出國報告（出國類別：訪問）

2024 全球防詐高峰會亞洲場

服務機關：刑事警察局

姓名職稱：科長林書立

派赴國家：新加坡

出國期間：2024 年 10 月 20 日至 10 月 22 日

報告日期：2025 年 1 月 8 日

摘要

網路詐騙是通報最多的犯罪類型。全球大多數國家當前有關犯罪報告中顯示有20%-50%與網路詐欺有關。這僅是冰山一角，因為國際間推估只有 7%的詐騙受害者向執法部門舉報犯罪行為。去年全球損失近 1.026 兆美元，影響到全球四分之一的人口，各國亟需迅速採取行動。

全球反詐騙高峰會（GASS）於 2024 年 10 月 21 日至 22 日，假新加坡 Suntec 會議展覽中心舉行。高峰會的目標是將政府、消費者和金融機構、執法機構、知名保護機構和網路安全公司齊聚一起，分享經驗並制定聯合行動，以保護消費者免受詐騙。

本次會議緊接於 2024 年 6 月在歐洲舉行的全球反詐騙高峰會辦理，吸引了來自 100 多個國家 1,200 多名線上嘉賓和 360 名實際蒞臨嘉賓參加。強調必須採取統一行動，打擊日益複雜的網路詐騙網路。

2024 年，GASS 將舉辦三場活動，活動橫跨三大洲，下一場活動將在美洲進行，旨在透過利害關係人共同匯集資源、分享情報並制定協調一致的策略，以破壞和瓦解網路詐騙的複雜網絡。因為惟有齊心協力、統一行動，才能有效打擊普遍存在的網路詐騙威脅。

我刑事警察局預防科長林書立獲邀參加開幕首日主場地之「縮短訊息共享與犯罪偵查之差距(Bridging the Gap Between Signal Sharing and Criminal Investigations)」與英國警方經濟犯罪中心及 Abusix 智慧電郵安全增強公司創辦人等進行與談。

目次

本文

一、目的

新加坡一直是國際間受到高度重視的商業中心，國民素質高、外語能力強，尤其近年來在國際調查合作等，都有十分亮眼的表現。因此，本局以犯罪偵查合作與公私協力為前提參與此次論壇討論交流活動，另安排會後專訪新加坡警察部隊之打擊詐騙中心(1799)，期能透過參與國際打擊詐欺組織的交流活動，汲取全球打擊詐欺現況，同時分享我國在公私協力合作方面的進步發展。

二、過程

(一)行程

1.第一天行程（10 月 20 日）

桃園國際機場搭機，抵達新加坡，由新加坡警察部隊友軍派員接待，進行文化參訪：國會大廈／高等法院／魚尾獅公園／濱海藝術中心／金沙娛樂城／新加坡鄰里大樓參訪後，前往勘查第二天會議地點。

2.第二天行程（10 月 21 日）

前往 SUNTEC 城會議展覽中心，SUNTEC 城是新加坡前總理李光耀邀請香港首富李嘉誠等 11 位香港富商到新加坡考察後，決議集體合資建造一座建築群，SUNTEC 的五座大樓囊括金融、觀光、購物及娛樂等功能，設計就像一隻平放的左手，五根手指頭，手掌的部分則是一座噴泉－財富之泉，這也是 SUNTEC 城的地標。

3.第三天行程（10 月 22 日）

參訪新加坡警察部隊刑事偵查局／打擊詐欺犯罪中心後搭乘下午班機返台。

(二)經過

1.參加全球反詐欺論壇摘要：

GASA《亞洲詐騙調查報告》針對亞洲多達 13 個地區、將近 2 萬 5,000 名受訪者進行調查，列出亞洲各國最常見的十大詐騙手法，整體而言「個資盜用」、「投資詐騙」與「購物詐騙」為亞洲所有國家共同的隱憂，另外《亞洲詐騙調查報告 - 台灣篇》，深度解析台灣詐騙面貌，據報告指出台灣有超過五成民眾每週都會接觸到詐騙，更有近三成的受騙者在與詐騙接觸後一小時內支付金錢或提供個資。報告也進一步揭露多元詐騙手法與管道，為企業和民眾提供最新防詐趨勢而台灣民眾遭遇最多的威脅為個資盜用（24%），這與日本、新加坡、越南、中國等六個國家的情況相似，顯示個人資料安全問題日益嚴峻，而在韓國、馬來西亞、巴基斯坦與印尼則以投資詐騙最猖獗[1]。

[1] 詳如 GASA 與 WHOSCALL 官網；https://whoscall.com/zh-hant/blog/articles/1400-the-state-of-scams-in-taiwan-2024

本報告不同於警政署以受理報案為依據，而是依據調查民眾收到到詐騙訊息分析而來，因此顯示出許多因為無財損而未報案的詐欺手法，例如我國民眾接觸到詐騙訊息最多的是「個資盜用」，再其次是購物詐騙（15%）和企業冒名詐騙（13%），持續威脅消費者的財產安全。假冒親友詐騙與中獎、優惠詐騙則同以 11% 並列第四，反映詐騙手法多樣化且靈活運用人際信任及促銷心理。其他常見的詐騙手法還包括中獎詐騙(第五)、投資詐騙(第六)、假帳單詐騙及慈善捐款詐騙等，突顯詐騙主要從騙取個資開始，因此提醒民眾防範個資外洩，亦成為現代社會不可忽視的重要課題。

圖 1 台灣詐騙手法排名

來源:全球防詐聯盟 GASA（Global Anti-Scam Alliance）及 ScamAdviser 發布《亞洲詐騙調查報告》

(1) 受騙時間極短！

遇到不同詐騙手法時，民眾的反應時間也不同，報告也指出接近三成（27%）的台灣受騙民眾在首次接觸詐騙後一小時內，即落入詐騙陷阱，進而付款或提供個資，反映出詐騙運用恐慌或貪婪的心態，讓受害者幾乎沒有反應和防範的時間。值得注意的是，約有 19% 的受騙者會在幾天內上當，另外 15% 的受害者情況則更為複雜，騙局持續時間從數週、數月甚至數年不等，呼應投資與交友等類型詐騙從建立信任到詐財，「養、套、殺」三個階段詐騙集團要花上至少 1 個月設局。

