2026年2月25日
駐新加坡代表處

新加坡詐欺犯罪情勢及防制政策研析

TAIWAN

駐新加坡台北代表處
Taipei Representative Office in Singapore

版權頁（Copyright & Imprint）
《新加坡詐欺犯罪情勢及防制政策研析》
（Analysis of Fraud Crime Landscape and Prevention Policies in Singapore）
出版機關：駐新加坡台北代表處（Taipei Representative Office in Singapore）
出版年月：中華民國115年2月（2026年2月）
機關地址：460 Alexandra Road, #23-00 mTower, Singapore 119963
官方網站：https://www.roc-taiwan.org/sg/
Email：sgp@mofa.gov.tw
Phone：（+65）6500-0100

目錄

圖目錄

表目錄

摘要

近年來，新加坡面臨詐騙案件急遽攀升的嚴峻挑戰，詐騙問題已被正式提升為與反恐與反洗錢並列的國家級安全議題。根據2024年官方統計，全年通報的詐騙案件高達51,501起，年增10.6%，總財務損失更首度突破11億新幣，創下歷史新高。詐騙不僅成為社會信任的侵蝕者，也對金融體系與數位治理構成結構性壓力。

新加坡政府意識到，傳統以事後偵查為主的執法模式已不足以因應當前情勢。關鍵原因在於，多達82.4%的案件屬於受害者在高度心理操控下「自願轉帳」，顯示詐騙已由單純的技術犯罪，演化為隱蔽性極高的社交工程與認知操作行為。面對犯罪型態轉變，新加坡自2019年起逐步推動結合法規、科技與公私協力的整體戰略，試圖從源頭阻斷工具供應、於過程中即時攔截金流，並在事後強化追懲與嚇阻，建構一套多面向之防詐治理體系。

從犯罪趨勢來看，案件數最多的仍是電子商務詐騙，例如網購未到貨或假賣家案件，雖然發生頻繁，但個案損失金額通常較低；相對而言，投資詐騙與假冒官員詐騙的案件數雖非最高，卻因涉及高額資金與長時間心理操控，財損總額相對較高。

2024年總財損金額的跳升，更明顯受到少數極端大額案件影響，其中單一惡意軟體詐騙案造成1.25億新幣的驚人損失。同時，加密貨幣相關詐騙的損失占比已攀升至24.3%，顯示虛擬資產正快速成為詐騙與洗錢活動的重要工具之一。在接觸管道上，詐騙集團主要透過Meta旗下社群平台與Telegram接觸潛在受害者，並大量利用人頭SIM卡註冊帳號，以規避追查與身分溯源。

在法制層面，新加坡於2024年至2025年間陸續修法，目標不僅在於補漏洞，更賦予執法機關提前介入之權力。透過修訂《電腦濫用法》與《雜項犯罪法》，提供或濫用數位個人身分（如Singpass）以及SIM卡代辦、人頭註冊等行為被明確入罪，降低過去在主觀構成要件上的舉證門檻，從源頭切斷詐騙集團取得通訊與金融工具的供應鏈。警方更於2025年3月依據新修訂的《雜項犯罪法》，查獲電信門市員工盜用客戶資料註冊人頭SIM卡的案件，展現新法的嚇阻效果。

同時，新制定的《網路犯罪危害法》賦予政府對大型平台發布具法律效力指令的

權限，內政部於2025年9月及11月分別對Meta、Apple及Google發出「實施指令」，要求即時移除詐騙帳號、封鎖內容或攔截冒充政府之簡訊，未配合者將面臨高額罰款。

在金流監管方面，透過修訂《支付服務法》，將加密貨幣與跨境匯款納入更嚴格監管，金管局並於2025年6月首度依該法對5家未盡合規查核義務的支付機構處以罰款，展現監理決心；《貪腐、販毒與其他嚴重犯罪（沒收利益）法》則增設「魯莽」與「過失」洗錢罪，即便車手主張不知情，只要未盡合理查證義務，仍可能構成犯罪。

新制定的《防詐騙保障法》賦予警方發布限制令的權力，使執法機關得以在高度風險情境下，暫停堅持轉帳的受害者帳戶使用，突破過去的執法困境。截至2025年8月，警方已實際發出限制令凍結潛在受害者帳戶。

隨著新法介入，2025年上半年受害者「自願轉帳」案件比率已由前一年的86.1%下降至78.8%。在此基礎上，新加坡亦透過《刑事法（雜項修正）法案》，將詐騙主謀、核心成員與協力者納入鞭刑適用範圍，以極具象徵性的嚴刑峻罰，強化對犯罪集團的威嚇效果。

科技層面的策略轉型，則是新加坡防詐政策的另一重點。防詐措施已從早期的被動查詢與宣導，進一步升級為以AI為基礎的主動偵測與即時阻斷。ScamShield由原本的單一App，擴充為整合熱線、網站與通訊平台的防詐套裝，能自動過濾詐騙簡訊與來電，並支援一鍵通報，截至2025年下載量已突破135萬次，成為全民防詐的第一道防線；政府更全面導入「gov.sg」單一簡訊識別碼，截至2025年6月發送逾1.8億則簡訊且未遭偽冒。

此外，「詐騙分析及戰術性介入系統」（SATIS），每日自動掃描超過十萬個網站，辨識釣魚連結與假冒平台，並與搜尋引擎與社群業者合作，在詐騙內容大規模擴散前即時封鎖，僅2024年即成功下架近4.5萬個詐騙網站及4萬多個WhatsApp帳號。

公私協力則為整體戰略提供了運作效率與實務彈性。反詐騙指揮處整合警方、主要銀行與大型電商平台合署運作，使銀行人員能即時配合凍結資金，將原本需時數天

的流程壓縮至即時處理，2024年因此成功追回逾新幣1.82億元的受害款項。

在制度層面，「共同責任架構」明確要求金融與電信業者分擔釣魚詐騙的賠償責任，促使銀行全面升級帳戶安全措施，包括引入「資金鎖定」功能（截至2025年6月已鎖定逾300億新幣資產）、取消簡訊OTP改用數位驗證，以及對高風險轉帳設置冷卻期。與此同時，政府也透過自動化簡訊預警、樂齡防詐志工與社群平台廣告驗證機制，將防詐觸角延伸至社區與日常生活場域。

整體而言，新加坡的防詐模式展現出高度的政策整合力與執行彈性。雖然整體趨勢尚未逆轉，但成長幅度已見趨緩，且透過科技攔阻與早期介入，成功避免了大量潛在損失。其經驗的核心，在於政府跨部門快速整合的能力、成熟的數位基礎建設、高度社會信任，以及採取強制凍結與嚴刑峻罰等高強度手段。這套結合法律威嚇、科技阻斷與社會聯防的治理模式，為高度數位化社會對抗複雜詐騙威脅，提供了一個具體且可操作的範例。

第一章 緒論

1.1 報告背景

當全球加速邁向數位化的同時，詐騙犯罪也呈現科技化、跨境化與組織化的發展趨勢。新加坡雖然長期被評為全球最安全的國家之一，惟近年來詐騙案件數與損失金額卻急遽上升，對國家安全與社會信任體系帶來嚴重挑戰。

