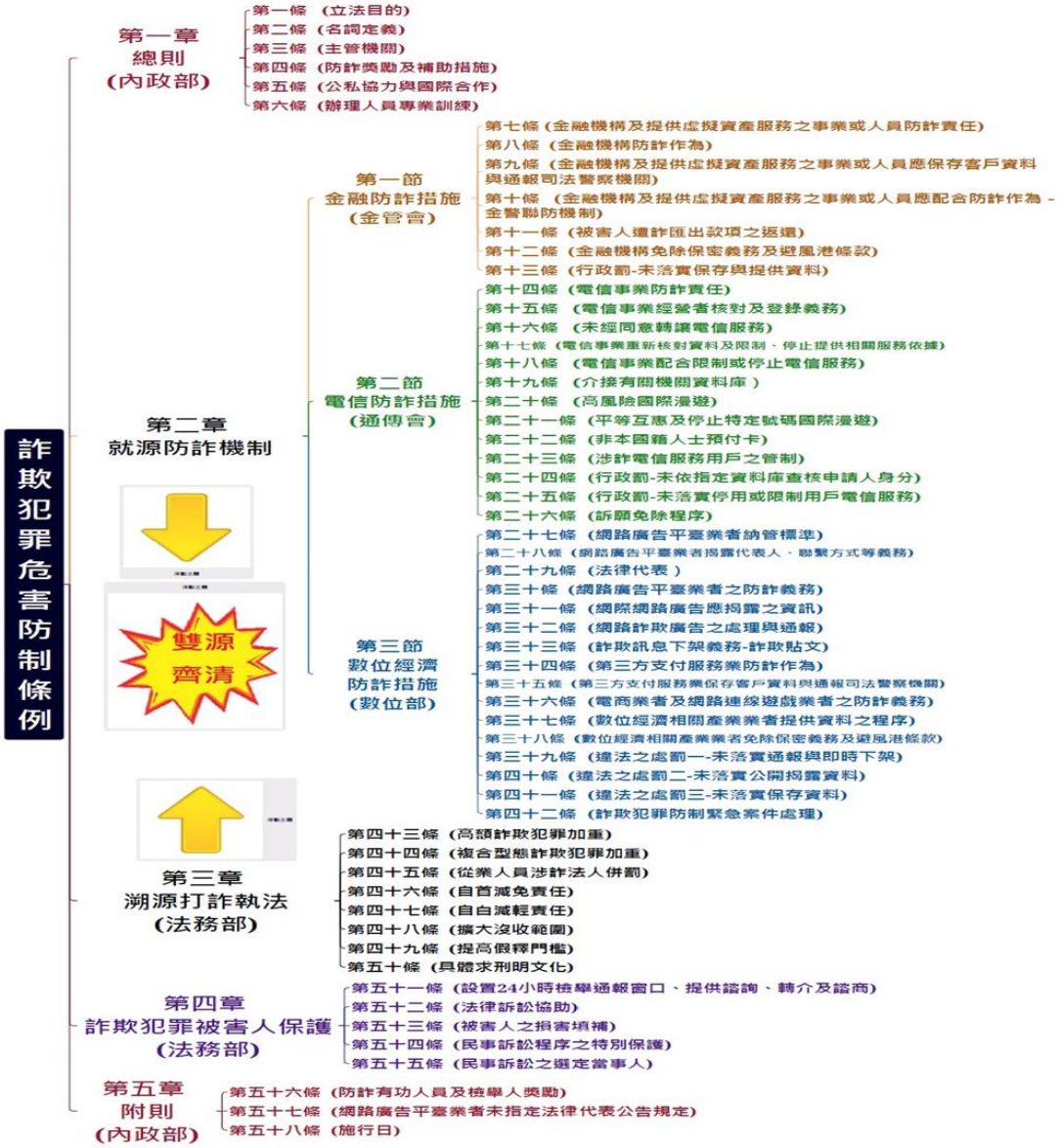


圖 2-19 臺灣詐欺犯罪危害防制條例架構圖

資料來源：黃國師（2024）。打詐專法立法分析。警政與警察法相關圓桌論壇(第 68 場)，中華警政研究學會。頁 14。取自：http://www.acpr.org.tw/PDF/Panel_20240809_the%20legal%20evaluation%20of%20new%20anti-fraud%20relative%20acts.pdf，最後瀏覽日期：2025 年 6 月 19 日。

另外配套三法賦予執法機關透過正當程序，運用科技偵查工具加強執法，達成臺灣強力痛擊詐欺的目標，以及將新興洗錢犯罪手法入刑化，以符合國際規範要求，強化偵查辦案時的法源依據，期能在第一時點破獲，並瓦解詐欺犯罪集團。

自打詐綱領 1.5 執行期程屆滿後，為因應詐欺犯罪態樣不斷演變及手法日益科技化之挑戰，行政院再於 2025 年 2 月 18 日核定並追溯自同年 1 月起實施打詐綱領 2.0，作為全國打詐政策推動之最新依據。該綱領除承襲原有識詐、堵詐、阻詐、懲詐四大面向外，新增「防詐（數位經濟面）」作為第五面向，體現數位時代下防制詐欺之政策轉型。整體綱領依據「一宗旨、三目標、五面向、七產業」為核心架構(如圖 2-20)，宗旨為「抑制詐欺犯罪」，三大目標為「強化防詐意識」、「減少詐欺發生件數」及「降低民眾財產損失」，五面向則分別為識詐（教育宣導）、堵詐（電信服務）、防詐（數位經濟）、阻詐（金流攔阻）與懲詐（偵查查緝）；另納入七項關鍵防詐產業，涵蓋金融機構、虛擬資產服務提供者、電信事業、網路廣告平臺、第三方支付服務、電商及網路連線遊戲業者，推動跨領域公私協力機制。政策策略層面方面，打詐綱領 2.0 不僅調整「堵詐」面向定義為「電信服務」，亦新增「防詐」面向，由數位發展部（下稱數發部）統籌，專責數位經濟領域之防詐治理與監理事務；法制面上，則結合 2024 年通過之《詐欺犯罪危害防制條例》(即所謂「打詐專法」) 與《刑事訴訟法》(特殊強制處分章)、《洗錢防制法》及《通訊保障及監察法》等四部關鍵法規（合稱「打詐新四法」），強化查緝手段與源頭管理之法源基礎。



圖 2-20 臺灣打詐綱領 2.0 核心概念

資料來源：行政院(2024)。新世代打擊詐欺策略行動綱領 2.0 版。取自：https://www.ey.gov.tw/Page/9277F759E41CCD91/526a9b40-50cb-49e7-83a9-e8c49a1475ed，最後瀏覽日期：2025 年 6 月 20 日。

組織面方面，原行政院設置之「打擊詐欺辦公室」轉型為「打詐指揮中心」(如圖 2-21)，由內政部次長兼任指揮官，並增設執行秘書以強化跨部會整合協調效能，形成具備政策規劃、通報調度與社會溝通功能之常設執行平台。從功能劃分來看，各面向亦有明確權責分工：其中「識詐」由內政部統籌，透過分齡、分層與分眾之宣導教育策略，提升民眾辨識詐欺能力並厚植青少年法治素養；「堵詐」由國家通訊傳播委員會負責，聚焦電信

門號實名制、阻斷簡訊詐欺等電信基礎設施管理；「防詐」由數發部主導，針對網路廣告、第三方支付及遊戲點數洗錢等數位經濟環節進行監管與淨化；「阻詐」由金融監督管理委員會統籌，重點落在攔阻非法資金流向與監管虛擬資產服務提供者（VASP）；「懲詐」則由法務部統整檢警調查打量能，強化跨境合作與贓款追查，並提供被害補償與罪贓返還制度。面對假投資、跨境詐欺與虛擬金流等新型詐欺威脅時之前瞻管理視野與制度規劃能力。



圖 2-21 臺灣打詐綱領 2.0 組織架構

資料來源：行政院(2024)。新世代打擊詐欺策略行動綱領 2.0 版。取自：https://www.ey.gov.tw/Page/9277F759E41CCD91/526a9b40-50cb-49e7-83a9-e8c49a1475ed，最後瀏覽日期：2025 年 6 月 20 日。

此外，該綱領延續先前政策慣例，動員行政院各部會（含內政、數位、金管、法務、通傳等二十餘單位）共同推動相關政策機制，並透過法制、科技與組織三者並進，實現「上游防制、中游攔阻、下游偵查」之全方位防詐政策鏈結。整體而言，打詐綱領 2.0 不僅整合前期政策經驗與新興科技工具，亦回應當前詐欺犯罪日趨複雜之防制需求。

四、臺灣防制電信網路詐欺犯罪成效

本研究綜整官方文件、統計數據與學術研究成果，從打詐五面向系統性分析臺灣防制電信網路詐欺犯罪之執行成效，並進一步探討其在假投資詐欺防制上的具體貢獻與制度困境。在打詐綱領 2.0 執行 7 個月後，行政院於 2025 年 8 月 15 日，向立法院第 11 屆第 3 會期，提出「新世代打擊詐欺策略行動綱領 2.0 執行成效專案報告」（行政院，2025），該報告指示，根據 165 打詐儀錶板統計，詐欺案件受理數自 2024 年 8 月（19,590 件）下降至 2025 年 7 月（15,177 件）下降 22.5%，同期財損金額由 131 億新臺幣下降至 81 億元，降幅達 37.7%(如表 2-10)，其中假投資及假交友投資詐欺下降幅度最為顯著，顯示整體策略已初步展現抑制成效。然而，若進一步分析犯罪結構，可發現「假投資」與「假交友投資」詐欺仍占整體財損比重高達 80%，其中假投資詐欺單一類型即占 64%，顯示雖然案件總量下降，但高風險詐術仍具強韌生命力，對執法與政策形成嚴峻挑戰。

表 2-10 2024 年 8 月至 2025 年 7 月臺灣全般詐欺犯罪發生數及財損數

年月	發生數(件)	財損金額（萬元）	年月	發生數(件)	財損金額（萬元）
2024 年 8 月	19,590	1,311,047	2025 年 2 月	9,821	572,477
2024 年 9 月	16,950	1,142,029	2025 年 3 月	15,491	671,492
2024 年 10 月	17,008	1,143,078	2025 年 4 月	14,771	727,632
2024 年 11 月	17,147	1,152,601	2025 年 5 月	14,818	825,535
2024 年 12 月	16,703	1,182,695	2025 年 6 月	15,259	844,371
2025 年 1 月	12,248	932,509	2025 年 7 月	15,177	817,261

資料來源：整理自內政部警政署(2025c)。165 打詐儀錶板。取自 https://165dashboard.tw/，最後瀏覽日期：2025 年 8 月 1 日。

(一)識詐面向：防詐意識的擴散與效果侷限

「識詐」為前端預防之核心策略，強調提升民眾對詐欺手法的辨識能力。政府透過多元管道進行分齡、分眾宣導，包括社群媒體、廣播、校園教育及超商端口等，2025 年上半年觸及人次達 9,872 萬人次。同時，金融機構行員與超商店員亦被納入識詐體系，強化其主動攔阻與通報能力，成功攔阻金額達 83 億餘元。

(二) 堵詐面向：電信攔阻技術與跨境限制

「堵詐」策略重點在於攔阻詐欺訊息與來電，以削減受害接觸面。2025 年上半年，政府透過 AI 技術攔阻境外詐欺來話 247 萬通、詐欺簡訊 149 萬則，並拒發 2,403 萬則可疑商業簡訊，展現出數位管理的即時性。

(三) 防詐面向：數位平臺管理與 AI 監理挑戰

防詐策略係打詐綱領 2.0 新增的重要面向，由數位發展部統籌，聚焦於數位經濟產業源頭防制。政府於 2025 年 1 至 7 月主動蒐報 15 萬餘件可疑詐欺訊息，攔阻涉詐網域 5 萬餘件，下架廣告 9 萬餘則，並對國際平臺業者開罰以督促自律。

(四) 阻詐面向：金融預警與金流追蹤成效

阻詐策略聚焦金流防堵與帳戶監理，全國銀行建置「疑涉詐欺金融帳戶預警機制」，可即時偵測異常交易並通報警政單位。另設置「信用卡詐欺防制通報平臺」與「爭議包裹協處機制」，退還金額逾 1 億 6 千萬元。

(五)懲詐面向：查緝量能與跨境合作

懲詐面向整合檢警調能量，自 2025 年 1 至 7 月共查獲 2,025 詐欺集團、逮捕 1 萬 5,912 人次，查扣不法所得 40 億元，並推動 1,271 件跨境合作。

(六) 假投資詐欺的成效與制度瓶頸

假投資詐欺受理案件自 2024 年 8 月每日平均 175.8 件降至 2025 年 7 月 86.7 件，減少 51%；平均每日財損由 2 億 8,737 萬元降至 1 億 3,833 萬元，減幅達 52%，顯示短期抑制效果。

(七)綜合評析：從政策整合走向防制韌性

整體而言，打詐綱領 2.0 展現制度性進步，透過 AI 科技、跨部會合作與法制強化，已達量的下降之成果。

五、臺灣防制電信網路詐欺犯罪困境分析

詐欺集團透過駭客竊取民眾個資，在遠端利用資通訊工具(如竄改來話、通訊軟體)聯繫被害人，隱匿蹤跡，詐欺手法不斷推陳出新，多數民眾防詐意識不足，很容易輕信詐欺集團之話術進而匯款；詐欺集團收取贓款後，利用金融科技(如人頭帳戶、虛擬通貨)便利性迅速轉帳，隱匿贓款流向，而造成以下的防制困境(警政署，2022a,b)

(一)犯罪宣導困境

詐欺手法日新月異，犯罪集團針對人性心理弱點，利用各種詐欺話術及科技工具，編造各種以假亂真的情境，民眾識別和預防不易，只要稍有不慎，容易誤入詐欺集團所設圈套。另外各類防詐資訊雖經各機關長年大量宣導及媒體反覆報導，許多民眾產生麻木及過度自信心態，甚而對宣導資訊視而不見，亦未有轉告、提醒親友的警覺性，導致遭詐風險提高(警政署刑事警察局，2024)部分民眾甚至心存僥倖或利令智昏，夢想一夕致富，使得詐欺集團有機可乘，被害人深陷詐欺情境仍不自知，造成詐欺發生數及財損一再創新高。

(二)資安管理困境

隨著電信網際網路科技迅速發展，犯嫌為躲避警方查緝，利用電信金融法規及資安防護嚴謹度未完善之漏洞，在遠端藉由加密通訊 APP、VPN 跳板及跨境寬頻網路(xDSL、Cable、FTTB 等)、新型態電信服務 (4G、5G、DMT、VoWiFi)或 Skype、ISR 等國際話務服務上網連結網路電話(VoIP)，配合群呼系統(I.V.R)發話給民眾，以隱匿真實身分同時竄改境外來電顯示，輔以駭客盜取的民眾個資及非法取得之人頭金融帳戶，再透過社交（交友）軟體（Instagram、Tinder、派愛族等）、手機通訊軟體（Line、WeChat、Telegram 等）等遠程非接觸式工具，與民眾接觸，詐欺財物，造成法人員查緝困境。

(三)金流追查困境

犯罪集團運用金融交易數位化及支付工具多樣、迅速、便利的特性，網銀遠端身分認證鬆散及國際間尚未形成有系統的防制洗錢合作機制之漏洞，使用人頭電話、人頭帳戶以設立偵查斷點，民眾對於有償或無償提供帳戶予他人使用，未具可能淪為詐欺幫助犯意識，而詐欺集團多利用「代辦貸款」等話術取得人頭帳戶進行詐欺，依刑事警察局之分析 2021 至 2022 年間警示帳戶中虛擬帳號遭利用之公司行號，其中約 40%集中於第三方支付或電商業者，顯見犯嫌多利用審核較寬鬆之第三方支付代收款虛擬帳號，作為進行收取贓款之主要帳戶工具，後續則結合(高價值)虛擬通貨[6] (諸如比特幣、泰達幣)匯至電子錢包隱匿贓款資金流向，因無對應之中央目的事業主管機關，導致警方調閱資料不易，殊難追查。另詐欺集團常用之洗錢工具已結合虛擬通貨，藉由其具流通性、且可隨時兌現之特性，要求被害人透過虛擬通貨交易所、BTM[7] 或個人幣商購買虛擬通貨，續匯入犯嫌指定之人頭電子錢包多層移轉，利用去中心化特性隱匿贓款流向，再透過網路進行跨境洗錢並由車手集團取款(警政署刑事警察局，2024)，藉以隱匿贓款流向並製造金流斷點，造成後續調查取證、贓款沒收、返還、凍結之困境。

(四)跨境查緝困境

詐欺集團採行層級管理、分工細密，組織結構一般劃分為金主及幕後首腦、核心管理幹部、話務機房、系統商、轉帳水房、車手集團、組織結構完整，且因加入管理要素，使

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

7.BTM：Bitcoin Teller Machine，比特幣自動櫃員機，透過與加密資產錢包之連結，進行法定通貨與加密資產之兌換服務。

該犯罪組織更具效率。各節點間彼此均透過通訊軟體代號方式聯繫，亟難掌握成員間真實身分，易致警方查緝溯源中遭遇層層斷點，鮮少查獲幕後首腦偵破整團犯罪組織。(警政署刑事警察局，2024)在資通訊、金流工具沒有落實管制情況下，利用資(通)訊科技設備及方法以分散犯罪地點並隱身境外實行犯罪，並在當地國刻意保護包庇下使得警方查緝無門，即便當地國意配合查緝，亦因雙方法制與司法管轄主張不一，且偵查技術及相關設備存在落差，導致調查取證與案件聯結有相當困難度，在缺乏完備犯罪事證情況下，難以溯源緝獲幕後主嫌，僅能查獲詐欺集團的基層角色，且被判之刑責通常偏低，使得犯罪集團有恃無恐，犯罪氣陷日益囂張，造成偵查打擊之困境。

六、小結

近 20 餘年來電信網路詐欺犯罪一直是臺灣最嚴重的治安問題之一，犯罪集團利用民眾恐懼、貪財、貪色等心理弱點，使用各式新型的資通訊工具，採取利益誘惑、虛構危險、虛假恐嚇等犯罪手法，誘騙或盜取被害人資金匯（存）入其控制的銀行人頭帳戶之犯罪行為，近年來隨著資通訊科技進步，犯罪手法的演變，治安機關查緝能力的強化，犯罪集團基於犯罪理性選擇，逐漸將實施電信網路詐欺犯罪的機房，從臺灣逐漸往世界各國蔓延。

為因應詐欺犯罪情勢，臺灣政府自 2004 年即開始持續建置更新「165 反詐欺諮詢專線」，目前派駐警力約 53 名，線路 8 線，負責受理民眾電話諮詢、檢舉及報案；協調電信監理單位，有效阻斷非法話務；聯繫金融機構，阻斷非法資金流通；與網路業者建立聯繫窗口，即時處置網路詐欺情資；統計相關數據、彙整相關犯罪情資配合外勤隊偵查犯罪、執行停話與復話及人頭約制審核等相關作業；整合詐欺情資建立「165 反詐欺系統平台」，將全國警察機關有關詐欺類案件資料統一彙整，以最完整、快速與便民之方式，有效協助民眾報案與相關資料彙整。並於 2006 年與「金融機構」建立聯防及通報機制即時攔阻被害款項。2008 年與「電信業者」成立聯合服務平臺有效阻斷非法話務。2011 年與「網路業者」建立情資交換平臺針對異常帳號機先停權。2018 年與「遊戲點數及虛擬貨幣業者」進行聯防即時凍結遭詐點數。2009 年與中國大陸簽訂共打協議生效後，兩岸警方多次與東南亞區國家同步執行大規模查緝行動並獲致良好成效，惟隨著兩岸政治大環境的變化，自 2016 年 4 月起，陸續發生中國大陸警方將在世界各地查獲的臺灣藉嫌犯遣送至中國大陸追訴，間接造成近年來兩岸合作共同打擊跨境電信網路詐欺案件持續低盪。警政署刑事警察局於 2016 年成立「打擊詐欺犯罪中心」，據以統整情資、建立資料庫、調整策略，希望從提升查緝國內車手量能，以量多帶動質變，有效提升偵查能量，強化打擊詐欺臺灣人民的犯罪集團。同時多次修訂刑法與刑事訴訟法、洗錢防制法及組織犯罪防制條例等與詐欺犯罪相關規範。

為遏止電信網路詐欺犯罪持續高發，行政院於 2022 年 7 月 15 日訂頒打詐綱領，結合法務部、內政部、國家通訊傳播委員會、金融監督管理委員會等機關成立『打詐國家隊』，以「識詐、堵詐、阻詐、懲詐」4 大面向破解詐欺手法，建立國內「防詐欺、毀工具、擋金流、清集團」終極目標。惟實施後詐欺案件發生數及財損金額仍持續高發，政府再於 2023 年 6 月 9 日訂頒打詐綱領 1.5，新增減少接觸(透過技術跟法律面阻斷措施，減少民眾接觸機會)，減少誤信(透過各種警訊及提醒，避免民眾誤信詐欺話術)，減少損害(透過銀行警示及臨櫃關懷，降低民眾財產損失)之「3 減」策略及特設行政院打擊詐欺辦公室；臺灣高等檢察署成立查緝詐欺及資通犯罪中心、法務部調查局成立北部、中部、南部、跨境詐欺防制中心，另 6 都直轄市調查處機動工作站成立打詐專案組；警政署成立專案指揮暨資料研析合作平臺(北、中、南工作站)。另中央結合各縣市政府打詐地方隊及民間團體力量，公私協力，以全力遏阻詐欺犯罪，將打詐效能極大化。並由國家發展委員會會

同行政院打擊詐欺辦公室(督考機關/單位)，分年度依各面向之分項指標進行管考，再依業務分工由各面向統籌機關督促項下各行動策略之主、協辦機關落實推動辦理。並增修《刑法》、《人口販運防制法》、《個人資料保護法》、《洗錢防制法》、《證券投資信託及顧問法》等「打詐五法」。同時編列相關預算，俾賡續透過「宣導教育」、「犯罪通路」、「贓款流向」及「偵查打擊」等四大面向，整合各部會力量，希冀透過公私部門協力，從法律面和技術面減少通信流及加重詐欺刑責，發揮「前端阻卻」及「後端查緝」之效用，以減少受害者，掃除詐欺集團，達到有效抑制詐欺犯罪，保障人民財產安全的目標。

但在相關單位採行強化防制措施後，詐欺集團犯罪模式與手法亦隨之改變，致產生法令不足情形。政府為落實打詐綱領，嚴懲詐欺犯罪，認有賦予執法機關使用科技偵查手段法律基礎之必要，且須完備相關法制面，以落實源頭管理，俾利精準打擊詐欺犯罪。經立法院陸續於 2024 年 7 月 12 日及 7 月 16 日三讀通過《詐防條例》、《通訊保障及監察法》修正草案、《刑事訴訟法》增訂特殊強制處分專章，以及《洗錢防制法》修正草案。其中，「打詐專法」採取「就源」及「溯源」此一「雙源齊清」方向，以「強化防詐作為、打擊詐欺集團、保護犯罪被害」三大重點為主軸，從金融(含虛擬資產)、電信及數位經濟相關產業(含網路廣告平臺、第三方支付服務、網路連線遊戲及電商業者)等三面向著手。

為因應詐欺犯罪日趨科技化與跨境化之挑戰，行政院於 2025 年 2 月核定打詐綱領 2.0（溯自 2025 年 1 月起實施），作為全國打詐政策推動之核心依據。該綱領在延續 1.5 版「識詐、堵詐、阻詐與懲詐」四大面向的基礎上，新增「防詐（數位經濟面）」政策主軸，並由數位發展部統籌推動，以回應數位經濟快速發展所衍生之新興詐欺風險。

在策略架構上，綱領以「一宗旨、三目標、五面向、七產業」為整體設計主軸，強調跨部會合作與公私協力，涵蓋金融、電信、第三方支付、網路廣告、電子商務、虛擬資產及線上遊戲平台等關鍵產業，透過明確分工與責任配置，提升整體打詐政策之執行效能。法制層面則配合整合《詐欺犯罪危害防制條例》等「打詐新四法」，逐步建構兼顧防制與查緝之法源基礎。

在組織運作方面，原「打擊詐欺辦公室」轉型為「打詐指揮中心」，並由內政部次長擔任指揮官，藉以強化跨部會橫向協調與政策資源整合。各政策面向分別由內政部、國家通訊傳播委員會、數位發展部、金融監督管理委員會及法務部負責主政，依序就識詐宣導、電信管理、數位平台監理、金流攔阻與偵查追訴等任務分工執行，展現政府建構全方位詐欺防制體系之政策藍圖。

第三節　主要國家電信網路詐欺犯罪現況及防制策略

電信網路詐欺集團已走向專業化，利用各種詐欺手法，無孔不入地影響民眾生活，並造成民眾財產鉅大損失，根據非營利組織全球反詐欺聯盟（Global Anti-Scam Alliance-Gasa）和資料服務供應商 ScamAdviser 發表 2023 年全球詐欺調查報告，該聯合研究係透過直接訪問來自 43 國共 49,459 名受訪者的抽樣調查，該研究報告揭露 2022 年 8 月到 2023 年 8 月間，全球有高達 25.5%人口被詐欺，損失總金額大約 1.02 兆美元，比 2021 年損失金額 553 億美元和 2020 年 478 億美元高出許多，詐欺犯罪已成為全世界關注議題。以受害者平均損失而言，新加坡每位受害者平均損失 4,031 美元（約 13.15 萬元）排名第一，瑞士損失 3,767 美元排名第二，奧地利損失 3,484 美元排名第三，而臺灣每位受害者平均財損則落在 1200 美元左右，排名全球第 23 名，顯示詐欺犯罪不僅威脅著個人財產安全，也嚴重損害國際金融秩序(全球反詐欺聯盟(GASA,2024)，為掌握電信網路詐欺犯罪之國際發展趨勢與主要防制策略樣態，本研究選取詐欺犯罪統計資料取得相對完整且公開性較

高之日本、新加坡、英國與澳洲等四個國家，蒐整其近年電信網路詐欺犯罪情勢與相關防制政策。惟鑑於各國在統計編製方式、案件類型劃分與政策關注重點上均存在差異，若僅以數據對照作為分析核心，恐難以充分反映其防制策略設計之實質內涵，故本節不以建立一致口徑之量化比較為目的。基此，本研究爰依據我國打詐綱領 2.0 所揭示之打詐五面向防制架構，將防制電信網路詐欺之政策作為區分為五大面向：識詐（宣導教育面）、堵詐（電信防護面）、防詐（數位經濟平臺面）、阻詐（資金流向面）與懲詐（司法執法面），作為分析主要國家防制策略之共同觀察重點。藉以歸納其政策邏輯與防制特色，作為後續理論建構與實證分析之基礎。

一、日本

臺灣所稱的電信網路詐欺犯罪與日本所稱的特殊詐欺犯罪相類似，在日本特殊詐欺犯罪者利用電話、傳真、電子郵件等資通訊工具以非接觸的方式，誘使被害人誤信犯罪者的話術，進而詐取被害人錢財，且被害人大都是對老年人等社會弱勢群體，本研究蒐集日本特殊詐欺犯罪手法及近四年（2021-2024）日本警察廳公布之犯罪統計數據與相關防制策略及成效分析如下。

(一)犯罪情勢

1.犯罪手法

日本東京警視庁自 2020 年 1 月 1 日起，將特殊詐欺手法分為以下 10 類：

(1)猜猜我是誰詐欺(オレオレ詐欺)

犯罪者撥打被害人電話偽稱是其親戚朋友等熟人，並說「我啦！我啦！（Ore！Ore！）」等來詐欺（或威脅）被害人交付金錢的方法。

(2)儲蓄詐欺(預貯金詐欺)

犯罪者以資通訊工具偽稱警察或銀行員工來電告知被害人：「您的銀行帳戶正被用於犯罪活動」接著要求被害人交付金融卡及密碼，再盜領被害人金融機構的錢財。

(3)虛假帳單詐欺(架空料金請求詐欺)

犯罪者透過電子郵件或 SNS[8]等發送諸如「您有未付款項，如果不付款，將被起訴」要求被害人支付不存在的帳單款項，或在被害人以電腦上網時顯示「您的電腦已感染病毒」等訊息，並以使用防毒支援費用來詐欺（威脅）金錢等伎倆。

(4)退款詐欺(還付金詐欺)

犯罪者先以資通訊工具向被害人謊稱要退還醫療費、稅金或保險費等，再誘騙被害人依犯罪者指示操作自動櫃員機（ATM），將錢從被害人帳戶轉入犯罪者的帳戶。

(5)貸款擔保詐欺(融資保証金詐欺)

犯罪者以資通訊工具向欲申請貸款的被害人謊稱須先繳納押金，才可輕鬆獲得貸款等話術，以詐欺取被害人交付金錢。

(6)金融產品詐欺(金融商品詐欺)

犯罪者透過資通訊工具鼓吹被害人投資虛構之高獲利未上市股票、公司債等有價證券或購買昂貴商品等假投資訊息，以詐欺被害人交付金錢。

8.SNS：社群網路服務（Social Networking Service 簡稱：SNS）是一種線上社群媒體平台，人們可以通過它來建立與其他人分享類似個人或職業內容、興趣、活動、背景或現實生活聯絡的社群網路或社交關係。

(7)賭博詐欺(ギャンブル詐欺)

犯罪者在雜誌上發布或發送電子郵件等方式，以「招募彈珠機玩家」等名義，欺騙被害人申請會員註冊並支付註冊費或資訊費等詐欺犯罪手法。

(8)假交友詐欺(交際あっせん詐欺)

(9)犯罪者在雜誌上發布或發送電子郵件等方式，以「介紹女性」為幌子，向被害人詐欺會員註冊費或保證金的詐欺手法。

(10)其他特殊詐欺(その他の特殊詐欺)

指不屬於上述類別的特殊詐欺行為。

(11)金融卡詐欺竊盜（キャッシュカード詐欺盜（窃盗）

犯罪者打電話向被害人謊稱是警察、銀行、大型百貨公司員工等，聲稱被害人的金融卡被盜用，待取信被害人後，犯罪者便冒充便衣警察或銀行工作人員，以「檢查金融卡」等藉口來到被害人家中，誘騙被害人將金融卡和一張寫有密碼的紙放入信封內並要求被害人蓋章密封，再趁被害人拿取印章時，將預先準備好裝有毫無價值的積分卡信封與其掉包，同時告知被害人為確保可疑資金不被提取，在一定日數內不可打開信封，待得手後犯罪者即持被害人所有的金融卡從其帳戶中盜領現金。（日本東京警視庁,2020）。

2.犯罪統計數據

(1)依據日本警察廳公布 2021 年特殊詐欺犯罪統計，認定件數為 14,498 件比 2020 年 13,550 件增加 948 件（+7%），財損金額 28,199,462,547 日圓（以下同）比 2020 年 28,523,359,039 元減少 323,896,492 元（-1.1%）主要犯罪工具電話佔 88.9%；電子郵件佔 7%；明信片、密封信件、傳真、網站等佔 4.1%。依犯罪手法分析，猜猜我是誰詐欺和退款詐欺 99%使用電話進行詐欺；虛假帳單詐欺 46%使用電子郵件，33%使用電話，相關數據分析如下（警察庁,2022）：

A.發生數前 5 名

第 1 名：退款詐欺(還付金詐欺)4,004 件。第 2 名：猜猜我是誰詐欺(オレオレ詐欺)3,085 件。第 3 名：其他特殊詐欺(その他の特殊詐欺)2,602 件。第 4 名：儲蓄詐欺(預貯金詐欺)2,431 件。第 5 名：虛假帳單詐欺(架空料金請求詐欺)2,117 件。（如表 2-11）。

表 2-11 2021 年日本詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	退款詐欺(還付金詐欺)	4,004
2	猜猜我是誰詐欺(オレオレ詐欺)	3,085
3	其他特殊詐欺(その他の特殊詐欺)	2,602
4	儲蓄詐欺(預貯金詐欺)	2,431
5	虛假帳單詐欺(架空料金請求詐欺)	2,117

資料來源：整理自警察庁（2022）。令和３年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form:https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/tokushusagi_toukei2021.pdf，Last viewed date：July 4, 2024

B.財損數前 5 名

第 1 名：猜猜我是誰詐欺(オレオレ詐欺)9,060,728,729 元。第 2 名：虛假帳單詐欺(架空料金請求詐欺)6,807,621,000 元。第 3 名：退款詐欺(還付金詐欺)4,518,427,000 元。第 4 名：其他特殊詐欺(その他の特殊詐欺)3,948,502,359 元。第 5 名：儲蓄詐欺(預貯金詐欺)3,058,074,459 元。(如表 2-12)。

表 2-12 2021 年日本詐欺案件財損數前 5 名

排名	犯罪手法	日圓/元
1	猜猜我是誰詐欺(オレオレ詐欺)	9,060,728,729
2	虛假帳單詐欺(架空料金請求詐欺)	6,807,621,000
3	退款詐欺(還付金詐欺)	4,518,427,000
4	其他特殊詐欺(その他の特殊詐欺)	3,948,502,359
5	儲蓄詐欺(預貯金詐欺)	3,058,074,459

資料來源：整理自警察庁（2022）。令和３年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form:https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/tokushusagi_toukei2021.pdf，Last viewed date：July 4, 2024.

C.使用犯罪工具前 3 名

第 1 名：電話佔 88.9%。第 2 名：電子郵件佔 7%。第 3 名：明信片、密封信件、傳真、網站等佔 4.1%。(如表 2-13)。

表 2-13 2021 年日本欺案件使用犯罪工具前 3 名

排名	犯罪手法	佔比
1	電話	88.9%
2	電子郵件	7%
3	明信片、密封信件、傳真、網站等	4.1%

資料來源：整理自警察庁（2022）。令和３年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form:https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/tokushusagi_toukei2021.pdf，Last viewed date：July 4, 2024.

(2)依據日本警察廳公布 2022 年特殊詐欺犯罪統計，認定件數為 17,570 件比 2021 年 14,498 件增加 3072 件（+17.4%），財損金額 37,081,354,580 元比 2021 年 28,199,462,547 元增加 8,881,892,033 元（+31.4%）。主要犯罪工具電話佔 86.3%；電子郵件佔 8.1%；明信片、密封信件、傳真、網站等佔 0.08%。依犯罪手法分析，猜猜我是誰詐欺和退款詐欺 99%使用電話進行詐欺；虛假帳單詐欺 47%使用電子郵件，24%使用電話，相關數據分析如下（警察庁,2023）：

A.發生數前 5 名

第 1 名：退款詐欺(還付金詐欺)4,679 件。第 2 名：猜猜我是誰詐欺(オレオレ詐欺)4,287 件。第 3 名：其他特殊詐欺(その他の特殊詐欺)3,074 件。第 4 名：虛假帳單詐欺(架空料金請求詐欺)2,922 件。第 5 名：儲蓄詐欺(預貯金詐欺)2,363 件。(如表 2-14)。

表 2-14 2022 年日本詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	退款詐欺(還付金詐欺)	4,679
2	猜猜我是誰詐欺(オレオレ詐欺)	4,287
3	其他特殊詐欺(その他の特殊詐欺)	3,074
4	虛假帳單詐欺(架空料金請求詐欺)	2,922
5	儲蓄詐欺(預貯金詐欺)	2,363

資料來源：整理自警察庁（2023）。令和４年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/tokushusagi_toukei2022.pdf，Last viewed date：July 5, 2024.

B.財損數前 5 名

第 1 名： 猜猜我是誰詐欺(オレオレ詐欺)12,933,603,000 元。第 2 名：虛假帳單詐欺(架空料金請求詐欺)10,177,798,000 元。第 3 名：退款詐欺(還付金詐欺)5,367,626,000 元。第 4 名：其他特殊詐欺(その他の特殊詐欺)4,686,253,006 元。第 5 名：儲蓄詐欺(預貯金詐欺)2,889,621,574 元。（如表 2-15）。

表 2-15 2022 年日本詐欺案件財損數前 5 名

排名	犯罪手法	日圓/元
1	猜猜我是誰詐欺(オレオレ詐欺)	12,933,603,000
2	虛假帳單詐欺(架空料金請求詐欺)	10,177,798,000
3	退款詐欺(還付金詐欺)	5,367,626,00
4	其他特殊詐欺(その他の特殊詐欺)	4,686,253,006
5	儲蓄詐欺(預貯金詐欺)	2,889,621,574

資料來源：整理自警察庁（2023）。令和４年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/tokushusagi_toukei2022.pdf，Last viewed date：July 5, 2024.

C.使用犯罪工具前 3 名

第 1 名：電話佔 86.3%。第 2 名：電子郵件佔 8.1%。第 3 名：明信片、密封信件、傳真、網站等佔 0.08%（如表 2-16）。

表 2-16 2022 年日本詐欺案件使用犯罪工具前 3 名

排名	犯罪手法	佔比
1	電話	86.3%
2	電子郵件	8.1%
3	明信片、密封信件、傳真、網站等	0.08%

資料來源：整理自警察庁（2023）。令和４年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/tokushusagi_toukei2022.pdf，Last viewed date：July 5, 2024.

(3)依據日本警察廳公布2023年特殊詐欺犯罪統計，認定件數為19,038件比2022年17,570件增加1,468件（+8.3%），財損金額45,256,436,710元比2022年37,081,354,580增加8,175,082,130元（+22%）。主要犯罪工具電話佔77.5%；彈跳視窗[9]佔12.2%；SMS[10]、SNS、電子郵件佔9.1%；明信片、密封信件、傳真、網站等佔1.1%。依犯罪手法分析，猜猜我是誰詐欺和退款詐欺 99.9%使用電話進行詐欺；虛假帳單詐欺 43.7%使用彈出視窗，30.0%使用電話，25.5%使用電子郵件，相關數據分析如下（警察庁,2024）：

A.發生數前5名

第1名:虛假帳單詐欺(架空料金請求詐欺)5,198件。第2名:退款詐欺(還付金詐欺)4,185件。第3名：猜猜我是誰詐欺(オレオレ詐欺)3,955 件。第 4 名：儲蓄詐欺(預貯金詐欺)2,754件。第5名：其他特殊詐欺(その他の特殊詐欺)2,217件（如表2-17）。

表 2-17 2023 年日本詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	虛假帳單詐欺(架空料金請求詐欺)	5,198
2	退款詐欺(還付金詐欺)	4,185
3	猜猜我是誰詐欺(オレオレ詐欺)	3,955
4	儲蓄詐欺(預貯金詐欺)	2,754
5	其他特殊詐欺(その他の特殊詐欺)	2,217

資料來源：警察庁（2024）。令和５年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2023.pdf，Last viewed date：July 6, 2024.

B.財損數前5名

第1名： 虛假帳單詐欺(架空料金請求詐欺)14,038,598,000元。第2名：猜猜我是誰詐欺(オレオレ詐欺)13,348,134,110元。第3名：退款詐欺(還付金詐欺)5,131,511,000元。第4名：儲蓄詐欺(預貯金詐欺)3,846,364,500元。第5名：其他特殊詐欺(その他の特殊詐欺)2,981,704,100元（如表2-18）。

表 2-18 2023 年日本詐欺案件財損數前 5 名

排名	犯罪手法	日圓/元
1	虛假帳單詐欺(架空料金請求詐欺)	14,038,598,000
2	猜猜我是誰詐欺(オレオレ詐欺)	13,348,134,110
3	退款詐欺(還付金詐欺)	5,131,511,000
4	儲蓄詐欺(預貯金詐欺)	3,846,364,500
5	其他特殊詐欺(その他の特殊詐欺)	2,981,704,100

資料來源：警察庁（2024）。令和５年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2023.pdf，Last viewed date：July 6, 2024.

9.使用電腦、智慧型手機等瀏覽網站時突然彈跳出現的視窗。

10.SMS：簡訊服務（Short Message Service 簡稱：SMS）允許在行動裝置之間交換簡短的文字訊息，SMS訊息通常具有160個字元的最大長度，並且可以在各種行動網路上傳送和接收，SMS廣泛用於個人和商業通訊，提供了一種快速便捷的方式向個人或群組傳送簡短的訊息。

C.使用犯罪工具前 4 名

第 1 名：電話佔 77.5%。第 2 名：彈跳視窗佔 12.2%。第 3 名：SMS 、SNS、電子郵件佔 9.1%。第 4 名：明信片、密封信件、傳真、網站等佔 1.1%。（如表 2-19）。

表 2-19 2023 年日本詐欺案件使用犯罪工具前 4 名

排名	犯罪手法	佔比
1	電話	77.5%
2	彈跳視窗	12.2%
3	SMS 、SNS、電子郵件	9.1%
4	明信片、密封信件、傳真、網站等	1.1%

資料來源：警察庁（2024）。令和５年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2023.pdf，Last viewed date：July 6, 2024.

(4) 依據日本警察廳公布 2024 年特殊詐欺犯罪統計，認定件數為 21,043 件比 2023 年 19,038 件增加 2,005 件(+10.5%)，財損金額 71,877,275,370 元比 2023 年 45,256,436,710 增加 26,620,838,660 元（+58.8%）。主要犯罪工具電話佔 79%；SMS、SNS、電子郵件佔 10%；彈跳視窗佔 8.8%；明信片、密封信件、傳真、網站等佔 2.2%。依犯罪手法分析，猜猜我是誰詐欺和退款詐欺 99%使用電話進行詐欺；虛假帳單詐欺 35.7%使用電話，31.1%使用彈出視窗，28.0%使用電子郵件，相關數據分析如下（警察庁,2025）

A.發生數前 5 名

第 1 名： 猜猜我是誰詐欺(オレオレ詐欺)6,752 件。第 2 名：虛假帳單詐欺(架空料金請求詐欺)5,716 件。第 3 名：退款詐欺(還付金詐欺)4,070 件。第 4 名：儲蓄詐欺(預貯金詐欺)2,276 件。第 5 名：其他特殊詐欺(その他の特殊詐欺)1,385 件（如表 2-20）。

表 2-20 2024 年日本詐欺案件發生數前 5 名

排名	*犯罪手法*	*件數*
1	*猜猜我是誰詐欺(オレオレ詐欺)*	*6,752*
2	*虛假帳單詐欺(架空料金請求詐欺)*	*5,716*
3	*退款詐欺(還付金詐欺)*	*4,070*
4	*儲蓄詐欺(預貯金詐欺)*	*2,276*
5	*其他特殊詐欺(その他の特殊詐欺)*	*1,385*

資料來源：警察庁（2025）。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）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/teisei_sagi2024.pdf，Last viewed date：October 28,2025.

B.財損數前 5 名

第 1 名：猜猜我是誰詐欺(オレオレ詐欺)45,842,900,700 元。第 2 名：虛假帳單詐欺(架空料金請求詐欺)13,384,799,000 元。第 3 名：退款詐欺(還付金詐欺)6,369,672,000 元。第 4 名：儲蓄詐欺(預貯金詐欺)2,551,871,450 元。第 5 名：其他特殊詐欺(その他の特殊詐欺)1,822,489,220 元（如表 2-21）。

表 2-21 2024 年日本詐欺案件財損數前 5 名

排名	犯罪手法	日圓/元
1	猜猜我是誰詐欺(オレオレ詐欺)	45,842,900,700
2	虛假帳單詐欺(架空料金請求詐欺)	13,384,799,000
3	退款詐欺(還付金詐欺)	6,369,672,000
4	儲蓄詐欺(預貯金詐欺)	2,551,871,450
5	其他特殊詐欺(その他の特殊詐欺)	1,822,489,220

資料來源：警察庁（2025）。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）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/teisei_sagi2024.pdf，Last viewed date：October 28,2025.

C.使用犯罪工具前 4 名

第 1 名：電話佔 79%。第 2 名：SMS、SNS、電子郵件佔 10%。第 3 名：彈跳視窗佔 8.8%。第 4 名：明信片、密封信件、傳真、網站等佔 2.2%。（如表 2-22）。

表 2-22 2024 年日本詐欺案件使用犯罪工具前 4 名

排名	犯罪手法	佔比
1	電話	79%
2	SMS、SNS、電子郵件	10%
3	彈跳視窗	8.8%
4	明信片、密封信件、傳真、網站等	2.2%

資料來源：警察庁（2025）。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）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/teisei_sagi2024.pdf，Last viewed date：October 28,2025.

(二)防制策略

1.日本自 2021 年以來，以老年人為主的特殊詐欺案件數量不斷增加，犯罪者透過通訊軟體招募從事強盜及詐欺犯罪案件層出不窮，在群眾焦慮感日益增強的情況下，2023 年 3 月 17 日前日本首相岸田文雄召開第 36 次犯罪對策閣僚會議（類似臺灣行政院治安會議）頒布「透過通訊軟體招募從事強盜及詐欺犯罪緊急對策計畫」（ＳＮＳで実行犯を募集する手口による強盗や特殊詐欺事案に関する緊急対策プラン）。採取防止犯罪組織招募成員、消除犯罪工具、營造安全社會環境、儘速緝捕首謀犯嫌等四大面向措施（犯罪対策閣僚会議,2023），茲摘要說明如下：

(1)防止犯罪組織招募成員措施

A.蒐證、刪除及取締暗網。

B.移除違法及有害的招募求職網路訊息。

C.加強青少年道德教育促勿從事違法行為。

D.對強盜及詐欺罪犯加強法定處罰力度。

(2)消除犯罪工具措施

A.強化個人資訊保護，防止個人資料外洩，成為潛在被害標的。

B.推動申辦行動電話實名制並防止不法電話轉接服務。
C.推動 SIM 卡業者與申辦人簽約時遵守實名制規定。
D.防止銀行帳戶遭非法使用。
E.強化資通訊犯罪工具解析能力。
F.防杜高匿名性的通訊軟體遭非法使用
G.防止在日外藉人士持有的銀行帳戶和手機遭非法使用。

(3)營造安全社會環境措施
A.與快遞公司合作，防止犯罪者冒充快遞公司實施搶劫。
B.協助民眾設置具有犯罪預防功能的建築設備、監視器及郵箱
C.協助年長者安裝具有預防犯罪功能的住宅電話及更改電話號碼。
D.制定防止年長者接到詐欺集團撥打住宅電話號碼的相關對策。
E.制定防止年長者在家中存放現金的措施。
F.強化警察巡邏服務。

(4)儘速緝捕首謀犯嫌措施
A.推動有效調查及打擊詐欺犯罪集團措施。
B.強化跨國偵查及與國外執法機構合作能力。
C.強化打擊跨國洗錢犯罪能力。

2.儘管公私部門根據「透過通訊軟體招募從事強盜及詐欺犯罪緊急對策計畫」共同採取對策，但 2023 年日本的詐欺損失(約 1,630 億日元)卻比 2022 年倍增。近年來，隨著社群媒體和線上支付日益普遍，犯罪集團利用此趨勢使得犯罪手法變得更加複雜和多樣化，並加速擴大詐欺犯罪造成的損害。鑒此，日本前首相岸田文雄於 2024 年 6 月 18 日召開第 39 次犯罪對策閣僚會議提出「保護公民免受詐欺的綜合措施」(国民を詐欺から守るための総合対策)，採取避免成為受害者、防止犯罪組織招募成員、剝奪犯罪工具、強化查緝犯罪者等四大面向措施（犯罪対策閣僚会議,2024），茲摘要說明如下：

(1)避免成為受害者的措施
A.針對 SNS 假投資及假戀愛詐欺措施
（a）向潛在受害者發出警告
要求 SNS 業者向可能成為潛在受害者的使用者發出警告，例如當使用者開始與可疑帳戶互動時。
（b）促請業者採取有效的廣告篩選。
甲. 要求 SNS 業者制定並公佈平台上發布的廣告的篩選標準，並完善篩選系統（特別是充分配置了解日語和日本社會等的人員），加強廣告發布者的身份驗證等。
乙. 要求 SNS 業者根據調查機構所提供「用於詐欺的帳號」等資訊及時刪除廣告。
（c）推動刪除虛假廣告措施
甲. 對於詐欺虛假廣告等，通知行業協會要求 SNS 經營者根據使用條款採取刪除欺騙性廣告等措施。
乙. 針對網路假訊息、虛假廣告，結合國際情勢，推動包括制度措施在內的綜合對策。
（d）要求大型平台業者加快刪除違法訊息
針對大型平台業者網路違法有害訊息，要求依《資訊傳播平台對策法》，規定加快刪除速度、公開營運狀況，並落實資訊發布平台適用規定。
（e）SNS 業者須確保在使用者新增好友時，顯示有效警告並徵得同意
在 SNS 假投資及假戀愛詐欺犯罪過程中，最初接觸工具中 SNS 佔大多數，民眾經常被

SNS 上的陌生人拉入 SNS 群組，為防止 SNS 被濫用，SNS 業者須確保使用者在將陌生帳戶(海外帳戶)添加為好友時，必須採取顯示有效警告和徵得當事人的同意等措施。

（f）開設交友軟體帳戶時加強身分驗證

交友軟體擁有大量的交友機會，並且有很多人使用，讓結識朋友變得容易，但交友軟體上顯示的個人資料是否真實無法驗證。因此，鼓勵交友軟體業者在使用者開設帳戶時，使用公共個人認證服務以實施更嚴格的身份驗證。

（g）推出金融教育提高防詐意識

日本金融經濟教育振興機構（J-FLEC[11]）與相關部會和機構合作，透過在學校、工作場所以及社區中心和圖書館等當地社區等不同環境中向廣泛年齡層提供金融和經濟教育，包括如何應對金融詐欺和金融風險，讓他們正確認識投資風險和如何應對財務困難。

B.針對網路釣魚所採取的措施

（a）推動對發送網域認證技術（DMARC[12]（Domain-based Message Authentication, Reporting and Conformance）等）的支持

為讓釣魚郵件無法與使用者接觸，有系統地向網路服務供應商等電子郵件接收企業和金融機構等電子郵件發送企業導入發送網域認證技術。

（b）推動關閉釣魚網站

2023 年 2 月日本政府要求遭網路釣魚攻擊的企業敦促託管企業關閉釣魚網站。後續將要求被冒充的企業主動要求關閉釣魚網站，並加強與相關組織和網路犯罪預防志工的合作，鼓勵更廣泛的主動要求關閉。

（c）根據釣魚網站的特性進行防範

根據釣魚網站的趨勢與特性，(例如在同一 IP 位址上建立多個釣魚網站)，除可透過報告和協商確認外，還可根據特徵實施先發制人的應對措施，以識別未發現的網路釣魚網站，並在防毒軟體上顯示警告。

C.針對特殊詐欺採取的措施。

（a）擴大拒絕國際通話申請

為了防止犯罪者利用國際來話進行詐欺，進一步擴大營運「拒絕國際通話受理中心」受理民眾拒絕國際來電申請。

（b）推廣針對不當使用簡訊的措施

推廣使用簡訊過濾系統，以防止簡訊濫用，並對感染惡意軟體的智慧型手機或裝置進行識別和警告。

（c）對邊操作 ATM 邊使用手機者提出警示

在特殊詐欺犯罪中，被害人一邊操作 ATM，一邊透過手機等接收指令的情況較多，因此日本政府與金融機構及其他相關組織合作，努力向邊操作 ATM 邊使用手機者提出警示。

(2)防止犯罪組織招募成員措施

A.推進「黑暗打工[13]」等資訊蒐集、刪除、打擊等

11.J-FLEC：(Financial and Economic Education Promotion Corporation）是日本根據《關於提供金融服務和改善使用環境等的法律》於 2024 年 4 月成立的法人，旨在為廣泛的年齡群體提供金融和經濟教育機會，該機構由金融資訊中央委員會（秘書處：日本銀行)、日本銀行家協會和日本證券交易商協會共同創立，並透過公共和私營夥伴關係將該系統擴展到全國。

12.DMARC：基於網域的訊息驗證、報告和一致性的縮寫，如果收到的郵件的網域名稱與寄件者的網域名稱（標頭 From）相符，則將其投遞至郵箱上的收件箱，視為身分驗證成功，如果與寄件者的網域不相符，則視為身份驗證成功該技術可以將電子郵件作為垃圾郵件資料夾進行隔離或拒絕。

13.以「黑暗打工」、「秘密打工」等字眼或暗示支付極高費用等方式招募犯罪人員的帖子，但未公開工作

警方將透過「網路熱線中心」和「網路巡警中心[14]」的有效運作，努力消除「黑打工」等網絡訊息，並推動利用回覆功能對發文者進行單獨警告，同時鼓勵網路服務商確保刪除此類信息。

B.杜絕犯罪組織在網路招募成員

（a）在網路傳播招募犯罪分子的「黑暗兼職」等信息，涉嫌「僱用危害公眾健康工作為目的」，違反日本「就業保障法」（職業安定法[15]）第 63 條第 2 項規定，為了確保勞動市場健康，警方將進行線上巡查活動，以打擊非法召募。

（b）要求招聘媒體、企業主等行業組織採取必要措施，杜絕發布違法有害招聘信息（含可疑信息，下同）。

（c）要求招聘媒體等行業組織和企業主與警方合作，如果發現發布非法或有害的招聘訊息，將採取適當措施。

（d）通知都道府縣勞動局，如發現非法或有害的招聘信息，必須配合警方採取適當行動。

C.防止青少年打工犯罪的教育啟蒙

（a）推動淨化青少年不良環境措施。

（b）推動防止兒童、學生等不良行為。

（c）紮實培養運用資訊的能力，包括資訊道德，遵守網路規則和禮儀。

（d）舉辦犯罪預防課程，防止年輕人簡單化思維而參與犯罪。

D.針對犯罪集團的通訊工具措施

（a）關於濫用高度保密軟體的警報

加強宣導並防止「黑暗兼職」的求職者在犯罪者的引導下，使用高度保密的通訊軟體進行交流，例如使用者在進入可能是「黑暗打工」等應用軟體時顯示警告訊息。

（b）協助分析作為證據扣押的智慧型手機設備等

加強分析最新電子設備和應用程式的技術能力，並購置分析智慧型手機的設備，同時與相關機構合作共享對檢察官、偵查人員進行訓練，以強化資訊科技分析的態勢。

E.推動對搶劫、特殊詐欺犯罪者實施應有懲罰

全力偵破手段極為惡劣的搶劫及特殊詐欺案件，確保將犯罪者繩之以法，並在法庭上適當地主張和證明惡意情節。

F.防止曾參與詐欺犯罪[16]的未成年人再犯

與未成年人培訓學校等相關機構合作，舉辦預防未成年人犯罪學習班等，推動預防未成年人犯罪再次發生。

(3)剝奪犯罪工具措施

A.確保有效的身份驗證措施

民眾在簽訂使用手機通訊服務合約時，原則上統一使用個人編號卡等電子驗證方法進行身份驗證。

性質及帖子相關資訊。對此，有人指出，這樣的表述讓人們更容易隨意參與犯罪。因此在對青少年的宣傳和啟蒙中，將繼續適當使用「犯罪者招募資訊」等用語。

14.日本網路巡警中心已引進了人工智慧搜尋系統，加強對違法有害資訊的打擊力道。

15.參照昭和 22 年法律第 141 号，https://laws.e-gov.go.jp/law/322AC0000000141（最後瀏覽時間：2024 年 11 月 25 日）。

16.指 SNS 假投資及假戀愛詐欺、特殊詐騙等及與網路釣魚相關的犯罪。

B.與金融機構合作推動逮捕措施
金融機構應建立監控和偵測涉嫌詐欺的提款和匯款等交易機制，採取措施防止未經授權的使用，並及時與警方共享有關詐欺帳戶資訊。

C.防止使用電子貨幣犯罪的措施
由政府建立預支付工具發行人系統，加強監控以及時發現電子貨幣被盜情況，以便在發現使用詐欺性電子貨幣時可以及時向警方提供資訊。

D.加強防止未經授權使用儲蓄帳戶等的措施。
推動交易時進一步嚴格查核，防止未經授權使用儲蓄帳戶，包括公司帳戶。

E.促進加密資產的沒收和保全
為了使沒收加密資產更加順利和可靠，日本政府將著手起草立(修)法程序，以引入加密資產執行程序和保存程序。

(4)強化查緝犯罪者措施

A.強化打擊匿名流動的犯罪集團並明晰實情
（a）強化打擊匿名性與流動性犯罪集團
甲. 建立打擊並澄清事實制度。
乙. 建立澄清犯罪所得等的制度。

（b）執行有效打擊並明確實際狀況
甲. 有效打擊並查明犯罪集團的真實情況等。
乙. 查明犯罪基地並逮捕主要嫌疑人。
丙. 請 SNS 業者在日本落地設立應對調查機構及詢問聯絡點，並建立快速應對詢問系統。

（c）推動適當懲罰
甲. 推動實現對搶劫和特殊詐欺犯罪者的適當懲罰。
乙. 採取有效控制教唆犯罪者的行為。

B.促進海外據點曝光
（a）徹底的國際調查並與外國當局合作
甲. 推進海外犯罪基地偵查。
乙. 強化境外移送犯罪嫌疑人制度。

（b）加強針對非法攜帶現金出境的管制措施

C.促進防止企業被濫用洗錢的努力
採取新措施，防止非實質公司被用於洗錢。

D.促進財產損失的恢復
推動損害賠償賠償制度、銀行轉帳詐欺救濟法等有效運作。

3.日本政府雖於 2024 年推出「保護公民免受詐欺的綜合措施」(国民を詐欺から守るための総合対策)，但 2024 年日本詐欺犯罪財損金額仍突破 3,000 億日圓，創下歷史新高。其中 SNS 投資詐欺與戀愛詐欺受害金額約達 1,268 億日圓，較前 2023 年暴增三倍，另外，特殊詐欺（冒充公務員、假親友等）被害金額 722 億日圓，也超過歷年高點。因此，日本前首相石破茂於 2025 年 4 月 22 日召開第 42 次犯罪對策閣僚會議指出，詐欺集團

多為跨國化、網路化與匿名化型態，並結合 AI 技術、VPN 及假帳號進行洗錢與詐欺。故提出「保護公民免受詐欺的綜合措施 2.0」(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,2025），以整合跨部會力量，以數位監管與公私協力為核心，建構「從預防到處罰」的循環防詐機制，茲摘要說明如下：

(1)整體策略架構

A.對策分為五大主軸：SNS 型投資與戀愛詐欺防制、特殊詐欺防制、ID 與密碼竊取防制、治安基盤與國際合作強化、犯罪收益追繳與 AI 偵查技術導入。

B.政府強調跨部會協調，由內閣府統籌，結合警察廳、總務省、金融廳、數位廳、法務省及地方政府共同推動，並與國際刑警組織（ICPO）及聯合國毒品和犯罪問題辦公室（United Nations Office on Drugs and Crime,簡稱：UNODC）合作。

(2)主要防詐措施

A.SNS 型投資與戀愛詐欺防制：要求 SNS 與交友 App 導入 My Number 卡及 SIM 卡實名制，禁止匿名註冊；金融廳與警察廳建立即時凍結系統，強化實質受益人揭露；AI 偵測詐欺內容並自動警示用戶。

B.防止民眾成為加害者：設置網路熱線中心監測犯罪招募訊息，導入 AI 自動警示系統，並提供青少年保護管道。

C.特殊詐欺防制：改革電話號碼管理制度，防止號碼偽造與濫用；推動防詐電話補助及國際電話封鎖制度；導入 DMARC 郵件認證防釣魚詐欺。

D.釣魚詐欺防制：以 AI 辨識釣魚網站，自動封鎖可疑網址；推動 Passkey 無密碼登入制度；要求電商與信用卡業者定期檢測資安漏洞。

E.金融監管強化：監管虛擬資產交易所，建立交易追蹤及異常轉帳警示制度；金融機構導入即時凍結平台，阻斷詐欺金流。

F.SNS 業者協力義務化：規定平台 24 小時內回應警方資料請求，並設置日本法人窗口協助跨境取證。

G.國際合作強化：與七大工業國組織（Group of Seven,簡稱：G7）[17]及 UNODC 合作建立跨國追訴與收益剝奪機制；加強與東南亞國家之警務連線與據點查緝。

H.治安基盤強化：建立 AI 數據分析中心整合金融、電信與犯罪情資；培育具 AI 與加密分析技能之網路偵查人才；推動社區巡守與地方防詐聯防機制。

(三)防制成效

日本政府自 2023 年起推動「保護公民免受詐欺的綜合措施」(国民を詐欺から守るための総合対策)，其政策核心目標在於建構橫跨電信、金融、數位平台及教育領域之全國性防詐體系，以系統化整合各部會之防詐作為，強化民眾防詐能力並阻斷犯罪資金流向。該措施施行至 2025 年 3 月底止，SNS 投資型及戀愛詐欺之被害金額仍呈上升趨勢，顯示詐欺犯罪型態持續朝向高科技化與多元化發展，網路詐欺風險未見明顯緩解。以下所述之日本防制詐欺主要措施與成效，係研究者依據日本內閣官房於 2025 年 3 月底公布之

17.由世界七大已開發國家經濟體組成的政府間政治論壇，正式成員國為美國、德國、英國、法國、日本、義大利、加拿大，歐盟為非正式成員。

《「全面保護國民免受詐欺侵害的措施」等的進展情況》(《「国民を詐欺から守るための総合対策」等の取組状況について（令和 7 年 3 月末時点）》) 進行整理與歸納。其所引用之統計及政策數據，均為官方跨部會彙整之施政進度資料，部分數據則為研究者依原文政策段落內容進行推估或整併。本文所列資料均依日本官方原始文件整理，僅供學術研究與國際政策比較分析使用，不得作為正式統計引用。

1.防止國民成為詐欺被害者

(1)SNS 型投資詐欺防制：主要 SNS 平台全面導入身分確認制度，導入率達九成；2024 年度受理投資詐欺通報約 8,200 件，成功下架違法廣告約 2,100 件。

(2)導入 AI 辨識假投資內容系統，辨識準確率達 92%，有效攔阻偽造金融顧問及假投資 App。

(3)修訂《金融商品交易法》指針，規範 SNS 投資廣告之招攬行為須具合法註冊資格。

(4)釣魚詐欺防制：DMARC 郵件認證導入率達 98%，關閉釣魚網站約 3 萬 3,000 個，Passkey 無密碼認證普及率達 85%。

(5)特殊詐欺防制：全國發放防詐電話 56 萬台，封鎖國際電話約 1,800 萬通、攔阻冒名簡訊約 1,500 萬則；ATM 異常警示系統通報阻詐約 2.3 萬件，成功避免損失約 70 億日圓。

2.防止國民被捲入犯罪

(1)闇打工取締：以 AI 監測 SNS 違法招募訊息，刪除約 12 萬則職缺；並修訂《職業安定法》，將非法刊登列為刑事犯罪，累計移送案件 57 件。

(2)青少年防詐教育：於校園推動防詐教材，全國約 1,200 所高中及大學舉辦講座，參與學生人數約 60 萬人；官方製作防詐教育影片，累積播放量達 1.8 億次。

3.奪取犯罪工具與金流阻斷

(1)電信監理：全面實施資料通信 SIM 實名制，更新登錄資料約 2,200 萬件；97 家轉接電話業者完成認證，非法轉接案件減少約 48%。

(2)金融帳戶防詐：透過警銀即時凍結平台共凍結可疑帳戶約 6.4 萬戶，攔阻金額約 280 億日圓；電子支付系統 AI 警示攔阻交易約 1,900 件。

(3)虛擬資產追查：依據國際《Travel Rule》規範強化追蹤，查扣虛擬資產總值約 9.8 億日圓；查獲個資販售案件 37 件，裁處罰鍰約 3.6 億日圓。

4.確保犯罪者無法逃逸（懲詐面向）

(1)跨國偵查合作：AI 數據中心整合跨境金流分析，2024 年共遣返嫌犯 83 人，並拆除境外詐欺機房 12 處。

(2)國際追訴與犯罪收益剝奪：與 G7 及 UNODC 合作，首次執行跨國沒收金額約 4 億日圓。

(3)被害救濟：依據日本《防制匯款詐欺被害回復及返還金分配法》(《振込詐欺救濟法》) 返還金額達 59 億日圓（回復率約 25%），虛擬資產返還平台受理案件 94 件。

5.創新作為

(1)公私協力宣導

日本警察廳於 2023 年 12 月 25 日指出，2023 年 1 至 11 月，共發生 5,147 件假冒銀行發送電子郵件（簡訊）夾帶釣魚網站的詐欺案件，造成高達 80.1 億日元的金錢損失，不論案件發生數及財損金額均創歷史新高。為因應詐欺集團以假冒銀行發送電子郵件（簡訊）夾帶釣魚網站，讓不知情的民眾受騙上當，致將個人資料及一次性的驗證碼提

供給詐欺集團致使網路銀行遭盜領損害的案件增多，遂結合金融廳、一般社團法人全國銀行協會及日本網路犯罪對策中心之公私協力方式，透過網路及新聞媒體向民眾宣導勿點選來路不明的簡訊或電子郵件連結及輸入密碼與個人資料，避免產生財物損失（日本警察廳,2023）

(2)降低提（匯）款額度及減緩匯款速度

日本銀行為減少民眾因釣魚網站受騙上當提款或匯款所造成的損害，有多家銀行於2023年度做出降低提（匯）款額度及減緩匯款速度，調整情形如下：

A.瑞穗銀行：每日提款上限由100萬日幣調降為50萬日元，匯款上限由200萬日幣調降為100萬日元

B.三井住友信託銀行:網銀匯款限1次只能匯50萬日幣,平日夜間及假日停止匯款服務。

C.au じぶん銀行：全面停止24小時內能立即匯款到其他家銀行的服務。

(3)日本警方最新打擊詐欺犯罪措施（日本の朝日新聞,2023）:

A.增加編列打詐預算金額

明年增加編列打擊詐欺犯罪預算金額為5億3千萬元日幣。

B.調派員警支援查緝詐欺集團

警察廳過往曾調集各道、府、縣警察本部偵查員至東京都警視廳、埼玉縣、千葉縣、神奈川縣警察本部協助調閱監錄系統影象、追緝詐欺集團車手及分析查扣手機通話紀錄，明年將研議再增派偵查員至大阪府警察本部協緝，以強化對各都會區查緝詐欺犯罪能量。

C.增購手機鑑識分析設備

警察廳再增購手機鑑識分析50台機器設備，未來將有140台手機鑑識設備，以提高手機鑑識分析效率。

D.委外請客服中心致電提醒潛在被害民眾

詐欺集團常針對日本老年人詐欺，警方從查扣詐欺犯嫌的電話資料中，清查潛在被害人電話號碼後，委外請客服中心致電提醒遭鎖定詐欺的民眾，經統計2021年有175件民眾因提醒而免於受騙的案件，目前警方需提醒可能受騙的民眾電話約有50萬筆，估算明年將有90萬筆。

E.2024年組改新設打詐指揮官

警察廳2024年將透過組改修法，新設打詐指揮官，由警察廳官房參事官（預計提升為擔任過本部長之課長，層級為警視正，相當於臺灣三線一）統籌指揮調度。

（四）小結

日本所稱「特殊詐欺」係指犯罪者運用電話、傳真、電子郵件或社群媒體等資通訊工具，以非接觸方式誘使被害人陷入誤信而交付財物之犯罪類型，性質上與臺灣所稱電信網路詐欺相似。此類犯罪受害者多為高齡族群，行為特徵呈現話術誘導、冒名身分與遠端控制等形式。根據日本警察廳統計，2021年至2024年間特殊詐欺認知件數與財損金額均呈上升趨勢，案件由2021年的14,498件增至2024年的21,043件，財損金額由約282億日圓攀升至約719億日圓。犯罪手法以退款詐欺（還付金詐欺）、猜猜我是誰（オレオレ詐欺、虛假帳單詐欺（架空料金請求詐欺）及儲蓄詐欺（預貯金詐欺）為主要型態，犯罪工具仍以電話為核心，但自2023年起「彈跳視窗」及「SNS、SMS與電子郵件」等新興媒

介使用比例大幅提升，顯示詐欺手法由語音通信逐步擴展至數位網路環境。為系統分析其防制結構與政策邏輯，本研究依打詐五面向歸納日本政府與警察機關自 2023 年至 2025 年推動之整體防制策略。

1.識詐面向

日本在識詐政策上強調針對高齡者及社群媒體使用者之分眾教育與警示介入，藉由多層溝通與科技預警以縮短被害人由接觸到警覺的時間差。2023 年 3 月所發布的「透過通訊軟體招募強盜及特殊詐欺犯罪緊急對策」指出，需透過教育與資訊揭露防止青少年及一般民眾被犯罪組織招募為「黑暗打工」成員，並加強媒體宣導及社區安全巡守，藉此提升社會防詐意識。2024 年 6 月推出的「保護公民免受詐欺的綜合措施」進一步強化識詐作為，要求 SNS 平台對可疑互動顯示警告、於陌生帳戶新增時須經雙重確認、並建立廣告審核與違法訊息即時刪除機制。為防範假投資與戀愛詐欺，政府要求交友及投資型應用程式實施 My Number 與 SIM 卡實名制，並導入 AI 偵測可疑內容，以主動警示潛在受害者。金融教育部分，由日本金融經濟教育振興機構（J-FLEC）與各部會合作推行校園與社區金融風險教育，以提升民眾辨識詐欺之能力。此外，郵件與釣魚防制措施亦納入識詐體系核心，推動 DMARC 郵件認證及釣魚網站關閉制度，並擴大拒絕國際來電申請與簡訊過濾系統。根據官方資料，截至 2025 年 3 月，主要 SNS 平台導入身分確認制度比例已達九成，2024 年度受理投資詐欺通報約 8,200 件，刪除違法廣告 2,100 件，AI 辨識假投資內容之準確率達 92%，DMARC 導入率達 98%，關閉釣魚網站約 3.3 萬個，Passkey 無密碼登入普及率達 85%，顯示前端警示與風險教育已逐步形成具體成效。

2.堵詐面向

堵詐政策聚焦於通信源頭與資訊內容之管理，以技術封鎖與網絡管制降低詐欺接觸面。日本政府針對國際電話詐欺頻繁現象，擴大「拒絕國際來電受理中心」運作，允許民眾登錄並封鎖跨境來電；同時要求電信業者強化電話號碼管理與實名驗證，防止偽冒號碼與不法轉接服務。簡訊過濾系統及惡意軟體偵測技術亦被制度化，對於感染可疑應用程式的智慧型裝置即時提出警告。對釣魚攻擊，政府要求遭冒充之企業主動請求託管商關閉釣魚網站，並依據同一 IP 多站特徵進行先發制處理，在防毒與瀏覽端顯示警示訊息。自 2023 年以降，「彈跳視窗」成為虛假帳單詐欺的新型載具，主管機關因此要求瀏覽器開發者與防毒軟體業者合作建立即時辨識機制，以減少此類高欺詐風險資訊的暴露機會。整體而言，日本堵詐面向已由單一通訊管理轉向整合式內容管理，兼顧技術防護與民眾回報機制。

3.防詐面向

防詐層面主要透過法制強化與業者義務化，建立前端制度性防線。政府要求 SNS 及交友平台全面實施實名認證，禁止匿名註冊，並規範金融商品招攬廣告必須具合法註冊資格。郵件通信部分則推動 DMARC、SPF 等網域驗證技術，以防止釣魚郵件進入用戶端。教育宣導方面，政府與民間機構共同推動多層防詐教育，包括於學校與社區講授「識別假投資與假戀愛」之技巧。2025 年「綜合對策 2.0」將防詐體系升級為跨部會常設機制，由內閣府統籌，整合警察廳、金融廳、總務省、法務省與數位廳，建立「公私協力一體化」運作模式，要求主要平台於 24 小時內回覆警方資料請求，並設立日本法人窗口以協助跨境取證。平台亦被要求導入 AI 辨識、Passkey 登入及資安稽核制度，以強化身分、內容與系統三層防護。此種制度化防詐設計，使日本能夠在網絡廣告、交友互動與投資招攬等前端場景中即時攔截可疑行為，達成「早期辨識、即時阻斷」的預防目標。

4.阻詐面向

阻詐策略以金流凍結、交易控管與工具剝奪為主軸，藉由即時技術與跨域合作削弱詐欺報酬結構。警察廳與金融機構共同運作的「即時凍結平台」於 2024 年凍結可疑帳戶約 6.4 萬戶，攔阻金額約 280 億日圓；電子支付系統則藉 AI 警示攔阻約 1,900 件可疑交易。各銀行亦同步採取「限額與降速」措施，例如瑞穗銀行調降每日提款上限為 50 萬日圓、三井住友信託銀行限制單次匯款上限 50 萬日圓並暫停夜間服務、au じぶん銀行則全面停止 24 小時跨行即時匯款功能，以延緩詐欺資金流動速度。電信層面推動 SIM 實名制，更新登錄資料約 2,200 萬筆，97 家轉接電話業者完成認證，非法轉接案件下降 48%。虛擬資產部分，依「Travel Rule」規範追蹤可疑轉帳並查扣資產總值約 9.8 億日圓，同時針對個資販售案件裁罰約 3.6 億日圓。金融卡詐欺竊盜案件則由銀行端即時監測異常取款並結合警察到宅勸阻，形成以科技與人工介入並行之防堵模式。此一多層阻詐架構有效降低被害資金外流速度，顯示金融監管與科技應用的結合已成為日本防詐政策之核心。

5.懲詐面向

懲詐政策結合偵查強化、司法量刑與國際合作，以確保犯罪者遭受有效追訴與收益剝奪。2023 年後，日本警方加強對「黑暗打工」違法招募之線上巡查與取締，並透過修訂《職業安定法》提高刑責。警察廳擴充偵查能量，增購手機鑑識設備至 140 台，並計畫於 2024 年設立「打詐指揮官」統籌跨縣偵查資源以集中指揮案件偵辦。跨境偵查方面，日本與東南亞、G7 及 UNODC 合作，於 2024 年遣返涉詐嫌犯 83 人，拆除境外詐欺機房 12 處，並執行跨國犯罪收益沒收金額約 4 億日圓。為確保被害人權益，政府依《防制匯款詐欺被害回復及返還金分配法》（振込詐欺救濟法）返還金額達 59 億日圓，回復率約 25%，另設立虛擬資產返還平台處理 94 件案件。警方同時運用 AI 數據分析與金融情資比對技術，提升詐欺集團網絡結構分析能力，以促進國際聯合查緝。此一懲詐體系結合技術鑑識與國際司法互助，使日本在跨境犯罪防制中具備高度執行力與延展性。

6.綜合評析

綜合觀察，日本自 2023 年起透過「緊急對策」「綜合對策」及「綜合對策 2.0」三階段逐步建構防制體系，其政策邏輯呈現由教育警示、通訊防護、平台責任、金融防線至司法處罰的循環防制架構，形成跨部會合作與民間參與並行的整合模式。若以情境犯罪預防理論觀之，日本的防制策略充分體現「改變犯罪機會結構」的核心精神：識詐面以 AI 識別、行為科學化宣導與分眾教育提升被害人警覺性，強化社會整體的風險認知；堵詐面藉通訊號碼實名制與惡意內容攔截提高詐欺行為成本；防詐面以制度化規範與平臺法遵義務確立前端防護，增加犯罪者施行難度；阻詐面透過即時凍結、限額匯款與異常金流監測降低犯罪報酬；懲詐面則整合跨境偵查、AI 鑑識與收益剝奪，移除持續犯罪的誘因。整體而言，日本的防制體系兼具「增加努力、提升風險、降低報酬、移除藉口」四項策略特質，展現以科技管理與制度合作為基礎的高韌性防制模式。然而，2024 年財損金額再創新高，反映出 AI 生成內容與 SNS 詐欺手法的演化速度超越現行防制能量。未來若能深化平台防詐義務落實、強化 AI 風險分析及跨國追訴合作，將有助於提升日本防制特殊詐欺的長期穩定性與政策示範價值。

二、新加坡

本研究依據新加坡警察部隊(Singapore Police Force)所公佈 2021 年度犯罪簡報（Annual Crime Brief 2021）、2022 年度詐欺與網路犯罪簡報（Annual Scams and Cybercrime Brief 2022）、2023 年度詐欺與網路犯罪簡報（Annual Scams and Cybercrime Brief 2023）、2024 年度詐欺與網路犯罪簡報（Annual Scams and Cybercrime Brief

2024），及 ScamShield Website[18]資料所介紹新加坡近四年（2021-2024）遭遇詐欺問題的嚴重性及星國當局所採行的防制策略分析如下。

(一)犯罪情勢

1.2021 年新加坡警察部隊,合計受理 23,933 件詐欺犯罪報案,前十大詐欺案類財損約 6.32 億元新加坡幣（以下同) (Singapore Police Force,(2022)。

(1)發生數前 5 名

第 1 名假求職詐欺：發生數 4,550 件；財損 9,100 萬元；詐欺者常利用各種社群媒體平台（如 Facebook、Instagram、Telegram 和 TikTok）、WhatsApp 和簡訊(SMSes)上投放廣告，以及透過約會平台（如探探和 Facebook Dating）與被害人進行接觸。第 2 名非銀行類釣魚簡訊詐欺：發生數 2,787 件；財損 1,540 萬元；詐欺者常利用簡訊、電話和電子郵件與被害人進行接觸。第 3 名網路購物詐欺：發生數 2,729 件；財損 590 萬元；詐欺者常利用平台包括 Carousell[19]、Facebook 和蝦皮（Shopee）與被害人進行接觸。第 4 名假投資詐欺：發生數 2,476 件；財損 1.902 億元；詐欺者常利用各種社群媒體平台（Facebook、Tinder 和 Instagram）與被害人進行接觸。第 5 名貸款詐欺：發生數 2,273 件；財損 1,830 萬；詐欺者常利用各種網站、簡訊、WhatsApp 訊息以及社群媒體或電子商務網站上的廣告與被害人進行接觸(如表 2-23)。

表 2-23 2021 年新加坡詐欺案件發生數前 5 名（含財損）

排名	犯罪手法	件數	財損（新加坡幣/萬元）
1	假求職詐欺	4,550	9,100
2	非銀行類釣魚簡訊詐欺	2,787	1,540
3	網路購物詐欺	2,729	590
4	假投資詐欺	2,476	19,020
5	貸款詐欺	2,273	1,830

資料來源：整理自 Singapore Police Force (2022)。Annual Crime Brief 2021。Retrieved form:https://www.police.gov.sg/Media-Room/Statistics?page=2，Last viewed date：September 20, 2024.

(2) 使用犯罪工具前 5 名

第 1 名：社群媒體（Social media）6,095 件。第 2 名：訊息傳遞平台（Messaging Platforms）5,095 件。第 3 名：電話（phone calls）2,883 件。第 4 名：其他網站（Other Websites）2,519 件。第 5 名：簡訊（SMSes）2,367 件（如表 2-24）。

18.由新加坡內政部（Singapore Ministry of Home Affairs）、警察部隊（Singapore Police Force）、開放政府產品（OPEN GOVERNMENT PRODUCTS）和國家預防犯罪委員會（National Crime Prevention Council）所共同建構一套有助於防禦詐騙的產品和工具，包括 ScamShield 幫助熱線（可撥打 1799）、ScamShield 應用程式（適用於 iPhone 和 Android）、及提供一系列反詐騙資源的網站（www.scamshield.gov.sg）以及 WhatsApp 和 ScamShield 上的 ScamShield 警報社交頻道。並於 2024 年 9 月推出 ScamShield Suite，旨在將所有反詐騙資源整合到一個值得信賴的品牌上(https://www.scamshield.gov.sg/)（最後瀏覽日期：2024 年 9 月 21 日)。

19. Carousell 是一個透過智慧型手機及網站並進行 C2C 和 B2C 的網上拍賣平台，總部設在新加坡，成立並推出於 2012 年 5 月。Carousel 可在 iOS 和 Android 設備上使用。截至 2022 年 12 月，Carousell 的服務範圍適用於新加坡、馬來西亞、印尼、菲律賓、加拿大、澳洲、紐西蘭、香港、澳門和臺灣。

表 2-24 2021 年新加坡詐欺案件使用犯罪工具前 5 名

排名	犯罪手法	件數
1	社群媒體（Social media）	6,095
2	訊息傳遞平台（Messaging Platforms）	5,095
3	電話（phone calls）	2,883
4	其他網站（Other Websites）	2,519
5	簡訊（SMSes）	2,367

資料來源：整理自 Singapore Police Force (2022)。Annual Crime Brief 2021。Retrieved form:https://www.police.gov.sg/Media-Room/Statistics?page=2，Last viewed date：September 20, 2024.