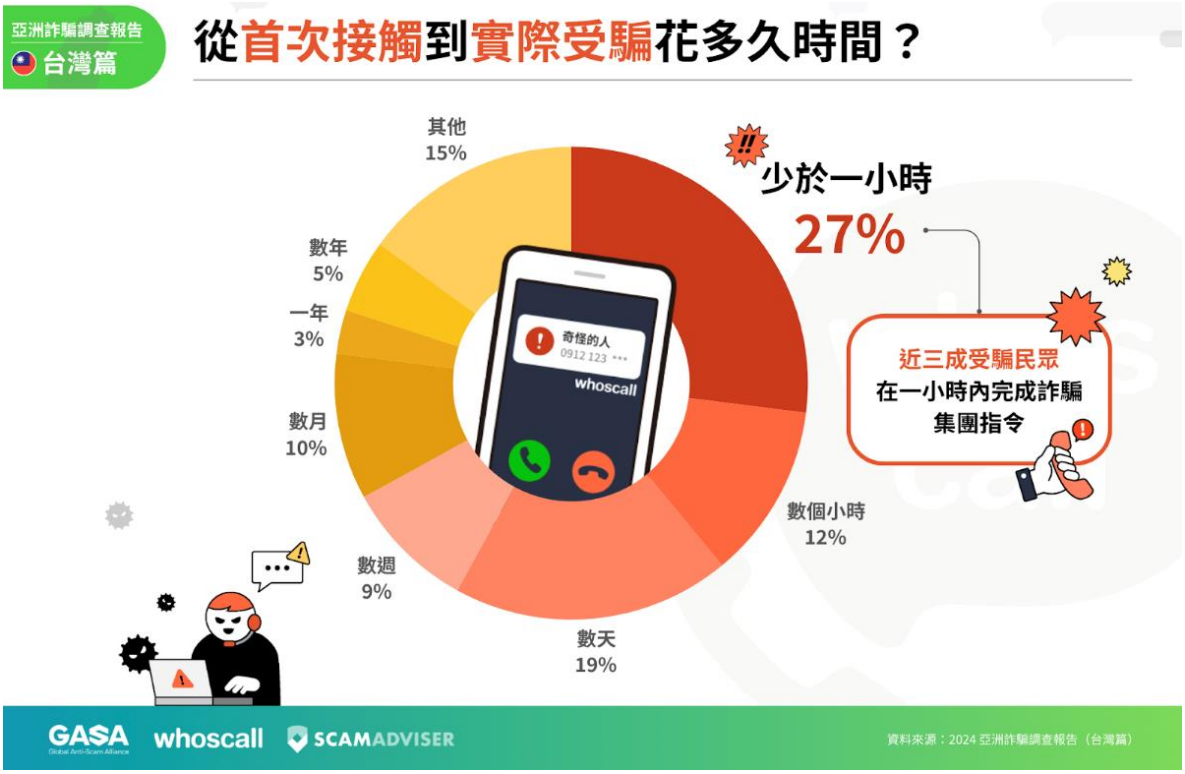

圖 2 台灣近三成詐騙受害者在一小時內上當

(2) 詐騙電話、簡訊無所不在！社群平台成新興詐騙熱點

隨著民眾接觸資訊的方式日益多元，詐騙集團的手法也逐漸滲透至日常資訊中。根據 調查報告分析，三大詐騙管道為電話、社群平台、簡訊，有超過五成民眾都曾在上述管道接觸過詐騙。台灣數位信任協會 9 月發布的《冒名詐騙報告》也指出，去年至今年 4 月，冒名類型的高風險電話和簡訊高達近 300 萬筆，詐騙的話術多元、手法不斷翻新，商品促銷、繳費逾期、急難捐款都是常見的手法。這也強調了防詐工具的重要性，例如即時防詐辨識服務，能協助民眾迅速識別可疑來電、簡訊、網站，並在短時間內作出判斷，有效降低受騙風險。

值得注意的是，社群平台詐騙的成長速度最快，與去年相比增加了 21%，並躍升為第二大詐騙管道。其他常見的詐騙媒介還包含通訊軟體、Email、電商平台及交友軟體等，顯示詐騙逐漸轉移至數位平台行騙。然而，仍有超過兩成的民眾表示曾收過詐騙包裹或信件，說明實體詐騙與線上詐騙依然並存。

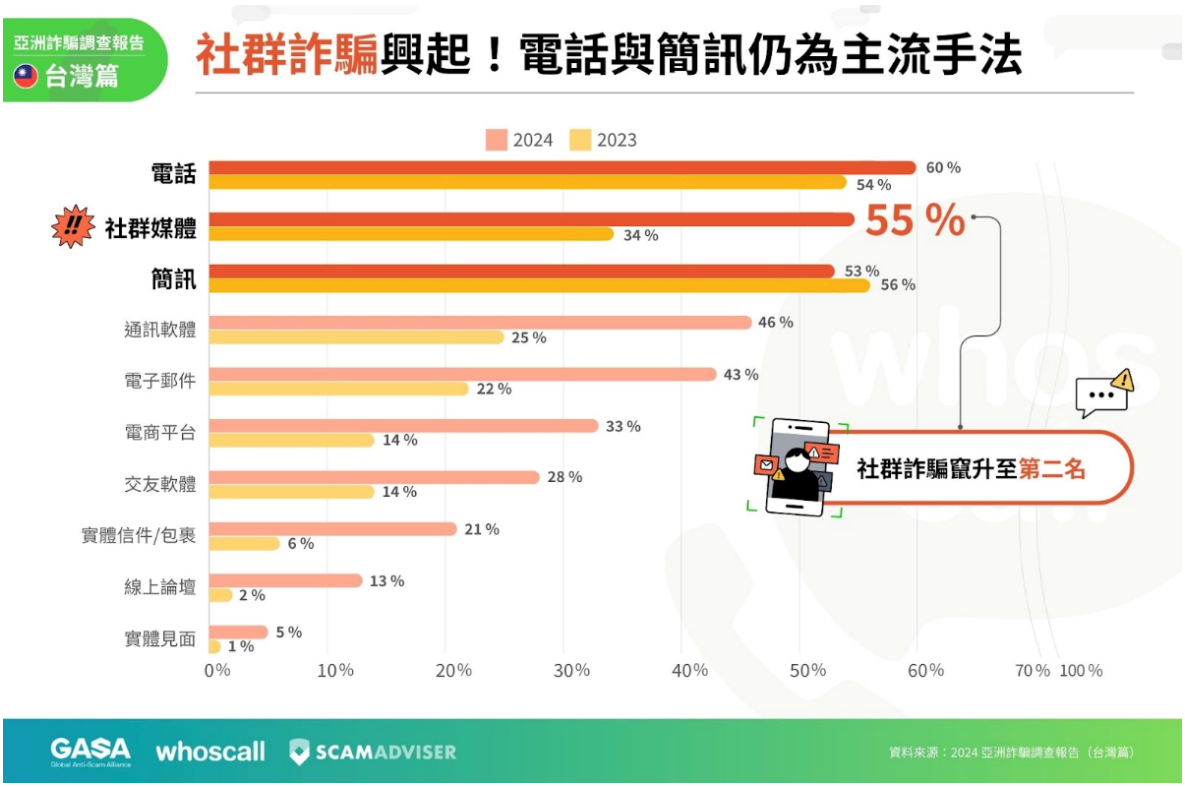

圖 3 詐欺集團用來接近民眾的管道

(3) Facebook 連兩年被視為台灣詐騙數位平台之首！

根據《Digital 2024: Taiwan》報告顯示，台灣約有 1,920 萬名社群用戶，相當於八成 民眾皆有使用社群的習慣，其中，最常使用的社群平台依序為 LINE、Facebook 與 Instagram。GASA & Whoscall《亞洲詐騙調查報告 - 台灣篇》指出，詐騙集團專門鎖定用戶數最多的社群平台行騙，當台灣民眾在被詢問到曾經在哪些數位平台遇過詐騙時，Facebook 連續兩年名列詐騙接觸率最高的社群媒介，有超過六成（63 %）的民眾都曾遇過詐騙。詐騙手法以假冒投資專家或分析師投放廣告為主，引誘受害者投資或購買假的金融產品。此外，亦有詐騙抓緊民眾貪小便宜的心態，在 Marketplace 以低於市價的商品吸引消費者，當民眾匯款後卻未收到正品，或是根本未收到商品。

LINE 作為台灣使用率最高的通訊軟體，詐騙行為也層出不窮。調查顯示，近五成（47.1%）的用戶表示曾在 LINE 上遇到詐騙。除了常見的假投資群組外，詐騙手法也越來越多樣化，利用「寵物投票」、「輔助認證」等誘餌，吸引民眾點擊不明連結，引導至釣魚網頁輸入 LINE 帳號密碼或個資，進而導致個資或 LINE 帳號密碼被盜用。

除了 Facebook 和 LINE，Gmail、Instagram 和蝦皮購物（Shopee）也是詐騙集團活躍的場域。約 25% 的台灣民眾表示曾在這些平台上遭遇詐騙，透過釣魚郵件、假冒賣家，或是透過社群媒體進行詐騙。隨著社群媒體與數位平台的普及，詐騙的手法與管道也變得更加多元且隱蔽，民眾需時刻保持警惕，避免落入詐騙陷阱。