至2024年底，新加坡一年詐騙與案件總數超過51,000起，詐騙總損失更達到驚人的11億新幣，為歷年之最。其中高達82%的詐騙案件係由受害者「自願匯出款項」，顯示詐騙集團非僅靠駭客技術竊取資訊，更透過高明的社會工程技巧操縱人心，也有更完整的犯罪分工，基此，新加坡政府亦認知到，打詐與防詐措施應跳脫技術邏輯，並有進一步跨部門協作、法規創新之必要。

為因應此趨勢，新加坡政府自2019年起陸續推動多項措施，包括：設立反詐騙中心[1]、加強公私部門協力機制、運用AI與大數據分析預警可疑交易，並於2024年推動一系列修法與立法工程，最後形成全面性「科技—法制—協力」三軸並進的打詐體系。

本報告擬透過對新加坡經驗及制度之剖析，釐清該國在面對詐騙問題時的作為與挑戰，當我國在發展自身防詐機制時，亦能有所參考。

1.2 報告目的

本報告以「問題」為導向，藉由提出以下三個核心問題，並透過檢視新加坡防制詐騙犯罪的政策工具效益、其法制結構及跨機關的協作經驗，找出其具體成功因素與潛在瓶頸，以提供我國借鏡參考。

一、新加坡面對的詐騙現況與趨勢為何？

本處將盤點星國自2018年至2024年間的官方數據與公開報告，觀察詐騙案件的數量變化、受害者結構、手法類型（如電商詐騙、假冒官員詐騙、AI詐騙等）與通訊平台（如Telegram、WhatsApp[2]）的使用趨勢，以理解新加坡在面對詐騙議題時的問題處理取向。

二、新加坡採取了哪些應對措施？

針對政府推動的法規修訂（如電腦濫用法、詐騙防治法及線上犯罪危害法等）、

1 反詐騙中心(ASC)於2019年成立，並2022年改制升格為反詐騙指揮處(Anti-Scam Command, ASCom)，隸屬於新加坡警察部隊。

2 新加坡與台灣民眾慣用Line（超過90%之使用率）作為通訊軟體的習慣有別，根據挪威媒體監測與數位情報分析公司Meltwater 2024年調查，最多新加坡民眾使用之社群平台（含通訊軟體）排名依序是：1. WhatsApp(74. 7%)、2. 臉書(72. 7%)、3. Instagram(60. 3%)、4. Tiktok(52. 5%)、5. Telegram(47. 8%)。https://www. meltwater. com/en/blog/social-media-statistics-singapore?utm_source=chatgpt. com

科技工具（如ScamShield、詐騙分析及戰術性介入系統）、執法行動（如凍結帳戶、跨境合作）及民間參與（如反詐熱線、公私協力機制）等策略進行歸納與分類，說明不同政策背後之思維。

三、新加坡採取的措施是否達到預期成效？

藉由分析前開政策措施，說明上開政策的整體成效與執行挑戰。

第二章 新加坡詐騙犯罪現況、趨勢與變化

2.1 現況概述（2024年）

根據新加坡警察部隊（Singapore Police Force, 簡稱SPF）《Annual Scams and Cybercrime Brief 2024》報告，該國在2024年面臨前所未有的詐騙犯罪挑戰。詐騙案件數量達到51,501起，較2023年的46,563起增長了10.6%。詐騙造成的經濟損失亦大幅上升，總額高達11億新幣，較2023年的6.518億新幣增長了70.6%[3]（見表1）。

另依據「全球反詐騙聯盟」[4]於2024年發布之調查報告《State of Scams in Singapore 2024》，65%的新加坡人每月至少遭遇一次詐騙嘗試，54%的民眾表示，受詐騙威脅頻率較一年前增加[5]，自上述數字透露之端倪可看出，詐騙是新加坡人民有感且在意的犯罪型態。

儘管新加坡政府採取了多項打擊措施，然而詐騙犯罪的規模與影響仍在持續擴大，新加坡的打詐之路仍是一場長期抗戰。

表1、新加坡2024年詐騙犯罪概況

詐騙犯罪指標	2024現況	年增率
詐騙案件數	51,501 件	+10.6%
經濟損失金額	11億新幣	+70.6%
每人每月遇詐比例	65%	–
詐騙威脅上升感受之比例	54%	

資料來源：SPF, Annual Scams and Cybercrime Brief 2024（Singapore: SPF, 2025), p. 1; Global Anti-Scam Alliance（GASA）and Feedzai, The State of Scams in Singapore 2024（ Singapore: GASA, 2024), pp. 10-11.

2.1.1 主要詐騙類型

就案件數量而言，電子商務詐騙[6]（22.7%）、求職詐騙（17.6%）、網路釣魚詐騙（16.6%）、投資詐騙（13.2%）及假朋友詐騙（8.1%）是2024年新加坡排名前五名的詐騙類型（見表2）。

3 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p.1.

4 全球反詐騙聯盟（Global Anti-Scam Alliance, GASA）係一國際性非營利組織，致力於推動全球各界合作對抗詐騙行為。該聯盟透過研究報告、公民教育與產業合作，強化政府、企業與公眾在預防詐騙上的能力。2024年該聯盟與風險科技公司Feedzai針對新加坡詐騙現況，共同執行並發表《State of Scams in Singapore 2024》，並計訪問約1,200名新加坡民眾。

5 Global Anti-Scam Alliance (GASA) in collaboration with Feedzai, The State of Scams in Singapore 2024 (Singapore: GASA, 2024), pp.10-11.

6 電子商務與電子支付在台灣及新加坡均廣泛使用，也是兩國共同面對之打詐課題，根據電子支付平台Ecopay 2025年彙整之數據，新加坡電子支付（含Apple Pay、Samsung Pay、Paypal及Paynow即時轉帳等）普及率已達96%；與之對照，台灣2023年非現金支付金額佔民間消費總金額的比率也已達63.47%，使用行動支付的民眾亦達77.1%。

表2、新加坡2024年詐騙犯罪概況

排名	詐騙類型	案件數	佔比
1	電子商務詐騙	11, 665	22. 7%
2	求職詐騙	9, 043	17. 6%
3	網路釣魚詐騙	8, 552	16. 6%
4	投資詐騙	6, 814	13. 2%
5	假朋友詐騙	4, 179	8. 1%
6	冒充政府官員詐騙	1, 504	2. 9%
7	性服務詐騙	1, 162	2. 3%
8	貸款詐騙	1, 154	2. 2%
9	網路戀愛詐騙	852	1. 7%
10	社群媒體冒用詐騙	728	1. 4%

資料來源：SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 4.

如依損失總額統計，投資詐騙（28. 8%）、求職詐騙（14%）、冒充政府官員詐騙（13. 6%）、惡意程式詐騙（11. 6%）及電子郵件詐騙（8%）為前五大詐騙類型（見表3）。

表3、新加坡2024年各類型詐騙損失金額及佔比

排名	詐騙類型	金額（新幣）	佔比
1	投資詐騙	3億2070萬	28. 8%
2	求職詐騙	1億5620萬	14. 0%
3	冒充政府官員詐騙	1億5130萬	13. 6%
4	惡意程式詐騙	1億2910萬	11. 6%
5	電子郵件詐騙	8, 850萬	8. 0%
6	網路釣魚詐騙	5, 940萬	5. 3%
7	網路戀愛詐騙	2, 760萬	2. 5%
8	社群媒體冒用詐騙	2, 640萬	2. 4%
9	電子商務詐騙	1, 750萬	1. 6%
10	假朋友詐騙	1, 360萬	1. 2%

資料來源：SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 5.