2.2022 年新加坡警察部隊，受理合計 31,728 件詐欺犯罪報案，財損約 6.607 億元(Singapore Police Force,2023)。

(1)發生數前 5 名

第 1 名釣魚簡訊詐欺：發生數 7,097 件；財損 1,650 萬元；詐欺者常利用各種通訊軟體（特別是應用程式內通話，例如 WhatsApp）、簡訊和應用程式內聊天訊息與被害人進行接觸。第 2 名假求職詐欺：發生數 6,492 件；財損 1.174 億元；詐欺者常利用包括 Telegram 和 WhatsApp 與被害人進行接觸。第 3 名網路購物詐欺：發生數 4,762 件；財損 2,130 萬元；詐欺者常利用包括 Carousell、Facebook 和蝦皮（Shopee）與被害人進行接觸。第 4 名假投資詐欺：發生數 3,108 件；財損 1.983 億元；詐欺者常利用包括 Instagram、Facebook 和 Telegram 與被害人進行接觸。第 5 名假交友詐欺：發生數 2,106 件；財損 880 萬元；詐欺者常利用電話和 WhatsApp 與被害人進行接觸。（如表 2-25）。

表 2-25 2022 年新加坡詐欺案件發生數前 5 名（含財損）

排名	犯罪手法	件數	財損（新加坡幣/萬元）
1	釣魚簡訊詐欺	7,097	1,650
2	假求職詐欺	6,492	11,740
3	網路購物詐欺	4,762	2,113
4	假投資詐欺	3,108	19,983
5	假交友詐欺	2,106	880

資料來源：整理自 Singapore Police Force (2023)。Annual Scams and Cybercrime Brief 2022。Retrieved form:https://www.police.gov.sg/Media-Room/Statistics?page=2，Last viewed date：September 20, 2024.

(2)使用犯罪工具前 5 名

第 1 名：訊息傳遞平台（Messaging Platforms）7,599 件。第 2 名：社群媒體（Social media）7,539 件。第 3 名：網路購物平台（online shopping platforms）4,818 件。第 4 名：電話（phone calls）3,602 件。第 5 名：簡訊（SMSes）2,625 件。（如表 2-26）。

表 2-26 2022 年新加坡詐欺案件使用犯罪工具前 5 名

排名	犯罪手法	件數
1	訊息傳遞平台（Messaging Platforms）	7,599
2	社群媒體（Social media）	7,539
3	網路購物平台（online shopping platforms）	4,818
4	電話（phone calls）	3,602
5	簡訊（SMSes）	2,625

資料來源：整理自 Singapore Police Force (2023)。Annual Scams and Cybercrime Brief 2022。Retrieved form:https://www.police.gov.sg/Media-Room/Statistics?page=2，Last viewed date：September 20, 2024.

3.2023 年新加坡警察部隊,合計受理 46,563 件詐欺犯罪報案,財損約 6.518 億元(Singapore Police Force ,2024)。

(1)發生數前 5 名

第 1 名假求職詐欺：發生數 9,914 件；財損 1.357 億元；詐欺者常利用包括 WhatsApp 和 Telegram 與被害人進行接觸。第 2 名網路購物詐欺：發生數 9,783 件；財損 1,390 萬元；詐欺者常利用包括 Facebook、Carousell 和 Telegram 與被害人進行接觸。第 3 名假交友詐欺：發生數 6,859 件；財損 2,310 萬元；詐欺者常利用包括電話和 WhatsApp 與被害人進行接觸。第 4 名釣魚簡訊詐欺：發生數 5,938 件；財損 1,420 萬元；詐欺者常利用各種通訊軟體（特別是應用程式內通話，例如 WhatsApp）、簡訊和應用程式內聊天訊息與被害人進行接觸。與被害人進行接觸。第 5 名假投資詐欺：發生數 4,030 件；財損 2.045 億元；詐欺者常利用包括 Facebook、Telegram 和 Instagram 與被害人進行接觸（如表 2-27）。

表 2-27 2023 年新加坡詐欺案件發生數前 5 名（含財損）

排名	犯罪手法	件數	財損（新加坡幣/萬元）
1	假求職詐欺	9,914	13,570
2	網路購物詐欺	9,783	1,390
3	假交友詐欺	6,859	2,310
4	釣魚簡訊詐欺	5,938	1,420
5	假投資詐欺	4,030	20,450

資料來源：整理自 Singapore Police Force (2024)。Annual Scams and Cybercrime Brief 2023。Retrieved form:https://www.police.gov.sg/Media-Room/Statistics?page=2，Last viewed date：September 20, 2024.

(2)使用犯罪工具前 5 名

第 1 名：社群媒體（Social media）13,725 件。第 2 名：訊息傳遞平台（Messaging Platforms）12,368 件。第 3 名：電話（phone calls）7,196 件。第 4 名：網路購物平台（online shopping platforms）4,893 件。第 5 名：其他網站（Other Websites）1,677 件（如表 2-28）。

表 2-28 2023 年新加坡詐欺案件使用犯罪工具前 5 名

排名	犯罪手法	件數
1	社群媒體（Social media）	13,725
2	訊息傳遞平台（Messaging Platforms）	12,368
3	電話（phone calls）	7,196
4	網路購物平台（online shopping platforms）	4,893
5	簡訊（SMSes）	1,677

資料來源：整理自 Singapore Police Force (2024)。Annual Scams and Cybercrime Brief 2023。Retrieved form:https://www.police.gov.sg/Media-Room/Statistics?page=2，Last viewed date：September 20, 2024.

4.2024 年新加坡警察部隊，合計受理 51,501 件詐欺犯罪報案，財損約 11 億元(Singapore Police Force ,2025)。

(1)發生數前 5 名

第 1 名網路購物詐欺：發生數 11,665 件；財損 1,750 萬元；詐欺者常利用包括 Facebook、Carousell 和 Telegram 與被害人進行接觸。第 2 名假求職詐欺：發生數 9,043 件；財損 15,620 萬元；詐欺者常利用包括 WhatsApp 和 Telegram 與被害人進行接觸。第 3 名釣魚簡訊詐欺：發生數 8,552 件；財損 5,940 萬元；詐欺者常利用各種通訊軟體（特別是應用程式內通話，例如 WhatsApp）、簡訊和應用程式內聊天訊息與被害人進行接觸。與被害人進行接觸。第 4 名假投資詐欺：發生數 6,814 件；財損 32,070 萬元；詐欺者常利用包括 Facebook、Telegram 和 Instagram 與被害人進行接觸。第 5 名假交友詐欺：發生數 4,179 件；財損 1,360 萬元；詐欺者常利用包括電話和 WhatsApp 與被害人進行接觸（如表 2-29）。

表 2-29 2024 年新加坡詐欺案件發生數前 5 名（含財損）

排名	犯罪手法	件數	財損（新加坡幣/萬元）
1	網路購物詐欺	11,665	1,750
2	假求職詐欺	9,043	15,620
3	釣魚簡訊詐欺	8,552	5,940
4	假投資詐欺	6,814	32,070
5	假交友詐欺	4,179	1,360

資料來源：整理自 Singapore Police Force (2025)。Annual Scams and Cybercrime Brief 2024。Retrieved form: https://www.police.gov.sg/Media-Hub/Statistics?type=Type&year=2025&month=All%20Months&keyword=，Last viewed date：October 29, 2025.

(2)使用犯罪工具前 5 名

第 1 名：訊息傳遞平台（Messaging Platforms）15,145 件。第 2 名：社群媒體（Social media）14,991 件。第 3 名：電話（phone calls）6,739 件。第 4 名：網路購物平台（online shopping platforms）5,079 件。第 5 名：其他網站（Other Websites）2,056 件（如表 2-30）。

表 2-30 2024 年新加坡詐欺案件使用犯罪工具前 5 名

排名	犯罪手法	件數
1	訊息傳遞平台（Messaging Platforms）	15,145
2	社群媒體（Social media）	14,991
3	電話（phone calls）	6,739
4	網路購物平台（online shopping platforms）	5,079
5	簡訊（SMSes）	2,056

資料來源：整理自 Singapore Police Force (2025)。Annual Scams and Cybercrime Brief 2024。Retrieved form: https://www.police.gov.sg/Media-Hub/Statistics?type=Type&year=2025&month=All%20Months&keyword=，Last viewed date：October 29, 2025.

(二)防制策略

1.成立反詐欺指揮部（Anti-Scam Command, ASCom）

(1)為了在各種反詐欺單位之間實現更大的協同效應，新加坡警隊商業事務部（CAD）於 2021 年 3 月 22 日成立了反詐欺指揮部（ASCom），該指揮部係由一個反詐欺中心(類似臺灣 165 專線)、三個反詐欺調查外勤隊所組成，並負責督導新加坡七個地方警署(等同臺灣地方警察局)的詐欺打擊小組。

(2)反詐欺指揮部（ASCom）整合了打詐領域的專業知識，強化在調查、情報、詐欺干預、執法政策及利益相關者參與等範圍相關策略及活動之管理，並與 SSTs 密切合作，透過聯合調查及執法行動來應對與解決涉及跨區或跨國詐欺案件。

(3)反詐欺指揮部（ASCom）另與當地電信公司密切合作，終止被用於詐欺的行動電話號碼，以及與社群媒體平台與網路電商合作，下架可疑帳戶及廣告。從 2022 年 1 月到 6 月，終止了超過 1,600 個本地行動電話號碼，並刪除了超過 2,500 個可疑的線上帳戶名或廣告。在同一時期，ASC 還提交了超過 13,200 個被認為用於詐欺的 WhatsApp 帳戶進行審查和刪除。

(4)自從 2022 年 3 月成立反詐欺指揮處（ASCom）後，已將其合作夥伴關係擴展到超過 90 家機構，包括新加坡本地及外國銀行、信用卡/金融卡安全組織、金融科技公司、加密貨幣業者及提供匯款服務業者等，俾利迅速凍結帳戶及追回資金，以減少受詐欺者之損失，依據反詐欺中心（ASCom）的 2023 年上半年度報告（新加坡警察部隊，2023），計凍結了 9,000 多個銀行帳戶，並追回約 5,080 萬。

(5)自 2022 年 7 月 25 日起，反詐欺指揮處（ASCom）邀請星展銀行（Development Bank of Singapore,簡稱：DBS）、華僑銀行（Oversea-Chinese Banking Corporation,簡稱：OCBC）、大華銀行（United Overseas Bank,簡稱：UOB）、渣打銀行（Standard Chartered Bank,簡稱：SCB）、匯豐銀行（The Hongkong and Shanghai Banking Corporation,簡稱：HSB）及聯昌國際（Commerce International Merchant Bankers,簡稱：CIMB）等新加坡六大銀行派員進駐一同辦公，積極加強與警方的即時協調以進行調查工作、追查資金流向以及凍結涉案的銀行帳戶，使新加坡警察部隊（SPF）能夠利用新加坡數位身分證（Singpass）[20]的欺騙分析能力來識別並標記 Singpass 帳戶中的異常活動，且能更快速

20. Singpass 是新加坡居民可信任的數位身分，可以輕鬆安全連線辦理 1,700 多項政府及民營機構的網路與實體服務。用戶可以使用改良版 Singpass 登入以使用各種數位服務、在進行場外交易時進行身份驗證，並以數位方式簽署文件等多項功能。

凍結銀行帳戶，以及與銀行分享資訊，進而阻止受害者匯款至歹待指定帳戶。ASCom 識別了 800 多名不知情的詐欺受害者，成功阻止超過 500 萬的潛在損失。

(6)反詐欺指揮處（ASCom）專注於前端介入識別並警告受害者，利用技術來增強其偵測能力。反詐欺指揮處（ASCom）與華僑銀行（OCBC）、大華銀行（UOB）及星展銀行（DBS）合作，進行自動化資訊共享、資訊處理及向詐欺受害者發送警告簡訊。許多民眾在收到警方的警告簡訊並建議他們立即停止進一步轉帳匯款後，才發現自己是詐欺受害者。2023 年上半年度已經發送了超過 6,900 則警告簡訊，提醒超過 5,700 名受害者，成功阻止了超過 3900 萬星幣的潛在損失。

(7)ASC 與其他防制詐欺相關平台及業者密切合作，如本地電信公司及線上購物平台，計有超過 3,700 個行動電話號碼與超過 1 萬 300 個 WhatsApp 號碼被認為與詐欺活動相關，並提交終止其使用；另有涉嫌詐欺的 1,500 多個線上假帳號及廣告已被刪除。

2.簡訊實名註冊制(SMS Sender ID Registry,「SSIR」)

隨著詐欺簡訊的激增，新加坡資訊通信媒體發展局(INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY,IMDA)於 2022 年 3 月開始推行實施簡訊實名登記制，此為自願性登記，提供相關企業單位或政府部門等組織可以進行簡訊實名登記，以防止其組織名稱遭詐欺簡訊冒用，但民眾仍然有可能受到未登記實名之簡訊詐欺(例如未進行實名登記之組織或不屬於任何組織之簡訊)。因此，為進一步防止民眾遭詐欺，自 2023 年 1 月 31 日開始，所有未經實名認證之簡訊，將會被標注為「可疑詐欺 (Likely-SCAM)」

3.反詐欺簡訊過濾方案(SMS anti-scam filtering solution)

自 2022 年 10 月開始實施，要求行動網絡運營商業者(Mobile Network Operators, MNO ）將網絡中的簡訊發送至消費者之前，使用行動網路防詐欺過濾器及機器閱讀技術識別、過濾及排除潛藏有詐欺網站的惡意鏈接，以保護新加坡消費者。

4.ScamShield 手機應用程式（ALLEN & GLEDHILL,2023）

(1) ScamShield 手機應用程式是由新加坡「國家犯罪預防委員會」(National Crime Prevention Council)與「政府科技局」(Government Technology Agency)，以及新加坡警察部隊(SPF ）合作開發，該應用程式可以識別並過濾詐欺簡訊，並封鎖被認證為詐欺相關電話號碼的來電。這兩項功能減少了詐欺分子接觸可能受害者的機會。此外，該應用程式還允許用戶檢舉詐欺訊息，並接收有關近期常見詐欺的警告訊息。

(2)該應用程式於 2020 年 11 月 20 日上線後，已被用戶下載超過 60 萬次、超過 740 萬則簡訊被檢舉為潛在詐欺訊息，並封鎖了超過 7 萬個涉及詐欺的電話號碼。

(3)主要功能

A.詐欺來電偵測

該應用程式使用已知詐欺電話的資料庫來識別及標記詐欺來電，並利用使用者提供的廣泛資訊不斷更新與改善資料庫內容。

B.詐欺簡訊過濾

ScamShield 也能利用人工智慧進行識別、過濾及封鎖詐欺簡訊，包括一般簡訊及 Whats App 訊息。

C.即時詐欺警報

該應用程式提供關於新詐欺案、新興詐欺趨勢及潛在威脅的即時警報。使用者將收到相關通知，俾利隨時瞭解並謹慎應對最新的詐欺活動。

D.檢舉詐欺

使用者可以直接通過該應用程式檢舉詐欺來電、簡訊及可疑活動。這些檢舉有助官方單

位追蹤及調查詐欺案件，提高應用程式的整體功效。

E. 來電阻擋與個人封鎖清單：

ScamShield 允許使用者封鎖與詐欺有關的特定電話號碼。此外，使用者還可以建立個人封鎖清單，自訂希望封鎖的號碼。

F. 詐欺統計與資訊：

提供有關新加坡詐欺案件的整體統計數據及資訊，令民眾能瞭解國內詐欺活動的情形及性質。

(4)「Whoscall」與「ScamShield」差異如下：

A.不同區域性

Whoscall 是一個來電辨識應用程式，在多個國家包括新加坡都有提供。它提供來電者身分的資訊，讓使用者能夠封鎖不想要的來電；另 ScamShield 則是專門針對新加坡所開發之反詐軟體，目的在於解決在地所面臨的詐欺問題，並提供符合當地情境的功能。

B.詐欺偵測

Whoscall 提供一般的來電辨識及阻擋垃圾來電（spam call）功能；而 ScamShield 則專注於識別與阻擋詐欺來電及簡訊，利用已知詐欺電話與模式的全面性資料庫，提供民眾專門針對詐欺的保護。

C.詐欺檢舉

ScamShield 允許使用者直接通過程式檢舉詐欺來電及簡訊，有助於系統的整體防詐成效，並協助政府追蹤與調查詐欺案件。而 Whoscall 則著重於提供來電資訊及封鎖不想要的來電，並未特別強調詐欺檢舉功能。

D.政府支持

ScamShield 是新加坡政府的一項官方計畫，由國家犯罪預防委員會與政府科技局政府公開產品部門，以及新加坡警察部隊共同開發，該程式有政府資源支持，以打擊詐欺及確保民眾安全；而 Whoscall 則是由私人公司開發的商業來電辨識應用程式。

5.強化打擊詐欺執法行動

(1)針對當地詐欺及洗錢嫌犯繼續採取強硬的反詐欺執法行動，星國警方於 2022 年進行 20 餘次全島性反詐欺執法行動，並針對投資詐欺、就業詐欺及將 Singpass 帳戶（星國數位身分認證）出售給詐欺分子等進行取締掃盪。

(2)2023 年 3 月至 5 月，新加坡警方進行了兩次全島執法行動，掃盪了 8 家手機店業者、偵訊了 16 名手機店業主及員工，並停用了超過 1,900 個電話號碼。詐欺嫌犯利用註冊的預付費 SIM 卡作為非法活動的匿名通訊管道，如非法放貸、詐欺及賣淫等，超過 110 名手機用戶因涉嫌非法註冊 SIM 卡而接受調查。

6.修法加強打擊詐欺車手

(1)2020 年至 2022 年間，新加坡警方查緝了超過 19,000 名車手，但最終被起訴的案件不到 250 起。因此，於 2023 年 4 月新加坡智慧國及數位政府工作團（Smart Nation and Digital Government Group, SNDGG）及內政部針對此問題，將對「貪污、販毒及其他重大犯罪所得利益沒收法」（Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act,簡稱：CDSA）與「電腦濫用法」（Computer Misuse Act,簡稱：CMA）進行修法，以加強對車手之查緝。這些修改已於 2023 年底生效，賦予新加坡警方更有效地打擊車手及濫用 Singpass 進行詐欺，以及應對其他犯罪的權力。

(2)修法之目的即在於讓執法機關更容易起訴罪責較低之車手，因為目前只有證明車手知情或有合理理由相信其銀行帳戶交易資金與犯罪行為有關時，才能起訴車手，但由於難以證明車手犯罪意圖，導致警方查緝的車手人數與最後實際遭起訴之數量顯不相當。

(3)修法之重點摘要如下：

A.增加魯莽(Rash)及過失(Negligent)的洗錢罪行：

魯莽洗錢是指一個人儘管懷疑資金的非法來源，卻魯莽地進行交易。過失洗錢是指一個人不顧明顯的危險訊號繼續進行交易。

B.擴大洗錢責任範圍：

包括協助他人保留犯罪所得，例如允許他人使用、操作或控制其帳戶，卻未能採取相對之合理保護或審查措施。

C.增加金錢裁罰：

魯莽洗錢罪將面臨最高 25 萬的罰款或五年監禁，或兩者併罰。 過失洗錢罪將被處以最高 15 萬的罰款或三年監禁，或兩者併罰。協助他人保留犯罪行為所得利益的罪名最高可處以最高 50,000 元的罰款或三年監禁，或兩者併罰。

（三）防制成效

本研究綜整新加坡警察部隊(Singapore Police Force)2025 年 2 月 25 日公佈，「2024 年度詐欺與網路犯罪簡報」（Annual Scams and Cybercrime Brief 2024）(Singapore Police Force,2025)，有關新加坡警察部隊及政府各部門共同打擊詐欺和網路犯罪相關措施，摘述如下：

1.立法與制度強化面向

(1)修訂反洗錢與電腦濫用相關法規：2023 年修正《貪污、毒品販運與其他嚴重犯罪法》（CDSA）與《電腦濫用法》（CMA），2024 年 2 月生效，新增打擊人頭帳戶與濫用 Singpass 行為罪名，並由量刑諮詢小組制定嚴格刑期指引。

(2)刑事化 SIM 卡濫用行為：2024 年 4 月通過《執法及其他事項法案》（LEOM），修訂《雜項罪行法》，明定轉售或代註冊本地 SIM 卡屬犯罪，自 2025 年 1 月起施行。

(3)施行《網路犯罪危害法》（OCHA）：2024 年起分階段落實，要求社群平臺與電商主動移除詐欺內容。

(4)通過《防制詐欺法案》（Protection from Scams Bill）：2025 年起實施，授權警方可對疑似受騙者帳戶發布交易限制令。

2.警察執法與科技偵防面向

(1)成立「反詐指揮中心」（ASCom）：整合各警區打詐單位並導入人工智慧分析。

(2)開發「詐欺分析與戰術介入系統」（SATIS）：與政府科技局合作，2024 年攔阻 57,700 組手機號碼、40,500 組 WhatsApp 帳號及 44,900 個詐欺網站。

(3)全島聯合執法行動：2024 年調查 8,000 名詐欺者與人頭帳戶持有人，起訴 660 人。

(4)打擊 SIM 卡濫用與非法 OTP 服務：查獲 31,000 張 SIM 卡，逮捕 13 名嫌犯。

(5)凍結與追回詐欺資金：凍結 21,000 個帳戶，追回 1.82 億新幣。

3.跨國合作與資產追贓面向

(1)擴大國際執法合作：2024 年破獲 16 個跨國詐欺集團，逮捕 150 名海外嫌犯。

(2)成立「FRONTIER+跨國資產追回聯盟」：與港、馬、韓、泰、馬爾地夫合作。

(3)參與國際刑警行動：封鎖 5,100 個銀行帳戶與 1,000 個虛擬資產帳戶。

(4)重大案例：2024 年追回東帝汶商業電郵詐欺案資金 5,720 萬新幣。

4.社會動員與公私協力面向

(1)推行「Project A.S.T.R.O.」警示簡訊計畫：警示 55,600 名潛在受害者，避免損失 4.2 億新幣。

(2)即時介入與勸阻機制：介入 550 起高風險轉帳案，防止 6,330 萬新幣損失。

(3)推出「ScamShield 防詐套件」：App 用戶達 118 萬、專線每日 500 通。

(4)推動「I can ACT against Scams」運動：強調 Add、Check、Tell 三步驟。
(5)企業與社區合作：與亞馬遜及商圈組織合作宣導防詐資訊。
(6)教育推廣：#XiamTheScams 遊戲吸引 51.9 萬人參與，成立志工防詐團體。

5.跨部會整合防制（WOG）面向
(1)金融管理局（Monetary Authority of Singapore,簡稱：MAS）：推動「Money Lock」資金鎖定功能及共享責任機制（簡稱：SRF）。
(2)資訊媒體發展局（Infocomm Media Development Authority,簡稱：IMDA）：提供封鎖國際來電與簡訊功能，50 萬人啟用。
(3)網路安全局（Cyber Security Agency of Singapore,簡稱：CSA）：與 Google 合作「加強詐欺防護計畫」（EFP），阻止 160 萬次惡意應用安裝。
(4)開放政府產品局（Open Government Products,簡稱：OGP）：統一政府簡訊代碼「gov.sg」，升級 ScamShield 應用程式。
(5)中央公積金局（Central Provident Fund Board,簡稱：CPFB）：下修提款上限至每日 5 萬新幣，導入提款鎖與冷卻期制度。

6.整體策略特色與成效
(1)展現「警政主導、法制支撐、科技偵測、公私協力」四大特徵。
(2)2024 年追回 1.82 億新幣、預防損失 4.8 億新幣。
(3)建立打詐五面向五層防制架構。
(4)全政府（WOG）合作模式確保跨部會協調與民間參與，提升防制韌性。

（四）小結

新加坡近年詐欺與網路犯罪呈加速擴張態勢，案件量與財損同步上升，且手法明顯往社群媒體與即時通訊平臺移動。依新加坡警察部隊（Singapore Police Force, SPF）之官方簡報資料，受理報案自 2021 年之 23,933 件，增至 2024 年之 51,501 件，財損亦由約 6.32 億新幣攀升至約 11 億新幣。案件型態方面，假求職、網路購物、釣魚簡訊、假投資與假交友長期位居前段；傳播與接觸管道則由電話與簡訊逐步擴展至社群與訊息傳遞平臺，例如 Facebook、Instagram、Carousell、Telegram 與 WhatsApp 等。工具面統計亦顯示，自 2022 年起訊息傳遞平臺與社群媒體的涉案量持續走高，2023 年與 2024 年更分居第一或第二位，反映詐欺生態之數位化、去中心化與跨平臺化。本研究依打詐五面向整理新加坡於 2021－2024 年的防制作為與制度建構，並據以提出整體評析如次。

1.識詐面向

新加坡在識詐策略上以「官方科技工具＋分眾傳播」為主軸，透過行動應用與風險提示縮短受害者從接觸到警覺之時間差。由國家犯罪預防委員會與政府科技局攜手 SPF 推出之 ScamShield 應用程式，能辨識與過濾詐欺簡訊、封鎖可疑來電，並提供即時詐欺警報與檢舉機制；自 2020 年底上線以來，累計下載已逾六十萬次，使用者回報之潛在詐欺簡訊逾七百四十萬則，封鎖涉及詐欺之電話號碼超過七萬個。警政宣導同步以「I can ACT against Scams」口號推動日常化的風險溝通，並結合社群、廣播及校園等多層通道強化觸及。從犯罪樣態觀之，2021 年至 2024 年間，假求職與假投資分別在景氣循環與網路投資氛圍下成為高風險類別；釣魚簡訊則在多年度內持續列居前五，顯示以裝置端提醒、郵件與簡訊內容之可見化警示，對於提升民眾面對不明連結與陌生交涉之防禦直覺，具有關鍵效果。整體而言，新加坡將識詐定位為第一道制度化防線，結合官方工具與社會動員，使民眾在平臺化社會中維持「即時辨識、快速求證、主動通報」的日常能力。

2.堵詐面向

堵詐工作著眼於通訊端與內容端之前置阻斷，核心機制為簡訊實名註冊與網路過濾

管理。資訊通信媒體發展局（IMDA）自 2022 年 3 月實施 SMS Sender ID Registry（SSIR），允許政府機關與企業進行發信實名登記，以防詐欺訊息冒用合法名義；並自 2023 年 1 月 31 日起，對未經實名之簡訊一律標示「Likely-SCAM」，在終端顯著提示風險。自 2022 年 10 月起，行動網路經營者落實「反詐簡訊過濾方案」，於訊息抵達消費者前，以機器閱讀與惡意連結指紋等技術進行篩檢與阻擋，降低釣魚網站觸達機率。在平臺合作上，警方結合電信公司、社群與電商通報機制，對涉詐電話號碼、WhatsApp 帳號、可疑販售頁與廣告採取快速下架或封鎖。從 2021 年至 2024 年各年度工具排名可見，社群與訊息平臺持續成為主要載體，堵詐措施因而轉向管道及內容管理的雙軌配置，以制度化標記與前置過濾降低受害暴露面。

3.防詐面向

防詐層面以法制強化與部門合作為支柱，目的在於透過明確義務與裁罰框架，建立可執行的前端防護網。其一，修法針對車手與人頭帳戶加重處罰，並納入魯莽與過失形態之洗錢罪，使「明知」「重大可非難之疏失」皆得提訴；其二，透過制度要求平臺與電商對涉詐內容與廣告採取主動性處置，包含身份驗證、廣告審查與疑似詐欺資訊之即時刪除；其三，針對 SIM 卡濫用推動刑事化規範，杜絕匿名通信工具作為詐欺基礎設施；其四，配合 ScamShield 之官方生態，將警示、回報與教育置於同一防制場域，形成可追溯、可升級之前端防護。整體觀之，防詐的制度設計強調將「業者注意義務」與「身分與內容驗證」及「行政與刑事裁量」相互耦合，使平臺端與通訊端成為可實施的第一線守門人。

4.阻詐面向

阻詐之要旨在於即時凍結與追償金流，透過跨機構聯防降低損失擴散。商業事務部於 2021 年成立反詐欺指揮部（Anti-Scam Command, ASCom），統整反詐欺中心與地方警署打詐小組，並與本地主要銀行與金融科技業者進駐合作，形塑「即時偵測—即時凍結—即時通報」的金流防線。2022 年上半年，ASCom 已終止逾 1,600 個本地行動電話號碼、刪除逾 2,500 個線上可疑帳號或廣告，另就逾 13,200 個 WhatsApp 可疑帳號提請平臺處理；2023 年上半年凍結銀行帳戶數逾 9,000 個、追回約 5,080 萬新幣，並以警示簡訊介入潛在被害交易、挽回損失約 3,900 萬新幣；2024 年進一步擴大凍結與追回規模，總計凍結帳戶達 2.1 萬個並追回約 1.82 億新幣。阻詐策略亦延伸至交易限制及資金鎖定等銀行端前置控管，包括調降單日提款或單次匯款上限、限制夜間或即時跨行匯款，以創造人工覆核與風險評估之時間窗。整體而言，阻詐作為以警銀合作為核心，結合裝置端與平臺端的高風險交易提示，使資金外流於最短時間內受控。

5.懲詐面向

懲詐策略兼顧島內掃蕩、平臺執法與跨境合作，旨在透過持續偵辦與司法制裁提升犯罪代價。警方於 2022 年推動多次全島性行動，針對投資詐欺、就業詐欺與濫用 Singpass 等態樣展開偵處；2023 年進一步查緝非法註冊與流通之預付費 SIM 卡，停用逾 1,900 個涉案號碼，並對涉嫌非法註冊者展開調查。配合法制調整後，針對「協助他人保留犯罪所得」之行為，加重處罰至罰金與徒刑並行，透過量刑指引提升裁判一致性與威懾效果。懲詐面亦結合國際執法合作與跨境資產追償，警方在多起行動中同步封鎖涉案銀行與虛擬資產帳戶，並以案件合作機制追討海外被轉移之資金。其整體配置，呈現自切斷犯罪運作之關鍵環節、金流圍堵到司法追訴之整體防制機制。

6.綜合評析

綜合觀察，2021 年至 2024 年間，新加坡已在打詐五面向建立起高度整合的防制架構。若從情境犯罪預防理論觀之，該體系充分體現「改變犯罪機會結構」的核心理念。識詐面以 ScamShield 與分層宣導建構社會化的風險感知環境，藉提升民眾警覺性與資訊辨識力增加犯罪者的施行難度；堵詐面透過簡訊實名制（SSIR）與過濾技術在通訊前端封

鎖可疑流量，有效提高詐欺行為之技術成本；防詐面則藉修法與平臺責任化機制，將身分驗證、內容監理與交易審查納入制度性防線，降低犯罪可行性；阻詐面以反詐欺指揮部（ASCom）為核心，整合警銀即時凍結、Money Lock 與 SRF 等資金控管機制，削弱犯罪報酬並強化資金追蹤；懲詐面結合本地偵查、平臺下架與跨國合作追償，移除重複犯行之誘因。整體而言，新加坡防制策略展現「增加努力、提升風險、降低報酬、移除藉口」的多層防禦精神，以「警政主導、法制支撐、科技偵測、公私協力」為核心，形成即時、可持續的防詐策略體系。惟仍面臨跨境追訴限制、平臺責任與用戶隱私平衡及弱勢族群防詐教育推進等挑戰。整體發展顯示，新加坡已建立一套兼具制度化與科技化的情境防詐模式，對臺灣推動「打詐 2.0」下之跨域合作與防制政策具有重要借鏡價值。

三、澳洲

本研究依據澳洲國家反詐欺中心，蒐集 Scamwatch[21]、Report Cyber[22]、AFCX[23]、IDCARE[24]、ASIC[25]等 12 家金融組織和其他政府機構所統計近四年（2021-2024）詐欺犯罪資料 (Australian Governmen,2025) 及澳洲統計局 (ABS) (Australian Bureau of Statistics,2025)個人詐欺資料與相關防制策略分析如下。

(一)犯罪情勢

1.2021 年澳洲的金融組織和其他政府機構，合計受理 286,622 件詐欺犯罪報案，財損約 323,723,459 澳元（以下同）(Australian Governmen,2025)。

(1) 發生數前 5 名

第 1 名：網路釣魚（Phishing），報案數 71,310 件。第 2 名：威脅生命、逮捕或其他（Threats to life, arrest or other），報案數 32,426 件。第 3 名：購物詐欺（Shopping Scams），報案數 30,254 件。第 4 名：身分盜竊（Identity theft），報案數 22,354 件。第 5 名：虛假帳單（False billing），報案數 21,545 件（如表 2-31）。

表 2-31 2021 年澳洲詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	網路釣魚（Phishing）	71,310
2	威脅生命、逮捕或其他（Threats to life, arrest or other）	32,426
3	購物詐欺（Shopping Scams）	30,254
4	身分盜竊（Identity Theft）	22,354
5	虛假帳單（False Billing）	21,546

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

21.於 2002 年成立，由澳洲競爭與消費者委員會（ACCC）營運，該單位之除提供民眾識詐、舉報詐欺犯罪外，亦與其他政府部門、執法單位及私人單位等進行情報分享及合作，並在 2022 年國家詐欺反詐騙中成立後納入該中心(https://www.scamwatch.gov.au/)（最後瀏覽日期：2024 年 10 月 1 日)。

22.澳洲網路報案網路犯罪之工具(https://www.cyber.gov.au/report-and-recover/report) 。

23.澳洲金融犯罪交換網路(Australian Financial Crimes Exchange,簡稱 AFCX) 係獨立之非營利組織，由 4 大私人銀行成立，為公私部門間協調金融和網絡犯罪情報之主要管道，似臺灣之財團法人金融法制暨犯罪防制中心，下設有詐欺報告交流平臺(FRX)。

24.澳洲及紐西蘭身分認證及網路服務，成立目的是提供個人面對身分認證及網路安全問題時的幫助，屬非營利組織(https://www.idcare.org/about-idcare/what-is-idcare) （最後瀏覽日期：2024 年 10 月 1 日)。

25.澳洲證券及投資委員會(Australian Securities & Investments Commission,簡稱 ASIC)1998 年成立，類似臺灣金管會之澳洲獨立機關，依法獨立對公司、投資行為、金融產品和服務行使監管職能。

(2) 財損數前 5 名

第 1 名：投資詐欺（Investment Scams），177,184,295 元。第 2 名：約會和浪漫詐欺（Dating &Romance Scams），56,175,428 元。第 3 名：虛假帳單（False Billing），17,303,665 元。第 4 名：假冒技術支援詐欺 / IT 技術支援詐欺（IT Support Scam）[26]，16,412,258 元。第 5 名：購物詐欺（Shopping Scams），15,189,041 元（如表 2-32）。

表 2-32 2021 年澳洲詐欺案件財損數前 5 名

排名	犯罪手法	澳元
1	投資詐欺（Investment Scams）	177,184,295
2	約會和浪漫詐欺（Dating & Romance Scams）	56,175,428
3	虛假帳單（False Billing）	17,303,665
4	假冒技術支援詐欺 / IT 技術支援詐欺（IT Support Scam）	16,412,258
5	購物詐欺（Shopping Scams）	15,189,041

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

(3) 使用犯罪工具前 5 名

第 1 名：電話（Phone），144,603 件。第 2 名：簡訊（Text Message），67,180 件。第 3 名：電郵（Email），40,185 件。第 4 名：網路（Online），29,185 件。第 5 名：郵寄信件（Mail），2,218 件（如表 2-33）。

表 2-33 2021 年澳洲詐欺案件使用犯罪工具前 5 名

排名	犯罪手法	件數
1	電話（Phone Call）	144,603
2	簡訊（Text Message）	67,180
3	電郵（Email）	40,185
4	網路（Online）	29,185
5	郵寄信件（Mail）	2,218

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

2.2022 年澳洲的金融組織和其他政府機構，合計受理 239,239 件詐欺犯罪報案，財損約 506,674,458 元(Australian Governmen,2025)。

(1) 發生數前 5 名

第 1 名：網路釣魚（Phishing），報案數 74,575 件。第 2 名：購物詐欺（Shopping Scams），報案數 28,535 件。第 3 名：虛假帳單（False Billing），報案數 27,489 件。第 4 名：身分盜竊（Identity Theft），報案數 16,213 件。第 5 名：假冒技術支援詐欺 / IT 技術支援詐欺（IT Support Scam），報案數 11,792 件（如表 2-34）。

26.詐騙者假冒微軟、Telstra、Apple 等公司技術人員，謊稱你的電腦中毒或帳號異常，誘導安裝遠端控制軟體或支付虛構修復費用。

表 2-34 2022 年澳洲詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	網路釣魚（Phishing）	74,575
2	購物詐欺（Shopping Scams）	28,535
3	虛假帳單（False Billing）	27,489
4	身分盜竊（Identity Theft）	16,213
5	假冒技術支援詐欺 / IT 技術支援詐欺（IT Support Scam）	11,792

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

(2) 財損數前 5 名

第 1 名：投資詐欺（Investment Scams）315,286,614 元。第 2 名：約會和浪漫詐欺（Dating & Romance Scams）40,675,825 元。 第 3 名：虛假帳單（False Billing），25,312,185 元。第 4 名：網路釣魚（Phishing），24,617,192 元。第 5 名：假冒技術支援詐欺 / IT 技術支援詐欺（IT Support Scam），21,744,454 元（如表 2-35）。

表 2-35 2022 年澳洲詐欺案件財損數前 5 名

排名	犯罪手法	澳元
1	投資詐欺（Investment Scams）	315,286,614
2	約會和浪漫詐欺（Dating & Romance Scams）	40,675,825
3	虛假帳單（False Billing）	25,312,185
4	網路釣魚（Phishing）	24,617,192
5	假冒技術支援詐欺 / IT 技術支援詐欺（IT Support Scam）	21,744,454

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

(3) 使用犯罪工具前 5 名

第 1 名：簡訊（Text Message），79,835 件。第 2 名：電話（Phone Call），63,821 件。第 3 名：電郵（Email），52,159 件。 第 4 名：網路（Online），37,178 件。第 5 名：郵寄信件（Mail），2,342 件（如表 2-36）。

表 2-36 2022 年澳洲詐欺案件使用犯罪工具前 5 名

排名	犯罪手法	件數
1	簡訊（Text Message）	79,835
2	電話（Phone Call）	63,821
3	電郵（Email）	52,159
4	網路（Online）	37,178
5	郵寄信件（Mail）	2,342

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

3.2023 年澳洲的金融組織和其他政府機構，合計受理 301,765 件詐欺犯罪報案，財損約 476,778,116 元(Australian Governmen,2025)。

(1) 發生數前 5 名

第 1 名：網路釣魚（Phishing），報案數 108,626 件。第 2 名：虛假帳單（False Billing），報案數 39,587 件。第 3 名：購物詐欺（Shopping Scams），報案數 32,877 件。第 4 名：身分盜竊（Identity Theft），報案數 19,896 件。第 5 名：假冒技術支援詐欺 / IT 技術支援詐欺（IT Support Scam）8,975 件（如表 2-37）。

表 2-37 2023 年澳洲詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	網路釣魚（Phishing）	108,626
2	虛假帳單（False Billing）	39,587
3	購物詐欺（Shopping Scams）	32,877
4	身分盜竊（Identity Theft）	19,896
5	假冒技術支援詐欺 / IT 技術支援詐欺（IT Support Scam）	8,975

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

(2) 財損數前 5 名

第 1 名：投資詐欺（Investment Scams）291,868,811 元。 第 2 名：約會和浪漫詐欺（Dating & Romance Scams）34,344,656 元。 第 3 名：虛假帳單（False Billing），27,991,378 元。第 4 名：網路釣魚（Phishing），25,898,114 元。第 5 名：工作和就業詐欺（Jobs And Employment Scams），24,393,665 元（如表 2-38）。

表 2-38 2023 年澳洲詐欺案件財損數前 5 名

排名	犯罪手法	澳元
1	投資詐欺（Investment Scams）	291,868,811
2	約會和浪漫詐欺（Dating & Romance Scams）	34,344,656
3	虛假帳單（False Billing）	27,991,378
4	網路釣魚（Phishing）	25,898,114
5	工作和就業詐欺（Jobs And Employment Scams）	24,393,665

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

(3) 使用犯罪工具前 5 名：

第 1 名：簡訊（Text Message），109,615 件。 第 2 名：電郵（Email），85,935 件。 第 3 名： 電話（Phone Call），55,418 件。第 4 名：網路（Online），43,208 件。第 5 名：面對面詐欺（In person ）[27]，3,614 件。（如表 2-39）。

27.在現場直接接觸受害者，常見於假慈善募款、假投資說明會或假公務人員臨檢情境。

表 2-39 2023 年澳洲詐欺案件使用犯罪工具前 5 名

排名	犯罪手法	件數
1	簡訊（Text Message）	109,615
2	電郵（Email）	85,935
3	電話（Phone Call）	55,418
4	網路（Online）	43,208
5	面對面詐欺（In person ）	3,614

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

根據澳洲統計局(Australian Bureau of Statistics,簡稱：ABS)個人詐欺資料顯示，在 2022-23 財年，有 2.5%澳洲人民(514,300 人)經歷過詐欺（民眾對詐欺行為作出回應並提供金錢或個人信息或尋求更多信息，又或者鏈接與詐欺相關的網站，則被視為經歷過詐欺）。69%經歷過詐欺的人民有通報政府機構（或被政府機構通知）。也就是說，還有大約 30%經歷過詐欺的人沒有向政府機構報案。許多沒有報案的人民，可能只有遭受少量或並沒有經濟損失，因此，詐欺報案黑數並不足代表如果這些人報案的話，整體財損將會增加 30%。還有一些被害人在 2023 年因詐欺而損失金錢，但他們還不知道自己被騙。例如：投資和愛情詐欺是長期騙局，在受害者意識到詐欺之前，通常會與詐欺者維持數月甚至數年的關係。（Australian Bureau of Statistics,2024）

4.2024 年澳洲的金融組織和其他政府機構，合計受理 249,448 件詐欺犯罪報案，財損約 318,762,688.02 元(Australian Governmen,2025)。

(1) 發生數前 5 名

第 1 名：網路釣魚（Phishing），報案數 97,831 件。第 2 名：虛假帳單（False Billing），報案數 27,045 件。第 3 名：購物詐欺（Shopping Scams），報案數 24,916 件。第 4 名：身分盜竊（Identity Theft），報案數 18,512 件。第 5 名：投資詐欺（Investment Scams），報案數 6,765 件。（如表 2-40）。

表 2-40 2024 年澳洲詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	網路釣魚（Phishing）	97,831
2	虛假帳單（False Billing）	27,045
3	購物詐欺（Shopping Scams）	24,916
4	身分盜竊（Identity Theft）	18,512
5	投資詐欺（Investment Scams）	6,765

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

(2) 財損數前 5 名

第 1 名：投資詐欺（Investment Scams）192,349,778 元。第 2 名：約會和浪漫詐欺（Dating & Romance Scams）23,561,744 元。 第 3 名：網路釣魚（Phishing），20,510,355 元。第 4 名：虛假帳單（False Billing），15,818,245 元。 第 5 名：恐嚇勒索詐欺(Threats and Extortion Scam) [28]，13,889,676 元（如表 2-41）。

表 2-41 2024 年澳洲詐欺案件財損數前 5 名

排名	犯罪手法	澳元
1	投資詐欺（Investment Scams）	192,349,778
2	約會和浪漫詐欺（Dating & Romance Scams）	23,561,744
3	網路釣魚（Phishing）	20,510,355
4	虛假帳單（False billing）	15,818,245
5	恐嚇勒索詐欺(Threats and Extortion Scam)	13,889,676

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

(3) 使用犯罪工具前 5 名：

第 1 名：電郵（Email），90,819 件。第 2 名：簡訊（Text Message），77,365 件。 第 3 名： 電話（Phone Call），41,742 件。第 4 名：網路（Online），33,544 件。第 5 名：面對面詐欺（In person ），3,245 件（如表 2-42）。

表 2-42 2024 年澳洲詐欺案件使用犯罪工具前 5 名

排名	犯罪手法	件數
1	電郵（Email）	90,819
2	簡訊（Text Message）	77,365
3	電話（Phone Call）	41,742
4	網路（Online）	33,544
5	面對面詐欺（In person ）	3,245

資料來源：整理自 Australian Government（2025）。Scam statistics。Retrieved form:https://www.nasc.gov.au/scam-statistics，Last viewed date：October 30, 2025.

根據澳洲統計局(ABS)個人詐欺資料顯示，澳洲人民詐欺盛行率從 2022-23 財年的 2.5%(514,300 人)上升到 2023-24 財年的 3.1%（675,300 人）經歷過詐欺（民眾對詐欺行為作出回應並提供金錢或個人信息或尋求更多信息，又或者鏈接與詐欺相關的網站，則被視為經歷過詐欺）。據估計，在 2023-24 財年 71%經歷過詐欺的人民有通報政府機構（或被政府機構通知），與 2022-23 年的情況類似（69%），但也仍有大約 29%經歷過詐欺的人沒有向政府機構報案，也與 2022-23 年的情況類似（30%）。這也代表仍有許多被害人沒有報案（Australian Bureau of Statistics,2025）。

28.假冒警察、稅務局、移民局或黑客，以恐嚇手段要求匯款或提供資料。

(二)防制策略

1.建置國家反詐欺中心

澳洲政府於 2023 年 7 月 1 日在 ACCC [29]內設立了國家反詐欺中心[30]，在 2023 至 2024 年預算中，澳洲政府將提供 8,650 萬元的資金，用於建構國家反詐欺中心以作為政府機構和產業之間的合作機制；建立澳洲第一個簡訊寄件者 ID 註冊表，以防止詐欺者模仿受信任的產業或政府機構寄件者 ID；推動澳洲證券和投資委員會識別和取締投資詐欺網站的工作，國家反詐欺中心的 3 個主要任務：

(1)科技與情報分享阻詐

開發可行的行動和技術方法，以促進快速蒐集詐欺情報和資訊共享服務，此新的數位功能將使詐欺情報能夠即時地與防止詐欺組織進行交換，從 2024 年下半年起有更多政府機構和關鍵企業將透過國家反詐欺中心連接和交換資料。

(2)政府與民間合作防詐

A.擴大國家反詐欺中心刪除詐欺網站能力，以確保詐欺網站在造成廣泛危害之前被刪除，同時改進 Scamwatch 檢舉服務，方便民眾更容易檢舉詐欺，從 2024 年 7 月起，澳洲人民可以快速檢舉詐欺網站，以阻止詐欺網站或詐欺廣告。

B.促進民間企業、社區組織、執法和技術服務部門與國家反詐欺中心合作，共同開發針對特定詐欺的工具和流程，亦可透過合作夥伴入口網站存取與他們相關的詐欺資訊。

C.由國家反詐欺中心組建專案融合小組，以匯集專業知識和訊息，提出創新的解決方案；該專案小組首先將關注人民受害最嚴重的投資詐欺。

D.推動國家反詐欺中心與澳洲金融犯罪交易所合作，建立詐欺情報循環與分享，支援打擊詐欺行動。

(3)加強意識和保護

A.透過以上措施，使得詐欺報案和支援服務將更加一體化，受害者將能夠更快地獲得所需的支持，並確信相關資訊正在與執法部門共享。

B.澳洲人民還將受益於針對他們的詐欺以及如何避免這些詐欺的更頻繁和一致的訊息。

C.國家反詐欺中心將協調識詐宣導活動，以確保防詐訊息一致，並對高風險社區進行有效的宣傳。

D.國家反詐欺中心整合不同防詐生態系統擁有的專業知識，以共同努力提高澳洲人民對詐欺者的防禦能力，保護公民免受犯罪集團的侵害。

2.具體反詐欺措施

澳洲國家反詐欺中心是澳洲政府承諾打擊詐欺的關鍵機制，主要目標是實現政府、執法部門和產業之間加強合作，包括與 AFCX 和其他組織的詐欺情報資訊共享，或當受害者在不知情的情況下試圖向詐欺者付款時，能即時地識別詐欺電話號碼、銀行帳戶和社交媒體帳戶，從而在發生詐欺事件時及時進行干預。以避免人民的經濟損失。隨著該中心技術建構完成，將可實現關鍵組織之間詐欺數據即時共享，預計將提高早期預防、檢測、破壞和因應詐欺的能力。另外國家反詐欺中心也與州和聯邦警察合作，為澳洲和海外的詐欺

29.澳洲競爭與消費者委員會(Australian Competition and Consumer Commission ,簡稱 ACCC) 類似臺灣消費者保護會與公平交易委員會之綜合體，為澳洲市場競爭、消費者保護以及國家基礎建設的主管機關，除提供相關企業結合之主管機關文件查詢外，ACCC 也針對媒體合併議題定期發布媒體合併指南（Media merger guidelines）以供查詢。

30.國家反詐騙中心(National Anti-Scam Centre,簡稱 NASC)係 2023 年 7 月新成立，原 ScamWatch 合併納入該中心。

調查提供資訊和轉介，並就打擊詐欺措施開展合作，以下即為澳洲國家反詐欺中心和ASIC 領導的投資詐欺專案融合小組實施的防控機制。

(1)公告防詐欺法律架構

澳洲政府於 2023 年底發布防詐欺法律架構諮詢意見，該法律架構重點關注銀行、電信和數位平台等業者的角色和責任，將為所有受監管的企業引入最低限度且一致的義務，以預防、檢測、破壞和應對詐欺犯罪，受監管的企業必須採取強而有力的措施，以應對在提供服務中的面臨的詐欺風險，如果企業未能履行其義務，將受到嚴厲處罰，最終目的在使澳洲人民成為更難詐欺的目標。

(2)銀行加強對加密貨幣交易所的控管

A.根據 2022-23 財年末的 AFCX 數據顯示，有將近 50%的詐欺損失是透過加密貨幣交易所處理的；因此，管制措施將持續限制在「高水準」。

B.控管措施可能會減少直接詐欺付款，特別是投資詐欺，並減少一些犯罪分子在澳洲活動的動機，因為轉移金融犯罪收益變得更加困難。

C.ASIC 的網站刪除服務

D.作為政府「打擊詐欺」計畫的一部分，ASIC 建立了投資詐欺網站刪除能力，並透過投資詐欺融合小組與國家反詐欺中心和合作夥伴合作，識別並刪除包含惡意網路釣魚和投資詐欺資訊的網站。

E.在投資詐欺融合細胞（fusion cell）期間，截至 2024 年 3 月 4 日止已有超過 3,500 個(Australian Securities De Investmente Commission,2024)網站被刪除。

F. ASIC 也於 2023 年 11 月推出了新的投資者警報清單(Australian Securities De Investmente Commission,2023)，向潛在投資者提供詐欺企業和網站的警告。

(3)停止呼叫(Call Stop)倡議

A.Optus[31]與 AFCX 的銀行成員共同制定了一項針對的回撥詐欺的「呼叫停止」（Call Stop）計畫(Optus,2023)，即當民眾收到一封電子郵件或簡訊，聲稱其銀行帳戶出現問題（通常是使用其帳戶進行未經授權的付款，或者有其他人登錄其帳戶），並要求民眾依詐欺集團提供的電話回撥確認。當民眾撥打該號碼，就會進入冒充銀行的詐欺集團所設定的圈套。然後，詐欺者誘騙受害者提供其帳戶的存取權限，或將錢轉入詐欺者控制的帳戶。「呼叫停止」（Call Stop）可防止民眾撥打已被識別的詐欺電話號碼，而是將通話轉接至自動訊息以警告客戶注意詐欺。「呼叫停止」（Call Stop）會將通話轉接到語音訊息，其中顯示：「您所撥打的號碼已被報告為用於詐欺活動。欲了解更多信息，請訪問optus.com.au/CallStop。然後，該呼叫將被阻止，以防止客戶被詐欺，並會清楚地向民眾表明收到的警告或威脅確實是虛假的詐欺訊息，無需採取任何措施。

B.使用轉移電話聯繫技術，將使詐欺者無法實施複雜且高財損（平均約 26.4 萬元）的投資詐欺，在融合細胞（fusion cell）期間，有 113 通電話被轉移，可能已減少數百萬元的詐欺損失。

(4)詐欺指示器工具和付款提示

A.2023 年中期，Telstra[32]和 CBA[33]宣布(Telstra Plus,2024)一項試點計畫，聯合使用詐欺指

31. 新加坡電信旗下的一家公司，自 2001 年起由新加坡電信完全擁有，目前是澳洲第二大電信供應商，僅次於澳洲電信公司。

32.澳洲電信，是澳洲最大的電訊公司，總部位於墨爾本的澳洲電信中心大廈。公司目前採取公私合營模式經營，目前在澳洲本地固網電訊市場擁有壟斷性地位，並擁有行動電話服務股權，本地消費者、商業數據服務及有線電視服務。

33.澳洲聯邦銀行（Commonwealth Bank of Australia，簡稱 CBA）是澳洲的一間主要銀行，位列澳洲四大

示器幫助客戶偵測和防止電話詐欺，詐欺指示器使 CBA 能夠確認客戶在與 CBA 進行交易時如果正在通話，即表示可能發生詐欺，從而可能使銀行檢測電話詐欺的成功率提高一倍。

B.NAB[34]還在數位銀行中導入付款提示，以幫助客戶發現潛在的危險信號，從而使客戶在八個月內減少超過 5,000 萬元的損失。

(5)電信措施

A.作為政府「打擊詐欺」計畫的一部分，澳洲通訊與媒體管理局(Australian Communications and Media Authority,簡稱：ACMA)正在實施簡訊發送者 ID 註冊表。註冊機構將保護品牌和政府機構的字母數位訊息標頭（例如「ATO」、「MyGov」或「NAB」）免遭簡訊冒充。2023 年 12 月，ACMA 啟動了註冊試點階段，該階段將與一些知名品牌和機構整合現有的寄件者 ID 保護。

B.根據《電信守則》(Australian Government,2022)，2023 年 10 月至 12 月期間，電信業者報告攔截了超過 2.467 億通詐欺電話和超過 1.067 億則詐欺簡訊(Australian Government,2024)。

C.2023 年期間，ACMA 指示多家電信業者遵守《電信準則》。一旦指示提供者遵守規定，未來如果發現違規行為（包括民事執法）的處罰將可減輕。

(6)收款人驗證技術和詐欺安全協議（Scam Safe Accord）

A.2023 年，多家銀行宣布(Commonwealth Bank of Australia,2023)推出收款人確認技術，收款人的確認可以確保人們確認他們正在將錢轉給他們想要的人，有助於減少詐欺，這可以減少受支付重新導向詐欺和冒充詐欺影響的人數。

B.2023 年 11 月，澳洲銀行業協會和國營銀行業協會宣布 (Australian Banking Association,2023)社區所有銀行、建房協會、信用合作社和商業銀行之間達成了一項詐欺安全協議，其中包括一套適用於整個行業的反詐欺措施。該協議概述了業界將投資 1 億澳元建立新的收款人確認系統，該系統將在所有澳洲銀行中推廣，在所有銀行實施時，收款人確認將對降低詐欺損失產生重大影響。

(7)2024 年減少詐欺主要活動

A.制定強制性和可執行的義務，要求銀行、電信供應商和數位平台預防、偵測、破壞和應對詐欺。

B.國家反詐欺中心將試行取締更廣泛的詐欺網站，並為澳洲人民制定檢舉詐欺網站和廣告的簡單流程。

C.第二個融合細胞將可瓦解特定類型的騙局。

D.國家反詐欺中心將有 10 個合作夥伴參與資料共享安排，並利用其可操作的情報服務來破壞詐欺並發布即時詐欺警報。

E.銀行業將推進收款人確認制度預期將可減少商業電子郵件詐欺和冒充銀行詐欺造成的損失。

F. ACMA 將擴大簡訊寄件者 ID 註冊表試點範圍，並專注於成為假冒詐欺目標的品牌。

G.ASIC 將與國家反詐欺中心合作，自動推薦投資詐欺網站以進行拆除，從而拆除更多網站。

H.國家反詐欺中心和 AFCX 反詐欺情報循環之間的資料共享將導致更快地採取行動阻止詐欺銀行帳戶，並提供更好的情報來通知參與組織的詐欺偵測和阻止。

銀行之一，總部位於雪梨。

34.澳洲國民銀行，澳洲主要金融服務銀行，位列澳洲四大銀行之一，是世界第 21 大銀行；總部位於維多利亞州的墨爾本濱海港區，在全球 10 個國家開展業務，擁有 3,500 多家分行、7000 多部自動櫃員機。

I. 與私部門、社區組織和支持服務機構合作，國家反詐欺中心將透過詐欺意識週（2024 年 8 月）以及教育和社區外展活動等活動提高人們對詐欺的認識。這將包括增強高風險群體識別和避免詐欺的能力，並增加檢舉行為。

（三）防制成效

本研究依據澳洲「打擊詐欺：國家反詐欺中心 2024 年詐欺數據和活動報告」（Targeting scams Report of the National Anti-Scam Centre on scams data and activity 2024）（Australian Competition and Consumer Commission,2025）摘述該國打擊詐欺犯罪主要措施及成效如下：

1.整體架構與策略方向

澳洲於 2024 年持續由「國家反詐欺中心（National Anti-Scam Centre,簡稱：NASC）」統籌政府、警察、通訊、金融與數位產業的防詐生態系，透過「全生態系統（whole-of-ecosystem）」防制理念，推動跨部門合作與數據共享機制，形成結合預防（prevent）、偵測（detect）、中斷（disrupt）、通報（report）、應對（respond）的立體防詐體系。該年度報告指出，澳洲詐欺通報件數為 49 萬 4,732 件，較 2023 年下降 17.8%，詐欺損失額為 20.3 億澳元，減少約 25.9%，顯示整體防制作為已產生初步成效。

2.主要防制措施與機制

(1)電信及通訊領域防制作為

澳洲通訊與媒體管理局（ACMA）持續推動《減少詐欺電話與簡訊業界守則》，並強化執行與查核。2024 年各電信業者共攔阻約 4.56 億通詐欺電話及 4.14 億則詐欺簡訊。ACMA 並完成 6 件電信業者違規調查，發出 4 項強制改進指令，以封堵詐欺通訊通道。政府另推動「簡訊發送者識別碼登錄制度（SMS Sender ID Register）」，防止冒用政府或企業名稱之假簡訊，預計於 2025 年強制實施。各大電信公司同步研發 AI 與機器學習攔截技術（如 Telstra「Cleaner Pipes」專案、TPG 智能辨識系統、Optus「Call Stop」計畫），並設立詐欺檢舉與通報機制，加強跨網絡情資交流。

(2)金融體系防詐改革

澳洲銀行公會（Australian Banking Association,簡稱：ABA）推行「Scam-Safe Accord」，導入多項詐欺阻斷與驗證技術。例如：各大銀行實施通話身分驗證（CallerCheck、CallSafe）、交易名稱比對（NameCheck、Verify）、即時警示與延遲付款措施，部分銀行如 CommBank、NAB、Westpac 亦建立「不發起號碼清單（Do-Not-Originate）」以防止冒名來電詐欺。同時，銀行與金融犯罪交換中心（AFCX）建立反詐情資迴路，實現跨行實時資訊交換，藉由行為異常分析與生物辨識技術強化對人頭帳戶及高風險交易的攔截。

(3)數位與社群媒體防制作為

2024 年 7 月，數位產業組織（Digital Industry Group Inc,簡稱：DIGI）發布《澳洲線上詐欺業界自律守則（Australian Online Scams Code）》，由 Apple、Google、Meta、TikTok、X 等平台簽署。守則涵蓋九大領域，包括封鎖與下架機制、用戶通報途徑、詐欺廣告過濾、私訊防護、執法合作與情資共享等。Meta 並與銀行及 AFCX 合作建立「詐欺情資互惠交換系統（Fraud Intelligence Reciprocal Exchange,簡稱：FIRE）」，清除 9,000 餘個詐欺頁面與 AI 假冒內容。Google 亦推出「全球詐欺訊號交換平台（Global Signal Exchange）」，強化跨界偵測與應變速度。

(4)執法與國際合作

澳洲聯邦警察（AFP）與 NASC、歐洲刑警（EUROPOL）等單位合作執行多項行動，包括「Operation NEBULAE」偵破跨國釣魚詐欺系統 LabHost、及「Operation FIRESTORM」

鎖定東南亞與東歐跨境詐欺集團。NASC 亦與外國執法單位共同分析受害資料，通知 3.7 萬名潛在被害人停止投資或尋求協助。國際層面則與新加坡政府、東協（ASEAN）會員國、英國金融犯罪單位等建立交流與能力建構合作，展現澳洲作為區域防詐領導國的角色。

(5)消費者宣導與教育

NASC 透過多元媒體推動「停止、查證、保護（Stop. Check. Protect.）」全國宣導運動，強化公眾防詐意識。2024 年該中心重新設計 Scamwatch 官方網站，並開設社群帳號，發佈近 500 則反詐資訊，觸及逾 1600 萬人次。另針對弱勢群體推出「防詐小冊（Little Book of Scams）」多語版本（含 17 種語言），並與原住民廣播電台及地方社區合作進行廣播宣導。年度「詐欺意識週（Scams Awareness Week）」主題為「分享經驗、阻止詐欺」，強調去除受害污名與鼓勵通報。

(6)被害人支持與法律改革

NASC 與 IDCARE 建立自動轉介系統，2024 年共轉介 7,670 名被害人接受客製化心理與復原協助，並主動聯絡 1,300 名受害者提供防害指引。政府同步推動《詐欺防制框架法（Scams Prevention Framework Act 2025）》，建立具法律約束力之「指定責任實體」制度，要求銀行、電信及數位平台負起防詐、偵測、通報、補償之法定義務，違反者將面臨民事罰則與賠償責任。該法亦設立統一之外部爭議解決機制，由澳洲金融申訴機構（AFCA）負責，保障被害者申訴與求償權益。

3.主要成效與評估

2024 年澳洲各界防詐措施已顯現整體改善趨勢：

(1)詐欺報案與損失金額明顯下降。

(2)網頁與假投資網站下架超過 8,000 件。

(3)電信業者封鎖數億次詐欺通訊。

(4)銀行實施多層防護機制，阻斷逾 2 億澳元可疑交易。

(5)消費者防詐意識與跨界情資共享明顯提升。

4.綜合觀察

澳洲防制詐欺政策已從「事後處罰」轉向「事前預防與即時中斷」，呈現高整合化與法制化趨勢。NASC 透過科技建設與跨域合作，實現政府、企業、民間「共治模式」；而《詐欺防制框架法》之立法，則象徵澳洲正式邁向「強制責任與賠償導向」的制度新階段。惟未來仍須持續面對跨境詐欺、AI 假冒與人頭帳戶等挑戰，並深化國際合作與社會韌性培力，以維持詐欺下降趨勢並鞏固全民防詐體系。

（四）小結

根據澳洲國家反詐欺中心彙整之 Scamwatch、Report Cyber、AFCX、IDCARE、ASIC 等 12 家金融組織與政府機構之統計（2021–2024），以及澳洲統計局（ABS）個人詐欺資料，近年澳洲詐欺犯罪持續高位運行，於不同年度呈現案量與財損結構的變動。2021 年受理 286,622 件，財損約 3.237 億澳元；2022 年受理 239,239 件、財損約 5.067 億澳元；2023 年受理 301,765 件、財損約 4.768 億澳元；2024 年受理 249,448 件、財損約 3.188 億澳元。案類分布上，2021 年發生數前五為網路釣魚（71,310 件）、威脅生命／逮捕或其他（32,426 件）、購物詐欺（30,254 件）、身分盜竊（22,354 件）、虛假帳單（21,545 件）；財損前五則以投資詐欺居首（1.7718 億），其次為約會與浪漫詐欺（5,617 萬）、虛假帳單（1,730 萬）、IT 技術支援詐欺（1,641 萬）、購物詐欺（1,518 萬）。2022 年與 2023 年同樣呈現「大

量網路釣魚＋投資詐欺高額損失」的雙峰態勢，例如 2022 年投資詐欺損失 3.1529 億、2023 年仍達 2.9187 億，顯示投資型詐欺對整體財損具有關鍵影響力；2024 年投資詐欺損失仍以 1.9235 億居首，且網路釣魚損失達 2,051 萬。犯罪工具上，2021 年以電話（144,603 件）與簡訊（67,180 件）為主；2022 年簡訊居首（79,835 件）；2023 年簡訊（109,615 件）與電郵（85,935 件）均大幅；2024 年電郵升至第一（90,819 件），簡訊次之（77,365 件），反映攻擊向度由語音與 SMS 逐步擴展至電郵與線上管道的多點突破。ABS 個人詐欺資料顯示，2022–23 財年有 2.5%（約 51.4 萬人）經歷過詐欺，其中約 69%有通報（或被通知）；2023–24 財年上升為 3.1%（約 67.5 萬人），通報率約 71%，仍有近三成未通報，意即黑數存在且不宜低估。在此脈絡下，為呈現防制邏輯之全貌，本研究依打詐五面向系統化整理澳洲近年之制度建構與執行重點。

1.識詐面向

識詐教育採多元載體並提升一致性。國家反詐欺中心（NASC）整合宣導資源，推動「Stop. Check. Protect.」核心訊息，重新設計 Scamwatch 官網並強化社群發布，擴大觸及；製作《防詐小冊》多語版本並與在地社群合作，提升高風險族群的理解與反應能力。透過年度「詐欺意識週」與常態化警示，降低民眾對釣魚連結、投資詐欺與冒名簡訊的可得性與可信度。識詐面向亦強調檢舉便利化，改版後的 Scamwatch 建立快速檢舉詐欺網站與廣告流程，降低蒐證與回報門檻，促進社會參與。ABS 資料顯示仍有約三成未通報，故識詐與通報文化之強化仍是政策核心。

2.堵詐面向

堵詐聚焦於通訊源頭與攔阻機制。ACMA 推動《減少詐欺電話與簡訊業界守則》，要求電信業者強化封鎖技術與回報機制，並建立「簡訊寄件者 ID 註冊表（SMS Sender ID Register）」以防字母數位標頭遭冒用。2023 年 10 至 12 月，電信業者攔阻超過 2.467 億通詐欺電話與 1.067 億則詐欺簡訊；2024 年攔阻量級續維持數以億計。業者並以機器學習強化辨識（如 Telstra「Cleaner Pipes」、Optus「Call Stop」、TPG 智能偵測），其中「Call Stop」把民眾撥向詐欺號碼的通話導向警示語音並中止通話，減少受騙機率。通訊端的即時攔阻使高風險載體（電話、簡訊、電郵）之再利用成本上升。

3.防詐面向

防詐以制度設計與跨域合作為核心。2023 年 7 月設於 ACCC 之 NASC，定位為政府—產業合作樞紐，建置可操作的情資共享服務，逐步導入即時交換與夥伴入口。NASC 與 AFCX、金融機構與平台之合作，形成前端偵測、中端通報、後端移除的鏈結。針對投資詐欺，ASIC 建置網站下架能力並發布投資者警示清單，截至 2024 年 3 月 4 日已下架超過 3,500 個不法網站；平台側亦推動自律與過濾機制。政府並就「防詐欺法律架構」提出諮詢，指向銀行、電信、數位平台的最低義務基準與違反處置。金融端則透過業界協議與技術升級降低誤信與誤付：收款人確認（Confirmation of Payee 類型）於多家銀行導入，搭配付款前提示（如 NAB）與通話裝置風險指標（TelstraxCBA 試點），強化情境阻斷。

4.阻詐面向

阻詐著重金流中斷與資產保全。銀行業與 AFCX 建立反詐情資迴路，對可疑交易採延遲付款與即時警示；收款人確認系統以跨行一致的名稱比對降低轉付錯誤與仿冒風險。行業面另透過「詐欺安全協議（Scam Safe Accord）」投資建置收款人確認與共通防護，提升跨行一致性。在加密資產與跨境金流面，透過與合作夥伴之情資共享與帳戶黑名單快速流通，縮短凍結與封堵時差；電信端之號碼、簡訊、電郵封鎖與網站下架形成通訊、平臺及金流三點阻斷。NASC 亦建立受害者轉介至 IDCARE 之機制，協助身分復原與後續防護，避免二次損失。

5.懲詐面向

懲詐面向涵蓋專案化偵辦與跨境合作。依據 NASC 年度報告與澳洲警方公開資料綜整，澳洲警方與 NASC、海外執法機關合作，對釣魚套件、跨國詐欺機房與洗錢網絡進行專案化偵查；並以平台下架、域名移除、帳戶凍結與資料交換等手段結合，對組織化詐欺鏈條進行同步打擊。就內部制度而言，政府研議具約束力的「指定責任實體」制度，賦予銀行、電信與數位平台在偵測、通報、補救上的法定責任基礎；同時透過外部爭議解決機制保障被害者求償流程。執法端亦針對 SIM 卡濫用與一次性密碼(One-Time Password,簡稱 OTP)非法服務進行查緝，從供給端壓減匿名與冒名的犯罪土壤。

6.綜合評析

綜合觀察，澳洲自 2021 年至 2024 年間已逐步建構以國家防詐中心（National Anti-Scam Centre, NASC）為核心的整合性防制體系，其防制邏輯呈現由上游的通訊與平台防護、中游的金融監理與延遲機制、下游的偵查與跨境合作所構成的循環結構。若以情境犯罪預防理論觀之，澳洲的防制模式呈現「提升風險、增加難度、降低報酬」三項核心原理。識詐層面透過全國性宣導與檢舉平台，提升民眾風險感知與警覺意識，降低被害機會；堵詐層面藉由電信端 AI 與機器學習（Machine Learning,簡稱：ML）技術攔阻詐欺電話與簡訊，結合「收款人確認（confirmation of payee）」制度與惡意網站下架措施，增加犯罪施行成本；防詐層面透過強化業界守則與跨部會協議，促進科技業、金融業與通訊業的責任化運作，確立前端預防制度；阻詐層面則以金融端交易延遲、AI 異常偵測及多層認證系統為核心，削弱詐欺報酬結構並強化資金追蹤；懲詐層面則結合警政專案化偵查與國際執法合作，針對跨境投資詐欺與洗錢網絡進行源頭打擊。整體而言，澳洲的防制詐欺體系兼具教育導向、技術導向與制度導向三重特性，展現出以科技監理為支撐、跨域合作為核心的多層防禦體系。惟仍面臨三項挑戰：其一，澳洲統計局（ABS）揭示約三成案件未通報，黑數問題仍高；其二，投資與情感詐欺具長期化與滯後揭露特性；其三，多主體合作下權限與資訊整合尚待深化。未來若能持續擴充即時情資共享網絡、強化平台自律、完善事後補償與高風險類型的分眾介入，將有助於鞏固澳洲防詐體系的持續韌性與策略成熟度。

四、英國

英國的詐欺犯罪數據係由多個不同單位，各就本身業務所需進行統計並無統一的彙整單位，且對詐欺犯罪的定義、分類及犯罪數據統計方式與臺灣亦多有所不同。因此，兩國之詐欺犯罪數據難於比較，但該國的詐欺犯罪趨勢及相關防制策略仍具有參考價值，本研究綜合近四年（2021-2024）UK Action fraud 、Cifas 、UK Finance 及 CSEW 、ONS 等犯罪統計數據與相關防制策略分析如下。

(一)犯罪情勢

1.2021 年

(1)UK Action fraud 統計 2021 年度發生 400,763 件，比 2020 年度 348,105 件，增加 52,631 件(+15%)。Cifas 轉介其組織成員受害案件 329,442，較 2020 年 299,786 件，增加 29,656 件（+10%），UK Finance 共計轉介 190,327 件詐欺犯罪案件，較 2020 年 106,701 件，增加 83,626 件（+78%）；英國國家詐欺情報局(National Fraud Intelligence Bureau,簡稱：NFIB) 綜合上述統計數據顯示，本年度案件總數為 920,532 件，較 2020 年 754,592 件增加 165,940 件(+22%) （Office for National Statistics,2022a;b）（如表 2-43）。

表 2-43 英國詐欺案件發生數 2021 年與 2020 年比較表

統計單位	2020	2021	增減數
UK Action fraud	348,105	400,763	增加 52,631 件（+15%）
UK Finance	106,701	190,327	增加 83,626 件（+78%）
Cifas	299,786	329,442	增加 29,656 件（+10%）
英國國家詐欺情報局(NFIB)	754,592	920,532	增加 165,940 件(+22%)

資料來源：整理自 Office for National Statistics（2022b）。Crime in England and Wales: Appendix tables。Retrieved form:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date：November 3, 2024.

「預付費詐欺」2021 發生 51,667 件比 2020 年度 46,105 件，增加 5,562 件（+12%）;「金融投資詐欺」發生 22,683 件比 2020 年度 17,538 件，增加 5,145 件（+29%）(如表 2-44)。

表 2-44 英國預付費詐欺與金融投資詐欺案件發生數 2021 年與 2022 年比較表

罪名	2020	2021	增減數
預付費詐欺	46,105	51,667	增加 5,562 件（+12%）
金融投資詐欺	17,538	22,683	增加 5,145 件（+29%）。

資料來源：整理自 Office for National Statistics（2022b）。Crime in England and Wales: Appendix tables。Retrieved form:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date：November 3, 2024.

(2)依據英格蘭與威爾斯電話犯罪調查（Telephone-operated Crime Survey for England and Wales,TCSEW[35]）統計，2021 年度推估約發生 520 萬件詐欺犯罪案件，較 2019 年增加約 41%，成為少數未受疫情後整體犯罪下降趨勢影響的類型之一。在詐欺犯罪類型中，「預付費詐欺（Advance Fee Fraud）[36]」及「消費者與零售詐欺（Consumer and Retail Fraud）」大幅增加，顯示詐欺集團利用 COVID-19 疫情期間民眾增加線上購物與網路交易的行為特性進行詐欺。在詐欺手法上，網路釣魚（Phishing）成為主要類型，佔所有詐欺案件的 53%。TCSEW 受訪者中，有 56%表示曾收到冒充快遞公司之詐欺簡訊或電子郵件，34%收到偽冒銀行或金融機構訊息，另有 28%收到假冒電子商務業者資訊。約有 3%的受訪者曾點擊或回覆詐欺訊息，而其中 14%的人進一步提供了個資（相當於總體受訪者中不到 1%）。此結果顯示，在疫情導致的數位生活化背景下，英國詐欺活動迅速轉向線上環境，網路釣魚與電子詐欺成為主流手法（Office for National Statistics, 2022a）。

(3)發生數前 5 名

35.TCSEW 英格蘭和威爾斯電話犯罪調查，於 2020 年 5 月 20 日開始運作，以取代因新型冠狀病毒(COVID-19)疫情大流行，而於 2020 年 3 月 17 日暫停的 CSEW。其估計數據來自於 2021 年 1 月 1 日至 2021 年 12 月 31 日期間，對英格蘭和威爾斯年齡在 18 歲及以上的家庭居民進行的總共 37,332 次電話訪談。由於某些受訪者的報告期間重疊，TCSEW 的估計值無法與 2020 年度的估計值進行比較。因此，TCSEW 估計值與 2019 年度的 CSEW 估計值進行比較。CSEW 於 2021 年 10 月重新啟動後，TCSEW 於 2022 年 3 月關閉。

36.被害人預先支付款項購買金融商品或服務但最終並未獲得所購買之物品或服務。

第 1 名：支票、信用卡和網路銀行帳戶（非 PSP）（Cheque, plastic card and online bank accounts 【not PSP】），418,045 件。第 2 名：其他詐欺行為（其他未涵蓋）（Other fraud【not covered elsewhere】，144,729 件。第 3 名：網上購物和拍賣（Online shopping and auctions），83,990 件。第 4 名：申請詐欺（不包括抵押貸款）Application fraud (excluding mortgages)，75,920 件。第 5 名：其他預付費用詐欺（Other advance fee frauds），29,914 件（如表 2-45）。

表 2-45 2021 年英國詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	支票、信用卡和網路銀行帳戶（非 PSP）（Cheque, plastic card and online bank accounts 【not PSP】	418,045
2	其他詐欺行為（其他未涵蓋）（Other fraud【not covered elsewhere】	144,729
3	網上購物和拍賣（Online shopping and auctions）	83,990
4	申請詐欺（不包括抵押貸款）Application fraud (excluding mortgages)	75,920
5	其他預付費用詐欺（Other advance fee frauds）	29,914

資料來源：整理自 Office for National Statistics（2022b）。Crime in England and Wales: Appendix tables。Retrieved form:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date：November 3, 2024.

2.2022 年

(1)依 UK Action fraud 統計指出，本年度發生 298,792 件，比 2021 年度 400,763 件，減少 101,971 件（-25%）。這可能與解除社交接觸限制等行為變化有關[37]。本年度 Cifas 轉介其組織成員受害案 373,882 件，較 2021 年 329,442 件，增加 444,40 件（+13%）。本年度 UK Finance 共計轉介 467,371 件詐欺犯罪案件，較 2021 年 190,327 件，增加 277,044 件（+146%）；這是由於英國金融界的參與，現有會員的報案告增加，以及 2021 年底加入的新會員提交的報案增加的結果。英國國家詐欺情報局(NFIB)綜合上述統計數據顯示，2022 年案件總數為 1,140,045 件，較 2021 年 920,532 件增加 219,513 件(+23.84%)（Office for National Statistics,2023a;b），參閱表 2-46。

表 2-46 英國詐欺案件發生數 2022 年與 2021 年比較表

統計單位	2021	2022	增減數
UK Action fraud	400,763	298,792	減少 101,971 件（-25%）
Cifas	329,442	373,882	增加 444,40 件（+13%）
UK Finance	190,327	467,371	增加 277,044 件（+146%）
英國國家詐欺情報局(NFIB)	920,532	1,140,045	增加 219,513 件(+23.84%)

資料來源：整理自 Office for National Statistics（2023b）。Crime in England and Wales: Appendix tables。Retrieved form:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date：November 3, 2024.

37.上述數據並不包括德文郡和康沃爾郡警方，因為系統變更影響該兩郡數據的準確性。

減少主要原因為「其他詐欺」本年度發生 85,227 件比 2021 年度 144,729 件，減少 59,502 件（-41%）；以及消費者和零售詐欺本年度發生 107,831 件比 2021 年度 141,115 件，減少 33,284 件（-23%）（如表 2-47）。

表 2-47 英國其他詐欺與零售詐欺案件發生數 2021 年與 2022 年比較表

罪名	2021	2022	增減數
其他詐欺	144,729	85,227	減少 59,502 件（-41%）
消費者和零售詐欺	141,115	107,831	減少 33,284 件（-23%）

資料來源：整理自 Office for National Statistics（2023b）。Crime in England and Wales: Appendix tables。Retrieved form:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date：November 3, 2024.