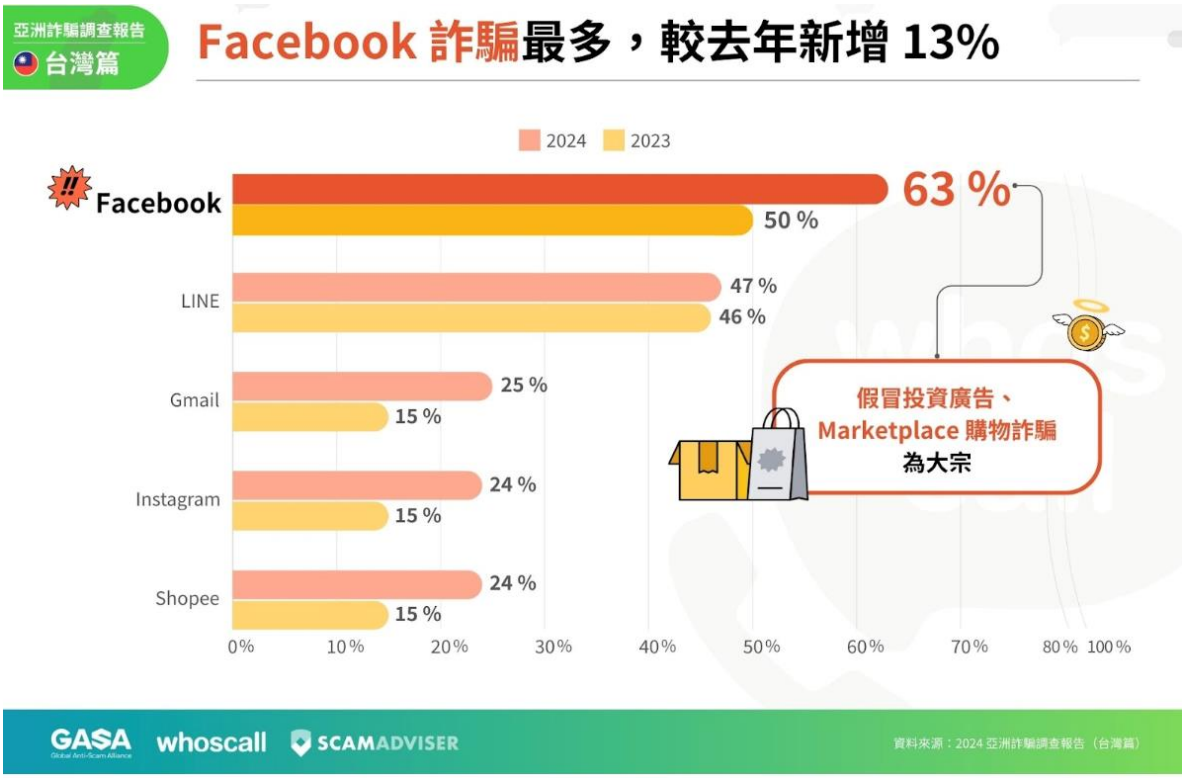

圖 4 社群媒體成為被騙民眾主要接觸來源

(4) 生成式 AI 成為詐騙集團犯罪新利器

隨著 AI 技術日益成熟，不僅被用來加速工作流程，也被詐騙集團作為犯罪工具。本次《亞洲詐騙調查報告 - 台灣篇》調查了民眾是否曾接觸過疑似運用 AI 的詐騙，結果顯示，近四成的受訪者自認曾收到疑似透過 AI 生成的詐騙簡訊。詐騙集團利用生成式 AI 大幅加快詐騙文本生成速度，再加上 AI 機器人自動化發送，使詐騙案件層出不窮。

除此之外，詐騙手法還蔓延至即時通訊軟體、語音電話、圖片與影片等多種形式。尤其是「深偽技術」（Deepfake）的崛起，透過變臉或聲音合成冒充親友或名人進行詐騙，風險不斷增加。特別是經常在電視或公開場合發言的公眾人物，更容易成為詐騙集團的目標。只要截取其發言片段，AI 就能模仿出與真人極為相似的聲音，讓 AI 詐騙案件更防不勝防。

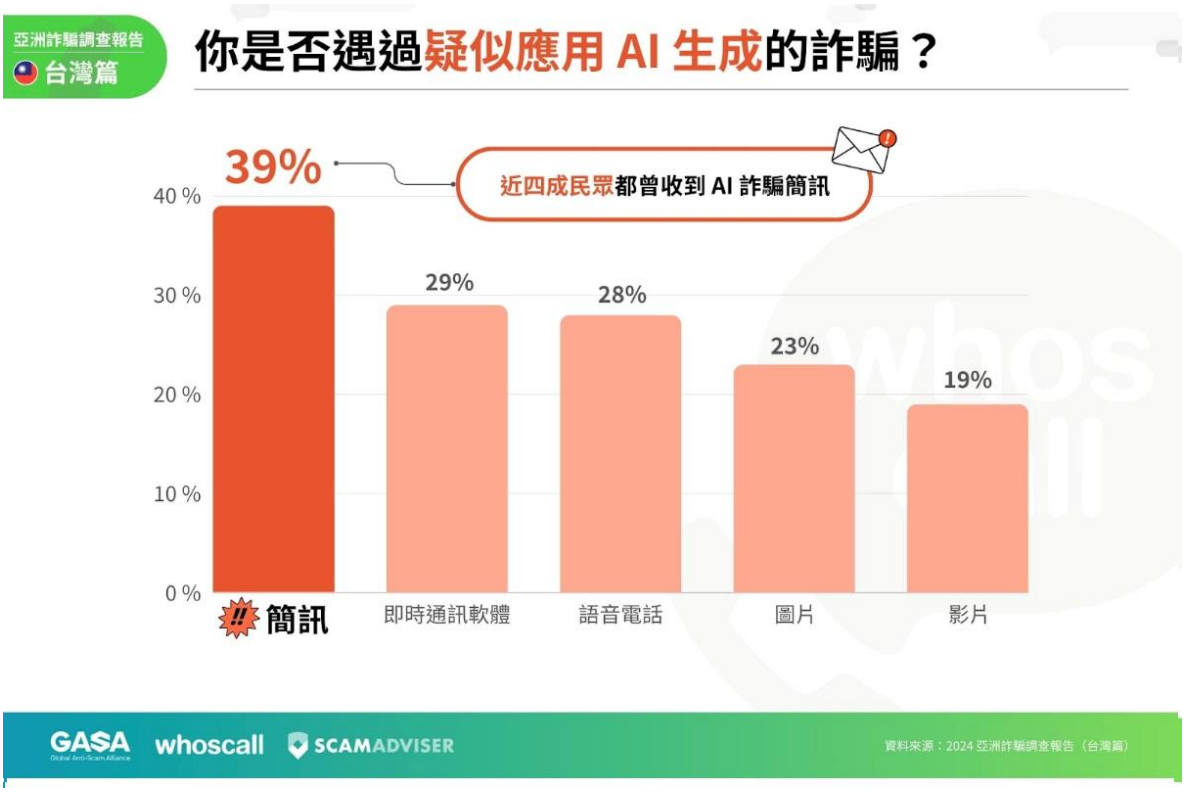

圖 5 生成式 AI 成為混淆民眾的詐欺工具

(5) 詐騙支付手段以匯款、現金收款、信用卡為三大金流

在分析完詐騙類型、手法、交易時間後，GASA & Whoscall《亞洲詐騙調查 - 台灣篇》也調查民眾支付詐騙的方式，銀行匯款依然是台灣詐騙集團最常使用的支付方式，曾用此方法受騙的民眾高達 39%，許多金融機構也因此加強防詐宣導，在客戶臨櫃第一線的行員發現異常、積極關切後，匯款情境亦逐漸轉移到網路銀行。此外，現金交易則以近三成比例緊隨其後，信用卡支付或盜刷也來到 22%。