根據表4，新加坡2024年各類詐騙若以「每案平均受害金額」來看，呈現出高度集中的結構性差異。惡意程式詐騙居於首位，每案平均受害金額高達446, 713新幣，遠高於其他類型。緊接其後的是商業電子郵件詐騙，每案平均損失達240, 489新幣，此二案件類型，案件數相對較低，但受當年度極端大額案件的影響，衝高平均財損。

排名第三的冒充政府官員詐騙，每案平均受害金額為100, 622新幣，雖與前兩類有差距，但亦屬高額損失類型，顯示「公權力」與「法律風險」的心理壓力，仍是詐騙者有效操控決策的重要工具。

表4、新加坡2024年各類詐騙每案平均受害金額前五名

排名	詐騙類型	每案平均受害金額（新幣）
1	惡意程式詐騙	446, 713
2	商業電子郵件詐騙	240, 489
3	冒充政府官員詐騙	100, 622
4	投資詐騙	47, 077
5	社群媒體冒用詐騙	36, 283

資料來源：SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), pp. 4-5.

綜合表2至表4所示，不同詐騙類型的氾濫與損害嚴重度並不相同，可總結下現象：

案件數排名第1的電子商務詐騙，總受害金額1, 750萬，僅排第9名，每案平均受害金額約1, 508新幣，排第12名。易言之，此類詐騙屬於平均個案財損較輕，但影響層面廣泛的詐騙類型，常見的手法是「網購未交貨」，詐騙者利用拍賣平台、社群媒體刊登電子產品、演唱會門票等熱門商品，以低價吸引受害者上當。

反之，2024年平均受害金額居前二名的惡意程式詐騙及商業電子郵件詐騙，案件數分別為289及368件，佔年度案件數僅不足1%。然而因一起受損金額高達1. 25億新幣的惡意程式詐騙個案，及另一起5, 720萬新幣的的電子郵件詐騙個案，致整體受害金額衝高。

此外，投資詐騙、求職詐騙、冒充政府官員詐騙屬於案件數與受害金額均相對較高的案件類型，這幾類詐騙將是新加坡政府須優先處理的重要課題。

2. 1. 2 受害者結構

2024年，70. 9%的受害者年齡在50歲以下，其中30–49歲的受害者最多，占比41. 2%[7]，此一年齡層在多個高案件數的詐騙類型中，都為最主要受害年齡區間，包括：45. 1%的電子商務詐騙案件受害者、44. 2%的投資詐騙受害者、44. 5%求職詐騙受害者及42. 2%的網路釣魚受害者（見表5）。

新加坡警方未揭露各年齡層受詐金額數據，然報告指出，65歲以上的受害者總數佔比雖不高，但每人平均損失金額為各年齡層中最高[8]，這亦可從高齡者最常受害的詐

7 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p.8.
8 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p.7.

騙類型觀察得知，65歲以上族群最常受害的類型依序分別是網路釣魚、投資詐騙及假朋友詐騙，相對年輕族群受害集中於個案金額較低電子商務詐騙，高齡族群受害情形值得特別關注。

表5、2024年詐騙受害者年齡比例

年齡層	佔總受害者比例	前三大詐騙類型（以案件數計）
19歲以下	6.3%	電子商務詐騙，求職詐騙，網路釣魚詐騙
20–29歲	23.4%	電子商務詐騙，求職詐騙，網路釣魚詐騙
30–49歲	41.2%	電子商務詐騙，求職詐騙，網路釣魚詐騙
50–64歲	20.7%	網路釣魚詐騙，投資詐騙，假朋友詐騙
65歲以上	8.4%	網路釣魚詐騙，投資詐騙，假朋友詐騙

資料來源：SPF, Annual Scams and Cybercrime Brief 2024（Singapore: SPF, 2025）, p. 8.

2.2 長期趨勢與變化（2018–2024年）

2.2.1 案件數量及受害金額激增

圖1呈現新加坡2018年至2024年詐騙犯罪概況，2018年起，新加坡詐騙案件數量大幅增長。根據新加坡警察部隊年報[9]提供之相關數據，2018年為6,730起，2019年增至9,545起（增長41.8%），2020年達15,651起（增長64.0%），2021年為23,933起（增長52.9%），2022年為31,728起（增長32.6%），2023年為46,563起（增長46.8%），2024年則達到51,501起（增長10.6%），六年間增長約665%，年均複合成長率為40.4%，顯示其增長是連續多年快速累積的結果。

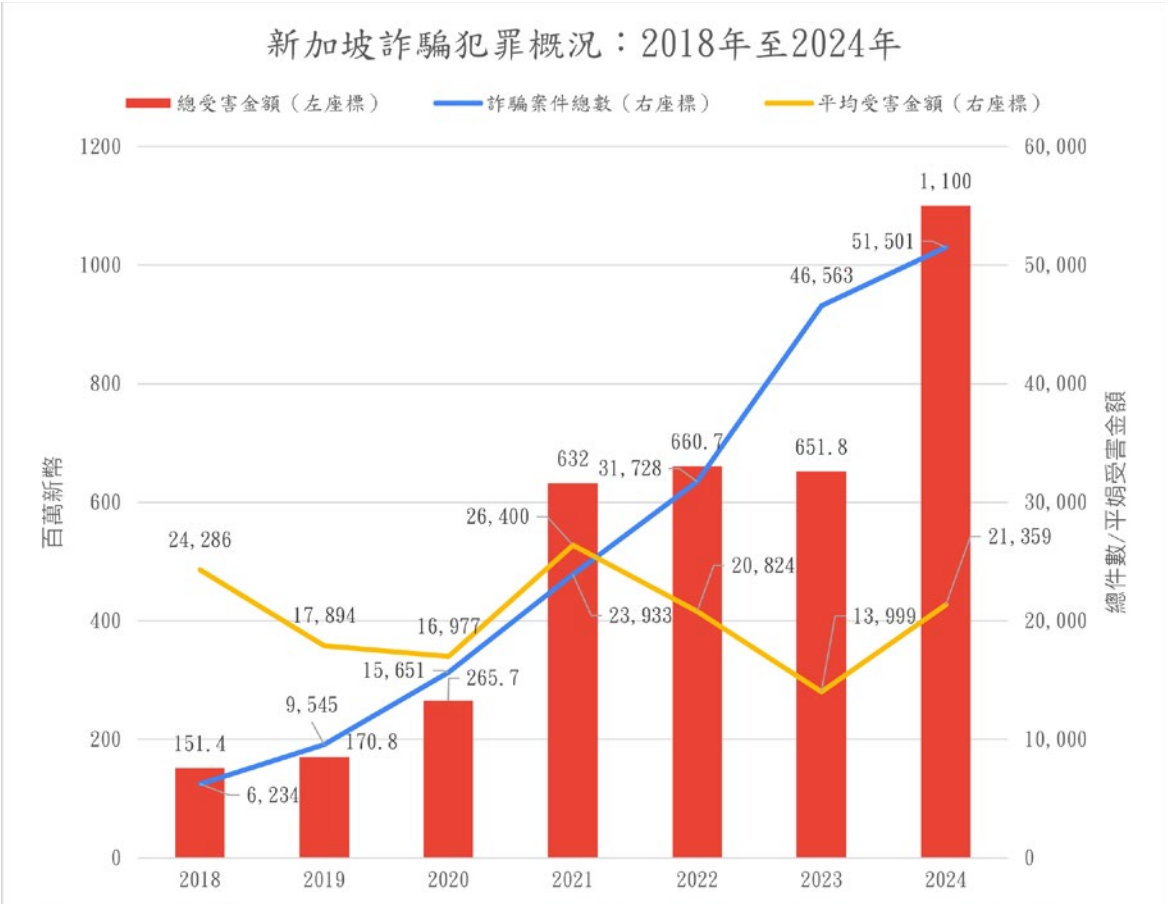
隨著案件數激增，新加坡詐騙犯罪的經濟損失在2018年至2024年間也顯著擴大。根據上述報告，2018年詐騙損失金額約為1.51億新幣，2019年上升至1.71億新幣（增長13.2%），2020年增至2.66億新幣（增長55.6%），2021年增至6.32億新幣（增長137.6%），2022年緩增至6.61億新幣（增長4.6%），2023年略降至6.52億新幣（減少1.4%），2024年則首度突破11億新幣，年增幅近70%，2018至2024這6年間受害金額增加超過720%。儘管年度增率波動極大（2021年暴衝、2023年短暫回落），年均複合成長率為39.2%，顯示詐騙的經濟衝擊並非偶發，而是結構性放大。