(2)根據 TCSEW 資料，2022 年英格蘭與威爾斯推估約發生 370 萬件詐欺案件，與疫情前（2020 年 3 月止）調查結果相當，顯示詐欺犯罪總量已回復至疫情前水準。然而，詐欺犯罪的內部結構產生顯著變化：「銀行與信用帳戶詐欺（Bank and Credit Account Fraud）」下降約 14%（由 250 萬件降至 210 萬件），但「預付費詐欺」則暴增近八倍（自 6 萬件上升至 45.4 萬件）。此一變化反映疫情後期網路詐欺產業化與技術化的趨勢。詐欺集團利用線上理財、假投資平台及虛擬貨幣為誘因吸引民眾匯款，顯示詐欺行為的數位化及跨境化風險上升。（Office for National Statistics, 2023a）

(3)發生數前 5 名

第 1 名：支票、信用卡和網路銀行帳戶（非 PSP）（Cheque, plastic card and online bank accounts 【not PSP】），698,319 件。第 2 名：申請詐欺（不包括抵押貸款）Application fraud (excluding mortgages)，93,704 件。第 3 名：其他詐欺行為（其他未涵蓋）（Other fraud【not covered elsewhere】，85,227 件。第 4 名：網上購物和拍賣（Online shopping and auctions），62,314 件。第 5 名：其他預付費用詐欺（Other advance fee frauds），27,225 件（如表 2-48）。

表 2-48 2022 年英國詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	支票、信用卡和網路銀行帳戶（非 PSP）（Cheque, plastic card and online bank accounts 【not PSP】	698,319
2	申請詐欺（不包括抵押貸款）Application fraud (excluding mortgages)	93,704
3	其他詐欺行為（其他未涵蓋）（Other fraud【not covered elsewhere】	85,227
4	網上購物和拍賣（Online shopping and auctions	62,314
5	其他預付費用詐欺（Other advance fee frauds）	27,225

資料來源：整理自 Office for National Statistics（2023b）。Crime in England and Wales: Appendix tables。Retrieved form:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date：November 3, 2024.

3.2023 年

(1)依 UK Action fraud 統計指出，本年度發生 308,033 件，比 2022 年度 298,792 件，增加 9,241 件(+3.09%)。本年度 Cifas 轉介其組織成員受害案 338,948 件，較 2022 年 373,882 件，減少 349,34 件（-9%）。本年度 UK Finance 共計轉介 515,575 件詐欺犯罪案件，較

2022 年 467,371 件，增加 48,204 件（+10%）。英國國家詐欺情報局(NFIB)綜合上述統計數據顯示，2023 年案件總數為 1,162,566 件，較 2022 年 1,140,045 件增加 22,521 件(+1.97%)（如表 2-49）（Office for National Statistics,2024 a;b）。

表 2-49 英國詐欺案件發生數 2023 年與 2022 年比較表

統計單位	2022	2023	增減數
UK Action fraud	298,792	308,033	增加 9,241 件（+3.09）
Cifas	373,882	338,948	減少 34,934 件（-9%）
UK Finance	467,371	515,575	增加 48,204 件（+10%）
英國國家詐欺情報局(NFIB)	1,140,045	1,162,556	增加 22,511 件(+1.97%)

資料來源：整理自 Office for National Statistics（2024b）。Crime in England and Wales: Appendix tables。Retrieved form: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date：October 31, 2025.

(2)依據英格蘭與威爾斯犯罪調查（Crime Survey for England and Wales, CSEW）統計，2023 年度估計發生約 310 萬件詐欺案件，相較 2022 年的 370 萬件減少 16%。主要類型中，「銀行與信用帳戶詐欺」減少 13%、「預付費詐欺」減少 34%、「其他詐欺」則減少 50%。此顯示英國防詐政策（特別是金融監理與平台自律）已見初步成效。然而，CSEW 同時指出詐欺犯罪仍有嚴重的「黑數（dark figure of crime）」問題。根據「英格蘭與威爾斯犯罪：年度趨勢與人口統計資料集（Crime in England and Wales: Annual Trend and Demographic Dataset）」顯示，僅約 14.29%的詐欺案件有被報案至警方或 Action Fraud（全國詐欺通報中心），即約每七起詐欺中僅一件進入正式通報程序（Office for National Statistics, 2024a）。

(3)發生數前 5 名

第 1 名：支票、信用卡和網路銀行帳戶（非 PSP）（Cheque, plastic card and online bank accounts 【not PSP】），748,033 件。第 2 名：申請詐欺（不包括抵押貸款）Application fraud (excluding mortgages)，81,992 件。第 3 名：其他詐欺行為（其他未涵蓋）（Other fraud【not covered elsewhere】，80,842 件。第 4 名：網上購物和拍賣（Online shopping and auctions），67,589 件。第 5 名：其他預付費用詐欺（Other advance fee frauds），29,534 件（如表 2-50）。

表 2-50 2023 年英國詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	支票、信用卡和網路銀行帳戶（非 PSP）（Cheque, plastic card and online bank accounts 【not PSP】	748,033
2	申請詐欺（不包括抵押貸款）Application fraud (excluding mortgages)	81,992
3	其他詐欺行為（其他未涵蓋）（Other fraud【not covered elsewhere】	80,842
4	網上購物和拍賣（Online shopping and auctions	67,589
5	其他預付費用詐欺（Other advance fee frauds）	29,534

資料來源：整理自 Office for National Statistics（2025b）。Crime in England and Wales: Appendix tables。Retrieved form: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date：October 31, 2025.

4.2024 年

(1)依 UK Action fraud 統計指出，本年度發生 301,972 件，比 2023 年度 308,033 件，減少 6,061 件(-1.96%)。本年度 Cifas 轉介其組織成員受害案 378,697 件，較 2023 年 338,948 件，增加 39,749 件(+11.7%)。本年度 UK Finance 共計轉介 557,007 件詐欺犯罪案件，較 2023 年 515,575 件，增加 41,432 件（+8.03%）。英國國家詐欺情報局(NFIB)綜合上述統計數據顯示，2024 年案件總數為 1,237,676 件，較 2023 年 1,162,566 件增加 75,120 件(+6.46%)（如表 2-51）（Office for National Statistics,2025 a;b）。

表 2-51 英國詐欺案件發生數 2024 年與 2023 年比較表

統計單位	2023	2024	增減數
UK Action fraud	308,033	301,972	減少 6,061 件（-1.96%）
Cifas	338,948	378,697	增加 39,749 件（+11.7%）
UK Finance	515,575	557,007	增加 41,432 件（+8.03%）
英國國家詐欺情報局(NFIB)	1,162,556	1,237,676	增加 75,120 件(+6.46%)

資料來源：整理自 Office for National Statistics（2025b）。Crime in England and Wales: Appendix tables。Retrieved form: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date：October 31, 2025.

(2)2024 年 CSEW 統計顯示，英格蘭與威爾斯全年約發生 410 萬件詐欺案件，較 2023 年（310 萬件）增加 33%，也較疫情前（2020 年）增加約 12%。主要類型中：銀行與信用卡帳戶詐欺 增加 27%，達約 240 萬件；消費者與零售詐欺增加 35%，達約 110 萬件。在所有詐欺案件中，約有 300 萬件造成實際財損，其中 210 萬件的受害者獲得全額賠償，顯示英國銀行體系與金融監理的補償機制已逐步完善。根據 ONS 最新統計，僅約七分之一的詐欺案件向警方或 Action Fraud(全國詐欺與網路犯罪檢舉中心)通報。NFIB（國家防詐情報局）彙整自三個報告來源：Action Fraud、Cifas（全國身分防詐資料庫）及 UK Finance（金融業防詐組織）。截至 2024 年底，NFIB 記錄案件總數達 120 萬件，年增 6%。其中：UK Finance 報告案件上升 8%（達 557,007 件）；Cifas 上升 12%（達 378,697 件）；Action Fraud 通報案件略降 2%（由 308,033 件降至 301,972 件）。此顯示英國雖已強化防詐通報體系，但詐欺仍持續以金融與電子商務為主要途徑，跨業整合的資料共享與防制機制仍須強化（Office for National Statistics, 2025a）。

(3)發生數前 5 名

第 1 名：支票、信用卡和網路銀行帳戶（非 PSP）（Cheque, plastic card and online bank accounts 【not PSP】），805,439 件。第 2 名：其他詐欺行為（其他未涵蓋）（Other fraud【not covered elsewhere】，85,045 件。第 3 名：申請詐欺（不包括抵押貸款）Application fraud (excluding mortgages)，71,667 件。第 4 名：網上購物和拍賣（Online shopping and auctions），50,484 件。第 5 名：其他預付費用詐欺（Other advance fee frauds），29,262 件（如表 2-52）。

表 2-52 2024 年英國詐欺案件發生數前 5 名

排名	犯罪手法	件數
1	支票、信用卡和網路銀行帳戶（非 PSP）（Cheque, plastic card and online bank accounts 【not PSP】	805,439
2	其他詐欺行為（其他未涵蓋）（Other fraud【not covered elsewhere】	85,045
3	申請詐欺（不包括抵押貸款）Application fraud (excluding mortgages)	71,667
4	網上購物和拍賣（Online shopping and auctions	50,484
5	其他預付費用詐欺（Other advance fee frauds）	29,262

資料來源：整理自 Office for National Statistics（2025）。Crime in England and Wales: Appendix tables。Retrieved form: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date：October 31, 2025.

(二)防制策略

英國政府於 2023 年 5 月公布政策文件《詐欺策略：阻止詐欺並保護公眾》（Fraud Strategy: Stopping Scams and Protecting the Public），明確揭示英國整體詐欺防制政策之中長期方向（GOV.UK, 2023）。該策略規劃政府、執法機關、監管機構、相關產業及慈善組織之共同角色與分工，透過跨部門合作與公私協力機制，期望於本屆國會任期結束前，使整體詐欺案件數較 2019 年新冠疫情前水準減少 10%。為達成上述政策目標，該策略進一步提出下列主要行動方向。

1.追捕詐欺犯（Pursue Fraudster）

英國政府為強化對詐欺犯罪之回應能力，規劃投入 1 億英鎊，全面提升執法、情報蒐集與刑事司法體系在詐欺犯罪偵查、起訴與制裁上的整體效能，並加強被害人財產損失之追償機制。英國政府並預期，至本屆國會任期結束前，僅透過「追捕詐欺犯」相關措施，即可防止逾 30 萬件詐欺犯罪發生。其主要推動機制如下

(1)跨部門整合打擊詐欺犯罪之組織分工

A.由英國內政部負責防制詐欺犯罪之整體政策方向、策略規劃與跨部會統籌。

B.國家犯罪局((National Crime Agency,簡稱 NCA))透過所屬之國家經濟犯罪中心(National Economic Crime Centre,簡稱：NECC)，統籌並領導英國執法機關、情報單位與產業部門，共同推動防制詐欺犯罪工作。

C.倫敦市警察局（City of London Police,簡稱：CoLP）負責領導與協調英格蘭及威爾斯地區之防治區域組織犯罪小組（Regional Organised Crime Unit Network,簡稱：ROCU[38]），以及全國 43 支地方警察機關，執行反詐欺犯罪行動。

D.英國各地警察機關與英格蘭、威爾斯地區之 ROCU，負責處理國內多數詐欺案件之偵查工作，並提供在地被害人及企業必要之支援與協助。

E.重大詐欺犯罪偵查署（Serious Fraud Office,簡稱：SFO[39]）則持續運用其專責之偵查體

38.ROCU：區域組織犯罪小組負責管理【跨境】嚴重和有組織犯罪威脅，與國家犯罪局、警隊和其他合作夥伴密切合作，利用一系列專業策略和能力來識別、瓦解和應對有組織犯罪構成的日益複雜的威脅，工作涵蓋現代奴隸制、毒品和槍支進口、兒童性虐待和性剝削以及經濟和網路犯罪。

39.SFO： 重大詐欺犯罪偵查署，英國政府的一個非內閣部門，負責調查和起訴英格蘭、威爾斯和北愛爾蘭的嚴重或複雜的詐騙和貪污行為。重大詐欺犯罪偵查署根據《1987 年刑事司法法令》（Criminal Justice Act 1987）設立，並對英格蘭及威爾斯檢察總長負責。

系與法定權限，處理涉及高度複雜性與跨境特性的重大詐欺犯罪案件。

(2)成立國家打擊詐欺犯罪小組(National Fraud Squad)

英國政府規劃新設「國家打擊詐欺犯罪小組」（National Fraud Squad），以強化對個人及企業受害詐欺案件之調查與打擊能量。該小組配置於國家犯罪局（NCA）、倫敦市警察局（CoLP）及英格蘭、威爾斯地區之防治區域組織犯罪小組（ROCU）等單位體系中，目前已增補 300 餘名具專業訓練之詐欺犯罪調查人員，並規劃於 2025 年再行增聘 100 名，以擴充全國層級之專責偵查能量。

(3)強化情報導向之詐欺犯罪防制機制

依倫敦市警察局（CoLP）估計，英國超過 70%之詐欺被害案件涉及跨境犯罪行為；另據英國警務智庫於 2016 年之分析，約近 50%之詐欺及網路犯罪係由有組織犯罪集團所為。鑑此，英國於其情報體系（UK Intelligence Community,簡稱：UKIC[40]）內部設立專責打擊詐欺犯罪之重點單位，強化以情報導向之犯罪防制策略，並結合全球合作夥伴網絡，於境外即行阻斷詐欺犯罪活動。同時，國家犯罪局（NCA）亦成立新的詐欺犯罪打擊單位，進一步整合情資蒐集、分析與行動部署，以提升跨境詐欺案件之整體應處效能。

(4)精進英國國家詐欺和網絡犯罪檢舉中心（Action Fraud）之服務系統

英國內政部承諾於三年內投入逾 3,000 萬英鎊，並結合倫敦市法團[41]（City of London Corporation）之捐款資源，全面升級英國國家詐欺與網路犯罪檢舉中心（Action Fraud）之服務系統。改革重點在於簡化被害人報案流程，並提升執法機關對案件之即時回應能力。新系統導入自動化與資料分析技術，以加速案件分流至警察機關，並透過線上報案資料之分析，辨識弱勢被害人案件，優先提供評估與支持。同時，系統亦升級呼叫中心以縮短等待時間，並建置被害人專屬入口網站，使其得以即時掌握案件進度。此外，國家詐欺情報局（NFIB）負責對報案資料進行評估，並將具即時行動價值之案件通報執法機關。該機構運用進階分析能力與多元資料來源，加速行動部署，協助金融機構阻斷詐欺資金流向，或關閉吸引大量被害人之可疑網站，並透過資訊回饋機制，提升被害人對政府防制作為之信任感。

(5)改善刑事司法制度

A.提升詐欺犯罪之偵查與起訴效能

英國政府透過制度與程序改革，加速詐欺犯罪案件自偵查至起訴之流程，降低司法運作中因證據龐雜與程序負荷所形成之結構性障礙。具體措施包括：透過 NFS 等專責機制，提升執法效率；建構符合數位環境之案件揭露制度，以簡化涉及大量數位證據之詐欺案件處理流程，減輕執法機關與檢察官之實務負擔；並依據《嚴重及組織犯罪法》（Serious and Organised Crime Act 2005），運用誘因機制促使犯罪者提供關鍵證據，以瓦解詐欺犯罪網絡。此外，英國亦善用 2022 年生效之英美數據存取協議（The UK-US Data Access Agreement），使政府得直接向美國科技公司調取數位資料，作為預防、偵查、調查與起

40.UKIC：英國情報組織負責英國國家安全情報的收集、分析和傳播，對英國的政策制定和國家安全問題有至關重要的影響。最著名的機構是負責外國情報的秘密情報局 (SIS/MI6)、負責國內問題的安全局 (MI5)、負責信號情報和電子資訊 (SIGINT) 的通用通訊總部 (GCHQ) 以及國防部國防部(MoD) 的情報(DI)。

41.倫敦市法團（City of London Corporation Limited），亦稱倫敦法團，是英國倫敦的老城區—倫敦市的自治組織和地方政府。其轄區只涵蓋倫敦市，而不是整個大倫敦。倫敦市法團的宗旨有三：推廣倫敦市作為世界領先的國際金融和商務中心的地位；作為地方政府為市民提供服務；及為倫敦、所有倫敦市民和國家提供一系列其它服務。

訴詐欺等重大犯罪之依據，迄今已提出逾三千件請求，對於案件突破與跨境執法合作具有實質成效。

B.擴大詐欺案件之審理與司法承載能力

為將更多詐欺犯罪者繩之以法，英國政府同步針對刑事司法體系之量能進行結構性調整，包括減少刑事法院積案、加速案件審理時程、取消法院開庭天數上限，並增聘約二千名法官，以整體提升司法處理能力。同時，政府亦全面檢視詐欺案件自報案至判決終結所需之時間，強化案件分流與處理效率。在硬體與人力配置上，英國規劃新建倫敦市法院，預計自 2026 年起每年可增加審理約 550 件複雜之詐欺、網路及經濟犯罪案件；並透過司法學院對法官與治安法官實施專門訓練，以提升其處理長期與高度複雜案件之專業能力。同時，亦考慮修正《欺詐法》（Fraud Act 2006），將部分輕微詐欺案件移由治安法院處理，以優化案件分配結構。

C.建構相稱之懲罰機制與再犯防制工具

在制裁與預防層面，英國政府擬強化「嚴重犯罪預防令」（Serious Crime Prevention Order, 簡稱：SCPO[42]）之適用彈性，賦予執法機關更多工具，以提前介入並限制高風險詐欺犯罪者（包含尚未定罪者）之活動。同時，倫敦市警察局（CoLP）亦與私部門進行試辦合作，探索透過民事執法或債權機制追討詐欺犯罪所得，以提高被害人返還款項之可能性。此外，英國亦透過《經濟犯罪與企業透明度法》引入「未能防止詐欺」之企業犯罪責任，要求企業對員工為公司利益所實施之詐欺行為負起防制義務，以促進企業內控與治理責任。

2.防止詐欺（Block Fraud）

據英國獨立組織公民建議（Citizens Advice[43]）指稱，在英國每 3 名成年人中就有 2 人曾經成為網路詐欺的目標，英國通信管理局（Office of Communications,簡稱：Ofcom[44]）研究顯示，2022 年的前三個月，英國就有超過 4000 萬成年人成為可疑詐欺簡訊或電話的目標，英國為減少詐欺犯罪的機會和影響，並提高社會對詐欺的抵抗力，推出以下具體作法或機制

(1)鼓勵民間產業界加入防詐行動

A.由首相任命西蒙菲爾(Simon Fell)為反欺詐鬥士（Anti-Fraud Champion）[45]

負責在政策層級上統籌英國整體反詐欺行動，並將英國定位為國際社會打擊詐欺犯罪之重要領導者。其核心任務在於促進政府、產業界與國際企業之合作，確保關鍵利害關係人均能依其角色分工積極投入防詐行動，以共同推動並落實整體防制策略目標。

42.嚴重犯罪預防令（Serious Crime Prevention Order 簡稱 SCPO）可由檢察長、嚴重詐欺辦公室主任、北愛爾蘭檢察長和蘇格蘭檢察長提出申請，如果某人被判犯有嚴重罪行，則向皇家法院提出申請；如果該人曾參與嚴重犯罪，則向高等法院單獨提出申請。SCPO 是由 2007 年《嚴重犯罪法》第 1 部分引入的，該法附表 1 中列出了可以適用 SCPO 的「嚴重犯罪」指示性清單。SCPO 可以透過對某人施加各種條件來防止參與嚴重犯罪；例如，限制可以交往的人、旅行，或規定有義務向警方報案告自身的財務狀況。命令的有效期限最長可達五年，違反其條件即構成刑事犯罪，最高可判處五年徒刑。雖然 SCPO 可以作為高等法院的「獨立」命令實施，但它們大多用於對付刑事法院被判犯有嚴重罪行的人，使用這些命令的執法機構發現它是打擊嚴重組織犯罪的非常有效的工具。

43.公民建議（Citizens Advice）英國獨立組織，專門提供機密資訊和建議，以幫助人們獲得法律援助。

44.英國通信管理局（Office of Communications,簡稱：Ofcom）在電視、廣播、電信和郵政領域擁有廣泛的權力，它有代表公民和消費者利益透過促進競爭和保護公眾免受有害或冒犯性材料侵害的法定義務。主要監管領域包括電視和廣播標準、寬頻和電話、網路視訊共享平台、無線頻譜和郵政服務。

45.西蒙·菲爾(Simon Fell)英國首相任命的反欺詐鬥士（Anti-Fraud Champion），於 2023 年 12 月 13 日接替安東尼布朗（Anthony Browne）出任該職位。

B.定期發布詐欺模式資料，強化消費者知情與產業責任

英國政府要求民間產業界與監管機構、公部門合作，定期彙整並發布有關詐欺犯罪手法與趨勢之統計資料，以提升消費者對詐欺風險之認知，並作為行為預警與自我防護之依據。同時，此一機制亦明確要求企業與金融機構自業務源頭即承擔防詐責任，而非僅於案件發生後被動應處。政府並透過反詐欺鬥士之協調角色，促成與社群媒體、電信業者等關鍵產業之合作，透過制度誘因與政策引導，鼓勵企業持續投入並深化防制詐欺之作為。

C.透過聯合詐欺特別工作組(JFT)**推動跨域防詐合作**

英國政府與產業界透過設置「聯合詐欺特別工作組」(Joint Fraud Taskforce,簡稱：JFT[46])，建立跨部門、跨產業之合作平臺，以共同防止詐欺犯罪。該工作組由政府安全部長主持，成員涵蓋政府部門、執法機關、監管機構、產業界及民間社會之代表，旨在整合多元利害關係人之資源與行動，共同推動防詐政策。JFT 於 2021 年 10 月重新啟動後，負責統籌並管理詐欺相關產業之憲章推動工作，並於董事會與實務層級同步運作，涵蓋通訊詐欺、網路詐欺及被害人保護等多項工作流程。至 2022 年 11 月，JFT 進一步達成共識，將共同建立評估機制，以衡量產業界防詐作為對於整體詐欺防制成效之實際影響。

D.簽署自願性「防範網路詐欺章程」(Online Fraud Charter)。

英國內政部（Home Office）於 2023 年 11 月 30 日與全球 13 家主要線上平臺與服務提供者簽署自願性「防範網路詐欺章程」(Online Fraud Charter)，藉此促進網路產業落實防詐責任。參與簽署之業者包括 Amazon、eBay、Facebook、Google、Instagram、LinkedIn、Match Group、Microsoft、Snapchat、TikTok、X（Twitter）、techUK 及 YouTube 等重要數位平臺與產業組織。該章程針對網路平臺與服務提供者，提出三項核心防詐要求：其一，建構詐欺行為之監測與預防機制；其二，建立便捷且有效之檢舉通報管道；其三，配合公部門推動防詐宣導與教育工作。依章程規定，簽署之平臺與服務提供者須於六個月內完成相關措施之落實。然而，由於該章程屬自願性質，其實際約束力與長期防制成效，仍有待後續政策評估與實證觀察。

E.宣布並推動新的保險詐欺章程（insurance fraud charter）

英國內政部於 2024 年 10 月 25 日宣布推出新的自願性「保險詐欺章程」(Insurance Fraud Charter)，旨在系統性檢視保險市場中可能遭詐欺利用之制度漏洞，並進一步強化保險產業與刑事司法體系之合作，以深化對保險詐欺問題嚴重性之理解，並改善對被害人之支持機制。

（a）由國家犯罪局所屬之國家評估中心，針對保險產業中「專業推動者」之角色進行審查，特別關注其是否提供虛假證據以支撐不實之保險理賠申請，藉以識別並遏止結構性詐欺行為。

（b）辨識遭「非法保險中介人」利用之保單樣態，包括冒充合法經紀人或向消費者販售完全虛構之保險商品，以防堵保險通路遭不法分子滲透。

（c）強化資料安全與個資保護措施，防止保險詐欺者不當利用客戶之個人與財務資訊，鎖定特定高風險族群進行詐欺行為。

（d）審查詐欺集團用以宣傳虛假保險優惠之策略與相關網站運作模式，並參考銀行業已證實具成效之高風險被害人通報流程，藉以提升對潛在受害者之辨識能力，並加強後續支持與協助機制。

(2)實施科技治理相關規範，以防止犯罪分子濫用數位技術

46.聯合詐欺特別工作組(Joint Fraud Taskforce,簡稱：JFT)是私部門、政府和執法部門之間的合作夥伴關係，旨在共同打擊詐欺行為。

為降低科技工具遭犯罪分子利用之風險，英國政府透過立法、監管與跨機關合作等多元手段，強化對通訊、金融與數位廣告環境之治理，藉以從源頭抑制詐欺犯罪之發生。其主要作法如下

A.推動並落實《網路安全法》，強化科技業者之防詐責任

英國透過制定並實施網路安全法，明確要求科技公司承擔防制網路詐欺之法定責任，對未善盡管理義務或未配合相關規範之企業，得課以高額罰鍰，以提高業者投入防詐作為之誘因。

B.禁止金融產品之亂槍打鳥式電話推銷

為防止詐欺行為假借金融行銷之名義進行，英國明文禁止各類金融產品採取無差別、大量撥打之電話推銷方式，以降低民眾接觸詐欺資訊之機會。

C.限制高容量 SIM 設備之販售與使用

英國禁止販售及使用可同時容納並操作數百張 SIM 卡之電信或網路設備，以阻斷犯罪者快速、大量發送詐欺簡訊及撥打詐欺電話之技術基礎，從而削弱其規模化作案能力。

D.強化大量簡訊發送設備之審查與使用者註冊制度

針對可大量發送簡訊之設備，英國實施更嚴格之審查與實名註冊要求，以提高使用門檻，並強化事後追查能力，藉此抑制詐欺簡訊與虛假來電之產生。

E.與英國通信管理局合作阻斷欺騙性來電

英國政府並與 英國通信管理局（Ofcom）密切合作，透過通訊監理與技術措施，阻止詐欺與欺騙性電話進入通訊網路體系。

F. 強化付費網路廣告之防詐監管架構

文化、媒體與體育部（Department for Culture, Media and Sport,簡稱：DCMS）則以《網路安全法》中關於詐欺廣告之規範為基礎，透過立法與非立法改革並行之方式，強化既有付費網路廣告之監管架構，以降低詐欺與惡意廣告對社會之危害。

(3)加強民間產業界對客戶之保護

支付服務提供者(PSP)應採用新的風險控管方法，以調查潛在的詐欺性支付，FCA 也將對金融公司的防詐系統和控制進行評估。

(4)以大規模技術治理確保網路使用者安全

英國政府透過國家層級之網路安全治理架構，結合技術防護、產業合作與執法權限擴充，於犯罪接觸點之前即行介入，降低民眾暴露於詐欺資訊與不法網站之風險。其主要作法如下

A.持續阻斷詐欺資訊與民眾之接觸

國家網路安全中心（National Cyber Security Centre,簡稱：NCSC）持續運用技術手段，阻止詐欺資訊進入一般民眾之網路使用環境，並與產業界合作進行威脅調查與分析，以系統性方式降低公眾接觸詐欺內容之整體規模。

B.建構國家級「共享與防禦」中心，強化大規模防護能力

NCSC 所建置之國家級「共享與防禦」中心，透過跨部門與跨產業之即時資訊共享與聯防機制，可在詐欺訊息尚未廣泛擴散前即予以攔阻，預期可防止數以百萬計之詐欺訊息進入消費者端，顯著提升整體網路防護效能。

C.賦予執法機關取締詐欺網站之新權限

英國政府並透過法制調整，賦予執法機關新的權限，使其得迅速取得對犯罪或詐欺網站之控制權，並即時關閉或取締相關不法網域，以縮短詐欺活動之存續時間，降低其對社會之危害程度。

3.賦能於人民（Empower People）

英國每年有數百萬名民眾與企業遭受詐欺犯罪侵害，不僅造成金錢損失，亦侵蝕社會互信，甚而引發被害人之心理與身心健康問題。為降低民眾被害風險並協助被害人復原，英國政府將「賦能於人民」定位為防制詐欺之核心支柱之一，透過提供必要之工具與知識，強化公眾自我防護能力，並同時確保被害人能儘速取回遭詐資金。其具體推動機制如下（GOV.UK,2023）：

(1)強化公共溝通與風險意識建構

A.整合並簡化公共反詐溝通體系

英國政府致力於整合執法機關、政府部門、非營利組織與產業界之反詐溝通管道，並推動簡明一致之跨政府宣導行動，以全面改革既有公共反詐資訊傳遞模式，提升民眾對詐欺風險之辨識能力。

B.建構與網路保護相銜接之警察防護網絡

透過建置與網路安全防護機制相互配合之專用警察防護網絡，英國藉以提升公眾對詐欺風險之警覺性，並擴充對潛在被害者之即時支援能量。

C.推動校園反詐與網路安全教育

英國政府提供教師專門之反詐欺教學資源與課程，協助年輕世代及早建立關鍵之反詐欺與網路安全知能，以強化長期社會防護基礎。

(2)強化對詐欺被害人之支持機制

A.簡化報案流程並升級報案系統

英國持續精進被害人報案機制，簡化報案程序，並將 Action Fraud 更新為更先進之數位系統，以提升接案效率與被害人使用便利性。

B.建構一致化之被害人支持體系

透過擴充專責保護經濟犯罪被害人之國家級單位，並整合多機構防制詐欺措施，英國致力於為英格蘭與威爾斯地區之詐欺被害人，提供一致且可持續之支持服務。

(3)保護民眾免於身分詐欺之風險

A.建立安全可信之數位身分市場

英國由科學創新暨技術部（Department for Science, Innovation and Technology 簡稱：DSIT）主導，推動建立具可信度與安全性之數位身分市場（digital identity market），以降低身分遭冒用之風險。

B.提供身分修復支持與指引機制

政府確保身分遭盜用之被害人，能獲得修復身分所需之協助，並引入身分查核清單，明確說明恢復及保護被盜身分之必要步驟。

C.檢討並研議限制身分資料濫用之法制措施

英國亦探索透過新立法，限制身分資料之不當建構、販售與處理，並防止未經授權之存取、複製或蒐集行為。

D.提升公司登記資訊之透明度與可用性

透過強化公司註冊資訊之正確性與可查驗性，並將相關資訊納入防詐應用，防止犯罪者利用假冒公司作為詐欺掩護。

(4)修正法制以協助被害人追回遭詐資金

A.建立支付服務業者之補償責任機制

英國透過立法，授權 支付系統監管機構（Payment Systems Regulator ,簡稱：PSR），要求受其監管之支付服務業者（PSP）對授權詐欺案件進行補償，以提高被害人取回資金

之可能性。

B.建構一致化之資金返還制度框架

政府並持續評估後續政策方向，確保建立一套一致且可執行之制度架構，使詐欺資金得以有效返還予被害人。

4.提升國際合作的關鍵能力（Enhance key international and domestic capabilities）

面對詐欺犯罪高度跨境化與組織化之發展趨勢，英國政府將國際合作視為防制詐欺不可或缺之核心能力之一，優先推動跨國共同打擊與預防詐欺犯罪之行動，並透過雙邊與多邊合作機制，強化對詐欺犯罪集團之追捕力道。同時，英國亦積極協調各國執法機構、跨國企業與民間社會組織，採取一致之防制作為，並推動防詐專業知能交流與犯罪數據共享，以提升共同因應洗錢網路等跨域犯罪問題之整體能力。

(1)強化國際能力建構與合作機制

A.倡議將打擊詐欺列為各國施政優先事項

英國於國際層級倡議將詐欺犯罪防制定位為各國政府之施政重點，並於 2023 年 3 月 11 日在英國召開首屆「全球詐欺峰會」，邀集 G7、五眼聯盟[47]、新加坡 及 南韓 等國家與夥伴參與，由內政大臣主持，藉以凝聚國際共識，推動全球打擊詐欺行動。

B.深化雙邊合作以提升各國防詐能力

英國並與主要國家建立雙邊合作關係，透過經驗交流、技術支援與制度輸出，協助夥伴國家提升防制詐欺犯罪之整體能力，以擴大國際打擊詐欺之實質成效。

(2)跨境追捕詐欺犯罪者之合作作為

A.強化對犯罪來源與設備流向之掌握

英國致力於加強對詐欺犯罪者所在地、作案設備來源國及其運作模式之掌握，以提升跨境追查與即時應處之精準度。

B.制定以情報為導向之跨國打擊行動計畫

英國推動以情報導向為核心之國際防詐行動計畫，並與重點關注國家建立合作，涵蓋執法協作、被害人支持、網路安全應對及資產追回等流程建議，以提升跨國行動之整體一致性。

C.複製成功執法經驗以擴散防詐效益

英國並以其與各國相關機構成功合作查緝詐欺犯罪之經驗為基礎，推動制度化之國際合作模式，促使有效作法得以在其他國家複製與落實。

(3)透過國際協調阻止詐欺犯罪發生

A.動員國際公私部門共同要求跨國企業承擔防詐責任

英國推動國際公私部門合作，協調一致要求跨國企業，特別是科技產業，採取更多具體措施防制網路詐欺。

B.促進各國法制調和以堵塞制度漏洞

透過協調各國調整或修正相關法律架構與監管規範，英國致力於避免詐欺犯罪者利用不同國家法制落差或監管不一致之處從事不法行為。

C.推廣安全支付機制以降低跨國詐欺風險

英國亦支持在其他國家推廣安全支付方式，以強化個人與財務資訊之保護，並降低詐欺犯罪之發生風險。

47.五眼聯盟（Five Eyes，縮寫為 FVEY），是由五個英語圈國家所組成的情報聯盟，在英美協定下組成的國際情報分享團體，成員國包括澳大利亞、加拿大、紐西蘭、英國和美國。

(4)賦能於人民之國際推廣作為

A.分享防詐專業知能與教育資源

英國與其他國家分享防詐相關專業知能，協助教育個人與企業了解詐欺風險，並培養辨識與避免詐欺之能力。

B.提供國際訓練以強化在地防詐能量

英國並為其他國家之執法機構與民間社會組織提供教育訓練，提升其預防與應對詐欺犯罪之專業能力。

C.協助建構被害人支持與報案制度

透過制度與技術支援，英國支持其他國家發展詐欺報案與被害人支持系統，以確保被害人能獲得即時且適切之協助。

(5)強化數據共享與跨政府合作能力

A.深化五眼聯盟之數據共享機制

五眼聯盟各國政府持續與其部門及合作夥伴協作，並於必要時透過立法手段，最大化數據共享機制之運用，以提升防制詐欺犯罪之整體效能。

B.運用共享數據支援公共部門防詐決策

透過威脅評估結果與相關數據之共享，支持公共部門進行更精準之詐欺犯罪防制規劃與行動部署。

(6)因應錢騾(Money Mules[48])網路之跨部門行動

英國發布新的跨部門查緝「錢騾」（Money Mules）行動計畫，透過整合執法、金融監理與國際合作資源，擾亂資金轉移網絡，並降低民眾遭利用為錢騾之風險，以強化整體防詐體系之末端防護能力。

（三）防制成效

根據「英國金融業 2025 年度詐欺報告」《UK Finance Annual Fraud Report 2025》（UK Finance,2025)英國金融服務業透過跨部門合作機制，逐步建立以預防、偵測、攔阻與補償為核心的整合性防詐體系。該體系由政府監理機關、銀行業、金融機構、警政單位及科技產業共同參與，構成多層次防詐防制架構，具體措施如下。

1.在警政合作面向，金融業資助成立「專責卡片與支付犯罪偵查小組」（Dedicated Card and Payment Crime Unit,簡稱：DCPCU），由倫敦警察局及大都會警察共同運作，專責查緝金融及支付詐欺案件。2024 年該單位共破獲與瓦解 90 個有組織詐欺集團，挽回損失約 6,490 萬英鎊，促成 75 件成功定罪，展現警銀合作模式的實質成效。

2.在情報共享與風險監測面，UK Finance 設置「金融情報單位」（Intelligence Unit），負責蒐集及通報可疑卡號與資料外洩事件，並即時與執法機關交換情資。2024 該單位共通報約 248 萬筆遭外洩資料，發出 514 次警示通報，舉辦 128 場情資合作會議，九成以上資料得以即時與警方共享，提升跨部門預警與防詐效率。

3.在前端攔阻措施上，推動「銀行警示通報機制」（Banking Protocol），由 UK Finance、地方警方及全國貿易標準署（National Trading Standards）共同執行。透過訓練銀行行員辨識高風險交易與可疑客戶行為，並即時通報警方介入。2024 年此機制共阻止詐欺損失

48.錢騾是指作為第三方協助移轉或收受犯罪所得之人（即『洗錢幫手』），屬於《洗錢防制法》第 2 條第 3 款所稱之『協助洗錢行為之人』。」

6,130 萬英鎊，觸發 12,034 通即時通報及 136 件逮捕行動。

4.在弱勢族群保護機制方面，UK Finance 與警方合作推動「弱勢被害人通報制度」（Vulnerable Victims Notification），使警方能主動通知銀行特定高風險客戶。2024 年共處理 624 件通報案件，較前一年增加 107%，約三分之二的地方警察機關已採用此制度，降低高齡及易受騙族群的受害風險。

5.在金融補償與消費者保障機制方面，2024 年 10 月起依《支付系統監理機構》（Payment Systems Regulator, PSR）規定正式實施「授權付款詐欺補償機制」（Authorised Push Payment, APP）。金融機構有義務對詐欺受害者提供退款補償。UK Finance 建置「最佳實務登錄系統」（Best Practice Standards, BPS）以監測各銀行處理效率。2024 年約 16 萬件案件納入該系統，受害者獲得返還金額共計 1.215 億英鎊。

6.在跨產業合作與科技防詐方面，UK Finance 與 GSMA（全球行動通訊業者協會）共同推動「Scam Signal 計畫」，使銀行可即時接收電信業傳送之可疑詐欺信號，提前攔阻受害者進行高風險交易。該技術亦被應用於信用卡交易風險偵測。UK Finance 同時協助監管機關 Ofcom 制定《線上安全法》（Online Safety Act 2024）執行細則，要求社群媒體及搜尋平台落實詐欺廣告審查與用戶警示義務，強化科技業防詐責任。

7.在社會倡議與防詐教育方面，持續推動全國性宣導運動「Take Five to Stop Fraud」，協助民眾提升警覺。2024 年共有 38 家大型銀行及金融機構參與，推出互動防詐測驗、社群宣導及針對弱勢族群的易讀教材。另透過「Don’ t Be Fooled」教育計畫進入 430 所學校，推廣防制「人頭帳戶」（Money Mule）教育，強化青年防詐意識。

8.在人工智慧應用與風險偵測方面，金融業已廣泛導入 AI 交易偵測系統，2024 年共防止約 14.5 億英鎊的未授權詐欺交易。業界亦針對 AI 被犯罪者濫用的風險提出警示，並強化跨行資料交換與行為分析以預防「人頭帳戶」操作。

綜上所述，英國防制詐欺犯罪的策略已由事後補救轉向主動預防與跨域合作，形成以資料共享、科技監理與社會教育為三大核心的防詐生態體系。其關鍵成功因素在於政府、金融業、科技業之間的制度化合作，並將防詐議題提升至國家經濟安全與社會信任維護層次，成為國際防制詐欺犯罪的重要典範。

（四）小結

英國詐欺犯罪統計由多個機構各自蒐編，涵蓋警方受理、金融與身分風險資料及住戶調查，口徑不一而難以與臺灣直接比對，然其趨勢與防制策略具參考價值。整體觀之，英國國家詐欺情報局（NFIB）彙整來源顯示，案件量自 2021 年 92 萬餘件上升至 2024 年逾 123 萬件，期間 UK Finance 轉介由 19 萬餘件增至 55 萬餘件，Cifas 轉介亦由 32 萬餘件增至 37 萬餘件；Action Fraud 則在 2021 年達 40 萬餘件後於 2022 年降至 29 萬餘件、2023 年小幅回升、2024 年再度微幅下降。住戶層面的 TCSEW 及 CSEW 則呈現疫情後結構性轉移：2021 年推估約 520 萬件，網路釣魚佔比過半；2022 年總量約 370 萬件、預付費詐欺激增；2023 年約 310 萬件、銀行帳戶與預付費詐欺同步回落；2024 年約 410 萬件再度攀升，其中銀行與信用帳戶詐欺、消費者與零售詐欺分別擴張，且僅約七分之一進入正式通報程序。以細項類型觀察，2021 年至 2024 年「支票、信用卡與網路銀行帳戶（非 PSP）」長期位列發生數首位，網路購物與拍賣、申請詐欺、其他預付費詐欺等亦持續占比。此一調查總量高、警方通報有限、金融面向凸顯的結構，勾勒出英國以金融與通訊節點作為防制樞紐的政策必然。

1.識詐面向

英國之識詐策略以中央政策傳播與跨部門合作為主軸，透過《詐欺策略：阻止詐欺並保護公眾》（2023）整合政府、監管機關與產業訊息，提升公共傳播的一致性與可近性。其中，Take Five 行動將金融教育嵌入實際交易情境，引導民眾於轉帳、授權或回應可疑聯繫等關鍵時刻暫停、查證與思考，以降低衝動決策風險。政策執行上，英國同步推動校園教材與警政保護網絡，並以重塑 Action Fraud 通報流程，作為提升被害人報案意願與早期介入的重要工程。其識詐作為亦延伸至產業自律與平台治理，內政部與主要平台簽署防詐章程，要求建立監測、檢舉與宣導機制，並結合 Ofcom 研究定期揭露高風險接觸態樣，強化民眾風險辨識。整體而言，英國逐步將識詐由單向宣導轉化為與交易行為、通報機制及補償制度相銜接的情境化防制策略。

2.堵詐面向

堵詐政策聚焦於通訊與廣告生態的源頭管理。英國藉由 Ofcom 權限與《網路安全法》框架，對不配合之科技公司課以高額罰則，並禁止金融產品之冷不防推銷，限制可大量傳送簡訊或容納多張 SIM 卡之設備，要求發訊器材註冊與溯源，以抑制詐欺簡訊與偽裝來電。政府並與電信監管機關協同阻截欺騙型通話，推動付費廣告框架改革，要求平臺對詐欺與惡意廣告強化事前審查與事後下架。另由 NCSC 建置「共享與防禦」中心，透過威脅情報與基礎設施處置，降低公眾接觸詐欺內容之機率。在產業面，政府重啟並運作聯合詐欺特別工作組（JFT），以部門憲章與量化評估機制對齊企業減詐目標，藉由「反詐鬥士」跨域協調，促使社群媒體、搜尋與電商平臺在流量入口實施更嚴格的前置過濾，將高風險接觸封堵於傳播前端。

3.防詐面向

防詐著眼於制度與責任之前移與明確化。2023 年詐欺策略以追捕、阻卻、賦能、強化能力為主軸，要求支付服務提供者採用新風險控管方法，並由金融監管機構評估內部防詐控制。身分管理方面，政府推動可信數位身分市場，強化身分盜用修復流程，並提升公司登記資訊的實質有效性，以降低假冒殼公司濫用空間。行為端則以廣告與平臺義務化落實內容管理，文化、媒體與體育部配合立法與非立法改革，對網路廣告加強監管。司法端透過建立倫敦市法院、擴充審判能量與專業訓練，優化巨量數位證據之揭露機制，並評估調整《詐欺法》處理輕微個案之方式，以提高系統處理量能與可近性；同時研究以民事權能追討不法收益，輔以新「未能防止詐欺」企業罪，促使企業強化內部控制。上述規範密織於平臺、金融與司法節點，形成身分、內容、交易、訴訟的環環相扣前置防線。

4.阻詐面向

阻詐以金流凍結、交易補償與端點合作為核心。UK Finance 主導之跨業框架下，銀行端實施「銀行警示通報機制」，藉行員辨識高風險交易即時通報警方，2024 年阻止損失達 6,130 萬英鎊，並觸發逮捕行動與現場勸阻。補償制度方面，支付系統監理機構自 2024 年 10 月推動授權付款詐欺（APP）強制補償，配合「最佳實務登錄系統」監測處理效率，2024 年約 16 萬件納入，返還金額達 1.215 億英鎊。情報與技術上，UK Finance 設置「金融情報單位」通報資料外洩與高風險卡號，2024 年通報約 248 萬筆並多次發布警示；同年串聯 GSMA 執行「Scam Signal」使銀行即時接收電信可疑信號，於交易前啟動風控。產業自律與監管協力並行，使可疑交易偵測、即時凍結、補償返還形成制度化循環，金融體系的攔阻與緩衝效應據此顯著。

5.懲詐面向

懲詐以專責偵查、情報導向與量能提升為要。國家詐欺小組在 NCA、倫敦市警察局

與區域組織犯罪小組中擴編專業調查人力，配合 UKIC 設置詐欺重點部門，以情報驅動跨境追訴；同時透過英美數據存取協議加速取得關鍵平臺證據，降低數位蒐證障礙。警銀合作層次上，金融業資助之「專責卡片與支付犯罪偵查小組」（DCPCU）於 2024 年瓦解 90 個有組織詐欺集團、挽回約 6,490 萬英鎊並促成 75 件定罪，展現以行業資源支撐警政偵查之效能。司法體系則藉取消開庭日上限、增聘法官與強化陪審指引，提高複雜經濟犯罪之審理效率，並以嚴重犯罪預防令、企業刑事責任與民事追討並用，達成定罪、限制、追償的多層制裁。

6.綜合評析

英國的防制詐欺體系以政府主導、監理驅動、金融樞紐、平臺責任及警政專責為核心，透過識詐宣導、通訊封鎖、制度前移、金流攔阻與偵審制裁形成循環防制策略。藉由多元統計資料支撐，警方、金融機構及住戶調查得以同步掌握接觸、報案與交易風險。然而，英格蘭與威爾斯犯罪調查（CSEW）顯示，詐欺案件通報率仍偏低，且 2024 年總量再度上升，反映詐欺集團能迅速運用數位廣告、人工智慧與跨境網絡調整策略。從情境犯罪預防理論觀之，英國防制思維體現改變犯罪機會結構之核心精神：前端以通訊監理與網路廣告控管提升犯罪風險；中段透過警銀合作與 AI 偵測增加行為成本；後端則以授權付款補償與銀行警示制度降低犯罪報酬，並透過企業防詐責任與平臺合規義務移除作案藉口。此一制度化、科技化且高度協作的設計，使犯罪於接觸、交易與資金外流各環節皆受阻斷與延遲，逐步形成以金融體系為核心、平臺與警政為雙支撐之動態防詐模式，對臺灣推動金流防詐、跨部會合作與被害補償制度具有重要借鑑價值。

第四節 臺灣與主要國家防制電信網路詐欺策略比較

承接前節所建立之打詐五面向分析架構與主要國家個別防制策略樣態之整理，本節進一步以臺灣為比較基準，系統性對照日本、新加坡、澳洲與英國在防制電信網路詐欺策略上的制度設計與防制路徑。比較之重點不在於單一措施成效之高低，而在於各國如何透過策略組合與流程設計，於前端降低民眾接觸與誤信風險，中段強化通訊、網路平臺與金流環節之管控，後端則透過偵查追訴、財產刑與跨境合作提升阻斷與剝奪之確定性，以形塑多層次且具連續性的整體防制體系。透過此一比較分析，本研究得以歸納主要國家在打詐五面向防制策略上的共通趨勢與差異特徵，並進一步檢視臺灣現行防制詐欺犯罪策略在制度整合、時間管理與流程連貫性上的優勢、限制與精進空間，作為後續綜合評析與政策建議之重要依據。

一、犯罪概況

近年全球電信網路詐欺犯罪普遍呈現跨境化、科技化與組織化之共同結構。特別是假投資詐欺高度依賴社群媒體、即時通訊工具與加密資產（或替代性數位支付）等環境條件，並在疫情後遠端社交與數位交易常態化的背景下快速擴張。此類犯罪在接觸階段更易透過演算法推播與廣告投放精準觸及，在互動階段則藉由情境化話術、情感操控與權威冒用建構信任，並於出金階段透過多層轉移、跨境通道與匿名工具製造金流追查斷點，使監管與查緝同時面臨證據取得、處置時效與跨境協作等多重壓力。準此，犯罪概況之比較宜回到風險焦點、防制斷點與制度回應三個層次加以觀察，而非以統計口徑差異甚大的數據進行直觀對照。

(一)臺灣情勢

臺灣近年詐欺犯罪案件發生數與財損數額持續升高，其中假投資詐欺在案件數與財損占比皆居高不下，顯示假投資詐欺犯罪產業鏈具有持續再生與轉型之能力。即使政府推動打詐綱領 2.0 並強化制度與科技工具，犯罪仍可能在更高密度的查緝環境中調整作案流程與工具組合。整體而言，臺灣的防制關鍵不僅在於案件量本身，更在於具階段性的詐欺腳本運作模式：前端以廣告與社群導流建構接觸機會，中段以通訊與私密社群軟體群組互動深化信任，後端再以金流與虛擬資產工具快速完成外移與斷點化。故若僅以單一措施重複堆疊，往往難以阻斷其跨階段串接之流程，防制策略必須更強調跨節點、跨部門、跨產業的連續鏈結與時間管理。

(二)主要國家比較

日本以高齡者受害之特殊詐欺為重要議題，犯罪樣態逐漸朝科技化與情境化發展，並需同時處理高齡族群風險辨識能力不足與詐術擬真化的雙重問題；新加坡案件集中於網路購物、假求職與假投資詐欺，反映平台與支付生態所帶來的高風險集中特徵，政策因而偏向平台責任與支付安全的整合防制策略；澳洲詐欺樣態呈現多元並行之整合性犯罪結構，政策更強調跨產業守則與全國性合作平台以提升一致處置能力；英國因金融市場成熟與線上交易頻繁，使授權付款詐欺與網路釣魚成為核心風險類型，防制焦點多落在支付流程的事前警示、風險分擔與補償制度，以及平台廣告生態的責任化。整體而言，各國雖在主要詐術與被害族群上有所差異，但共同面臨數位環境快速變化、跨境金流與虛擬資產應用所導致的監理與查緝挑戰。

二、防制策略

本研究以打詐五面向分析主要國家發現各國普遍建構多層次防線，並強調公私協力、數據共享與科技應用。值得注意者在於，防制重點已由單點措施移轉為階段式防制設計：亦即把風險提示、攔阻、審核、延遲、複核、凍結、追償與追繳等機制，嵌入搜尋、點擊、通訊互動、轉帳與兌現等關鍵介入點，並以資料標準化與名單同步支撐跨平台、跨銀行與跨機關的一致處置。以下分就五面向比較各國政策邏輯與防制特色。

(一)識詐面向（宣導教育面）

本面向的政策演進趨勢，已由傳統單向宣導，逐步轉向行為導向並將風險提示嵌入高風險關鍵介入點之作法。亦即，政策關注不再僅是訊息是否被看見，而更在意民眾是否在搜尋、點擊、下載、匯款、轉帳等高風險情境中實際採取查核、阻斷與通報等防詐行為。日本在高齡社會背景下，除強調生活型風險宣導與在地接觸管道外，亦透過情境演練、通話模擬與風險提示工具，提升高齡族群對情境化詐術的辨識能力；新加坡透過全國性防詐平台結合推播與回報機制，強化看見、回報、處置的前端承接；澳洲運用中央平台整合訊息與多語傳播，提高多元族群在日常使用情境中的可近性；英國以 Take Five 等行動將金融教育融入交易情境，鼓勵民眾在關鍵時刻停下思考並查證來源。臺灣近年以分齡分眾宣導、校園教育、社群行銷與通路合作擴大訊息覆蓋，並逐步強化警示與承接機制；惟若要進一步提升成效，仍宜由觸及導向推進至行為轉化導向，例如以可操作的查核步驟與即時回報路徑，將宣導訊息轉化為可執行的防禦行動，並使通報、金融關懷與平台處置能有效承接識詐所觸發的求助需求（如表 2-53）。

表 2-53 主要國家識詐面向作法與政策特徵

國家	主要作法	政策特徵
臺灣	分齡分眾宣導、校園與通路合作、結合警示與通報承接	需由觸及導向轉為行為轉化導向，強化查核、阻斷、通報的可操作設計
日本	高齡情境宣導、在地接觸管道、逐步導入風險提示	聚焦高齡脆弱性與情境化詐術，重視社區支持與情境演練
新加坡	全國性防詐平台、推播與回報機制整合	強調即時承接與可操作流程，提升回報與處置效率
澳洲	中央平台整合訊息、多語宣導與媒體協作	兼顧多元族群可近性與一致訊息，強化社會動員之連續性
英國	Take Five 等行動、金融教育融入交易情境	以行為規範化降低誤信，重視在關鍵時刻促發查證行動

資料來源：本研究自行整理。

(二)堵詐面向（電信防護面）

堵詐旨在以電信與通訊端之技術與制度措施，降低民眾接觸詐欺訊息的機會，其防制重點在於建構多層攔阻並以明確法源與資料標準化確保可執行性。國際經驗顯示，來電識別、簡訊寄件者識別制度、惡意網址封鎖與可疑號源處置等措施，若缺乏一致性標準與資料接口，易形成各自攔阻、難以串接的防制斷點；反之，若能在監管授權下建立高風險號碼與網址名單的共享與更新機制，並對重複違規來源採取一致性之限制與停權處置，則可有效降低詐欺訊息的擴散效率。日本、新加坡、澳洲與英國分別在來電管理、簡訊寄件者制度與投資類惡意網址處置上建立較完整制度設計，並強化重複違規者的權限限制與封鎖。臺灣近年亦推進門號管理、簡訊識別與 AI 攔阻等作法；惟跨境 VOIP、境外主機與 VPN 跳板仍可能形成監理斷點，後續宜朝跨境名單同步、處置一致與協作常態化推進，以縮小境外來源在不同法域間的游移空間（如表 2-54）。

表 2-54 主要國家堵詐面向作法與政策特徵

國家	主要作法	政策特徵
臺灣	門號管理、簡訊識別、AI 攔阻與可疑來電及網址處置	需強化跨境合作與名單同步，補足境外來源與跳板造成的監理斷點
日本	來電風險管理、簡訊過濾、釣魚與投資網址封鎖	著重境外滲透的前置攔阻，強化通訊端情境提示
新加坡	簡訊寄件者制度化、風險標示與封鎖	以來源識別提升可辨識性，並強化處置一致性
澳洲	電信監理合作、惡意連結處置、技術攔阻	多點攔阻與快速處置並行，重視資料標準化
英國	監理要求電信及平台反詐義務、偽冒與群發管理	以義務化推動源頭管理，強化一致處置與可檢核性

資料來源：本研究自行整理。

(三)防詐面向（數位經濟平臺面）

防詐面向的核心在於平台責任化與流程管理，亦即將防詐義務由事後下架前移至入口審核、風險標示、帳號管理與跨平台一致處置。各國作法凸顯涉投資廣告必須在入口階段即完成審核與風險提示，涉詐帳號除即時停權外，更需將其風險訊號納入名單共享機制，以降低重複違規者於不同服務間游移；同時，平台管理正與金融阻斷逐步整合，當高風險內容導向私密社群軟體群組或轉帳行為時，防制焦點不再侷限於內容移除，而是透過入口、內容、社群、金流的多層控制降低犯罪完成率。日本於「綜合對策 2.0」中要求 SNS 與搜尋平台導入 AI 事前審查、身分驗證與重複違規帳號的一致性處置機制。新加坡與澳洲在政府與業者的組織合作下，強化平台在地管理責任與資料配合義務，並要求於一定期限內完成防詐措施建置；英國則透過產業承諾與監管要求，推動大型平台加強涉詐內容與帳號管理並提升透明度。臺灣在打詐綱領 2.0 新增「防詐（數位經濟面）」後，防制版圖已延伸至網路廣告、第三方支付與平台責任；後續仍需精緻化分級處置與一致性標準，並強化跨平台名單同步與資料接口，以壓縮重複違規者的迴避空間並提升流程管理的連續性（如表 2-55）。

表 2-55 主要國家防詐面向作法與政策特徵

國家	主要作法	政策特徵
臺灣	防詐面向制度化，加強廣告與平台及第三方支付管理	需建立分級處置與一致標準，強化跨平台名單同步以壓縮重複違規空間
日本	平台內容管理、身分驗證與回應機制強化	風險控管前移至入口與帳號管理，重視即時回應與協作
新加坡	平台責任法制化、在地化管理與資料配合義務	強調期限、標準與可執行性，促成高密度協作
澳洲	產業守則、跨業協議與政府監督	以流程管理串接入口、內容與金流，凸顯協議管理的可持續性
英國	產業承諾與監管要求、透明度提升	以監理驅動平台責任化，強調一致處置與可檢核合規框架

資料來源：本研究自行整理。

(四)阻詐面向（資金流向面）

阻詐面向的國際經驗共同指向時間管理的重要性：在開戶、收受資金、轉出、跨境與兌現等關鍵介入點設置多重把關，並以延遲交易、複核流程與多重驗證搶回處置時間，是降低財損擴大的核心。各國普遍建置跨行資訊平台與標準化欄位，使風險標註與名單同步可即時運作，以縮短警察與金融機構在資訊掌握與處置上的時間落差。日本透過轉帳限額、即時凍結與金融機構通報義務，將時間管理前移至金流啟動初期，新加坡以集中機制統籌即時凍結與被害保護，凸顯快速處置與被害導向並重；澳洲以收款人確認與延遲處理兼顧阻斷與誤攔的平衡；英國以事前警示機制與支付流程管理連結後端補償，使金融機構在交易端承擔更高密度之風控責任。臺灣近年推動跨行預警、臨櫃關懷與風險標註等作法，亦逐步面對虛擬資產、第三方支付與跨境通道造成的處置落差；後續宜持續強化延遲、複核及同步標註的制度前置設計，並提升警銀資訊交換的即時性與欄位一致性，以確保阻詐措施能在流程上形成連續、可追蹤的處置鏈結（如表 2-56）。

表 2-56 主要國家阻詐面向作法與政策特徵

國家	主要作法	政策特徵
臺灣	跨行預警、臨櫃關懷、風險標註與同步	需強化延遲複核制度前置與欄位標準化，以縮短處置時間差
日本	高風險交易控管、即時處置	以速度管理降低外移機率，重視交易關鍵點處置能力
新加坡	集中機制統籌凍結與被害保護	以中樞協作確保即時性，強化被害導向的制度設計
澳洲	收款人確認、延遲處理與分層風控	在阻斷與誤攔間求取平衡，凸顯流程管理與風險分層
英國	事前警示、支付流程管理與責任分擔	以流程義務提高金融端風控密度，並連結補償制度形成誘因

資料來源：本研究自行整理。

(五)懲詐面向（司法執法面）

懲詐面向的政策重點，已由傳統人犯到案、判刑處遇擴展為專責化偵查、跨境合作常態化與財產刑前置化的整合策略。主要國家多採行自由刑量刑與財產刑並重之作法，並在制度設計階段即納入追繳、沒收與返還等機制，以提升剝奪不法所得之確定性與效率；另透過跨境警務合作與情資交換，建立標準化請求程序與即時聯繫管道，提升境外資產凍結與返還之可行性。日本、新加坡、澳洲與英國分別透過專責機構或中央統籌整合查緝能量，聚焦瓦解詐欺集團與追查洗錢水房等核心節點。臺灣近年亦透過檢警調整合、科技偵查法制化與跨境合作推進查緝；惟面對跨境證據取得、追贓返還效率與制裁一致性等結構性限制，後續仍宜強化財產刑工具之前置設計與跨境合作之常態化運作，使懲詐在制度上更具可預測性與確定性，並有效降低犯罪者對犯罪低風險之期待（如表 2-57）。

表 2-57 主要國家懲詐面向作法與政策特徵

國家	主要作法	政策特徵
臺灣	專責化整合、科技偵查法制、跨境合作與追贓	需強化財產刑前置與追贓返還效率，並提升制裁一致性
日本	中央統籌與專責化、跨境查緝與情資交換	強調溯源打擊與境外節點處置，降低跨境斷點對偵查的影響
新加坡	中央合作、跨境追償與司法合作	將追訴與追償並重，程序化、標準化以提高跨境處置效率
澳洲	跨機關合作、聚焦洗錢與數位證據	以科技偵查與司法工具並行，鎖定犯罪鏈的金流與資產節點
英國	專責偵辦、情資導向、產業合作與財產刑工具	將剝奪不法所得納入制度設計，並以跨域整合提升威嚇效果

資料來源：本研究自行整理。

三、綜合評析

整體觀察臺灣與主要國家的防制經驗，可以看出多數法域都已逐步形成從識詐到懲詐的多層次防線；各國政策雖因法制背景、行政架構與風險焦點而有所差異，但其共同邏輯在於以流程管理串接五面向、以時間管理提升阻斷機率、以財產刑提高剝奪確定性。若從情境犯罪預防的角度分析，識詐重在提升風險警覺並促發查核與通報行為；堵詐透過電信攔阻與來源識別增加犯罪者成本；防詐以平台義務與一致處置標準移除可乘之機；阻詐以延遲、複核與同步標註搶回處置時間；懲詐則以追繳、沒收與跨境合作提高犯罪後果之確定性。五面向相互支持，形成由前端預防、中段阻斷到後端追訴的連續防制策略。

若再以犯罪腳本分析方式檢視各國作法，可發現有效防制策略多能對應詐欺犯罪流程中的關鍵階段。其一，犯罪前準備階段包含組織建構、成員招募與技術工具配置，宜透過法制規範、產業責任與技術管制等制度性介入，抬高犯罪起始門檻與整體運作成本。其二，於前端誘導受眾階段，防制重點在於強化投資類廣告之事前審查與明確風險標示，並將警示訊息嵌入搜尋、點擊等高風險介入點，以降低民眾初次接觸詐騙資訊之誤信可能。其三，互動階段則須在社群導流、站外連結或即時通訊過程中設置即時提示與回報管道，使民眾在信任逐步被植入前，仍保有查證與退出之空間。其四，於出金階段，則透過延遲交易、行為確認與即時凍結等機制，爭取緊急處置時間並抑制財損擴大。若其中任一環節形成制度缺口，詐欺集團即可能迅速恢復既有詐欺犯罪之階段性運作，爰此，防制策略應強調跨階段、跨節點之運作連貫性，而非僅仰賴單一措施之重複堆疊，方能有效削弱假投資詐欺犯罪之整體運作能力。

綜合主要國家之制度設計，對臺灣至少具有三點具體可行的借鑑方向：第一，識詐成效評估宜由活動與觸及轉向行為指標，並依高風險族群與使用情境精準投放可操作的查核、阻斷與通報訊息；第二，涉詐內容下架、帳號停權與風險名單共享宜建立明確的分級處置與一致性標準，並推動跨平台共同執行，以降低重複違規者在不同服務間游移；第三，阻詐與懲詐須強化時間管理與財產刑工具的前置設計，在金融交易端預設延遲、收款人確認與跨行同步標註以提升即時性，並在制度規劃階段即納入追繳與沒收，使剝奪不法所得更具效率與確定性。準此，臺灣後續防制策略宜持續沿行為導向識詐精準化、通訊端堵詐制度化、平台責任防詐一致化、金流阻詐時間管理化、司法懲詐財產刑前置化五項方向推進，以提升整體防制策略之可持續性與可回饋性。

第三章 研究設計與實施

本研究在探討相關文獻後，發現現階段臺灣警察防制電信網路假投資詐欺犯罪策略仍存有諸多困境，在文獻資料蒐集過程中亦發現，此類型犯罪隨人類資通訊科技的快速發展及臺灣政治、法律、經濟、社會、文化等背景的改變而不斷演化，國外雖有類似犯罪研究，但與臺灣本土犯罪環境及手法明顯有別，而臺灣相關實證研究亦未臻完整，為解決本研究所發現的相關問題，遂延續前揭文獻探討之相關理論基礎及主要國家防制策略，以順利達成本研究目的為前題，賡續於本章探討包括研究步驟與架構、資料蒐集方法、研究工具、抽樣方法與樣本來源、資料處理與分析、預期研究成果以及研究倫理與限制等。

第一節 研究步驟與架構

一、研究流程與步驟

為達成本研究目的，依據相關文獻擬定研究架構，並運用深度訪談蒐集研究所需資料，本研究相關流程如圖 3-1 所示。

(一)瞭解研究相關問題與背景。

(二)確立研究主題之目的與範圍。

(三)相關文獻資料蒐集研析與探討。

(四)建立研究架構及提出研究計畫。

(五)質性訪談大綱之編製、修正與執行訪談。

(六)訪談資料蒐集與處理及分析編碼。

(七)撰寫論文並提出研究結果和建議。

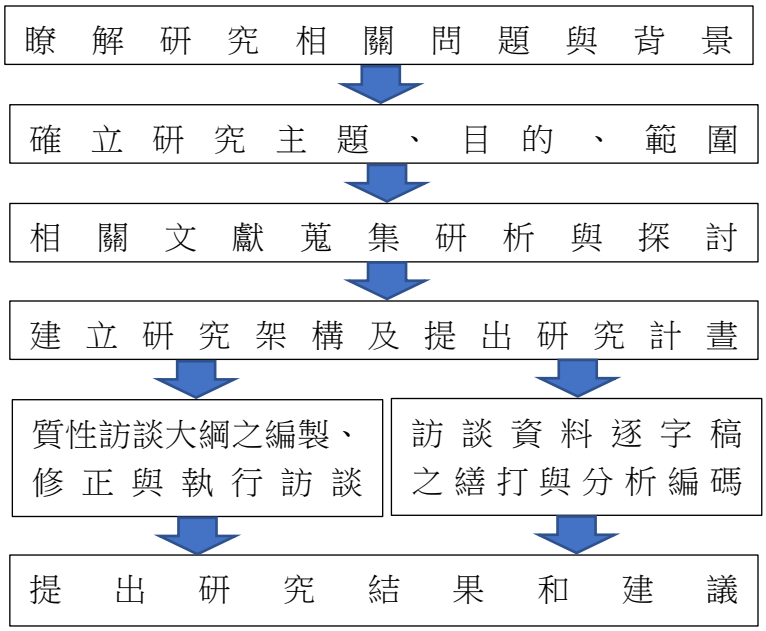


圖 3-1 本研究流程示意圖

資料來源：本研究自繪。

此外，為掌握本研究相關流程，避免發生拖延或遲誤等情事，遂規劃為期 17 個月之研究期程俾強化本研究進度的控管，甘特圖(Gannt’ s Chart)（如圖 3-2）示。

月次 / 工作項目	第 1~3 個月	第 4~7 個月	第 8~9 個月	第 10~12 個月	第 13~14 個月	第 15 個月	第 16 個月	第 17 個月
瞭解研究問題並確定主題	■							
蒐集相關文獻並進行探討		■						
建立研究架構並提出計畫書			■					
修訂訪談大綱與深度訪談				■				
資料編碼與處理				■	■			
資料分析						■		
提出研究結果與建議							■	
提出論文初稿								■
修改論文								
研究進度累計百分比	10%	30%	40%	70%	85%	90%	95%	100%

圖 3-2 本研究工作進度甘特圖

資料來源：本研究自繪。

圖 3-2 所列相關工作項目中，依研究內容性質而分，大致可以區分如下：

(一) 研究整備

本研究方向及主題成立後，旋即進行主題範疇界定，並蒐集各國相關研究文獻資料後，著手執行期程最長之文獻資料回顧與撰寫。

(二) 研擬研究工具

本研究資料蒐集方法係採深度訪談方式之質性實證研究，並根據相關文獻、論理基礎建構本研究架構，深入剖析研究內容，依序研擬深入訪談大綱，同時經過與指導教授多次研討後逐漸定案，並逐步形成相關訪談架構，是本研究實地訪談不可或缺之醞釀階段。

(三) 實施實地訪談

在確立深度訪談大綱後，選定適合訪談的對象並事先約定受訪者，執行實地或電話訪談。訪談期間，研究者將恪遵相關研究倫理規定，同時讓受訪者在心無罣礙情境下，願意真心誠意回答訪問題項，此為實證資料蒐集最重要之階段。

(四) 資料處理與完成研究

由於訪談資料之處理極度耗費時間，且為避免因記憶之流失而影響訪談紀錄之準確度將在完成訪談後隨即整理逐字稿，繼而進行訪談資料的整理與分析。於訪談過程亦將逐步歸納出細類與主類別並時時回顧本研究目的與方向。最後則是撰寫研究成果報告，並提出論文審查之申請。

二、研究架構

依本研究目的、相關理論基礎及國內、外之研究文獻，擬定研究架構如圖 3-3。後續以警察機關、相關政府部門人員及業者為對象的深度訪談，均係以此研究架構為根據。

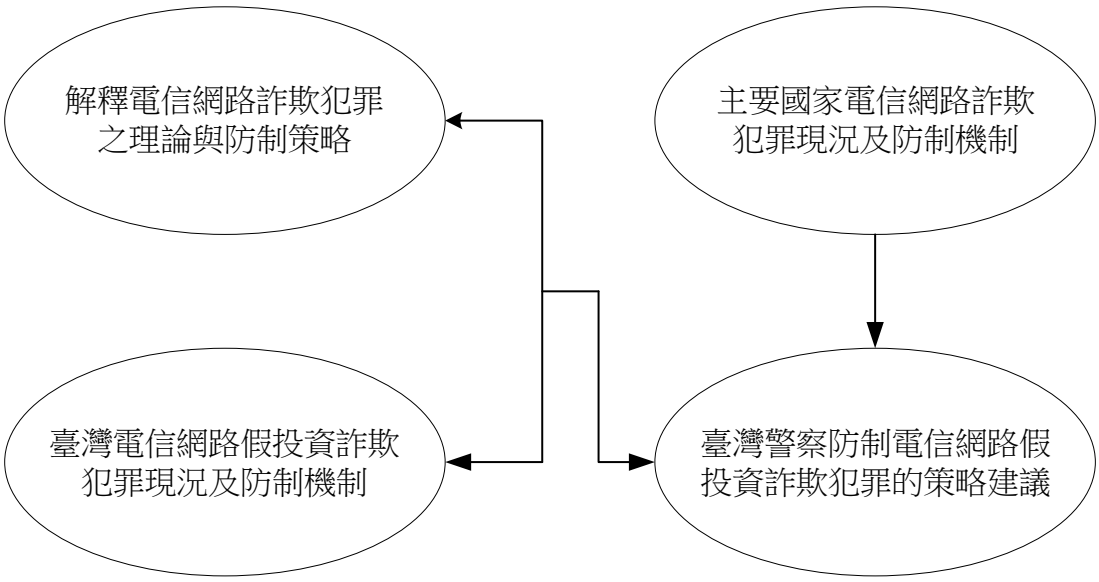


圖 3-3 本研究架構圖

資料來源：本研究自繪。

本研究架構中「解釋電信網路假投資詐欺犯罪之理論與防制策略」概念面向，係本研究在蒐集國內外相關文獻並在進行研讀之後，發現臺灣目前對電信網路假投資詐欺犯罪事件發生的當下的環境因素，尚缺成熟的解釋的能力。因此，本研究參採環境犯罪學觀點，以理性選擇理論詮釋電信網路假投資詐欺犯罪者在尋找犯罪「機會」和「選擇」犯罪行為時的有限理性；續以日常活動理論分析有動機的犯罪者、合適的標的物及缺乏有能力的監控者等三種促進犯罪因素同時存在的時空環境，解析犯罪者參與犯罪與民眾被害的影響因素，以全面瞭解影響犯罪發生的情境因素；再蒐集相關犯罪案例，並以犯罪腳本理論作為分析工具，將犯罪行為順序的所有階段，詳細並全面的描述，使犯罪過程更容易識別和理解，續以問題導向警政理論分析相關防制犯罪策略，最後運用情境犯罪預防理論以改變目標環境為手段來預防電信網路假投資詐欺犯罪的發生，作為擬定臺灣警察防制電信網路假投資詐欺犯罪有效策略之假設。

在「臺灣電信網路假投資詐欺犯罪現況及防制機制」及「主要國家電信網路詐欺犯罪現況及防制機制」等概念面向，係分別蒐集分析臺灣警政署及法務部與日本、新加坡、澳

洲、英國等地區的官方次級（統計）資料，藉以瞭解比較臺灣與主要地區(國家)電信網路假投資詐欺犯罪現況與發展趨勢及防制機制。

因此，本研究運用深入訪談警察人員、相關政府部門人員及業者，藉以蒐集犯罪者動機來源及日常生活形態與被害人的特徵及受害情境；犯罪全部過程的腳本；並分析臺灣相關防制策略。最後以問題導向警政理論綜合分析犯罪腳本羅列之所有可能干預阻斷犯罪完成的重要節點，將這些可干預犯罪完成的重要節點，運用情境犯罪預防理論的觀點並參考主要國家防制策略，研提臺灣警察防制電信網路假投資詐欺犯罪策略的建議。

第二節 資料蒐集方法

本研究係透過蒐集國內、外相關研究與實務對策為理論基礎，並進而採用深度訪談方法進行實證資料之蒐集而達成相關研究目的。具體而言，本研究資料蒐集方法包括：

一、文獻探討法

本研究盡量蒐集國內、外有關電信網路假投資詐欺犯罪之相關論文或期刊等文獻，以及日本、新加坡、英國、澳洲等國家防制策略。此外蒐集 2024 年 1 月 1 日至 9 月 24 日警政署刑事警察破獲之假投資案件新聞資料個案計 35 件，分別就新聞發布日期、查獲時間、查獲地點、查獲嫌犯、案情摘要、查獲贓證物等整理歸納分析(如附錄一)，藉以瞭解臺灣電信網路假投資詐欺犯罪現況，據以形成本研究主要概念架構，以及後續研究建議方向。

二、深度訪談法

本研究所採用的質性研究資料蒐集法(Qualitative method)之一，即深度訪談(In-depthinterview method)，由研究者事先擬定半結構式訪談大綱，再訪談警察、相關政府部門人員及業者等實務專家，藉以蒐集電信網路假投資詐欺犯罪者選擇犯罪標的理由及犯罪標的吸引潛在犯罪人的原因；以及犯罪全部過程的腳本；並瞭解臺灣目前防制電信網路假投資詐欺犯罪策略的缺漏，以及目前實務界面臨之困境外，同時尋求有效的對策。簡言之，即藉上揭相關基本問題的釐清，以為建構及修正本研究概念架構之依據。

在「解釋電信網路假投資詐欺犯罪之理論與防制策略」部分主要想透過警察人員瞭解犯罪者的理性？環境對犯罪的影響？犯罪者及被害人的生活形態？犯罪者與被害人接觸的主要管道？透過所有被訪談者瞭解完整的犯罪腳本（包括：犯罪前準備行為、主要犯罪行為、犯罪後行為）？民眾被害要關鍵？阻斷犯罪的主要關鍵？等，在「臺灣電信網路假投資詐欺犯罪現況及防制機制」部分；主要想透過所有被訪談者瞭解臺灣防制電信網路假投資詐欺犯罪的成效？困境？對未來策略之建議？等。

第三節 研究工具

根據前揭本研究之設計，本研究之訪談對象主要區分為三類：一、行政院打擊詐欺指揮中心相關部會人員；二、內政部警政署刑事警察局「詐欺犯罪防制中心」的相關業務主管、承辦人及外勤大隊有偵辦「電信網路假投資詐欺犯罪」經驗的主管及第一線偵查人員，與直轄市政府警察局及縣市警察局刑事警察大隊有偵辦「電信網路假投資詐欺犯罪」經驗之主管及第一線員警；三、相關業者(知名網路平台之合規遵循和風險管理主管人員)，訪談內容主要為前述研究架構中所含蓋的：解釋電信網路假投資詐欺犯罪之理論與防制策略及臺灣電信網路假投資詐欺犯罪現況及防制機制等方面的概念，惟此三類人員各有業務職掌分工及專業背景均有不同，故而訪談內容亦有所不同，有關訪談大綱內容詳如（如附錄二）。

第四節 抽樣方法與樣本來源

本研究訪談對象之取樣方式，係以立意抽樣（Purposive sampling)為主，輔以滾雪球方式，直到資料飽和為止。訪問對象在中央政府部分，包含行政院打擊詐欺指揮中心(含內政部、國家通訊傳播委員會、數位發展部、金融監督管理委員會)及內政部警政署刑事警察局「詐欺犯罪防制中心」的相關業務主管、承辦人與外勤大隊有偵辦「電信網路假投資詐欺犯罪」經驗的主管及第一線偵查人員；在直轄市政府警察局及縣市警察局部分，則訪談新北市政府警察局分局偵查隊及新竹縣政府警察局刑事警察大隊有偵辦「電信網路假投資詐欺犯罪」經驗之主管及第一線員警，在相關業者部分則訪談知名網路平台之合規遵循和風險管理主管人員總計 13 名，訪談對象分配表（如表 3-1）。

表 3-1 深度訪談對象分配表

編號	職業類別	年齡	業務（工作）職掌	工作年資
P1	刑事警察	57	防制詐欺犯罪策略規劃及執行	33 年（1992 年開始）
P2	刑事警察	54	防制詐欺犯罪策略規劃及執行	34 年（1991 年開始）
P3	刑事警察	50	防制詐欺犯罪策略規劃及執行	28 年（1998 年開始）
P4	刑事警察	52	防制詐欺犯罪策略規劃及執行	29 年（1997 年開始）
P5	刑事警察	38	執行防制詐欺犯罪策略	17 年（2008 年開始）
P6	刑事警察	38	執行防制詐欺犯罪策略	18 年（2007 年開始）
P7	刑事警察	34	執行防制詐欺犯罪策略	7 年（2017 年開始）
P8	刑事警察	45	執行防制詐欺犯罪策略	23 年（2002 年開始）
P9	刑事警察	48	執行防制詐欺犯罪策略	24 年（2001 年開始）
G1	部會人員	55	督導部會執行防制詐欺策略	22 年（2003 年開始）
G2	部會人員	37	督導部會執行防制詐欺策略	2 年（2023 年開始）
G3	部會人員	43	督導部會執行防制詐欺策略	12 年（2013 年開始）
B1	民間業者	40	合規遵循和風險管理	12 年（2013 年開始）

資料來源：本研究自製。

第五節 資料處理與分析

研究者在製作訪談逐字稿前將先仔細聆聽一次訪談過程錄音，以建構被訪談者整體思維脈絡及情境過程，然後，再由研究者親自製作訪談逐字稿，進行資料整理與分析，在資料分析過程將逐步歸納出細目類別與主要類別。詳言之，本研究訪談資料之處理與分析，依次如下：

一、仔細聆聽一次訪談過程錄音
二、製作訪談逐字稿。
三、檢視並修正逐字稿。
四、執行概念之文義編碼。
五、整合各文義編碼，再發展細目類別。
六、修正細目類別，再發展主要類別。

第六節 研究倫理

本研究採文獻探討與深度訪談法進行資料蒐集與分析，故研究者對倫理的考量貫穿本研究各階段。回顧研究倫理的歷史脈絡，二次世界大戰後學界省思生物醫學領域對研究參與者身心福祉之忽視，而逐漸形成現代研究倫理架構，包括 1947 年《紐倫堡守則》強調知情同意與自主權、1964 年《赫爾辛基宣言》確立研究參與者福祉優先原則，及 1978 年《貝爾蒙報告》提出尊重人格、行善與正義三大原則（蔡甫昌、林芝宇、張至寧，2008；洪瑞斌、莊騏嘉、陳筱婷，2015）。此等規範雖源自生物醫學研究，但其精神亦被廣泛應用於人文與社會科學研究領域（李安明，2016）。

然而，質性研究強調研究者與研究參與者在情境脈絡中的互動關係，重視人的主體性、意義建構及脈絡彈性（Doyle & Buckley, 2017）。此種研究特質使實證主義取向的研究倫理架構在某些情況下顯得不完全適用。尤其本研究的研究參與者均具備有專業身分及素養，若一律視為被動受保護的「受試者」，反而可能忽略其參與研究的主體地位；又如研究倫理審查若僅依循實證主義觀點而忽略質性研究的開放性與過程性特質，也可能限制研究者依照研究情境調整研究方法的空間。此外，質性研究中研究者與研究參與者之間關係常隨時間及研究進程而產生而變化，研究者不可能在研究初始即能預知後續可能遭遇的倫理情境（Doyle & Buckley, 2017）。