網路購物付款方式推陳出新，尤以電子支付方式居多，造成虛擬貨幣與數位錢包等新興支付方式的詐騙比例也逐年上升，儘管佔比不及傳統手法，但其靈活性與匿名性使其成為詐騙分子青睞的工具之一。其他被利用的支付方式還包括遊戲點數卡與禮物卡、數位錢包和海外常見的支付 PayPal 等。

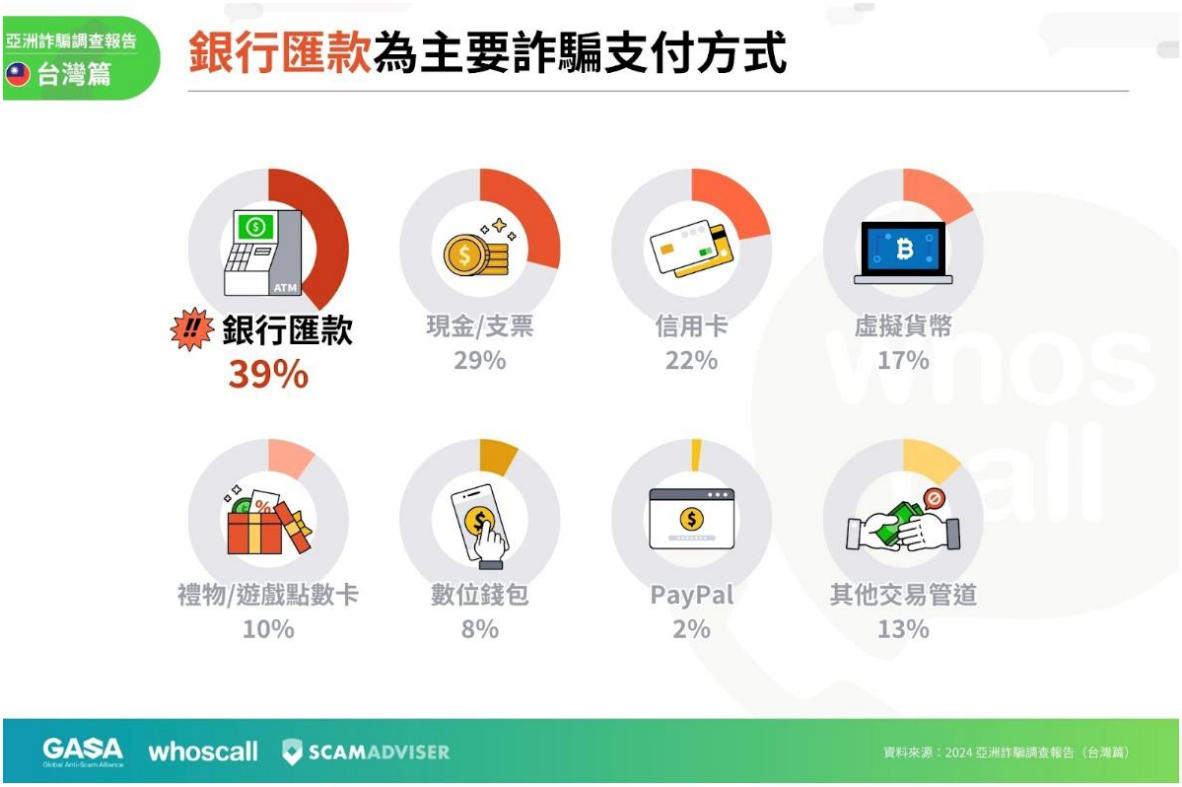

圖 6 銀行匯款 仍是主流

(6) 詐欺被害責任除了被害人，社群平台、網路營運業者難辭其咎

在詐騙案件頻傳的情況下，近五成（46%）的民眾傾向將責任歸咎於社群平台，認為平台應負起最大責任，起因為未能有效攔截詐騙廣告或刪除不實帳號。尤其是在假冒投資專家、網購詐騙等情況下，平台的審查機制及防護措施受到民眾質疑，導致詐騙行為屢見不鮮。其中，更有四成的民眾咎責於網路營運業者，原因來自於未能充分保護消費者資料，讓詐騙者有機可乘，也使得企業面臨愈來愈多的外界壓力和責難。

此外，金融機構與政府單位也被 35% 的受訪者列為應負責的單位，顯示民眾對於平台與相關機構在詐騙防制上的期待日益提升。隨著詐騙手段的變化和複雜性增加，強化社會大眾的防騙意識以及加強數位信任科技的普及，將成為對抗詐騙的重要關鍵。

亞洲詐騙調查顯示詐騙威脅已從線下轉線上。在數位化浪潮及數位轉型趨勢下，如何保護消費者免受詐騙威脅，已成為企業的社會責任及公司治理的重要議題，唯有積極投入防詐措施，才能同時兼顧有效降低營運風險及善盡社會責任。此舉不僅保護企業聲譽，也能進一步強化與消費者間的信任關係。台灣數位信任協會也將持續和跨產業夥伴攜手，投入防詐教育及素養提升等推動，以提高全民識詐能力。」

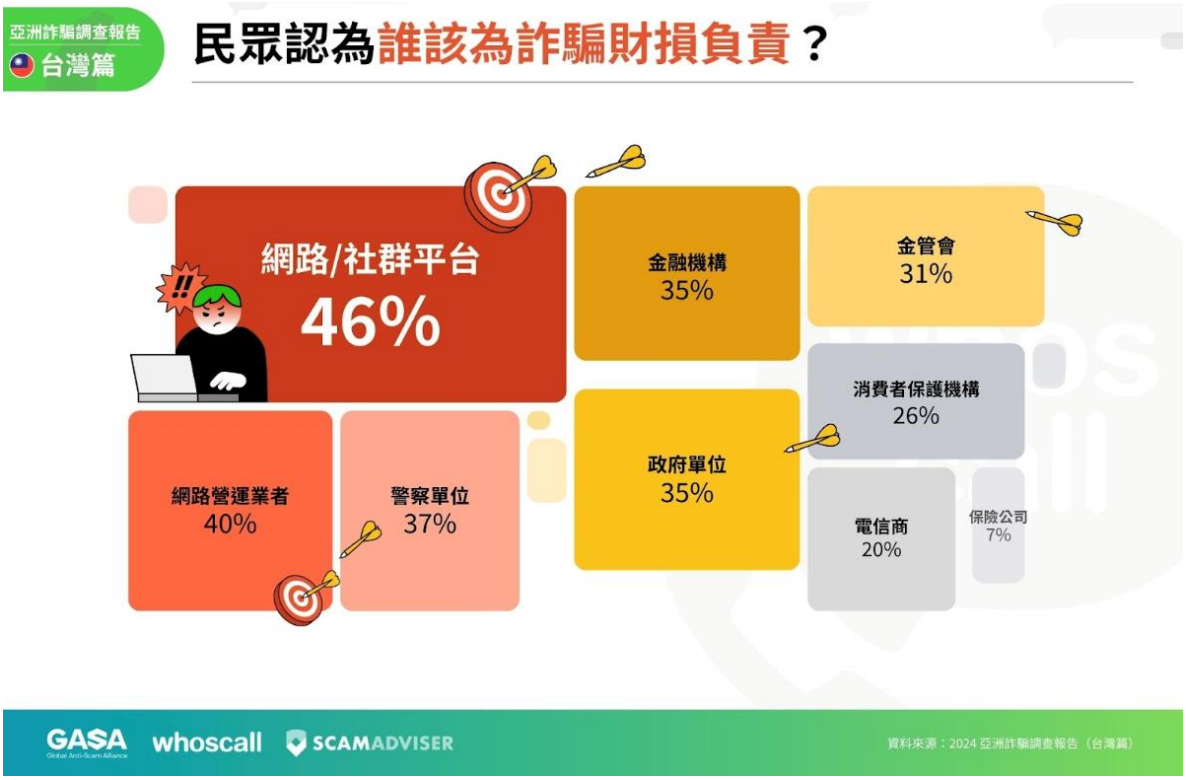

圖 7 除了被害人 誰該為詐欺猖獗負責

三、參加國際會議與新加坡打擊詐騙中心心得及建議：

(一) 心得

新加坡打擊詐欺犯罪現況

新加坡近年遭遇詐騙問題急速嚴重上升，新加坡警察部隊於 2019 年派員參訪我國刑事警察局 165，並參考英國打擊詐騙作法並持續精進改良，成立新加坡反詐騙指揮部，以便迅速追蹤資金並凍結涉及詐騙的銀行帳戶，2023 年凍結超過 19,600 個銀行帳戶，追回超過 1 億美元