特別的是，2024年受害金額成長，係由少數高額個案推升。其中一起單一惡意軟體詐騙案即造成了1.25億新幣的損失，詐騙者提供偽造的線上會議連結，經受害者點擊後，隨即被要求在電腦上運行特定的不明程式，該程式鎖定並攻擊受害者的加密貨

9 SPF, Annual Scams and Cybercrime Brief 2022 (Singapore: SPF, 2023), p. 2; SPF, Annual Scams and Cybercrime Brief 2023 (Singapore: SPF, 2024), p. 1; SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 1.

幣錢包，受害者直到發現有未經授權的加密貨幣交易後，才意識遭受詐騙。另外三起高額案件，受害金額分別高達5,720萬、3,380萬及2,170萬新幣，這些案件凸顯損失集中化的趨勢，少數重大詐騙即可對整體數據造成重大影響（見表6）。

圖1、新加坡2018年至2024年詐騙犯罪概況



資料來源：SPF, Annual Scams and Cybercrime Brief 2022 (Singapore: SPF, 2023), p. 2; SPF, Annual Scams and Cybercrime Brief 2023 (Singapore: SPF, 2024), p. 1; SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 1.

表6、新加坡2024年受害金額最大之4件詐騙個案情形

類型	案件說明	金額	自願轉帳
惡意軟體詐騙	受害者點擊假冒的會議連結，遭遠端盜走加密貨幣	約1.25億新幣	
商業電郵詐騙	受害者收到假冒之供應商修改帳戶資訊，誤信並轉帳	約5,720萬新幣	是
網路釣魚詐騙	假冒錢包網站騙取帳號密碼後，轉走加密貨幣	約3,380萬新幣	
社群平台假冒詐騙	受害者誤認公司主管指示，轉帳加密貨幣	約2,170萬新幣	是

資料來源：SPF, Annual Scams and Cybercrime Brief 2024（Singapore: SPF, 2025), pp. 23–24

2.2.3 詐騙類型演變

圖2至4分別以案件數、總受害金額及平均受害金額為準，呈現新加坡2018年至2024年主要詐騙類型變化趨勢，自圖表及數據可以觀察出新加坡詐騙類型之變化與主要挑戰：

一、詐騙類型集中化

以案件數而言，2018年至2024年集中於電子商務詐騙、求職詐騙、網路釣魚詐騙、假朋友電話詐騙及投資詐騙等主要類型，較其他類型明顯為高。以總受害金額觀之，投資詐騙、假官員詐騙與求職詐騙常年居高不下，應係優先解決之課題。

二、主要詐騙類型損害情形分化

進一步觀察，前段提到之主要詐騙類型，發展型態並不相同，可約略分為「高案件量、低平均損害」及「高案件量、高平均損害」兩類，分述如次：

（一）高案件量、低平均損害

此類型以電子商務詐騙為主，電子商務詐騙案件數在2023年爆增105.4%至9,783件，並在2024年以11,665件高居案件數榜首，但平均受害金額在2023年下降68.2%，至新幣1,428元，2024年亦維持在1,508元之低水準，此可能係反詐騙措施發揮成效，例如電商支付保障及公眾宣導。

類似的情形也發生在求職詐騙中，自2021年起，新加坡的求職詐騙大幅成長，但長期而言，已能有效遏制平均受害金額增長。此二類詐騙之平均受害金額雖受控制，但持續上升的案件數量顯示其影響廣泛，仍不容忽視。