基於上述考量，本研究雖側重研究倫理重要國際規範，但仍依質性研究特性調整適用方式。因此，本研究在正式訪談前，均依循《紐倫堡守則》與《貝爾蒙原則》的核心精神，向受訪者充分說明研究目的、訪談方式、資料使用範圍、個資保護方式與可能風險，並告知其享有隨時退出研究之權利，不須負擔任何不利益；待受訪者理解並同意後方簽署訪談同意書（附錄三），以確保其自主意志與人格尊重之原則。

此外，本研究之受訪者包含刑事警察人員與政府官員，涵涉敏感之犯罪事實、詐欺手

法與偵查技術等議題，若不慎揭露逐字內容，極易使熟識者辨識其身分，增加其人身與職涯風險。因此，本研究訪談所得內容僅作整體性分析，並於後續處理中進行去識別化處理，以維護受訪者之隱私與個資安全。並且不將訪談逐字稿及簽署之同意書檢附於論文附件，僅於論文審查時備查；論文附錄僅提供空白同意書與訪談大綱，以避免可能之倫理風險。

總言之，本研究之研究倫理實踐以尊重、行善與正義為核心，兼顧質性研究之互動性、脈絡性與參與者主體性，確保研究過程與成果均符合倫理要求，並維護研究參與者之權益與安全。

第四章 深度訪談資料分析與討論

本研究採質性研究訪談資料蒐集法之深度訪談，訪談對象為臺灣刑事警察人員 9 位（受訪者編碼代號：P1-P9）;「行政院打擊詐欺指揮中心」督導各部會執行防制詐欺策略人員 3 位（受訪者編碼代號：G1-G3）；知名網路平台之合規遵循和風險管理主管人員 1 位（受訪者編碼代號：B1），合計 13 位，依各自專業領域及實務經驗，就目前臺灣警察防制電信網路假投資詐欺犯罪策略表達看法，本研究在完成受訪者訪談逐字稿後，即將所得資料歸類、排序與分組，同時透過比較及交叉比對方式，評估資料的可信度，以作為改進對資料組型的理解，本研究資料分析較傾向採用歸納（Inductive reasoning）方式，但在適當時機，同時採用演繹（Deductive reasoning）思考的方式，作為撰寫抽象的綜合性論題或概念時的思維邏輯，以下謹就本研究深度訪談資料進行分析與討論。

第一節 電信網路假投資犯罪的成因與現況

為瞭解我國電信網路假投資詐欺犯罪的成因及現況，作為推動警察防制是類犯罪策略參考，本研究循理性選擇及日常活動理論觀點，分析有動機的犯罪者及合適的被害人的有限理性及日常生活形態，並剖析缺乏有監控能力者在場的情境，以瞭解促進犯罪事件發生不可或缺的三要素，同時闡明犯罪者參與犯罪的影響因素，再綜合上述促使犯罪發生因素，企盼提出更具體的干預防制策略，以有效降低犯罪機會。爰此，本節請受訪者分別就電信網路詐欺犯罪者動機來源及日常生活形態、合適的被害人之日常生活形態；及缺乏有監控能力者在場的情境等促進犯罪發生的三要素，與犯罪者參與犯罪的影響因素；表達意見及看法後分析如次。

一、犯罪者動機來源及日常生活形態

理性選擇觀點強調環境會對犯罪行為產生直接影響，而環境因素包括日常生活的方式及動機、需求與誘因等，同時也是為實現特定目標而採取工具性行動的特殊環境，該觀點認為，犯罪是一種有目的、蓄意的行為，是為了使犯罪者受益，犯罪的好處包括滿足通常的人性動機，如性滿足、興奮、自主、欽佩、報復、控制、減輕緊張、物質財富等的慾望。當然，金錢可以買到許多這樣的滿足感，因此它就成為犯罪的一個方便而重要的目標，而電信網路假投資詐欺犯罪的目的即是在獲取金錢，該類犯罪的本質即涵蓋被查獲或犯罪失敗的風險，犯罪的成本和可獲得的利益也很難提前估算，縱使犯罪者盡最大努力評估對自己有利與不利的因素後，採取最有利於己的行動，然而，犯罪者的掌握的資訊及犯罪能力均有其限度，因此，犯罪者最後可能只會獲得「滿意」的結果，而不是「最佳」的結果。根據以上的觀點，本研究分析發現從事電信網路假投資詐欺犯罪的目的都在獲取金錢利益，大都有好逸惡勞，貪圖物質享受情形，且參與黑道幫派犯罪組織情況明顯，犯罪者多為男性，年齡多介於 15 至 40 歲之間，教育程度則大都集中於國（高）中或輟學，多無正當職業，其謀生能力較低下，但仍有少部分具有專業能力。

(一)犯罪的目的都在獲取金錢利益

電信網路假投資詐欺犯罪集團善於利用資通訊科技設備及方法，以分散犯罪地點並隱身境外實行犯罪，在當地國刻意保護包庇下不易為警方查獲，即便遭到查獲詐欺犯罪行為，也常因該等犯罪行為涉及跨境執法合作，完整取證相當困難，在缺乏完備犯罪事證情況下，被判之刑責通常偏低。因此，全數受訪者都認為，犯罪者基於理性選擇，認為從事電信網路假投資詐欺犯罪，遭執法人員查獲的機率不高，犯罪風險小，獲取不法金錢利益快速而安全。

我想當然都是為了錢啦(P1-1-1-1)

你看有的都是「甲賀道相報」(閩南語)，為什麼是「賀」(閩南語)就是利益 (P2-1-3-2)

我覺得營利是 1 個最大的目標啦(P3-1-1-1)

對於一個領著基本工資、看不到未來的年輕人來說，當個「車手」一天就能賺到一個月的薪水，這種誘惑幾乎無法抗拒。 (P4-1-1-1)

我們實務上看到蠻多人，其實都是以電信詐欺維生，所以我相信那是他的動機，也是他的目的啦(P5-1-1-1)

都是為了利益，都是為了錢，他們的目的他們自己都有評估過，可能做這樣的事情，被抓的機會是比較低，都有僥倖心態在(P6-1-1-1)

十之八九都是，幾乎都是為了錢(P7-1-1-1)

大多都是因為經濟狀況不佳缺錢，或者是年輕人想要做輕鬆、快速賺錢的工作，而因而來參與犯罪的 (P8-1-1-1)

就是要賺錢嘛，他們就是幫派的成員，你要賺錢，所以他們去從事這個詐欺。(P9-1-1-1)

但是詐欺在刑法法益來講，它就是金錢法益，所以他動機就是錢嘛(B1-1-1-1)

(二)大都有好逸惡勞，且貪圖物質享受情形

人類天生本有好逸惡勞及趨吉避兇的本能，所以會選擇最輕鬆的方法來實現生活目標。因此，人們在日常生活中的行為都是在避免痛苦、追求快樂及滿足自我利益，受訪者 P4、P5 及 P8 即表示，電信網路假投資詐欺犯罪者，是一群低自我控制，好逸惡勞，想快速致富，生活作息不正常且貪圖物質享受的群體。

一旦體驗過那種揮霍的生活，要他再回去領一個月三萬塊的薪水，他會覺得那根本不是人過的日子。(P4-1-1-2)

他們就是一群很生活糜爛的一夥人，沒什麼謀生能力，你叫他去做苦工，他沒辦法，但是你就要他去 ATM 按一按領錢這樣他就能賺錢了，錢拿到了就去買二手車，去酒店，然後每天都睡到中午 12 點(P5-1-3-2)

參與犯罪的人的生活模式，大多是傾向比較好逸惡勞的那種心態，或者是他眼高手低，然後想要快速的賺錢致富，不願意用正當的方式來賺取合法的錢財 (P8-1-3-2)

(三)參與黑道幫派犯罪組織情況明顯

依據內政部警政署刑事警察局統計，近五年臺灣電信網路假投資詐欺犯罪的財損將近 484 億元，持續穩居臺灣詐欺類犯罪財損第一名，歸納多位受訪者意見，由於此類犯罪相較於傳統暴力犯罪，犯罪者的人身安全風險極低，而獲取不法利益額度卻極為龐大，且有不易遭執法單位查獲，就算遭查緝被判之刑責通常偏低的特性，促使黑道幫派組織在成本效益考量的理性選擇下紛紛糾集幫眾加入犯罪，加上黑道幫派組織比較容易召募到各專業領域的不肖人員，又可運用黑惡勢力有效制約車手，防範遭黑吃黑，且洗錢的管道暢通，並可為境外詐欺機房撐起保護傘，不受當地的黑道幫派組織侵擾，使得此類犯罪成為黑道幫派組織的重要由經濟來源。

我覺得他的黑道身分，可能讓他更便於去找這些詐欺集團的成員，或者是他在別的國家，他

要能夠在當地不要被侵擾，它的黑道身份，有一定的幫助。(P3-1-3-1)

前一兩年的台版柬埔寨那些，或許就需要一些黑道來控制，因為車手時有所聞啊，他們會把帳款拿了就黑吃黑跑掉了啊，一定要幫派的人才有辦法將這些人抓回來。(P5-1-3-1)

黑幫介入的很大的 1 塊都是在車手端，很大的原因是因為怕車手黑吃黑，唯有靠黑幫的力量才有辦法去約制，把所有的錢拿回來。(P6-1-3-1)

我們正常人是沒有辦法洗錢的，不管你再厲害都一樣，你一定要有 1 個固定的組織去做統整規劃，那大部分上面應該是黑道啦。(P7-1-3-1)

許多黑道幫派都有經營詐欺的產業，從上游到下游，都會派他的幫眾來參與，那比起用強暴、脅迫的手段來取得錢財來的輕鬆好賺，又不用以命來跟他相拼，稍微比較安全一點（P8-1-3-1）

因為他們要分工啊，彼此都要信任啊，如果不同公司的人或者不認識或不熟，很可能會被黑吃黑，所以他們要在同 1 個 Team 裡面，就是在同 1 個幫派裡面。(P9-1-3-1)

(四)犯罪者多為男性，年齡多介於 15 至 40 歲之間

依據內政部警政署刑事警察局統計近 5 年(2020-2024)查獲詐欺犯罪分布年齡顯示，犯罪集團多召募 18 至 39 歲之間互相不認識之年輕人實施參與犯罪，與多位受訪者的觀察相近。

犯嫌年紀二十歲到四十歲，這個 Range 是最多的。(P2-1-3-3)
犯罪人年紀在 25 歲到 40 歲之間。(P3-1-3-3)
年紀其實都比較偏年輕…大概可能二、三十歲是最多的。(P6-1-3-3)
那年紀來講，二、三十歲的還是佔比較大的比例。(P8-1-3-3)
大概在 20 歲上下吧（P9-1-3-3）

受訪者 P7 及 P9 更認為犯罪集團會糾集未成年或 20 歲以下的人員擔任車手，除比較容易操控外，亦可預防遭車手黑吃黑捲款潛逃，同時可規避法律責任，至於招募犯罪成員階層*與收水階層的成員，則由犯罪集團核心人員擔任其年齡大都介於 20 歲到 30 歲之間。*

年齡段 20 到 30 的比較多…屬於招募階層跟收水階層，車手他們其實不會用自己的人來作…車手現在越來越年輕了…他們會盡量先找未成年的，未成年的找不到之後，可能就會找一些 20 歲以下的(P7-1-3-3)
也有很多未成年的，十四五歲的（P9-1-3-3）

另外，多位受訪者認為，參與電信網路假投資詐欺犯罪者大都為男性為主，女性則相對少見，受訪者 P2 表示臺灣社會對女性的性別刻板印象仍然存在，社會對女性的期待與要求也比較多，而且女性在人格特質上，也比較不會輕易的參與詐欺犯罪。

還是以男性為主，…女性在人格特質上，也比較不會輕易的就走這條路（P2-1-3-3）
男生居多，六比四…我看到的都是男生(P3-1-3-3)
大概都是男生啦(P5-1-3-3)
性別男生幾乎大概是八比二，對女生(P6-1-3-3)
男性居多，很少遇到女性(P7-1-3-3)
大部分還是以男性為居多啦（P8-1-3-3）

受訪者 P6 則更進一步說明，有些犯罪集團會利用懷孕的女性擔任取款車手，藉以利用刑事訴訟法第 467 條所規定懷胎五月以上，為保障孕婦和胎兒的健康，避免在懷孕期間進行羈押之規定，以避免遭查獲時被檢察官向法院聲請羈押。

我們之前有發現有一些詐欺集團會請懷孕的女生去當車手，為什麼？因為她不會被羈押，一定交保，那是刑訴法寫的懷孕超過 5 個月，就是交保(P6-1-3-3)

(五)教育程度大都集中於國（高）中或輟學，且多無正當職業

多位受訪者認為，參與電信網路假投資詐欺犯罪者的學歷大都集中國(高)中甚至輟學的青少年，如受訪者 P5 及 P7 即表示，犯罪集團常吸收家庭結構不完整，沒有學習熱忱，對學校依附較差的青少年加入犯罪集團，再由這些青少年向同儕炫耀高犯罪所得，如購買高價手機，花錢出手濶綽等偏差價值觀，吸引同儕融入偏差的生活環境，進而參與犯罪。

大概都可能國中或高中就是很多都是輟學的，其實就是剛剛前面講的，早早就交到壞朋友就離開學校了(P5-1-3-3)

他們會想要過得比較奢華…然後炫耀…跟同儕炫耀是 1 個很重要動機(P7-1-3)

不滿高中吧，高中未畢業蠻多的(P7-1-3-3)

在國中階段就輟學了，就沒讀書了（P9-1-3-3)。

學歷以高中職為主（P8-1-3-3)

但受訪者 P3 表示，由於制作網路假廣告需具備相當的資工專業知識及技能，所以犯罪者多為大學資工相關科系畢業，學歷較一般機房接電話的電話手或收款的車手為高。

假廣告學歷會比較高，大學啦(P3-1-3-3)。

多位受訪者表示，犯罪者大多數無正當職業或經濟收入較弱勢的族群，受訪者 P6 更進一步表示，有很多的犯罪成員都是宮廟中負責特定科儀或任務的陣頭組織人員。

很多職業都是宮廟的，宮廟的八加九非常的多(P6-1-3-3)

通常都是無業，無業才會作這個(P7-1-3-3)

大部分其實也沒有什麼正當職業，不然就是，因為沒有好的工作，才會去從事這個詐欺（P8-1-3-3)

大概十三四歲就開始出社會了，都沒有正常職業（P9-1-3-3)

(六)大部分謀生能力較低下，少部分具有專業能力

依理性選擇理論顯示，當前的客觀環境因素常是促使人們犯罪與否的重要影響因素，而犯罪者自身的謀生能力即是一個重要因素，如受訪者 P1 表示，參與實施電信網路假投資詐欺犯罪者一般沒有一技之長，不具備專業能力，謀生能力較差，且有經濟能力窘迫的情形；受訪者 P3 則認為，參與犯罪者有低薪或失業的情形，需要參與電信網路假投資詐欺犯罪以改善其經濟生活。

他們在臺灣沒有一技之長…這些基層的詐欺集團成員啊，你叫他出來作正當的事，他能夠做什麼事？他能夠賺多少錢？(P1-1-3)

可能是比較藍領階級的，…因為他如果在臺灣薪水好，他也不會做詐欺集團，可能會有一些想要轉職的想法，或者是在臺灣沒有工作了，然後他去轉行作這個(P3-1-3-2)

但受訪者 P1 及 P3 亦同時表示，由於電信網路假投資詐欺犯罪過程亟需擁有專業知能的人員加入協助，諸如協助製作詐欺廣告；開發假投資 APP；提供資通訊系統架設及金融科技(如人頭帳戶、虛擬通貨)服務等資通訊技術；甚至吸收不肖執法人員或律師以包庇犯並掌握執法人員偵查進度；銀行從業人員協助匯款及洗錢；地政士協助詐欺被害人不動產。

那種所謂的專業人士，在協助設置詐欺平台的、在洗錢的、在幫忙不動產過戶抵押的地政士啊、幫忙打官司的律師等等這些人。(P1-1-3)

但是如果前半段的資通訊的服務，我覺得可能會有一些合法的業者來幫忙(P3-1-3)

二、被害人的特徵及受害情境

依照日常活動理論揭示，民眾之所以會成為電信網路假投資詐欺犯罪的被害人，大多數是因為其日常生活形態，經常曝露在有利於有動機的犯罪者出現的環境，加上本身欠缺識詐及防詐知能，誤信犯罪集團提供的虛假投資訊息，在追逐最大利益的有限理性認知下，選擇自認為最有利，最能滿足自己需求的投資行為，而誤陷犯罪集團所設圈套致蒙受鉅額金錢損失。近年來臺灣的科技產業發達，造就人民收入日益提高及民間各種投資風氣盛行，詐欺集團利用民眾急於獲利心態，趁機鎖定經濟情況較為寬裕，手頭有一定積蓄，且有投資獲利需求的民眾，以投資飆股、虛擬貨幣、期貨、外匯及基金等名義吸引民眾加入詐欺集團所架設的不實投資網站或下載 APP，再利用精心編製客製化詐欺劇本，以獲取不知情被害民眾的信任，使其深陷在詐欺情境中，直到被掏光所有錢財，始驚覺遭詐欺，造成民眾鉅額財產損失。根據以上的觀點，本研究分析發現，電信網路假投資詐欺被害人多數為退休人士，且女性多於男性；渠等日常 生活單純孤僻，對自身投資能力有自信；經濟情況較為寬裕，且有投資獲利需求； 經常瀏覽網路社群媒體投資資訊，且識詐能力不足； 遭詐時間跨度長，且常有重複被害情況發生。

(一)多數為退休人士，且女性多於男性

依據內政部警政署刑事警察局統計，2024 年臺灣詐欺被害總人數為 132,445 人，其中 65 歲以上被害人數為 9,335 人（占比約 7.05%）。這些高齡被害人又以電信網路假投資詐欺犯罪受害情形最為嚴重，被害人數高達 4737 人（佔比約 50.74%）。而本研究多數受訪者亦表示，電信網路假投資詐欺犯罪的被害人多數為年紀稍長的退休人士，因閒暇時間較多，長時間滑手機，經常曝露在有利於有動機的犯罪者出現的網路環境中，較易成為詐欺集團鎖定對象，造成受害情況較高，受訪者 P1 更表示，此類案件的被害人，有女性高於男性的現象。

假投資詐欺基本上…是退休人員居多，而且年齡稍微偏長…而且女性被害人會高過於男性，大概有這樣子的特徵。(P1-1-2-2)

我們今天要討論的是假投資，如果是被害人的角度的話…這一些退休族群的生活模式吃飽太閒。(P2-1-4)

有一些老人家其實他退休之後，在家沒事一直滑，像滑抖音一樣，以前的那個網站要看十分鐘，然後那個 youtube 要看五分鐘，那抖音只要 30 秒一直滑，所以抖音會餵給你，你喜歡看的東西，那民眾現在只要她對網路上它有一定的黏著度，然後加上詐欺集團，他能夠透過一些假廣告去投注，事實上它可以目標到這些人，這些人就很容易變成被害。(P3-1-2-2)

許多退休長者、單身人士缺乏傾訴的對象，騙子正好填補了這個心理缺口。(P4-1-2-2)

被害人的樣子，看起來其實都是比較單純的退休人員啦。(P5-1-4)

年輕人比較不會被假投資詐欺。(P6-1-2-2)

被害者大部分都是…，退休的族群或者是長者，他們的生活模式大概是這樣，有時候太閒，就是一直會去看一些投資的理財的資訊。(P8-1-4)

(二)生活單純孤僻，對自身投資能力有自信

受訪者 P3、P5、P7 表示，詐欺集團經常鎖定高齡退休族群，利用渠等年老退休，社交圈變得比較封閉，或因長期獨居，欠缺親人關懷，人際關係較為疏離，讓犯罪集團有可趁之機，偽以虛情假意的噓寒問暖，逐步拉近與被害人之間的距離並取得其信任，如果再加上被害人人格特質比較孤僻，容易固執己見，對詐欺手法與最新話術又缺乏了解，即容易使得這些人誤入犯罪集團預設的騙局而不自知。

有時候可能是跟被害人的特質有關，第 1 個這個被害人可能比較孤僻，家人不關心…變成孤僻的個性，誰都不相信，當電話的那 1 頭進來問候…他找不到人家問，他最後選擇就是跳入情境被騙。(P3-1-4-2)

他們噓寒問暖，取得了被害人的信任，這個信任就成了詐欺的破口。(P4-1-2-2)

就是社交比較封閉，他沒有辦法接受新的事物。(P5-1-4)

認真說就是你缺乏警覺，缺乏社交，缺乏實際上的社交，我發現好像蠻常會有這種情況就是你交友圈不夠廣，然後去用這些東西的時候，很容易就受騙了(P7-1-4)

另外，受訪者 P6 提到，部分被害人自認本身對各項金融商品投資運作很熟悉，對自已投資理財能力亦相當有自信，但仍不敵犯罪集團掌握資訊不對等的優勢，運用配合社會脈動，利用精心杜撰的客製化假投資詐欺劇本，由多名成員分別扮演不同詐欺角色，藉以操弄、掌握被害人急於獲利的心態，誘騙渠等在跟風投資的羊群效應下，將大筆錢財投入虛假的投資標的，造成鉅額財產損失。

以假投資來說的話…他們可能都覺得自己會看什麼線圖會分析，相關的什麼技術指標等等(P6-1-4-1)

(三)經濟情況較為寬裕，且有投資獲利需求

過去 60 餘年來，在臺灣全民胼手胝足的共同努力下，經濟發展表現亮眼，展現強勁的活力與韌性，並在國際競爭力排名中持續進步。隨著經濟穩定的發展，近年來臺灣人民收入日益提高，隨著財富持續累積，民間游資日益氾濫，使得百姓投資風氣盛行，各項金融投資工具亦推陳出新，讓人眼花瞭亂。因此，多數的受訪者均表示，電信網路假投資詐欺犯罪集團，趁機鎖定經濟情況較為寬裕，手頭有一定積蓄，且有投資獲利需求，急於快速獲利致富傾向的民眾，以各種名義虛構不實投資訊息，吸引民眾踏入歹徒所設置情境陷阱，造成民眾鉅額財產損失。

可能是對我們整個社會投資環境運作不是很熟悉，又有時間又有一點錢的這些特質的人，他就容易被這樣子的 1 個假投資詐欺吸引(P1-1-2-2)。

這個還是屬於 1 個財產性犯罪，你如果身上沒有錢，你就不會這麼想，但是你這個錢一定是閒錢…你的念頭其實就是，你的需要跟想要以外，你還有更多的…在經濟金錢上的滿足。(P2-1-2-2)

一個宣稱「保證獲利」、「穩賺不賠」、「掌握內線消息」的投資機會出現，就像是沙漠中的綠洲，對焦慮的民眾有致命的吸引力。(P4-1-2-2)

你要講投資詐欺，因為金額都很高嘛，你退休家裡有錢，你才有可能對不對？…這幾年的台股，這個整個資金進來，台積電什麼大家都會想要被動收入，更多人想要去投資，就會讓大家更容易成為那個被害人，…想要被動收入嘛，對啊，一堆少年股神，大家都在報明牌啊，這也一夜致富，還是買什麼虛擬貨幣，大家也想拚一下，結果一拼都被詐欺(P5-1-2-2)

他們可能本身已經有一定的資產了所以想要投資，然後想要致富…就是投其所好，你今天就是在網路上，就是讓他充斥這個明牌，讓他充斥著某某投資顧問老師的這樣的一些字眼，就吸引他一步一步的踏入那個陷阱，我覺得被害人自己其實他也是心甘情願被引導到這裡面，他會覺得這麼剛好，我剛好有想要投資，剛好臉書上面就跳出來，所以一拍即合他就進去了嘛(P6-1-2-2)

會被騙錢的大概都是，想要投資的人，就是我遇到很多都是最近被害人，被騙錢的大概都是錢很多沒地方放的人。他們就會去網路上，可能看到有什麼投資標的，比如說什麼朋友介紹，什麼股友社的那種飆股的群組，他們就會加入了，大概就是比較有閒的人吧(P7-1-4-1)。

被害者大部分都是因為退休了，然後在家閒閒沒事，手上又有一些積蓄想要投資賺錢…他們的生活模式大概是這樣，對有時候太閒，就是一直會去看一些投資的理財的資訊 (P8-1-4)

(四)經常瀏覽網路社群媒體投資資訊，且識詐能力不足

近年來資通訊科技高度發達，大幅改變人類社交及經濟活動模式，網路社群媒體為提高廣告效益，利用數據分析和預測的技術，採用演算法推播廣告，以實現更有效的分眾行銷，惟此項技術卻遭犯罪集團掌握並利用，為犯罪者提供更多元接觸被害人的管道。多位受訪者表示，電信網路假投資詐欺集團利用演算法來預測和選擇，最有可能對假投資詐欺廣告產生興趣的用戶，在渠瀏覽網路社群媒體投資資訊時，強制彈跳出「高獲利投資理財」等廣告，讓詐欺訊息更容易出現在使用者眼前，吸引民眾一時好奇點選觀看，又或以美女或俊男身分利用網際網路在臉書、IG 等社群網站結識被害人，再引誘民眾加入渠所架設的不實投資網站，而遂行詐欺目的。

假投資詐欺基本上…對我們整個社會投資環境運作不是很熟悉。(P1-1-2-2)。

我剛剛有提到兩個部分，1 個是詐團主動丟訊息給你的，1 個是你閒閒無聊透過社群自己去看到，你持續的在瀏覽，主動跟被動這兩種方式…主力還是在網路跟通訊軟體平台…前端先接觸到 WEB 網路之後，他再叫你去 APP 上 LINE、IG 去跟他做聯絡 (P2-1-5)

民眾他喜歡在網路上搜尋資訊，而且他沒有查證的能力…只要他對網路有一定的黏著度，然後加上詐欺集團，他能夠透過一些假廣告去投注，事實上它可以目標到這些人，這些人就很容易變成被害(P3-1-2-2)

詐欺集團製作的 App 或網站，介面精美、功能齊全，K 線圖、數據跳動一應俱全，看起來比真的券商 App 或網站還專業。(P4-1-2-2)

現在的網路社群發達，還有一些科技虛擬貨幣的發展得太眼花撩亂了，…他們對於辨別現在最新的一些科技發展，一些像什麼電子金融還是什麼，其實他們是沒有辨識能力的，才造成很容易就被詐團牽去，按照他的指示，把錢匯出去了(P5-1-4)

因為演算法的關係，他在 google 上面，有在做一些投資方面的檢索他只要有檢索過，這個紀錄就會被記憶，所以說不是剛好，是演算法帶你到這邊(P6-1-2-2)

就是網路使用長短也會有關係，因為你常常在網路上，他們就會有更多的機會去跟你接觸(P7-1-2-2)

我們日常生活中佈滿各種投資賺錢的一些資訊，那會讓民眾混淆判斷，哪一些是真的合法的投資管道，哪一些是假的，因為作的太像了，會讓民眾搞不清楚而陷入到這個圈套當中，而且造成被騙 (P8-1-2-2)

他的說法很貼近平台的一些政策，讓他真假不清…只要當他們沒有辦法去辨別這是真假的時候，他們就很容易出狀況(B1-1-2-2)

(五)遭詐時間跨度長，且常有重複被害情況發生

多數的受訪者均表示，詐欺集團掌握人性「貪心」與「不甘心」的心理弱點，利用各種資通訊科技工具，編造各種以假亂真的情境，以獲取不知情民眾的信任，當被害人心存僥倖或利令智昏，夢想一夕致富，相信詐欺話術深陷在詐欺情境時，他人縱使費盡九牛二虎之力勸說，亦難撼動被害人對犯罪集團的信任，也有些被害人雖懷疑自己被詐欺，卻因貪於虛假的高報酬率或礙於面子而不願承認，因為沒人想承認自己是傻瓜，直到被掏光所有錢財，始驚覺遭詐欺。

今年度就有 1 個高收入職業的醫生，重複被害面交了 13 次之後，第 13 次那 1 個車手被警方抓到了，重點是警察請他去做筆錄之後，隔天他又去匯款，200 多萬，到詐團指定的帳戶去，已經報案了，還是持續被騙，被害人認為詐團不會騙他。(P2-1-4-2)

他說我今天如果不相信他，我所投資的錢就沒了，所以他一次多次被害就這樣，所以接下來會有 1 個假律師、假警察，跟他講說我可以幫你把錢討回來，他還是想我的錢會回來，所以又被騙了。(P3-1-4-2)

他不願意相信這是騙啊！因為他只要不相信這是騙的話，那他就還是抱有那一點希望有 1 天還是可以拿回來，…他不願意相信那是那是詐欺，因為相信了其實就很多是這種不甘心的，還有

抱有最後一絲幻想(P5-1-4-2)

我說了二次詐欺是被騙完一次之後，演算法又帶他到另外 1 個介面，說我可以幫你找回損失的款項，這叫二次詐欺，啊你就會相信他，你就會繳了 10%的服務費給他，然後就發現你又被詐欺了(P6-1-4-2)

我今天遇到 1 個，他同時在很多個集團，很多個飆股群組裡面，這邊被騙完報完警之後，另外一邊以為是真的又再匯的也有(P7-1-4-2)

少部分的人會有重複被害的情形，因為這些被害者他們先前雖然曾經有被騙有遭受過損失，後續他另外又接到其他的話術，他們又陷入想要把之前被騙或損失的錢賺回來的想法，持續陷入在這個想法當中，但是他又沒有去查清楚，他這個投資管道是不是安全正當的，因而又再一次被騙（P8-1-4-2）

三、缺乏有監控能力者在場的情境

電信網路假投資詐欺犯罪集團往往組織嚴密，並擁有跨國運作的能力，犯罪者們利用各國法制差異與司法管轄主張不一，將犯罪行為拆解至多個國家，大幅增加警察調查、取證與跨國案件串聯的難度。日常活動理論強調，若犯罪者與合適目標之間缺乏有效監管者，犯罪發生的可能性將大幅增加。在此脈絡下，監管者的角色極為關鍵。而所謂監管者並不僅限於警察或司法機關，而是涵蓋了電信與網路服務提供者、金融科技與支付平台、法律規範與監理策略，甚至擴展至整體社會的防詐安全網。這些監管者若能發揮作用，便能降低被害人暴露於詐欺環境的機率。然而，當其中一環出現缺位或效能不足時，便會為詐欺行為提供機會。例如，私密社群與通訊軟體難以有效監控，使得詐欺集團得以經營「假投資群組」,營造獲利假象;金融機構與第三方支付平台若缺乏嚴格的身分驗證機制，則容易衍生人頭帳戶，成為犯罪金流的斷點；而跨國平台基於商業利益或文化差異，未能及時下架虛假廣告，更讓詐欺訊息持續氾濫。本研究依上述論點，訪談相關人員後，從電信網路與金融科技、法律規範與防制策略及 社會防詐安全網等面向，探討 缺乏有監控能力者在場的情境，是如促進電信網路假投資詐欺犯罪發生。

(一)電信網路與金融科技面

犯罪者利用法律漏洞或以蒐購方式取得大量的人頭門號，再據此申請社群媒體與搜尋引擎帳號，用以投放假投資廣告或建立虛構群組，雖然我國《詐防條例》已在「數位經濟防詐措施」中明文規範廣告平台相關管理責任，但在實務上效果有限，加上跨國平台業者常基於商業利益或文化差異，未能及時過濾與下架虛假廣告，造成假投資訊息氾濫，復以現行法規對於網路社群私密群組管控不足，導致犯罪者得以經營「假投資群組」，透過群體互動與情緒操弄營造獲利假象，使被害人誤信而遭詐，另一方面，詐欺集團利用金融交易數位化與多元支付工具，由同夥將資金迅速轉換為虛擬通貨，再透過多層錢包轉移及去中心化交易掩飾資金流向，最終由車手提領現金，製造金流斷點。本研究根據訪談資料分析也發現，電信門號及網路帳號管理未能落實，網路社群媒體假投資廣告管理不善，社群通訊軟體監管不足及 犯罪金流追蹤困難，是當前防制電信網路假投資犯罪遭遇之電信網路與金融科技層面問題。

1.電信門號及網路帳號管理未能落實

犯罪集團利用法律漏洞以換號的方式取得大量電信公司門號，或在黑暗網路及特定的網路社群大量蒐購人頭門號，再據以申請社群媒體或網路搜尋引擎帳號。受訪者 P1 即指出，犯罪集團利用我國電信法規的不完備，運用電信門號換號機制漏洞，以重複換號方式，取得大量電信公司門號，據以申請網路平台帳號。另外，受訪者 P8 則表示，大部分的犯罪集團會透過黑暗網路及特定的網路社群大量蒐購人頭門號，來作為犯罪工具。

這個門號在某 1 個認證過程中被否決了，那你可以去換號，或者是你已經申請到 1 個帳號，你要在這個平臺申請另外 1 個帳號，你可以再用這個門號再換另外 1 個門號去申請。(P1-1-2-3)

大部分還是跟人頭買，向這些缺錢的人買他們名下的電話，作為犯罪工具。(P8-2-1-3)

2.網路社群媒體假投資廣告管理不善

雖然，我國「詐防條例」第 32 條規定：網路廣告平臺業者於知悉其所刊播之廣告有詐欺情事時，應主動或於司法警察機關、數位經濟相關產業主管機關或各目的事業主管機關作成之通知期限內，移除、限制瀏覽或停止播送該廣告，或採取其他必要之處置。但跨國社群媒體或網路搜尋引擎業者基於商業利益考量，不願意採取積極防範作為，或因文化差異，而無法辨識過濾虛假廣告，又或犯罪集團利用民眾對網路平台所傳遞訊息的信任，而投放偽造的訊息，導致假投資廣告氾濫。如受訪者 P3 表示，網路社群媒體業者基於商業利益不願投入資源有效過濾「保證獲利」、「名人代言」等詐欺廣告，或因文化差異不了解臺灣的民情，而無法作廣告的過濾。受訪者 P4 表示，社群媒體業者常以只是提供網路平台，基於法律保障言論自由，不能限制用戶在平台上發送的訊息，作為卸責之詞。受訪者 B1 表示，犯罪集團利用民眾對網路平台所傳遞訊息的信任基礎，而投放偽造的訊息，使潛在被害人信以為真而受騙。

詐欺集團投注大量的錢在作廣告，如果社群媒體強力去掃蕩這些廣告，一定會濾掉一些正常的，可能會影響到他們的商務。另外，他不了解臺灣的民情，他無法作廣告的過濾。(P3-1-2-3)

我們只是平台，管不了用戶說什麼，是網路業者卸責之詞。(P4-1-2-3)

民眾信任這個平台，詐欺集團偽造 1 個可以博取他們信任的機制或網站。(B1-1-2-2)

3.社群通訊軟體監管不足

從我國法律規定及前述文獻分析中可以發現；雖然，我國針對網路廣告平臺管理，已於「詐防條例」；第二章「就源防詐機制」；第三節「數位經濟防詐措施」（第 27 條至 42 條）規範，其中第 30 條規定：網路廣告平臺業者刊登或推播廣告不得含有涉及詐欺之內容及建立相關管理措施；第 31 條規定：網路廣告平臺刊登或推播廣告之管理；第 32 條規定：涉詐網路廣告之移除、限制瀏覽、停止播送及涉詐帳號停權，並提送資料予司法警察機關；第 33 條規定：網路廣告平臺接獲通知，應限制接取、瀏覽或移除涉詐廣告內容等均有明文規定。但仍不能有效監控社交（交友）軟體（Instagram、Tinder、派愛族等）及手機通訊軟體（Line、WeChat、Telegram 等）網路社群私密群組，使得犯罪者可在其中創建「假投資群組」，據以營造虛假獲利氛圍，使潛在被害人誤信而遭詐。受訪者 P4 及 P5 就直言，臉書、Google、LINE 等大型跨國平台，是傳播假投資詐欺廣告和訊息的主要載體，但當警察機關要求渠等下架詐欺內容或提供使用者資料時，這些跨國公司常以「言論自由」、「保護用戶隱私」、「總部在海外」等理由塘塞，拒絕提供協助，或以繁瑣程序消極作為，拖延時間，待警察機關收到業者回復，大多已經緩不濟急。受訪者 P6 也表示，我國「詐防條例」已有相關監管規定，業者應主動下架詐欺相關訊息，且警察機關亦認為在技術端是可行的，但業者並未積極配合，大多是警察機關講一動作一動，並無主動積極作為。

但當我們要求下架詐欺內容或提供使用者資料時，他們常以「言論自由」、「保護用戶隱私」、「總部在海外」等理由，程序繁瑣、反應緩慢。(P4-1-2-3)

Line 上面的詐欺也很多，他也不管，他也是說言論自由，你那個私密聯繫(P5-1-2-3)

詐欺犯罪防治危害條例裡面都有寫到，只是業者沒有配合。(P6-1-2-1)

4.犯罪金流追蹤困難

從前述文獻分析可知；詐欺犯罪集團利用金融交易數位化帶來的快速、便利與多元支

付工具，加上網路銀行遠端身分驗證不嚴謹，以及國際間防制洗錢合作尚未完善的漏洞，透過人頭電話與人頭帳戶設下斷點，規避偵查，也有許多民眾在有償或無償情況下將帳戶交給他人使用，卻未意識到可能因此成為詐欺幫助犯，詐欺集團亦常以「協助辦理貸款」等話術誘使民眾提供帳戶，再將這些帳戶作為詐欺工具。據內政部警政署刑事警察局分析顯示，2021 至 2022 年間被標示為警示帳戶的公司行號中，約有四成屬於第三方支付或電商業者，可見詐欺集團偏好利用審核相對寬鬆的第三方支付虛擬帳號來收取贓款，其後，犯嫌再將資金轉換為比特幣、泰達幣等高價值虛擬通貨，轉入電子錢包以隱匿資金流向。由於缺乏相對應的中央主管機關，警方在調閱資料時困難重重，偵辦更加不易；另一方面，虛擬通貨已成為詐欺集團重要的洗錢工具，他們利用虛擬通貨具高度流通性且可隨時兌現的特性，要求被害人透過交易所、比特幣提款機(BTM)或個人幣商購買虛擬通貨，再轉入犯嫌指定的人頭電子錢包，經過多層移轉與去中心化操作隱匿資金流向，最後再透過網路完成洗錢，並由車手集團提領現金，藉以隱匿贓款流向並製造金流斷點，造成後續調查取證、贓款沒收、返還、凍結之困境。綜合多數的受訪者的意見，詐欺集團會交叉運用多種手法誘導被害人交付款項，導致洗錢通路高度多元且無法單一化，許多被害人會依指示匯款或提供人頭帳戶，犯罪分子再利用人頭帳戶層層轉帳，並由車手提領現金後購買虛擬貨幣，再轉入國內外交易所或境外電子錢包。由於警察人員對虛擬貨幣移轉流程並非人人熟悉，且部分交易不受即時監管，犯罪集團可採一對一或透過國內外交易所多重轉換獲利，最終資金常被匯往如泰國、緬甸等境外帳戶，或透過地下匯兌出境。因為不同交易所與錢包之間多次轉移造成資金斷點，增加警方凍結與追查的困難，雖然，被害人交付款項大致可歸納為五至六種模式，但仍多以虛擬貨幣作為跨境出款的主要工具。

詐欺集團誘導被害人，不同的手法他會交叉被使用，它能匯款安全的匯款，就會匯款。(P1-2-2-6)

洗錢的管道多元化…目前沒有辦法單一化。(P2-2-3-1)

虛擬貨幣的轉錢流程，執法單位不是每個人都懂，而且也不需要經過監管，他可以一對一，也可以透過國內或國外交易所賺錢。(P3-2-3-1)

利用人頭帳戶層層轉帳，再由車手提款後購買虛擬貨幣，轉到國外境外交易所的錢包。(P4-2-3)

虛擬貨幣轉到國外去，不用外匯管制，也不用什麼地下匯兌又快。(P5-2-3-1)。

被害人交付被騙的款項大概有五、六種模式。(P6-2-2-6)

最後虛擬貨幣流到的是泰國、緬甸那邊的帳戶。(P7-2-3-1)(P7-2-2-7)。

地下匯兌轉到國外去，詐欺集團的帳戶也騙來的或買來的，轉到最後，還是靠虛擬貨幣匯出去。(P9-2-2-1)

在不同的虛擬資產交易所開立不同的錢包，轉來轉去，產生資金斷點，導致警察無法掌握他的 1 個金流的方向來凍結追查。(G1-2-2-1)

(二)法律規範與防制策略面

隨著詐欺集團不斷演化，現在詐欺機房多設置於境外地區，由於涉及不同主權與法律體系，執法機關往往面臨管轄權不足的困境，造成實際查緝成效有限，使詐欺集團得以持續擴張，並在短時間內轉移犯罪據點或洗白資金，增加追緝難度。此外，隨著新興投資型態快速興起，各種虛擬通貨發展迅速且種類繁多，使得傳統金融監管法律規範難以及時因應，讓詐欺者得以利用監管灰色地帶設計複雜的投資陷阱，吸引民眾投入資金。儘管政府部門與金融監理機構持續透過各種方式、管道，向社會大眾發布防詐資訊，然而並未能形成整合性的防詐知識庫，也未能時即時觸達潛在目標，導致民眾雖具備部分防詐意識，卻仍無法在關鍵決策瞬間獲得警示，形成防詐宣導與實際需求間的落差。本研究分析訪談資料後也發現，跨國（境）查緝困難、法律規範不足、防詐資訊未能觸達潛在受害者，是警察防制電信網路假投資犯罪所遭遇之法律規範與防制策略面問題。

1.跨國（境）查緝困難

電信網路假投資詐欺集團仿照大型跨國企業採層級管理，分工細緻，利用資(通)訊科技設備及方法，將犯罪組織結構，分散在多個國家地區，並將犯罪集團最重要的機房及洗錢中心設於東南亞地區國家，在當地國刻意保護包庇下，使得警方查緝溯源中遭遇層層斷點，鮮少查獲幕後首腦偵破整團犯罪組織。受訪者 P1 指出，最近幾年有不少的臺灣民眾被騙或自願前往東南亞地區國家，參與跨國（境）詐欺犯罪行為，因為人數眾多，警察機關還曾動用員警在機場勸阻。

前幾年臺灣的民眾一直被帶到或騙到或自願到柬埔寨、緬北等等之類的地區。(P1-2-1)

其中，擔任刑事警察局第一線外勤主管的受訪者 P2、P2、P5 更異口同聲，明確表示，電信網路假投資詐欺犯罪的機房，十之八九都是隱身在柬埔寨。

肯定詐欺集團的機房都是在東南亞柬埔寨…我們受理的 10 件裡面有 9 件（P2-1-2-3）
我們了解都在柬埔寨，都是跨國的(P3-2-2-7)
主要像機房成員就是躲在國外啊，像柬埔寨就是。(P5-2-3-2)。

在刑事警察局擔任防制詐欺犯罪策略規劃及執行的受訪者 P4 則提到，犯罪集團利用資(通)訊科技，實現犯罪組織跨國（境）化境，犯罪者匿名化，詐欺集團將伺服器設在與我國沒有司法互助的國家，金流則透過加密貨幣（如 USDT）跨國（境）層層轉換，通訊也是採用國外加密軟體，造成警察查緝困難重重。

詐欺集團的伺服器設在根本沒有司法互助的國家，金流透過加密貨幣（如 USDT）洗到天涯海角，通訊用的是國外的加密軟體。(P4-1-2-3)

2.法律規範不足

隨著電信網際網路科技迅速發展，及新興金融投資工具百花齊放，假投資詐欺集團在躲避警方查緝的犯罪理性選擇下，利用電信金融法規及資安防護缺乏明確監管，嚴謹度亦未臻完善之灰色地帶，在遠端藉由加密通訊、寬頻網路、新型態電信服務等國際話務服務，輔以非法取得之人頭金融帳戶，再透過社交（交友）軟體、手機通訊軟體等遠程非接觸式工具，藉由快速獲利及穩賺不賠的虛偽投資廣告與民眾接觸，誘騙被害人交付財物，造成執法人員查緝困境。綜合受訪者 P2、P4、P5 的看法，咸認為公務人員的核心價值在依法行政，但執行防制電信網路假投資詐欺犯罪的警察人員，卻常需要在沒有充分的法律授權情境下，超前部署提前為民眾建構起詐欺犯罪防護網，而對人民或私人企業採取相關行政處分措施，例如：查找潛在被害人，要求網路社群媒體與搜尋引擎業者下架假投資廣告。另外在法律執行層面上，雖然我國《詐防條例》已明文規範廣告平台相關業者的管理責任，但這些發生犯罪「場域」的管理者，卻沒有負起相應的管理責任，更何況法律更新速度，永遠跟不上犯罪手法的演變。

依法行政，是行政機關的核心，但是查找潛在被害人，法律授權在哪裡？（P2-3）
法律的更新速度，永遠跟不上犯罪手法的演變，他們是犯罪發生的「場域」，卻沒有負起相應的管理責任。(P4-1-2-3)
我們是到這一兩年才有詐防條例可以下架假投資廣告，不然之前我們要求下架，業者說你箝制言論自由。(P5-1-2-3)

另外，受訪者 P3 則表示，為使投資管道透明化，我國可參考韓國立法例，明文禁止在網際網路從事投資相關事業，讓金融監管部門可依法取締，也讓百姓知道不能在網路上隨便聽信假投資廣告。

在韓國沒有這種網路投資，所以這個我們要宣導啦，金管會要抓啦。(P3-2-4)。

3.防詐資訊未能觸達潛在受害者

犯罪集團善於利用人性弱點，不斷翻新詐欺手法，結合話術與科技營造逼真情境，使民眾難以辨識、輕易陷入圈套。雖然，警政與金融監理機構持續發布防詐資訊，但多屬被動、分散，無法即時傳達至潛在受害者，更因長期大量的宣導與媒體報導，反而使部分民眾產生麻木或過度自信，對警示訊息漠視，甚至缺乏提醒親友的警覺，進一步提高受騙風險，另有部分民眾因僥倖心理或貪圖暴利，誤信「快速致富」的誘因，最終深陷詐欺情境仍渾然不覺，導致案件數與財損金額持續攀升。綜合多位受訪者的意見，政府防範假投資詐欺犯罪措施及犯罪宣導的深度及廣度，跟不上犯罪集團掌握人性弱點，快速翻新犯罪手法的腳步，導致潛在受害者無法及時接收到最新的防詐資訊，加上政府長期大量的宣導與媒體報導，致使社會大眾出現宣導疲乏情況，而易成詐欺集團鎖定之犯罪標的。

民眾接觸訊息的層面，比警察防治面廣，民眾當下是否認為有利可圖，警方無法預測。(P2-4)。

現在的被害人樣貌非常多元，騙子攻擊的是人性的共通弱點。(P4-1-2-2)

坦白講現在有點宣導疲乏了，我們宣導有沒有到位，還是說有沒有符合那個情境？(P5-4-1)

FB 有管啊！我們曾經給他檢舉過啊，可是詐欺集團的動作太快了，太多了啊。(P9-1-2-3)

(三)社會防詐安全網

電信網路假投資詐欺兼具「情感詐欺」與「財務詐欺」特徵。犯罪集團透過長期互動培養情感依附，在被害人缺乏社會支持與外部監管下，逐步以心理操控與資訊控制，使其在認知偏誤與情感承諾驅動下交付金錢。雖然我國已於金融、電信與網路領域設立相關防制規範，但主管機關作為偏向被動，欠缺跨部門協調與前端預防，防制工作多仰賴警察機關的事後偵辦。然而，警方並非目的事業主管機關，無法有效驅動金融與電信業者積極配合，導致民間參與度不足，整體成效有限。此外，我國基礎理財教育與投資風險意識培養不足，社會大眾對金融市場與虛擬資產認知有限，易受詐欺訊息誤導。特別是高齡族群與低投資知識者，由於缺乏防詐教育與數位金融素養，無法辨識異常投資訊號，遂成為詐欺組織高度鎖定之高風險對象。本研究將依訪談結果從被害人的家庭與社交支持薄弱、公私部門積極度不足、防詐教育未能普及等面向，分析社會防詐安全網效果不張的情形。

1.被害人的家庭與社交支持薄弱

電信網路假投資詐欺結合了「情感詐欺」與「財務詐欺」的雙重特徵。當犯罪者透過長期互動建立情感依附，而被害人又因缺乏社會支持而無法獲得外部監管時，詐欺集團得以透過逐步的心理操控與資訊控制，使被害人最終在認知偏誤與情感承諾的驅動下，將金錢交付予犯罪者。就如同受訪者 P1 所言，犯罪集團與被害人培養了二、三個月的感情，我們警察只跟他講不到十分鐘，就要勸說被害人，這是不可能的，所以警察要學習詐欺集團的黏著性，多花時間勸說潛在被害人。受訪者 P3 也說，一些年長者因長期獨居個性較為孤僻，誰都不相信，當詐欺集團天天打電話或傳訊息來問候，加上找不到其他人可以諮詢，最後就選擇相信對方把錢交出去了，導致一發不可收拾。受訪者 P4 則表示，很多年長被害人的孩子在外地工作，很少回家，而老人家獨居在家，就算被騙，也因為擔心遭子女責罵，而不敢說實話，年輕的被害人則是認為投資理財是個人的隱私，不願與親朋好友分享討論並諮詢意見，因而失去他人給予提醒建議的機會。受訪者 P7 認為，由於被害人缺乏防詐警覺及欠缺真實社交的社會支持，很容易就受騙了。受訪者 P8 則認為，當前民眾普遍使用手機，作為社交及溝通工具，造成潛在被害人很容易在虛擬空間接觸到假投資資訊並加入私密網路社群平台，讓家人及朋友很難在第一時間就察覺被害人可能遭詐欺，而加以阻止。

詐欺集團的黏著性是我們應該要學習的，因為我們花的時間太少了。(P1-4-4)

他第一時間找不到人談，他就直接相信對方給錢出去了，所以導致後頭一發不可收拾。(P3-1-4-2)

怕被子女責罵「貪心、笨」，而不敢說，年輕人也一樣，很多人認為投資理財是自己的事，不願與家人朋友討論，失去了被提醒的機會。(P4-1-2-3)

你缺乏警覺，缺乏社交，缺乏實際上的社交，很容易就受騙了。(P7-2-4)

現在人手有一支手機，要去接觸這些假投資平台跟資訊是很容易的，讓家人朋友很難在第一時間就察覺而去阻止他。(P8-1-2-3)

2.公私部門積極度不足

雖然我國在金融、電信與網路領域已建立相關防制假投資詐欺的規範，但由於主管機關態度偏向被動，欠缺跨部門協調與主動預防措施，使得防制工作多仰賴警察機關的事後偵辦。然而，警方並非目的事業主管機關，無法有效驅動金融與電信業者的積極配合，導致民間配合度不足，整體防詐成效有限。例如受訪者 P3 即指出，依據 165 統計，目前詐欺犯罪案件有將近九成都是在網際網路發生。因此，網際網路管理是當前很重要的問題，包含 Social Media、社群媒體、通訊軟體、虛擬金流、第三方支付、遊戲點數，這些都需要主管機關落實實名制的有效安全管理。受訪者 P4 更進一步表示，政府強調要從源頭著手有效管理，但是詐欺廣告和訊息的主要載體臉書、Google、LINE 等大型跨國平台的管理，需要主管機關 NCC 及數發部的全力支持，採取迅速有效的管理措施。受訪者 P5 也認為，金融、電信、網路的事業目的主管機關大都採取被動保守作為，雖然警察已在法律授權範圍內採取主動積極作為，但畢竟是干涉取締的角色，無法有效要求業者積極配合。受訪者 G1 則表示，目前國內大型金融機構，如中國信託商業銀行、國泰世華商業銀行、臺北富邦銀行等都會投入大筆資金，進行 AI 技術研發，希望藉由先進的監控技術及大數據分析，辨識異常交易，但中小型銀行在這方面的技術，還有財力上明顯有不足，所以整個金融體系會呈現很大的落差，無法有效形成的防詐聯防。

網路治理是 1 個很重要的問題，我們現在看到 165 的詐欺，將近九成都是網路。(P3-2-5)

政府一直強調要從源頭著手，但是需要主管機關 NCC 及數發部的全力支持，他們動作要加快才有辦法。(P4-4-2)

我覺得大家都趨於被動保守，警察很主動，但是我們畢竟還是 1 個干涉取締的角色，我們不是目的事業主管機關(P5-4)

銀行的監控無法有效形成 1 個聯防，因為他們彼此之間的 1 個技術發展不均。(G1-4-4)

3.防詐教育未能普及

我國在基礎理財教育與投資風險意識的培養上仍存在顯著缺口，潛在被害人對金融市場與虛擬貨幣的理解不足，導致其容易受到詐欺集團的虛假訊息影響並深信不疑，特別是高齡族群與低投資知識者，由於缺乏足夠的防詐教育與數位金融素養，無法辨識異常投資訊息，遂成為犯罪集團高度鎖定的對象。綜合多位受訪者的意見，發現多數被害人對投資環境運作不熟悉，因而對詐欺集團所傳遞的資訊深信不疑，甚至誤以為對方不會欺騙自己，我國基礎教育中缺乏理財課程，使大眾欠缺金融風險意識，若具備基本理財概念，即能辨識「超高獲利無風險」投資商品的不合理性。此外，隨著科技與虛擬貨幣快速發展，金融工具日益複雜，使高齡族群難以跟上新興投資趨勢，成為詐欺集團高度鎖定的脆弱族群。

對投資環境運作不是很熟悉。(P1-1-2-2)。

被害人深信不疑，認為詐團不會騙人。(P2-1-4-2)。

我國的基礎教育缺乏理財的教育，若大家都有理財的概念，就會知道沒有這種超高獲利的投

資商品了。(P4-2-4)

科技虛擬貨幣的發展得太眼花撩亂了，讓那些上年紀的人沒有辦法跟上。(P5-1-4)

四、犯罪者參與犯罪的影響因素

本研究以理性選擇觀點為理論基礎，將參與電信網路假投資詐欺的犯罪者劃分為「引發」、「習慣化」與「終止」三個階段，並比較各階段中影響其參與行為的關鍵變項。訪談與分析結果顯示：首次投入此類犯罪的決定，常受到以往犯罪經驗、個人性格與成長背景、當前生活型態與需求、以及可被利用的犯罪機會與誘因所影響；而是否持續犯罪或選擇終止，則取決於犯罪成功的可能性以及犯罪對個人生活方式所造成的正負影響。現實生活中的外在因素（如健康、婚姻、家庭重大變故等）與犯罪本身的節奏，也會促使犯罪參與發生變化，促成從引發到終止的轉換。此外，犯罪者往往同時涉足多種類型的犯罪，其在一類犯罪中累積的技術與經驗，可能促使其跨時、跨域（包括不同國家或不同目標）重複實施相同或變形的詐欺行為。當犯罪行為取得成功經驗後，個體更可能由外圍角色（如領款車手、電話手）升遷為第二線、第三線或機房管理等核心角色，或採用其他型態的犯罪手法繼續作案。

(一)犯罪者初次參與犯罪的影響因素

依文獻探訪分析可以發現，影響犯罪者初次參與電信網路假投資詐欺犯罪的主要原因，包括個體的背景因素、經驗與學習、當前生活狀況、需求與動機、機會與誘因及對犯罪情境因素的評估。潛在犯罪者在經過上述一系列理性評估後，如認為參與電信網路假投資詐欺犯罪比不參與有利，即可能著手作犯罪。以下謹依受訪者的意見分析如次。

1.背景因素

依文獻顯示，背景因素對引發潛在犯罪者是否選擇犯罪的影響最大，因為它同時決定了個體累積的知識、能力和經驗，以及目前的生活環境，本研究從犯罪者的理性選擇角度出發，發現電信網路假投資詐欺犯罪者有多為男性且年齡多介於 15 至 40 歲之間，教育程度則大都集中於國（高）中或輟學，且多無正當職業，其謀生能力較低下，但仍有少部分具有專業能力，參與黑道幫派犯罪組織情況明顯，大都有好逸惡勞且貪圖物質享受情形，犯罪的目的都在獲取金錢利益等等特徵（如前述「犯罪者日常生活形態的描繪」），與前揭文獻揭示，犯罪者的生活背景、社會價值觀、生活態度和人格心理特質發展等背景因素，將對實施電信網路假投資詐欺犯罪決策時，產生具有關鍵性影響的判斷與認知有相當解釋力。此外，受訪者 P3 及 P5 表示，電信網路假投資詐欺犯罪者的家庭功能多欠缺正常，可能是社會弱勢群體，經濟收入較低，甚至背負債務，或家庭成員有家庭暴力、使用毒品、犯罪遭通緝等情形，而無法提供犯罪者所需的物質、生理、心理及環境支持，導致其決意選擇參與電信網路假投資詐欺犯罪以解決目前的生活困境。

家庭的狀況都不太好，低收入戶、吸毒、或者是家暴，或者是社會邊緣人、在臺灣欠債、或者是通緝等等。(P3-1-1-3)。

他家庭本來就很破碎的話，基本上他還是需要作詐欺去讓他維生。(P5-1-1-3)

因為這些人，第一家庭也沒有溫暖，所以他根本就不會回家，也不會去學校，他沒有沒有地方可以取得他的認同感，幫派就是利用這些把它吸收進來，他在裡面就會有認同感，所以就跟著他們一起做這些事情。(P9-1-3-2)

2.經驗與學習

受訪者 P3、P5、P6 均提及，吸引初次犯罪者實施電信網路假投資詐欺犯罪的原因，包括犯罪技術門檻低，工作輕鬆時間短暫且單純，例如：利用人頭銀行帳戶，或藉由資通

訊工具隱匿身分，使用金融科技在網路上開戶並操作網銀轉帳快速轉移贓款，或購買虛擬通貨，以製造金流斷點，遭執法機關緝獲的風險不高。

這些犯罪者認為這種詐欺手法能夠吸引他的原因之一，它的門檻那麼的低，而且風險也不高。(P3-1-1-1)

現在大家都用網路，我網路上操作就好了，然後你獲利高，然後入門門檻很低啊。(P5-1-1-1)

我覺得我1天只要可能工作個四五個小時，然後把錢轉到另外1個帳戶或把錢轉到虛擬貨幣，他們覺得這樣的工作很單純，而且可能被抓的風險也很低。(P6-1-1-1)

另外，受訪者 P7 則指出，參與實施電信網路假投資詐欺犯罪的犯罪人，大都有犯罪前科素行，本身已具有一定程度的犯罪經驗，相對於一般人民有更多管道可接觸到犯罪訊息。

這些人大概都是有前科的啦，要嘛毒品前科，要嘛詐欺前科這些的，他們本來就認識一些比較接近犯罪的人。(P7-1-1-1)

3.當前生活狀況

多數受訪者均表示，同儕或朋友是影響初次參與實施電信網路假投資詐欺犯罪者參與犯罪的重要因素之一，特別是青少年的同儕團體與偏差行為有關時，更會直接影響使其更傾向於參與犯罪活動。受訪者 P1 就認為，同儕是影響青少年初次參與犯罪的重要因素，可能使得原無犯罪動機的青少年，因受到同儕蠱惑而參與實施電信網路假投資詐欺犯罪。受訪者 P5 也表示，初次參與犯罪者的朋友在詐欺犯罪集團所扮演的角色，會影響其參與詐欺犯罪的角色，如朋友在詐欺犯罪集團擔任提款車手，渠就極可能成為提款車手，如朋友在詐欺犯罪集團擔任洗錢工作，渠就極可能會參與洗錢水房工作。另外，黑道幫派滲透校園利誘青少年加入詐欺集團擔任提款車手，是影響初次參與犯罪者，參與犯罪的主要管道。受訪者 P7 就提及，黑道幫派滲透校園情況嚴重，導致青少年在學校就可能很容易接觸到由黑道幫派分子組織的詐欺犯罪集團，導致被引誘加入犯罪集團擔任提款車手。

青少年同儕之間的影響都很重要…一旦誤入歧途之後，那就會大家牽著走，所以同儕之間的影響，我覺得是非常的可能。(P1-1-1-1)

如果是電詐的話，朋友拉朋友，在整個集團裡面看的到的，非常的嚴重，吃好逗相報，走頭無路的，還是我來跟你靠看看的。(P2-1-1-1)

我們抓到的很多年輕底層成員，都是被朋友、同學、或是地方上的「哥哥」給拉進來的。(P4-1-1-1)

車手間的招攬都是互相介紹阿，如果說他朋友，今天有人作車手，他覺得好作，他就會做車手，但有些朋友是作洗錢他就會作洗錢。(P5-1-1-1)

學校可能就是會有一些小朋友去接觸，應該說接觸到一些幫派份子…他們可能會引誘學生作詐欺車手…所以滲透校園的情況其實蠻嚴重的。(P7-1-1-1)

4.需求與動機

依據理性選擇觀點相關文獻顯示，犯罪的需求指涉犯罪者試圖滿足的特定心理或物質需求，犯罪動機則是促使犯罪者實施犯罪行為的心理原因，也是犯罪者做出決定並採取行動的主要因素，而且犯罪需求和動機常常交織在一起，犯罪者為滿足需求，而產生犯罪動機，這些動機驅使犯罪者評估不同的犯罪選項，並根據自身的需求和價值觀來做出最符合其利益的選擇，以滿足自己的需求。因此，多數受訪者均表示，電信網路假投資詐欺的犯罪者基於金錢的迫切需求，在希望快速致富的需求下，經理性評估後選擇可輕鬆、快速、安全獲得鉅額金錢電信網路假投資詐欺犯罪，以作為滿足自身對金錢需求的方法。

影響他應該是現在整個社會的氛圍，還是以金錢至上的概念，所以笑貧不笑娼。(P2-1-1-1)

賺快錢是最主要的驅動力，這絕對是最強的誘因，沒有之一。(P4-1-1-1)

最主要是因為其實坦白講現在臺灣的經濟環境，一般年輕人認真工作其實錢賺的應該比不上做電信詐欺的這個酬勞啦。(P5-1-1-1)

今天這個甲車手看到同學怎麼換了一支手機，他就非常的心動，然後問他說你怎麼會有錢辦手機，他可能就會講說，我只是幫人家去領了1條錢，那人家就給我一兩萬塊。(P6-1-1-1)

大多都是因為經濟狀況不佳缺錢，或者是年輕人想要做輕鬆、快速賺錢的工作，而因而來參與犯罪的。(P8-1-1-1)

5.機會與誘因

多數受訪者都表示，初次參與詐欺犯罪者的動機都是為了金錢利益，潛在犯罪者依據本身累積的經驗和知識理性評估後，如果認為參與電信網路假投資詐欺犯罪計畫成功的機會及獲利都很高，而且投入成本相對低廉就會參與犯罪。如受訪者 P1、P3、P4、P6 即表示，假投資詐欺是所有詐欺犯罪手法中不法獲利最高，且具犯罪門檻低，犯罪模式複製容易，遭警察機關查獲風險低等有利於犯罪的機會，導致諸多犯罪集團在嚐到龐大犯罪利益後均趨之若鶩，紛紛基於快速獲取大量財貨的誘因而投入是類犯罪。

假投資的詐欺是獲利最高的，所以可能大部分的集團，他們到後來都會轉向作假投資詐欺…，可以複製加上獲利高，所以很多的詐團都會來作。(P1-1-1-1)

它的門檻那麼的低，而且風險也不高。(P3-1-1-1)

他們會跟新人說，這只是金融糾紛，不是什麼大罪，你沒前科，就算被抓到也是初犯，法官看你年輕，最多判個緩刑，不會有事的啦。(P4-1-1-1)。

都是為了利益，都是為了錢，他們自己都有評估過，可能做這樣的事情，被抓的機會是比較低，都有僥倖心態在。(P6-1-1-1)

6.對犯罪情境因素的評估

初次參與假投資詐欺犯罪者，會被當前自身所處的社會、經濟等外在環境，及對道德、良知等內在感知的情境因素影響，在經過有限理性評估參與犯罪的利弊後，如發現參與犯罪獲得的利益超過不參與犯罪則會加入犯罪行列。誠如受訪者 P3 所言，假投資詐欺犯罪者僅需付出極小的成本，即可獲得鉅額的不法利益，就算被警察機關查獲，法官所判刑期通常都很輕微，對犯罪者而言是很划算的。又如受訪者 P4 表示，電信網路假投資詐欺是一種非接觸性的犯罪，犯罪者無法感受到被害人遭詐之後傾家蕩產及家破人亡的慘況，只會覺得自己並不是在犯罪而是在工作，並無感受到任何的良心道德譴責。再如受訪者 P5 表示，以臺灣當前的社會經濟環境，一般腳踏實地認真工作的年輕人，其收入遠比不上參與電信網路假投資詐欺犯罪所獲的酬勞。

以假投資來講…成本很低就可以騙到將近好幾百萬的錢，其實是很划算啊，我後頭被抓到，頂多判6個月以下徒刑。(P3-1-1-1)

這是非接觸性的，提供帳戶的「簿子戶」或取錢的「車手」，他看不到被害人一生積蓄被騙光的樣子，也聽不到被害人絕望的哭喊。(P4-1-1-1)

一般年輕人認真工作錢賺的應該比不上作假投資詐欺的酬勞啦。(P5-1-1-1)

(二)犯罪者習慣參與犯罪的影響因素

文獻指出，在電信網路假投資詐欺犯罪的「習慣化階段」，犯罪者的行為動機逐漸脫離原有的背景因素影響，而更多受到犯罪過程中所得不法利益與生活環境變化的驅動。隨著犯罪經驗的累積，犯罪者可能因結識同樣從事詐欺的同夥、掌握更精細的犯罪技能，並內化與犯罪相容的價值觀與生活方式，而強化其持續參與犯罪的傾向。是否繼續或停止犯

罪的決定，亦受到犯罪成功率與其對生活穩定性的雙重影響。現實中，外部事件如健康惡化、婚姻或家庭變故等，可能成為犯罪節奏變化的契機，促使其犯罪行為轉向或終止。此外，部分犯罪者具有多重犯罪參與的特性，在不同犯罪型態間轉換與學習，使各類犯罪經驗相互影響。由此可見，電信網路假投資詐欺犯罪者的習慣化歷程，實為一動態且多層次的過程，受個人收益、社會關係與生活變遷等多重因素交互作用所塑造。根據訪談分析可以發現，影響犯罪者習慣參與電信網路假投資詐欺犯罪的主要原因，包括個體的社交生活圈的改變、犯罪專業性的增加、生活方式及價值觀產生變化等以下謹依受訪者的意見分析如次。

1.社交生活圈的改變

電信網路假投資詐欺犯罪者隨著犯罪次數增加，逐漸溶入犯罪次文化，同時會認識結交更多犯罪人，也會被社會貼上犯罪標籤，並與擁有正當職業及正常生活的朋友疏遠，也可能被家人發現參與犯罪而發生爭執衝突。如受訪者 P2 表示，因為從事電詐犯罪的報酬高、處罰輕，且犯罪者在被警察查獲後，所屬犯罪集團都會聘請律師協助打官司，因此犯罪者對於犯罪集團的忠誠度通常都很高，所以在官司告一段落或服刑結束後，大都會再回籠持續犯罪。受訪者 P4 則指稱，有詐欺前科者一旦被社會貼上犯罪標籤，將不見容於一般企業，就業難度會顯著提高，但犯罪集團卻因渠等的犯罪資歷而張開雙臂歡迎。受訪者 P9 認為，操控詐欺犯罪的黑道幫派，為增加認同歸屬感及方便控制幫眾，都會要求幫眾將該幫派特有的圖騰刺在身體，使得被吸收進入幫派的青少年很難回頭，只能繼續犯罪。

他們對於這個犯罪集團的忠誠度是高的，就是你雖然被抓了，但是我會幫你處理一些事情，所以你告一段落，你還是會再回籠。(P2-1-1-2)

社會把他推開，但犯罪圈子卻張開雙臂歡迎，他過去的「前科」反而成了圈子裡的「資歷」。(P4-1-1-2)

他一定會被叫去刺青，刺下去之後，就很難回頭。(P9-1-1-2)

2.犯罪專業性的增加

電信網路假投資詐欺犯罪者在成功遂行多次犯罪後，因自身習得擁有的犯罪技能和知識，可有效降低被警察機關查獲的風險而感到自豪，同時對本身的犯罪能力也愈來愈有自信，會更勇於透過有計畫的篩選犯罪目標，以獲得豐厚的犯罪收益，並培養提升規避執法機關查緝及和法院對抗的能力。受訪者 P1 認為，假投資詐欺犯罪者在被警察機關查獲過後，如再度參與犯罪，其犯罪手法就會更為精明，犯罪過程也會更為謹慎小心，規避查緝的能力也會隨著犯罪次數增多而增強。受訪者 P3 指稱，多次犯罪者會覺得假投資詐欺犯罪被查獲的風險沒有比他想像的來得高，甚至認為此類犯罪是安全且可穩定獲利的事業，而促使犯罪者更積極參與犯罪。受訪者 P5 表示，很多假投資詐欺犯罪者最初僅是販賣人頭帳戶，但會隨著犯罪經驗的累積，進而成為取款車手，甚至再進階為車手頭，在犯罪集團中所扮演角色也會日漸重要。

他會更謹慎、會更難抓，這就是一種學習理論，所以他越來越精了。(P1-1-1-2)

累犯覺得整個犯罪的風險沒有想像的來得高，所以他認為這是像 1 個犯罪事業，而且是 1 個非常安全的事業，他就會更想要去騙更多人。(P3-1-1-2)

很多人第 1 條詐欺前科先賣本子，後來第二次抓到他變成車手，第三次抓到他變車手頭，他都會一直升級上去。(P5-1-1-2)

3.生活方式及價值觀產生變化

犯罪者逐漸意識到，參與電信網路假投資詐欺犯罪收益是重要經濟來源，只要選擇不斷的犯罪，即可在付出很少勞力的情況下，不斷取得豐厚的金錢來源，使其快速改善經濟

能力，享受當下揮霍的生活。因此，犯罪者在追求最大利益的理性選擇下，會從一開始因為沒有其他謀生能力，迫於生活需要而參與犯罪，慢慢變得貪得無厭，認為合法工作價值低，不足以維持現在優渥的物質享受，而合理化現在的犯罪行為。例如受訪者 P2 認為犯罪者在發現從事假投資詐欺所獲得的優渥報酬，比每天辛勞工作所獲得的報酬有明顯的差異時，就會理性選擇現在的犯罪生活節奏而一再的犯罪。受訪者 P3 及 P5 則進一步說明，假投資詐欺犯罪人，除資通訊犯罪外並沒有其他的謀生能力，所以此類犯罪的累犯有越來越嚴重的趨勢。受訪者 P4 及 P5 則提及，在遂行假投資詐欺犯罪後，所獲得的鉅額金錢，為犯罪者揮霍生活所需提供有力的支持，此時犯罪者再也不會想回到往日低薪的日子。

他的心理上，就是比每天作苦工還要好，這已經不一樣了，他已經習慣那個節奏了。(P2-1-1-2)

他們也沒有其他的謀生能力，他們比較擅長做這種資通訊的犯罪。(P3-1-1-2)

一旦體驗過那種揮霍的生活，要他再回去領一個月三萬塊的薪水，他會覺得那根本不是人過的日子，從一開始的「需要」，慢慢就變成了純粹的「貪婪」。(P4-1-1-2)

基本上他在社會上就沒有正常的方式可以賺到錢，所以他就算被抓，他為了活下去，他一定會持續作詐欺的(P5-1-1-2)

賺過詐欺的錢之後，很難再去作其他苦力的工作，他會覺得這個 CP 值太低了。(P6-1-1-2)

(三)犯罪者停止犯罪的影響因素

文獻指出，在電信網路假投資詐欺犯罪的終止階段，背景因素已不再影響犯罪者的決策，取而代之的是風險與報酬的理性權衡。隨著政府強化防詐政策、警方查緝能量提升及民眾防詐意識普遍提高，犯罪者對被查獲風險的感知大幅增加，犯罪報酬與投入成本之間的落差逐漸擴大，導致其在理性計算後認為停止犯罪較為有利。此外，個人生活環境的轉變亦為重要影響因素，如婚姻關係建立、家庭責任增加、身體健康惡化、或獲得合法工作機會等，都可能促使犯罪者重新評估其生活重心與風險承擔意願。部分犯罪者在遭受偵查、羈押或刑罰後，因社會標籤化與再犯成本上升，也可能選擇脫離詐欺活動。整體而言，電信網路假投資詐欺犯罪的終止過程呈現出理性選擇與社會結構變遷交互作用的結果，顯示犯罪停止並非單一事件，而是一種受制度壓力與個人生活歷程共同塑造的漸進過程。依訪談資料分析可以發現，影響犯罪者終止參與電信網路假投資詐欺犯罪的主要原因，包括擔心遭執法機關查獲、家庭因素、獲得合法工作、遭查獲服刑中、良心發現、賺夠了等，以下謹依受訪者的意見分析如次。

1.擔心遭執法機關查獲

電信網路假投資詐欺犯罪者，因為感知到遭執法機關查獲的風險日益增加而終止犯罪。如受訪者 P2 即認為，犯罪者擔心終有一朝會被警察機關查獲，而終上犯罪。受訪者 P4 更進一步表示，很多犯罪者會隨著年齡的增長，逐漸厭倦每天過著，害怕被警察查獲，擔心被同夥黑吃黑、或遭自己人出賣，這種身心俱疲，提心吊膽的日子。

他怕真的有 1 天，被抓到了。(P2-1-1-3)

很多人是單純「累了」、「怕了」，幹這一行的壓力其實非常大，每天提心吊膽，怕警察、怕黑吃黑、怕被自己人出賣。(P4-1-1-3)

2.屢次犯罪失敗

受訪者 P3 則指出，犯罪者可能因為技術不佳，導致製作的犯罪劇本屢次詐欺失敗，使其覺得犯罪獲利不如預期，因而停止犯罪。

他作出來的腳本，劇本都騙不成功。(P3-1-1-3)

3.家庭因素

多數受訪者均認為，有些犯罪者受同儕影響而參與犯罪，可能會因生活社交環境產生變化，如結交正向的異性朋友，因對方無法容忍他的犯罪行為，而停止犯罪。或因結婚生子而多了家庭羈絆，突然意識到，不希望孩子知道爸爸是個騙子，更不想因為坐牢而錯過孩子的成長。或因親朋好友間的非議而終止犯罪。

畢竟這個是見不得光的，親戚朋友會問。(P2-1-1-3)
他交了一個穩定的女友或結婚了，而對方無法容忍他的犯罪行為。(P4-1-1-3)
我覺得從良或許是家庭的因素吧。(P5-1-1-3)
家庭的照顧跟關懷，是可以讓青少年導正的 1 個很重要的原因。(P6-1-1-3)
有了老婆、小孩之後為了家庭停止。(P7-1-1-3)

4.獲得合法工作

受訪者 P4 認為，犯罪者或更生人經政府就業輔導、技能培訓，終尋得願意接納他們的友善雇主，而獲得一份合法的工作，使渠自覺必須靠自己雙手、有尊嚴地活下去，而終止犯罪。

有一個能讓他靠自己雙手，有尊嚴地活下去的正當機會。(P4-1-1-3)

5.遭查獲服刑中

受訪者 P4 及 P8 均指出，將犯罪者收押或送入監獄服刑，運用嚴厲的法律制裁，使其沒有辦法繼續犯罪，並實際體驗失去自由、與家人隔絕的生活，利用獄中艱苦的環境，使其澈底清醒，打破輕鬆賺錢的幻想，是讓犯罪者停止犯罪最直接的因素

法律制裁是最直接的因素。(P4-1-1-3)
他去入獄服刑，或者是被收押，所以就會沒有辦法犯罪。(P8-1-1-3)

6.良心發現

受訪者 P3 及 P4 指出，犯罪者可能發現自己的親友也被詐欺，或是在法庭上，遭被害人聲淚俱下的控訴，逼使他正視自己造成的傷害，讓長久以來麻痺的良知突然被喚醒，而產生同理心停止犯罪。

作這個會良心不安，就這樣停止了。(P3-1-1-3)
產生同理心，逼使他去正視自己造成的傷害。(P4-1-1-3)

7.賺夠了

受訪者 P2、P7、P8 認為，電信網路假投資詐欺犯罪者，在多次犯罪獲得鉅額利潤後，發現已經賺夠了，就會轉投資，漂白去做其他的正當的經濟活動。

想要漂白去做其他的正當的經濟活動。(P2-1-1-3)
他會發現已經賺夠了。(P7-1-1-3)
覺得說我賺夠了，賺飽了。(P8-1-1-3)

第二節 電信網路假投資詐欺犯罪的犯罪腳本

本研究運用犯罪腳本分析技術，建構電信網路假投資詐欺犯罪者，在犯罪過程中所作的選擇和決策模式，並擴展到犯罪行為順序的所有階段，詳細且全面的描述犯罪者實施特定犯罪行為全部過程。基此，本研究先蒐集整理電信網路假投資詐欺犯相關案例資料，再深度訪談具有策訂防制及偵辦是類犯罪經驗的相關業務主管與第一線員警，請渠等表示意見及看法後整理歸納分析，發現電信網路假投資詐欺犯罪集團在獲取不法利益極大化、被捕風險最小化的理性選擇下，會反復運用最容易得手且最安全的犯罪模式實施詐欺犯罪，因此，電信網路假投資詐欺犯罪腳本可區分為犯罪前行為與準備、主要犯罪行為、犯罪後行為（如圖 4-1），茲說明如下：

一、犯罪前行為與準備

在電信網路假投資詐欺的犯罪腳本理論分析中，犯罪前準備行為是構成整體詐欺流程的基礎，亦是犯罪集團得以高效率運作的重要節點。電信網路假投資詐欺已成為黑道幫派組織不法獲利的主要來源之一，為了確保犯罪運作能有效規避警察機關查緝，集團往往透過接近、引誘乃至賄賂等方式拉攏不肖執法人員，藉以建立外部保護網絡。此外，犯罪集團亦積極招募各專業領域的不肖從業人員，如廣告投放商、APP 開發工程師、資通系統架設商、銀行從業人員、律師與代書等，使其分別在廣告宣傳、技術維護、金融流轉及法律掩護等方面提供支援，藉此形成跨領域合作的犯罪基本盤。在組織架構上，集團往往依功能分工切割為多個子單位，包括集團首腦、詐欺機房與話務團隊、車手與人頭帳戶提供者、駭客與資通技術支援群組，以及地下匯兌與洗錢網絡等，各子集團雖鬆散但透過網絡化管理模式相互連結，並由具專業背景之成員負責管理及訓練，提升整體行動之效率與隱匿性。基此，本研究認為，犯罪前準備行為可從「召募犯罪成員」與「準備犯罪工具」兩個面向加以分析：前者涉及人力資源的擴張與專業化，後者則涵蓋技術設備、金融帳戶與法律掩護之全面性準備。透過上述多層次的規劃，詐欺犯罪不僅具高度組織性，亦展現出專業化與跨領域合作的特徵，使其危害更為深遠，對執法機關之偵查與防制形成嚴峻挑戰。

（一）招募犯罪成員

電信網路假投資詐欺犯罪是黑道幫派組織犯罪不法獲利重要來源，犯罪集團為逃避執法機關查緝，會想方設法接近、引誘、賄賂不肖執法人員加入犯罪行列或為犯罪集團提供保護傘，並網羅廣告投放商、APP 開發工程師、資通系統架設商、銀行從業人員、律師、代書等各專業領域的不肖人員，再運用細密的犯罪分工，組成關係鬆散的犯罪網絡組織，並將整個犯罪集團切割成為集團首腦、詐欺機房、召募詐欺機房電話手集團、提領贓款車手集團、提供人頭帳戶集團、竊取個資駭客集團、地下匯兌洗錢集團、提供資通訊技術集團等，各組織均有明確任務分工，並由具有各項專業背景人員負責管理及訓練，組織結構完整，又採用網絡管理模式，讓整個犯罪組織更具效率，使其危害程度更加嚴重。根據以上的觀點，本研究分析發現從事電信網路假投資詐欺的主要犯罪人員多具有黑道幫派犯罪組織背景，並常以金錢利益為餌，同時透過刊登廣告、利用人際關係網絡、或以誘騙，或以犯罪技術分工為導向，或招募社會邊緣人或通緝犯等方式及管道，引誘新成員加入犯罪。