反詐騙中心，設詐騙諮詢專線 1799，去年更針對該國內日益嚴重的詐欺犯罪問題，採取積極立法針對防制詐欺等網路犯罪危害的特別法草案---《網路犯罪危害法》(ONLINE CRIMINAL HARMS ACT 2023(No. 24 of 2023))，該法於 2023 年 7 月 5 日經國會立法通過並於同月 24 日經總統公布，於 2024 年 2 月 1 日生效。新加坡警察部隊所採行的打詐政策，無論在立法及執法等層面均付出相當努力，展現積極解決問題的企圖心。

依據新加坡警察部隊 2023 年報(Annual Crime Brief 2023 Physical Crime Situation)及新加坡詐欺及網路犯罪 2023 年報(Annual Scams and Cybercrime Brief 2023 Overall Scams and Cybercrime Situation)顯示，目前尚未見打擊詐欺明顯成效，顯然在當前全球詐欺攀升趨勢下，一樣面臨難以有效遏止詐騙案件困境。

新加坡之詐騙案件若包括惡意軟體詐騙攻擊，詐騙及網路罪案發生數由 2022 年的 33,669 件上升 49.6%至 50,376 件。至於一般詐騙案件總數由 2022 年的 31,728 件增加 46.8%至 2023 年的 46,563 件。

新加坡是個很特別的東南亞國家，面積僅有台灣的五十分之一，卻已經是個高度發展的已開發國家，國民平均所得約為台灣的兩倍。新加坡也是個多元種族國家，超過 500 萬人口中，有七成五為華人、一成五為馬來人、其餘為印度人及其他種族，馬來語也是官方語言，教育學習的教科書皆用英語學習，但又因華人居多，所以平時會在家用華語溝通，因此受理反詐騙諮詢報案有多種語言均可溝通，筆錄則以英文為主。

新加坡前十大詐騙類型，以件數進行排名前五名為求職詐騙(Job Scams)、電子商務詐騙(E-Commerce Scams)、假朋友電話詐騙(Fake Friend Call Scams)、網路釣魚詐騙(Phishing Scams)和投資詐騙(Investment Scams)詐騙。然而，2023 年前十大詐騙案類，冒充政府官員騙案(Government Officials Impersonation Scams(GOIS))則是平均損失最高的案類(與我國統計狀況類似)，每件約 10 萬 3,600 新加坡幣，其次是投資騙案，每件約 5 萬 700 元。這兩種騙局類型涉及在一段時間內進行的欺騙和社交工程，使用一系列複雜的騙局方法。

表 1 新加坡十大詐騙案類

Top 10 scam types in Singapore (Based on number of reported cases)

Types of Scams	Cases reported		Total amount lost (at least)		Average amount lost per case		
	2023	2022	2023	2022	2023	2022	Difference
Job Scam	9,914	6,492	$135.7M	$117.4M	$13,692	$18,089	↓ $4,397
E-commerce Scam	9,783	4,762	$13.9M	$21.3M	$1,428	$4,491	↓ $3,063
Fake Friend Call Scam	6,859	2,106	$23.1M	$8.8M	$3,373	$4,201	↓ $828
Phishing Scam	5,938	7,097	$14.2M	$16.5M	$2,394	$2,338	↑ $56
Investment Scam	4,030	3,108	$204.5M	$198.3M	$50,754	$63,834	↓ $13,080
Malware-enabled Scam	1,899	-	$34.1M	-	$17,960	-	-
Social Media Impersonation Scam	1,570	1,696	$9.7M	$3.7M	$6,184	$2,231	↑ $3,953
Loan Scam	914	1,031	$6.1M	$9.3M	$6,676	$9,082	↓ $2,406
Internet Love Scam	913	868	$39.8M	$35.7M	$43,677	$41,200	↑ $2,477
Government Officials Impersonation Scam	893	771	$92.5M	$97.6M	$103,657	$126,697	↓ $23,040
Top 10 scams	42,713	27,931	$573.9M	$509.2M	$13,438	$18,232	↓ $4,794

Note: Total amount lost may not tally due to rounding.

在我國已經躍升為件數與財損最高的投資詐騙 (Investment Scams)中，新加坡 2023 年亦發生 4,030 件投資詐騙個案，較 2022 年的 3,108 件增加 29.7%。投資詐騙造成的總損失從 2022 年的 1.983 億元增加到 2023 年的 2.045 億元，增長了 3.1%。在十大騙局類型中，投資騙局的損失最高，儘管每宗投資騙局的平均損失金額從 2022 年的 63,834 元下降到 2023 年的 50,754 元，但損失金額仍是最高。

新加坡投資詐騙案受害人年齡介於 30 至 49 歲，占該類詐騙案受騙受害人的 45.1%。Facebook、Telegram 和 Instagram 是投資詐騙者聯繫潛在受害者的最常見平臺。惡意軟體詐騙在 2023 年，大約有 1,899 件受害人將惡意軟體下載到手機上的案件，損失總額至少為 3,410 萬元。每個惡意軟體的詐騙案件的平均損失金額約為 17,960 元。

受害人一般會回應 Facebook 及 Instagram 等社交媒體平臺上的服務廣告（例如家居清潔、購買食物及寵物美容）。詐騙集團以支付服務費用為藉口，通過 WhatsApp 向受害者發送檔或 URL 連結，要求他們下載 Android Package Kit（APK）檔，這是為 Android 操作系統創建的應用程式。這些 APK 檔包含針對受害者設備的惡意軟體。受害人下載 APK 檔後，騙徒可能會指示受害人向類似於銀行登錄網站的欺騙網站提供他們的銀行憑證和/或銀行卡詳細資訊來付款。該惡意軟體還可能允許詐騙者遠端訪問受害者的設備。這將允許詐騙者通過鍵盤記錄或監控受害者對其設備的使用方式來獲取受害者的銀行憑證和/或銀行卡詳細資訊。隨後，受害者在討論時會意識到他們被騙。

大多數啟用惡意軟體的詐騙受害者年齡在 30 至 49 歲之間，占此類詐騙類型受害者的 43.7%。Facebook 和 Instagram 是詐騙者用來聯繫潛在受害者的最常見平臺。為應對惡意軟體詐騙攻擊，政府推出了一系列保護新加坡人的措施，因此 2023 年底詐欺案例有所下降。全政府（WOG）的反惡意軟體詐

騙措施包括加強措施，以保障中央公積金(Central Provident Fund (CPF))的款項、發佈安全應用程式標準（the Safe App Standard）以及與銀行合作推出反惡意軟體詐騙措施（counter malwareenabled scams measures）。

綜上，儘管新加坡詐騙個案數目有所增加，但 2023 年的損失總額由 2022 年的 6 億 6070 萬元微跌 1.3%至 6 億 5180 萬元。這是過去五年來新加坡因詐騙而損失的總金額首次下降。