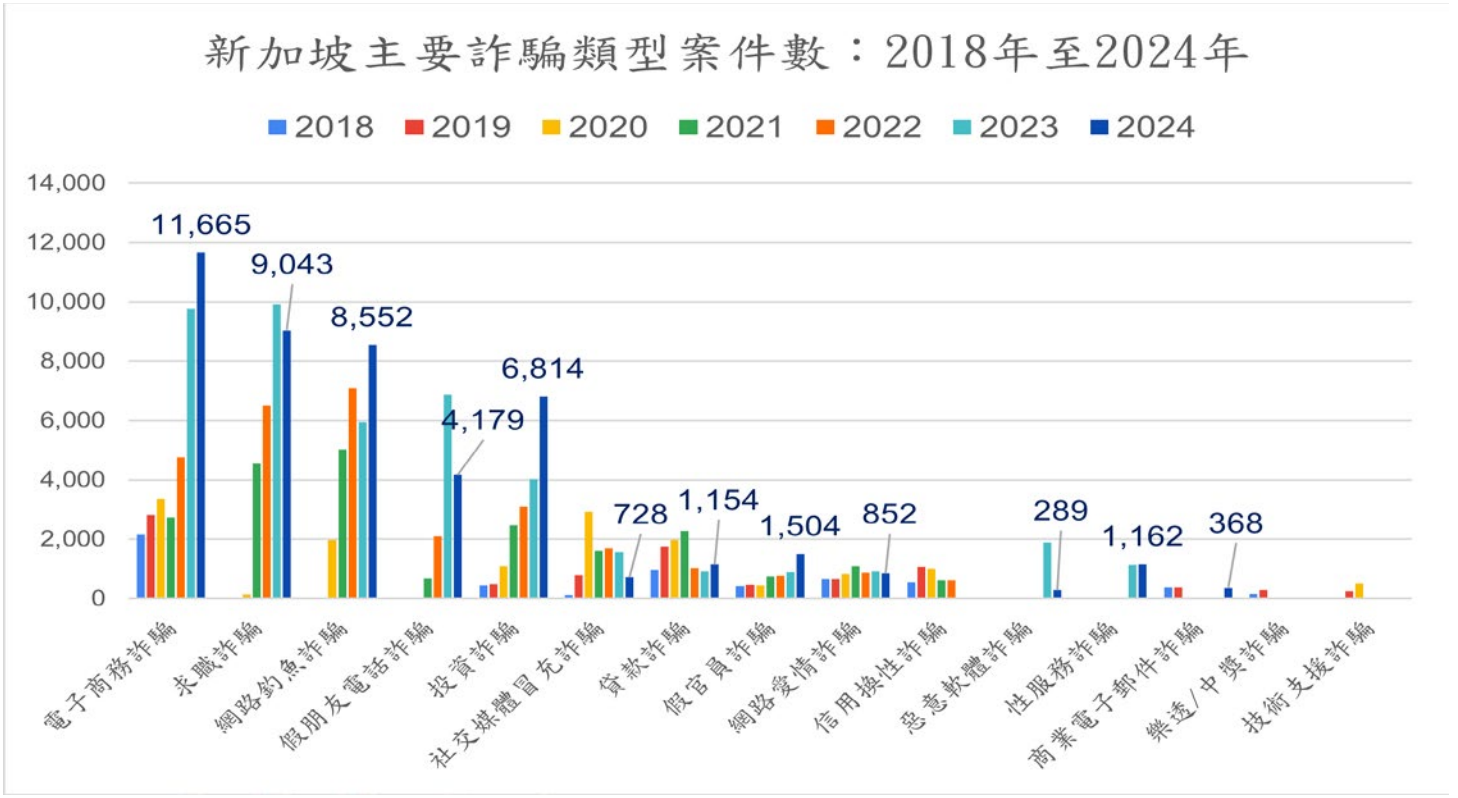
（二）高案件量、高平均損害

相對地，假官員詐騙與投資詐騙每年均有相當案件量，且平均受害金額居高不下，假官員詐騙自2021年起連續4年之個案平均金額超過10萬新幣，而投資詐騙則因其總案件數與平均損失金額均高，其總受害金額已連續4年高居新加坡各類型詐騙之首，此二類詐騙均係典型詐騙集團以心理操控進而使受害者自願轉帳之類型，係星國政府須優先著手介入的課題。

三、單一高損失案件之影響

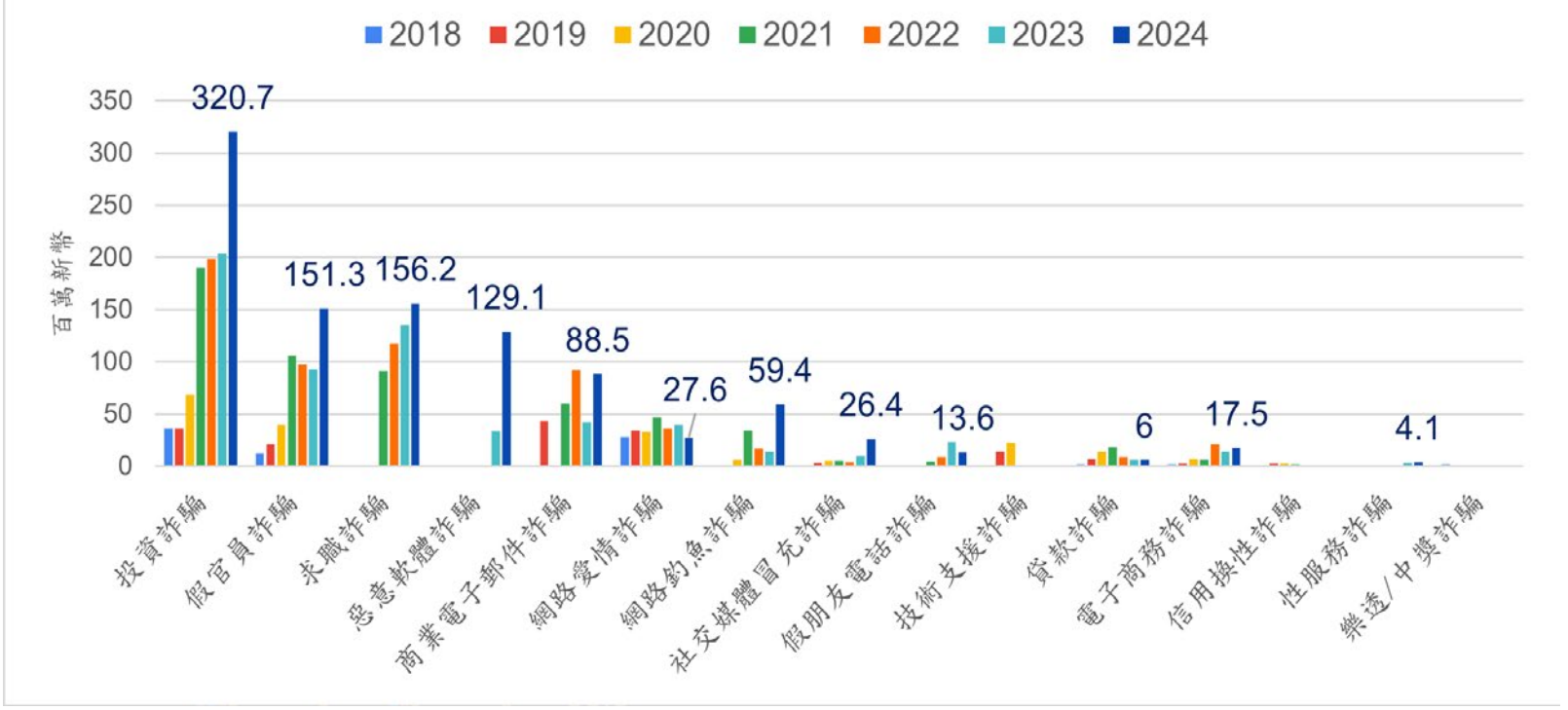
部分詐騙類型依案件數觀察，已受到相當控制，但偶發的重大案件仍使當年的受害金額飆升。例如2024年惡意軟體詐騙案件總數銳減84.8%，呈現一定的遏制成效，但因為一起高達1.25億新幣的詐騙案，致總受害金額暴增278.6%，由於係極端案例，其問題嚴重性與防詐成效的評估，或應持續觀察未來一、二年之變化。