1.主要犯罪人員多具有黑道幫派犯罪組織背景

歸納多數受訪者意見，由於此類犯罪相較於傳統暴力犯罪，犯罪者的人身安全風險極

低，而獲取不法利益額度卻極為龐大，且有不易遭執法單位查獲，就算遭查緝被判之刑責通常偏低的特性，促使黑道幫派組織在犯罪成本效益考量的理性選擇下紛紛糾集幫眾加入犯罪，加上黑道幫派組織比較容易召募到各專業領域的不肖人員，又可運用黑惡勢力有效制約犯罪集團成員，防範遭黑吃黑，且洗錢的管道暢通，並可為境外詐欺機房撐起保護傘，不受當地的黑道幫派組織侵擾，使得此類犯罪成為黑道幫派組織的重要由經濟來源。

我覺得他的黑道身分，可能讓他更便於去找這些詐欺集團的成員，或者是他在別的國家，他要能夠在當地不要被侵擾，它的黑道身份，有一定的幫助，我覺得我遇到的是這樣的狀況。(P3-1-3-1)

像臺灣前一兩年的那個台版的柬埔寨那些，或許就需要一些黑道來控制，因為車手時有所聞啊，他們會把帳款拿了就黑吃黑跑掉了啊，一定要幫派的人才有辦法將這些人抓回來。(P5-1-3-1)

我們現在實務上看到有黑幫的介入很重要的一點就是其實黑幫介入的很大的1塊都是在車手端，車手需要黑幫的介入，很大的原因是因為他怕車手黑吃黑，唯有靠黑幫的力量他才有辦法去約制，把所有的錢拿回來，其實這是黑道會去介入的原因。(P6-1-3-1)

我們正常人是沒有辦法洗錢的，不管你再厲害都一樣，你一定要有1個固定的組織去做統整規劃，那大部分上面應該是黑道啦，如果把角頭也算到黑道的話，那都是黑道。(P7-1-3-1)

許多黑道幫派他們都有經營詐欺的產業，從上游到下游，都會派他的幫眾來參與，那比起用強暴、脅迫的手段來取得錢財來的輕鬆好賺，又不用以命來跟他相拼，稍微比較安全一點。(P8-1-3-1)

因為他們接觸的都是現金，而且大量現金，所以你如果不熟的話，很可能就會被黑吃黑，所以他們要在同1個Team裡面，就是在同1個幫派裡面。(P9-1-3-1)

2.常用以金錢利益為餌引誘犯罪成員加入

電信網路假投資詐欺犯罪集團善於利用資通訊科技設備及方法，以分散犯罪地點並隱身境外實行犯罪，在當地國刻意保護包庇下不易為警方查獲，即便遭到查獲詐欺犯罪行為，也常因該等犯罪行為涉及跨境執法合作，完整取證相當困難，在缺乏完備犯罪事證情況下，被判之刑責通常偏低。因此，所有受訪者均認為，犯罪者基於理性選擇，認為從事電信網路假投資詐欺犯罪，遭執法人員查獲的機率不高，犯罪風險小，獲取不法金錢利益快速而安全。

我想當然都是為了錢啦。(P1-1-1-1)

你看有的都是「甲賀道相報」(閩南語)，為什麼是「賀」(閩南語)就是利益。(P2-1-3-2)

我覺得營利是1個最大的目標啦。(P3-1-1-1)

賺快錢是最主要的驅動力，這絕對是最強的誘因，沒有之一。(P4-1-1-1)

我們實務上看到蠻多人，其實都是以電信詐欺維生，所以我相信那是他的動機，也是他的目的啦。(P5-1-1-1)

都是為了利益，都是為了錢，他們的目的他們自己都有評估過，可能做這樣的事情，被抓的機會是比較低，都有僥倖心態在。(P6-1-1-1)

十之八九都是，幾乎都是為了錢。(P7-1-1-1)

大多都是因為經濟狀況不佳缺錢，或者是年輕人想要做輕鬆、快速賺錢的工作，而因而來參與犯罪的。(P8-1-1-1)

就是要賺錢嘛，他們就是幫派的成員，你要賺錢，所以他們去從事這個詐欺。(P9-1-1-1)

3.招募犯罪成員模式及管道

根據訪談結果資料顯示，電信網路假投資詐欺犯罪集團招募犯罪成員的方式相當多元，經整理受訪者的意見，招募犯罪成員的方式包括：刊登廣告、利用人際關係網絡、以誘騙方式、以犯罪技術分工為導向、招募社會邊緣人或通緝犯加入等，茲分述如下

(1)以刊登廣告方式進行招募

受訪者 P5、P8 表示，犯罪集團的組織者會在 Facebook、Telegram、LINE 等社群媒體或地下論壇，以免經驗、工作輕鬆、快速致富或出國工作等作為噱頭，刊登廣告進行招募。

許多銀行的從業人員他也會上求職網啊，還是說去看說有沒有要賺外快的，我真的覺得現在大家都很缺錢，房價太高大家都想賺錢。(P5-2-1-1)

電話手跟車手的部分，大多都是透過刊登免經驗，工作輕鬆的廣告就可以招募到這些角色的人。(P8-2-1-1)

(2)利用人際關係網絡進行招募

綜合受訪者 P2、P5、P6、P8 的意見，犯罪組織內成員會透過人際關係網絡，拉攏口風緊且願意協助詐欺犯罪的同學、朋友、親戚等熟識或有交情者加入犯罪組織，待渠等加入後，再依照他們原本的職業角色協助犯罪，例如：銀行從業人員可協助提供客戶的個資，律師則是將偵查中的秘密洩漏給犯罪集團，讓詐欺集團高層知悉檢警偵查進度，代書則是協助被害人辦理不動產抵押貸款。

至於說你說律師、銀行人員，那是漸進式的，在推展過程當中，我可能就是一家銀行的客戶…你跟行員點一下，也許就有人會就接，所以人員來源不會斷掉，他是被吸收的，就跟警察、司法人員、檢察官都一樣。(P2-2-1-1)

常跟那個銀行來往或有些交情的客戶，然後我在作詐，你來幫我們，我們合作一下。(P5-2-1-1)

我觀察到大部分都是主嫌的朋友，是主嫌去找的，1 個 1 個找他信得過的人，就像很多那個銀行的從業人員，也都是他小時候的玩伴，所以這一些人都不是隨便亂找的，這一些人本身要口風緊，要願意協助他們。(P6-2-1-1)

銀行的從業人員、律師、代書這一些比較高技術性的核心層次的一些角色，則是從平常業務先接觸開始，然後有意無意的去探尋他們有沒有要配合詐團的這個可能，以此來吸收作為幫忙做詐欺的工作，然後再依照它原本的職業角色協助。(P8-2-1-1)

(3)以誘騙方式進行招募

誘騙不懂法律規定的年輕人或不知情的求職者參與犯罪，如 P4 表示，犯罪集團會以「這只是金錢糾紛」、「法官會對初犯輕判」等話術，欺瞞不諳法律規定且無前科素行的年輕人參與犯罪。P9 則指出，犯罪集團會在網路上假冒知名公司發出徵人告示，召募不知情的民眾充當取款車手。

他們會跟新人說：「這只是金融糾紛，不是什麼大罪」、「你沒前科，就算被抓到也是初犯，法官看你年輕，最多判個緩刑，不會有事的啦，對於一個不懂法律的年輕人來說，這聽起來非常合理。(P4-1-1-1)

我們有辦過，其實他們也不知情，他們只是要賺取佣金而已，所以他們也不知道說這些被害人是被騙的，這些應該大部分都不知道。(P9-2-1-1)

(4)以犯罪技術分工為導向進行招募

歸納受訪者 P2、P4、P8 的意見，發現犯罪集團仿照企業經營模式，以犯罪技術分工導向，建構完整的犯罪產業鏈，將整個犯罪集團切割成數個互不隸屬組織，再召募具有各項專業背景人員參與犯罪，組成關係鬆散的犯罪網絡組織，各節點間彼此均透過通訊軟體代號方式聯繫，以製造聯繫斷點，讓得警方亟難掌握成員間真實身分。

科技公司，或者是資訊公司，他幫忙寫 APP 或者架設 WEB 的 SERVER，所以他們被吸收，我們的解讀是叫吸收，對他來講叫商業行為。(P2-2-1-3)

詐欺集團不是一個垂直型的組織，而是由各種不同功能的團伙集合出來的產業鏈，詐團施詐前會先找好有需要的合作對象，依詐欺手法案類不同，會有不同的排列組合，比如說，假投資案件，必需與廣告商、轉帳水房、車手集團配合。(P4-2-1)

資通訊系統的架設商屬於詐團的協力廠商，他們都是按件計酬，大部分都不是詐團組織的當中的一員，詐團只需要找到有這些專業能力的人接案就可以了，不需要特別的招募進來，當作 1 個固定的一員（P8-2-1-3）

(5)招募社會邊緣人或通緝犯加入

受訪者 P4 指出，犯罪集團會引誘有詐欺犯罪前科，導致求職無門的社會邊緣人，加入犯罪集團。受訪者 P8 表示，犯罪集團也會吸收或利用因犯罪遭通緝，在臺灣走投無路的通緝犯，協助安排或引誘這些通緝犯前往國外詐欺犯罪機房參與犯罪。

哪個老闆敢用一個有詐欺前科的人來管錢或接觸客戶？社會把他推開，但犯罪圈子卻張開雙臂歡迎他，他過去的「前科」反而成了圈子裡的「資歷」。(P4-1-1-2)

蠻多都是在臺灣作車手，被抓好幾次然後發現要被通緝了，還是要執行了，他就直接前往國外詐欺就變成電話手，很多機房其實都是那些車手化身為電話手。(P5-2-1-1)

(二)準備犯罪工具

詐欺集團為逃避警察機關追查，將所施詐術與電信、網路等路徑相互結合，利用網際網路資訊互通開放，不受時間、空間、地域限制所影響的特性，輕易將大量詐欺訊息傳送給不知情的民眾，特別在通訊與資訊技術結合後，利用通訊系統轉接網路再轉接通訊系統或利用通訊軟體，不但犯罪者的帳號身分隱匿，IP 位址更可以藉由虛擬私人網路 VPN（Virtual Private Network）專業技術加以隱匿，再輔以犯罪集團配合社會脈動事先精心編造各式假投資詐欺劇本，假借各種虛構之身分及名義，由多名成員分別扮演不同詐欺角色，利用資訊、通訊及大眾傳播媒介等管道，傳遞不正訊息給社會大眾，再進一步操弄、掌握及誘騙，使民眾輕易掉入犯罪集團所設陷阱，造成鉅額財產損失。根據以上的觀點，本研究分析發現實施電信網路假投資詐欺的的犯罪過程中需要製作假投資廣告、人頭電話與帳戶、車手集團、洗錢水房、詐欺機房等各種技術工具、平台與輔助資源。

1.製作假投資廣告

詐欺犯罪集團結合廣告商，盜用名人照片或利用各種名義設計精美誘人的假投資廣告，並透過網路社群平台投放，吸引潛在被害人點閱，再引導渠加入詐團機房成員成立的假投資 LINE 群組。有關假投資廣告來源。綜合受訪者 P3、P4、P5、P9 意見，假投資廣告的來源，包含被詐欺集團欺騙，誤認為是幫合法公司做行銷，或是心照不宣收錢辦事，或與詐欺集團有合作關係。

作這種廣告的人，可能會因為這樣被騙，說我是要幫公司做行銷…就是被詐欺集團騙去作廣告的人，這些人他多少是知道這個廣告有問題的，…講難聽一點，他為什麼要作？因為我平常只收張三這個 Nobody 只要 1 個人 1 萬塊，這個人給我 100 萬，我為什麼不收。(P3-2-1-4)

詐欺集團不會去養廣告產業鏈，他一定是說這個人平常就在作廣告，然後他可以跟他做合夥，夾帶詐欺廣告。(P4-2-1-4)

應該是有專門的人在作，詐團就是委託你幫我作…所以廣告就給你去設計啊，後面有 1 個加 line 的連結。(P5-2-1-4)

廣告投放商很細，就是他們會找人去設計這些廣告…這些人就是，我有錢就好了，我問這麼多幹嘛。(P9-2-1-4)

2.人頭電話

綜合多數受訪者意見，詐欺集團人頭電話的來源，包括：在黑暗網路或者網路社群平台收購，或收購流通在外的公司門號或者外勞電話卡等二手或預付卡，或者境外門號，藉以隱匿真實身分，躲避執法機關查緝。

以前有一些公司門號流通在外，還有一些外勞卡有流通在外…以前你在網路上就買的到一門

300 元，現在台哥大大概是 5000 至 7000 元。(P2-2-1-3)

在黑暗網路或者是特定的 Telegram，那些群組都買得到。(P3-2)

蠻多人會為了那一點錢去出賣自己名下所申辦的金融或電信服務。(P5-2-1-3)

大部分還是跟人頭來買，這些想缺錢的人來買他們名下申請的門號來做人頭電話，作為犯罪工具。(P8-2-1-3)

可能用那種 852 境外門號，現在很多境外門號，你來旅遊的根本就不用申請啦。很簡單就可以拿到那些門號了，那個一次可以買好幾萬張，1 張 500 塊。(P9-2-1-3)

3.人頭帳戶

綜合歸納受訪者多位意見，詐欺集團取得人頭帳戶常見有四種方式，第一種方式，在黑暗網路或者網路社群平台，向帳戶所有人蒐購；第二種方式，帳戶所有人出於借貸需求，將金融帳戶交給詐欺集團，詐團再以美化帳戶金額進出，以提高貸款金額等話術，要求帳戶所有人配合，提供提款卡密碼供詐欺集團使用或是協助領取現金；第三種方式，帳戶所有人在求職的過程，遭詐欺集團以薪資轉帳需要，欺瞞帳戶所有人提供銀行存摺及印章作驗證等藉口，以騙取金融帳戶存摺及印章；第四種方式最為惡質，犯罪集團為最大化人頭帳戶使用效益，將帳戶所有人私行拘禁或以毒品控制，以免被人頭帳戶所有人提領帳戶內款項或應人頭帳戶所屬金融機構驗證帳戶持有者身分所需或臨櫃辦理相關手續。

有三種的主要來源，第 1 個就是應徵，第 2 是假貸款…第 3 種真的是實際去收購。(P2-2-1-2)

因為他怕我離開的話，會去把錢領走，還是說銀行帳戶被警示，我必須帶著你去臨櫃處理一些事情，所以那些人是要入控，臺版柬埔寨那些人就是比較惡劣，不想付那個錢，就用一些毒品去控制他們。(P5-2-1-2)

現在大部分八成用騙的，兩成用收購的…因為人頭帳戶現在一本二三十萬，我都還沒開始騙人，我就先花這個成本，怎麼可以，所以他們現在都用騙的。(P6-2-1-2)

就是去詐欺一些沒錢但有帳戶的人，他們都用騙的，很少用買的。(P7-2-1-2)

賣的人很少了，那所以他們就是轉換成用騙的方式騙你的帳戶。(P8-2-1-2)

去 FB 登偏門工作，他們也有朋友拉朋友，跟朋友問，你有沒有缺錢，需要錢我一本帳戶 20 萬、30 萬跟你買啊。一本 20 萬缺錢的人就會賣了。(P9-2-1-2)

4.車手集團

受訪者 P6 指出，有些犯罪集團會利用懷孕的女性擔任取款車手，藉以利用刑事訴訟法第 467 條所規定懷胎五月以上，為保障孕婦和胎兒的健康，避免在懷孕期間進行羈押之規定，以避免遭查獲時被檢察官向法院聲請羈押。

我們之前有發現有一些詐欺集團會請懷孕的女生去當車手，為什麼？因為她不會被羈押，一定交保，那是刑訴法寫的懷孕超過 5 個月，就是交保。(P6-1-3-3)

受訪者 P7 認為，犯罪集團會糾集未成年或 20 歲以下的人員擔任車手，除比較容易操控外，亦可預防遭車手黑吃黑捲款潛逃，同時可規避法律責任。

車手他們其實不會用自己的人來作…車手現在越來越年輕了…他們會盡量先找未成年的，未成年的找不到之後，可能就會找一些 20 歲以下的。(P7-1-3-3)

受訪者 P9 表示，車手集團大都由黑道幫派組織所掌控，並以承攬派工及單線領導方式，指揮個別車手向被害人收取動產或出金給被害人，以製造查緝斷點，使得警察機關難以溯源查緝幕後主嫌。

我要找哪 1 個車隊，就是有得抽成就好了，所以他們都是個別發展的不會有人 1 條龍全包的。(P5-2-1-4)

我現在需要車隊 1 號車手（指第 1 層車手直接向被害人收款的犯罪者）、2 號車手（指接收 1 號車手贓款的犯罪者）、3 號車手（指接收 2 號車手贓款的犯罪者），我就會在幫派的群組裡面問說，今天有沒有誰要做，包這個工程就對了。(P9-1-3-1)

5.洗錢水房

電信網路假投資詐欺犯罪集團，運用金融交易數位化及支付工具多樣化的特點，利用人頭開設銀行帳戶，或藉由資通訊工具隱匿身分，使用金融科技在網路上開戶並快速轉移贓款，或利用為數眾多，提款地點便利的自動櫃員機提取轉移贓款。近年來虛擬通貨在世界各國陸續掀起流行浪潮，迄今在市場上流通的種類已超過上萬種，因其具有點對點交易、去中心化、匿名性的特性，在追查不易且國際互助有限的情況下，已有愈來愈多的犯罪集團利用虛擬通貨冷錢包地址接收從被害人取得之虛擬通貨，再將資金轉到中心化交易所的地址以兌換成法定貨幣，以製造金流斷點，造成後續調查取證、贓款沒收、返還、凍結之困難性。經綜合多位受訪者意見，由黑道幫派掌控並設於臺灣境內或東南亞地區國家的洗錢水房，透過人頭帳戶層層轉帳，或由車手集團成員向被害人收取款項，或由被害人自行購買虛擬通貨，再由轉帳水房統一購買虛擬通貨或接收害人自行購買虛擬通貨，轉至境外交易所的錢包。

以洗錢的管道來講，虛幣是電詐集團最喜歡用的。(P2-2-3-3)

利用人頭帳戶層層轉帳，再由車手提款後購買虛擬貨幣，轉到國外境外交易所的錢包。(P4-2-3)

因為他有很多斷點，我可以洗好幾層，洗到國外，然後再從某 1 個虛擬通貨交易所出來，然後最後面領出來。(P5-2-3-1)

最後虛擬貨幣流到泰國、緬甸那邊的帳戶的申請人，錢會流到東南亞去比較多啦。(P7-2-3-1)

轉帳水房的部分…他設置的地點有可能是在國內、國外都可能會有。(P8-2-2-7)

6.詐欺機房

依據多位受訪者意見指出，犯罪集團利用資(通)訊科技設備及方法並隱身於柬埔寨及緬甸等東南亞地區國家實行電信網路假投資詐欺犯罪，並在當地國刻意保護包庇下使得警方查緝無門，使得犯罪集團有恃無恐，犯罪氣陷日益囂張，造成偵查打擊之困境。

我們剛剛在討論的這個詐欺群組…看起來大概在柬埔寨很多，然後緬甸。(P1-2-2-7)

詐欺集團的機房都是在東南亞柬埔寨。(P2-2-2-7)

都在泰國跟柬埔寨邊緣，那個可信度很高，應該都在那邊。(P3-2-2-7)

詐欺機房的部分，大部分都會設在國外，而且比較集中，在什麼柬埔寨，然後緬甸這些詐欺園區啦，什麼什麼 kk 園區，什麼西港園區等等。(P8-2-2-7)

跨國犯罪據點通常會在這個東南亞、柬埔寨、還有緬甸，然後會利用這些海外的機房、跳板機房或境外人員去操控。(G2-2-2-7)

二、主要犯罪行為

詐欺集團透過交友平臺以假份美女或俊男方式結識潛在被害人，待時機成熟再慫恿渠等加入特定網路社群媒體的理財群組，或利用潛在被害人在觀看理財新聞或影片時，透過網路演算法的機制，強制彈跳出「高獲利投資理財」等廣告，在渠等一時好奇點選觀看聯結時，即遭引流加入特定理財群組。隨後犯罪集團利用渠等急於獲利心態，以投資飆股、虛擬貨幣、期貨、外匯及基金等名義吸引加入詐欺集團所架設的不實投資網站或下載 APP，初期讓被害人小額獲利，待其誤信為真而投入大量資金，欲實現獲利時，即以各種理由拒絕出金，俟被害人發現帳號遭凍結或網站關閉始知遭詐，造成鉅額財產損失。詐欺集團掌

握人性「貪心」與「不甘心」等心理因素，利用各種資通訊科技工具，編製客製化詐欺劇本，以獲取不知情民眾的信任，當被害人相信詐欺話術深陷在詐欺情境時，他人縱使費盡九牛二虎之力勸說，亦難撼動被害人對犯罪集團的信任。也有些被害人雖懷疑自己被詐欺，卻因貪於虛假的高報酬率或礙於面子而不願承認，因為沒人想承認自己是傻瓜，直到被掏光所有錢財，始驚覺遭詐欺。根據以上的觀點，本研究依據受訪者的意見，將灣電信網路假投資詐欺犯罪的主要犯罪行為區分為 利用資通訊工具投放虛假投資訊息以吸引民眾注意，以通訊軟體群組，與潛在被害人建立信任，營造高獲利假象，對被害人洗腦，提供小額獲利，以獲得被害人信任，慫恿被害人，大量投入金錢，最後詐欺完成，犯罪集團成員全數失聯等階段。

(一)利用資通訊工具投放假投資訊息，吸引民眾注意

綜合受訪者 P1、P7 所表示意見，詐欺集團成員利用虛偽頭像（人頭照片）假扮的美女或俊男，再利用網路社群媒體例如：Line 或 WeChat 等通訊軟體與潛在被害人互加為好友。

他會用通訊軟體跟你互加好友。(P1-2-2-3)
先到臉書投放，然後是交友軟體交朋友，然後引誘被害人加 LINE。(P7-2-2-3)

綜合受訪者 P2、P4、P5、P6、P8 所表示意見，詐欺集團利用潛在被害人在使用網路社群媒體，例如：臉書、IG、YOUTUBE 等觀看理財新聞或影片時，透過網路演算法的機制，強制彈跳出「高獲利投資理財」等廣告。

在網路上投放假投資訊息讓你點擊，你如果對有興趣就加 LINE，都是你主動連上去的。(P2)
先叫廣告商盜用名人照片投放誘人廣告吸引被害人。(P4)
他的起手式是要先放詐欺廣告，要投放詐欺廣告，那個演算法它有高度專業。(P5-2-1-1)
像 FaceBook、Google、Youtube 這一種就是受眾族群最多的，國人受眾族群最多的，他就會去投廣告。(P6-2-2-3)
透過二類電信公司代為投放這個假投資的詐欺簡訊，簡訊裡面也會有讓你加 Line 的連結，另一種方式，就是用電信簡訊的方式 (P8-2-2-3)

(二)透過通訊軟體群組，與潛在被害人建立信任

受訪者 P1 表示，詐欺集團成員與潛在被害人透過通訊軟體互加好友後，接續對其發動柔情攻勢，每天噓寒問暖以取得被害人信任，並發展網路戀情，待時機成熟再慫恿渠等加入特定網路社群媒體的理財群組

他會先跟你發生一段這個網路的戀情…會瞭解你這個人的生活習慣，你的喜好，不定時的寄一些禮物給你，甚至會給你寄蛋糕等等，接下來推薦被害人去下載理財 APP，然後加入群組。(P1-2-2-3)

綜合受訪者 P2、P3、P5、P7、P8 所表示意見，潛在被害人在瀏覽假投資廣告、網頁的過程中可能會因一時好奇而點選頁面的連結，而加入詐欺集團事先創建為數數十人至百人的虛假理財通訊群組，該群組內成員可能包括理財助理、老師、會員等等，但僅有少部分是潛在被害人，絕大部分是為取信潛在被害人，而由數位詐欺集團人員以一人分飾多角的方式所所假冒，在取信潛在被害人過程中詐欺集團會用罐頭訊息或者是機器人對話方式，營造群組內熱絡討論投資訊息的假象，甚至要求潛在被害人參加投資講座，以塑造正面投資形象。

那個群組有很多人共同在騙，他們就是 1 個人操控了很多個帳號，用罐頭訊息或者是機器人

跟你在聊，我們有爬梳一些個案，他 1 個人大概會掌控著 10 個以上的帳號，同時經營幾十個群組。(P2-2-2-1)。

理財群組裡面的助理會過濾你有沒有真的要投資，先看看你懂不懂，如不懂會請你去上課。(P3)

裡面會有一些老師，每天 PO 一些投資的訊息，那其他帳號都是詐團的人，他就說感謝老師啊，那個真的很準，我賺多少錢幹嘛，然後就一直 PO，其實就是想洗你啦。(P5-2-2-4)

這個群組有 100 個人，只有 1 個被害的人，就是你自己，其他 99 個都是他們的暗樁。(P6-2-2-4)

會有個講的老師，然後會有一大堆的暗樁，然後去跟老師說啊，今天賺錢啦。(P7-2-2-4)

被害的頂多一、兩個而已，其他都是他們的暗樁。(P8-2-2-4)

(三)營造高獲利假象，對被害人洗腦

綜合受訪者 P2、P5、P6、P8 所表示意見，犯罪集團再利用預先佈置謊稱助理、老師的成員帶領操盤，並逐日貼出偽冒對帳單；或利用工程師操控一些以假亂真的投資 APP，以營造高獲利的情況，並利用暗樁在群組內不停的聲稱已經有高額的獲利，藉以吸引潛在被害人加入假投資平臺。

工程師他們控盤，你要看到什麼我都能夠給你秀，但是最後今天的收盤都跟市場的一模一樣。(P2-2-2-2)

他們會買斷一些 APP，所以有辦法去調哪幾個股價怎樣獲利多少。(P5-2-2-4)

你就每天看到這個群組每天都在賺錢，然後每天就在那個 PO 那個對帳單，又加了好幾百萬，這樣你心就你就開始癢了。(P6-2-2-4)

營造高報酬、低風險、穩賺不賠，持續獲利的假象。(P8-2-2-4)

(四)提供小額獲利，以獲得被害人信任

綜合受訪者 P1、P3、P6、P8、P9 所表示意見，待被害人初步配合詐欺集團指示匯款到指定人頭帳戶進行投資，接續為取信被害人，使其相信假投資理財群組中老師所言及其他人獲利都是真實，會假造高額獲利，並小額出金給被害人，營造出專業投資人的形象，以增加其信任感，並鼓吹被害人加碼投資，另外，現在詐欺集團大都會指示出金車手直接用面交出金的方式出金，以規避轉帳匯款，或指示其他被害人以匯方式出金，例如：A 被害人匯款（出金）給 B 被害人，以躲避警察機關查緝。

他會指示車手要去銀行或者是用網路轉帳給特定的帳號，這些特定的帳號就是被害人，這個叫做出金。(P1-2-2-6)

你就想說，買 1 個看看，結果隔天就漲停了，然後可能 10%的獲利，他會馬上把獲利匯到你的帳戶，會讓你相信這是可以出金的。(P3)

有一些也是被害人再匯給被害人，他會跟你講說這個要繳會費啊。你今天加入我這個投資群組要繳一萬塊的會費，其實你匯給某 1 個帳號，其實這個帳號，是另外 1 個被害人的帳號。(P6-2-2-5)

就是照常會收購一些專門用來出金的人頭帳戶，然後由出金手轉帳到被害人的帳戶裡面。(P8-2-2-5)

我今天從 A 被害人收錢，比如說 100 萬，其中 10 萬塊，直接叫一號車手去交給 B 被害人，直接用面交出金的方式，就是規避轉帳匯款，因為你匯款會被抓會紀錄。(P9-2-2-5)

(五)慫恿被害人，大量投入金錢

綜合受訪者 P1、P3、P8、P9 所表示意見，當被害人相信騙局之後，詐欺集團就會誘使民眾大量匯款至犯罪集團提供的人員帳戶，或要求被害人備妥鉅額現金或介紹被害人向假冒商家購買巨額虛擬通貨，犯罪集團再派出「理財專員」到府出示身分、面交收款鉅

額現金或虛擬通貨。

群組的人會作 sakura（作場面）說一定要這個加碼投資，去引誘這個被害人，開始大把的錢投進去了。(P1-2-2-6)

因為高額金額，而且面交，我曾經看到有的案例在臺北市可以面交 29 次到 40 幾次都有。(P3-2-2-6)

讓你覺得我有賺到錢，他就越投越多越陷越深。(P8-2-2-4)

你每個禮拜或每個月你都有收到錢，就越投資越多。(P9-1-4)

(六)詐欺完成，犯罪集團成員全數失聯

受訪者 P1、P2、P4 表示，待被害人投入鉅額錢財，欲出金實現獲利時，客服人員即以各種理由拖延、未回訊息、謊稱駭客入侵，甚至關閉網站，致使被害人求償無門後，始知遭到詐欺。

他把錢全部都投資進去，然後把他踢出群組。(P1-2-2-6)

等到你持續加碼，被洗腦後，再投資更多的時候，就把你 close。(P2-2-2-6)

最後，再以各種理由拖延出金，甚至踢出群組、關閉網站，最終使被害人血本無歸。(P4-2-2)

三、犯罪後行為

電信網路假投資詐欺集團在騙得被害人錢財後，為順利隱匿犯罪所得並規避執法人員的追查，會利用金融科技(如人頭帳戶、虛擬通貨)便利性迅速轉帳，或利用地下匯兌等多元洗錢管道製造斷點以隱匿贓款，再利用多種金融工具，將其犯罪所得漂白，使得犯罪者得以合法使用該所得。另外，近年來虛擬通貨在比特幣（Bitcoin）問世後，開始掀起民間發幣熱潮，乙太坊（Ethereum）、瑞波幣（Ripple）等各式各樣虛擬通貨陸續問世，迄今在市場上流通的種類已超過上萬種，理性的犯罪集團亦趁此機會利用虛擬通貨點對點交易、去中心化、匿名性及可與法定貨幣相互兌換之特性，先誘騙被害人購買虛擬通貨存入冷錢包帳號，再轉移到詐欺集團持有之虛擬通貨冷錢包地址，再轉至中心化交易所地址兌換成法定貨幣，以製造犯罪金流斷點，為後續警察及司法機關調查取證、贓款沒收、返還、凍結帶來極高難度。而在脫免遭警察機關逮捕部分，犯罪集團為獲取更佳的犯罪機會，經理性思考後，運用資(通)訊科技設備及方法，將犯罪地點分散在數個國家(地區)，並將最重要的詐欺機房設置在執法機關對是類犯罪缺乏辨識能力，且偵查技術及相關設備不足之國家(地區)，加上當地國刻意保護包庇使得警方查緝無門。

(一) 隱匿贓款

詐欺集團收取贓款後，利用金融科技(如人頭帳戶、虛擬通貨)便利性迅速轉帳，或利用地下匯兌等多元洗錢管道製造斷點以隱匿贓款，以規避執法人員的追查，其取得贓款方式包括： 利用金融人頭帳戶轉帳或轉匯、 由被害人親自面交給取款車手、 由 車 手 前 往金融機構或自動櫃員機提領款、 被害人將金融機構提款卡交付車手提領、 被害人自行購買虛擬通貨交付詐團。而隱匿贓款方式及管道則包括：換成虛擬貨幣，再於境外提領法幣、透過地下匯兌，將贓款先出境外、購買貴金屬，再走私出境、購買不動產，將贓款漂白、購買藝術品或投資（購買）高價商品等。

1.詐欺集團取得贓款方式

(1)利用金融人頭帳戶轉帳或轉匯

受訪者 P6、P7 指出，詐欺集團會指示被害人先前往金融機構，將詐欺集團提供的人

頭帳戶設定為約定轉帳帳戶，再要求被害人透過網路轉帳，將被詐款項轉匯至詐欺集團事先開設的人頭帳戶。

透過人頭帳戶嘛，就是他今天詐欺集團給你 1 個帳戶，叫你把錢匯到會到裡面去。(P6-2-2-6)

他們會請你去做約定帳戶，才可以大額匯款領錢，所以假投資大概就是約定帳戶。(P7-2-2-6)

(2)由被害人親自面交給取款車手

受訪者 P2、P5 指出，詐欺集團會指示被害人將手上的鉅額現金或要求前往金融機構領取大筆現金後，再指示面交車手至被害人住居所或工作地點收取，或約被害人前往詐欺集團事先勘查好，監視錄影鏡頭比較不密集的地點如：公園、停車場、橋梁旁與車手面交現金。

都會躲避鏡頭密集的公園、停車場、橋梁旁邊，但是，也有直接到被害人的住家裡面侵門踏戶。(P2-2-3-2)

假投資詐欺的最主要的收款方式是現金，他就是說我派投資專員去跟你簽約收取你股款。(P5-2-2-6)

(3)由車手前往金融機構或自動櫃員機提領款

受訪者 P8 指出，待被害人將被詐款項轉匯至詐欺集團事先開設的人頭帳戶後，詐欺集團會即時指揮取款車手，持事先開設的人頭帳戶存摺印章或金融卡前往金融機構或自動櫃員機提領現金。

比較簡單一點，就是叫車手去臨櫃，把錢領出來或者是去 ATM 把錢給領走啦。(P8-2-3-1)

(4)被害人將金融機構提款卡交付車手提領

受訪者 P6 指出，詐欺集團會指示被害人將金融卡交付給犯罪集團成員，再交由提款車手持被害人提款卡，前往自動櫃員機逐日以螞蟻搬家方式提領現金，直至被害人遭提領一空。

他們現在叫被害人把提款卡給他，他們用提款卡每天領十萬。(P6-2-2-6)

(5)被害人自行購買虛擬通貨交付詐團

受訪者 P2、P6 指出，詐欺集團指示被害人先開立虛擬通貨電子冷錢包帳號後，再要求被害人持鉅額現金前往虛擬通貨交易所，購買虛擬通貨並存入開立的冷錢包帳號，再轉移到詐欺集團的冷錢包。

開立 1 個冷錢包帳號…要求他把現金所購買的虛幣，轉移到指定的錢包地址。(P2-2-1)

叫被害人把現金領出來之後，不是交給車手，是去換成虛擬貨幣，再轉到詐欺集團的錢包。(P6-2-2-6)

2.隱匿贓款方式及管道

(1)換成虛擬貨幣，再於境外提領法幣

大部分的受訪者均指出，詐欺集團指派車手前往被害人住處取走現金，隨後至實體加密貨幣交易所（如「幣想」）將現金兌換為 USDT，並將該虛擬貨幣轉入詐欺集團掌控的加密錢包。此外，亦有詐欺集團直接指示被害人親自前往實體交易所，將現金兌換為 USDT，並轉入指定的加密錢包，以規避資金流向追查。又或詐欺集團引誘被害人將資金匯入特定金融帳戶，該資金經由地下金流「水房」層層轉帳後，匯入國內加密貨幣交易所的入金帳戶，再轉換為虛擬貨幣，最終匯入詐欺集團控制之其他加密錢包中，達成資金去識別化與跨境流動之目的。

我就去那個實體店面買虛幣，我就轉到錢包去。(P1-2-3-1)

最終的洗錢型態就是虛擬貨幣，百分之百應該都是。(P3-2-3-1)

利用人頭帳戶層層轉帳，再由車手提款後購買虛擬貨幣，轉到國外境外交易所的錢包。(P4-2-3)

我只要再跟國外的交易所把它換成現金你就拿到了，他都是算 U（虛擬貨幣）的。(P5-2-3-1)

買虛擬貨幣，然後透過這個提幣、轉幣的方式…去隱匿不法所得。(P8-2-3-1)

(2)透過地下匯兌，將贓款先出境外

受訪者 P8 指出，詐欺集團的車手或水房在收到被害人交付的款項後，即將現金攜往以銀樓、旅行社、國際貿易公司等名義作為掩護，實際上非法經營地下通匯的洗錢集團據點，以國內付新臺幣，國外提領等值（扣除洗錢集團手續費）的當地法定貨幣之方式隱匿贓款，以規避警察機關查緝。

過我們常見的傳統的方式就是會去銀樓啦、旅行社啦，或者是有做國際貿易生意的一些地點，去透過地下匯兌把騙到的錢洗出去，就是 A 地付錢，B 地換成相對的錢。(P8-2-3-1)

(3)購買貴金屬，再走私出境

受訪者 P8、P9 指出，詐欺集團的車手或水房在收到被害人交付的款項後，即前往銀樓購買體積小、價值高、去識別化且易於攜帶隱藏的黃金或鑽石等貴金屬，以方便隱匿或交走私集團走私出境後，在國外出售轉換成當地法定貨幣，以降低詐欺所得被警方發現的風險。

去銀樓用現金購買黃金的方式把它變成黃金。(P8-2-3-2)

台灣黃金的價格跟越南黃金的價格，利潤大概會有 10%，所以他們又再賺一手，比如說他會用走私的方式，走到越南，所以黃金就出去了，在國外就變成現金了。(P9-1-3-2)

(4)購買不動產，將贓款漂白

受訪者 P2、P8 指出，詐欺集團的車手或水房在收到被害人交付的大筆現金後，即指派犯罪成員攜帶這些現金，以一次付清的方式購買不動產，以隱匿犯罪所得，使得警察機關難以透過追查金流方式偵知詐欺集團的犯罪所得。

房地產也有一部分是他們轉投資。(P2-2-3-3)

用現金去買不動產，一次把他付清。(P8-2-3-2)

(5)購買藝術品或投資（購買）高價商品

受訪者 P2 指出，詐欺集團會利用被害人交付的大筆現金，購買高價藝術品或奢侈品，以隱匿犯罪所得，使得警察機關難以透過追查金流方式偵知詐欺集團的犯罪所得。

買高檔的字畫古董跟超跑。(P2-2-3-3)

(二) 脫免逮捕

綜合多數受訪者意見指出，電信網路假投資詐欺集團在資通訊、金流工具沒有落實管制情況下，利用資(通)訊科技設備及方法以分散犯罪地點並隱身境外實行犯罪，並在當地國刻意保護包庇下使得警方查緝無門，即便當地國意配合查緝，亦因雙方法制與司法管轄主張不一，且偵查技術及相關設備存在落差，導致調查取證與案件聯結有相當困難度，在缺乏完備犯罪事證情況下，難以溯源緝獲幕後主嫌。

主要像機房成員就是躲在國外啊。(P5-2-3-2)

用人頭電話跟人頭金融帳戶或者是 vpn 其實這 3 個都是為了要規避查緝。(P6-2-3-3)

就是有很多的斷點，就是他們會車手，收水，水房的斷點會作的很多層。(P7-2-3-2)

如果是透過網路的話，他會透過 VPN 跳板會隱藏真實上網的 IP…跑去這些立場比較不願意跟

我國合作執法的，這些什麼柬埔寨、緬甸的國家。(P8-2-3-3)

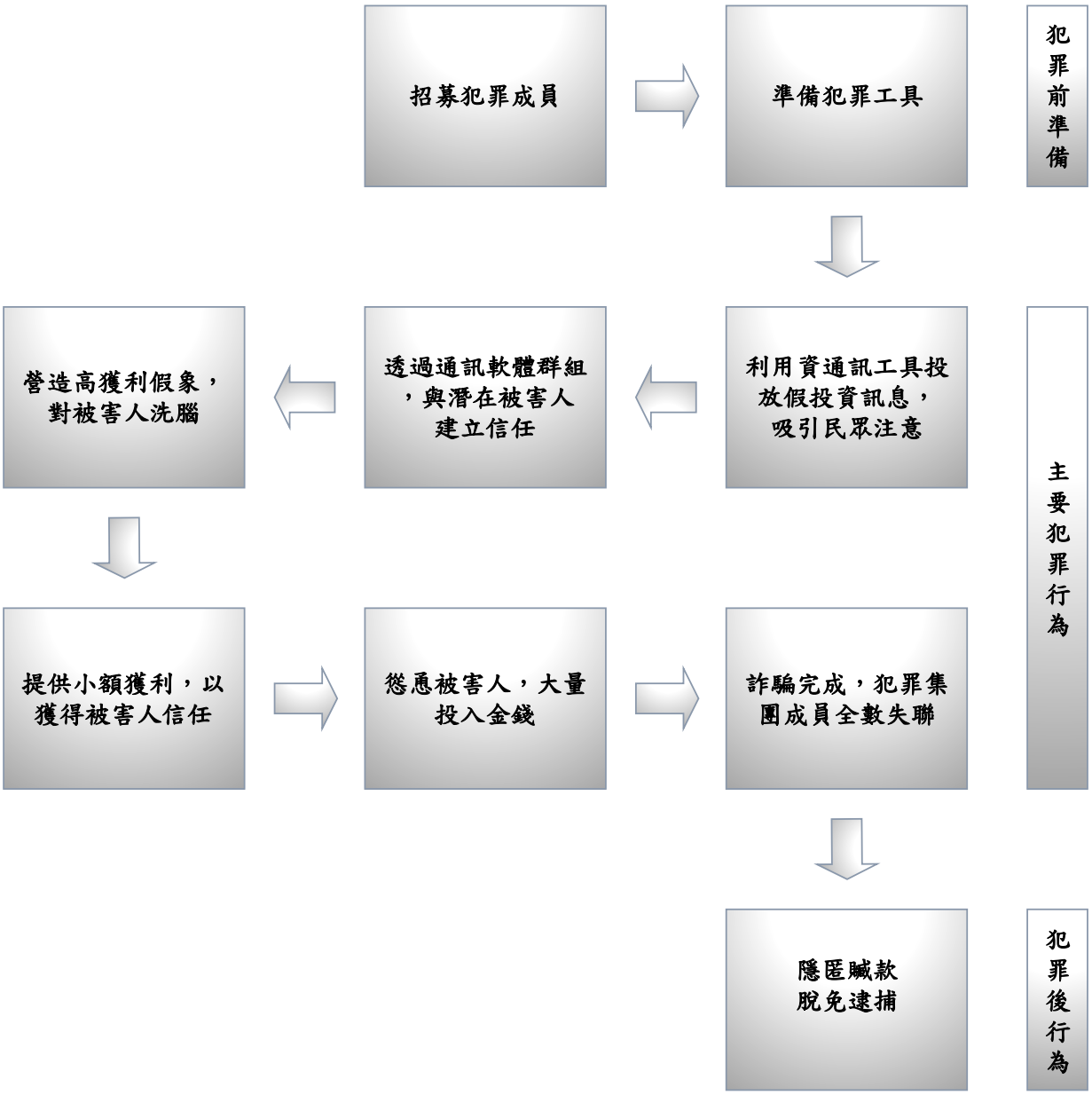


圖 4-1 電信網路假投資詐欺犯罪腳本流程

資料來源：本研究自繪。

第三節 防制電信網路假投資詐欺犯罪面臨的困境與對策

為深入分析臺灣防制電信網路假投資詐欺犯罪之執行困境與改進方向，本研究依據打詐綱領 2.0 所揭示架構，從打詐五面向出發，檢視政策執行現況與制度落差。透過受訪者意見歸納各面向之主要問題與建議對策，期能建構具體可行之防制策略，以作為未來警政及跨部會修正防詐政策之參考，達成提升全民防詐意識、減少詐欺案件與降低財損之政策目標。

一、識詐面向的困境與解決的對策

在電信「識詐」（宣導教育面）由內政部統籌並結合警政、教育、金融及數位管理等跨部會力量，推動分層、分眾、分齡的犯罪預防宣導工作，透過校園教育、社群媒體宣導、社區講座及公私合作機制，培養青少年正確法治觀念與民眾防詐識能，期能厚植社會整體防詐免疫力。根據官方統計顯示，防詐宣導活動雖已累計觸及人次已逾四億，顯示政府在識詐政策推動上已具廣泛影響力。然而，詐欺犯罪受害情形卻仍未顯著減少，2024 年 1 月至 11 月間，23 歲以下被害人即達 2 萬 851 人，占總被害人數 18.9%，突顯青少年族群在識詐教育面仍有缺漏(行政院，2024)。為強化此一不足，打詐行動綱領 2.0 進一步提出分齡分眾識詐策略，並推動金融機構關懷提問與即時攔阻措施、強化網路推播與多元宣導觸及、建立正確法治觀念及跨部會合作模式。希能提升全民辨識詐欺風險之能力，並透過警銀及民間合作網絡，形塑全民共同防詐的社會氛圍，奠定防制電信網路詐欺犯罪之基礎工程。

(一)面臨的困境

「識詐」面向由內政部統籌跨部會推動多元宣導。然而，實務執行仍面臨宣導成效有限與受眾落差等困境。現行宣導多偏重量的擴散，欠缺質的滲透，導致民眾雖普遍接觸防詐資訊，卻未能內化為具體行動。再者，宣導疲勞與樂觀偏誤等心理因素，使部分民眾對詐欺風險產生輕忽或抗拒，降低識詐成效。此外，分眾精準化不足、媒介使用與族群特性不符，以及高風險族群（如高齡者、青少年）難以有效觸及，亦限制政策實效。整體而言，雖識詐體系已具規模，但在訊息傳遞深度、行為轉化與社會滲透層面仍存落差，亟需提升策略精準度與教育連貫性，以強化全民防詐免疫力。依據本研究訪談分析資料顯示，臺灣識詐工作面臨宣導成效有限與民眾防詐意識落差；宣導內容形式化且精準化不足；宣導疲勞與樂觀偏誤心理；高風險族群難觸及與情境斷層等困境

1.宣導成效有限與民眾防詐意識落差

在電信網路詐欺防制體系中，「識詐」屬於最前端的防線，其核心目標在於促進民眾具備辨識與拒絕詐欺的能力。此面向屬於犯罪預防政策中之「初級預防」（primary prevention），強調透過教育與宣導降低潛在被害風險。然而，臺灣現行識詐宣導雖覆蓋廣泛，卻普遍存在民眾參與度低、記憶不足、實際行為改變有限等問題。宣導多偏重短期曝光效果，缺乏系統性追蹤與成效評估，使得民眾雖「看過」相關資訊，卻未必能

「記得」或「相信」。此外，民眾對詐欺風險的主觀評估往往低於實際威脅，導致防詐知能無法轉化為行動，呈現出知識與行為落差」的現象。如受訪者 P1 指出，多數人對防詐資訊的接受度取決於個人興趣與生活習慣，願意主動了解的群體僅限於部分警覺性高者。受訪者 P6 表示，民眾對防詐訊息缺乏興趣與信任，導致宣導資訊未能形成持久印象；即使政府持續宣導，仍有大量民眾不知道 165 反詐專線的存在。另有受訪者 P7 認為，會被詐欺的民眾往往未接觸過防詐宣導，說明現行識詐機制在受眾觸及上仍有明顯不足，由上可知，雖然政府各機關已透過多種媒體與場合積極推動防詐宣導，但民眾的防詐意識提升有限。

識詐的問題，我覺得受眾會聽的還是會聽，不會聽的還是不會聽。(P1-4-1)
警察一直在作識詐宣導，但民眾幾乎不會去看那些廣告，甚至還不知道 165。(P6-4-1)
宣導效果有限，因為會被騙的人，他們就是沒有看到警察在宣導。(P7-4-1)

2.宣導內容形式化且精準化不足

防詐宣導的關鍵在於精準傳遞與受眾對位，若宣導活動僅著重形式或曝光次數，則無法促進實質行為改變，所謂精準宣導應以不同族群的風險特性、媒介使用習慣與資訊接收行為為基礎，進行策略設計。然而，實務上多以一次性活動、廣告投放或名人代言作為主要手段，缺乏科學化的受眾分析與差異化內容，導致政策成效有限。政府雖以打詐行動綱領 2.0 為藍圖推動識詐，但因行政資源分散、執行標準不一，使識詐活動仍停留在徒具宣導形式、但卻無實益，造成民眾無感。誠如受訪者 P2 認為，精準宣導多淪為口號，缺乏科學分析的具體執行模式，當前真實狀況是政府宣導機關找明星、網紅、球員等名人擔任宣導主角，但這些名人與受眾並無沒有任何連結，而無法達到宣導效果。受訪者 P3 則補充，識詐應如同防疫教育，需全面滲透至生活各面向，但目前仍停留於廣告性推播階段。另有受訪者 B1 指出，不同世代對媒介的依附度差異極大，若仍以單一形式進行宣導，目前的宣導模式難以涵蓋中老年族群或偏鄉民眾，由此可見政府並未針對目標受眾作為導向，採取不同策略與方式導致宣導成效不佳。綜上分析，可知現行識詐宣導的策略性不足與內容形式化，導致其難以達到政策目標。

綱領 2.0 的核心是作精準宣導，但是精準宣導只是 1 個口號，真實的狀況是我們找了明星、網紅、球員，跟投放的受眾沒有任何的連結。(P2-4-1)
識詐的問題在於我們的客群…應該像疫情宣導這樣。(P3-4-1)
中老年人這 1 塊的訊息，我覺得他們的訊息的接收程度，就不會像年輕人這麼高。(B1-4-1)

3.宣導疲勞與樂觀偏誤心理

在社會心理層面上，宣導疲勞與樂觀偏誤構成識詐教育的重要障礙，當相同內容重複出現而缺乏變化時，民眾容易產生心理抗拒與麻木反應，導致防詐訊息被視為社會環境背景噪音而忽略。另一方面，樂觀偏誤則使個人高估自身免疫力，認為詐欺不會發生在自己身上，此種認知偏差削弱了防詐宣導的警示功能，使政策推動陷入資訊傳遞充分但警覺不足的困境。受訪者 P4 指出，電視、銀行、網路等皆大量充斥防詐口號，卻引發反效果，形成宣導疲勞；加上，多數民眾普遍存在樂觀偏誤心理，對詐欺風險持輕視態度，認為受害者都是不夠聰明才會上當。受訪者 P5 表示，防詐內容未能融入生活脈絡與情境，使宣導缺乏臨場感與真實性，難以喚起情緒共鳴，導致識詐政策的潛在成效

大幅折損。綜上分析，識詐宣導雖頻繁出現於生活空間，但因內容過於雷同，民眾逐漸失去注意力。

到處都是防詐標語，民眾已經看到麻木了，更嚴重的是樂觀偏誤，每個人都覺得自己很聰明，那種騙術只能騙到老人家或笨蛋。(P4-4-1)

識詐的話，坦白講就是現在有點宣導疲乏了，我們宣導沒有到位，沒有符合情境。(P5-4-1)

4.高風險族群難觸及與情境斷層

識詐政策若無法接觸到高風險族群，即使宣導量再大，也難以有效預防犯罪，電信網路假投資詐欺受害高風險族群包括長期使用社群媒體、從事高風險投資或孤立社會關係者，這些族群常被詐欺集團鎖定，並藉由封閉式社群（如假投資群組、情感詐欺聊天室）建立信任關係，使官方防詐訊息難以滲透，當識詐內容與實際詐欺情境脫節，被害人更難辨識風險。受訪者 P4 即指出，假投資詐欺被害人多沉浸於詐欺集團事先創建為數十人至百人的封閉式虛假理財通訊群組，外部警示難以進入，被害民眾往往將詐欺者視為「熟人」或「知己」，使政府宣導內容所稱「不要點擊不明連結」、「不要聽信陌生人」顯得與自身無關，導致情境斷層問題愈趨嚴重。受訪者 P9 則指出，警方即使掌握潛在被害者，也難以主動介入，既受限於人力，又受限於法律責任。綜上分析，識詐政策在觸及高風險族群方面存在明顯瓶頸。

那些真正高風險的被害人，他們正沉浸在封閉的 LINE 投資群組裡…我們的聲音，根本進不去那個同溫層…那個連結不是「不明連結」，而是「知己」分享給他、要帶他賺大錢的內部管道。(P4-4-1)

警察找不到那些潛在被害人…你可能會被她告，會被他罵，所以要有極度的耐心跟時間。(P9-4-1)

(二)解決的對策

本研究綜整受訪者意見建議，臺灣識詐工作應採取分眾分齡宣導策略與精準傳播；跨平台合作與多元宣導管道整合；社區基層宣導與教育紮根化；AI 預警與大數據識詐機制建構等對策解決。

1.分眾分齡策略與精準傳播

為提升識詐政策效能，應導入分齡、分眾與行為導向的策略，政府可依據年齡層、教育程度及媒介偏好建立多層宣導架構，針對青少年、上班族與銀髮族分別設計語言與內容，青少年應以互動式網路宣導為主，中壯年可結合企業教育與理財課程，高齡族群則以社區講座、地方媒體為重。唯有透過精準傳播，方能提升識詐宣導之滲透率與信服力，受訪者 P5 指出，情境式宣導能讓民眾更感同身受，也會更容易理解詐欺的實際手法。受訪者 P6 主張，應根據不同場合及平台，採取不同的方式，投放合適的宣導內容；另有受訪者 B1 建議，針對特定網頁或關鍵字設置即時警示視窗，可在關鍵行為發生前即進行介入，避免民眾誤觸陷阱。綜合上述分析可知，識詐宣導需以分眾化策略為核心。

我覺得情境式的宣導會比較有用。(P5-5-1)

針對不同的場合及平台的受眾，投其所好放他們喜歡的東西。(P6-5-1)

點開特定的視窗之後，我們會跳出特定的視窗，這種感覺是比較有效的。(B1-5-1)

2.跨平台合作與多元宣導管道整合

隨媒體生態快速轉變，政府部門需與民間媒體、企業及社群網路建立合作機制。多元管道的合作能擴大宣導範圍並提升觸及率。傳統媒體可鞏固中老年群體，網紅與 YouTuber 則能有效接觸年輕族群，而企業內部訓練可延伸至職場教育，形成防詐網絡。受訪者 P3 認為，應結合網紅與地方媒體進行置入式行銷宣導，以自然語言傳遞防詐訊息。受訪者 P4 建議，政府可與企業合作將防詐教育納入內部訓練，並透過財經節目或 Podcast 進行潛移默化的宣導，對於退休人員及老年人，則採用電視、廣播等傳統媒體和社區活動及廟會文化等活動等實體接觸管道，以跨平台整合兼顧不同世代與媒介偏好，使識詐宣導更具滲透性。

有些網紅是比較 Local 甚至低俗，但我覺得不能忽略他們，我們要置入化行銷。(P3-5-1)

中年上班族是假投資詐欺的最大受害者，應該與大型企業合作，將防詐課程納入員工內訓或資安教育的一部分，對退休銀髮族，傳統媒體和實體社群依然是最好的管道。(P4-5-1)

3.社區基層宣導與教育紮根化

防詐教育若要長期發揮效益，必須結合社區力量，建立地方化、常態化的宣導模式，地方基層具有社會信任基礎與穩定人脈，能作為識詐政策的前哨，透過社區志工、里長及長青學苑講座推動防詐教育，可讓防詐概念滲入日常生活，逐步形成社會防護網。受訪者 P4 認為，社區志工與里長最能與在地居民建立互信，應透過訓練使其成為識詐種子，同時地方政府應將識詐教育納入社區安全計畫，結合民政、警政及教育單位共同執行，確保政策能深耕基層並長期持續。

要培訓里長、社區志工成為防詐種子，用他們聽得懂的語言，面對面地溝通。(P4-5-1)

4.AI 預警與大數據識詐機制建構

為克服宣導反應時間過長與內容更新落後之問題，應運用 AI 與大數據技術建立即時識詐機制，透過對報案資料、網路對話與詐欺網站關鍵字進行分析，可快速掌握詐欺新趨勢，再配合自動化警示推播，主動提醒潛在受害者，將被動宣導轉為主動防護。受訪者 P4 指出，整合 165 報案大數據並導入 AI 分析，可迅速辨識新型詐欺話術與釣魚網站樣態，當系統偵測到異常訊息時，能即時透過電信業者或社群平台推送警示，強化即時防護，此舉不僅提升政策反應速度，也能有效補足人工宣導之不足。

整合 165 報案大數據，利用 AI 去分析、標記最新的詐欺話術…發展『詐欺劇本 AI 快篩與即時預警系統』。(P4-5-1)

二、堵詐面向的困境與解決對策

「堵詐」(電信服務面）由國家通訊傳播委員會（NCC）擔任統籌機關，主要任務在於防杜境外詐欺來話、遏止人頭門號濫用、攔阻惡意簡訊傳播，並強化電信業者對涉詐網域及網址之聯防機制，以確保電信服務不被詐欺集團利用。此一政策旨在透過完善電信事業管理措施，建立多層防線以截堵詐欺訊息流通，維護國內通信環境之安全與信賴。然而，實務上仍面臨諸多挑戰。檢警調機關多次查獲詐欺集團利用境外電信事業門號（俗稱「黑莓卡」）及國際漫遊服務進行詐欺，導致通聯來源難以追查，形成執法斷

點。此外，部分不法人士透過大量申辦或收購人頭門號從事詐欺活動，增加電信管理難度，亦暴露現行法規及查核機制之不足。面對此一態勢，堵詐政策除須持續強化電信門號實名制及跨境技術聯防外，亦需結合司法互助與跨部會合作，以整合電信監理、執法偵查與國際協調能量，建立更具韌性與即時性的電信防詐管理架構，作為防制電信網路詐欺犯罪的第二道防線。

(一)面臨的困境

在「堵詐」面向上主要透過遏止人頭門號、攔阻惡意簡訊及強化電信業者對涉詐網域與網址之聯防機制，以防杜電信服務遭詐欺集團濫用，並削弱犯罪者與被害人之接觸途徑。然而，在實務執行層面卻面臨電信監理權限與通訊自由之間存在法理衝突，跨境匿名詐欺來電普遍利用 VOIP、VPN 及境外主機轉接技術，導致攔阻與溯源困難，形成執法與追查斷點。此外，人頭門號氾濫與企業簡訊遭濫用問題嚴重，詐欺集團得以藉此偽裝合法通信身分持續行騙；而部分平台及電信業者反應遲緩、聯防合作不足，進一步削弱即時防堵與執法威懾效果等多重挑戰。歸納分析受訪者意見發現，臺灣堵詐工作面臨電信監管機關權限與通訊言論自由的衝突；跨境匿名詐欺來電，攔阻與阻斷均屬困難；人頭門號氾濫，企業簡訊遭濫用；平台業者回應速度緩慢，缺乏即時聯防與執法威懾力弱等困境。

1.電信監管機關權限與通訊言論自由的衝突

NCC 與相關單位因須尊重民眾通訊祕密與言論自由等憲法賦予基本權利，不得任意全面封鎖「無來電顯示」或廣泛監控電話及簡訊，導致防堵措施在法律與人權考量下受限，執行常處於被動。受訪者 P1、P5 即表示，目前「無來電顯示」的來電中，涉詐比例相當高，因此有人建議是否可全面阻斷此類來電。然而，國家通訊傳播委員會（NCC）表示，此作法將涉及侵犯民眾「秘密通訊自由」的問題，依法不可行。事實上，在詐欺行為尚處於「犯罪著手」階段時，若採取過度阻斷或監控措施，確實可能干預人民的言論與通訊自由。換言之，在防制詐欺與保障基本權利之間，仍存在執行上的界線與兩難。受訪者 P5 更進一步指出，雖然現行法規已提供防制依據，但在實務執行上仍遭遇詐欺集團的規避策略。詐團常針對既有的過濾與攔截機制刻意變通，例如在簡訊或網路廣告中拆字、加空格、置換同音字，或以符號取代關鍵字，導致傳統的關鍵字比對機制難以有效偵測。若監管機關為強化辨識與封鎖此類變形文字而採取更廣泛的技術性管制措施，則可能產生干預民眾秘密通訊自由的疑慮，顯示防詐與保障基本權利之間存在制度性平衡的挑戰。

沒有來話顯示的來電，涉詐的比例很高，你能不能阻斷所有沒有來話顯示的來電？…NCC 告訴我們不行，因為會違反秘密通訊的自由。(P1-4-2)

他只是在犯罪著手，你做太多還是會干預到言論自由。(P5-4-2)

他還是會根據我們防堵的，像那個簡訊啊，他有一些關鍵字還是什麼，他會去閃啊。(P5-4-2)

2.跨境匿名詐欺來電，攔阻與阻斷均屬困難

詐欺集團利用 VOIP、VPN、境外主機與頻繁變更號碼等技術，造成號碼偽造與來源 IP 位址飄忽不定，致使國內執法單位難以追蹤源頭；如欲從技術源頭進行攔截，包

括電話、簡訊，將會非常依賴跟跨國（境）電信商的合作，但由於跨國合作與司法互助程序繁瑣，經常造成警察機關偵查詐欺犯罪的斷點。受訪者 P4、G2 認為，詐欺機房設於柬埔寨、網站伺服器位於歐洲、網域名稱在巴拿馬註冊；犯罪集團以 VOIP 撥打電話、任意變換號碼，並透過 VPN 上網使 IP 位址飄忽不定。由於我國缺乏與這些跨境電信業者的合作管道，導致警察偵查時如同被綁住手腳，難以攻及境外犯罪核心。

犯罪的跨境與匿名性，是所有問題的根源。(P4-4-2)
我們缺乏與這些跨境電信業者合作的方式(G2-4-2)

受訪者 P9 也說，詐欺集團運用國外通訊軟體的匿名性與跨境特性，將其利用作為電信與網路詐欺的媒介，造成偵查人員一旦遇到此類通訊工具，常難以追溯來源或還原內容，顯著增加偵查與取證的困難。

黑莓的 APP，還有 RS，很多啦，都是沒辦法破解，我們抓很多，科偵只要遇到這種的沒辦法破解，沒辦法還原。(P9-4-2)

3.人頭門號氾濫，企業簡訊遭濫用

儘管我國已實施電信門號實名制，詐欺集團仍利用假證件、透過外籍移工代辦或直接收購人頭門號，並以合法外觀的「企業簡訊」服務散布釣魚訊息；由於來源看似正常，電信業者難以即時辨識與攔截。此外，偽造門號與假門號大量流竄、頻繁換號，以及非實名的預付卡或漫遊卡等存在，使得現行以黑名單為主的攔截機制效果受限，成為防堵漏洞。綜合受訪者 P4、P9、G2 意見指出，目前人頭門號氾濫，更麻煩的是，詐欺集團經常租用合法的「企業簡訊」服務發送釣魚訊息；因來源呈現為合法企業，電信業者難以在第一時間攔截。再加上境外門號數量龐大、假門號與偽門號大量流竄，還有頻繁換號問題，以及非實名預付卡（如黑莓卡）等存在，致使黑名單與既有攔截機制效果受限，查證與資料更新速度亟待加強。

他們現在會租用合法的「企業簡訊」服務，發送釣魚簡訊。因為來源是合法的企業，我們的電信商很難在第一時間攔截。(P4-4-2)
現在的人頭電話太多了，還有境外的門號也很多。(P9-4-2)
假門號和偽門號大量的流竄，還有頻繁的換號的問題，還有像黑莓卡那種非實名是的預付卡，導致我們這個黑名單的效果是有限(G2-4-2)

4.平台業者回應速度緩慢，缺乏即時聯防與執法威懾力弱

詐欺網站及社群帳號之下架處理常有延滯，無法在短時間內切斷犯罪鏈路。跨機關與業者間之資訊共享機制不完備，黑名單更新亦欠缺即時性，進一步削弱偵防與攔截成效。此外，現行對業者之罰鍰標準偏低，難以發揮實質嚇阻效果，綜合造成防堵機制無法形成具有強制力與時效性的聯防體系。綜合多位受訪者觀點，認為主管機關應落實預防導向之安全管理與業者聯防機制，與其他國家相比，我國在即時聯防與業者回應速度上仍有落後，業者多處於被動回應，造成警政單位與業者之間形成「與時間賽跑」的局面，常在警察機關發現詐欺網站或社群帳號後，通報業者的處理時效快則一、二日，慢則一至二週，甚至無回應，致使停話、下架與停權等措施無法及時切斷犯罪鏈路，政府雖強調要從源頭著手，但若主管機關（例如 NCC）未能加速作為並強化執法與協調能

力，防制成效難以顯現。另現行裁罰金額相對偏低，對業者缺乏實質嚇阻力，需檢討法制與處罰工具，以促使業者主動強化防護與即時回應。

我覺得目前來講，我們跟其他國家比起來，我們是落後的，業者都是處於被動。(P3-4-2)

發現一個詐欺網站或臉書粉絲專頁，通報給業者，他們的回應流程非常慢。快則一兩天，慢則一兩個禮拜，甚至石沉大海。(P4-4-2)

就是停斷話比如說，還有下架網站以及停權帳號的這 1 件事情，也是有時候速度不夠快，會緩不濟急。(P8-4-2)

這些錢對他們來講都是小錢啊，你裁罰只要五十萬，他怎麼會怕，他完全不會痛啦。(P6-4-2)

(二)解決的對策

本研究綜整受訪者意見建議，臺灣堵詐工作應檢討修法並強化主管機關權限；落實電信門號實名制與申辦數量管控；課予平台業者共同防堵義務與法律責任；強化攔阻技術並運用媒體公開揭露施壓等對策解決。

1.檢討修法並強化主管機關權限

受訪者普遍認為，現行法制尚有若干待檢討與修正之處，主管機關應落實事前安全管理並強化與業者之聯防機制。雖然國家通訊傳播委員會（NCC）已執行部分攔阻措施，然在實務操作上，對於停斷話務、網站下架及帳號停權等關鍵處置，其反應時效常顯不足，經常出現處置延緩、緩不濟急之情形，形成防詐的一大困境。

有一些法律要去檢討，要去滾修正。(P1-5-2)

主管機關要落實安全管理，要作期前的預防，包含跟業者之間的那個聯防。(P3-5-2)

政府一直說強調要從源頭著手，但是然需要主管機關 NCC 的全力支持，他們動作要加快才有辦法。(P8-5-2)

2.落實電信門號實名制與申辦數量管控

多位受訪者建議，應從源頭強化電信門號管理，對於國際漫遊卡之發卡端，若未落實實名制應予以即時停機，對於公司戶或業者大量申請門號的行為應施以管制與審查。具體措施包括限制每人可申請之門號數量、強化實名驗證程序與發卡審核標準，並設定開辦數量上限，以降低人頭門號濫用之風險。

要求國際漫遊卡的發卡端，如未落實實名制應該即時停斷話，同時對於公司戶大量申請電信門號的要作管制措施。(P2-5-2)

要控管每個人電信門號申請的數量，比如說最多 1 個人兩個門號應該就很多了吧，不需要到 3 個吧。(P8-5-2)。

可以強化門號的實名驗證機制，那並且限制這個開辦的數量。(G2-5-2)

此外，受訪者 G2 更進一步主張，應健全異常使用通報與處置政策，強化警民合作機制（例如透過 165 防詐專線加速攔阻可疑門號）、縮短跨單位資訊共享時差，並提升跨境查緝與司法互助能量。綜合而言，透過源頭管制、即時通報與加強國際合作，可提升門號可追溯性與攔截時效，進而抑制以門號為媒介之詐欺活動。

強化門號實名制與異常使用政策及警民合作，包含 165 阻斷可疑門號，縮短資訊共享時差，提升跨境查緝能力（G2-5-2)。

3.課予平台業者共同防堵義務與法律責任

任職於警政署刑事警察局，負責全國警察機關防制詐欺犯罪策略規劃及執行的受訪者 P4 主張，政府應由事後被動下架機制轉向對平台業者課予共同責任，將防制壓力由執法機關部分移轉至提供散布詐欺工具之業者。具體建議包括：於《打詐專法》或其子法明文規定社群平臺、搜尋引擎與電商平臺，對疑涉詐欺之廣告或帳號負有事前過濾及快速審核下架之義務；若因業者延誤或不作為致使民眾蒙受重大損失，應負連帶賠償責任並處以具有實質嚇阻效果之罰鍰。另建議對刊登「投資類型」廣告之廣告主實施「實名且實地」雙重驗證，以提高廣告投放成本與風險，從源頭提高詐欺集團之介入門檻，預期可促使業者主動強化審查機制並增進整體防詐成效。

從「被動下架」走向「課予平台業者共同責任」…必須將壓力轉移到提供犯罪工具的業者身上…在《打詐專法》或相關子法中明確規定，對於社群平台、搜尋引擎、電商平台上的詐欺廣告或帳號，業者負有「快速審核下架」與「事前過濾」的義務，若因其延誤或不作為導致民眾重大損失，應負擔連帶賠償責任。強制要求刊登「投資類型」廣告的廣告主，必須通過「實名且實地」的雙重驗證。增加犯罪集團投放廣告的成本與風險（P4-5-2）。

4.強化攔阻技術並運用媒體公開揭露施壓

受訪者 P4 提議，應自通訊基礎設施端強化預警與驗證機制：一方面全面要求電信事業對境外來電於接通前播放受話者語音警示（例如「此為國際來電，請注意詐欺」），作為各業者之標準配備；另一方面推動「官方簡訊專用簽章」制度，強制政府、金融與大型電商等機構之簡訊通過認證並在訊息開頭顯示不可仿冒之官方簽章，藉此提高民眾對訊息真偽之辨識能力。

全面強制「國際來電語音警示」…只要是境外透過電信或網路撥接進來的電話，接通前就先播放「此為國際電話，請注意詐欺」的語音，並推動「官方簡訊專用簽章」制度（SMS Branding），強制要求政府、金融、電商等機構發送的簡訊，必須通過認證，並在訊息開頭顯示無法被仿冒的官方簽章。(P4-5-2)

受訪者 P6 則強調，對於拒絕配合或回應遲緩之電信服務業者，應運用公開揭露與媒體報導形成輿論壓力，使其承擔社會責任並被動員納入聯防體系。

我覺得要讓媒體去渲染，說他們其實就是 1 個犯罪的溫床，讓這個民氣可用，讓民眾去抵制這樣的 1 個行為，我覺得會是更好的。(P6-5-2)

三、防詐面向的困境與解決的對策

「防詐」（數位經濟面）係我國打詐體系中「淨網路」的重要任務，由數位發展部統籌推動，旨在透過管理數位經濟產業與網路生態，防止詐欺集團濫用網路平臺及新興金融工具進行犯罪。其主要策略包括防制網路詐欺廣告、遏止詐欺網站連結、建立政府專屬短碼簡訊發送機制、強化電商業者資安維護，以及防堵第三方支付與網路遊戲點數成為詐欺洗錢工具等。此一作為意在構築安全可信的數位環境，保障民眾於線上消費與社交活動中的資訊安全與財產權益。政府近年亦修正《證券投資信託及顧問法》，針對網路投資廣告明定移除義務與法律責任，以遏止虛假投資資訊氾濫。然而，詐欺集團隨之調整策略，持續以多重帳號與境外伺服器散布詐欺廣告，使網路平臺防制難度升高。

實務上，Meta 及 Google 等國際社群媒體仍為詐欺廣告主要來源，據警政署刑事警察局分析顯示，2024 年 7 月投資詐欺案件中，被害人接觸詐欺內容之管道以 Meta 廣告占 97.9%居首，其次為 Google 廣告 2.1%；被害人多於點擊廣告後，透過 LINE 通訊軟體遭誘導加入投資群組，占比高達 79.8%(行政院，2024)。此現象顯示，數位經濟之便利亦成為詐欺滲透的重要媒介，凸顯防詐策略須強化跨平臺合作與網路內容監理，以有效構築全民數位防詐防線。

(一)面臨的困境

在「防詐」面向之推動過程中，業者基於商業利益考量，對政府防詐要求多持消極態度，並常以法律授權不足、言論自由及用戶隱私為由，拒絕強化廣告審查與涉詐帳號管理，而現行罰則過輕亦難形成嚇阻效果，阻礙公私協力防詐的成效。由於防詐工作涉及多部會權責，但存有資訊整合與協調機制不足，權責重疊與資源分配不均問題，多數機關並將防詐責任歸於警察體系，而忽略平臺與金流源頭管理的重要性，加上業者對涉詐帳號停權及廣告移除多採被動應對，執行落差嚴重，國際平臺未在臺灣實質落地，多以境外法令與隱私保護為由拒絕調查配合，更使執法與取證受限。整體而言，法規約束力不足與平臺責任不明確，已成我國數位防詐體系亟待突破的核心瓶頸。依據本研究訪談分析資料顯示，臺灣防詐工作面臨，數位經濟業者防詐責任與商業利益衝突；跨部會合作失衡與防制困境；涉詐帳號停權與執行機制不落實；國際合作與境外數位金融監理缺口等困境

1.數位經濟業者防詐責任與商業利益衝突

民間數位經濟業者面對政府要求協助防詐，在商業利益考量下，多以法律規範不足為理由，對自家平台播放之廣告審查與內容監管多採消極態度，並常以言論自由與用戶隱私為由加以抵制，對於業者的不配合作為，現行相關罰則又過輕，難以形成嚇阻效果，是造成公私協力防詐成效不張之主因。受訪者 P4 指出，平台業者必須兼顧營運成本、用戶隱私（個資法）與自身商業模式，若政府要求其落實更嚴格的廣告刊登與內容審查，業者往往以影響營收為由而持保留態度，在缺乏強制性法律規範的情況下，公私協力的實質效能受到明顯限制。

民間企業，要考慮成本、用戶隱私（個資法）、以及商業模式。我們要求平台業者落實更嚴格的廣告刊登審查，他們會說這影響營收…在法律沒有強制規定的情況下，這種「協力」的力道就大打折扣。(P4-4-3)

受訪者 P5 並進一步說明，目前社群媒體與通訊軟體多屬缺乏監管者的數位環境。以 Facebook 為例，平台經常以言論自由為由抵制外部監督；LINE 亦主張其屬於私密聯繫空間，無從辨識詐欺訊息內容；而 Google 與 YouTube 則認為廣告或推播內容屬於使用者原創，非平台責任範疇，此種以自由與私領域為由的消極態度，使防詐措施難以落實。

臉書就是 1 個沒有監控者的環境，你去監控他還會說你箝制言論自由…Line 上面的詐欺也很多，他也不管，也是說言論自由，是私密聯繫，業者說我怎麼知道他在講詐欺，還有 google 廣告，還有 youtube 推播廣告，他說那也是原創內容啊，你不能叫我管啊。(P5-4-3)

此外，現行罰則過輕亦削弱嚇阻效果。受訪者 P6 指出，若僅處以五十萬元罰鍰，對仰賴廣告收益的國際平台而言，幾乎無實質影響，使得業者在衡量商業利益與合規成本後，多採取僅在形式上遵循，或以消極的態度應對。

你裁罰只要五十萬，他怎麼會怕，他們就是以廣告維生的啊，顯不相當啊，是他完全不會痛啦。(P6-4-3)

受訪者 P3、B1、G3 認為，唯有透過法律明確規定違法廣告的下架標準，並提高罰則金額，使其經濟損失顯著，方能促使業者主動強化內容審查與防詐管理機制。然而，目前平台多僅依自家政策進行內部規範，欠缺一致性與強制力，導致防詐合作的制度化基礎仍然薄弱。

除非法令要求我，不然我原則上是消極對抗，我覺得是他們是這種態度。(P3-4-3)

他們的收益是來自廣告，對他們來講，他們要衡量這件事情的平衡點，你要跟我很明確講是什麼，我才有可能撤下來(B1-4-3)

Meta 有花心力，可是他們應該可以作得更好，我的直覺是他們可以作的更好，但就是沒有(G3-4-3)

2.跨部會合作失衡與防詐策略困境

防制詐欺涉及多個部會權責，但實務運作上卻有跨部會資訊整合與協調機制不足，權責重疊與資源分配不均問題，更嚴重的是各部會大多認為打擊詐欺犯罪是警察機關的責任，其他各部會僅是配合執行，而忽略犯罪源頭管理才是打詐成功的關鍵因素。任職於警政署刑事警察局，負責全國警察機關防制詐欺犯罪策略規劃及執行的受訪者 P4 指出，防詐體系涉及內政部（警政署）、金管會、國家通訊傳播委員會（NCC）、法務部及數位發展部等多個主管機關，但各單位皆依自身法規、權責與行政優先順序行事，缺乏統一協調機制。雖然跨部會會議上各機關皆表達合作意願，但回到部門執行階段，往往因權責不明與程序僵化而難以落實。

涉及內政部（警政署）、金管會（銀行）、NCC（電信）、法務部、數位發展部等…開會時大家都說要合作，但回到各自的單位，執行起來就困難重重。(P4-4-3)

受訪者 P4 更進一步形容，警察常處於孤軍奮戰的狀態，必須在犯罪已發生後進行追查與補救，卻難以從源頭預防，犯罪的根源多位於網路、電信與金融體系上游，而相關單位若未能及時控管，將導致詐欺活動不斷重複，受訪者無奈的以「我們在下游拼命清垃圾，但上游傾倒垃圾的源頭如果管不住，垃圾是永遠清不完的」比喻現況，凸顯警察部門在防詐體系中長期面臨的結構性困境與執行壓力。

警察在第一線拚命，常感覺像孤軍奮戰…但犯罪的源頭在網路、在電信、在金融，我們常自嘲，我們是在下游拼命清垃圾，但上游傾倒垃圾的源頭如果管不住，垃圾是永遠清不完的。(P4-4-3)

3.涉詐帳號停權與執行機制不落實

數位經濟業者對自家平台帳號管理與涉詐廣告審查的落實程度，與防詐措施是否有效至關重要，然而業者仍有被動應對及對涉詐帳號停權未落實之情況，導致防詐成效受限，亦反映涉詐帳號停權執行落差與防詐機制的缺陷。**受訪者 P1 指出**，即使同一帳號

所投放的詐欺廣告已被下架，該帳號仍能繼續投放其他廣告，其中部分內容依然涉及詐欺，顯示帳號停權制度未落實執行。

對於相同的帳號投放的廣告下架之後，這個帳號還能夠投其他的詐欺廣告，等於這個帳號的停權執行不落實(P1-4-3)

受訪者 P1 進一步表示，現行主管機關對於違規平台缺乏積極處理態度與有效罰則。受訪者 P9 以 Facebook 為例指出，業者往往採被動式應對，僅在接獲警方通報或民眾檢舉後才進行下架處理。受訪者 G3 也說，數位經濟業者雖聲稱每日篩檢數萬則疑似詐欺訊息，但數位部仍能在平台上持續發現大量詐欺廣告，顯示篩檢與刪除機制流於形式，未能發揮實質防制效果。

希望主管機關希望能夠很積極、快速的，對於不遵守規定的平台業者能夠處罰(P1-4-3)
FB 應該是說他們現在都是被動式的，我們警察怎麼講，他們才這麼做，沒有人檢舉他們不理啊。(P9-4-3)
他們的官方說，他們每天都篩了好幾萬個詐欺訊息，他們篩完之後，數發部自己去他們的平台又篩了很多個(G3-4-3)

另外，受訪者 P5 告訴研究者，他們僅靠 3 名員警在兩年間即協助下架約十九萬則詐欺廣告，但詐欺訊息仍層出不窮，形成愈刪愈多的惡性循環。受訪者 G3 則表示，詐團更持續利用技術手段規避監測，例如在偽冒名人廣告中故意於姓名間插入空格（如「黃 空一格 仁 空一格 勳」），藉此逃避關鍵字偵測，顯示詐團具備高度技術適應性，能快速調整策略以突破平台防線，使警方與平台始終處於被動防禦的狀態。