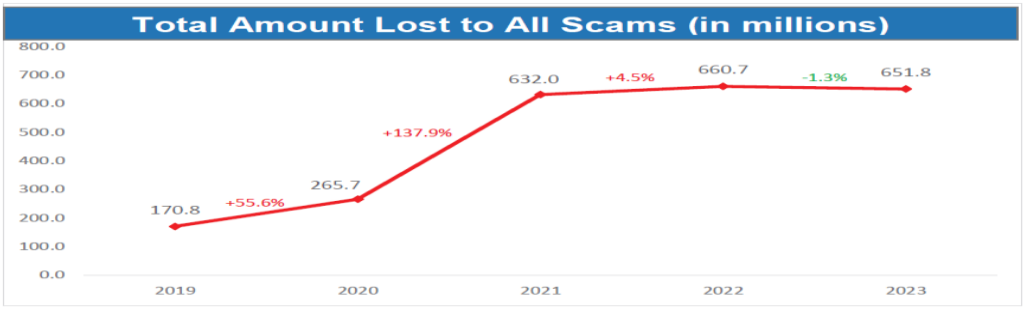

圖 新加坡詐騙損失數目

五大詐騙類型的平均損失金額普遍下降。整體而言，所有已報案的每件詐騙個案的平均損失金額亦有所下降，由 2022 年的 20,824 元下降至 2023 年的 13,999 元，跌幅約 32.8%。

損失略有改善的部分原因可能是新加坡警察部隊（SPF）、資訊通信媒體發展局(Infocomm Media Development Authority (IMDA))、新加坡網路安全域(Cyber Security Agency of Singapore (CSA))、智慧國家集團(Smart Nation Group (SNG))、新加坡金融管理局(Monetary Authority of Singapore (MAS))和私人安全利益相關者(private sector stakeholders)為防止詐騙並阻止或減輕正在進行的詐騙期間的損失而做出的積極和協調努力，以及提高公眾對個人可以採取的措施的認識，以避免被騙。

然而，涉及使用社交工程和欺騙手段誘使受害人將錢款轉給騙徒的騙局損失仍然很高。通過社交媒體和消息平臺（如 Facebook、Instagram、WhatsApp 和 Telegram）實施的詐騙數量急劇增加感到擔憂。民眾通過隨時了解詐欺趨勢並謹慎行事，保持警惕仍然至關重要。

(二) 建議

1. 可立即比照新加坡提升打詐效能

(1) 銀行人員進駐打詐指揮中心即時分析金流與追蹤凍結

新加坡打擊詐騙指揮中心，為有效進行降低民眾財產損害，要求帳戶最多的前六大銀行，派員進駐指揮中心，這六大銀行同時也是民眾受損最多的銀行，除派遣人員進駐外，亦讓各家銀行專屬溝通系統可以連線至反詐騙中心立即凍結，並分析金流，若金流轉至其他銀行，因為多已派員在同一辦公室，可以立即追蹤金流分析，有流出至其他未進駐銀行，亦可即時通報查詢回復，短時間當場追出轉帳數層之金流，有利於警方辦案，同時將金流分析結果提供警方偵辦。

(2) 約聘人員投入接聽電話，警衛外包予保全公司，執法警力專責偵辦與分析

新加坡反詐騙諮詢專線，考量警力係經過國家長期培訓之執法人員，人力資源珍貴，所以 1799 反詐騙諮詢專線係臨時招聘，以一年一聘之方式，招募人力經訓練後，負責接聽反詐騙電話，以樽節警力，使警力全數投入於犯罪偵查與分析，即使駐地之安全維護，亦外包由優質的保全公司，聘僱等級較高的保全人員負責，警察人員僅專責負責執法工作，非必要的一般保全與行政工作不浪費警力執行。

(3) 開放客戶在受到威脅時自己申請暫停凍結自己帳戶

被害帳戶棟及除了要求六家銀行派員進駐打詐指揮中心外，各個銀行開始實施民眾同意自行緊急自助服務"終止開關"，允許銀行客戶在受到威脅時自己快速暫停凍結自己帳戶

(4) 識詐宣導由國家犯罪預防委員會（NCPC）要求重要部會共同執行

National Crime Prevention Council 屬於政府出資的非營利組織，致力於提高公眾對犯罪的認識和關注，並傳播預防犯罪的自救理念。該委員會由商業和工業部門、消費者保護以及公共部門與新加坡警察部隊（SPF）的代表一同組成。主要依靠政府捐贈和民間贊助來拓展宣導計畫和活動。NCPC 是動員社區團體、組織和個人一起支持與警方密切合作的預防犯罪催化劑，設有顧問及合作夥伴。與各種專業、社會和金融貿易組織建立密切的聯盟，以解決犯罪問題。

(5) 預留檢察官辦公桌，可進駐協助立即裁定扣押犯罪資產：

為有效立即開立搜索票或裁定扣押詐欺犯罪資產，打詐指揮中心設有兩席辦公處所供輪值之檢察官進駐，協助開立查扣所需的扣押裁定書等。

2. 國際反詐欺趨勢可參考建立三流分析：

從 GASA 的交流分析可知，全球打擊詐欺犯罪情勢短期難見曙光，應建立長期策略，欲有效破解電信網路詐欺，必須團整合三個詐騙主流，電信流、資訊流與資金流，彙整出詐欺的關鍵節點與流向，方能找除重要「節點」予以阻斷，

方有機會降低詐欺犯罪現況。

我國「打詐行動綱領」即將邁向 2.0，但去年電信網路詐欺案件數量仍將近 3 萬件，今年九月開始採用「打詐儀表板」每日公布數據看來，每日詐欺大約發生 600 件，每日財損約新臺幣四億元，不但持續創歷史新高，以打詐儀表板當前數據推估，2024 我國詐欺財損與件數，將成為世界詐騙犯罪之巔，成為各國矚目焦點，經過數日與國際執法機構與科技公司交流後，亟待整合的「三流資訊」分析與建議如下：

(1) 電信流：

有關電信門號管制，今年已經開始注意到海外或企業用戶浮濫問題，予以管制，然而目前仍有許多非法電信設備在幫助詐欺集團可以輕易偽造號碼來連繫被害人，例如目前電信詐欺三大利器 1.貓池（Moden Pool）2.DMT(數位節費器設備; Digital Mobile Trunk）3.偽基站(Fake tower signal: SIM card swapping 也稱為 SSRP)，這些設備多來自海外輸入，設備多數也是中國大陸製造，我國海關應建立實施特別管制，此外這些電子設備也應納入監管，例如取得核發許可與追蹤設備流向，這些設備是近年，造成民眾在電信上仍會收到不明簡訊與連結的電信主要破口，特別是偽基地台的簡訊詐騙輕易突破政府短碼 111 減害政策，不但對用戶直接造成了轉連結後的慘痛經濟損失，也會經由此一方式先騙取民眾個資，取得民眾個資後轉賣其他集團，因為個資的外洩，在針對被害人溝通聯繫時才容易取得信任，爾後持續發展造成後續的嚴重損害，各國已經開始注意到個資的盜取釣魚嚴重性，偽基地台詐騙+釣魚=完美個資黑色電信產業，目前尚難以深入背後的產業運作模式，但偽基地台的氾濫與 GSM、2G 通訊網路漏洞有關，單純持有這些設備難有重罰，如今這些設備僅需 700 美元就能輕易購置成立一座偽基地台，以此獲利非常容易，設備目前可縮小到背包背負即可。目前歐美各國正在研究如何抵制偽基地台，譬如透過成立特別調查小組，透過電信業實施網路升級，相關部門、業者也必須提出對策，對於中國日益繁多的電子設備生產領域，予以抑制，特別是偽基地台簡訊氾濫已多時。過去由偽基站主機板、功率擴大機、機箱、控制設備組成，這些舊款設備，控制需要配一台筆記型電腦，非常笨重容易被發現多裝置於汽車上。然而去年開始升級為「背包機」，設備縮小，提昇隱蔽性，我國應發展類似中國 360 手機衛士軟體，主動攔截偽基地台詐騙簡訊等，同時，加強追緝偽基地台不法信號偵測，電信主管機關與業者也應自主研究詐欺的電信黑色產業發展，否則 165 詐騙專線難以要求主動加以斷話，成為台灣電信詐騙訊號猖獗，無法停止斷話的主因。