圖2、2018年至2024年新加坡主要詐騙類型（以案件數為準）



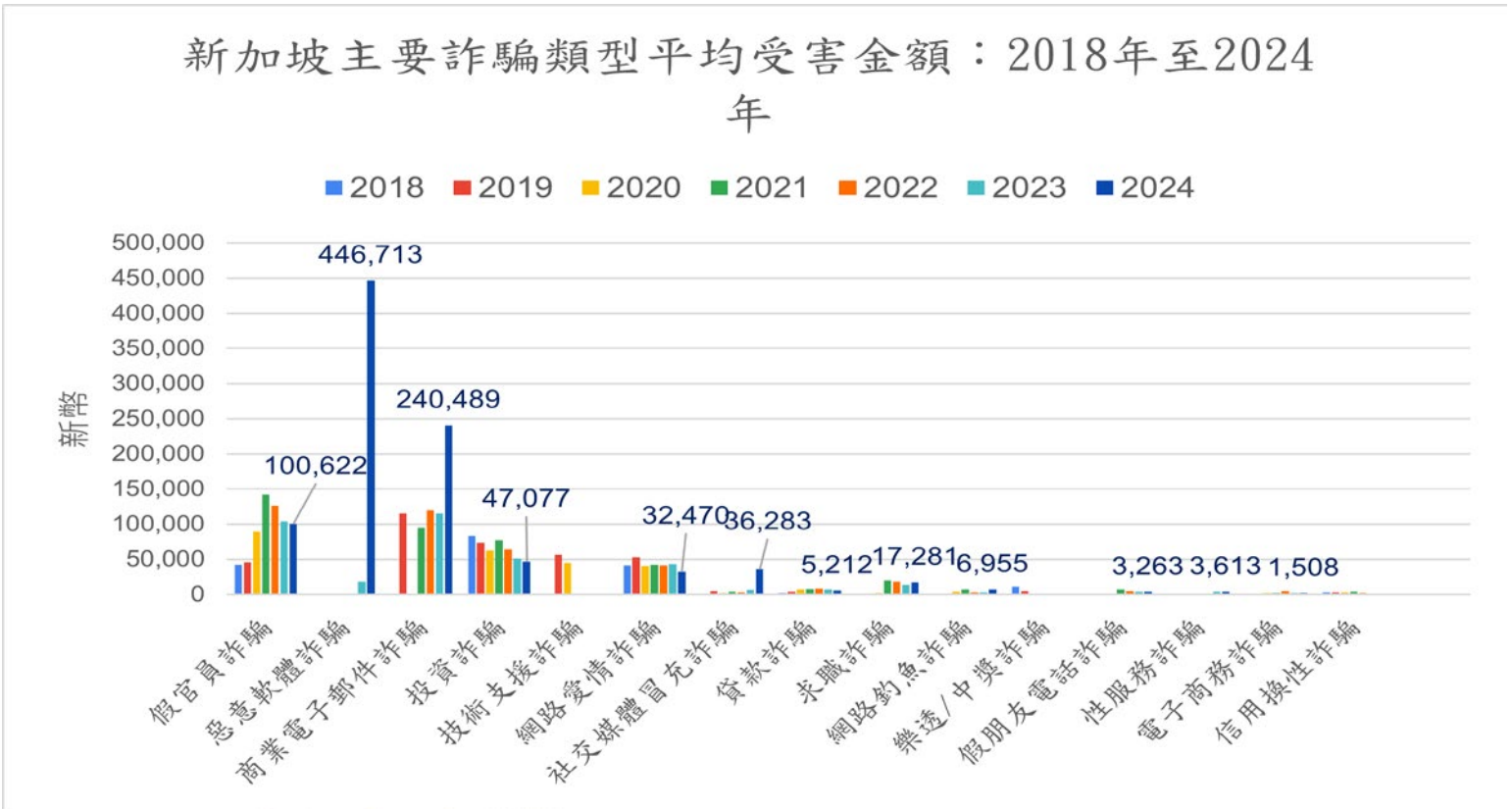
資料來源：駐新加坡代表處整理

圖3、2018年至2024年新加坡主要詐騙類型（以總受害金額為準）



資料來源：駐新加坡代表處整理

圖4、2018年至2024年新加坡主要詐騙類型（以平均受害金額為準）



資料來源：駐新加坡代表處整理

2.2.4 科技化與跨國化

與傳統的詐欺相比，現今之詐騙案之所以得擴大其接觸面、犯罪規模與社會影響力，即是因為資訊科技提供詐騙犯以遠端或虛擬空間實施詐騙行為之可能。新加坡警方指出，網路與智慧型手機普遍滲透於大眾生活，正是現今詐騙犯罪得以發展的背景因素[10]。科技的應用使詐騙犯罪走向跨國化，新加坡警方多次指出，絕大多數新加坡詐騙案件，均由詐騙集團於境外施行。

圖5呈現新加坡詐騙案件使用之聯繫管道變化情形，社交媒體與通訊軟體係毫無疑問的前二名，而在星國主流通訊與社交媒體平台中，臉書母集團(Meta)旗下的產品(臉書、WhatsApp、Instagram）是詐騙犯接觸潛在受害者的主要管道，新加坡警方特別指出，上述Meta之三項產品，受詐騙集團偏好，不成比例地被濫用於各類詐騙案件，特別受星國政府關注。

舉例而言，「臉書市場」在2022至2025年連續被評為新加坡各主要電商平台中安全等級最差者，該平台於電子商務案詐騙案件佔比於2023年為46.5、2024年為37.6%[11]，均居各平台之首。

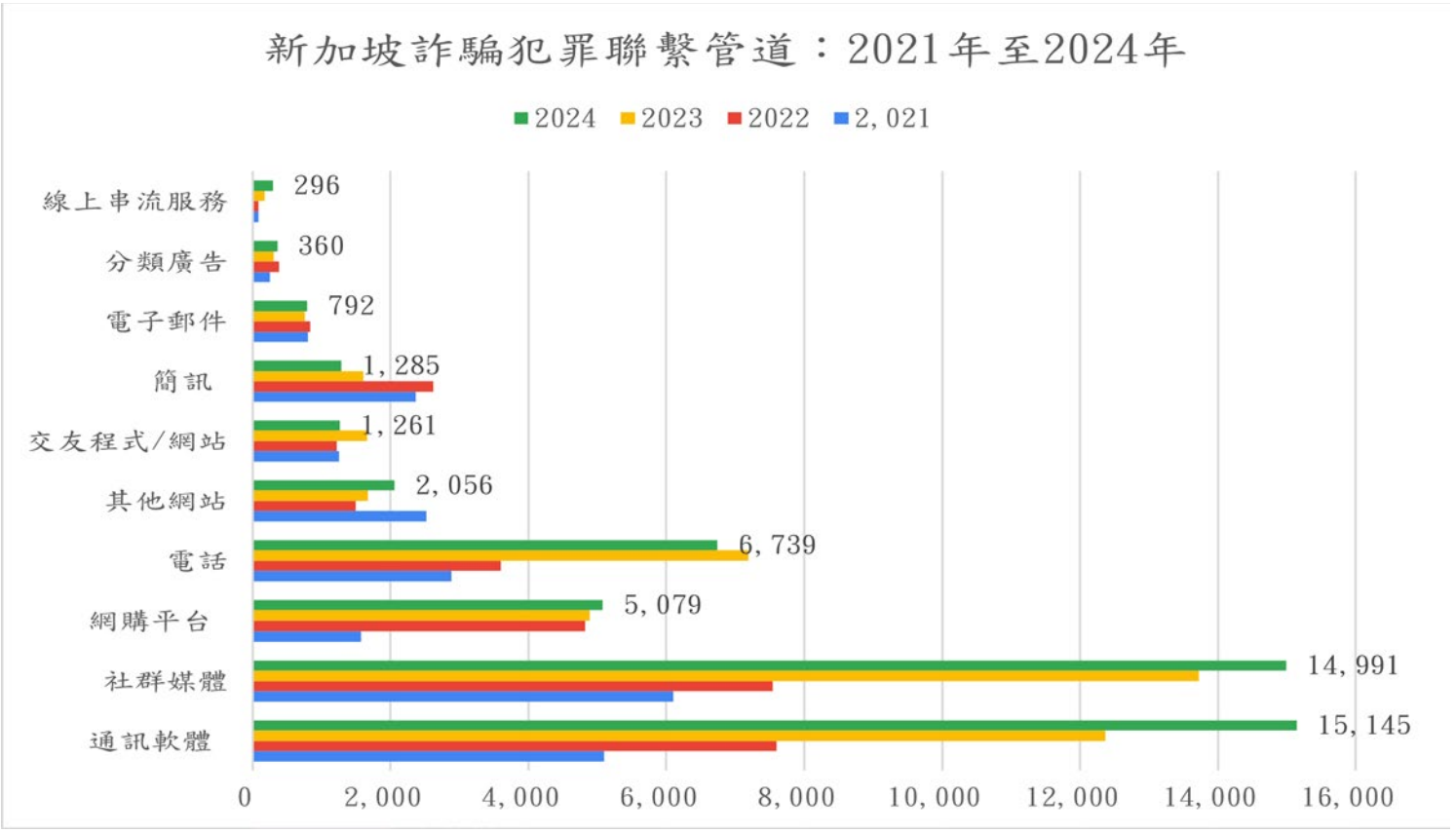
此外，2022年發生在社交媒體上的詐騙案件中，59.6%發生於臉書、34.2%於Instagram[12]，此一比例於2023年分別為71.1%與18.5%[13]，2024年為59.8%與18.0%[14]，