我們就 3 個人喔，弄兩年下架了十九萬個廣告，但是還是會看到廣告啊。(P5-4-3)
我們原本很直接想說黃仁勳 3 個字連在一起，他就給他空 1 格空 1 格，所以詐團也是很聰明，一直在變啊(G3-4-3)

4.國際合作與境外數位金融監理缺口

在全球化數位環境下，國際數位平台如 Google、Facebook、LINE 等業者均未確實在臺灣落地，並多以境外法令與隱私保護為由，拒絕配合政府調查或資料調取，使得執法與取證困難，造成我國防制詐欺執法顯著阻礙。另外，現行法規約束力不足，使平台責任難以落實，亦使金流與資訊監管產生漏洞。受訪者 P3 及 G3 指出，Facebook（Meta）對臺灣詐欺議題態度消極，國內現行法令對其要求薄弱，難以促使其在臺投資或承擔相應的安全管理成本。LINE 則以公司設於日本、伺服器在海外為由，主張通訊秘密與外國法適用，對臺灣執法單位提出的數據請求多有保留，致使刑事警察偵查人員與數位發展部在取得關鍵資料時屢屢受限。

臉書在臺灣的安全管理沒有投資…臉書對於臺灣詐欺情況是不重視的，我們的國家法令，對於臉書的要求是薄弱的…Line 的態度就是說，我們是日本公司，伺服器在日本，你要調這些隱私資料…希望你們依照日本法來跟我們申請(P3-4-3)
刑事局跟數發部要求 Line 配合，依我們的打詐專法提供資料，他們說這是通訊秘密…要受限於資訊協議保護。(G3-4-3)

受訪者 P5 及 B1 均指出，現行「打詐專法」雖要求平台設置法律代表人，但該規定在實務上缺乏可執行之法律責任，未能形成有效的制度約束。

臉書跟 Google 都是富可敵國…那你要他落地納管配合，我認為最困難的是在這邊(P5-4-3)

打詐專法是只有要求他們要設立法律代表人，但老實說那是沒有法律責任的…他們的論述都是我們是外國企業，我們可能依據我們自己的平台規範，或者是我們跟主管機關配合。(B1-4-3)

受訪者 B1 及 G3 更進一步說明，目前大型國際平台普遍未在臺設立實質營運或受監管機構，使政府在尋求合作時多處於「請求」而非「命令」的地位；相較於歐盟趨向要求平台承擔更多責任，國內管理仍難以強制業者履責。

目前比較前四大的社群平台都是沒有落地的，變成比較像是政府尋求他的合作和配合，而不是要求他來配合政府(B1-4-3)

過去網路廣告平臺業者認為自己只是中介，提供網路買賣空間與社群聊天室，不該負擔這麼多責任，但歐盟都要求平臺業者負起更多責任。(G3-4-3)

此外，受訪者 P8 反映出虛擬通貨與境外幣商構成重要的金流遮蔽點，詐團透過境外交易所購買或轉移虛擬通貨，導致我方在追查資金流向與調取交易資料時面臨重大障礙。

這些詐團的成員他們都是到境外的幣商那邊購買，購買虛擬貨幣，然後你就調不到資料，我們警察就調不到資料（P8-4-3）

(二)解決的對策

本研究綜整受訪者意見建議，臺灣防詐工作應強化法制約束與落實罰則執行；落實企業社會責任與前端風險控管；建構常設指揮體系與跨部會資訊整合平台；深化 AI 防詐技術與強化國際監理合作等對策解決。

1.強化法制約束與落實罰則執行

多位受訪者指出，現行法規對數位經濟業者的約束力不足，導致防詐規範難以落實，加上處罰金額過低，對高營收的跨國平台並無嚇阻效果，因此。建議政府應修訂相關法令，明確規範網路廣告平臺業者防詐義務，並提高罰款金額，以建立具實質約束力的裁罰機制。另外，主管機關應透過行政裁罰督促業者履行源頭管理責任，並結合媒體監督與社會壓力，強化輿論制衡與公民抵制力量，促使企業自律成為制度化常態。

所以你罰則要落實執行，罰金要提高。(P1-5-3)

我們現在有詐防條例，就用裁罰手段去督促他來遵守…我們的策略是希望用法律行政裁罰的目的手段去督促這業者自律源頭管理。(P5-5-3)

我覺得政策上面能作的都作了，就是一直在不斷的裁罰，那我覺得也是要讓媒體去渲染……讓民氣可用，讓民眾去抵制這樣的行為。(P6-5-3)

需要數發部強力去裁罰這些登詐欺廣告的社群平台。(P8-5-3)

2.落實企業社會責任與前端風險控管

防制詐犯罪不應僅是政府的責任，企業端亦應共同負起強化「環境」、「社會」和「治理」（Envirement、Socility、Govener;簡稱：ESG）工作與前端風險管理。受訪者 P2 建議，應要求平台業者於服務流程中導入「認識你的客戶」（Know Your Customer;簡稱：KYC）制度，確保使用者於接觸投資或交易服務前即受風險辨識與安全防護。受訪者 G3 則指出，企業應在平台端設立風險攔截與用戶驗證機制，並提出「防詐營運計畫書」接受主管機關審查，以確保防詐措施具體可行、可檢核。

要求業者要善盡 ESG，在前端做好 KYC 讓民眾要接觸的時候，能夠在企業端也提供良善的保護機制。(P2-5-3)

數發部本身要求他們這些四大業者，他們的網路的詐欺犯罪的防治計畫書要寫得更完善。(G3-5-3)

3.建構常設指揮體系與跨部會資訊整合平台

針對多頭管理與協調困境，任職於警政署刑事警察局，負責全國警察機關防制詐欺犯罪策略規劃及執行的受訪者 P4 認為應建立「常設且實體化的國家級打詐指揮中心」，具備預算、人力及指揮權，整合金管會、NCC、法務部、數位部與警政署等資源，從「橫向聯繫」轉為「垂直指揮」。同時應建置「公私部門數據整合與情報共享平台」，讓金融機構、電信業者與警方能即時上傳異常交易或話務特徵，藉由 AI 交叉比對描繪犯罪網絡，提升防詐預警與系統性打擊能力。

從『多頭馬車』走向『一體化指揮作戰』，跨部會的協調必須打破壁壘，化學反應才會出現。

成立『常設且實體化』的國家級打詐指揮中心……層級要夠高，才能調動、整合金管會、NCC、數位部、法務部與警政署的資源，從『橫向聯繫』提升為『垂直指揮』。(P4-5-3)

建立『公私部門數據整合與情報共享平台』……讓金融機構即時上傳疑似詐欺交易模式，電信業者上傳異常話務特徵，警方提供最新犯罪手法情資。(P4-5-3)

過 AI 進行交叉比對，描繪出犯罪網絡的圖像，才能進行系統性的打擊。(P4-5-3)

4.深化 AI 防詐技術與強化國際監理合作

面對詐欺手法不斷翻新，受訪者 P3 及 B1 認為應導入 AI 與語言模型技術，提升詐欺偵測精準度。例如 Meta 與微軟的「PhotoDNA」可進行圖片雜湊辨識與自動下架，臺灣亦可仿效建立 AI 比對系統，利用語言模型學習詐欺語境，以辨識假投資廣告。此類 AI 系統需投入人力與成本進行持續訓練，政府應提供技術支援並納入法定要求。同時，針對虛擬通貨與境外幣商監理不足的問題，應加強國際合作與司法互助機制，以補足跨境數位金融監理缺口。

臉書跟微軟有做了 1 個叫做 PhotoDNA……全世界統一的，在每個國家的臉書都配合。(P3-5-3)

針對一定的犯罪行為，我們會導入大型語言模式，就是 LLM 進行 AI 的學習…針對類似那種語言學習的方式……人工先去讓他判定，然後讓機器去學習，篩選出來…你要搭配語言學習……現在有 AI，你要讓他去做學習…我們花一定的成本和人力再去判斷這件事情讓模型可以運作。(B1-5-3)

四、阻詐面向的困境與解決的對策

「阻詐」（贓款流向面）為我國打詐體系中關鍵的一環，由金融監督管理委員會統籌，旨在透過金融監理與金流防制措施，攔阻非法資金流向，以降低民眾財產損失。其主要策略包括防制人頭帳戶及信用卡詐欺、強化虛擬資產服務提供業者（Virtual Asset Service Provider;簡稱：VASP）之洗錢防制與詐欺防制管理，並針對貨到付款及一頁式詐欺模式採取管控措施，以建構完善之金融防詐網絡。惟近年金融帳戶涉詐情形仍持續攀升，截至 2024 年 9 月 30 日，銀行及信用合作社警示帳戶數達 14 萬 2403 戶，較 3 月底增加 12.7%，較 2023 年同期更上升 28.6%(行政院，2024)，顯示詐欺金流攔阻工作仍具挑戰。詐欺集團為規避監管與帳戶凍結，逐漸轉向收購或申辦公司戶，以其較高提匯額度進行大額資金轉移，增加追查難度。同時，虛擬資產之匿名性、去中心化及跨境流通

特質，使其成為詐欺集團洗錢與轉移贓款的重要管道。部分詐欺行為更假借「個人幣商」交易名義，以虛擬資產買賣掩飾詐欺所得，藉此規避刑責。整體而言，面對金融數位化與虛擬資產交易快速發展，阻詐策略需持續強化跨行聯防、監理科技運用及金流追蹤能力，方能有效防堵詐欺資金流動，健全國家整體防詐體系。

(一)面臨的困境

在「阻詐」面向中，由於虛擬貨幣的匿名性與去中心化特質，已成為犯罪者轉移贓款與洗錢之主要工具，但政府對虛擬資產業者的監理力道卻明顯弱於傳統銀行體系，使詐欺金流層層隔離，造成警察難以追溯犯罪者真實帳戶，雖金管會推動銀行導入 AI 偵測系統，但業者多因擔憂客戶負面反應而受阻，且跨行資料因隱私與商業利益難以共享，聯防機制形同虛設，而中小銀行在技術研發與數據分析上亦顯不足，加上阻詐措施涉及個資保護、帳戶凍結與警示權限等敏感議題，使警銀合作受限，民眾配合度不足，部分被害人仍拒絕相信並接受行員與警方勸阻，使第一線防線形同受限，反映阻詐工作在制度、技術與人為層面仍存在明顯斷點。依據本研究訪談分析資料顯示，臺灣阻詐工作面臨，虛擬貨幣監理不足與金流追查困難；金融機構 AI 阻詐執行侷限與跨行資訊聯防不足；法源授權不明與警銀合作機制侷限；被害人信任與社會配合度不足等困境

1.虛擬貨幣監理不足與金流追查困難

虛擬貨幣已成為詐欺集團轉移贓款與洗錢的重要工具，因其具匿名性與去中心化特性，導致警方與金融監理機關難以即時追蹤資金流向。臺灣雖有虛擬資產管理規範，但目前仍屬「登記制」，納管力道遠不及傳統銀行體系。此一監理落差，使得詐欺金流形成多層隔離，165 攔阻系統常被卡在虛擬帳戶層，無法延伸至真實銀行帳戶，嚴重影響阻詐成效。受訪者 P1 指出，一般民眾與執法單位對虛擬貨幣皆不熟悉，導致偵查時效受影響，同時降低犯罪者的犯罪風險，提高其犯罪動機。另受訪者 P3 提及，詐團常先將贓款轉入虛擬帳戶再轉入銀行帳戶，使 165 系統僅能攔阻虛擬帳戶層，無法延伸至真實帳戶。P4 則形容，虛擬貨幣是金流追緝上的癌症，因其交易脫離傳統監管體系，即便區塊鏈流向公開，仍難以將匿名錢包地址與實際個人連結。受訪者 P6 表示，阻詐最主要的困境來自於虛擬貨幣的管理，臺灣目前對虛擬資產的管理係採「登記制」，其監管力道僅是傳統銀行體系的 1%。受訪者 G1 認為，因世界各國虛擬貨幣管理法制發展緩慢，遠不及虛擬通貨的發展速度，使詐欺犯罪集團得以利用監理落差之制度性縫隙進行犯罪。

因為一般的民眾對虛擬貨幣不熟悉，警察單位對他也不熟悉，造成查緝上的困難，犯罪者的風險降低了，就會耽誤我們偵查的這個時效。(P1-4-4)

詐欺集團將錢轉到虛擬帳戶，再轉到銀行帳戶，所以 165 只攔到虛擬帳戶，永遠在真實的銀行帳戶之前都會有 1 道阻隔。(P3-4-4)

虛擬貨幣（特別是 USDT）可以說是金流追緝上最大的癌症…錢一旦變成虛擬貨幣，就脫離了傳統銀行的監管體系……要將一個匿名的錢包地址與一個境外的真人連結起來，在技術和法律上都極其困難。(P4-4-4)

阻詐最主要的困境就是虛擬貨幣的部分，虛擬貨幣現在是登記制而已……納管的力道遠遠不及銀行的 1%。(P6-4-4)

各國對於虛擬資產的 1 個管制還是因應的比較慢……法治因應趕不上他的變化。(G1-4-4)

2.金融機構 AI 阻詐執行侷限與跨行資訊聯防不足

雖然金管會要求銀行導入 AI 偵測系統以強化阻詐，但銀行多顧慮誤攔而遭客訴及與客戶體驗感受，傾向僅偵測而不攔阻，造成 AI 技術雖可提供警示，但卻無法進行進金流攔阻行動的現象，另外，各家銀行 AI 模型與資料標準不一，且受限於隱私與商業利益考量，交易異常資訊難以即時共享，使跨行聯防形同具文，且中小銀行在 AI 研發資源與技術上落後，導致防詐能力落差成為詐欺集團利用的漏洞。受訪者 P3 指出雖金管會要求銀行導入 AI 偵測，但多數銀行因憂心誤攔而遭顧客申訴，而傾向僅進行偵測但不實施金流攔阻，使 AI 技術流於警示而非實際行動，另外，各銀行之 AI 模型、資料格式與偵測標準不一，且因隱私及商業利益顧慮，異常交易資訊難以即時共享，致跨行聯防無法形成整合機制。而受訪者 G1 則認為，國內大型金融機構具備技術優勢與資金投入防詐 AI 偵測模型研發，但中小型銀行則明顯不足，形成防詐落差，使詐團可藉此差異化風險進行測試與滲透，如若各金融機構間防詐資訊共享無法即時通報或反應，AI 模型的預警能力將大幅受限，削弱阻詐整體成效。

金管會現在要銀行做 AI 偵測，但是銀行的 AI 偵測有 1 個問題……他們對於攔阻這件事情有 1 個很大的包袱就是客訴…165 的資訊傳給銀行業者打造聯防，但各銀行作法不同，相互間沒有溝通管道，各自為政，使得金融聯防大打折扣。(P3-4-4)

銀行的監控無法有效形成 1 個聯防……中小型銀行在這方面的技術、財力明顯不足…金融機構在阻詐面向所面臨的困境，就是資訊共享受到限制……若無法即時共享交易異常資訊，就不能提高 AI 模型的預警能力。(G1-4-4)

3.法源授權不明與警銀合作機制侷限

阻詐工作涉及個資保護、帳戶凍結與潛在被害人警示等敏感議題，但現行法制未明確授權警察與金融機構的職權範圍。檢警對阻詐的介入程度存有歧見，擔心行政機關超越職權或侵害人權，金管會對 AI 攔阻與跨行合作態度亦相對保守，使警銀聯防體系缺乏明確法律依據。受訪者 P2 即表示，民主法治國家行政機關的核心在於行法行政，檢察官認為警方在查找潛在被害人、暫停帳戶等行為上欠缺明確授權，恐涉超越職權，而有違法疑慮。受訪者 P3 則指出，雖我國《打詐條例》授予檢警偵查機關有一定的阻詐職能，當前阻作作為亦有相當成果，但金管會態度仍保守，未明確要求金融業者積極配合。受訪者 P5 認為，警方雖出於保護被害人之良善思維，但在未有法律明確授下，逕行凍結被害人持有之金融機構帳戶，恐有遭質疑侵害人權之嫌。此外受訪者 G1 提出 ，銀行在 AI 偵測可疑交易後仍需依規定人工審查，時間延遲常致詐團趁隙轉移現金，此顯示阻詐行動欠缺明確法制支撐與操作標準，警銀合作難以達成即時、合法且協同的執行效果。

檢方認為警察做太多，因為依法行政，是行政機關的核心，但是查找潛在被害人，沒有法律授權。(P2-4-4)

阻詐現在問題是…不夠精實，而且法律沒有賦予他們很強大的工具……金管會的態度不明。(P3-4-4)

被害人帳戶被暫停……要警察作，就要給我法律依據，沒有就侵害人權。(P5-4-4)

監管法規也需要及時因應……銀行若偵測到可疑交易，仍需人工審查，延遲造成詐團轉移現金。(G1-4-4)

4.被害人信任與社會配合度不足

阻詐最終能否成功，仍仰賴民眾的配合與信任。然而，詐欺受害者多深陷情感操控或高獲利幻覺，即便警察與行員勸阻，仍有高達三成拒絕相信。部分金融機構行員因顧慮客訴或關懷提問流於形式，使勸阻成效受限。此外，詐欺集團會教導被害人如何應付行員盤問，進一步削弱第一線防線。受訪者 P1 指出，雖警方與銀行行員常及時勸阻，但約有三成被害人拒絕相信，因詐團早已透過長期互動建立情感依附，導致被害人對警銀的防詐訊息產生排斥與不信任。受訪者 P4 則認為，被害人沈浸在詐欺集團長時間洗腦的情境，加上犯罪者都會預先教導被害人如何應對金融機構行員的關懷提問，而錯置的將警察及銀行行員，視為阻疑其發財的拌腳石，此種情況已形成防詐措施的障礙。受訪者 P8 則提出，部分金融機構因顧慮客訴或程序繁瑣，使得關懷提問流於形式，進一步削弱勸阻效果。由以上分析顯示，阻詐不僅是技術與制度問題，亦涉及心理層面與社會信任的建構，若未能從民眾端強化認知與信任，阻詐措施將難以發揮實質作用。

警察和金融機構行員發現被害人被詐欺……仍有三成被害人不相信警察及金融機構行員。（P1-4-4）

銀行行員是很重要的防線……被害人被洗腦後，會把行員當成阻礙他發財的敵人。(P4-4-4)

很多金融機構，礙於怕得罪客戶關懷提問的時候，經常流於形式。(P8-4-4)

(二)解決的對策

本研究綜整受訪者意見建議，臺灣阻詐工作應採強化虛擬貨幣監理與金流追蹤機制；推動 AI 阻詐技術升級與跨行資訊聯防；明確法源授權並設置避風港條款；強化行員專業與民眾防詐配合等對策解決。

1.強化虛擬貨幣監理與金流追蹤機制

面對虛擬資產監管鬆散與金流追查困難的問題，首先應強化虛擬貨幣監理與金流追蹤機制，制定虛擬貨幣專法、落實實名制（KYC），並將虛擬資產服務提供商（VASP）納入金融監理體系。此舉可透過洗錢防制法規範賦予執法機關查核與凍結權限，確保虛擬幣流與真實金流之間的可追溯性，避免詐欺金流「斷點化」。此外，建議全面納管在臺營運之交易所，對不符規範或拒絕配合者應撤銷許可，以強化制度威嚇效果。如受訪者 P4 即建議，應全面納管虛擬貨幣交易所，強制『實名制（KYC）』與『幣流追蹤』並有能力提供完整的交易軌跡，以滿足執法機關偵查犯罪需求，對於無法配合或技術未達標的業者，應直接吊銷其營業許可。受訪者 P6 則建議，應儘速訂定虛擬貨幣的專法，將虛擬貨幣交易所納管，使其成為金融機構的特許事業，以加強監管的力道，將虛擬貨幣交易所化身為打詐團隊的得力成員。受訪者 G1 則提出，金管會應積極推動虛擬資產的監管專法的立法，規定資產虛擬資產交易所要建置有效的阻詐機制。

全面納管虛擬貨幣交易所，強制『實名制(KYC)』與『幣流追蹤』……對於無法配合或技術不達標的業者，應直接吊銷其營業許可。(P4-5-4)

儘速訂定虛擬貨幣的專法…讓監管力道變強…加入我們成為打詐團隊的一員。(P6-5-4)

金管會要積極推動虛擬資產的監管專法的立法。(G1-5-4)

2.推動 AI 阻詐技術升級與跨行資訊聯防

為克服金融機構間 AI 阻詐效能不一與資訊共享不足的困境，應由金管會統籌推動

金融阻詐聯防平台，導入聯合學習技術，使各銀行能在不直接交換客戶資料的前提下，共享防詐模型與風險特徵。大型銀行的 AI 技術與模型可作為中小銀行的學習樣本，縮小防詐落差。此外，應鼓勵導入「AI 異常交易偵測與延遲入帳」制度，建立自動化「冷靜期」機制，當 AI 偵測到可疑交易時，自動暫緩入帳並通報警方與客戶，提供 24 小時反應時間，爭取阻詐黃金期。受訪者 P4 指出，建議金管會推動金融機構導入『AI 異常交易偵測與延遲入帳』機制系統，該系統應包含但不限『自動暫緩』可疑的異常交易 24 小時的『冷靜期』，並可同時對客戶與警方發出警示，為警察阻詐爭取黃金時間。受訪者 G1 則建議，由金管會推動金融阻詐聯防平台，規定大型銀行業者應透過聯合學習方式與中小型銀行共享防詐模型與風險特徵技術，讓中小型銀行也能學習到防詐技術。另外，金管會亦應要求銀行建立電子化照會平台，強化金融機構間的合作，迅速傳達警方辦案通報警示帳戶的需求。受訪者 P3 則認為，應將 165 升級成立國家級詐欺情資分析中心，作為金融阻詐聯防平台，以即時整合分享各金融機構研發的防詐模型與風險特徵技術。

推動金融機構導入『AI 異常交易偵測與延遲入帳』機制……系統應能『自動暫緩』該筆交易 24 小時，並同時對客戶與警方發出警示，…就是我們阻詐的黃金時間」(P4-5-4)

由金管會推動金融阻詐聯防平台……透過聯合學習的技術，讓中小型銀行也能學習到這個防詐技術…金管會應要求銀行端建立電子化照會平台，強化金融機構間的合作，迅速傳達警方辦案通報警示帳戶的需求。(G1-5-4)

成立 1 個類似詐欺情資分析中心去幫銀行做連動，或許把 165 升級也是 1 個方法，(P3-5-4)

3.明確法源授權並設置避風港條款

針對警銀合作法源不明確及執行顧慮，應研修《詐防條例》與相關規範，賦予行政機關及協助攔阻人員法定職權與法律保障，讓所有參與阻詐工作的個人及機構在協助時，能於法定授權下執行並享有「避風港條款」之免責保障，此舉不僅可消除執行端的顧慮，也能建立激勵制度，促進社會多元參與防詐行動。同時，建議修訂相關金融與個資法令，在兼顧隱私保護的前提下，允許跨機關金融資料串聯與共享，以利即時辨識異常金流並啟動阻詐措施。受訪者 P1 建議主管機關能夠修訂相關法令，讓各金融機構的資料能互相串連，俾利警察機關偵辦案件時能在不違反個人資保護法的原則下，更加方便運用。受訪者 P2 希望政府推動《詐防條例》修法，賦予警察機關、銀行行員、超商店員、計程車司機等協助詐欺攔阻人員避風港條款，讓所有參與阻詐工作的個人及機構可以免責，甚至有獎勵的措施。受訪者 P3 則建議金管會修訂法律賦予金融機構，對可疑帳戶可採取暫時性的管制，以形成保護機制，延遲可疑被詐欺或從事詐欺帳戶裡面的款項被提領的時間。受訪者 G3 提議研修「詐防條例」第三節數位經濟防詐措施與強化打詐行動綱領 2.0 防詐面向，讓法律與政策相輔相成。

修訂相關法令，讓金融資料的串連，在不違反個資法的原則下能夠更加的方便。(P1-5-4)

推動詐防條例修法，賦予行政機關及協助詐欺攔阻人員……避風港條款，讓他可以免責，甚至有獎勵的措施。(P2-5-4)

請金管會賦予銀行單位可以採行保護機制，對可疑帳戶作暫時性的管制。(P3-5-4)

研修『詐欺犯罪危害防制條例』第三節數位經濟防詐措施與強化『新世代打擊詐欺策略行動綱領 2.0』防詐面向，讓法律與政策相輔相成。(G3-5-4)

4.強化行員專業與民眾防詐配合

阻詐工作的最後一道防線仍在第一線金融機構行員與民眾互動的關口，行員在關懷提問過程中應保持高度耐心與警覺，不可因客訴壓力而流於形式；同時，金融機構應建立內部獎懲與教育機制，提升行員識詐能力與溝通技巧。此外，應透過跨部門宣導與警銀合作，建立民眾信任基礎，使被害人能在早期察覺異常時接受勸阻，降低資金流出風險。受訪者 P8 指出，金融機構的行員及相關主管應該再精進對被害人關懷提問的技巧與耐心，對於詐欺被害人仍要不厭其煩的進行關懷勸阻。受訪者 P7 則表示，人民必須要建立自我防詐意識，以期早期察覺異常，不要落入詐欺者的圈套。受訪者 G1 認為，金管會應要求銀行端與虛擬資產交易所業者建立異業聯防機制，擴大聯防範圍，以配合警察機關的辦案需求。

金融機構行員跟主管仍要不厭其煩的進行關懷。(P8-5-4)
然後人民的自我防詐意識是要有的。(P7-5-4)
金管會應要求銀行端與虛擬資產交易所業者建立異業聯防機制，擴大聯防範圍，以配合警察機關的辦案需求。(G1-5-4)

五、懲詐面向的困境與解決的對策

「懲詐」(偵查打擊面）為我國防制電信網路詐欺犯罪體系中最後且最關鍵的一環，由法務部統籌，整合檢察、警察及調查機關之偵查能量，透過刑事偵查結果反饋行政機關，以精進打詐機制並強化整體效能，其主要目標在全面清剿詐欺集團、追緝境外嫌犯、查扣犯罪所得，並落實被害人保護與贓款返還，然而，實務運作面臨犯罪集團多採跨國分工與境外設點模式，犯罪者常將機房設於東南亞等地，透過招募、誘騙或人口販運方式使臺籍成員出境作案，導致執法機關在追查過程中受限於司法管轄權與證據蒐集困難，常造成偵辦斷點與金流追蹤中止，使詐欺集團得以持續於境外活動並逃避制裁等挑戰，面對此現象，亟需深化跨境執法合作與情報交換，建立高效率國際合作管道，並結合科技偵查工具強化對境外詐欺網絡之滲透與剿除，同時完善被害人保護與贓款返還制度，以提升我國懲詐政策整體效能。

(一)面臨的困境

在「懲詐」面向雖多次透過修法強化刑度與擴大追訴範圍，然實務上在法院量刑普遍偏輕，詐欺犯罪不法所得雖鉅大，但基層車手輕判與緩刑現象普遍，多數僅服刑數月，造成社會觀感與司法裁量之落差，削弱刑罰威嚇效果，詐欺集團多將機房設於境外利用資通訊技術與司法管轄權限制規避查緝，致使跨境追訴曠日廢時甚至無疾而終，形成境外詐欺打擊之灰色地帶。而警察查緝工作受限於績效考核導向，常忽略追查上游主嫌，偵查資源過度集中於末端層級。現行刑罰制度仍以自由刑為主，忽略財產刑與沒收制度之實質嚇阻功能，導致未能有效剝奪犯罪所得，使詐欺犯罪所獲得利益遠大弊害，成為懲詐成效不足的重要結構性因素。依據本研究訪談分析資料顯示，臺灣懲詐工作面臨，刑罰輕微與量刑寬鬆削弱嚇阻功能；跨境追訴困難與境外主腦免責化；執法績效導向與資源錯置；刑罰偏重自由刑、忽略財產刑等困境。

1.刑罰輕微與量刑寬鬆削弱嚇阻功能

依刑事政策與嚇阻理論角度，刑罰的核心功能在於透過嚴厲制裁，使潛在犯罪者在理性評估成本與利益時，放棄犯罪行為。然而臺灣對電信網路詐欺犯罪之刑度長期偏低，量刑標準亦顯寬鬆，導致懲罰威嚇力不足。雖然我國曾多次修法提高詐欺犯罪法定刑，期能加重處罰犯罪行為，但司法實務對初犯及從犯仍多採輕判、緩刑或合併執行之方式，使得「低風險、高報酬」的犯罪預期未被打破，削弱刑罰的預防功能。受訪者 P1 指出，臺灣司法對詐欺犯罪行為的刑度偏低，形成詐欺有利可圖的氛圍，使一般民眾誤以為詐欺行為風險有限。受訪者 P3 表示，雖然警察機關努力緝獲大量的詐欺犯罪嫌疑人，且處罰假投資詐欺犯罪的法律條文亦設有加重條款，但司法審判機關卻常選擇輕判，使加重刑罰流於形式。受訪者 P4 認為，刑事警察人員經長時間，不眠不休的努力，克服萬難始緝獲詐欺犯罪團成員，但在司法判決實務上多數被捕的車手，都量刑過輕，無法有效震懾有動機的犯罪者。受訪者 P7 補充，司法機關對詐欺車手普遍輕判，僅需服刑數月即可出獄，對犯罪者缺乏警惕作用。

從事詐欺的風氣很盛，處罰又不重，大家就不事生產，想辦法來詐欺就好了。(P1-4-5)

臺灣的刑度那麼低，詐防條例規範好像可以罰很重，網路假投資是詐防條例加重其刑的要件，還是一樣照犯啊。(P3-4-5)

但現行法律下，一個初犯的車手，常常只被判幾個月或緩刑。(P4-4-5)

對於懲詐部分，我覺得車手的刑責太低了。(P7-4-5)

2.跨境追訴困難與境外主腦免責化

跨境詐欺犯罪涉及多國司法管轄，需仰賴國際刑事司法互助機制。然而政治考量與外交限制常導致程序遲滯，使境外詐欺集團主腦長期逍遙法外。此現象造成基層執法人員雖能查獲車手與水房，但上游策畫者難以繩之以法，形成結構性追訴落差。受訪者 P1 指出，詐欺集團經長時間與警察鬥智，深知將犯罪集團分散在不同國家（地區）比在單一國家（地區）遭查獲的風險為低，因此多會選擇與我國無合作共同打擊犯罪機制及司法互助國家設置詐欺機房，導致跨境追緝受阻。受訪者 P3 表示，黑道幫派設於境外的詐欺機房，會隨時注意警察查緝的動向，並據以快速轉移犯罪機房設置地點，以規避使執法單位的查緝。受訪者 P4 認為，臺灣警察機關，雖然能鎖定犯罪集團的詐欺機房或主要犯罪嫌人藏匿的國家（地區），但國際合作共同打擊犯罪及司法互助之踐行，常因雙方法制與司法管轄主張不一，且偵查技術及相關設備亦存在落差，導致調查取證與案件聯結有相當困難度且曠日廢時，使實際查緝效率低。受訪者 P9 進一步說明，詐團主腦利用資(通)訊科技設備及方法，分散犯罪地點並隱身於與臺灣無邦交及合作共同打擊犯罪關係的柬埔寨或緬甸地區實行犯罪，在當地國刻意保護包庇下使得警方查緝無門。

詐欺集團有做功課，知道那個地區不會被警察抓。(P1-4-5)

黑幫在境外成立假投資機房...根據警察查緝的動向到處轉移詐欺機房。(P3-4-5)

就算鎖定了主嫌在某個國家，要請該國協助調查或遣返，需要通過漫長的司法互助程序。(P4-4-5)

現在真正的頭都在國外，柬埔寨或緬甸，那些國家不會理我們...。(P9-4-5)

3.執法績效導向與資源錯置

現行警政體系在打擊詐欺犯罪上過度受限於專案計畫與績效考核制度，導致查緝行

動偏向「以量取績」而非「質的打擊」。許多基層員警為滿足上級所定的計畫指標，只能優先處理易破案的車手案件，而無法投入長期且高風險的上游查緝，形成資源錯置與打擊斷層。受訪者 P4 認為，犯罪集團刻意將犯罪過程切割成互不隸屬的小團體，使警察難以溯源查緝，加上警察機關過度注重查獲嫌犯人數及案件數量之績效指標，導致難以將犯罪集團連根拔起，致查緝效率不佳。受訪者 P5 表示，由於近年來警察機關戮力查緝詐欺案件，致移送各地檢署案件數及查獲人數均呈急速上升，已超出各地檢署負擔能量，致生少部分檢察官僅收本身地檢署管轄案件，造成查獲之警察機關必須將案件切割移送，而來回奔波於多個地檢署，造成警力之浪費。受訪者 P9 指出，各直轄市（縣、市）警察機關基層偵查人員，為滿足警政署所律定之查緝計畫指標，在上級考核壓力下，大都傾向挑選易破案案件，導致資源無法集中於核心組織。

警察非常努力，也抓到非常多犯罪者，但 90%以上都是最底層的車手和人頭戶。(P4-4-5)
現在因為案件量很多，很多檢察官都切割管轄，只收跟自己地檢署有關係的犯罪。(P5-4-5)
滿足刑事局的計畫案，你不可能去往上抓...我去抓最簡單的車手就好了...。(P9-4-5)

4.刑罰偏重自由刑、忽略財產刑

詐欺犯罪的本質在於經濟利益，然而現行制度在金流追查與贓款查扣方面仍存斷點。詐欺集團透過虛擬貨幣、分層轉帳與人頭帳戶掩護，造成查緝困難；加上財產刑執行力不足，使詐團即便入獄仍可保留非法所得，削弱懲罰效果與社會公信力。受訪者 P6 指出，法院對犯罪所得認定過於狹隘，犯罪者僅繳回部分贓款即可獲減刑，導致實際處罰偏輕，削弱刑罰嚇阻力，難以有效遏止詐欺行為的再犯與蔓延。受訪者 P8 表示，虛擬貨幣成為犯罪金流的隱匿工具，造成偵查與追查不法所得困難，難以有效扣押贓款，削弱懲罰與威懾效果。受訪者 B1 認為，執法偏重刑期而非財產追徵；對以金錢為主要動機的詐欺者，刑罰應聚焦財產面懲處而非僅以刑期為核心。

詐防條例有 1 個減刑條款...犯罪者僅需繳回自己分得的部分犯罪所得...。(P6-4-5)
虛擬貨幣經常還是形成我們的偵查斷點，難以扣到這些錢。(P8-4-5)
我覺得懲詐應該針對錢的這 1 塊去作懲罰。(B1-4-5)

(二)解決的對策

本研究綜整受訪者意見建議，臺灣懲詐工作應採提升量刑嚴謹性與司法執行力；深化跨境合作與國際司法互助；科技建警公私協力與改革警政績效體系；強化犯罪所得追徵與財產刑制等對策解決。

1.提升量刑嚴謹性與司法執行力

面對詐欺犯罪輕判普遍的現況，受訪者普遍認為應從「輕判幫助犯」走向「嚴懲組織核心」，透過修法與量刑改革加重刑罰，提高犯罪成本，法官應充分運用裁量權對詐欺行為判處更嚴厲刑度，並針對未揭露上手或多次犯案之車手加重處分，以形成實質威嚇力。此外，亦建議引進外國保安處分制度，讓犯罪者短期內無法迅速重返犯罪場域，藉此降低再犯率。如受訪者 P2 指出，刑罰是最直接有效的防詐手段，應強化打擊能量以發揮威懾作用。受訪者 P5 表示，司法官應喚醒道德良知與社會責任以落實重刑。受訪者 P3 建議，主張採行類似保安處分或體罰措施，提高對車手的刑責以抑制供應鏈，

讓犯罪者短期內無法迅速重返犯罪場域。

打擊是最有效的防治，有打的話就有效。(P2-5-5)
就是法官他要願意判重刑啊。(P5-5-5)
用類似保安處分的方法，援引其他國家的作法採用鞭刑...讓詐欺者不要那麼快回到犯罪場域。(P3-5-5)

2.深化跨境合作與國際司法互助

跨國（境）詐欺犯罪是懲詐的最大挑戰，對策上應透過外交與警政體系合作，避開政治與外交的阻礙，以「警察對警察」（P-P）的合作模式，建構直接快速的情報交換機制，推動與東南亞等詐欺集團主要據點國家簽訂雙邊協定或採非正式合作管道，以提升境外追訴與遣返效率，強化跨國警政合作網絡與科技偵查能力，是瓦解境外機房與掌握跨境金流的關鍵。受訪者 P1 表示，落實跨境合作，強化與境外政府情報交流與聯合打擊機制，從源頭瓦解海外詐團網絡，應可讓臺灣詐欺案件發生顯著下降。受訪者 P4 指出，因台灣的國際政治處境特殊，應透過非官方管道或簽訂雙邊協定的方式，與詐欺集團主要的窩藏國家（特別是東南亞）建立更直接、更快速的情報交換與共同打擊的合作模式。受訪者 P8 認為，電信網路假投資詐欺犯罪機房大都在國外，應以警察對警察的合作模式，加強跨國情報共享與合作共同打擊是壓制詐團運作的有效方式。

要國際合作打擊，讓隱藏在國外的詐團消失。(P1-5-5)
應透過非官方管道或簽訂雙邊協定。(P4-5-5)
加強國際情資的交流跟合作執法的速度。(P8-5-5)

3.科技建警公私協力與改革警政績效體系

面對詐欺技術專業化與組織化趨勢，單靠傳統辦案已難以因應，應以「科技建警、公私協力」為核心，建構跨部門科技偵查平台，結合通訊監控、金融數據分析與 AI 風險偵測，提升打擊效率，強化政府與金融、電信、平台業者之合作，形塑全方位懲詐聯防體系。同時優化現行警察打詐策略，減輕基層員警績效壓力，俾利專注溯源查緝。受訪者 P4 指出，防制電信網路詐欺犯罪需長期投入，應以「科技建警、公私協力」為核心策略，整合 AI 偵查與跨域合作機制，取代傳統警察辦案模式，建構科技化、系統化之全方位懲詐聯防體系。受訪者 P9 補充，應檢討現行績效導向之打詐計畫，減少無實益的文書與評核負擔，讓警察能專注於核心偵查工作，以提升查緝效能並聚焦打擊真正的犯罪主體。

總結起來就是八個字：「科技建警、公私協力」。(P4-5-5)
專心把精力時間花在這些從事詐欺的人身上。(P9-5-5)

4.強化犯罪所得追徵與財產刑制

為破解高報酬低風險的詐欺誘因，必須透過強化財產沒收制度，剝奪犯罪獲利，使詐團無利可圖，司法體系應積極追查犯罪所得來源與流向，除帳戶資金外，亦應沒收房產、名車、虛擬貨幣等衍生資產，並針對境外主嫌在國內的財產設法查扣，以建立從賺錢變虧錢的負報酬環境，減少犯罪動機。受訪者 P4 認為，司法應強化犯罪所得沒收與追徵機制，不僅凍結與查扣帳面現金，亦應追查並沒收以贓款購置之不動產、名車、虛擬貨幣等隱匿資產，即便主嫌在境外，只要在國內有資產，亦應透過跨部會與國際司法

互助設法查扣。受訪者 P8 指出，應努力查緝電信網路詐欺犯罪集團並查扣非法犯罪所得，更應確保財產面制裁以發揮嚇阻效果。

司法體系應更積極、徹底地執行犯罪所得的沒收與追徵。(P4-5-5)
除了要抓人之外，還要查扣不法所得，讓詐欺者付出更多代價。(P8-5-5)

第五章 結論與建議

本章依問題意識與研究目的，綜整前述環境犯罪學相關理論、主要國家的防制策略及成效、質性訪談、官方統計與政策文件等多元資料，提出電信網路假投資詐欺犯罪的整體結論與未來政策推動建議。第一節為主要研究發現，第二節提出未來政策推動建議，第三節為後續研究建議，第四節說明本研究之研究限制。

第一節 主要研究發現

本節從犯罪成因與現況、犯罪腳本建構、警察機關防制困境與對策，以及跨國防制策略比較等四個面向進行整合分析，說明假投資詐欺如何在犯罪者、被害人與情境環境的交互作用下，形成具可擴張性的運作基礎。其次，以犯罪腳本理論解析是類犯罪實施過程的所有階段，接續闡明警察機關於防制詐欺犯罪時，在打詐五面向所面臨的困境與對策，再借鑑日本、新加坡、澳洲與英國等國家的制度設計與政策成效，以辨識臺灣現行防制體系的侷限與可強化方向。最後，導入環境犯罪學相關觀點以阻斷或減少犯罪機會。

一、犯罪成因及現況

本研究結合理性選擇與日常活動等環境犯罪學理論觀點，透過整體詮釋與歸納分析方法，從犯罪者的動機與參與犯罪歷程、被害人的特徵與受害情境，以及缺乏有監控能力者在場的情境脈絡三個面向，建構電信網路假投資詐欺的成因與現況圖像。

(一)犯罪者的動機及參與歷程，顯示理性選擇與社會脆弱性的交錯影響

研究發現，假投資詐欺犯罪者多在有限理性條件下進行犯罪成本與效益權衡，主觀認知詐欺犯罪具有高報酬、低風險等特徵。跨境機房、匿名通訊與洗錢技術的普及，使犯罪者認為警察查緝困難，再加上刑罰輕微，進而強化投入詐騙的意願。多數犯罪者具有教育與就業能力不佳，工作不穩定、家庭功能失衡與社會支持匱乏等背景條件，長期處於社經地位弱勢，易產生相對剝奪感與社會疏離。黑道幫派與犯罪組織透過招募與保護網絡提供非法獲取暴利機會，使詐騙被視為風險可控且具吸引力的收入來源。身處此一結構環境中的個人，將高額報酬與即時現金視為翻轉處境的可行途徑，在認知偏誤與同儕示範影響下，更容易接受加入詐欺犯罪產業鏈作為可接受選項。

新進犯罪成員多以模仿與觀察快速習得並內化犯罪技巧，犯罪組織則提供系統化訓練，包含假投資網路平臺操作、詐騙話術腳本運用、金流處理流程與身分隱匿方式。隨著作案經驗累積，部分成員由基層角色晉升為技術或管理職務，犯罪專業化與報酬增加，使其更難以脫離詐騙犯罪場域。社交圈結構亦隨之改變，犯罪者逐漸脫離主流社會的支持網絡，轉而依附於犯罪團體，並在封閉次文化中重構成功標準與價值觀，將詐騙視為可以長期維持的工作樣態。而犯罪的終止，多半來自外部制度性壓力與內部心理性變化的共同作用。當政府強化打詐策略、提升科技偵查能量與加強金流監管措施使犯罪者感知遭查緝風險提升，或同業競爭與報酬下降削弱高報酬想像時，犯罪者對風險與報酬的主觀評估可能

逆轉。另外，婚姻、育兒與家庭責任以及合法就業機會出現時，亦會促使部分個案進行自我審思，重新評估持續犯罪的必要性。若能在此階段配合就業輔導與更生保護等支持措施，較有機會協助犯罪者脫離詐欺犯罪產業鏈。

(二)被害人特徵與受害歷程呈現結構性與程序化特性

研究顯示，假投資詐欺並非單純偶發事件，而是在有動機的犯罪者、合適標的與監控者缺位的數位環境中長期交織的結果。被害人多為中高齡或退休族群，具有一定儲蓄與可支配資金，平日習慣透過社群媒體與即時通訊軟體接觸投資訊息。退休後人際互動減少、家庭陪伴不足，使其更易在網路互動中對自稱投資顧問或分析老師者產生信任，甚至將詐騙集團成員視為重要情感支持來源。被害人投入假投資網路平臺多以改善財務狀況、償還債務或追求退休後經濟安全感為主要動機。詐騙集團刻意以低風險、高報酬的敘事作為引誘，並在初期提供小額獲利與成功出金經驗，使被害人相信平臺可靠，進而逐步加碼。決策過程深受主觀控制偏誤、厭惡損失、沉沒成本效應與權威認同等多重認知偏誤影響，被害人往往在自認為理性的投資行為中，逐步陷入犯罪集團所設計的情境化信任陷阱中。

從犯罪腳本觀點觀察，被害歷程具有高度程序化特徵，一般可分為初始接觸與導入、信任建構與情感經營、小額試投資與獲利示範、大額誘匯與資金集中，以及拒絕出金與集體失聯等階段。詐騙集團在每一階段均有相對應的話術與操作節奏，透過群組情境營造與假見證操作，使被害人反覆接觸虛假的成功敘事，並在同儕壓力與群體認同中進一步提高投入金額。防護被害制度的延遲與被害後支援不足，使損失易於擴大並提高重複被害風險。警政、金融與通訊監管機關間的資訊傳遞仍存在落差，凍結與追贓往往因程序與授權限制而錯失黃金時機。被害人因羞愧、自責與害怕責難而延遲報案或不願求助，亦使第二波「協助追回款項」或「代辦帳戶解鎖」等類詐騙有機可乘。

(三)監控者缺位與制度斷點形塑高風險的犯罪情境

本研究以日常活動理論觀點檢視相關實證所得資料，發現在電信網路與金融科技、法律規範與防制策略、社會防詐安全網等多個層面，存在監控者缺位或效能不足的情形，進一步擴大犯罪機會結構。

1.電信網路與金融科技面

帳號與門號管理鬆散，使犯罪者易取得大量電信門號與社群帳號，用於投放假投資廣告與維繫聯絡。廣告與社群內容管理效能不足，導致保證獲利、名人代言與投資教學等訊息能長期存留並不斷觸及民眾。金流追蹤則因人頭帳戶、多層轉帳與虛擬通貨轉換而呈現多處斷點，資料交換與留存規格不一，使警方在調閱與凍結資金時面臨時效與權限不足。

2.法律規範與防制策略面

跨境查緝受限於程序繁瑣與合作侷限，詐騙機房與伺服器多設於司法互助不足或執法能量薄弱地區，話務、技術與犯罪金流關鍵點拆散於多地，形成網絡式犯罪組織，使得警察機關縱使查獲單一機房也難以瓦解整體詐欺犯罪產業鏈。而前端防制亦受授權不明與灰色地帶影響，警察在快速下架涉詐廣告、停權帳號與預警高風險社群方面權限有限，宣導則存在時效不足與觸達不精準等問題。

3.社會防詐安全網面

家庭與社交支持不足使被害人更容易資訊封閉與不願求助，公私部門多以事後偵辦與被動回應為主，跨部門協調與主動預防投入仍有限。防詐教育雖有持續推動，卻未能在民眾接觸詐騙誘因的關鍵時點提供可操作的辨識工具，致使民眾難以及時啟動自我保護與求助行為。

二、犯罪腳本建構

本研究運用犯罪腳本分析技術，重新歸納電信網路假投資詐欺自犯罪前行為與準備、主要犯罪行為至犯罪後行為之整體犯罪歷程，發現此一犯罪樣態已由單一事件，發展為高度程序化且可複製之詐欺犯罪產業鏈。犯罪前準備包含組織建構、成員招募與技術工具配置，主要犯罪行為涵蓋前端誘導受眾、中段信任建構與試探，以及小額出金與高額誘匯等互動流程，犯罪後行為則聚焦於金流轉移隱匿、洗錢漂白與脫免查緝。相較傳統偶發性詐欺，假投資詐欺各階段均呈現高度標準化特徵，犯罪組織在長期營運目標下，預先設計任務分工與行動順序，使整體腳本運作模式趨近企業化流程。從理性選擇與日常活動觀點觀察，腳本化設計不僅降低犯案不確定性並提高成功率，亦使犯罪者在監控者缺位或效能不足的情境中，得以形塑穩定運作之詐欺犯罪產業鏈。

(一)前置階段腳本以組織建構與任務分工奠定詐欺犯罪產業鏈基礎

在犯罪前階段，詐欺犯罪集團並非以鬆散人際關係隨機犯案，而是以長期營運為目標進行犯罪組織建構與任務分工。研究顯示，詐欺犯罪集團多採階層化與功能化配置，上層掌握資金控制、洗錢水房與境外轉匯，負責決策與策略規劃；中層管理詐欺機房、話務與社群操作，承擔與被害人直接互動的核心任務；下層則包括車手、技術人員與後勤支援，負責提領及轉手被害人被詐款項、或系統維護與各項支援工作。各層級之間多採單線聯絡與節點隔離，個別成員僅掌握自身任務範圍內資訊，即使某一節點遭治安機關緝獲，其他節點仍可迅速替換或重組，使整體運作不致中斷。此種去中心化與網絡化犯罪組織設計，使詐欺犯罪集團在面對警察查緝時具有高度抗壓能力與自我修補能力，也讓犯罪腳本在組織層面呈現穩定且可持續的運作樣態。

(二)成員招募與內部管理腳本確保人力供應穩定與紀律維持

成員招募與內部管理是詐欺犯罪產業鏈能否持續運作的關鍵。研究發現，詐欺犯罪集團已形成可複製的招募腳本，透過社群媒體、即時通訊頻道與暗網或地下論壇大量刊登高薪、輕鬆與無經驗限制等招募訊息，以快速獲利為餌，引誘求職者與社會邊緣人。同時，犯罪組織亦運用既有成員的人際網絡，刻意拉攏信任度高、口風緊且對法律後果認知薄弱的對象或青少年，根據其技能與背景安排不同角色。對於具專業背景者，如熟悉金融、法務或資訊技術之人員，詐欺犯罪集團則以更高報酬與較少曝光風險的任務吸納，藉此補強廣告投放、網路平臺建置、資安維護與金流操作等技術節點。對於通緝犯或處境困難者，犯罪組織則透過短期庇護與高額報酬交換其承擔車手等高風險職務。內部管理上，詐欺犯罪集團廣泛使用分潤制度與績效指標，以誘匯金額、提領成功率或處理量決定報酬，強化成員提高效率的動機，同時結合威嚇、情感拉攏與物質誘因維持犯罪組織紀律。成員在此

類管理腳本下，逐漸將詐欺犯罪視為可長期從事的工作選項，人力供應因此呈現穩定且源源不絕的狀態。

（三）技術工具與人頭資源腳本建構雙重匿名與多重斷點

在技術準備與工具配置方面，詐欺犯罪集團以雙重匿名與多重斷點為核心目標，預先設計一套完整的技術腳本。研究顯示，詐欺犯罪集團會投入龐大資源製作假投資廣告與宣傳素材，結合專業排版、名人照片與專業語彙，營造具可信度的投資形象，並配合社群演算法將目標族群導入指定頁面或通訊管道。在人頭電話與人頭帳戶部分，詐欺犯罪集團已形成標準化取得與運營流程。常見作法包括在暗網或社群網路市集購買既有帳號與門號，以短期借貸或帳戶美化名義誘騙不知情被害人交付存摺與金融卡，或藉由求職詐騙要求被害人提供帳戶與印章，甚至透過拘禁與威嚇等方式強行取得提款工具。大量人頭電話與人頭帳戶使詐欺犯罪集團能在短時間內建構多重聯絡與金流節點，金流與人流一旦分散至多層帳戶與多個門號，追查難度即大幅提高。洗錢水房與虛擬資產應用則構成後端技術腳本的核心。水房透過多層人頭帳戶轉匯、地下匯兌與虛擬通貨轉換，使贓款在短時間內去識別化並跨境移轉，再以貴金屬、不動產與藝術品等形式完成漂白。整體而言，技術工具與人頭資源腳本在犯罪前階段即完成配置，使詐欺犯罪集團能在正式接觸被害人之前，已具備完善的匿名化與斷點設計。

（四）前端接觸與誘導腳本將大量受眾導入封閉場域

在主要犯罪行為的前端階段，詐欺犯罪集團的腳本目標在於將大量潛在被害人導入可控的互動場域。研究顯示，詐欺犯罪集團普遍透過社群廣告、關鍵字搜尋結果與貼文留言等方式投放假投資訊息，內容多標榜穩定高報酬、名師帶領投資或內線資訊。民眾一旦點擊，即被導向通訊軟體或仿真投資網站，再進一步被引導進入聊天室或投資群組。此一誘導腳本兼具篩選與分流功能。對於缺乏興趣者，詐欺犯罪集團多不再投入成本；對於表達興趣、留下聯絡方式或加入群組者，則視為已通過初步篩選之合適標的，後續由專責話務員接手。透過多輪廣告投放與持續優化標題、圖片與關鍵字，詐欺犯罪集團得以在短時間內精準接觸大量潛在被害人，並藉由誘導腳本將其逐步帶往封閉而難以從外部監督的互動情境。

（五）中段信任建構與試探獲利腳本穩固關係並放大投入金額

在中段階段，犯罪腳本的重心在於建立信任與情感連結，並透過小額試投資與出金，逐步引導被害人放大投入金額。話務員依預設話術腳本與被害人展開日常對話，包含生活關心、投資經驗分享與市場分析，以營造專業又親切的人際互動。詐欺犯罪集團並在通訊群組中安排多名暗樁扮演成功投資者與助理，持續張貼獲利截圖與感謝訊息，以群體互動營造出高績效與高可信度的氛圍。在此過程中，小額試投資與成功出金扮演關鍵角色。詐欺犯罪集團往往先引導被害人投入較小金額，並在短期內提供可見獲利與順利出金經驗，使被害人相信假投資詐欺平臺具有真實運作基礎，進一步削弱既有防詐認知。隨著投資次數累積，被害人逐漸將話務員視為可信賴的投資夥伴或情感支持對象，在主觀控制偏誤與厭惡損失心理作用下，更傾向相信詐欺犯罪集團提供的內線訊息與限時專案。中段腳本同時包含試探與調整功能。詐欺犯罪集團會依被害人的回應速度、提問內容與風險承受度，

調整互動節奏與投入金錢額度，對警戒心仍高的對象維持在較小金額範圍內反覆操作，對高度信任者則加快進入高額投資與集中資金階段。此一彈性調整能力，使中段腳本成為整體詐欺犯罪產業鏈中最具情境化與個別化的階段。

（六）後端資金收割與贓款去識別化腳本完成隱匿金流運作流程

在被害人信任與期待被推升至最高峰後，詐欺犯罪集團即啟動後端資金收割腳本。常見作法包括以限時高收益專案、內部會員方案或風險避險操作為由，要求被害人大額匯款或多次加碼，並引導其使用網路約定轉帳、購買虛擬通貨或面交現金等方式完成匯出。一旦資金到位，詐欺犯罪集團立即啟動金流斷點腳本，指示車手分批提領、轉交水房或轉換為虛擬資產。水房再透過多層帳戶轉匯、地下匯兌與境外虛擬錢包操作，使贓款在短時間內脫離金融監管。當被害人要求出金或質疑帳戶異常時，詐欺犯罪集團則依腳本以系統維護、帳戶凍結、稅務審核或國際匯款延遲等理由拖延，最終關閉網站、清空群組並集體失聯。在此階段，金流操作與聯絡斷線並行，形成贓款去識別化與被害人斷絕求償可能性的封閉結構。從犯罪腳本觀點來看，後端資金收割與洗錢腳本不僅完成單一案件的獲利，也透過斷點設計維護整體詐欺犯罪產業鏈的安全性。

（七）車手集團、水房與境外機房具詐欺犯罪關鍵節點功能

本研究也發現，車手網絡、水房與境外機房等節點在犯罪腳本中各自承擔不同功能，彼此之間卻高度互賴，共同維持詐欺犯罪產業鏈的封閉運作。車手網絡位於實體金流與帳戶金流的交界，負責提領現金、面交收款或搬運提款工具。為降低法律風險，詐欺犯罪集團傾向招募未成年、孕婦或無固定收入者擔任車手，並透過多筆小額提領的方式規避金融機構偵測。水房則扮演金流集中與再分散的核心樞紐，負責接收來自不同車手集團、不同帳戶的資金，再依犯罪組織策略轉為虛擬資產或其他形式，完成跨境移動與漂白。境外詐欺機房則是話術生產、情境設計與訓練的集中場域。機房多設於執法能量不足且可獲在地保護的境外地區，內部配備多機多線與標準化話術模組，能支援大量話務員同時運作。透過集中管理與即時監控，機房能依據被害人反應調整話術策略，也能快速訓練新進成員上線，使犯罪腳本在話務與情境操弄方面維持高度一致性與效率。

（八）模組化腳本設計強化詐欺產業鏈的循環再生能力

從犯罪腳本分析觀點來看，假投資詐欺之所以具備強大再生產能力，關鍵在於各階段流程已被標準化與模組化。廣告投放、誘導話術、群組互動、小額試投資、加碼節奏與出金拖延等元素，都可視為獨立模組，犯罪組織可依不同被害族群、投入金錢額度與區域條件進行組合與調整。這種模組化設計具備三項特徵。第一，具有高度教學性。詐欺犯罪集團可透過簡報、範例與模擬對話，快速將既有腳本傳授給新成員，使其在短時間內達到可操作水準。第二，具備量化管理空間。犯罪組織可根據誘匯成功率、回應時間與平均投入金額等指標，持續調整腳本內容與節奏，在類似實驗與修正過程中逐步優化。第三，便於跨區域複製。當某一套腳本在特定區域或族群證實有效後，可透過人員流動或技術分享快速外移至其他地區，使詐欺犯罪產業鏈具有跨境擴張的能力。

(九)時間差與斷點設計在腳本中的核心角色

本研究亦發現，時間差與斷點並非單純的犯罪副產品，而是被犯罪集團刻意納入犯罪腳本的設計元素。前端導入與中段互動階段透過長時間的情感經營與反覆示範，使被害人逐漸降低防備，延後其懷疑與查證的時間點。後端資金收割與洗錢階段則在極短時間內完成多層轉匯與轉換，使警察與金融機構即使在被害人報案後立即介入，也常因既有的時間差而無法有效阻斷並凍結遭詐贓款的轉移。斷點設計方面，詐欺犯罪集團透過人頭帳戶多層轉匯、跨平臺與跨境操作，使金流與人流在多個節點斷裂，讓單一機關難以重建全貌。資訊與權責若無整合，警察與監管機關在查緝上往往僅能看見部分片段，無法對整體詐欺犯罪產業鏈造成實質壓力。

綜合上述分析可知，電信網路假投資詐欺之犯罪腳本，已發展為一套具高度組織化、模組化與循環再生能力的封閉式作業流程，其運作橫跨犯罪前準備、主要犯罪行為與犯罪後行為等多個階段，並由多重節點與斷點共同支撐詐欺犯罪產業鏈的穩定運作。於犯罪前準備階段，詐欺集團透過組織建構、任務分工、成員招募與內部管理機制，確保人力供應穩定與行動紀律，同時結合技術工具、人頭門號、人頭帳戶等資源，形塑雙重匿名與多重斷點的基礎架構。

在主要犯罪行為階段，前端藉由假投資廣告、社群平台互動與封閉群組場域完成大量受眾導入與初步風險篩選；中段則透過腳本化話務應對、偽造投資資訊、小額出金與試探獲利等手法，逐步建構信任關係並推升被害人投入金額，藉此放大詐欺收益。進入犯罪後行為階段後，詐欺集團即透過車手集團、水房、地下匯兌、境外機房及虛擬資產轉換等關鍵節點，進行金流分拆、跨境移轉與贓款去識別化，藉由時間差與斷點設計降低查緝風險並去除跡證。

整體而言，各階段均依賴相對應的人力、技術與制度性資源，並以模組化腳本設計維持高度彈性，使詐欺集團得以依不同受害族群特性，調整語言包裝、互動節奏與金額設定，進而強化犯罪腳本的可複製性與擴散性。從警察防制觀點來看，若僅針對單一案件或單一節點進行查緝，難以破壞詐欺犯罪產業鏈的封閉循環結構。唯有回到犯罪腳本的整體視野，辨識各階段關鍵節點與可介入時點，並於受眾導入、互動歷程與出金行為等關鍵階段，同步配置打詐五面向的防制措施，方能逐步削弱其循環再生能力，促使詐欺犯罪由高報酬、低風險的結構，轉向高風險、低報酬之不利運作環境，作為後續政策建議與實務調整的重要基礎。

三、警察機關防制困境與對策

本研究以打詐綱領 2.0 為分析主軸，結合實務訪談與政策文本分析，從打詐五面向探討我國防制電信網路假投資詐欺犯罪之制度現況與執行困境。研究結果顯示，雖政府近年積極推動跨部會合作、修訂法規並導入科技偵防工具，但各面向仍存在宣導落差、法制侷限、跨境執法瓶頸及技術與資源不均等問題，致使整體防詐體系難以形成循環式防線。

(一)識詐面向

我國防詐宣導雖達成高觸及率，惟宣導內容多流於形式化與重複化，民眾防詐意識與實際行動仍存顯著落差。尤其高風險族群如中高齡者、網路投資族與情感脆弱者，對新型詐欺手法之辨識力有限。此現象反映出現行宣導策略缺乏精準分眾與持續性學習機制。未來宜透過 AI 與大數據分析民眾受騙特徵，設計動態化宣導內容，並強化地方社區與學校教育的防詐扎根，落實分齡、分眾、分域的宣導模式，方能有效提升民眾防詐免疫力。

(二)堵詐面向

電信監理與執法權責分散，導致電信門號實名制執行不一、企業簡訊審查鬆散、人頭門號仍層出不窮，加上境外 VOIP 及 VPN 詐欺來源難以攔阻，使堵詐政策效果受限。主管機關於實務上常面臨通訊自由與犯罪防制間之權衡困境。未來應檢討相關通訊法規，授予主管機關適度行政介入權，並要求平台業者履行即時通報及防堵義務。此外，跨境資訊共享與司法互助亦須制度化，以提升跨國攔阻之即時性與技術整合效率。

(三)防詐面向

隨著數位經濟快速擴張，社群媒體與線上廣告成為詐團滲透的重要管道。民間平台多以商業利益與言論自由為由，對防詐責任採取消極立場，致使政府防詐策略呈現公權力不足、私部門不作為之落差。加之跨部會合作與資訊流通效率不足，使防詐工作難以形成即時監理鏈。未來應推動防詐專法或修法明確界定業者之法律責任，並建立常設跨域合作機制，導入 AI 內容辨識、圖像比對與深偽監測技術，藉以強化網路環境淨化與平台管理能量，減少詐欺訊息之流通與曝光。

(四)阻詐面向

金融監理與金流攔阻成為假投資詐欺防制成效的關鍵。訪談結果指出，虛擬貨幣與跨境支付的匿名性，使金流追蹤與凍結極具挑戰。現行 AI 阻詐系統雖已普及於金融機構，但因跨行資訊未能即時共享，導致可疑交易監測出現延遲與偵測盲區。同時，警銀合作在法源授權不足及責任歸屬不明下，仍存執行顧慮。建議未來應強化監理科技與金融資訊安全平台整合，建立跨行 AI 聯防網絡，並修法增訂「避風港條款」以保護前線行員與協助攔阻人員之權益。另應深化虛擬資產服務提供者(VASP)監理，確保加密貨幣交易之透明化與可追蹤性，以阻斷詐欺金流外逃。

(五)懲詐面向

司法實務中量刑寬鬆與財產刑執行不足，削弱對犯罪者之嚇阻力。詐團多設境外機房與虛擬組織架構，使我國偵查單位難以鎖定上游主嫌，形成境內逮車手、境外免懲罰的落差。另執法機關績效導向偏重案件數量，忽略跨案整併與資金流追查，導致打擊深度有限。未來應提升量刑標準並強化財產刑與犯罪所得追徵，增設跨境執法協調平臺，促進與國際刑警組織（INTERPOL）、東南亞國家聯盟（Association of Southeast Asian Nations,簡稱：ASEAN）、亞太防制洗錢組織(Asia/Pacific Group on Money Laundering,簡稱 APG)等合作機制，提升跨國偵查與引渡效率。同時應完善被害人補償及贓款返還制度，確保司法公信與社會信任。

綜合而言，本研究發現臺灣防制電信網路假投資詐欺之五大面向，實質上構成一個政策鏈結體系，以識詐為教育基礎、防詐與堵詐為中介防線、阻詐與懲詐為終端抑制手段。然而，目前該鏈結體系仍呈現各自為政現象，部會間橫向協調不足、資訊互通機制尚未完善，致使整體防詐成效未臻理想。未來防制策略應朝整合管理與科技驅動雙軸並進發展，透過跨部會常設指揮架構統籌各面向資源，結合 AI 風險監測、區塊鏈金流追蹤、深偽內容偵測等新興科技，打造前端預警、中端攔阻、後端追訴的全方位防詐生態系。此外，民間參與與公私協力亦為關鍵。政府應建立社會防詐共同體概念，鼓勵金融業、通訊業、平台業者及社區組織共同承擔防詐責任，形成多層次守門人網絡，落實全民防詐願景。唯有透過法制強化、科技應用與社會動員三者協同運作，方能有效降低假投資詐欺犯罪發生率，維護社會秩序與國民財產安全，達成打詐五面向環環相扣的防制體系之終極目標。

四、主要國家的防制策略及成效

本研究蒐集日本、新加坡、澳洲與英國近年防制電信網路詐欺特別是假投資詐欺之政策文件與統計資料，分析各國犯罪概況與防制策略上的共通趨勢與差異特徵。整體觀之，全球詐欺犯罪呈現跨境化、科技化與組織化發展，假投資詐欺高度依賴社群媒體、即時通訊與加密資產，並在疫情後搭配遠端社交與數位交易常態化，迅速擴張。各國普遍建構以打詐五面向為主軸的循環防線，並強調公私協力與科技應用。

（一）犯罪概況比較顯示跨境化與科技化為共同結構

臺灣近年詐欺犯罪案件持續增加，假投資詐欺在案件數與財損占比皆居高不下，顯示假投資詐欺犯罪產業鏈具有強大再生與轉型能力。即使行政院推動打詐綱領 2.0，整體犯罪仍在強化查緝環境中持續轉型與調整。日本則以高齡者受害之特殊詐欺為重要議題，整體犯罪樣態逐漸朝科技化與情境化發展。新加坡案件集中於網路購物、假求職與假投資詐欺，反映網路平台與支付生態所帶來的高風險集中特徵。澳洲詐欺樣態呈現出多元並行的整合性犯罪結構，電信詐欺與投資詐欺為前兩大類。英國因金融市場成熟與線上交易頻繁，使授權付款詐欺與網路釣魚成為高風險類型。整體而言，各國雖在詐欺案件組成與被害族群上有所差異，但都面臨數位環境快速變化、跨境金流與虛擬資產應用導致的監管與查緝挑戰。

（二）識詐策略發展指向行為導向與科技化結合

主要國家的識詐政策已由傳統單向宣導，逐步轉向行為導向與科技化結合的模式。政策重點不再僅以場次與觸及數作為主要成效指標，而是更加關注民眾是否實際採取查核、阻斷與通報等防詐行為。在執行方法上，各國都嘗試將識詐訊息嵌入搜尋、點擊與轉帳等高風險關鍵介入點，例如於網路搜尋投資訊息時顯示警示頁面，在點擊疑似詐騙連結或安裝不明應用程式前提出提醒，或在進行境外匯款與大量轉帳操作前提供明確風險提示。對高齡者則透過情境演練與通話模擬等方式，加強其辨識情境化詐術的能力。日本在高齡社會背景下，特別重視生活型風險的宣導與在地接觸管道的建立，並逐步導入人工智慧風險提示。新加坡與澳洲則分別透過全國性防詐平台、廣播與社群推播，整合識詐宣導與回報

機制。英國則透過 Take Five 行動等方案，將金融教育融入日常生活情境，鼓勵民眾在關鍵時刻停下思考與查證。

（三）堵詐與防詐策略展現科技聯防與流程管理的制度化趨勢

在堵詐方面，各國普遍推動來電識別機制、簡訊發信註冊與惡意網址封鎖等措施，透過電信商與監管機關合作，建構多層次攔阻機制。關鍵在於明確法源授權與資料標準化，確保電信攔阻措施既具即時性，也能兼顧通訊自由與隱私保障。日本、新加坡、澳洲與英國分別在來電管理、簡訊發信註冊與假投資網址封鎖上建立較完整制度，對重複違規來源實施權限限制、停權與封鎖，並與警政與監管機關共享高風險號碼與網址名單。在防詐方面，各國逐漸由單點下架走向具階段連續性之防制策略。涉投資廣告的事前審核與風險標示被前移至平台入口，涉詐帳號的停權與名單共享則被納入平台責任範疇。社群與搜尋服務被要求對反覆違規者採取一致性處置標準，並建立跨平台名單共享機制。金流監控則以情境式規則為觸發點，導入延遲與複核等機制，實現平台管理與金融阻斷之整合控制。新加坡與澳洲在政府與業者組織合作下，強化網路平臺在地管理責任與資料配合義務，要求在一定期限內完成防詐措施建置；英國則透過產業承諾與監管要求，推動大型網路平台加強涉詐內容與帳號管理。整體趨勢顯示，入口、內容、社群與金流等多層管理機制，正逐步整合為跨前中後端之整體防制配置。

（四）阻詐與懲詐策略凸顯時間管理與財產刑的重要性

阻詐面向的國際經驗指出，於開戶、收受資金、轉出、跨境與兌現等關鍵介入點設置多重把關，是搶回時間優勢的關鍵。各國普遍要求在高風險交易情境自動觸發延遲交易與多重驗證，並建立跨行資訊平臺與標準化欄位，以利名單與風險標註即時同步。新加坡以集中機制統籌即時凍結與補償措施，澳洲透過收款人確認與轉帳延遲制度平衡誤攔與阻斷，英國則以授權付款補償制度與事前警示機制連結前端預防與後端補償。上述作法共同指向一個重點，即藉由制度義務與技術平臺的結合，縮短警察與金融機構在資訊掌握與處置上的時間落差。在懲詐層面，主要國家多採行自由刑量刑與財產刑並重之策略，將沒收與追繳機制置於制度設計階段，以提升剝奪不法所得之確定性與效率。另透過跨境警務合作與情資交換，削弱政治與管轄造成的阻礙，並建立即時聯繫機制與標準化請求程序，以強化境外資產凍結與返還之可行性。日本、新加坡、澳洲與英國分別透過專責機構或中央統籌機制整合查緝能量，致力於瓦解詐欺犯罪集團並追查洗錢水房。整體而言，量刑結構、國際合作、財產刑執行與在地化管理責任，是提升整體懲詐效果的四個重要支柱。

整體觀察臺灣與主要國家的防制經驗，可以看出多數法域皆已逐步形成從識詐到懲詐的多層次防線。臺灣在政策方向與制度架構上大致與國際趨勢一致，不過在制度義務的細緻化、科技整合的速度，以及關鍵節點的時間管理上，仍有進一步強化的空間。若從情境犯罪預防的角度觀之，各國常用策略在功能上各有側重：識詐著重於提升民眾對風險的警覺與基本辨識能力；堵詐透過電信與通訊措施增加犯罪者需付出的成本；防詐則將平台義務與金融機制納入前端治理，減少犯罪者可利用的便利條件；阻詐聚焦金流流程把關，藉由延遲、複核或身分確認爭取處置時間；懲詐則透過追繳、沒收與跨境合作，提高犯罪後果的確定性。五個面向彼此相扣，構成由前端預防至後端制裁的連續防制鏈結。

若進一步以犯罪腳本分析方式檢視各國作法，可發現有效防制策略多能對應詐欺犯罪之關鍵運作階段。首先，犯罪前準備階段包含組織建構、成員招募與技術工具配置，宜透過法制規範、產業責任與技術管制等制度性介入，抬高其起始門檻與整體運作成本。其次，在前端誘導受眾階段，防制重點在於強化投資類廣告之事前審查與明確風險標示，並將警示訊息嵌入搜尋、點擊等高風險介入點，以降低民眾初次接觸詐騙資訊時之誤信可能。再者，於互動階段，須在社群導流、站外連結或即時通訊過程中設置即時提示與回報管道，使民眾在信任逐步被植入之前，仍保有查證與退出之空間；至於出金階段，則以延遲交易、行為確認與即時凍結等機制爭取緊急處置時間，抑制財損擴大。若其中任一環節形成制度缺口，詐欺集團即可能迅速恢復既有詐欺犯罪之階段性運作，因此防制策略須強調跨階段、跨節點之運作連貫性，而非僅仰賴單一措施之重複堆疊。

綜合主要國家的制度實踐，對臺灣至少具有三項具體可行的借鑑方向：第一，識詐成效評估宜由活動場次與觸及人數，轉向民眾是否實際採取查核、阻斷與通報等行為指標，並針對高風險族群與使用情境進行更分眾、可操作的訊息投放；第二，涉詐內容下架、帳號停權與風險名單共享宜建立明確的分級處置與一致性標準，並推動跨平台共同執行，以降低重複違規者在不同服務間游移的空間；第三，阻詐與懲詐策略須強化時間管理與財產刑工具的前置設計，在金融交易端預設延遲、收款人確認與跨行同步標註，以提升即時性，並於制度規劃階段即納入追繳與沒收機制，使不法所得之剝奪更具效率與確定性，避免懲詐效果過度依賴人犯是否到案。

五、導入環境犯罪學相關觀點阻斷或減少犯罪機會

在前述實證分析與跨國比較基礎上，本研究進一步回到理性選擇、日常活動、犯罪腳本、問題導向警政與情境犯罪預防等環境犯罪學理論，綜合審思警察防制電信網路假投資詐欺之整體方向。研究顯示，若僅依賴事後偵辦與加重刑罰，難以有效對抗已呈現具階段性且跨境化之運作模式的詐欺犯罪產業鏈，必須透過情境犯罪預防技術，在犯罪腳本的關鍵節點設計多層次防線，重塑犯罪者與被害人在成本與風險上的主觀評估，並以問題導向警政作為制度化行動框架。

（一）以理性選擇與日常活動觀點重構犯罪成本效益

理性選擇理論提醒，犯罪者並非完全不顧風險，而是在主觀判斷中將風險視為可接受範圍內的成本。本研究發現，跨境設點、匿名工具、量刑偏輕與財產刑執行不足，使犯罪者傾向認為詐騙屬高報酬、低風險活動。若要改變此一認知結構，必須同時提升查緝確定性與犯罪所得剝奪可能性，使潛在犯罪者在成本效益衡量中重新計算風險。日常活動理論則強調，犯罪發生需要具動機犯罪者、合適標的與缺乏監控者三項條件同時存在。本研究顯示，電信網路與金融科技的快速發展使合適標的大量存在，而監控者在多個關鍵節點出現缺位或效能不足。因此，防制策略的核心在於讓有監控能力者於關鍵節點再現，包含網路平臺、金融機構、電信業者與公部門，在搜尋、誘導、互動與金流等節點重新出現，改變犯罪機會結構。

（二）運用犯罪腳本分析辨識可介入之關鍵防制節點

透過犯罪腳本分析，本研究將電信網路假投資詐欺之整體運作流程，區分為犯罪前準備、前端誘導、中段互動與後端出金等相互銜接之階段。各階段均仰賴特定人力、技術與制度性資源配置，並透過任務分工、時間差與斷點設計，形塑高度隱匿且可循環再生的詐欺犯罪產業鏈。此一分解方式，有助於警察與相關機關跳脫僅以案件結果為導向的查緝思維，轉而從犯罪腳本的整體結構中，辨識可導入情境犯罪預防技術之關鍵介入節點。

1.犯罪前準備階段

犯罪前準備階段係詐欺犯罪產業鏈得以啟動與穩定運作的基礎環節。詐欺集團通常透過組織建構、任務分工、成員招募與內部管理機制，確保人力供應穩定與行動紀律，並結合技術工具、人頭門號、人頭帳戶等資源，形塑雙重匿名與多重斷點的基礎架構。針對此一階段，防制策略不宜僅待犯罪行為實際發生後介入，而應著重於源頭風險控管，例如強化門號、帳戶與數位身分之實名驗證與異常使用監測，落實人頭資源查核與流向追蹤，並透過跨機關資料勾稽，及早辨識具組織化特徵之異常招募與資源配置行為，以削弱詐欺犯罪產業鏈的組織基礎。

2.前端誘導階段

前端誘導階段係詐欺犯罪中大量受眾導入與初步風險篩選的關鍵環節，犯罪集團多透過假投資廣告、搜尋結果操弄、社群平臺互動及通訊群組邀請等方式，引導民眾進入封閉式詐騙場域。針對此一階段，可於涉投資廣告投放、搜尋結果呈現與加入通訊群組等行為節點，導入事前審查、風險標示與警示頁面等措施，使潛在被害人在尚未進入詐騙互動流程前，即能接收到具即時性與可理解性的警示資訊。

3.中段互動階段

中段互動階段為詐欺集團透過腳本化話術、偽造投資資訊與試探性出金，逐步建構信任關係並放大被害人投入金額的核心階段。於此階段，犯罪行為多透過私訊誘導、群組互動、站外連結導入或要求安裝非官方應用程式等方式進行。相應之防制作為，可針對上述高風險情境，設計即時提示與防護機制，並由公權力或平臺主動提供查證管道，以干擾既有互動節奏並削弱信任累積效果。

4.後端出金階段

後端出金階段為詐欺犯罪實際完成金錢移轉與贓款去識別化的關鍵環節，詐欺集團往往透過車手集團、水房、地下匯兌與虛擬資產轉換等節點，進行金流分拆與跨境移轉。針對此一階段，可就首次匯款、重複匯款、大額交易與跨境匯款等高風險行為，導入預設延遲、多重驗證與人工複核流程，並結合金流模式偵測與關係圖譜分析，提高犯罪完成成本並壓縮其可行空間。

（三）情境犯罪預防技術可在五道防線中具體落實

結合本研究對打詐五面向的分析，可以看見情境犯罪預防技術在各面向皆有具體落實空間。

1.在識詐面向

情境犯罪預防並非僅透過知識傳遞，而是將提醒訊息嵌入實際操作流程，使民眾在高風險行為前被迫放慢決策速度並重新思考。例如在搜尋投資關鍵字或點擊高風險連結時，自動顯示警示頁面，並提供查證管道與求助資源。

2.在堵詐面向

可透過來電警示、簡訊發信註冊、黑名單整合與惡意網址封鎖等技術，增加犯罪者接觸被害人的犯罪阻力，削弱其利用通訊工具快速擴散的能力。

3.在防詐面向

可要求網路平臺業者在廣告審查、帳號管理與社群管理中導入人工智慧偵測與風險評分制度，對重複違規者施以分級與一致性處置標準，並將涉詐內容與帳號資訊回饋給警察與金融機構，形成跨域聯防。

4.在阻詐面向

可建置金融阻詐聯防平臺，以聯合學習與標準化欄位共享風險特徵，於高風險交易情境啟動預設延遲與多重驗證，使時間轉為防制方的有利資源。

5.在懲詐面向

可結合科技偵查與財產刑制度，透過區塊鏈交易與實體帳務資料之整合應用，將沒收與追徵內嵌於專案設計，縮短申請、核發與執行之間的時間落差。

（四）問題導向警政提供制度化的循環行動框架

問題導向警政強調以問題為核心，透過掃描、分析、回應與評估的循環架構，持續調整與修正防制策略。本研究發現，假投資詐欺的防制若能納入問題導向警政架構，可將偵查、監管、宣導與預防等分散作為，轉化為系統化的防制體系，以提升整體效能。