(2) 數位流：

假投資網路廣告是造成財損最大的主因，更可能是人民深度不滿的緣由，每個人都有親友已經造到鉅額投資詐欺損害，網路平台治理與監理制度仍亟待新建，針對網路假廣告猖獗，美國已經由聯邦貿易委員會 FTC 建立《聯邦貿易委員會法案》的標準，要求必須遵守《消費者評論和推薦使用規則》的具體禁止規定，FTC 於 2023 年修訂的廣告使用代言和推薦指南（Endorsement

Guides 代言指南）指出網路已將行銷人員與全國乃至世界各地的客戶聯繫起來。如果在網路上做廣告，應謹記保護消費者的規則和準則，也可透過維護網路作為行銷媒介的商譽來幫助企業。此外，FTC 還執行《告知消費者法案》，該法案要求網路市場應驗證其平台上高額銷售的第三方賣家的身份，並使消費者更容易檢舉可疑網路行為，此次修訂特別針對商品服務使用做出規範，規範亦適用於社交媒體（如 Facebook、Twitter 及各種類型的部落格等具互動性的媒體）中之心得分享，未來甚至在社交媒體對商品或服務所做出的各種評論，都有可能成為 FTC 管制的對象。

社交媒體中所傳遞之商品使用心得分享，特別是名人（在該領域分享心得出名者）所分享之訊息，因為對於網路使用者或消費者之影響甚大，甚至會改變是否購置該商品之意願，但真實性卻未必有相當之保障。因此 FTC 新修正之指南中針對這些用戶心得分享之訊息也作出相應規範，摘要如下：

A.心得分享者若由商品或服務提供者處受有金錢或利益給付者，即不屬於單純心得分享，而與廣告具有相同之性質。因此若有虛偽不實陳述狀況，亦視為不實廣告。

B.心得分享者必須揭露其與商品或服務提供者的利益關係，使其他消費者明瞭。

C.廣告中若有引用研究結果，而該研究機構為該公司所贊助時，廣告中必須揭露兩者的利益關係。

D.該指南同時適用於談話性節目以及社交媒體上所為之心得分享。

E.違反上述規定者，可能會遭到以違反美國聯邦交易委員會法第 5 條（FTC Act Sec.5）之相關規定每次最高得處以 1 萬 1 千美元罰鍰。

(3) 資金流：

詐欺的資金流問題來自於金融端人頭帳戶持續攀升，有關警示帳戶最新統計，截至今年六月底止，警示帳戶戶數合計共 13 萬 4350 戶，比起去年底的 11 萬 8356 戶，又增加 1 萬 5994 戶，金管會指出，依財金公司統計，截至 113 年 6 月經轉出行對申請約定帳戶的客戶進行關懷提問達 7927 筆，亦即有 7927 戶是疑似異常交易要進一步釐清的帳戶，警示帳戶越打越多的情形，顯示問題沒有獲得解決可能是越打越詐的主因，這些快速增加的人頭帳戶有待進一步分析追蹤，新加坡的詐欺金流追蹤主要由銀行端拉專屬金融連線到 1799，由發生最高的六家銀行派員進駐立即追蹤與處理，主管機關的原因分析能協助進行有效控管，此外對新一波虛擬貨幣制度，如何有效防制成為洗錢破口也有待加強管理。

詐騙集團最終目的不外乎取得金錢，因此，若能透過上游優化監管機制，建立清源防制才是提高打詐綜效的最具體預防成果，因此金流管制及洗錢防制等措施屬於打詐政策之最核心也最具有價值的一部分。

打擊詐欺的戰場若只在數位網路上將不易成功，因為網路跨國犯罪、國際社群媒體，與應設備無論在軟硬體設備上，都不利於政府單位的網路打詐，相較於網路與電信，金融業為政府高度監管行業，多數民眾的資金存款也都在

金融體系上，因此將打擊詐欺的主戰場聚焦至資金流，或許較能產生實質阻擋詐欺犯罪的效果，然而攔阻詐欺金額的部分，已經從金警合作轉移到三個不同戰場，分別是轉到空戰的虛擬貨幣、海戰的第三方支付與陸戰的到府收款，因此今年的攔阻詐欺將是一場苦戰，個案心得建議如下：

A. 詐欺收款的陸戰到府收款-建立紅、白、黑、灰名單聯防機制

傳統的金融管理，在約定轉帳戶與警示帳戶的各銀行自我勾稽比對不足，亦不敢輕易凍結動極高端客戶的網路轉帳功能，導致被害千萬以上詐欺案件，在提供警方匯款資金流時，多高達將近十個鉅額轉帳帳戶，這些轉帳的帳戶都是不同銀行，顯見詐欺集團利用跨銀行間資料不易流通的缺點，進行持續洗腦詐騙，若各家銀行能定期比對自己的客戶約定轉帳是否與警示帳戶有關聯，立即通知客戶來實體門市單位確認時，才能有效阻止自己客戶被害，若再能將相關情形建立系統通報其他銀行，才能發揮聯防阻詐效果，否則被害人會在轉帳無效後，受到詐欺集團指揮到他行提領現金，或設定他行約定轉帳資料，從而造成一、兩家攔阻成功，卻從第三家輕易領出等候詐欺集團到府收款，造成攔阻失敗，因此，金融阻詐，不能只有建立黑名單、灰名單，還要建立被害高風險的紅名單分享。另外近期警示帳戶兩大新趨勢，包括外籍移工、企業用戶變多，還有過去安全的舊(靜止)戶一開始被利用成為警示帳戶。

警示帳戶是指法院、檢警機關為偵辦刑事案件需要，通報銀行將存款帳戶列為警示，帳戶功能全部凍結，減少被害人的損失。警示帳戶持有人在其他銀行開立的帳戶，視為衍生管制帳戶，相關功能也會被暫停。

負責相關業務的民營銀行主管分析，警示帳戶大致有三大種，第一種是自願出賣人頭帳戶者，可能因財務突然發生困難，被歹徒誘惑出售帳戶。這種帳戶目前佔比也在增加。

此外近來因為警方告誡出賣帳戶策略產生效果，收購人頭帳戶轉向詐騙帳戶，詐欺集團鎖定求職、貸款等特定目標對象，用話術騙走帳戶資訊，民眾上網尋找求職工作，或上網查看貸款借錢時，被要求提供帳戶存摺、印章等資料，後來驚覺帳戶已被詐騙集團做為詐欺金流收款轉帳，而被銀行註記為警示帳戶。

B. 詐欺收款的海戰第三方支付-納入特許行業

目前第三方支付業者數量高達 1 萬 2 千餘業者，虛擬帳號在台灣雖然只有法人能申請，但業務為第 3 方支付時，一人公司的電商也算是法人，可產出 N 組虛擬帳號，因此曾被濫用成為詐騙集團的金流管道。可謂海量戰術，目前已指定數位發展部為第三方支付主管機關，啟動第三方支付服務業能量登錄制度，要求申請業者提出洗錢防制及法遵聲明書始能登錄、訂定「第三方支付服務業防制洗錢指引手冊」及其範本，協助業者進行法遵作業及落實客戶身分確認。然第三方支付服務業，仍屬於低度監理的類金融業，第三方支付服務業並非特許行業，僅需向經濟部商業司進行公司登記即可成立，資本額亦無特殊限制。迄 2024 年 7 月底完成能量登錄僅