10 SPF, Annual Scams and Cybercrime Brief 2019 (Singapore: SPF, 2020), p. 5
11 https://www.channelnewsasia.com/singapore/facebook-marketplace-anti-scam-rating-system-lowest-e-commerce-imcs-tsr-5321786
12 SPF, Annual Scams and Cybercrime Brief 2022 (Singapore: SPF, 2023), p. 7.
13 SPF, Annual Scams and Cybercrime Brief 2023 (Singapore: SPF, 2024), p. 10.
14 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 7.

始終居於高檔。

通訊軟體、社群平台在詐騙聯繫上的普遍性，衍生了SIM卡管理的問題，新加坡警方指出，近幾年有多件大量冒名購買並註冊SIM卡的案例，於註冊相關平台帳號時得以掩飾詐騙犯之身分、保持匿名，增加跨國詐騙集團對星國民眾施行詐騙的可行性，SIM卡也被詐騙集團用與新加坡廣泛使用的數位支付工具PayNow[15] 結合，收取詐騙款項，進一步體現科技化與金融數位化對防詐之挑戰。

圖5、2021至2024年新加坡詐騙案件各聯絡管道占比



資料來源：駐新加坡代表處整理

2.2.5 加密貨幣受害比例激增

2024年新加坡加密貨幣相關的詐騙損失比2023年大增3倍，佔詐騙總受害金額比例自6.8%翻升至24.3%[16]。加密貨幣匿名、不可逆及難以追蹤的特性，成為詐騙者偏好的收款方式，也是詐騙集團資安攻擊的目標。

加密貨幣並非單一的詐騙類型，而是作為詐騙集團鎖定高價值目標和洗錢的關鍵媒介，常出現在高損失的詐騙模式中，包含投資詐騙、惡意軟體詐騙及網路釣魚詐騙等。

2024年加密貨幣受詐損失金額飆升，源自於前述曾提到之3起高額個案，第一起案例受害者因誤下載惡意程式，遭盜取加密錢包資訊，損失1.25億新幣；第二起案例

15 PayNow是新加坡之最普遍使用之電子支付與轉帳系統，由新加坡銀行公會於2017年推出並由該國金融管理局監管。可用手機號碼、個人身分證或企業註冊碼，直接向個人、商家或政府機關即時收付款，無須銀行帳號資訊。PayNow於新加坡滲透率甚高，新加坡金融管理局指出，幾乎所有新加坡成人均註冊有PayNow帳號。

16 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 2.

受害者誤入偽冒網站輸入加密錢包登入資訊，損失3,380萬新幣；第三起案例受害者誤以為自己正接受公司高層指示，因而轉帳加密貨幣，損失2,170萬新幣[17]。

以上3案損失金額共達1億8,050萬新幣，佔全年詐騙損失之16.2%，可解釋相當大部分2024年新加坡加密貨幣詐騙案件損失激增的現象，但加密貨幣容易被鎖定成為詐取標的，及易為詐騙犯罪後端洗錢工具的特性，將為詐欺調查與追訴帶來前所未有的挑戰。

2.2.6 自願匯款案件居高不下

被害人自願匯款之詐騙並不涉及犯罪者駭入或強制控制受害者的帳戶，而是受害者依其自由意志，自行將資金轉交給詐騙分子。新加坡警方指出，自願匯款案件佔2024年所有詐騙案件的82.4%[18]，為詐騙犯罪的主流。

使受害人自願匯款，係透過操控受害者的心理，可見於各種類型的詐騙中，也與幾種典型的高損失詐騙類型相關。以假官員詐騙為例，詐騙者可透過假冒警察、海關或稅務機關，誆稱受害人涉嫌刑事或行政案件，要求轉帳「保證金」或其他名義款項，整個過程中並未竊取受害人任何帳戶資訊。投資詐騙與網路愛情詐騙亦具類似特徵，前者透過「高回報投資機會」誘導資金投入，後者則建立虛假戀愛關係後訛稱急需資金援助或共同創業，最終導致受害者匯款。

2024年受害金額前四大的個案中，其中兩筆即為受害者自行轉帳，2案造成7,890萬新幣的損失。反映出詐騙集團不僅掌握對一般民眾的心理誘導技巧，也能針對高資產群體亦能設計出更複雜、難察覺的詐欺腳本。和以惡意網頁、軟體騙取密碼或駭侵不同，自願匯款型詐騙，在較少技術介入下，由受害人自行完成金錢轉移的「最後一步」。這一趨勢使得傳統的防詐策略，例如以一次性簡訊密碼或雙重認證等之效果受限，因為詐騙並非發生於系統技術漏洞，而是利用受害者主觀誤信。

對政府而言，介入自願匯款案件更大的難處在於，受害者被詐騙者的說詞所惑，即便受害者家人、銀行或警方介入提醒，拒絕承認自己正遭詐騙，甚至阻止家人報警，當這類狀況發生時，傳統的公眾教育或防詐手段也常力有未逮。

2.3 小結：詐騙犯罪趨勢與未來防範重點

綜論新加坡自2018年以來詐騙案件的發展趨勢、可見之成效及遭遇之挑戰，新加坡的詐騙犯罪不再僅是單純的治安事件，而是演變為結合心理操控、跨國科技平台與

17 如表2-6
18 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 3.