1.掃描階段

透過熱點分析與案件型態分類，辨識高風險族群、網路平臺與金流模式。

2.分析階段

結合理性選擇、日常活動與犯罪腳本等理論，檢視制度漏洞與被害風險來源。

3.回應階段

整合警政、金融、電信、網路平臺與社會行政與福利等資源，針對特定問題設計情境化防制方案，例如高風險帳戶預警、高齡者專案訪查或特定平臺合作機制。

4.評估階段

透過量化指標與質化回饋，檢驗方案成效並進行調整，避免流於單點式處置與非整體性規劃。

（五）威嚇、預防與復歸的整合策略是長期穩定抑制的必要條件

研究顯示，若只強化單一犯罪環節的防制而忽略整體系統的運作，容易出現犯罪手法

轉換與詐騙模式迅速重組再現的情形。要達成長期穩定抑制，必須在威嚇、預防與復歸三個面向同時投入。

1.威懾面向

提升查緝確定性、強化財產刑執行並縮短跨境合作時距，使犯罪者真正感受到高風險與高成本。

2.預防面向

藉由識詐、堵詐、防詐與阻詐等多重措施，改變犯罪機會結構，讓詐欺犯罪集團在前端誘導、中段互動與後端出金三個階段都面臨更強的犯罪阻力與更大不確定性。

3.復歸面向

關注被害人與犯罪者的後續處境，為被害人提供心理支持與法律協助，降低重複被害風險；對犯罪者則透過就業輔導與更生保護，減少其重新投入詐欺犯罪產業鏈的誘因。

綜合本研究實證與理論分析，可以發現時間差與組織合作是情境犯罪預防能否發揮效果的兩項關鍵因素。時間差既是詐欺犯罪集團利用的工具，也是防制體系可以爭取的空間。透過預設延遲、二次確認與同步下架與凍結等制度設計，可以將原本對防制方不利的時間差轉化為風險評估與人工複核的緩衝期。組織合作方面，若黑名單與風險警示無法跨機構同步，打詐五面向之間的銜接便容易被時間差與資訊斷點破壞。唯有透過制度化的資訊共享、明確的權責分工與穩定的國內外合作機制，才能將單一案件偵辦的成果，轉化為對整體詐欺犯罪產業鏈的結構性壓制。假投資詐欺已成為結合科技、社會心理與跨境利益的數位結構性犯罪，警察防制策略若要有效抑制詐欺犯罪產業鏈，必須在理論與實務之間建立緊密連結，並透過組織合作與時間管理，把環境犯罪學的核心觀點具體轉化為可操作的情境防制技術，作為後續短期、中期與長期政策建議的重要基礎。

第二節 未來政策推動建議

本節以前述研究發現為基礎，依循打詐綱領 2.0 所揭示之打詐五面向防制架構，提出短期、中期與長期政策方向。整體而言，未來政策推動宜以制度統整、科技強化與行為導向為短期主軸，逐步推進至中期之制度化與科技化防制，並於長期邁向智慧警政與永續防詐，以形成可持續更新且具回饋機制之整體防制系統，亦與問題導向警政強調以具體問題為核心、跨域合作與循環式學習之防制精神相契合。就電信網路假投資詐欺之犯罪腳本觀之，其運作除呈現前端接觸與引流、中段互動與信任建構、後端資金收受與去識別化等階段性流程外，於犯罪前準備階段亦常透過組織建構、任務分工、成員招募與內部管理機制，確保人力供應穩定與行動紀律，並結合技術工具、人頭門號、人頭帳戶等資源，形塑雙重匿名與多重斷點之基礎架構，使後續各環節得以模組化複製與快速替換。基此，政策設計若僅聚焦於單一環節，常因犯罪者轉移與變形而使防制效能折損；相對地，若能依五大面向在犯罪腳本早、中、晚期同步配置阻斷點，便可在制度、技術與行為層次形成互補，系統性提高犯罪風險、增加犯罪成本並降低犯罪報酬，使其不易再以高報酬、低風險之誘因結構持續擴張。

一、識詐面向

識詐面向之政策推動，核心在於將防詐工作由傳統單向宣導，轉型為貼近日常行為情境之精準、互動與行為導向介入，使民眾在高風險情境中能即時啟動查證與自我保護。由於假投資詐欺多透過日常資訊接觸與投資想像逐步誘導被害人，若僅停留於概念性宣導，往往難以在關鍵時點轉化為實際防護行為，故識詐策略須依短期行為介入、中期社會化支持與長期制度化培養之路徑加以推動。

短期階段，應以分齡分眾的識詐教育模式作為主軸。警政署可與教育部、地方政府及民間團體合作，依年齡、職業與媒介偏好規劃不同宣導方案，例如青少年以校園課程與線上互動教材為主，中壯年投資族結合企業內部訓練、理財講座與社群推播，高齡者則透過地方廣播、社區據點與家屬協助提升觸達率。此一分眾策略有助於提升訊息到達率與理解度，避免宣導形式化而難以轉化為實際行為。

同屬短期作為者，識詐亦應進一步朝高風險行為節點之介入設計推動。依日常活動理論與情境犯罪預防觀點，民眾在搜尋高報酬投資關鍵字、點擊不明連結、加入陌生群組、下載不明投資應用程式，或準備將款項轉入境外帳戶等高風險行為發生前之關鍵時點，最需要立即且具體的風險提示。故建議在上述可介入之高風險行為節點導入系統自動跳出警示訊息或二次確認流程，引導民眾暫停操作並進行查證，以補強有監控能力者不在場的結構性缺口，使查證成為預設行為之一部分，縮短風險知覺與實際防護行為之間的時間落差。

此外，為提升各界宣導效率與一致性，短期亦可同步推動識詐素材共享平臺之建置，提供標準化宣導文案、案例影片與圖卡，供企業、學校及社區單位免費使用。透過資源集中與品質控管，降低各單位自製成本並提高訊息識別度，並配合案例更新機制維持素材之情境貼近性，以降低宣導疲勞所造成的注意力流失。

中期階段，識詐策略宜由個別宣導進一步走向制度化與社會化支持。可推動社區防詐守門員計畫，培訓里長、社區志工、金融行員與學校教師等，成為高風險族群身邊的第一線諮詢與勸阻對象，使防詐提醒能更頻繁地出現在日常互動情境中。並可設置被害人協助中心，整合心理輔導、法律諮詢與追償指導，協助被害者復歸日常生活，同時在適當情境下，將被害經驗轉化為具警示功能的公共教育資源。

長期而言，識詐應納入正式教育與終身學習體系，使防詐不再只是臨時性宣導或專案活動，而是國民基本素養之一環。透過教育制度的穩定輸送與世代累積，逐步形塑全民共同承擔之防詐文化，使社會層次的自然監護功能得以長期且穩定地運作，並從根本上降低民眾暴露於假投資詐欺風險情境中的可能性。

二、堵詐面向

堵詐面向之重點，在於於犯罪腳本前端即強化封鎖與導流管制，使詐欺集團難以透過電信、社群、廣告與網站等管道有效接觸潛在被害人。短期階段，關鍵在於建立跨部會常設協調機制，以取代現行專案式、片段式防詐行動，確保政策具有連續性與整體性。建議

由行政院設立具決策權之跨部會防詐決策平臺，例如跨部會防制電信網路詐欺策略推動委員會，由政務委員擔任召集人，納入法務部、警政署、數位發展部、金管會與國家通訊傳播委員會等核心機關代表，統整政策方向、資源配置與跨域協調，避免各機關各自為政。

在運作設計上，該常設平臺可建構政策統籌、執行協調與資料整合三層架構。政策統籌層負責全國防詐策略與年度資源分配；執行協調層整合警政、金融、通訊與數位機關之行動計畫；資料整合層建立跨域通報與定期會報制度，使資訊共享與作業節奏一致。更重要者在於形成持續性問題回饋迴路，依問題導向警政思維，將基層實務觀察與偵查經驗制度化回饋至決策層，藉由定期收集地方問題、案件分析報告與成效評估結果，滾動調整政策工具與資源配置，縮短政策回應時間，並逐步形成中央整合、地方執行之垂直防制體系，強化政策一致性與連貫性。

另就網路監理端之授權與執行而言，短期可先修正行政執行規範與作業基準，強化現行管理策略之可操作性與即時性，並明確通報、下架、封鎖與復核之程序界線，使處置標準一致且可受檢驗。中期則可要求一定規模之網路業者落地設置在地代表或法遵窗口，確保主管機關得以就下架、保存證據與協助調查等事項進行實質溝通與履行要求。長期而言，可參照英國《線上安全法案》之防制思維，推動通訊軟體管理專法之立法方向，使高風險通訊與內容傳播服務之風險評估、系統性防護與配合義務得以制度化，並形成更穩定的監理架構。

中期階段，堵詐之防制重點可進一步延伸至制度化公私協力與業者責任，將社群平臺、搜尋服務與相關數位服務業者納入防詐防制架構中，透過法制化或增訂相關專章，要求數位平臺設置詐欺內容辨識系統，對官方通報或用戶檢舉之假投資廣告與可疑帳號，在一定期間內完成處置並回報結果；若怠於作為，則得科以行政罰並視情節加重，以提高平臺配合度與回應速度。另可發展防詐標章制度，對導入完整防詐機制與用戶教育功能之業者給予認證，透過公開評比與名單揭露形成企業間良性競爭，使平臺防制作為由被動配合轉為主動內建。

長期而言，堵詐面向亦可與跨境合作機制逐步銜接，對跨境詐欺廣告投放、境外網站鏡像與工具替換等現象形成更穩定的聯防節奏，以降低犯罪者透過跨域落差尋求替代通道之空間。

三、防詐面向

防詐面向係指涉超越單點阻斷之制度性預防，其核心在於透過防制架構、運作標準與資料規範之建構，使整體防制體系具備穩定運作與自我調整能力。於短期階段，除前述跨部會常設協調機制外，亦須在資訊流通與資料整合上形成具可操作性之制度安排。就此而言，建置跨域資料整合與 AI 警示平臺，正可作為防詐面向的重要制度基礎之一。建議整合警政署 165 報案系統、金管會警示帳戶資料、國家通訊傳播委員會通訊封鎖名單、數位發展部詐欺網站清單與金融機構異常交易紀錄，建置跨域 AI 防詐資料中心，透過統一格式與標準欄位進行交叉比對，以消除資訊隔閡並提升決策品質。

在資料運用層面，短期亦應同步導入 AI 模型與即時通報機制，偵測重複出現之電話號碼、網址、社群帳號或虛擬資產錢包等風險標的。一旦多源通報集中於同一標的，即可自動產出風險報告並推送至相關機關或合作業者，啟動暫時封鎖或金流凍結措施。平臺可採模組化設計，提供金融、電信及網路業者以 API 方式接入並即時取得警示資訊，以維持資訊同步與作業節奏一致。惟跨域整合過程中，亦須確立明確的資料防制規範，界定資料使用目的、保存期限與權責分工，以確保符合法制與個資保護要求；同時保留匿名化後之歷史資料，作為政策研究與學術分析之基礎，逐步形成可持續更新的防詐知識體系。透過上述制度化資料防制與跨域協作，防詐工作得以由臨時性專案轉為常態性防制，並提升整體體系之韌性與證據導向程度。

中期階段，防詐防制宜進一步朝制度化與科技化深化。可成立 AI 反詐防制中心，作為全國層級之科技中樞，整合前期所建置之資料平臺與偵查工具，專責 AI 模型研發、效能調校與防制規範制定，以因應詐欺手法持續科技化與模組化之趨勢。同時，應建立 AI 技術倫理與防誤判機制，採取可解釋模型、外部稽核與申訴修正流程，使技術運用在提升防制效能之餘，仍能兼顧程序正當性與人民權益。

長期而言，防詐防制可在行政院層級設立國家防詐防制體系，透過政策規劃、科技防制、國際合作與社會動員等功能分組，統籌中長程防詐策略與制度發展方向，並定期發布國家防詐白皮書與政策回饋機制，以確保防詐政策具備延續性、透明度與可檢驗性。透過此一制度化問題學習機制，防詐防制得以隨科技演進與犯罪態樣變遷持續調整，逐步建構具自我修正能力之長期防制架構。

四、阻詐面向

阻詐面向之核心，在於攔阻詐欺金流並追查犯罪所得，使詐欺犯罪不再具有高報酬、低風險之誘因結構。短期階段，可透過建置跨域資料整合與 AI 警示平臺，使防制焦點前移至犯罪腳本的早期階段，於誘導與互動過程中即啟動警示與阻斷機制，縮短偵查與攔阻時距。在警察執行層面，強化科技查緝能量與績效制度調整，亦為短期阻詐策略之重要環節。建議由刑事警察局設立打詐科技偵查中心，整合 AI 語意分析、區塊鏈追蹤、深偽影像比對與社群輿情分析等工具，作為全國科技查緝支援樞紐，協助地方單位進行金流路徑還原、境外機房鎖定與跨案資料串聯，以提升辦案效率與精準度。

為使警察組織行為誘因與抑制詐欺犯罪產業鏈之政策目標相符，短期內亦宜同步檢討並調整警政績效指標，將上游查緝率、犯罪所得凍結與追徵金額，以及跨國協查案件完成率納入考核項目並逐步提高其權重，引導查緝重心由末端車手轉向上游組織與核心金流。同時，可推動科技查緝能力提升方案，規劃中短程專業培訓，選訓一定比例員警接受 AI 分析、數據判讀與數位取證訓練，並引進具資安或資料科學背景之民間專業人員加入專案小組，形成人力與科技互補之混合型查緝團隊。透過科技偵查基礎建構與績效導向修正，可逐步提升結構性嚇阻效果，使犯罪者在成本與風險評估時，明確感知到上游參與與金流操作之風險顯著提高。

中期階段，阻詐策略須進一步結合跨境追訴與國際合作之深化，以回應詐欺集團跨境

設點與金流外移之實務現況。建議建立駐外警務聯絡官與專責窗口，並與外交及駐外機構形成常態化工作網絡，強化情資蒐集與案件協查效率；同時，可與金融監理制度較成熟之國家簽訂雙邊合作備忘錄，或探索多邊金流合作協定，明確可疑金流凍結流程、資料交換格式與作業時限，以提升跨境追贓與資金攔阻之實效。此外，亦可積極參與亞太反洗錢組織及國際刑警組織等平臺之聯合行動與情資共享計畫，借重國際專業與技術資源，提升國內阻詐政策與實務之國際接軌程度，並逐步改變犯罪者對境外設點作為安全避風港的主觀認知。

長期而言，阻詐面向可進一步與智慧警政與雲端分析能力銜接，透過即時金流監控、風險預測模型與跨國資料串聯，使金流攔阻與預警機制更為即時與精準，並逐步形塑跨境聯防之常態化運作節奏。藉由持續削弱詐欺犯罪之金流可得性與報酬結構，阻詐策略得以在整體防制體系中發揮穩定且長效的嚇阻功能。

五、懲詐面向

懲詐面向之目的，在於透過法制面補強與司法制度調整，確保防詐行動具備程序正當性與可執行性，並在量刑與財產刑層次強化整體嚇阻與追贓效果。短期階段，修法重點宜同時補足攔阻端執行人員之法律授權、提高犯罪人之懲罰強度，並同步強化被害人保護，使第一線人員得以在合法且可受檢驗之框架下採取即時且積極之處置。以立法院於 2025 年 12 月 30 日三讀通過之《詐欺犯罪危害防制條例》部分條文修正為例，其透過下修高額詐欺門檻並提高法定刑與罰金額度，採取累進式加重架構以回應重大財損案件之嚇阻需求，並同時授權金融機構及虛擬資產服務相關單位加速攔阻可疑金流，增訂禁奢條款及被害人保護相關設計，使嚇阻、追贓與被害回復得以在制度層次形成連動。

就攔阻端授權而言，該次修法明確賦予司法警察與檢察機關於調查需要下，得主動通知金融機構或提供虛擬資產服務之事業，將疑似涉及詐欺之存款帳戶、電子支付帳戶、信用卡或虛擬資產帳號列為警示並暫停交易功能，以有效縮短處置時距；就被害人保護而言，則以被告於自首或首次自白後一定期間內實質返還被害人財損，或達成調解（和解），作為法院裁量是否減免刑責之重要前提；另就犯罪所得使用之不當利益控制面向，則透過禁奢條款，將犯罪後仍從事豪奢、浪費之行為納入量刑考量，回應社會對公平正義與國民法律感情之期待。

前述修法方向，亦與本研究所提出之懲詐政策建議高度相符。其一，在程序與權責面，宜持續強化攔阻端執行人員之法律授權與免責設計，使第一線得以在明確法源基礎下採取即時處置，降低因法律風險顧慮而遲疑不前之情形。其二，在懲罰與財產刑面，除提高刑責與罰金額度外，亦應透過禁奢條款、沒收與追徵制度之常態化運作，削弱犯罪者對犯罪所得可保全之心理預期。其三，在金融授權面，則應持續建構可即時啟動、可事後檢證之攔阻流程與審查機制，使先行處置與後續覆核得以兼顧效率與程序正當性。

中期階段，建議進一步改革司法量刑與財產刑制度，從理性選擇觀點出發，系統性調整犯罪者對成本與報酬之評估結構，並持續強化犯罪所得追徵與沒收機制。實務上可採取先凍結、後審理、並行追徵之原則，於偵查初期即聲請凍結疑似犯罪所得，並將以贓款購

置之不動產、虛擬貨幣與高價資產納入沒收範圍，以落實人、錢並辦之政策精神。另可建置跨機關犯罪資產追查平臺或資料庫，結合金融監理機關與銀行資料，透過技術分析快速鎖定與追蹤犯罪資產流向。

長期而言，懲詐面向亦宜納入制度化之政策評估與問責機制，使量刑實務、追徵與沒收成效得以被穩定監測，並作為後續資源配置與制度修正之重要依據。透過持續提高詐欺犯罪之法律風險與經濟成本，並確保犯罪所得難以保全，懲詐策略方能在整體防制體系中發揮長期且穩定之嚇阻功能。

六、綜合建議

綜合而言，本研究依循打詐綱領 2.0 所揭示之五大面向防制策略及前述犯罪腳本分析可知，本研究所提出之短期、中期與長期政策建議，並非零散政策工具之羅列，而係一組對應詐欺犯罪前準備、前端接觸、中段互動與後端金流等不同階段之整合性防制設計。此一設計，旨在回應電信網路假投資詐欺犯罪高度組織化、模組化與可快速替換之運作特性，避免防制策略僅停留於單一節點，而遭犯罪者轉移工具與通道所削弱。

就整體政策鏈觀之，短期建議以制度整合與即時反應為核心，透過跨部會常設協調機制、跨域資料與 AI 警示平臺、科技查緝能量與績效改革、法源授權與免責條款，以及精準識詐與行為導向宣導等措施，補強現行防詐體系在資訊斷裂、權責分散與反應遲滯等結構性缺口。中期則進一步將上述作為制度化與科技化，透過 AI 反詐策略中心、公私協力制度化、跨境追訴與國際合作、司法量刑與財產刑改革，以及防詐教育與信任重建，使防制體系逐步具備自我調整與持續演進之能力。長期則以智慧警政與永續防詐為目標，透過國家層級防詐防制體系、智慧警政與 AI 治安防制、全民防詐共同體、區域合作網絡與政策評估機制，促使防詐工作由事件處理導向，轉向結構性防制與風險管理邏輯。

若進一步從犯罪腳本之早、中、晚期阻斷點加以對照，則可更清楚看出五大面向之互補性。識詐與堵詐主要作用於犯罪前準備及前端接觸與引流階段，透過高風險行為發生前之關鍵時點警示、平臺防制責任、接觸管道封鎖與監理措施，降低被害人暴露於詐欺場域之機率，並對犯罪前準備所倚賴之人頭門號、數位工具與通訊資源供給面形成結構性防制壓力。防詐面向則在中段提供制度整合與資料防制支撐，使跨機關協作與資訊共享得以常態化運作，提升有監控能力者到場密度與回應效能，避免詐欺互動在制度縫隙中持續深化。阻詐與懲詐則於後端針對金流分流與去識別化行為進行攔阻與追查，並透過量刑、禁奢、追徵與沒收制度，削弱犯罪報酬可得性，強化對上游組織與核心成員之實質嚇阻。

若再從情境犯罪預防之整合觀點加以審思，前述五面向所構成之政策組合，實質上即係透過提高犯罪風險、增加犯罪成本、降低犯罪報酬與壓縮合理化空間等多重機制，持續改變詐欺犯罪之情境條件，使詐欺犯罪產業鏈之運作成本上升、成功機率下降且所得可得性降低。當犯罪成本被制度化提高、報酬被有效剝奪，且社會中有監控能力者能於不同階段穩定到場並持續運作時，電信網路假投資詐欺之機會結構將被系統性壓縮，整體防制亦將更有可能由事後處罰逐步轉向事前預防，並由政府主導邁向全民共同防制之長期目標。

第三節 後續研究建議

本研究以電信網路假投資詐欺犯罪為核心議題，結合環境犯罪學中理性選擇、日常活動、犯罪腳本、問題導向警政與情境犯罪預防等理論，建構一套兼具解釋力、操作性與評估基礎之防制策略分析架構。研究結果顯示，假投資詐欺兼具跨境化、產業化與科技化特徵，其防制成效不僅取決於單一措施之強度，更深受跨部門策略協調、工具組合方式與科技應用落差之影響。然而，受限於研究設計與資料可得性，本研究在理論深化與實證資料廣度上仍有延伸空間。未來研究宜持續拓展研究方法與資料來源，強化跨國比較與實務資料之運用，並深化警察實務與政策分析之連結，以持續檢驗並修正防詐策略設計的可行性、適切性與長期穩定性。

一、研究方法與資料面向之延伸建議

(一)質性研究樣本的多元化與延伸

本研究以深度訪談與文件分析為主要研究方法，樣本涵蓋警察機關、防詐政策推動單位，以及金融與電信業者，已能呈現防詐制度的核心運作脈絡。然而，未來研究可進一步納入地方政府、社區組織、教育機構、媒體單位與被害人及其家屬等角色，以補足防詐策略中尚未充分呈現的社會層面。此一擴展有助於理解不同層級與角色在防詐網絡中的互動方式，並檢視「有能力監控者」在實務上如何透過正式與非正式管道參與防制行動，進一步評估其實際介入效果與制度支持條件。

(二)量化資料與跨部門數據結合之可行性

現行防詐量化研究多以案件數、通報量或財損金額為分析基礎，較少進行跨部門資料整合。未來研究可嘗試建構跨域防詐資料整合，整合警政報案資料、金融警示帳戶、通訊封鎖紀錄與涉詐網站資訊，形成具時間序列特性的防詐監測資料庫。此類資料不僅有助於趨勢分析，亦可用於評估政策介入前後的行為變化。此外，研究亦可引入社會網絡分析或空間分析方法，分析犯罪流程中金流、資訊流與社群互動的交互關係，進一步檢驗情境犯罪預防理論在數位環境中的適用性。

(三)跨國比較資料蒐集與制度分析深化

本研究已初步比較日本、新加坡、澳洲與英國的防詐策略，歸納其在打詐五面向上的制度特色。未來研究可進一步從制度比較與政策評估角度，系統性分析各國政策演化脈絡、策略架構與執行效果。例如，日本在高齡者防詐教育與地方聯防制度、新加坡的全政府合作模式，以及英國以金融體系為核心的防詐策略路徑，皆具高度比較價值。透過文件比對、外部專家訪談或國際資料合作，未來研究可更深入說明這些制度如何實際影響防詐策略的可行性與執行成效，並作為臺灣制度調整與在地化修正之參考。

二、理論面之深化與整合建議

(一)環境犯罪學理論的在地化修正與擴充

本研究以環境犯罪學相關理論解釋假投資詐欺的犯罪機會結構與防制節點，顯示其

理論適用性。然而，臺灣在數位經濟與社群使用情境上的特殊性，亦凸顯理論在地化修正的必要性。例如，理性選擇理論可進一步納入心理偏誤與風險認知差異，日常活動理論則可將演算法推薦與 AI 預警視為新型監控形態。此外，情境犯罪預防理論中的「增加阻力、提升風險、降低報酬、移除藉口」等原則，亦可延伸至數位平台與虛擬資產交易場域，形成更符合數位社會特性的犯罪預防模型，作為發展本土數位環境犯罪學的重要基礎。

(二)犯罪腳本與行為預測模型之結合

本研究歸納假投資詐欺犯罪腳本，顯示其運作模式具高度模組化與可複製性；且在詐欺犯罪正式展開之前，犯罪前準備階段即已完成組織建構、成員招募與技術工具配置，突顯制度性介入以提高犯罪起始門檻之重要性。未來研究可結合機器學習與行為序列分析，發展可辨識詐欺行為運作模式的分析工具，以協助提前發現異常行為。若能進一步整合警政與金融資料，並以圖像化方式呈現詐欺犯罪階段性運作中較易發生風險的關鍵運作環節，將有助於實務單位更直觀掌握高風險樣態，提升決策與資源配置之精準度，並強化 SARA 模式中「掃描」與「分析」階段的實證基礎。

(三)問題導向警政與政策循環機制的制度化

防詐工作本質上屬於問題導向警政的一環。未來研究可進一步探討 SARA 模式在防詐策略中的制度化條件，例如如何將問題導向分析納入常態考核、如何建立跨機關資料分析能力，以及如何以行為指標評估防詐成效。此外，亦可發展產官學合作的行動研究架構，透過工作坊或共學機制，促進前線警察與研究者共同歸納與修正政策工具，形成可持續運作的政策學習循環。

三、實務與制度研究方向

(一)跨部會合作模式的持續追蹤與評估

跨部會合作是防詐策略中的關鍵挑戰。未來研究可採制度追蹤方法，長期觀察防詐政策推動過程中各部會權責配置、資源流動與決策節點的變化，評估常設協調機制的實際成效。同時，可建構合作成熟度評估架構，從制度化層級與合作密度兩個面向，分析跨部會合作的發展階段，作為政策調整與制度優化的依據。

(二)科技建警與 AI 防詐策略之倫理與法制研究

隨著 AI 技術逐步導入防詐實務，雖可提升風險辨識與即時攔阻能力，但亦引發隱私保護、決策透明與誤攔風險等議題。未來研究可聚焦 AI 防詐策略，從公共安全與基本權利平衡角度，檢視公權力介入數位風險管理的正當性，並探討演算法透明度、責任歸屬與補救機制等制度設計。

(三)被害人復歸機制與社會支持系統之研究

被害人是防詐政策中長期需要關注的核心對象。未來研究可進一步探討被害人復歸的心理與制度機制，例如其如何重建財務安全感，或轉化為防詐倡議者。研究可採混合方法，結合問卷、焦點團體與行動研究，評估心理輔導、法律協助與追償支持等措施對被害人復原歷程的影響，使防詐策略由防堵導向逐步延伸至修復性策略。

第四節 研究限制

總體而言，本研究揭示電信網路假投資詐欺的成因與防制困境，提出以五大理論支撐的系統性防制架構。然詐欺犯罪產業鏈的快速演化，使防制研究必須具備動態更新能力。未來研究若能結合多源資料、理論整合與跨國比較，並落實問題導向警政的循環精神，將可進一步推動防詐研究邁向「理論深化、實證精準、政策連結」的新階段。最終目標，在於形塑一個以科學分析為基礎、以制度合作為核心、以社會信任為支撐的防詐知識體系，使「警察防制電信網路詐欺犯罪策略」之研究，成為連結理論、實務與政策三者的永續學術典範。然而本研究仍有未竟之處，包括：

一、研究地區限制

本研究之區域為臺灣地區，本應含括臺灣本島、澎湖、金門、馬祖等臺灣主權所及的地區，然受限於質性立意抽樣方法與撙節人、物力等考量，故研究區域僅及於樣本所在地，至於非樣本所在的地區，則不屬本研究調查地區之範圍。

二、資料蒐集方法限制

由於本研究係採質性訪談方式為之，故僅能調查受測對象個體本身的想法或認知，正因調查樣本的數量有其侷限性，因此本研究結果並無法概括地類推適用到其他同類群體。

三、詐欺犯罪類型限制

因本研究係以電信網路假投資詐欺犯罪為研究類型，故本研究深度訪談所發現之相關成果，僅可作為解釋是類犯罪，然對於其他犯罪在解釋上恐存有扞格之處。

四、研究對象限制

本研究受限於人、物力，係以臺灣刑事警察人員為主要研究對象，雖輔以訪談部分「行政院打擊詐欺指揮中心」督導各部會執行防制詐欺策略人員及相關民間業者，但仍難以代表臺灣所有行政機關與民間企業的防制策略，因此本研究結果並不適合類推到其他行政機關與民間企業。

五、外在效度限制

本研究採深度訪談法，訪談對象以實際參與電信網路詐欺案件偵辦與防制之第一線警察人員為主，其經驗有助於掌握假投資詐欺之實務運作。然而，受訪者所見多限於已報案或已進入偵查程序之案件，較能反映犯罪被揭露後之樣態，對於尚未被發現或未進入司法體系之詐欺活動，其掌握相對有限。此外，警察觀點以執法實務為核心，對被害人未報案前之心理歷程及詐欺集團內部運作，仍多屬間接理解，故研究發現之推論仍須審慎解讀。

參考文獻

一、中文部分

內政部警政署(2022a)。警政署署務會報資料。臺北：內政部警政署。

內政部警政署(2022b)。2022 國際警察合作論壇—後疫情時代打擊跨境電信詐欺犯罪研討會議資料。臺北：內政部警政署。

內政部警政署(2024)。165 全民防騙網。取自：https://165.npa.gov.tw/#/，最後瀏覽日期：2024 年 9 月 25 日。

內政部警政署(2025a)。警政統計查詢網。取自：https://ba.npa.gov.tw/statis/webMain.aspx?k=defjsp，最後瀏覽日期：2025 年 4 月 18 日。

內政部警政署(2025b)。內政部警政署 165 全民防騙網。取自 https://165.npa.gov.tw/#/article/C/1351，最後瀏覽日期：2025 年 11 月 24 日。

內政部警政署(2025c)。165 打詐儀錶板。取自 https: https://165dashboard.tw/，最後瀏覽日期：2025 年 8 月 1 日。

內政部警政署 165 全民防騙臉書(2024)。前 5 大詐欺手法。取自：165.npa.gov.tw。最後瀏覽日期：2024 年 5 月 14 日。

內政部警政署刑事警察局（2000-2024）。刑案紀錄表（內部統計資料）。

內政部警政署刑事警察局(2024)。回應社論報導「展現執行力 剷除詐欺王國惡名」一警政署推動打詐專法抑制詐欺犯罪。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1886&serno=1f208fde-f54f-40b8-a729-37c3e9a0505c，最後瀏覽日期：2024 年 5 月 30 日。

內政部警政署刑事警察局(2025)。犯罪預防寶典：常見詐騙手法話術解析與因應之道。取自 https://www.cib.npa.gov.tw/ch/app/data/view?module=wg116&id=1909&serno=a4f8d5ab -3d53-4d22-9411-031fddde7a4e，最後瀏覽日期：2025 年 11 月 24 日。

田明府、黃麒然（2019）。165 反詐欺諮詢專線防詐機制探討。CyberSpace 2019 數位治理、數位創新、數位健康與數位城市聯合研討會。臺北：銘傳大學。

行政院(2022)。2022 年 6 月 21 日行政院 111 年第 3 次治安會報會議資料。臺北：行政院。

行政院(2023)。新世代打擊詐欺策略行動綱領 1.5 版。取自：https://www.moj.gov.tw/media/26683/ 15-% E4% BF%AE.pdf?mediaDL=true，最後瀏覽日期：2025 年 6 月 19 日。

行政院(2024)。新世代打擊詐欺策略行動綱領 2.0 版。取自：https://www.ey.gov.tw/Page/9277F759E41CCD91/526a9b40-50cb-49e7-83a9-e8c49a1475ed，最後瀏覽日期：2025 年 6 月 20 日。

行政院(2025)。立法院第 11 屆第 3 會期，2025 年 8 月 15 日，「新世代打擊詐欺策略行動綱領 2.0 執行成效專案報告」。取自：https://www.ey.gov.tw/File/ABB8FF7CEB3F71C9，最後瀏覽日期：2025 年 10 月 25 日。

何招凡(2010）。臺越警方首度合作打擊兩岸詐欺集團。刑事雙月刊，第 38 期，頁 4-8。

何招凡(2018)。全球執法合作：機制與實踐。臺北市：元照出版公司。

李安明(2016)。從教育領域的質性研究談研究倫理議題。教育研究月刊，第 272 期，頁 30-43。臺北市：高等教育出版公司。

李郁薇(2017)。打擊詐欺犯罪現況與具體策進作為。刑事雙月刊。第 76 期，頁 4-7。

李堅志(2010)。從臺泰合作經驗分析探討打擊兩岸跨境電信詐欺犯罪策略。刑事雙月刊 38 期，頁 9-15。

李彩溱(2024 年)。防制金融投資詐欺。全球合作暨訓練架構「打擊跨境詐欺犯罪」國際研習營。臺北市。

李雅村(2024)。國際警察打擊跨境犯罪機制之法制研究。立法院法制局專題研究報告。臺北市：立法院法制局。

汪子錫、葉毓蘭(2013)。跨境詐欺犯罪的類型與治理分析。探索與展望。第 11 卷第 3 期，頁 67-90。

孟維德(2010)。國際警察合作與跨國犯罪防制。桃園市：中央警察大學。

孟維德(2011a)。犯罪分析與安全治理（增訂第四版）。臺北市：五南圖書出版股份有限公司。

孟維德(2011b)。犯罪熱點與犯罪預防。警學叢刊，第 42 卷 3 期，頁 1-34。

孟維德(2015)。跨國犯罪（修訂第三版）。臺北市：五南圖書出版公司。

孟維德(2016)。從情境預防犯罪探討跨境犯罪—以 Call 戀愛詐欺為例。涉外執法與政策學報，第 6 期，頁 107-138。

孟維德(2019)。組織犯罪跨國蔓延之分析。涉外執法與政策學報，第 9 期，頁 1-27.。

林建隆(2024)。雙面刃-電信及網路科技如何助長詐欺犯罪激增。2024 國際警察合作論壇-打擊跨境詐欺犯罪研討會，臺北市。

林德華(2009)。海峽兩岸共同打擊跨境詐欺犯罪對策探討，第四屆海峽兩岸暨香港、澳門警學研討會。臺北市市：社團法人中華民國刑事偵防協會。

林德華(2010)。防制電信網路跨境詐欺犯罪新策略，第五屆海峽兩岸暨香港、澳門警學研討會。江蘇：中國警察協會。

林德華(2012)。兩岸共同打擊跨境有組織集團犯罪防制對策。第七屆海峽兩岸暨香港、澳門警學研討會。澳門：澳門警察總局。

法務部(2024)。「打詐四法三讀，展開打詐新篇章全面查緝詐欺犯罪，落實罪贓返還，完善被害保護」。法務部檢察司 113 年 7 月 17 日新聞稿。取自：https://www.moj.gov.tw/media/29382/1130717%E6%B3%95%E5%8B%99%E9%83%A8%E6%96%B0%E8%81%9E%E7%A8%BF-%E6%89%93%E8%A9%90%E5%9B%9B%E6%B3%95%E4%B8%89%E8%AE%80.pdf?mediaDL=true，最後瀏覽日期：2025 年 11 月 4 日。

柯宏宜(2010)。警政署 165 反詐欺諮詢專線流程再造之研究。玄奘大學公共事務管理學系碩士論文，未出版、新竹市。

洪瑞斌、莊騏嘉、陳筱婷(2015)。深思敘說研究之研究倫理議題：回到倫理學基礎探討。生命敘說與心理傳記學，第 3 輯，頁 55-79。

張榮興(2024 年 9 月 10 日)。臺灣防制詐欺犯罪經驗-金融、電信與數位經濟管理措施。2024 國際警察合作論壇-打擊跨境詐欺犯罪研討會，臺北市。

許春金(2007)。慢性犯罪者與犯罪理論。中央警察大學犯罪防治學報。第 8 期，頁 1-20。

許福生(2018)。犯罪學與犯罪預防。臺北市：元照出版股份有限公司。

陳玉書、曾百川 (2007)。網路詐欺犯罪理性選擇歷程之質性分析。犯罪防治學報，第 8 期，頁 115-145。

曾雅芬(2016)。行騙天下：臺灣跨境電信詐欺犯罪網絡之分析。國立政治大學國家發展研究所博士論文，未出版，臺北市。

黃光甫(2023)。跨境詐欺犯罪的脈絡與歷程-犯罪成因、網絡與生活型態之分析。國立中正大學犯罪防治學系暨研究所博士論文，未出版，嘉義。

黃國師(2024)。打詐專法立法分析。警政與警察法相關圓桌論壇。第 68 場。中華警政研究學會主辦。取自：http://www.acpr.org.tw/PDF/Panel_20240809_the%20legal%20evaluation%20of%20new%20anti-fraud%20relative%20acts.pdf，最後瀏覽日期：2025 年 6 月 19 日。

黃國師（2024）。數位科技詐欺與洗錢防制。2024 國際警察合作論壇-打擊跨境詐欺犯罪研討會，臺北市。

黃翠紋、孟維德(2017)。警察與犯罪預防（增訂第二版）。臺北市：五南圖書出版股份有限公司。

黃翠紋、蘇信雄(2020)。跨境電信網路詐欺犯罪之防制。黃文志、王寬弘主編。國境執法與合作，頁 477-516。臺北市：五南圖書出版股份有限公司。

塗凱竣(2020)。電信網路詐欺犯罪與偵查之研究-以假冒公務員面交車手詐欺集團為核心。中央警察大學犯罪防治學報。第 29 期，頁 37-72。桃園市：中央警察大學。

楊士隆、曾淑萍、周子敬、李政曉(2007)。詐欺犯罪防制策略之成效評估研究。內政部警政署刑事警察局委託研究報告，未出版，臺北市。

楊士隆、鄭瑞隆、許華孚、馬躍中(2024)。112 年全年度臺灣民眾對司 法與犯罪防制滿意度進行電訪調查研究。取自：https://www.facebook.com/CCUdeptcrmofficial/最後瀏覽日期：2024 年 9 月 6 日。

詹志文、吳柏寬（2017）。大數據析在打擊跨境電信詐欺犯罪之應用與成效。第十二屆海峽兩岸暨香港、澳門警學研討會。澳門：澳門警察總局。

蔡田木(2009)。兩岸詐欺犯罪趨勢與防制對策之探討。展望與探索月刊。第 7 卷第 7 期，頁 86-95。

蔡田木、陳永鎮(2006)。新興詐欺犯罪趨勢與防治對策之探討。犯罪防治學報，第 7 期，頁 309-331。

蔡甫昌、林芝宇、張至寧(2008)。研究倫理的歷史、原則與準則。臺灣醫學，第 12 卷，第 1 期，頁 107-122。

蔡德輝、楊士隆(2019)。犯罪學。臺北市：五南圖書出版股份有限公司。

鄧煌發(2010)。淺析海峽兩岸跨境詐欺犯罪。展望與探索月刊。第 8 卷第 8 期，頁 74-78。

鄭嘉慶(2024)。臺灣對防制投資詐欺之作為。全球合作暨訓練架構「打擊跨境詐欺犯罪」國際研習營，臺北市。

盧俊光(2007)。新興詐欺犯罪模式及其偵查作為之研究。中央警察大學刑事警察研究所碩士論文，未出版，桃園市。

賴鼎銘、范巽綠、趙永清、葉宜津、林文程、賴振昌、王麗珍(2024)。112 年「政府防制電信網路詐欺之對策與檢討」通案性案件調查研究。監察院調查研究報告。臺北市：監察院。

賴擁連、蔡田木、陳玉書、許春金、葉碧翠(2023)。台灣網路詐欺被害調查與防制研究。法務部司法官學院委託研究，未出版，臺北市。

羅婉云、章英華、于若蓉(2017)。國外政府調查與行政資料庫範例—英國國家資料庫。人文與社會科學簡訊 18 卷 4 期，頁 145-155。

蘇信雄(2020)。查緝跨境電信網路詐欺犯罪績效影響因素之研究。執法新知論衡，第 16 卷第 1 期，頁 31-522。

蘇信雄(2022)。電信網路詐欺犯罪機房跨境蔓延之研析。中央警察大學學報，第 59 期，頁 23-52。

二、英文部分

Aichhorn, A. (1935). *Wayward youth*. New York, NY: Viking Press.

ALLEN & GLEDHILL (2023). *IMDA Implements Mandatory Registration with Singapore SMS Sender ID Registry from 31 January 2023*. Retrieved from: https://www.allenandgledhill.com/sg/publication/articles/23255/imda-implements-mandatory-registration-with-sms-sender-id-registry-from-31-january-2023，Last viewed date: October 8, 2024.

Anderson, J. R. (1983). A spreading activation theory of memory. *Journal of Verbal Learning and Verbal Behavior*, 22(3), 261-295.

Augoustinos, M., Walker, I., & Donaghue, N. (2006). *Social Cognition: An Integrated introduction* (2nd ed.). London: Sage.

Australian Banking Association (2023). *Banks Unite to Declare War on Scammers*. Retrieved from: https://www.ausbanking.org.au/new-scam-safe-accord/，Last viewed date: October 3, 2024.

Australian Bureau of Statistics (2024). *Crime and Justice: Personal Fraud*. Retrieved from: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/2022-23 ， Last viewed date: November 3, 2025.

Australian Bureau of Statistics (2025). *Crime and Justice: Personal Fraud*. Retrieved from: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/2023-24#victimisation-summary，Last viewed date: November 3, 2025.

Australian Competition and Consumer Commission (2025). *Targeting Scams: Report of the National Anti-Scam Centre on scams data and activity 2024*. Retrieved from: https://www.

accc.gov.au/system/files/targeting-scams-report-2024.pdf，Last viewed date: November 3, 2025.

Australian Government (2022). *New Rules to Fight SMS Scams*. Retrieved from: https://www.acma.gov.au/articles/2022-07/new-rules-fight-sms-scams，Last viewed date: October 3, 2024.

Australian Government (2023). *Action on Telco Consumer Protections*. Retrieved from: https://www.acma.gov.au/publications/2024-02/report/action-telco-consumer-protections-october-december-2023，Last viewed date: October 3, 2024.

Australian Government (2024). *Scam Statistics*. Retrieved from: https://www.nasc.gov.au/scam-statistics，Last viewed date: October 1, 2024.

Australian Securities and Investments Commission (2023). *Investor Alert List*. Retrieved from: https://moneysmart.gov.au/check-and-report-scams/investor-alert-list，Last viewed date: October 2, 2024.

Australian Securities and Investments Commission (2024). *ASIC Shuts Down Nearly 3,500 Scam Websites, Steps Up Surveillance in Push to Protect Consumers*. Retrieved from: https://asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-037mr-asic-shuts-down-nearly-3-500-scam-websites-steps-up-surveillance-in-push-to-protect-consumers/ ，Last viewed date: October 2, 2024.

Baldwin, M. W. (1992). Relational schemas and the processing of social information. *Psychological Bulletin*, 112, 461-484.

Baldwin, M. W. (1995). Relational schemas and cognition in close relationships. *Journal of Social and Personal Relationships*, 12, 547-552.

Boba, R. (2003). *Problem Analysis in Policing*. Washington, DC: Police Foundation.

Boba, R., & Santos, R. (2011). *A police Organizational Model for Crime Reduction: Institutionalizing Problem-Solving, Analysis, and Accountability*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Borrion, H. (2013). Quality assurance in crime scripting. *Crime Science*, 2, 6. Retrieved from: http://www.crimesciencejournal.com/content/2/1/6，Last viewed date: June 3, 2024.

Braga, A., Kennedy, D., Waring, E., & Piehl, A. (2001). Problem-oriented policing, deterrence, and youth violence: An evaluation of Boston's Operation Ceasefire. *Journal of Research in Crime & Delinquency*, 38(3), 195-225.

Brantingham, P. J., & Brantingham, P. L. (1991). Introduction: The dimensions of crime. In P. Brantingham & P. Brantingham (eds.), *Environmental Criminology* (2nd ed.), 7-26. Prospect Heights, IL: Waveland Press.

Brantingham, P. J., & Brantingham, P. L. (eds.) (1981). *Environmental Criminology*. Beverly Hills, CA: Sage.

Chiu, Y.-N., Leclerc, B., & Townsley, M. (2011). Crime script analysis of drug manufacturing in clandestine laboratories: Implications for strategic intervention. *British Journal of*

Criminology, 51, 355-374.

Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice*, 4, 225-256.

Clarke, R. V. (1992). *Situational Crime Prevention: Successful Case Studies*. Harrow and Heston.

Clarke, R. V. (1995a). *Situational Crime Prevention*. New York, NY: Harrow and Heston.

Clarke, R. V. (1995b). *Situational Crime Prevention. Crime and Justice*, 19, 91-150.

Clarke, R. V. (1997a). *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Monsey, NY: Criminal Justice Press.

Clarke, R. V. (1997b). *Problem-Oriented Policing and the Potential Contribution of Criminology*. National Institute of Justice, U.S. Department of Justice.

Clarke, R. V. (2016). Situational crime prevention. In R. Wortley & M. Townsley (eds.), *Environmental Criminology and Crime Analysis* (2nd ed., pp. 286–303). London: Routledge.

Clarke, R. V. (ed.) (1997c). *Situational Crime Prevention: Successful Case Studies*. Harrow and Heston.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. In M. Tonry & N. Morris (eds.), *Crime and Justice: An Annual Review of Research*, Vol. 6 (pp. 147-185). Chicago, IL: University of Chicago Press.

Clarke, R. V., & Eck, J. (2003). *Become a Problem-Solving Crime Analyst: In 55 Steps*. London: Jill Dando Institute of Crime Science, UCL.

Clarke, R. V., & Eck, J. (2016). *Crime Analysis for Problem Solvers in 60 Small Steps*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Clarke, R. V., & Felson, M. (eds.) (2004). *Routine Activity and Rational Choice*. Transaction Publishers.

Clarke, R. V., & Goldstein, H. (2002). Reducing theft at construction sites: Lessons from a problem-oriented project. In N. Tilley (ed.), *Analysis for Crime Prevention*. *Crime Prevention Studies*, Vol. 13 (pp. 89-130). Monsey, NY: Criminal Justice Press.

Clarke, R. V., & Homel, R. (1997). A revised classification of situational crime prevention techniques. In S. P. Lab (ed.), *Crime prevention at A Crossroads* (pp. 17-26). Cincinnati, OH: Anderson.

Clarke, R. V., & Weisburd, D. (1990). On the distribution of deviance. In D. M. Gottfredson & R. V. Clarke (eds.), *Policy and Theory in Criminal Justice*. Aldershot, UK: Avebury.

Clarke, R.V. & Eck, J.E. (2005) *Crime Analysis for Problem Solvers in 60 Small Steps.* Washington, DC: Office of Community Oriented Policing Services, US Department of Justice.

Clarke, R.V. & Goldstein, H. (2003) Thefts from Cars in Center-city Parking Facili- ties: A Case Study in Implementing Problem-oriented Policing, in J. Knutsson (ed.) *Problem-Ooriented*

Policing: From Innovation to Mainstream Crime Prevention Studies, Vol. 15. Monsey, NY: Criminal Justice Press, pp. 257-298.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588-608.

Colvin, M. (2000). *Crime and Coercion: An Integrated theory of Chronic Criminality*. New York, NY: St. Martin's Press.

Commonwealth Bank of Australia (2023). *Name Check*. Retrieved from: https://www.commbank.com.au/support/security/namecheck.html and https://www.westpac.com.au/about-westpac/media/media-releases/2023/5-March/，Last viewed date: October 3, 2024.

Cordner, G. (1986). Fear of crime and the police: An evaluation of a fear-reduction strategy. *Journal of Police Science and Administration*, 14, 223–233.

Cornish, D. B. (1994a). Crimes as scripts. In D. Zahm & P. Cromwell (eds.), *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis* (pp. 30-45). Tallahassee, FL: Florida Statistical Analysis Center, Florida Criminal Justice Executive Institute, Florida Department of Law Enforcement.

Cornish, D. B. (1994b). The procedural analysis of offending, and its relevance for situational prevention. In R. V. Clarke (ed.), *Crime Prevention Studies*, Vol. 3 (pp. 151-196). Monsey, NY: Criminal Justice Press.

Cornish, D. B., & Clarke, R. V. (2016). The rational choice perspective. In R. Wortley & M. Townsley (eds.), *Environmental Criminology and Crime Analysis* (2nd ed., pp. 29-61). London: Routledge.

Doyle, E., & Buckley, P. (2017). Embracing qualitative research: A visual model for nuanced research ethics oversight. *Qualitative Research*, 17(1), 95-117.

Eck, J. (2003). Police problems: The complexity of problem theory, research and evaluation. *Crime Prevention Studies*, 15, 79-114.

Eck, J. (2016). *Assessing Responses to Problems: An Introductory Guide for Police Problem-Solvers*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Eck, J. E. (1995). A general model of the geography of illicit retail marketplaces. *Crime and Place*, 4, 67-93.

Eck, J. E., & Clarke, R. V. (2013). *Intelligence Analysis for Problem Solvers*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Eck, J. E., & Madensen, T. (2012). Situational crime prevention makes problem-oriented policing work. In N. Tilley & G. Farrell (eds.), *The Reasoning Criminologist* (pp. 89-92). London: Routledge.

Eck, J. E., & Spelman, W. (1987). *Problem-Solving: Problem-Oriented policing in Newport News*. Washington, DC: Police Executive Research Forum.

Ekblom, P., & Gill, M. (2016). Rewriting the script. *European Journal on Criminal Policy and*

Research, 22, 319-339.

Emig, M., Heck, R., & Kravitz, M. (1980). *Crime Analysis: A Selected Bibliography*. Washington, DC: U.S. National Criminal Justice Reference Service.

Felson, M. (2002). *Crime and Everyday Life* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Felson, M. (2003). The process of co-offending. In M. J. Smith & D. B. Cornish (eds.), *Theory for Practice in Situational Crime prevention*. *Crime Prevention Studies*, Vol. 16 (pp. 149-167). Monsey, NY: Criminal Justice Press.

Felson, M. (2006). Crime and Nature. Sage Pub.

Felson, M., & Clarke, R. V. (1998). *Opportunity Makes the Thief*. London, UK: UK Home Office.

Fiske, S. T., & Taylor, S. E. (1991). *Social Cognition* (2nd ed.). New York, NY: McGraw-Hill.

Gilmour, N. (2014). Understanding money laundering. *The European Review of Organised Crime*, 1(2), 35-56.

Gilmour, S. (2014). Using crime script analysis to understand money laundering activities. *Trends & Issues in Crime and Criminal Justice*, (473), 1-8.

Glueck, S., & Glueck, E. (1950). *Unraveling juvenile Delinquency*. Cambridge, MA: Harvard University Press.

Goldstein, H. (1977). *Policing a Free Society*. Cambridge, MA: Ballinger.

Goldstein, H. (1979). Improving policing: A problem-oriented approach. *Crime & Delinquency*, 25(2), 236-258. https://doi.org/10.1177/001112877902500207

Goldstein, H. (1990). *Problem-Oriented Policing*. New York, NY: McGraw-Hill.

Goldstein, H. (2001). *Problem-Oriented Policing in a Nutshell*. Presentation at the International Problem-oriented Policing Conference, San Diego, CA.

Goldstein, H., & Susmilch, C. E. (1982a).*The Drinking Driver in Madison: A Study of the Problem and the Communitys Response*. Retrieved from: www.popcenter.org/library/researcherprojects/DevelopmentofPOPVolII.pdf，Last viewed date: June 20, 2024.

Goldstein, H., & Susmilch, C. E. (1982b). *The Repeat Sexual Offender in Madison: A Memorandum on the Problem and the Community's Response*. Madison, WI: University of Wisconsin Law School.

Goldstein, H., & Susmilch, C. E. (1982c). *Experimenting with the Problem-Oriented Approach to Improve Police Service: A Report and Some Reflections on Two Case Studies*.. Madison, WI: University of Wisconsin Law School.

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

GOV.UK（2023）。*Policy Paper Fraud Strategy: Stopping Scams and Protecting the Public* (accessible) Updated 1 June 2023（This was published under the 2022 to 2024 Sunak Conservative government）。Retrieved form:https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public，Last viewed date：November 3, 2025

Guerette, R. T. (2009). The pull, push, and expansion of situational crime prevention evaluation. In J. Knutsson & N. Tilley (eds.), *Evaluating Crime Reduction Initiatives*. *Crime Prevention Studies*, 24, 29-58.

Hardy, J., Bell, P., & Allan, D. (2020). A crime script analysis of the Madoff investment scheme. *Crime Prevention and Community Safety*, 22(1), 68-97.

Hawley, A. H. (1950). *Human ecology: A Theory of Community Structure*. United States: Ronald Press Company.

Herrnstein, R. J. (1990). Rational choice theory: Necessary but not sufficient. *American Psychologist*, 45(3), 356–367.

Hewstone, M. (1989). *Causal Attribution: From Cognitive Processes to Collective Beliefs*. Oxford, UK: Blackwell.

Hirschfield, A. (2005). *Analysis for Prevention. In N. Tilley (ed.), Handbook of Crime Prevention and Community safety*. Cullompton, UK: Willan Publishing.

Hoare, M. A., Stewart, G., & Purcell, C. M. (1984). *The Problem-Oriented Approach: Four pilot studies*. London: Metropolitan Police, Management Services Department.

Jeffery, C. R. (1971). *Crime prevention through environmental design*. Beverly Hills, CA: Sage.

Jones, E. E. (1979). The rocky road from acts to dispositions. *American Psychologist*, 34, 107–117.

Katz, J. (1988). *Seductions of Crime*. New York, NY: Basic Books.

Kennedy, D. (2009). *Deterrence and Crime Prevention: Reconsidering the Prospect of Sanction*. London: Routledge.

Klingele, C., Scott, M. & Dickey, W. (2010) '*Reimagining Criminal Justice*', Wisconsin Law Review, 4,953-998.

Leclerc, B. & Reynald, D. (2015). When scripts and guardianship unite: A theoreti- cal script model to facilitate intervention by capable guardians. *Security Journal*,30,793-806.

Leclerc, B. (2013a). New developments in script analysis for situational crime prevention. In B. Leclerc & R. Wortley (eds.), *Cognition and Crime: Offender Decision-Making and Script Analyses* (pp. 221-236). London: Routledge.

Leclerc, B. (2013b). Script analysis for crime controllers. In S. Caneppele & F. Calderoni (eds.), *Organized Crime, Corruption, and Crime Prevention* (pp. 13–20). New York, NY: Springer.

Leclerc, B. (2016). Crime scripts. In R. Wortley & M. Townsley (eds.), *Environmental Criminology and Crime Analysis* (2nd ed., pp. 119-141). London: Routledge.

Loeber, R. (1990). Development and risk factors of juvenile antisocial behavior and delinquency. *Clinical Psychology Review*, 10(1), 1-41. https://doi.org/10.1016/0272-7358(90)90105-J

Maguire, M. & Hopkins, M. (2003) 'Data and Analysis for Problem-solving: Alcohol- related Crime in Pubs, Clubs and the Street', in K. Bullock and N. Tilley (eds) Crime Reduction and Problem-oriented Policing (pp126-153) Cullompton, UK: Willan Publishing.

Marcus Felson（2016）. The routine activity theroy . In R. Wortley & M.Townsley, M. (Eds.),*Environmental Criminology and Crime Analysis (2 nd ed)*（pp.87-97）.London: Routledge.

Mayhew, P., Clarke, R. V., Sturman, A., & Hough, J. M. (1976). *Crime as Opportunity*. Home Office Research Study No. 34. London: Home Office.

Mintzberg, H. (1987). The strategy concept I: Five Ps for strategy. *California Management Review*, 30(1), 11-24. https://doi.org/10.2307/41165263

Mintzberg, H. (1994). *The Rise and Fall of Strategic Planning*. New York, NY: Free Press.

Mischel, W. (1968). *Personality and Assessment*. New York, NY: Wiley.

Moreto, W. M., & Clarke, R. V. (2013). Script analysis of the transnational illegal market in endangered species. In B. Leclerc & R. Wortley (eds.), *Cognition and Crime: Offender Decision-Making and Script Analyses* (pp. 209-220). London: Routledge.

Morgenthaler, E., & Leclerc, B. (2023). Crime script analysis of drug importation into Australia facilitated by the dark net. *Global Crime*, 24(3), 169-194.

Morgenthaler, S., & Leclerc, B. (2023). Using crime script analysis to identify crime prevention points in darknet drug trafficking cases in Australia. *Crime Prevention and Community Safety*, 25(2), 105–124. https://doi.org/10.1057/s41300-023-00167-7

Morselli, C., & Roy, J. (2008). Brokerage qualifications in ringing operations. *Criminology*, 46(1), 71–98.

Newman, O. (1972). *Defensible space: Crime Prevention Through Urban Design*. New York, NY: Macmillan.

Office for National Statistics (2022a). *Crime in England and Wales: Year Ending December 2021*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date: November 3, 2024.

Office for National Statistics (2022b). *Crime in England and Wales: Appendix Tables*. Retrieved from:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date: November 3, 2024.

Office for National Statistics (2023a). *Crime in England and Wales: Year Ending December 2022*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2022，Last viewed date: November 3, 2024.

Office for National Statistics (2023b). *Crime in England and Wales: Appendix Tables*. Retrieved from:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date: November 3, 2024.

Office for National Statistics (2024a). *Crime in England and Wales: Year Ending December 2023*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2023，Last viewed date: November 3, 2025.

Office for National Statistics (2024b). *Crime in England and Wales: Appendix Tables*. Retrieved from:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date: November 3, 2025.

Office for National Statistics (2025a). *Crime in England and Wales: Appendix Tables*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2024，Last viewed date: November 3, 2025.

Office for National Statistics (2025b). *Crime in England and Wales: Appendix Tables*. Retrieved from:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables，Last viewed date: October 31, 2025.

Optus (2023). *Optus Call Stop to Fight off SMS Scams*. Retrieved from: https://www.optus.com.au/about/media-centre/media-releases/2023/07/optus-call-stop-to-fight-off-sms-scams，Last viewed date: October 3, 2024.

Peak, K. J., & Glensor, R. W. (2008). *Community Policing and Problem Solving: Strategies and practices (5th ed)*. Pearson Prentice Hall.

Pfohl, S. (1994). *Images of Deviance and Social Control: A Sociological History* (2nd ed.). New York, NY: McGraw-Hill.

Ross, L. (1977). The intuitive psychologist and his shortcomings. In L. Berkowitz (ed.), *Advances in Experimental Psychology*, Vol. 10 (pp. 173–220). New York, NY: Academic Press.

Rumelhart, D. E. (1980). On evaluating story grammars.

Ruth, H., & Reitz, K. (2003). *The Challenge of Crime: Rethinking Our Response*. Cambridge, MA: Harvard University Press.

Sampson, R. J., & Laub, J. H. (1993). *Crime in the Making: Pathways and Turning Points Through Life*. Cambridge, MA: Harvard University Press.

Savona, E.U. (2010). Infiltration by Italian organized crime (Mafia, N'drangheta and Camorra) of the public construction industry. In K. Bullok, R.V. Clarke and N. Tilley (Eds.), *Situational Prevention of Organized Crimes* (pp. 130-150). Devon, UK: Willan Publishing.

Savona, E.U., Giommoni, L., and Mancuso, M. (2013). Human trafficking for sexual exploitation in Italy. In B. Leclerc and R. Wortley (Eds.) *Cognition and Crime: Offender Decision-Making and Script Analyses* (pp. 140-163). Crime Science Series, London: Routledge.

Schank, R., & Abelson, R. P. (1977). *Scripts, Plans, Goals and Understanding*. Hillsdale, NJ: Erlbaum.

Scott, M. S., Eck, J. E., Knutsson, J., & Goldstein, H. (2016). Crime scripts. In R. Wortley & M. Townsley (eds.), *Environmental Criminology and Crime Analysis* (2nd ed., pp. 227-258). London: Routledge.

Scott, M., & Goldstein, H. (2005). *Shifting and Sharing Responsibility for Public-Safety Problems*. Problem-oriented Guides for Police, Response Guide Series No. 3. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Scott, M., & Goldstein, H. (2012). Ron Clarke's contribution to improving policing. In N. Tilley & G. Farrell (eds.), *The Reasoning Criminologist* (pp. 93-107). London: Routledge.

Sherman, L.W. (2013) 'The Rise of Evidence-based Policing: Targeting, Testing, and Tracking', *Crime and Justice*, 42(1): 377–451.

Siegel, L. J. (2007). *Criminology: Theories, Patterns, Typologies* (9th ed.). Thomson Wadsworth.

Singapore Police Force (2022). *Annual crime brief 2021*. Retrieved from: https://www.police.gov.sg/Media-Room/Statistics?page=2，Last viewed date: September 20, 2024.

Singapore Police Force (2023). *Annual Scams and Cybercrime Brief 2022*. Retrieved from: https://www.police.gov.sg/Media-Room/Statistics?page=2，Last viewed date: September 20, 2024.

Singapore Police Force (2024). *Annual Scams and Cybercrime Brief 2023*. Retrieved from: https://www.police.gov.sg/Media-Room/Statistics?page=2，Last viewed date: September 20, 2024.

Singapore Police Force (2025). *Annual Scams and Cybercrime Brief 2024*. Retrieved from: https://www.police.gov.sg/Media-Hub/Statistics，Last viewed date: October 29, 2025.

Stuntz, W. (2011). *The Collapse of American Criminal Justice*. Cambridge, MA: Belknap Press of Harvard University Press.

Sunshine, J., & Tyler, T. (2003). The role of procedural justice and legitimacy in shaping public support for policing. *Law and Society Review*, 37(3), 513–547.

Taylor, I., Walton, P., & Young, J. (1973). *The New Criminology*. London: Routledge & Kegan Paul.

Telstra Plus(2024)。*Keep Snitching on Scammers:How Our New 7226 Reporting Number is Fighting off SMS and MMS Scams*。Retrieved form:https://www.telstra.com.au/exchange/keep-snitching-on-scammers--how-our-new-7226-reporting-number-is.，Last viewed date：October 3, 2024

Thornberry, T. P. (1987). Toward an interactional theory of delinquency. *Criminology*, 25(4), 863–892. https://doi.org/10.1111/j.1745-9125.1987.tb00823.x

Tompson, L. & Chainey, S. (2011). Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy. *European Journal on Criminal Policy and Research*, 17, 179-201.

Tonry, M., & Farrington, D. P. (Eds.). (1995). *Building a Safer Society: Strategic Approaches to Crime Prevention*. Chicago, IL: University of Chicago Press.

UK Finance (2025). *Annual Fraud Report 2025*. Retrieved from: https://www.ukfinance.org.uk/system/files/2025-05/UK%20Finance%20Annual%20Fraud%20report%202025.pdf，Last viewed date: November 4, 2025.

Van Nguyen, T. (2022). The modus operandi of transnational computer fraud. *Trends in Organized Crime*, 25(2), 226–247.

Van Nguyen, T. (2022). Transnational cyber fraud in Vietnam. *Crime, Law and Social Change*,

78(4), 347-369. https://doi.org/10.1007/s10611-021-09986-6

Vestfold Police District, Norway (2004). *Gypsy Cabs in Tønsberg*. Retrieved from: www. popcenter.org /library/awards/goldstein/2004/04-35(F).pdf，Last viewed date: June 14, 2024.

White, M. (2008). *Enhancing the Problem-Solving Capacity of Crime Analysis Units*. Problem-Solving Tools Series No. 9. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Wilson, J. Q., & Herrnstein, R. J. (1985). *Crime and Human Nature*. New York, NY: Simon & Schuster.

Wilson, J. Q., & Kelling, G. L. (1982). Broken windows. *The Atlantic Monthly*, March, 29-38.

Wolfgang, M. E., Figlio, R. M., & Sellin, T. (1972). *Delinquency in a birth cohort*. Chicago, IL: University of Chicago Press.

Wortley, R. (1996). Guilt, shame and situational crime prevention. In R. Homel (ed.), *The Politics and Practice of Situational Crime Prevention*. *Crime Prevention Studies*, 5 (pp. 11-–132). Monsey, NY: Criminal Justice Press.

Wortley, R. (2001). A classification of techniques for controlling situational precipitators of crime. *Security Journal*, 14, 63-82.

Wortley, R. (2017). A classification of techniques for controlling situational precipitators of crime. In R. Wortley, *Crime Opportunity Theories* (pp. 425-444). London: Routledge.

Wortley, R., & Townsley, M. (2016). Environmental criminology and crime analysis: Situating the theory, analytic approach and application. In R. Wortley & M. Townsley (eds.), *Environmental Criminology and Crime Analysis* (2nd ed., pp. 1-26). London: Routledge.

三、日文部分

日本の朝日新聞（2023）。首都圏に捜査員集中、スマホ解析機器を増強特殊詐欺捜査を強化へ。Retrieved form: https://www.asahi.com/articles/ASR8Z4J8RR8YUTIL00C.html，Last viewed date：November 26, 2024.

日本東京警視庁（2020）。特殊詐欺について。Retrieved form: https://www-keishicho-metro-tokyo-lg-jp.translate.goog/kurashi/tokushu/furikome/furikome.html?_x_tr_sl=ja&_x_tr_tl=zh-TW&_x_tr_hl=zh-TW&_x_tr_pto=sc，Last viewed date：November 22, 2024

日本眾議院（1947）。昭和 22 年法律第 141 号。Retrieved form: https://laws.e-gov.go.jp/law/322AC0000000141，Last viewed date：November 25, 2024.

犯罪対策閣僚会議（2023）。ＳＮＳで実行犯を募集する手口による強盗や特殊詐欺事案に関する緊急対策プラン令和 5 年 3 月 17 日犯罪対策閣僚会議。Retrieved form: https://www.kantei.go.jp/jp/singi/hanzai/dai36/36gijisidai.html Last viewed date ： Last viewed date：November 23, 2024.

犯罪対策閣僚会議（2024）。国民を詐欺から守るための総合対策令和 6 年 6 月 18 日犯罪対策閣僚会議。Retrieved form: https://www.kantei.go.jp/jp/singi/hanzai/index.html，Last viewed date：November 24, 2024

犯罪対策閣僚会議（2025）。国民を詐欺から守るための総合対策 2.0，令和 7 年 4 月 22 日，犯罪対策閣僚会議。Retrieved form: https://www.kantei.go.jp/jp/singi/hanzai/dai42/42gijisidai.html，Last viewed date：October 29, 2025

警察庁（2022）。令和３年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form:https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/tokushusagi_toukei2021.pdf，Last viewed date：July 4, 2024

警察庁（2023）。令和４年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/tokushusagi_toukei2022.pdf，Last viewed date：July 5, 2024

警察庁（2024）。令和５年における特殊詐欺の認知・検挙状況等について（確定値版）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2023.pdf，Last viewed date：July 6, 2024

警察庁（2025）。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）。Retrieved form: https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/teisei_sagi2024.pdf，Last viewed date：October 28, 2025

Nippon Communications Foundation（2025）。2024 年の特殊詐欺：全国で被害 700 億円超す前年比 6 割近くも増加―警察庁。Retrieved form: https://www.nippon.com/ja/japan-data/h02424/?utm_source=chatgpt.com，Last viewed date：November 5, 2025

附錄一 電信網路假投資詐欺犯罪案例

編號	標題	案例內容
1	**偵破高盛優選股 APP 假投資詐欺集團案**	1.新聞發布日期：2024 年 1 月 5 日。 2.查獲時間：2023 年 10 月 25 日、27 日、2023 年 12 月 10 日。 3.查獲地點：新北市、嘉義市、臺南市、高雄市。 4.查獲嫌犯：陳○○(男，1987 年次)等 20 人。 5.案情摘要：刑事警察局清查「165 反詐欺平台」資料，發現不詳詐欺集團以「高盛優選股」等假投資犯罪手法，藉由網路交友平台、網頁、簡訊等方式，發送「飆股」訊息及 LINE 群組連結，俟被害人加入群組後，聽從「老師、助理、客服」之指示下載 APP 軟體並匯款至指定金融帳戶，期間以「小額出金」、「寄送月餅」等典型「養、套、殺」詐欺手法，使被害人廖○○等 20 人信以為真，誘使增加投資意願、金額，後續發現無法出金、提領，始知悉遭詐欺，損失金額達 2,000 餘萬元，乃訴警偵辦。 6.查獲贓證物：納智捷自小客車 1 部、沛納海手錶 1 支、手機 7 支、USB 隨身碟 2 支、公司印鑑 2 組、中信電子憑證 2 個、公司登記資料 1 份、中國信託商業銀行存簿 2 本、第一銀行存簿 3 本、加密貨幣買賣契約 1 張等證物。聲請扣押車手陳○○名下帳戶新臺幣 100 萬 5,786 元。 資料來源：內政部警政署刑事警察局（2024 年 1 月 5 日）。偵破高盛優選股 APP 假投資詐欺集團案。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=4399b3e1-2cb2-4506-b51b-05d32f81a652，最後瀏覽日期：2024 年 8 月 5 日。
2	**假幣商與海外詐欺集團勾結，騙取國人逾 2 億元**	1.新聞發布日期：2024 年 1 月 19 日。 2.查獲時間：2023 年 12 月。 3.查獲地點：臺南市。 4.查獲嫌犯：邱○○(1998 年次)等 11 名。 5.案情摘要：刑事警察局接獲民眾報案，指稱遭到詐欺，經追查發現一虛擬貨幣幣商集團，涉嫌與海外詐欺集團勾結，以投資虛擬貨幣名義詐欺民眾，經清查被害人多達 40 名，財損金額逾新臺幣 2 億元。犯嫌邱○○（具竹○幫背景）等 11 人均自稱幣商，自 2022 年 11 月起開始經營，與多家詐欺集團配合，遍布全台各地向被害人行騙，受騙民眾多達 40 名，遭詐金額高達新臺幣 2 億元之多，清查不少被害人為退休人士，聽從詐騙集團指示投資達數百上千萬元，致使積累一生存款在詐欺集團的花言巧語之下全都付之東流。該幣商集團成員搭乘高鐵南北往返與被害人面交，單日業績動輒上百萬，每個月成員交通開銷就需花費數萬元。 6.查獲贓證物：市值新臺幣 250 萬元自小客車，贓款 233 萬餘元，筆電，手機、點鈔機等贓證物。 資料來源：刑事警察局（2024 年 1 月 19 日）。假幣商與海外詐欺集團勾結，騙取國人逾 2 億元。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=2669417a-6014-4b80-9bca-7b5f4b74a643，最後瀏覽日期：2024 年 8 月 5 日。

3	打詐「斷投專案」第一彈刑事局破獲幫派成員經營洗錢集團案	1.新聞發布日期：2024 年 1 月 24 日。 2.查獲時間：2024 年 1 月 22 日。 3.查獲地點：臺北市、新北市。。 4.查獲嫌犯：陳○○(男，2000 年次)、賀○○(男，2004 年次)、葉○○(男，1999 年次)、葉○○(男，2003 年次)、葉○○(男，2002 年次)等 5 人。 5.案情摘要：刑事警察局打詐「情資研析中心」分析報案資料，發現被害民眾邱○○等 30 人透過通訊軟體加入投資群組及 APP，遭以投資股票、領取飆股及個股資訊為由誘騙。於去 2023 年 6 月至 9 月間匯款至人頭帳戶投資，獲利想要出金時，對方則告以需要先繳交紅利分成才可出金，被害民眾因短時間內無法籌湊資金繳納紅利，又遭業務員封鎖通訊軟體致無法取得聯繫，始驚覺遭詐欺。警方於 2023 年 11 月 14 日執行第一波行動，拘提具有幫派背景的洗錢犯嫌賀○○到案，復於 2024 年 1 月 22 日進行第二波行動，拘提協助詐欺集團洗錢的幫派分子陳○○等 4 人到案，並查扣開山刀、信號彈、鋁棒、現金、手機、存簿及提款卡等贓證物，初估被害人超過 30 名、詐欺金額約新臺幣 5 千萬元。 6.查獲贓證物：開山刀、信號彈、鋁棒、新臺幣 2 萬 3,000 元、手機、存簿及提款卡等贓證物。 資料來源：內政部警政署刑事警察局（2024 年 1 月 24 日）。打詐「斷投專案」第一彈刑事局破獲幫派成員經營洗錢集團案。。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=21481297-ac60-4937-a19d-f5b62a04da3d，最後瀏覽日期：2024 年 8 月 5 日。

4	**打詐「斷投專案」第二彈 刑事局破獲境外基金投資詐欺集團案**	1.新聞發布日期：2024 年 1 月 24 日。 2.查獲時間：2024 年 1 月 23 日、24 日。 3.查獲地點：臺北市、新北市、新竹市、臺中市及花蓮縣等地。 4.查獲嫌犯：戴○○(男，1962 年次)等 25 人。。 5.案情摘要：刑事警察局北部詐欺偵查中心於 2023 年 11 月間受理民眾報案稱「豐○○球資本公司」推出之境外基金「豐○○球外匯息差收益基金」，以投資國際外匯市場隔夜利息收益為名目，未經許可在國內向不特定人推銷認購，致使百餘人受騙投資，該公司於 2023 年 4 月對外公告無法支付投資紅利，投資人驚覺遭詐欺始向警方報案。經查豐○○球資本公司與自稱為澳洲券商合作，偽稱涉案基金係由該澳洲券商公司投入市場獲利，每年可固定獲利 14%，於國內與基金代銷「首○公司」配合，由代銷公司旗下業務對外招攬投資人參加實體及網路說明會，致使百餘人受騙投資未經金管會核准之境外基金「豐○○球外匯息差收益基金」。經調查發現該公司自 2020 年 4 月起在國內招募上開基金，約有上百名投資者，總金額高達美金 4,865 萬元(折合新臺幣約 14 億 7,400 餘萬元)。刑事局於 2024 年 1 月 23 日執行拘提並帶同主嫌戴○○、林○○、楊○○等 25 名銷售業務員到案，同時搜索 8 處相關處所，查扣基金備忘錄、基金 DM、投資匯款資料、空白基金協議書、金錢借貸契約書、基金購買協議書、交易明細等贓證物，並經法院核准財產扣押房屋、土地 4 筆及相關帳戶(市值約新臺幣 3 億元)。 6.查獲贓證物：基金備忘錄、基金 DM、投資匯款資料、空白基金協議書、金錢借貸契約書、基金購買協議書、交易明細等贓證物。法院核准財產扣押房屋、土地 4 筆及相關帳戶(市值約新臺幣 3 億元)。 資料來源：內政部警政署刑事警察局（2024 年 1 月 24 日）。打詐「斷投專案」第二彈 刑事局破獲境外基金投資詐欺集團案。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=99e52bed-645e-4eb5-a475-0520be172400，最後瀏覽日期：2024 年 8 月 5 日。

5	**打詐「斷投專案」第三彈 刑事局破獲「富達App」假投資詐欺洗錢水房案**	1.新聞發布日期：2024 年 1 月 25 日。 2.查獲時間：2024 年 1 月 16 日。 3.查獲地點：新北市、臺中市。 4.查獲嫌犯：官○○(男、1997 年次)、陳○○(男、2001 年次)、汪○○(男、2000 年次)、陳○○(男、1999 年次)、蔡○○(男、2001 年次)、謝○○(男、1987 年次)等 6 人。 5.案情摘要：刑事警察局北部詐欺偵查中心(偵查第七大隊)分析被害人報案資料，追查發現被害民眾謝○○等 10 餘人透過通訊軟體加入投資群組及「富達投資」APP，遭以投資股票、領取飆股及個股資訊為由誘騙。於 2023 年 4 月至 7 月間由車手假冒「富達投資」專員向被害人面交取款，再立即將贓款交給管理錢包的犯嫌轉成虛擬貨幣洗錢至詐欺集團。案經刑事警察局北部詐欺偵查中心報請臺北地檢署檢察官指揮偵辦，於蒐證完畢後，先於 2023 年 8 月 31 日執行第一波行動，拘提負責管理錢包犯嫌謝○○到案，復於 2024 年 1 月 16 日進行第二波行動，拘提負責指揮車手面交取款的治平對象官○○及面交車手等 5 人到案，並查扣以上贓證物，初估被害人 37 名、詐欺金額約新臺幣 2 億 4 千萬元。 6.查獲贓證物：現金 5 萬 8,000 元、銀行卡及存摺、開山刀、武士刀、西瓜刀、監視器設備 1 組、點鈔機 1 台、手機、K 他命等贓證物。 資料來源：內政部警政署刑事警察局（2024 年 1 月 25 日）。打詐「斷投專案」第三彈 刑事局破獲「富達 App」假投資詐欺洗錢水房案。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=742b5621-00fe-4d12-9e89-0d7823f2c4d3，最後瀏覽日期：2024 年 8 月 5 日。

6	**偵破假冒「貝○○」假投資詐欺集團系列專案**	1.新聞發布日期：2024 年 1 月 25 日。 2.查獲時間：2021 年 11 月 24 日至 2023 年 11 月 1 日。 3.查獲地點：高雄市、臺北市、新北市、桃園市、新竹市、臺中市、臺南市等地。 4.查獲嫌犯：主嫌余○○(男、1982 年次)、鄭○○(男，1982 年次)等共計 57 人。 5.案情摘要：刑事警察局電信偵查大隊分析 165 資料庫，針對以「貝○○」投資 App 進行詐欺之假投資詐欺集團進行分析，發現涉及被害人數眾多，嚴重影響社會治安，統計 2022 年至 2023 年國人被害人數總計共有 81 人，財損金額逾新臺幣 1 億 8,201 萬 8,044 元，經查其中單筆金額最多之財損為新臺幣 2,530 萬餘元。調查發現該詐欺集團「柬埔寨機房」端係先以「投資飆股」為話術誘使被害人加入投資股票 Line 群組「股市研討社」，群組內假股票老師(張○豐)及助理(林○萱)會再要被害人手機下載並註冊假投資 App「貝○○」，並要求被害人轉帳入金至詐欺集團提供之人頭帳戶，隨後在投資群組指示被害人每日跟隨老師當沖，初期股票贏錢該詐欺集團會先少量出金，取得被害人信任，俟被害人漸漸投入大量金額後，該詐欺集團即以系統錯誤無法順利出金為由，並將被害人踢出 Line 群組「股市研討社」，假投資 App「貝○○」亦隨之消失。另當被害人至各地金融機構轉帳遇到行員攔阻時，該詐欺集團則會利用 Line「官方客服」之身分，將偽造之轉帳單據傳送給被害人，並告知被害人該單據係其他學員轉帳儲值成功之紀錄，要求被害人將該金融機構內之全部資金提領出來再至其他金融機構轉帳，同時傳送偽造之「貝○○證券投資顧問事業營業執照」，取信被害人持續轉帳。專案小組，分別在高雄、臺北、新北、桃園、新竹、臺中、臺南等地區執行搜索與拘提，查獲該詐欺集團共計 57 名犯嫌到案，並查扣現金新臺幣 800 萬 5,000 餘元、美金 6,200 元、日幣 23 萬元、虛擬貨幣 USDT 共 18 萬 1924.6327 顆(約新臺幣 590 萬 8,891 餘元)、BMW、保時捷自小客各 1 部、手機數支、平板電腦、涉案帳戶存摺、提款卡、點鈔機、子彈、UPS 不斷電系統、NAS 雲端硬碟、保險箱、帳冊、印章等贓證物。 6. 查獲贓證物：查扣現金新臺幣 800 萬 5,000 餘元、美金 6,200 元、日幣 23 萬元、虛擬貨幣 USDT 共 18 萬 1924.6327 顆(約新臺幣 590 萬 8,891 餘元)、BMW、保時捷自小客各 1 部、手機數支、平板電腦、涉案帳戶存摺 16 本、提款卡 5 張、點鈔機、子彈、UPS 不斷電系統、NAS 雲端硬碟、保險箱、帳冊、印章 5 枚等贓證物。 資料來源：內政部警政署刑事警察局（2024 年 1 月 25 日）。偵破假冒「貝○○」假投資詐欺集團系列專案。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=a56da572-690c-47bc-b35a-696d4a1e775c，最後瀏覽日期：2024 年 8 月 5 日。