有 68 家左右。現在要利用第 3 方支付平台洗錢已經不如先前容易。
然而正本清源之道仍需將第 3 方支付與虛擬資產納入特許行業監管。
參照歐盟的電子支付業務「支付服務指令」(Payment Services Directive)，經營支付服務業務須取得許可，對支付機構的資本額與資金比例設定不同規範，採用分級監理與規範，對於業務分級、風險分級，採取不同規模適用不同規範的監管。日本支付業的主管機關則為金融廳的「資金清算法」(資金決済に関する法律)規範支付業，規範資金移轉業務、預付儲值型支付業務的監管要求，包含申請登記、資安管理、履約保證、交易限額等，可知，各國對於第三方支付的監管均趨向嚴格監管。
多透過「承作業務前須取得許可證」、「業務與風險分級」或「規模及交易限額」等手段，無非是因為支付業事涉金融體系穩定與交易秩序。我國在 2015 年制定電子支付機構管理條例，主管機關為金管會，該法於 2021 年大幅修正，擴大電子支付機構業務範圍，同時整併電子票證發行管理條例，但始終未將第三方支付服務業納入監管。

C. 詐欺取款的空戰虛擬貨幣

虛擬貨幣的去中心化、高度匿名及快速跨境移轉等特性，已成為詐騙集團詐欺洗錢犯罪之首要工具，因此詐騙集團取款與洗錢的管道已經逐漸轉到虛擬貨幣上，許多未受監管的「個人幣商」成為詐騙集團洗錢的新藍海，亟需建立幣商登記等監理措施，配合虛擬貨幣辦法來遏止虛擬貨幣洗錢的問題。
目前警察機關凍結虛擬貨幣金額龐大、刑事局開設「虛擬貨幣幣流分析課程」，擴大培訓建立虛擬貨幣分析追蹤警力並組成專案小組，分析反詐騙資料庫的幣流資料，鎖定詐團的虛擬貨幣錢包，主動查扣凍結虛幣，但對於返還方式尚未達成定見，因為虛擬貨幣去中心化交易的特性，使得資金移轉無國界限制，因此在虛擬貨幣的偵查上，有賴各國政府共同制定法律規範，透過完善虛擬貨幣及洗錢防制相關法規，將法人及個人幣商納入監管並規範其行為，以利警方執法打擊詐團。

3. 跨國、跨機關資訊交流合作仍有進步空間-建議成立刑事情報委員會：

隨著網際網路的蓬勃發展，結合電信流、資訊流與金流服務之詐欺案件，不斷在技術上進化，已經逐漸成為跨國化、集團化、組織化之犯罪模式。要能有效打擊此種電信網路跨國犯罪，必須強化我國跨機關的資訊追蹤整合以及國際執法機關間之合作，才能針對網路詐欺犯罪嚴加查緝。
我國新推出的打詐儀錶板，可以促進政府將詐欺相關數據開放給民間參與，透過開放官方資料，帶動民間加值服務與相關產業發展，為強化數位服務發展並帶反詐欺產業轉型之關鍵，除了政府資料開放資料釋出外，若還能結合

跨政府部門間與民間組織間之資料進行交換運用，應能更強化反詐欺產業之效率，然資料開放相關政策、法制、標準或執行機制等其他資料運用與推動措施，仍需存在跨機關間資料共享、跨部門間資料運用瓶頸與障礙，宜成立智庫進行意見徵集與利害關係人溝通，而規劃未來整體可行方向。

另外，跨境聯合執法、打擊跨境電信詐欺機制、查扣不法所得的實務、情報與情資交換及司法互助等議題，均有賴進一步深度之討論，以強化我國執法人員在跨國合作之運作與偵辦，建議我國應比照澳洲成立刑事情報委員會(Australian Criminal Intelligence Commission)或是刑事情報智庫研究中心，提供關鍵任務情報，以應對我國面臨的跨國嚴重的跨國、網路和組織犯罪的威脅。

4. 跨機關的資訊交流有待放寬個資法限制：

個人資料外洩容易遭到不法集團利用，藉以精準針對當事人量身訂製詐騙劇本進行詐騙行為，造成民眾權益受損。行政院新世代打擊詐欺策略行動綱領四大面向中之「堵詐」就包含個資保護之管制要求，現行個資法對於業者違反資安維護義務之罰鍰，首開先例是對於蝦皮網拍進行裁罰，首開非公務機關違反安全維護義務之罰鍰。

然而在防堵網路詐欺犯罪與詐騙方面，同樣受到客戶個資保護因素影響，必須要讓金融機構對於可疑帳戶進行通報，從黑名單到白名單甚至易遭詐騙名單均能排除個資法之限制，可以互相交流，因此刑事警察局與許多金融機構簽屬 MOU 以更進一步執行金融防詐的聯防合作。

警方與金融單位簽訂 MOU（合作備忘錄），都屬於跨部門合作與資訊交換，但對於交流金融犯罪或詐騙的個案資訊，許多部門法遵系統仍有顧慮，特別是對於高風險被害人的資訊交流，雖然放寬個資的部分在打詐四法已有詐防條例設立避風港條款，但是具體如何進行跨單位間個人隱私資訊的聯防合作，有待克服法律有關個資保護的解釋障礙並建立交流系統。

另外隨著全球數位化趨勢發展，跨境合作傳輸需求急遽增加，在 A 國蒐集犯罪個資後可能需跨境傳輸至 B 國處理或追偵，因為跨境電子商務交易、或雲端異地備份、等情形，在當前已屬常態，為加強保障隱私，世界各國對跨境個資或相關資料傳輸的規範日趨嚴格。例如歐盟自 2018 年 5 月施行一般資料保護規則（GDPR），未能遵守之國際巨擘可能遭受裁罰。

跨機關的資訊交流有三項重點，一是跨組織間彼此要有系統性、有效性地通知最新資訊，二是要分享跨機關間資訊要能安全避免外洩；三是能夠提供執法機構進一步的調查分析與協助，特別是網路與電信資訊用在分析金融犯罪、以及防制洗錢的金流追蹤。

全球化數位趨勢不斷加速，資料跨境傳輸急遽增加，個資侵害事件常牽涉境外因素，亦須透過跨國司法的互助合作，才能有效打擊不法、防止侵害擴大。

5.培養企業及個人及早建立應對詐欺之防護力：

網絡詐騙日趨嚴重，屬跨國有組織犯罪。此類犯罪集團已經發展成有系統的組織犯罪，分成多個部門，每個部門就其犯罪專長各司其職，從廣告、被害個人資訊、網頁架設、社群媒體經營到洗錢等一連串作為。由於每個犯罪部門接分開處理，透過社群交流技術隱匿犯罪行為，甚至將組織分散，遍佈多個不同國家司法管轄區，使得執法人員的調查增加許多難度。

詐欺的集團犯罪亦與其他類型的罪行有關，當中包括跨國人口販運、在犯罪集團下的電話中心強迫勞役，以及與朝鮮民主主義人民共和國非法網絡活動有關的大規模毀滅武器擴散資金籌集。 網絡詐騙洗錢的過程涉及洗錢集團及相關專業人員，而洗錢帳戶網絡除了借助錢騾（Money Mule），亦會利用空殼公司或合法業務，並牽涉各類金融機構，包括銀行、支付及匯款服務提供者，以及虛擬資產服務提供者。不法之徒亦會利用多種洗錢手法掩飾贓款的線索，包括使用現金、貿易洗錢及無牌服務。數位化促進科技發展，但也令網路詐騙罪犯得以發展和擴大其非法活動的規模、範圍及速度。

詐欺犯罪開使使用多種科技工具及接觸民眾的手法，利用社交媒體及通訊程式，在境外大規模招攬錢騾，並迅速利用新數位金融產品以及非傳統界面（例如電子商務、社群媒體及串流平台）的漏洞犯案。掌握受害人的心理狀況和感情，不斷攫取受害人的資金甚至貸款。最後利用數位貨幣，清洗金融資產的犯罪所得，再透過網路遠距開戶等虛擬服務，輕易設立海外帳戶清洗犯罪所得，再利用即時的金融交易轉回金流，已成為當前先進國家最嚴重的經濟犯罪。