7	打詐「斷投專案」第四彈 刑事局破獲黑幫設立網銀「機動轉帳水房」海詐被害人	1.新聞發布日期：2024 年 1 月 29 日。 2.查獲時間：2024 年 1 月 23 日。 3.查獲地點：新北市、新竹縣、嘉義縣等地。 4.查獲嫌犯：主嫌古○○(男，1992 年次)、蔡○○（男，1997 年次）、徐○○（女，1983 年次）、林○○（男，1981 年次）及印尼籍移工(女，1960 年次)等 5 人。 5.案情摘要：刑事警察局打詐「情資研析中心」彙整分析遭詐欺被害人資料，產出詐欺集團網銀轉帳水房情資，遂交由電偵大隊積極偵辦，據以深入追查轉帳水房據點，於 2024 年 1 月 23 日執行「斷投專案」，查獲以古姓男子為首，利用「網銀轉帳」洗錢之詐欺轉帳水房據點。本案被害人遭詐欺後匯入指定之銀行帳戶，均係以人頭成立之空殼公司或企業社名義所申請；該詐欺洗錢集團以「網路銀行」經多層轉匯，最後將贓款轉帳至香港境外金融帳戶進行洗錢。專案小組歷經 1 個月餘追查，鎖定新店地區幫派分子古姓犯嫌為首之轉帳水房，渠等以「機動轉帳水房」模式，使用網路銀行轉帳、匯兌美金後，再轉帳至香港銀行帳戶，被害人財損金額達新臺幣 1,500 萬元，案經蒐證完備後，於 2024 年 1 月 23 日執行專案勤務，並拘提主嫌古○○等人到案，現場查扣開山刀、電擊器、現金、存摺、提款卡、涉案人頭公司大小章、大麻等贓證物 查獲贓證物：工作手機 6 支、Acer 筆記型電腦 1 臺、中國信託存摺 1 本、郵局存摺 1 本、銀行提款卡 2 張、信用卡 2 張、涉案公司大小章各 1 個、現金新台幣 11 萬 2,500 元、美金 200 元、港幣 500 元、越南盾 128 萬 9,000 元、開山刀 1 支、電擊器 1 臺、電磁紀錄等贓證物。 資料來源：內政部警政署刑事警察局（2024 年 1 月 29 日）。打詐「斷投專案」第四彈 刑事局破獲黑幫設立網銀「機動轉帳水房」海詐被害人。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=b9832b8d-9040-4d45-97d0-d496433151a6，最後瀏覽日期：2024 年 8 月 5 日。

8	打詐「斷投專案」第五彈 刑事局破獲幫派成員經營洗錢集團案	1.新聞發布日期：2024 年 1 月 30 日。 2.查獲時間：2024 年 1 月 23 日。 3.查獲地點：臺北市、新北市。 4.查獲嫌犯：鄭○○(1990 年次)、游○○(2001 年次)、陳○○(1983 年次)、段○○(1988 年次)、鄭○○(2000 年次)、洪○○(1998 年次)、莊○○(1998 年次)、曾○○(2001 年次)、葉○○(1996 年次)及林○○(1995 年次)等 10 名。 5.案情摘要：刑事警察局打詐「情資研析中心」彙整分析遭假投資詐欺的被害人資料，產出詐欺集團虛擬貨幣交易流向異常情資，遂交由偵查第一大隊積極偵辦，專案小組深入追查發現被害人透係過臉書得知虛擬貨幣投資訊息，於被害人點擊該廣告後，詐欺集團以通訊軟體 LINE 邀請被害人加入投資群組及下載不同投資標的之 APP，佯稱虛擬貨幣後市看好，值得投資等話術，誘騙被害人至特定虛擬貨幣實體店面購買虛擬貨幣，初步清查本案因假投資遭詐欺被害人達 40 名，財損約 6,470 萬元。專案小組在蒐證完畢後，持臺灣新北地方檢察署及臺灣新北地方法院核發之拘票、搜索票，於臺北市及新北市等 10 處執行搜索，拘捕鄭○○等 10 人到案，專案小組於搜索處監控時，發現葉○○至現場行跡可疑，見機不可失，強力攻堅，當場查獲葉○○前來交付來源不明現金 116 萬元，立即以現行犯逮捕，現場查扣現金共計 131 萬元、筆電、棍棒、開山刀、防彈衣及幫派象徵畫等贓證物。 查獲贓證物：現金新臺幣(下同)131 萬元、筆電 19 臺、手機 51 支、點鈔機 1 臺、員工手則及陌生開發話術 4 份、考勤表 13 張、棍棒 7 根、開山刀 14 支、防彈衣 2 件、信號彈 1 個及幫派象徵畫 2 幅等證物。 資料來源：內政部警政署刑事警察局（2024 年 1 月 30 日）。打詐「斷投專案」第五彈 刑事局破獲幫派成員經營洗錢集團案。臺北：《內政部警政署刑事警察局新聞發布》。取自： https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=d3b1cf6d-de43-4d73-bd5e-0bec8943a62c，最後瀏覽日期：2024 年 8 月 5 日。

9	打詐「斷投專案」第六彈 刑事局破獲MERRYLAND假投資詐欺機房	1.新聞發布日期：2024年2月1日。 2.查獲時間：2024年1月8日、10日。 3.查獲地點：新北市樹林區、新北市蘆洲區 4.查獲嫌犯：陳○○、邱○○、林○○、林○○、張○○等5人 5.案情摘要：刑事警察局「打詐中心情資研析專責小組」深入分析165大數據資料，發現有不法分子於國內從事假投資詐欺機房，遂將情資研析結果該局偵查第二大隊與臺北市政府警察局刑事警察大隊、信義分局、新北市政府警察局樹林分局、基隆市警察局第三分局組成專案小組共同偵辦。經專案小組分析交付之情資，調查發現詐欺機房活動區域分別位於新北市樹林區及蘆洲區，進而跟監蒐證確認詐欺機房2處據點及機房5名成員身分，於2024年1月8日及10日持檢察官核發之拘票及法院搜索票攻堅，緝獲犯嫌陳○○等5人，查扣作案用電腦主機、筆記型電腦、手機、網路分享器等證物。經查該詐欺機房係使用通訊軟體Instagram、LINE申請大量帳號，再向不特定之多數人發送投資獲利訊息，倘被害人陷於錯誤，機房成員便會引導被害人購買加密貨幣入金至MERRYLAND等假投資網站(acs516.meryoyeus.com)，目前初步清查被害人計8人，總計被害金額新臺幣525萬元。 6.查獲贓證物：電腦主機9臺、筆記型電腦2臺、手機14支、網路分享器4臺、硬碟5顆、教戰守則2本、網路流量卡一批、LV及GUCCI等名牌包。 資料來源：內政部警政署刑事警察局（2024年2月1日）。打詐「斷投專案」第六彈 刑事局破獲MERRYLAND假投資詐欺機房。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=9525ebc4-f520-4a8e-b7f9-4f56ff176711，最後瀏覽日期：2024年8月5日。

10	打詐「斷投專案」第七彈 刑事局破獲「金〇百匯」虛擬資產公司涉嫌跨國愛情詐欺、洗錢及組織犯罪等案	1.新聞發布日期：2024 年 2 月 3 日。 2.查獲時間：2024 年 1 月 24 日。 3.查獲地點：臺北市、高雄市、嘉義市 4.查獲嫌犯：汪〇〇(男、1995 年次)、汪黃〇〇(女、1965 年次)、陳〇〇(女、1968 年次)等 18 人 5.案情摘要：「金〇百匯」係以實體店面經營之虛擬資產幣商，以補貼車資、消費滿額送禮等手法，配合境外詐欺機房指派車手及誘騙被害人前來將贓款以高於市價之虛擬貨幣轉至境外，且該公司在未完成洗錢防制法令遵循聲明之情形下，明知違法仍持續洗錢牟利。本案洗錢集團配合境外假交友之愛情詐欺機房，以謊稱伊拉克軍官、聯合國官員或逕以老婆相稱之網友，以柔情話術誘騙被害人掉入感情陷阱，並指引至「金〇百匯」公司交付現金以虛擬貨幣將被害款項提供給詐欺集團，「金〇百匯」公司協助洗錢並從中牟取暴利。案經高雄地方檢察署指揮偵辦，蒐證完畢後於 2024 年 1 月 24 日南北串聯同步執行搜索，一舉查獲主嫌汪〇〇等 18 人，並查扣現金新臺幣 2,600 萬餘元、保時捷 1 部、USDT 23,912 顆(市值約新臺幣 74 萬元)、保險箱、點鈔機、相關手機、電腦及文件等證物。 查獲贓證物：現金新臺幣 2,600 萬餘元、保時捷 1 部、USDT 23,912 顆(市值約新臺幣 74 萬元)、保險箱、點鈔機、相關手機、電腦及文件等證物。 資料來源：內政部警政署刑事警察局（2024 年 2 月 3 日）。打詐「斷投專案」第七彈 刑事局破獲「金〇百匯」虛擬資產公司涉嫌跨國愛情詐欺、洗錢及組織犯罪等案。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=63e1094f-1587-4717-905b-f51349b1c2dc，最後瀏覽日期：2024 年 8 月 5 日。

11	**打詐「斷投專案」第八彈 詐團掛假車牌收人頭帳戶 刑事局中打鎖定收網成擒**	1.新聞發布日期：2024 年 2 月 5 日。 2.查獲時間：2024 年 1 月 29 日。 3.查獲地點：高雄市 4.查獲嫌犯：蕭○○(男，33 歲)等 4 人 5.案情摘要：刑事警察局打詐「情資研析中心」分析報案資料，發現方姓等 3 名被害民眾遭歹徒以從事家庭代工可以領取補助款為由詐欺，在 2023 年 12 月間陸續寄出名下金融帳戶金融卡及密碼，而被害人在帳戶遭警示後始驚覺遭詐欺。刑事警察局中部打擊犯罪中心獲案後即報請臺灣嘉義地方檢察署檢察官指揮偵辦，鎖定收簿集團蕭姓犯嫌等成員，渠等在嘉義地區以名下車輛更換偽造及註銷車牌懸掛，並刻意橫跨縣市至超商領取被害人寄出之金融卡，再以金融卡至 ATM 提領被害人遭詐欺款項，蒐證完備後於 2024 年 1 月 29 日與嘉義縣警察局刑事警察大隊組成專案小組，持臺灣嘉義地方法院(檢察署)搜索票及拘票，拘提蕭姓犯嫌等 4 人到案，並查扣 21 萬餘元、手機、筆電、提款卡、註銷車牌等贓證物，全案警詢後依涉嫌刑法詐欺及洗錢防制法等罪嫌移送臺灣嘉義地方檢察署偵辦。 6.查獲贓證物：現金新臺幣 21 萬餘元、手機、筆電、提款卡、註銷車牌等贓證物。 資料來源：內政部警政署刑事警察局（2024 年 2 月 5 日）。打詐「斷投專案」第八彈 詐團掛假車牌收人頭帳戶 刑事局中打鎖定收網成擒。臺北：《內政部警政署刑事警察局新聞發布》。取自： https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=11d71bdd-5f2d-4d80-84ab-158844c4046a，最後瀏覽日期：2024 年 8 月 5 日。

12	打詐「斷投專案」第九彈 刑事局破獲黑幫經營假應徵真車手投資詐欺集團案	1.新聞發布日期：2024 年 2 月 5 日。 2.查獲時間：2024 年月日。 3.查獲地點：臺北市、新北市、桃園市及臺南市等處 4.查獲嫌犯：呂○穎(1993 年次)等 18 人 5.案情摘要：刑事警察局打詐「情資研析中心」，彙整分析遭假投資詐欺的被害人資料，產出以竹○幫太○堂臺○分會會長呂嫌為首之詐欺集團情資，遂交由該局偵查第九大隊偵辦，偵查發現以竹○幫太○堂臺○分會會長呂嫌為首成立之車手暨洗錢詐欺集團，與境外詐欺機房配合，由境外機房犯嫌以通訊軟體發放假投資廣告訊息，假冒知名分析師「楊○超」等傳送相關投資訊息，並解說投資細節，俟被害人信以為真後，便指示被害人下載投資 APP，將大筆投資金額匯入人頭帳戶，由水房成員層轉洗錢，續由呂嫌與其妻陳嫌以通訊軟體指揮所屬車手，前往提領贓款或以虛擬貨幣方式將贓款回流詐欺集團，以規避警方查緝，不法所得初估逾新臺幣 3 千萬元。本案詐欺集團另以發送「高報酬工作」及「輕鬆借貸」等廣告訊息招募人頭帳戶，當有人應徵時便指示前往新北市、桃園市等地之汽車旅館、飯店進行面試，後續由呂嫌指示所屬成員實施監控，帶往各金融機構辦理金融帳戶以作為詐欺使用。專案小組蒐證完成後，分別於 2023 年 7 至 8 月間，在臺灣新北地方檢察署指揮下，結合臺南市政府警察局第一分局、臺北市政府警察局中正第一分局、臺北市政府警察局中正第二分局、臺北市政府警察局士林分局及高雄市政府警察局刑事警察大隊等單位連續展開 4 波查緝行動，逮捕犯嫌 18 人，並查扣犯案手機、SIM 卡、存摺、提款卡、虛擬貨幣買賣聲請書(切結書)、營業登記資料及房屋租賃契約及背心等物品。 6.查獲贓證物：手機 11 支、存摺 7 本、提款卡 8 張、虛擬貨幣買賣聲請書(切結書)、營業登記資料及房屋租賃契約及背心(幫派標誌)1 件等。 資料來源：內政部警政署刑事警察局（2024 年 2 月 5 日）。打詐「斷投專案」第九彈 刑事局破獲黑幫經營假應徵真車手投資詐欺集團案。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=50874980-cf5f-49c7-b0c4-5f3250ef1202，最後瀏覽日期：2024 年 8 月 5 日。

13	**溯源四層追緝打擊詐欺犯罪中心情資研析「假投資」詐欺集團案**	1.新聞發布日期：2024 年 2 月 6 日。 2.查獲時間：2024 年 1 月 29 日。 3.查獲地點：雲林縣東勢鄉等地 4.查獲嫌犯：丁○○(男，1987 年次)等 6 名 5.案情摘要：刑事警察局打詐「情資研析中心」分析報案資料，發現歹徒透過臉書、IG 等社群網路投放假投資廣告或交友 APP 搭訕被害人，隨後再轉移至 LINE 等軟體持續聯繫，俟取得被害人信任後，便騙取其投資來路不明的虛擬貨幣網站，誘騙數十名被害人，且行騙得逞金額達新臺幣上千萬元，該局國際刑警科遂於斷『投』專案期間向臺灣雲林地方法院(檢察署)聲請搜索票、拘票後與雲林縣警察局臺西分局、北港分局、刑警大隊科技犯罪偵查隊、臺南市政府警察局永康分局、南投縣政府警察局信義分局、新北市政府警察局林口分局、新竹市警察局第一分局等單位，層層追緝該「假投資」詐欺集團犯罪網絡，並查扣克拉克制式手槍 2 把及仿金牛座改造手槍 2 把(均為火藥式，含子彈 107 發)、現金新臺幣 50 萬元、電腦、借據及帳冊一批、手機等不法贓證物 6.查獲贓證物：克拉克制式手槍 2 把及仿金牛座改造手槍 2 把、子彈 107 發、現金新臺幣 50 萬元、電腦、借據及帳冊一批、手機等不法贓證物。 資料來源：內政部警政署刑事警察局（2024 年 2 月 6 日）。溯源四層追緝打擊詐欺犯罪中心情資研析「假投資」詐欺集團案。臺北：《內政部警政署刑事警察局新聞發布》。取自： https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=65df3b04-2e3f-4262-9cf5-e8dd429a6162，最後瀏覽日期：2024 年 8 月 5 日。

14	**打詐「斷投專案」全面掃蕩假投資詐團洗錢案**	1.新聞發布日期：2024 年 2 月 6 日。 2.查獲時間：2024 年 1 月 29 日。 3.查獲地點：高雄市、臺中市、新北市。 4.查獲嫌犯：羅○○(男，1987 年次)等共計 16 名。 5.案情摘要：刑事警察局偵查第八大隊與高雄市政府警察局鼓山分局等單位，共組專案小組偵辦詐欺集團案件，由提領車手溯源發現，有詐欺集團以「德勝」、「達昌」、「百勝」等飆股投資顧問名義，於網路上投放廣告吸引投資人加入假投資平臺，再以詐術使投資人深信該假投資平臺能有穩定高獲利，投資人遂依照詐欺集團假客服人員指示，將投資款項匯入指定金融帳戶，等到獲利了結、投資人欲出金時，皆遭無故推託、延遲，才發現遭詐欺。初步調查被害人數逾 33 人，財損金額逾 1 千萬元。以羅姓男子為首之詐欺集團，以打工方式吸收車手加入，協助多個「假投資」詐欺集團提領詐欺贓款，並多層轉帳漂洗黑錢。警方蒐證掌握該犯罪集團車手、洗錢水房據點及犯罪事證，自 2022 年 11 月間至 2024 年 1 月間發動多次搜索、拘提行動，共計查獲犯嫌 16 人，查扣手機、點鈔機、電腦以及新臺幣(以下同)168 萬 3,600 元等贓、證物。 6.查獲贓證物：手機、點鈔機、電腦、贓款 168 萬 3,600 元等證物。 資料來源：內政部警政署刑事警察局（2024 年 2 月 6 日）。打詐「斷投專案」全面掃蕩假投資詐團洗錢案。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=bbc4b2c0-9b66-43c1-9d5a-eec2ecdddecb，最後瀏覽日期：2024 年 8 月 5 日。

15	A.I.智能投資躺著賺？刑事局破獲假投資詐欺集團	1.新聞發布日期：2024 年 3 月 11 日。 2.查獲時間：2023 年 8 月 30 日、2024 年 2 月 22 日。 3.查獲地點：新竹縣市、苗栗縣、臺南市 4.查獲嫌犯：鄭○○（男、1972 年次）、鄭○○（女、1976 年次）、林○○（男、1966 年次）、陳○○（男、1980 年次）、吳○○（女、1976 年次）、劉○○（女、1976 年次）、李○○（男、1981 年次）、彭○○（男、1981 年次）、楊○○（男、1972 年次）、邱○○（女、1974 年次）等 10 人 5.案情摘要：刑事警察局接獲民眾報案指稱，有吸金集團自 2015 年起以「環球金融交流平臺有限公司」之人工智能機器人交易功能，標榜自動操作股票、保險、基金、債券、外匯、貴金屬等金融產品交易，惟實質上並無該人工智能機器人及交易平臺，向被害人保證投資每年可穩定獲利 8.4%等話術，於新竹縣市、苗栗縣等地區招募銷售業務員向不特定人招攬投資，多名被害人直至 2022 年 12 月起未收取合約利息始驚覺被騙。經調查發現該犯罪集團係由主嫌鄭○○負責在海外成立假投資公司，並規劃不實人工智能機器人交易平臺合約，再交由陳、林 2 嫌以國內財經資訊公司名義對外吸引投資客入金。經多月蒐證後，於 2023 年 8 月 30 日同步執行查緝行動，拘捕犯嫌林○○等 6 人到案，並聲請法院裁定扣押主嫌鄭○○、鄭○○、林○○、陳○○、彭○○名下土地、房屋及車輛共新臺幣 1,531 萬餘元，經警方清查帳冊發現至少有 21 人被騙投資，總計入資金額達新臺幣 1 億 2,183 萬餘元。主嫌鄭男亦於 2024 年 2 月間自中國大陸廈門入境臺灣時遭警方緝獲，全案依違反刑法詐欺罪、銀行法等罪嫌移送臺灣新竹地方檢察署偵辦。 6.查獲贓證物：電腦主機、手機、客戶合約書、續期證明書、隨身碟、金融存摺、匯款單、筆記本、客戶利息資料、會計師帳冊等贓證物。 資料來源：內政部警政署刑事警察局（2024 年 3 月 11 日）。A.I.智能投資躺著賺？刑事局破獲假投資詐欺集團。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=cb0d84aa-a6ee-4933-aa6a-29623a1378fb，最後瀏覽日期：2024 年 8 月 6 日。

16	**全國首件!無良廣告商蔑視下架通知投放金融詐欺廣告檢警嚴查不貸**	1.新聞發布日期：2024 年 3 月 29 日。 2.查獲時間：2023 年 11 月下旬。 3.查獲地點：臺北市及桃園市等地區。 4.查獲嫌犯：石○○等 5 人。 5.案情摘要：刑事警察局情資研析小組及偵查第四大隊針對可疑之廣告代理商進行清查，分析發現主嫌石○○等人所任職德○公司，係知名外商廣告公司在臺分公司，該公司應用大數據分析網路使用者瀏覽網頁習慣，用以提供廣告主配套精準投放廣告，可曝光於全球及國內合作數位媒體。石嫌及公司主管等人為貪圖個人不法利益及龐大廣告代理收入，由共犯成立人頭公司層轉贓款，涉嫌勾結詐欺集團以該公司廣告平台系統，協助投放涉詐金融投資廣告，內容多為誇大投資賺錢效率等話術，其中更假冒「楊○光」、「阮○驊」等財經專家、名人代言，使不特定民眾誤信點擊「投資廣告頁面」，後即遭引導轉址、連結至「落地頁面」或 LINE 群組，逐步落入詐欺集團假投資詐欺之犯罪模式，進而遭詐交付金錢。期間該公司雖曾多次接獲刑事警察局通知下架涉詐廣告，仍蓄意協助詐欺集團繼續優化、投放金融廣告，顯然涉有詐欺犯意。經拘提、通知石嫌等 5 人到案，並扣押名下帳戶資金、不動產、自小客車及虛擬貨幣，查扣不法利得共計約 1 億多元。石嫌遭裁定羈押禁見，其他共犯以 15 至 50 萬元不等交保。 6.查獲贓證物：筆電 3 臺、平板電腦 2 臺、廣告代理商德○公司客戶資料及隨身碟、主機資料庫、投放廣告素材等；扣押主嫌石○○等人名下帳戶、房屋 2 棟、自小客車 2 輛、大型重機 2 部及 USDT 虛擬貨幣 3,322 顆。 資料來源：內政部警政署刑事警察局（2024 年 3 月 29 日）。全國首件!無良廣告商蔑視下架通知投放金融詐欺廣告檢警嚴查不貸。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=a0e95e8f-1715-4bdf-9486-ed5ae5bf1f71，最後瀏覽日期：2024 年 8 月 6 日。

17	**刑事局南打掃蕩南北幫派詐欺集團及洗錢水房，25名犯嫌落網!!**	1.新聞發布日期：2024年3月29日。 2.查獲時間：2023年9月至2024年3月。 3.查獲地點：新北市、高雄市、臺南市等地 4.查獲嫌犯：張○○(男、29歲)、陳○○（男、26歲）等25人。 5.案情摘要：刑事警察局南部打擊犯罪中心針對詐欺集團自稱「源○投資公司」、「威○有限公司」等虛設投資公司行號名義詐欺國人假投資案件，分析後結合相關友軍單位擴大偵辦，近半年間執行數波查緝行動，共逮獲25名犯嫌到案。偵辦期間發現詐欺集團透過社群媒體以高獲利及假冒知名投顧老師等手法招攬被害人加入假投資詐欺群組，並依指示安裝手機APP應用程式。為取信被害人，詐欺集團先透過調整應用程式上數據使被害人誤信有獲益，並先匯款數仟至數萬元不等小額獲利予被害人，使被害人誤信有賺頭而加碼進場匯款，調查期間亦發現有水房集團成員有黑吃黑侵吞贓款遭拘禁凌虐。全案自2023年9月起至2024年3月間執行數波查緝行動，先於9月間搜索攻堅高雄市鼓山區1處水房據點，並拘捕陳姓犯嫌等5名犯嫌到案，近日循線追查後，針對新北市樹林區另1處水房據點執行攻堅搜索並拘捕張姓犯嫌到案，相關犯嫌於警詢後依涉嫌刑法詐欺及洗錢防制法等案解送該管地檢署偵辦，另針對涉案層轉人頭公司帳戶贓款向該管地方法院聲請扣押裁定獲准，扣押金額計新臺幣189萬餘元。 6.查獲贓證物：存摺、行動電話、電腦主機、人頭公司大小章及申辦資料、等證物1批，扣押裁定贓款189萬元。 資料來源：內政部警政署刑事警察局（2024年3月29日）。刑事局南打掃蕩南北幫派詐欺集團及洗錢水房，25名犯嫌落網!! 。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=9b87a5bf-4907-4af9-8f11-7362253fabb0，最後瀏覽日期：2024年8月6日。

18	**打詐溯源建功 查扣千萬顆泰達幣**	1.新聞發布日期：2024 年 4 月 24 日。 2.查獲時間：2023 年 10 月 25 日、2024 年 4 月 15 日。 3.查獲地點：新北市、高雄市等地。 4.查獲嫌犯：陳○霆（男、1993 年次）、林○宇（男、1993 年次）、朱○蔚（男、1997 年次）、何○德（男、1992 年次）、蔡○勳（男、1993 年次）、洪○妤（女、1998 年次）、林○翔（男、1971 年次）、陳○源（男、1979 年次）、鍾○彣（男、1993 年次）、林○志（男、1997 年次）、伍○明（男、1986 年次）、陳○韓（男、1988 年次）、謝○如（女、1987 年次）等 13 人。 5.案情摘要：刑事警察局偵查第七大隊受理民眾遭假投資詐欺案件，經過濾、分析金流及虛擬貨幣流向，鎖定以陳姓主嫌為首之詐欺集團，渠等以虛擬貨幣後市可期等話術取信被害人匯款新臺幣入金投資，或派遣自稱幣商之面交車手向被害人收款、簽立泰達幣買賣契約，塑造正當交易之假象，再由面交車手協助被害人將泰達幣轉至詐欺集團指定之電子錢包佯裝成功入金。案經報請臺灣臺北地方檢察署指揮偵辦，於 2023 年 12 月至 2024 年 4 月分 3 波查緝，共查獲陳姓犯嫌等 13 人到案，另發現陳嫌為防東窗事發，事先備妥買賣虛擬貨幣相關免責聲明，以掩飾犯行；初估本案被害人約 50 人，財損金額逾臺幣 4,000 萬元。 6.查獲贓證物：手機、點鈔機、監視器、筆記型電腦、虛擬貨幣買賣合約書及新臺幣 39 萬 8,000 元等證物。 資料來源：內政部警政署刑事警察局（2024 年 4 月 24 日）。打詐溯源建功 查扣千萬顆泰達幣。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=41aed3cb-82ca-4d20-a31f-ae0054f4e5d6，最後瀏覽日期：2024 年 8 月 6 日。

19	**刑事局偵破貓鼠虛擬寵物投資平臺吸金詐欺上億元**	1.新聞發布日期：2024 年 5 月 6 日。 2.查獲時間：2024 年 2 月 26 日。 3.查獲地點：新北市、新竹縣、苗栗縣及花蓮縣 4.查獲嫌犯：劉○○(1970 年次)等 21 人 5.案情摘要：刑事警察局中部打擊犯罪中心偵辦「錢鼠投資平臺」人頭帳戶案，經大量金流交易數據分析及過濾相關資料後，鎖定劉嫌為首之詐欺集團涉有重嫌，劉嫌曾以「珍菌堂公司」名義吸金遭臺灣臺北地方檢察署偵辦起訴在案，竟不知悔改，利用區塊鏈熱潮，於 2019 年 7 月至 2020 年 6 月間，轉型成立「派特寵物街」、「錢鼠」及「百鳥朝鳳」等虛擬寵物投資平臺，宣稱該等平臺以區塊鏈為基礎設計，可保證獲利，並舉辦多場說明會用於推廣及取信投資人。平臺設立初期均能正常交易，俟投資人初嘗甜頭陸續加大投資金額後，詐欺集團即以投資平臺遭駭客攻擊為由惡意關閉，導致投資人血本無歸。全案於 2023 年 6 月 28 日至 2024 年 2 月 26 日數波查緝，共計緝獲劉嫌等 21 人到案，查扣現金 409 萬元、電腦主機、筆電、手機、平板、硬碟儲存裝置、金融帳戶及筆記本等贓證物，另由法院裁定財產扣押房地產 20 筆及金融帳戶款項總計約 2,500 萬元。經數位鑑識扣案電磁紀錄儲存設備，發現該等平臺經營期間，虛擬寵物交易金額高達數億元，顯示受騙民眾眾多。 6.查獲贓證物：現金新臺幣(以下同)409 萬元、電腦主機、筆電、手機、平板、硬碟儲存裝置、金融帳戶、筆記本等贓證物。 資料來源：內政部警政署刑事警察局（2024 年 5 月 6 日）。刑事局偵破貓鼠虛擬寵物投資平臺吸金詐欺上億元。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=0b3b2f3f-908c-48d3-a007-1110e5ff3260，最後瀏覽日期：2024 年 8 月 6 日。

20	**刑事局掃蕩徵才轉假投資話務機房**	1.新聞發布日期：2024 年 5 月 8 日。 2.查獲時間：2024 年 4 月 16 日。 3.查獲地點：臺南市中西區、南區、安平區等處 4.查獲嫌犯：蔡○○（男、1996 年次）、曾○○（男、2003 年次）、盧○○（男、2000 年次）、鄭○○（男、1998 年次）、朱○○（男、2000 年次）、范○○（男、2002 年次）、許○○（男、2003 年次）、陳○○（男、2003 年次）、王○○（男、2003 年次）、林○○（男、2004 年次）等 10 名 5.案情摘要：刑事警察局偵查第二大隊分析近期詐欺案件，發現有民眾於社群平台接觸家庭代工廣告，事後卻遭假投資詐欺，經深入追查，該集團於 Facebook 刊登徵才廣告，內容多為居家辦公、訂單處理之工作內容，再要求諮詢職缺之民眾加入 LINE 好友，歹徒假冒公司職員引導被害人處理假公司訂單，藉由虛偽雇傭關係培養信任感，再伺機介紹投資機會，誘騙被害人於詐欺集團設立之假網站投資，該集團使用多層話務手層層誘騙被害人中計，分工綿密，且針對有求職需求的民眾騙取大量金錢，初步清查被害人 3 名，不法所得新臺幣 80 萬 1,000 元，該局掌握不法集團犯罪模式，持續追查不法金流，報請臺灣臺南地方檢察署指揮偵辦，於 2024 年 4 月 16 日同步查緝該詐欺集團之假投資話務機房 3 處，拘提機房幹部蔡○○、曾○○及朱○○等 3 人及其餘 7 名成員到案，並於臺南市中西區查扣手機 20 支、電腦主機 13 臺、監視器主機 4 臺、Wi-Fi 路由器及銀行存摺 4 本等相關贓證物，該 10 名犯嫌經檢察官聲請羈押，法院裁定均收押禁見，全案依刑法詐欺罪、洗錢防制法及組織犯罪防制條例等罪嫌移送臺灣臺南地方檢察署偵辦。 6.查獲贓證物：查扣手機 20 支、電腦主機 13 臺、監視器主機 4 臺、Wi-Fi 路由器 1 臺、銀行存摺 4 本等相關贓證物。 資料來源：內政部警政署刑事警察局（2024 年 5 月 8 日）。刑事局掃蕩徵才轉假投資話務機房。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=12c56d8f-dc63-4e3b-accf-67e221420248，最後瀏覽日期：2024 年 8 月 6 日。

21	**偵破竹聯幫弘仁會以「鼎盛」假投資名義涉嫌詐欺集團案**	1.新聞發布日期：2024 年 5 月 24 日。 2.查獲時間：2023 年 10 月至 2024 年 3 月。 3.查獲地點：高雄市、臺中市、新北市、桃園市等地。 4.查獲嫌犯：林○○（92 年次）等共 39 名。 5.案情摘要：本案係被害人李○○等人於 112 年年中時向 165 反詐欺諮詢專線反映，稱接到「飆股簡訊及 LINE」而遭詐欺集團以假投資手法詐欺，損失達數仟萬餘元，刑事警察局南部詐欺偵查中心分析後，發現該集團係以「鼎盛」等假投資公司協助投顧名義，遊說被害人投資，甚至製作假公司員工名牌、蓋有公司大小章收據等取信被害人交付現金，當投資人要提領「獲利」時，即被封鎖或以各種理由推拖，最後投資網站關閉，致多人受害、損失金額高達數仟萬元。刑事局與高雄市刑大、楠梓、前鎮分局、臺中警局霧峰分局、新北警局海山、汐止分局等單位共組專案小組，追查贓款金流發現竹聯幫弘仁會成員共組詐欺集團，涉嫌以數十個帳戶轉帳洗錢，再交由全臺各地車手臨櫃及 ATM 提領；自 112 年迄今報請高雄、新北地檢署指揮偵辦，於 112 年 10 月至 113 年 4 月打擊詐欺專案期間，執行搜索、拘提行動，共查緝 39 人到案，查扣手機、筆電、點鈔機等證物，並查扣匯入贓款帳戶贓款共計有 1852 萬 7329 元。刑事局將持續針對打擊詐欺工作規劃掃蕩，並要求下架不實廣告，以展現打擊決心，不法分子切勿以身試法；並在此呼籲，假投資詐欺藉由通訊軟體發達之便利，廣發不實高額獲利廣告，誘騙民眾加入群組跟單投資，民眾對於相關廣告應提高警覺，如有任何疑問請撥打 165 反詐欺諮詢專線進行求證，以免受騙。 6.查獲贓證物：新臺幣 1852 萬 7329 元（現金 14 萬 3700 元、裁定扣押 1838 萬 3629 元）、手機 17 支、筆電 1 台、捆抄機 2 台、點鈔機 1 台、現金 14 萬 3,700 元等物。 資料來源：內政部警政署刑事警察局（2024 年 5 月 24 日）。偵破竹聯幫弘仁會以「鼎盛」假投資名義涉嫌詐欺集團案。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=43d10875-718c-4101-b4f9-9cd06cbe0917，最後瀏覽日期：2024 年 8 月 6 日。

22	**司法掮客偕同律師團疑似擔任假投資詐欺集團軍師**	1.新聞發布日期：2024 年 6 月 13 日。 2.查獲時間：2024 年 6 月 11 日。 3.查獲地點：高雄市、臺中市、屏東縣(市)等地區。 4.查獲嫌犯：律師陳○○（男，1983 年次）、律師林○○（女，1987 年次）、法務人員安○○（男，1979 年次）、律師鄭○○（女，1988 年次）、法務助理黃○○（女，71 年次）等 5 名 5.案情摘要：臺灣雲林地方檢察署(下稱雲林地檢)日前偵辦網路投資暨虛擬貨幣詐欺集團案時，發現該集團疑透過律師等專業人士擔任詐團軍師，企圖規避檢警查緝，遂指揮刑事局南部打擊犯罪中心(偵查第八大隊第三隊)、法務部調查局中部地區機動工作站、高雄市政府警察局刑事警察大隊(偵五隊)、雲林縣警察局虎尾分局、刑事警察大隊(偵一隊、科技偵查隊)等單位共組專案小組溯源偵辦。專案小組於今(113)年 6 月 11 日持臺灣雲林地方法院核發之搜索票及雲林地檢(勤股)檢察官核發之拘票，至高雄市、臺中市共 6 處執行搜索（含律師事務所）並拘提律師陳○○（男，72 年次）、律師林○○（女，76 年次）、法務人員安○○（男，68 年次），通知律師鄭○○（女，77 年次）及助理黃○○（女，71 年次）等人到案，並查扣查手機 8 支、電腦主機 1 台、銀行存摺 9 本、筆記本 3 本、律師章戳 1 批、辯護委任資料 1 批(18 卷)、現金 16 萬 7,800 元等證物，全案依組織犯罪、加重詐欺、洗錢、洩密及律師法等罪嫌，解送臺灣雲林地方檢察署偵辦。經檢察官偵訊後，認為法務人員安○○、律師陳○○涉嫌刑法 132 條第 3 項之非公務員洩漏國防以外秘密、刑法第 339 條之 4 第 1 項之加重詐欺、組織犯罪條例第 3 條第 1 項後段參與組織、洗錢防制法第 14 條第 1 項一般洗錢等罪嫌，安○○另涉嫌違反律師法第 127 條第 1 項之無律師證書意圖營利而辦理訴訟罪嫌，其 2 人犯罪嫌疑重大，且有逃亡、勾串共犯或證人之虞，於 6 月 12 日上午，向臺灣雲林地方法院聲請羈押，安○○經裁定羈押，律師陳○○則裁定交保 20 萬元；律師鄭○○、律師林○○、助理黃○○經雲林地檢檢察官訊問後，認為其 2 人涉嫌前開洩密等罪嫌，犯罪嫌疑重大，但無羈押之必要，分別予以 2 萬元、15 萬元具保，助理黃○○請回。 6.查獲贓證物：手機 8 支、電腦主機 1 台、銀行存摺 9 本、筆記本 3 本、律師章戳 1 批、辯護委任資料 1 批(18 卷)、現金新臺幣 16 萬 7,800 元等證物。 資料來源：內政部警政署刑事警察局（2024 年 6 月 13 日）。 司法掮客偕同律師團疑似擔任假投資詐欺集團軍師。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=0631db90-fc71-4878-84ae-4c6508d6ec47，最後瀏覽日期：2024 年 8 月 6 日。

23	黑幫涉詐 刑事局威力掃蕩再偵破假投資水房集團	1.新聞發布日期：2024 年 7 月 10 日。 2.查獲時間：2024 年 6 月 19 日、24 及 26 日等 3 日。 3.查獲地點：新竹縣、新竹市及苗栗縣等地。 4.查獲嫌犯：廖○○(86 年次)等 10 名。 5.案情摘要：刑事警察局北部詐欺偵查中心（偵七大隊）分析被害人報案資料，發現詐欺水房藏身在新竹縣新埔鎮透天住宅內，專替股票假投資詐欺集團從事洗錢不法行為，詐欺集團引誘被害人加 LINE 好友，再拉被害人入投資群組，分享飆股投資標的，鼓吹被害人下載假投資 APP 或交易平臺進行投資，並指示被害人將投資款項匯入指定的人頭帳戶，再由轉帳水房透過網路轉帳方式，將詐欺款項層轉到虛設的公司帳戶，再由集團車手至金融機構臨櫃大額提領。案經報請新竹地檢署廉股檢察官指揮偵辦，並與新竹縣及臺北市警力共組專案小組，先在新竹縣竹北市及苗栗縣竹南鎮銀行拘捕正在提領詐欺贓款車手，再至新埔鎮透天住宅掃蕩轉帳水房成員，共查獲廖姓等 10 名嫌犯到案，並查扣上述贓證物，清查被害人逾 20 人，遭詐欺金額超過 2 億 3800 萬餘元，全案依涉犯詐欺、洗錢防制法及組織犯罪防制條例等罪嫌移送偵辦，具有幫派身分之廖姓主嫌等 3 人經法院裁定羈押。 6.查獲贓證物：犯罪不法所得 393 萬 7,000 元(現金 238 萬餘元、裁定扣押 155 萬餘元)、汽車 2 輛、銀行存摺、提款卡、公司大小章、手機 7 支及筆電等贓證物 資料來源：內政部警政署刑事警察局（2024 年 7 月 10 日）。黑幫涉詐 刑事局威力掃蕩再偵破假投資水房集團。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=bb83243e-c9fa-421d-8369-b64951c18020，最後瀏覽日期：2024 年 8 月 6 日。

24	**破獲偽裝家庭代工假投資詐欺水房、收簿集團**	1.新聞發布日期：2024 年 7 月 19 日。 2.查獲時間：2024 年 3 月 5 日、6 日。 3.查獲地點：高雄市鳳山區、屏東縣屏東市、里港鄉、 4.查獲嫌犯：王○○(1988 年次)、張○○（2001 年次）、林○○（1997 年次）、張○○（1998 年次）、潘○○（1995 年次）、王○○（1983 年次）、黃○○（1999 年次）、瑪○○（1999 年次）、許○○（2004 年次）、何○○（2000 年次）等 10 名。 5.案情摘要：刑事警察局南部打擊犯罪中心研析 165 反詐欺平台資料庫，得知有詐欺集團自 112 年 9 月起透過 FACEBOOK、LINE 等通訊軟體，以署名「唐三徵工」偽裝家庭代工吸引民眾詢問，佯稱需設定薪轉帳戶，成功騙取金融帳戶及提款卡密碼，另以 MangoMall、MataTrader、LSEX 虛擬貨幣等假投資網站，採「拉入、洗腦、完詐」階段，使被害人誤認投資獲利，擴大投資，將資金匯入至騙取之金融帳戶，再指派旗下車手於高雄、臺南、屏東等地區提領，自 112 年 9 月至 113 年 4 月詐欺不法所得超過新臺幣 3,000 餘萬元。該詐欺集團故意招募無前科或非本國籍擔任車手，增加警方辨識犯嫌身分難度，並以權利車懸掛偽造車牌作為交通工具，每日提領之贓款均轉換成泰達幣（USDT），企圖製造金流斷點，以規避查緝。刑事警察局南部打擊犯罪中心與屏東縣警察局內埔分局、高雄市政府警察局刑事警察大隊等共組專案小組，針對上開犯行報請臺灣屏東地方檢察署（愛股）洪檢察官綸謙指揮偵辦，經長期蒐證，於 113 年 3 月 5、6 日在高雄市鳳山區等地陸續拘捕該詐欺集團水房主謀王○○及旗下成員等 10 人並執行搜索，經管轄法院裁定水房主謀王○○等 6 人羈押禁見，將賡續擴大偵辦，以全力杜絕詐欺情事發生 6.查獲贓證物：自小客車 3 輛、手機 17 支、現金新臺幣 60 萬元、小型點鈔機、wifi 分享機、銀行金融卡、第三級毒品咖啡包、電子磅秤、黑莓卡、偽造車牌 資料來源：內政部警政署刑事警察局（2024 年 7 月 19 日）。破獲偽裝家庭代工假投資詐欺水房、收簿集團。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=921ff12d-b73a-458d-a354-63eb4d33dc03，最後瀏覽日期：2024 年 10 月 15 日。

25	**刑事局破獲假投資詐欺「一條龍」系統整合商案**	1.新聞發布日期：2024 年 7 月 17 日。 2.查獲時間：2024 年 6 月 5 日。 3.查獲地點：桃園市及高雄市 4.查獲嫌犯：邱○雯（78 年次）等 15 人 5.案情摘要：刑事局「打詐情資研析中心」，彙整分析近期假投資網站詐欺案件資料，產出網站工程師邱嫌之詐欺集團情資，交由偵查第九大隊偵辦，於 113 年 6 間執行專案積極向上溯源查獲假投資網站詐欺集團犯嫌共 15 人。該假投資詐欺系統整合商提供一條龍式服務，招募工程師替不同詐欺集團客製化開發假投資網站，提供雲端伺服器設定、後端網站開發、前端網頁設計、資料庫建置、網域名稱註冊、網站客服及手機簡訊驗證等全方位網站服務，如同詐欺集團之 SI（System Integration）廠商。詐欺集團先於社群媒體投放可賺取被動收入廣告，吸引被害人點擊廣告連結加入犯嫌 LINE 對話群組，再以投資為由要求被害人註冊假投資網站並以新臺幣 1 萬元左右小額入金，以降低被害人警覺，俟被害人欲提領獲利時，再以話術告知因被害人未參與網站活動、操作錯誤、繳稅、增加投資獲利等各式理由誘騙投入更多金額，以達詐欺之目的。本案清查計有被害人 110 名，假投資網站網址 78 個，財損金額逾新臺幣 1,020 萬元及加密貨幣 USDT 16 萬顆。專案小組見時機成熟，於 113 年 6 月間展開查緝行動，共查獲系統商、車手、人頭帳戶等犯嫌 15 人，並查扣犯案筆電、手機、SIM 卡、存摺、車輛、銀行帳戶、現金及不動產等贓證物，全案後續將依刑法詐欺罪嫌移請高雄地檢署偵辦。 6.查獲贓證物：筆電 1 臺、手機 5 支、車輛 1 部（市值約 173 萬元）、銀行帳戶 4 個、不動產 1 間（市值約 800 萬元）及贓款新臺幣 56 萬元等。 資料來源：內政部警政署刑事警察局（2024 年 7 月 17 日）。刑事局破獲假投資詐欺「一條龍」系統整合商案。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=ad86ff99-a069-4a47-8d34-09ae092b343e，最後瀏覽日期：2024 年 10 月 15 日。

26	**刑事局解構臉書超夯假投資廣告反向追查首謀難逃**	1.新聞發布日期：2024 年 7 月 30 日。 2.查獲時間：2024 年 5 月 21 日。 3.查獲地點：新北市新莊區、臺北市信義區。 4.查獲嫌犯：徐○○(78 年次、緬甸籍)等 5 人。 5.案情摘要：刑事警察局打詐「情資研析中心」分析假投資案件，發現被害人瀏覽臉書投資廣告，點入該專頁連結網址後加入犯嫌指定之 LINE 群組，初期詐團成員先以介紹飆股及股市資訊取信被害人，後續再以投資虛擬貨幣及代操保證獲利等話術，引導購買泰達幣，再轉至指定陌生人持有之虛幣錢包作為儲值金，俟被害人要求出金時，再以帶單失誤及操作不慎等理由，誆稱被害人資金已全部虧損，經被害人警覺遭詐始報案，訴警偵辦。)案經刑事警察局北部詐欺偵查中心(偵查第七大隊)與新北市新莊分局共組專案小組，報請臺北地檢署指揮偵辦，並於蒐證完後執行查緝，反向追查確認幕後操控徐姓主嫌與其他成員等 5 人到案，現場並查扣犯罪用手機、電腦等上揭扣案證物，警詢後依刑法詐欺、洗錢防制法及組織犯罪防制條例等罪嫌移送地檢署偵辦。 6.查獲贓證物：查扣犯案用手機 79 支、桌腦 11 部、筆電 1 部、公司文件等證物。 資料來源：內政部警政署刑事警察局（2024 年 7 月 30 日）。刑事局解構臉書超夯假投資廣告反向追查首謀難逃。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=ac89004e-7f3c-4667-aa7e-4b7a1bc7fa5d，最後瀏覽日期：2024 年 10 月 15 日。

27	**刑事局電信偵查大隊掃蕩全臺收受詐欺贓款虛擬貨幣門市阻斷不法金流命脈**	1.新聞發布日期：2024 年 8 月 6 日。 2.查獲時間：2023 年 6 月 16 日至 2024 年 5 月 14 日。 3.查獲地點：臺北、新北、桃園、新竹、臺中、高雄地區。 4.查獲嫌犯：門市負責人李○○(男，2001 年次)、吳○○(男，2002 年次)、孫○○(男，1996 年次)、張○○(男，1988 年次)、涂○○(男，1975 年次)、毛○○(男，1992 年次)、董○○(男，1975 年次)、莊○○(男，1991 年次)等 40 人。 5.案情摘要：案緣刑事警察局電信偵查大隊(第一隊)於去年接獲情資，查獲臺北市萬華區一處「慢○餐食」疑為不法幫派天道盟成員所經營之虛擬貨幣實體門市，並涉嫌為假投資詐欺之洗錢場所；經持續清查，發現有不法集團疑似與詐欺集團勾結，以「A+CARD」實體儲值卡及「Alfred Wallet」等虛擬貨幣交易系統，販售虛擬貨幣及隱匿幣流，並於全臺廣設實體門市大量收受遭詐欺被害人贓款，企圖偽裝合法以掩飾非法、製造金流斷點而規避法律責任。為擴大偵辦，經與臺中市政府警察局刑事警察大隊(打詐中心)等單位共組專案小組，並報請各管轄地檢署指揮，先向上溯源查獲「Alfred Wallet」系統商，續查緝「A+CARD」儲值卡印製商「莫○公司」，並循線擴大掃蕩全臺各地之不法虛擬貨幣洗錢門市。)案經專案小組分析「A+CARD」儲值卡通路經銷商資料，發現有大量被害人依詐欺集團指示，前往門市交付現金以購買虛擬貨幣轉出，而許多被害人認為既有實體門市，因此大大降低戒心而遭受詐欺。專案小組自去(112)年 6 月起至今 (113) 年 5 月發動數波搜索，分別持臺灣臺北、新北、桃園、臺中、高雄地方法院之搜索票及檢察官核發之拘票查緝主嫌及成員共 40 餘人到案，查扣現金約 475 萬元、虛擬貨幣合計約 732 萬元、動產不動產約 4,000 萬元，客戶名冊、帳冊、手機、經銷商監視器主機及硬碟等贓證物，涉案經銷商分別於今年 6 月依詐欺、洗錢等罪嫌移送至新北、桃園、高雄地檢署偵辦。經調查本案被害人大多是加入來路不明之通訊軟體投資群組後，群組內由詐團成員假扮投顧老師會每日提供股票分析課程，待取得被害人信任，投顧老師即邀請被害人參加虛擬貨幣投資方案，並指示被害人前往指定之虛擬貨幣經銷商門市購買虛擬貨幣而門市人員為企圖卸責，會先讓被害人填寫「反詐欺免責聲明書」，再由門市人員代操作將虛擬貨幣從經銷商轉至詐欺集團指定之電子錢包，以創造假交易取信被害人有成功投資。直到該假投資平台消失後，被害人才知被詐欺。案經專案小組掃蕩「慢○餐食」、「米○」、「金○」、「馬○斯」、「U○C」、「幣○數字」、「哈○」、「鑫○代」等數間不法實體虛擬貨幣門市，清查統計遭詐欺之被害人逾 300 餘人，總財損金額高達 4 億 5,000 萬元。 6.查獲贓證物：現金約新臺幣(下同)475 萬元、虛擬貨幣合計約 732 萬元、動產、不動產約 4,000 萬元，客戶名冊、帳冊、手機、經銷商監視器主機及硬碟等。 資料來源：內政部警政署刑事警察局（2024 年 8 月 6 日）。刑事局電信偵查大隊掃蕩全臺收受詐欺贓款虛擬貨幣門市阻斷不法金流命脈。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=05555842-9155-4644-badb-9b9429cd46b4，最後瀏覽日期：2024 年 10 月 15 日。

28	**全力打擊詐欺破獲假冒國外知名券商 APP 詐團**	1.新聞發布日期：2024 年 8 月 7 日。 2.查獲時間：2023 年 11 月至 2024 年 7 月。 3.查獲地點：新北市、臺北市、臺中市等地區。 4.查獲嫌犯：陳○○（65 年次）、莊○○（88 年次）等 27 人。 5.案情摘要：刑事警察局偵查第九大隊接獲被害人報案，稱於臉書上看見投資廣告宣稱投資股票保證獲利，加入 LINE 投資群組，並下載假投資 APP「野○證券」操作，歹徒誆騙儲值「野○證券」投資平臺須匯款至指定金融帳戶，被害人遂依指示匯款至指定金融帳戶後，款項隨即遭詐欺集團指派之車手提領一空，案經刑事警察局偵查第九大隊與各地警力共組專案小組，並報請臺灣新北地方檢察署明股葉育宏檢察官指揮偵辦，在新北市、臺北市、臺中市等地，查獲犯嫌 27 人，查扣作案用手機、假投資收款收據及公司大小章等贓證物，清查被害人數逾 38 人、財損金額逾新臺幣 4 億元。 6.查獲贓證物：手機 1 批、假投資收款收據 1 批、人頭門號 SIM 卡數張、公司大小章 1 批、現金新臺幣 1 萬元、扣押金融帳戶 450 萬元。 資料來源：內政部警政署刑事警察局（2024 年 8 月 7 日）。全力打擊詐欺破獲假冒國外知名券商 APP 詐團。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=05555842-9155-4644-badb-9b9429cd46b4，最後瀏覽日期：2024 年 10 月 15 日。

29	異界結盟詐團產業鏈 連鎖實體虛幣店遭團滅	1.新聞發布日期：2024 年 8 月 9 日。 2.查獲時間：2024 年 7 月 10 日。 3.查獲地點：臺北市、新北市、桃園市、臺中市、彰化縣、臺南市、高雄市等地區。 4.查獲嫌犯：幣店負責人周○○(59 年次)、周○○(87 年次)等 23 名 5.案情摘要：臺灣雲林地方檢察署(下稱雲林地檢)勤股檢察官段可芳日前偵辦網路投資暨虛擬貨幣詐欺集團案時，發現該集團疑透過實體交易所店面進行洗錢，遂指揮刑事警察局南部打擊犯罪中心(偵查第八大隊第三隊)、高雄市政府警察局、雲林縣警察局及臺中市政府警察局、法務部調查局中部地區機動工作站、臺北市調查處、臺中市調查處、桃園市調查處、雲林縣調查站、調查局資安工作站等單位共組專案小組溯源偵辦。本案緣為檢警大力掃蕩個人幣商後，周姓主嫌等人竟成立實體虛擬貨幣幣店方式，發起犯罪組織，參與詐欺集團運作，與詐欺集團共同從事加重詐欺、洗錢行為，其等方式為詐欺機房端先將被害人基本資料傳給實體幣店管理人，並引導被害人至幣店開立錢包，幣店員工形式上做 KYC 及提醒被害人不要被騙，並簽立免責聲明，藉此切割幣店責任，幣店收取現金後，旋將 USDT 轉入被害人錢包，再由詐欺機房引導被害人將 USDT 轉投資至假交易平台所指定之錢包，幣店再將被害人交付之現金存入金融帳戶內，結匯後以美金購買 USDT 洗錢至境外機房，藉此製造資金斷點規避查緝。本案實體幣店每日營業額初估高達 3900 萬元，且 113 年間被害人遭詐欺金額已高達 15 億元。專案小組於今(113)年 7 月 10 日持臺灣雲林地方法院(下稱雲林地院)核發之搜索票及雲林地檢(勤股)檢察官核發之拘票，在北中南共 13 處所同步執行搜索，扣得現金約 986 萬元，另凍結帳戶內現金 910 萬元，拘提 12 名被告到案，其中 10 人經檢察官偵訊後，分別以 5 萬元至 10 萬元具保；虛擬貨幣實體店面負責人經檢察官訊問後，向雲林地院聲請羈押禁見獲准，全案依組織犯罪、加重詐欺、洗錢等罪嫌，解送臺灣雲林地方檢察署偵辦。 6.查獲贓證物：查扣現金新臺幣(下同)986 萬餘元、警示帳戶凍結 918 萬餘元、奧迪 TT 汽車 1 台、手機 31 支、I pad 平板電腦 10 台、電腦主機 13 組、點鈔機 9 台、監視器 6 組、發票機 3 台、電子發票 1 批、sim 卡 4 張、牌價機 4 台、便條紙 9 本、員工教學內容 2 張、接待客人 SOP 4 張、教戰守則 5 張等證物。 資料來源：內政部警政署刑事警察局（2024 年 8 月 9 日）。異界結盟詐團產業鏈 連鎖實體虛幣店遭團滅。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=8fd7957e-c832-4d15-a0fd-e1dcc9381f1a，最後瀏覽日期：2024 年 10 月 15 日。

30	**持續加強打詐力道，南打破獲假投資詐團**	1.新聞發布日期：2024 年 8 月 16 日。 2.查獲時間：2024 年 3 月 26 日、3 月 31 日、6 月 30 日、7 月 29 日。 3.查獲地點：新北市、桃園市等地區 4.查獲嫌犯：胡○○等 12 名 5.案情摘要：刑事警察局南部打擊詐欺犯罪中心與新北市政府警察局樹林分局等單位偵辦詐欺案，緝獲提款車手到案，依據到案犯嫌指述並依相關事證溯源追查，偵悉有一組織性詐欺集團於幕後指揮操縱，遂檢具事證報請臺灣新北地方檢察署(下稱新北地檢署)檢察官王雪鴻指揮偵辦。據查主嫌胡○○等人與位於大陸地區詐欺機房結盟，由機房架設「Atlant」假投資網站，以保證獲利、穩賺不賠等話術誘騙被害人投資。同時由胡○○在臺招募犯嫌王○○等 6 人擔任車手，指揮車手領取詐欺包裹、提領詐欺贓款、洗錢等犯罪活動；另胡○○為逃避查緝，與犯嫌葉○○同謀，由葉○○等人以私行拘禁等非法手段取得人頭帳戶後，交給胡○○轉交予所屬詐欺集團，用以漂洗不法所得。專案小組依偵蒐調查所獲資料，於 2024 年 3 月 26 日起共執行 3 波查緝行動，緝獲胡○○等 12 人到案，初步清查被害人逾 38 人，詐欺金額逾新臺幣 424 萬元。犯嫌胡○○等 4 人經臺灣新北地方法院裁定羈押禁見。 6.查獲贓證物：手機 15 支、新臺幣 8 萬 9,400 元、開山刀 1 把、黑莓卡 5 張、印章 10 個、本票 61 張等證物。 資料來源：內政部警政署刑事警察局（2024 年 8 月 16 日）。持續加強打詐力道，南打破獲假投資詐團。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=91bef8c4-76ea-484d-b56b-e2c93e1539ca，最後瀏覽日期：2024 年 10 月 15 日。

31	**假幣商真洗錢！兄妹共創虛擬貨幣公司洗錢遭警逮**	1.新聞發布日期：2024 年 8 月 28 日。 2.查獲時間：2024 年 4 月 16 日、7 月 1 日、7 月 26 日。 3.查獲地點：臺南市、高雄市、臺北市、嘉義縣等地。 4.查獲嫌犯：主嫌林○○（男）、車手林○○（男）等 19 人。 5.案情摘要：刑事警察局打擊詐欺情資研析小組彙整分析假投資詐欺案件資料，得知有數名被害人於通訊軟體 Line 遭他人加入投資群組，並誆稱有老師可幫忙代操股票獲利，被害人見群組內所報明牌均有獲利，即不疑有他，自 2023 年 11 月至 2024 年 1 月期間陸續匯款新臺幣 1,400 餘萬元進行股票投資，惟被害人欲將獲利出金時，卻遲遲無法收到獲利款項，被害人方驚覺遭詐欺，刑事局電信偵查大隊遂與嘉義市政府警察局刑事警察大隊、臺北市政府警察局大安分局、高雄市政府警察局六龜分局等單位共組專案小組，並報請臺灣臺北地方檢察署指揮偵辦。案經專案小組深入追查發現，該集團以林姓兄妹為首，於臺南市東區創設虛擬貨幣交易公司，並以該處為詐欺洗錢之據點，招攬數名親友作為自願性人頭帳戶及車手，並透過虛擬貨幣交易平台，以創造對話紀錄營造從事虛擬貨幣買、賣之假象，企圖掩飾詐欺洗錢之犯行，全案歷經數月偵辦，專案小組見時機成熟，在臺南市、高雄市、臺北市及嘉義縣等地執行 3 波查緝行動，查獲林嫌等 19 人，並查扣新臺幣 100 餘萬元、電腦(含主機)6 臺、手機 23 支、幣商公司營運資料 1 批等證物，全案依刑法詐欺罪、洗錢防制法等罪移請臺灣臺北地方檢察署偵辦。 6.查獲贓證物：新臺幣 100 餘萬元、電腦(含主機)6 臺、手機 23 支、幣商公司營運資料 1 批、公司大小章 1 副、存摺 22 本及提款卡 25 張等證物。 資料來源：內政部警政署刑事警察局（2024 年 8 月 28 日）。假幣商真洗錢！兄妹共創虛擬貨幣公司洗錢遭警逮。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=5cb9b5cc-22c9-43d1-aed0-0a171caae813，最後瀏覽日期：2024 年 10 月 15 日。

32	**刑事局偵破假投資詐欺集團案外案 3 律師涉洩密**	1.新聞發布日期：2024 年 8 月 29 日。 2.查獲時間：2024 年 8 月 26 日。 3.查獲地點：臺南市（東區、中西區、安平區、安南區）。 4.查獲嫌犯：陳○○（1983 年次）、黃○○（1985 年次）、唐○○（1990 年次）。 5.案情摘要：刑事警察局南部打擊犯罪中心日前偵辦一起網路假投資詐欺案件，報請臺灣屏東地方檢察署檢察官（月股）李忠勳指揮偵辦，並與屏東縣警察局內埔分局等單位共組專案小組，針對該詐欺集團水房、車手成員發動多波拘提搜索，偵辦過程中發現該詐團旗下多名成員於各地犯下多起詐欺案件均是委任現年 42 歲的陳姓律師或其名下律師事務所唐姓律師協助陪偵，甚至為規避檢警溯源調查，刻意聯絡其他律師事務所有私交的黃姓律師替該詐團辯護，疑似將檢警偵辦內容洩漏予詐團成員，藉以規避刑責。專案小組見時機成熟，於 8 月 26 日持臺灣屏東地方法院核發之搜索票至臺南市共 5 處執行搜索，並拘捕陳、黃、唐姓等 3 位律師到案，檢方偵訊後，認為陳○○、唐○○、黃○○等 3 名律師涉嫌洩漏國防以外秘密、加重詐欺、參與組織、洗錢等罪嫌嫌疑重大，且有逃亡、勾串共犯或證人之虞，檢方於 8 月 27 日晚間向屏東地院聲請羈押。 6.查獲贓證物：手機 5 支、（筆記型）電腦 5 臺、筆記本 1 本、監視器主機 1 臺等證物。 資料來源：內政部警政署刑事警察局（2024 年 8 月 29 日）。刑事局偵破假投資詐欺集團案外案 3 律師涉洩密。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=454d2b26-f196-4967-b878-8846af2285d3，最後瀏覽日期：2024 年 10 月 15 日。

33	**刑事查局破獲國內知名幫派假投資地下期貨機房、水房**	1.新聞發布日期：2024 年 9 月 2 日。 2.查獲時間：2023 年 10 月 25 日、113 年 7 月 1 日、2024 年 8 月 19 日。 3.查獲地點：臺北市中山區、新北市中和區、臺中市東區。 4.查獲嫌犯：陳○○(男、1996 年次)、劉○○(男、1996 年次)、曹○○(女、1984 年次)、林○○(女、1989 年次)等共計 24 人等。。 5.案情摘要：國內近年股市、期貨指數等投資市場交易熱絡，吸引民眾紛紛湧入投資，有幫派分子趁隙成立地下期貨機房，招募有證卷公司工作背景之人員擔任機房幹部，以其背景知識誘騙民眾稱「該公司獨家取得國外知名券商代理、國內期貨市場均透過該券商下單、高報酬、低風險」等話術，吸引民眾投資，以可竄改號碼之網路電話隨機撥號攬客，再利用多家人頭公司帳戶收取贓款，層層轉帳、洗錢，利用車手提領出贓款，製造「死轉手斷點」，民眾投入資金後，以不予出金之方式，致民眾受損，有被害人王○○等 10 人提出詐欺等告訴，刑事警察局偵查第四大隊獲知上情，遂報請臺灣臺北地方檢察署指揮偵辦。專案小組調查發現陳姓主嫌為天○盟太○會幫派成員，該幫派曾在臺北市、新北市地區涉及多起暴力案件，並插足詐欺犯罪，由陳姓主嫌在臺北市中山區等地承租商辦，提供作為機房使用，並結合臺中市東區轉帳水房，從事上述犯罪。為阻斷該幫派金流來源、溯源刨根，歷經半年蒐證，掌握犯嫌涉案事實，於 2024 年 7 月 1 日會同臺北市政府警察局、新北市政府警察局中和分局、桃園市政府警察局兵分多路，前往臺北市中山區、新北市中和區機房、臺中市東區水房多處同時打擊，當場查扣電腦等贓證物，並凍結涉案帳戶內資金達 1,000 餘萬元，共計查獲陳姓主嫌及共犯等 24 名，經統計涉案帳戶自 2023 年 9 月迄今收入高達 3,000 餘萬元，全案依違法組織犯罪防制條例、期貨交易法、刑法詐欺等罪移送地檢署偵辦。 6.查獲贓證物：查扣電腦 30 台、手機 77 台、網路電話 20 台、教戰守則、叩客名單、開戶資料、現金新臺幣 30 萬元等贓證物。 資料來源：內政部警政署刑事警察局（2024 年 9 月 2 日）。刑事查局破獲國內知名幫派假投資地下期貨機房、水房。臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=88952177-24b0-47c4-b14f-4e3ba7fee661，最後瀏覽日期：2024 年 10 月 15 日。

34	**刑事局南打掃蕩黑幫經營假投資詐欺集團 14 名犯嫌落網**	1.新聞發布日期：2024 年 9 月 3 日。 2.查獲時間：2024 年 3 月至 7 月期間。 3.查獲地點：高雄市、桃園市等地 4.查獲嫌犯：許○○(男、33 歲)等 14 人。 5.案情摘要：刑事局南部打擊犯罪中心針對自稱「滿○投資公司、永○投資公司」等虛設投資公司之名義詐欺國人假投資案件被害人資料進行分析後發現國內有 33 名被害人，財損金額逾數仟萬元，遂擴大偵辦。該詐欺集團透過社群媒體以高獲利及假冒投顧老師等手法招攬被害人加入假投資詐欺群組，並依指示安裝手機 APP 應用程式；另為取信被害人，詐欺集團先透過應用程式上不實數據使被害人誤信有獲益，並先匯款數仟至數萬元不等小額獲利予被害人，被害人誤信有賺頭而加碼進場匯款至犯嫌指定之人頭帳戶。全案自 2024 年 3 月起執行 3 波查緝行動，查緝許姓與劉姓及同案共犯等 14 人到案，該集團係以召募急需用錢之車手加入，指揮旗下成員設立人頭公司，再由集團車手至金融機構臨櫃提領贓款，偵辦期間亦發現集團除招攬成員擔任國內臨櫃車手外，如車手表現不佳則指派赴境外從事詐欺機房工作，上述犯嫌依詐欺、洗錢防制法及組織犯罪防制條例等罪嫌解送該管地檢署偵辦，另針對涉案層轉帳戶贓款向該管地方法院聲請扣押裁定獲准。 6.查獲贓證物：存摺、手機、點鈔機、棍棒等證物 1 批、扣押裁定贓款 168 萬元。) 資料來源：內政部警政署刑事警察局（2024 年 9 月 3 日）。刑事局南打掃蕩黑幫經營假投資詐欺集團 14 名犯嫌落網。臺北：《內政部警政署刑事警察局新聞發布》。取自： https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=b0330ef3-b328-471f-b27c-7d4a7e900641，最後瀏覽日期：2024 年 10 月 15 日。

35	刑事局破獲「假IG網美」投資詐欺機房案	1.新聞發布日期：2024 年 9 月 24 日。 2.查獲時間：2024 年 6 月、9 月。 3.查獲地點：高雄市、臺中市、臺南市。 4.查獲嫌犯：李○○(男、83 年次)等 8 人。 5.案情摘要：刑事警察局打詐中心情資研析小組分析 165 假投資案件，發現多名被害人見網美於 Instagram 限時動態分享投資獲利訊息，進而投資遭詐欺，刑事局偵一大隊接辦後，與高雄市政府警察局刑事警察大隊偵五隊、彰化縣警察局刑事警察大隊科偵隊、臺南市政府警察局永康分局共組專案小組，並報請臺灣高雄地方檢察署指揮偵辦。經專案小組深入追查，發現該詐欺集團假藉網美名義謊稱【○正】、【○漢】、【○富】、【○路】、【○度】等合法投資股份有限公司，具有高投資報酬率、穩賺不賠等話術，誘騙被害人投資，再變造高收益紀錄，讓被害人信以為真，持續入金，若被害人欲獲利出金時，詐欺集團會再以須繳交信託費用等理由延遲出金，交易自始至終均無法成交。該詐欺集團為了躲避警方查緝，以個人工作室經營詐欺機房，分散查緝風險；惟經專案小組積極縝密蒐證，確認該詐欺集團運行模式，於 2024 年 6 月在高雄市及臺中市同步發動第一波拘提、搜索行動，查獲主嫌等 3 人經營假投資詐欺個人機房及 2 名販賣人頭卡犯嫌，後續溯源追查，再於 9 月 3 日在高雄市及臺南市查獲 1 處個人詐欺機房、擷取美女照片製圖假網美人員及系統商等 3 名犯嫌，全案依違反刑法詐欺等罪嫌移送臺灣高雄地方檢察署偵辦。 6.查獲贓證物：新臺幣 296 萬元、手機 21 支、電腦 5 台、筆電 3 台、分享器 9 台、路由器 1 組、點鈔機 1 台、自小客 4 台。 資料來源：內政部警政署刑事警察局（2024 年 9 月 24 日）。刑事局破獲「假 IG 網美」投資詐欺機房案臺北：《內政部警政署刑事警察局新聞發布》。取自：https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=af0f4dc9-e252-4e41-b50f-219a35bb8887，最後瀏覽日期：2024 年 10 月 15 日。

附錄二之一 刑事警察人員訪談大綱

訪談時間：

年　　月　　日　　時　　分起　　時　　分止，共　　分。

地點：

次數： 次

一、個人基本資料

(一) 姓名：

(二) 性別及年齡（出生年）：

(三) 教育程度：

(四) 服務單位：

(五) 業務職掌：

二、訪談內容

項次	研究概念	訪談問題
(一)	犯罪者的理性選擇	依您對電信網路假投資詐欺犯罪的觀察，引發犯罪者初次參與犯罪的動機及目的為何?影響犯罪人初次犯罪因素為何？
		承上，累犯者的比率為何？累犯的犯罪動機及目的為何?影響犯罪人重複犯罪因素為何？與初次犯罪者有何不同？
		承上，促使犯罪者終止犯罪的因素為何？
(二)	促進犯罪發生的三要素	請依您的專業知能與辦案經驗，詳述以下三個促成電信網路假投資詐欺犯罪發生不可或缺的環境因素： 1.促進有動機的犯罪者出現的情境為何？及影響因素？ 2.促進民眾成為被害標的的情境為何？及影響因素？ 3.促進具有監控能力者不在場的情境為何？及影響因素？
(三)	犯罪者的生活形態	請依您對電信網路假投資詐欺犯罪的觀察，促成犯罪者參與犯罪的日常生活模式為何？犯罪者有參與黑道幫派？或黑道幫派有介入犯罪組織?犯罪者的性別？年紀？學歷？職業？
(四)	被害人的生活形態	承上，造成被害人受害的日常生活模式為何？有重複被害情形?重複被害原因為何?
		承上，犯罪者與被害人接觸的主要管道為何(電話、簡訊、網路、社群通訊軟體)？
(五)	電信網路假投資詐欺的犯罪腳本	請依您的專業知能與辦案經驗，詳述以下電信網路假投資詐欺犯罪集團犯罪前準備行為： 1.如何召募詐欺機房電話手、提領贓款車手、詐欺廣告投放商、APP 開發工程師、資通系統架設商、銀行從業人員、律師、代書等各專業領域人員參與犯罪？ 2.如何取得民眾個資?

		3.如何取得金融人頭帳戶？ 4.如何取得虛擬通貨管道？ 5.如何取得電信人頭門號 6.如何製作假投資廣告？ 7.其他準備行為？
		承上，請詳述是類犯罪以下主要犯罪行為： 1.犯罪集團（機房、水房、車手）的運作模式？ 2.使用的犯罪工具？ 3.詐欺廣告投放管道及方式？ 4.使用何種社群通訊軟體？群組的成員？如何運作？ 5.如何小額出金？出金管道？ 6.被害人如何交付款項？ 7.跨國(境)蔓延情形？ 8.其他犯罪行為？
		承上，是類犯罪詐得被害人財物後洗錢管道？隱匿贓款的手法？如何脫免執法人員查緝逮捕等等？
		承上，民眾被害的主要關鍵為何?如何預防？
		承上，**警察**阻斷犯罪的主要關鍵為何？及阻斷的方法？
(六)	**警察**防制電信網路假投資詐欺犯罪策略及機制	請依您的專業知能，詳述**警察**防制電信網路假投資詐欺犯罪策略及機制？
		承上，有無需要精進之處?
(七)	**警察**防制電信網路假投資詐欺犯罪成效	請依您的專業知能，詳述**警察**防制電信網路假投資詐欺犯罪的成效?
		承上，有何不足之處?
(八)	**警察**防制電信網路假投資詐欺犯罪的困境	請依您的專業知能與辦案經驗，詳述**警察**防制電信網路假投資詐欺犯罪在識詐、堵詐、防詐、阻詐、懲詐等面向上面臨那些困境？
(九)	對**警察**防制電信網路假投資詐欺犯罪的建議	請依您的專業知能與辦案經驗，詳述對**警察**防制電信網路假投資詐欺犯罪在識詐、堵詐、防詐、阻詐、懲詐等面向上策略的建議？

附錄二之二 金融監督管理委員會人員訪談大綱

訪談時間：

年　　月　　日，　　時　　分起　　時　　分止，共　　分。

地點：

次數： 次

一、個人基本資料

(一) 姓名：

(二) 性別及年齡（出生年）:

(三) 教育程度：

(四) 婚姻狀況：

(五) 服務單位：

(六) 業務職掌：

二、訪談內容

項次	研究概念	訪談問題
(一)	電信網路假投資詐欺的犯罪腳本	請依您的專業知能，詳述犯罪集團在犯罪前如何完成與**金融有關**的準備行為： 1.如何取得**金融**人頭帳戶？ 2.如何取得**虛擬通貨**管道？ 3.其他有關**金融**的準備行為
		承上，請詳述是類犯罪與**金融有關**的主要犯罪行為： 1.**金流**的運作模式？ 2.犯罪時使用的**金融**工具？ 3.小額出金的管道？ 4.被害人交付款項的**金融**工具？ 5.跨國(境)蔓延情形？
		承上，是類犯罪詐得被害人財物後**洗錢管道**？**隱匿贓款**的手法？如何脫免執法人員查緝？
		承上，民眾被害的主要關鍵（**與金融有關**）為何?
		承上，阻斷犯罪的主要關鍵（**與金融有關**）為何？
(二)	**與金融有關的**防制電信網路假投資詐欺犯罪策略及機制	請依您的專業知能，詳述**金融機構**防制電信網路假投資詐欺犯罪策略及機制？
		承上，有何不足之處?
(三)	**與金融有關的**防制電信網路假投資詐	請依您的專業知能，詳述**金融機構**防制電信網路假投資詐欺犯罪的成效?

	欺犯罪成效	承上，有無需要精進之處?
(四)	**與金融有關的**防制電信網路假投資詐欺犯罪的困境	請依您的專業知能，詳述**金融機構**防制電信網路假投資詐欺犯罪在識詐、堵詐、防詐、阻詐、懲詐等面向上面臨那些困境？
(五)	對防制電信網路假投資詐欺犯罪的建議（**與金融有關**）	請依您的專業知能，詳述對防制電信網路假投資詐欺犯罪在識詐、堵詐、防詐、阻詐、懲詐等面向上（**與金融有關**）策略的建議？

附錄二之三 國家通訊傳播委員會人員訪談大綱

訪談時間：

年　月　日，　時　分起　時　分止，共　分。

地點：

次數： 次

一、個人基本資料

(一) 姓名：

(二) 性別及年齡（出生年）：

(三) 教育程度：

(四) 婚姻狀況：

(五) 服務單位：

(六) 業務職掌：

二、訪談內容

項次	研究概念	訪談問題
(一)	電信網路假投資詐欺的犯罪腳本	請依您的專業知能，詳述犯罪集團在犯罪前如何完成與**電信有關**的準備行為： 1.如何取得民眾個資? 2.如何取得**電信人頭門號** 3.其他準備行為？
		承上，請詳述是類犯罪與**電信有關**的主要犯罪行為： 1.**電信流**的運作模式？ 2.犯罪所使用的**電信**工具？ 3.跨國(境)蔓延情形？ 4．其他犯罪行為？
		承上，民眾被害的主要關鍵（**與電信有關**）為何?
		承上，阻斷犯罪的主要關鍵（**與電信有關**）為何？
(二)	**與電信有關的**防制電信網路假投資詐欺犯罪策略及機制	請依您的專業知能，詳述**與電信有關的**防制電信網路假投資詐欺犯罪策略及機制？
		承上，有何不足之處?
(三)	**與電信有關的**防制電信網路假投資詐欺犯罪成效	請依您的專業知能，詳述防制電信網路假投資詐欺犯罪的成效（**與電信有關**）?
		承上，有無需要精進之處?
(四)	**與電信有關的**防制電信網路假投資詐	請依您的專業知能，詳述**電信公司**防制電信網路假投資詐欺犯罪在識詐、堵詐、防詐、阻詐、懲詐等面向上面臨那些困

	欺犯罪的困境	境？
(五)	對防制電信網路假投資詐欺犯罪的建議（**與電信有關**）	請依您的專業知能，詳述對防制電信網路假投資詐欺犯罪在識詐、堵詐、防詐、阻詐、懲詐等面向上（**與電信有關**）的策略建議？

附錄二之四 數位發展部人員及民間業者訪談大綱

訪談時間：

年　月　日　時　分起　時　分止，共　分。

地點：

次數： 次

一、個人基本資料

(一) 姓名：

(二) 性別及年齡（出生年）:

(三) 教育程度：

(四) 婚姻狀況：

(五) 服務單位：

(六) 業務職掌：

二、訪談內容

項次	研究概念	訪談問題
(一)	電信網路假投資詐欺的犯罪腳本	請依您的專業知能，詳述犯罪集團在犯罪前如何完成**與網路有關**的準備行為： 1.如何取得民眾個資? 2.其他有關**網路**的準備行為
		承上，請詳述是類犯罪**與網路有關**的主要犯罪行為： 1.**網路流**的運作模式？ 2.犯罪時使用的**網路工具**？ 3.如何成立**通訊群組**？使用之**社群軟體**? 4.被害人交付款項的**網路工具**？ 5.跨國(境)蔓延情形？
		承上，民眾被害的主要關鍵（**與網路有關**）為何?
		承上，阻斷犯罪的主要關鍵（**與網路有關**）為何？
(二)	與網路有關的防制電信網路假投資詐欺犯罪策略及機制	請依您的專業知能，詳述與**網路有關的**防制電信網路假投資詐欺犯罪策略及機制？
		承上，有何不足之處?
(三)	與網路有關的防制電信網路假投資詐欺犯罪成效	請依您的專業知能，詳述防制電信網路假投資詐欺犯罪的成效（**與網路有關**）?
		承上，有無需要精進之處?
(四)	與網路有關的防制電信網路假投資詐	請依您的專業知能，詳述防制電信網路假投資詐欺犯罪在識詐、堵詐、防詐、阻詐、懲詐等面向上面臨（**與網路有關**）那

	欺犯罪的困境	些困境？
(五)	對防制電信網路假投資詐欺犯罪的建議（**與網路有關**）	請依您的專業知能，詳述防制電信網路假投資詐欺犯罪策略在識詐、堵詐、防詐、阻詐、懲詐等面向上（**與網路有關**）的建議？

附錄三 訪談同意書

_____先生 女士，您好：

我是中央警察大學警察政策研究所博士生，正在進行「警察防制電信網路詐欺犯罪策略之研究：以假投資詐欺為中心」的研究，希望您能提供寶貴的經驗分享與協助，使社會大眾對於電信詐欺犯罪有更深入的認識與瞭解，您的參與對於研究深具重要意義。

為了資料整理與分析的正確性，避免資料遺漏及完整忠實呈現您的表達內容，因此將在訪談過程中進行錄音與筆記，錄音訪談資料僅供本研究使用，研究分析完後會立即銷毀。這是一項純學術的研究，對您自身的利益不會有任何的損害，過程中您有絕對自由來決定揭露隱私的程度，也有權利隨時提出疑義或終止訪談。本研究所蒐集的訪談資料將會呈現在書面研究報告中，有關您個人隱私部分，絕對以匿名處理。您的談話則完全保密，內容在經過整理之後，才會採用為研究資料，請您放心。

如果您同意參與本研究的訪談，煩請於下方簽名，非常感謝您的協助！

同意人（簽名）：_____研究者（簽名）：_____
日期：　　年　　月　　日

研究者：蘇信雄
聯絡電話：(03)3282321
電子信箱：bear58170630@gmail.com.
聯絡地址：333322 桃園市龜山區大崗里樹人路 56 號 中央警察大學警察政策研究所