複雜洗錢的複合型產業。總結當前趨勢，可歸納出以下四大優先處理目標：

一、損害規模極大化與「優先打擊目標」

整體而言，新加坡詐騙犯罪規模呈逐年上升趨勢（2024年達51,501件），且財損金額創下11億新幣的歷史新高。觀察各類型數據，詐騙發展呈現集中化趨勢。電子商務詐騙案件量最多，但平均財損較低，反觀特定類型詐騙如投資詐騙、求職詐騙等，不僅案件量高，財損金額亦相當龐大，這些詐騙類型因涉及大額財損與高度心理操控，將是新加坡政府須優先處理的首要課題。此外，惡意軟體詐騙雖案件數較少，但個案平均財損極高（如2024年最高金額個案財損1.25億新幣），亦屬重點防範對象。

二、犯罪手法的心理化：逾八成受害者為「自願轉帳」

數據顯示，2024年高達82.4%的詐騙案件中，受害者是「自願」將款項匯給詐騙集團。這標誌著防禦重心不能僅停留在資安防火牆，因為攻擊的目標已從系統漏洞轉向人性弱點。無論是假冒官員的恐嚇，還是投資詐騙的利誘，詐騙集團透過社交工程繞過了傳統技術防線，事前宣導阻詐更為重要。

三、接觸管道的平台化：社群媒體與通訊軟體成為溫床

通訊軟體及社群媒體是現今多數詐騙發生的場域。詐騙集團高度依賴Meta集團旗下產品（臉書，WhatsApp，Instagram）作為接觸管道。此外，非由本人使用的SIM卡常為詐騙集團大量收購，用於註冊虛假帳號以隱匿身分。因此，平台業者的管理責任與SIM卡的註冊控管，亦將是切斷詐騙接觸管道的關鍵。

四、洗錢工具的虛擬化：加密貨幣風險激增

隨著傳統金融監管加強，詐騙集團轉向監管較難觸及的領域。2024年涉及加密貨幣的詐騙損失激增3倍，佔總損失的24.3%。加密貨幣去中心化及不易追查的特性，使其成為投資詐騙與惡意軟體詐騙首選的洗錢工具，大幅增加了資金追回的難度。

基於上述趨勢，特別是針對投資、求職與假冒官員等高財損案件，未來的反詐政策將更著重於「阻斷金流」與「強制介入」，具體防範重點應包含：

一、針對「自願轉帳」的強制介入：

鑑於超過八成案件屬受害者自願轉帳，且勸導往往無效，未來的政策必須於受害者匯出款項前，爭取更多冷靜時間。

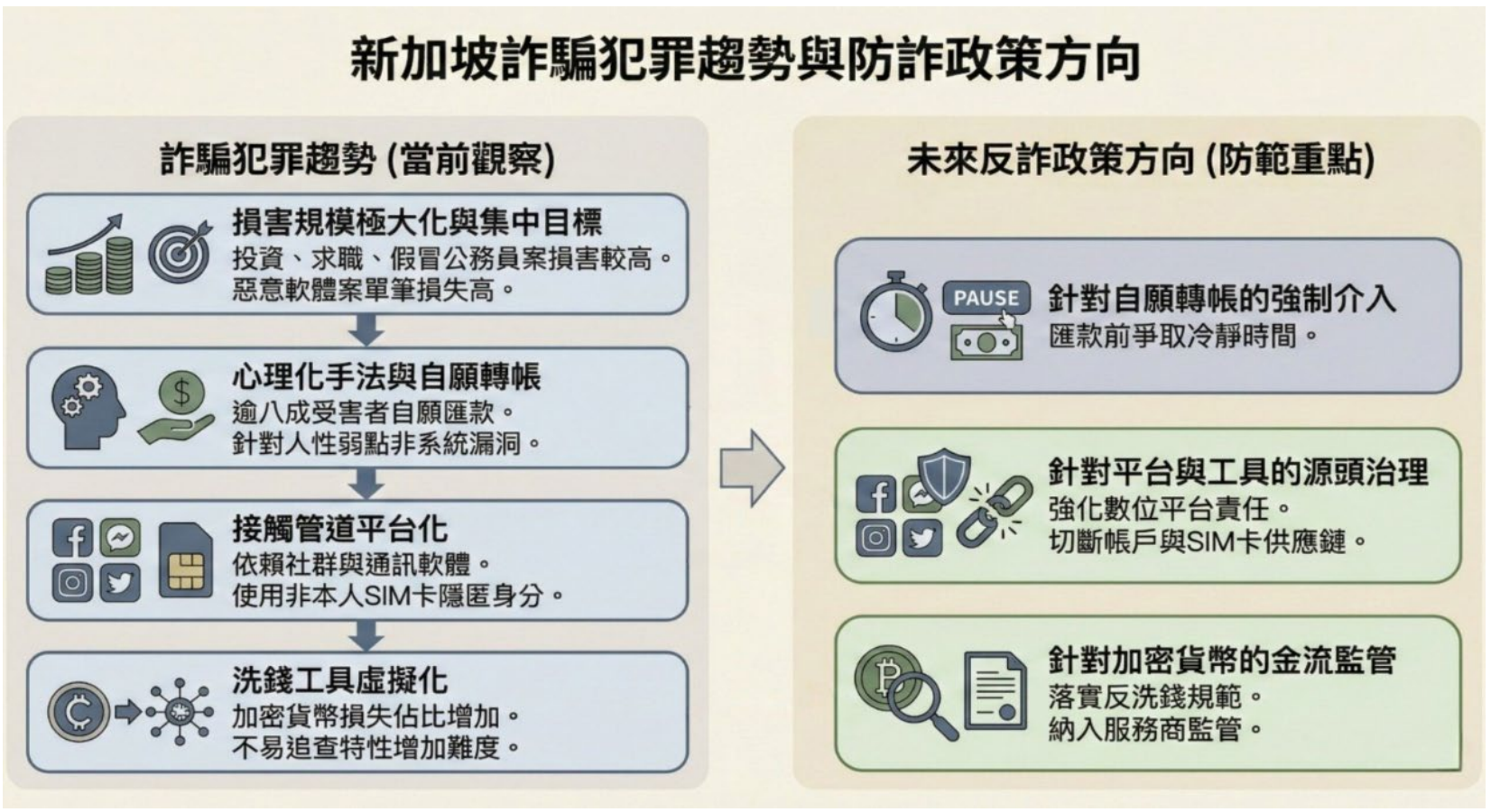
二、針對「平台與工具」的源頭治理：

絕大多數詐騙發生在社群平台且依賴人頭SIM卡，政策重點必須強化數位平台的看門人責任。切斷詐騙集團獲取通訊工具與人頭帳戶的供應鏈，並強制平台移除詐騙內容。

三、針對「加密貨幣」的金流監管：

面對加密貨幣詐騙損失佔比攀升至近四分之一，政策防線需擴展至虛擬資產端。這包括落實反洗錢規範，將加密貨幣服務商全面納入監管，並對協助洗錢的協力者制定更嚴格的規範。

圖6、新加坡詐騙犯罪趨勢與防詐政策方向



資料來源：駐新加坡代表處繪製

第三章 新加坡打擊詐騙犯罪的措施：法律面向

在面對詐騙犯罪規模化、數位化與心理操控化的發展趨勢下，新加坡政府意識到，單靠刑法條文與單一法律工具，已難以有效應對跨平台、跨境且迅速變化的詐騙手法。為此，2020年起，新加坡啟動一連串有系統的法制改革工程，逐步建構出一套具完整分工的防詐法律體系。

自2024年起，新加坡政府相繼完成立法及修訂之六部法規，包括：

一、《支付服務法》（Payment Services Act，2024年4月修訂生效）

二、《電腦濫用法》修訂（Computer Misuse Act，2024年2月修訂生效）

三、《線上犯罪危害法》（Online Criminal Harms Act，2024年2月生效）

四、《雜項犯罪法》修訂（Miscellaneous Offences Act，2025年1月修訂生效）

五、《貪腐、販毒與其他嚴重犯罪（沒收利益）法》修訂（CDSA，2024年2月修訂生效）

六、《防詐騙保障法》（Scam Prevention Act，2025年7月生效）

七、《刑事法（雜項修正）法案》，（Criminal Law（Miscellaneous Amendments）Bill，2025年11月4日修法通過）

這六部法規各有側重，合組成一套完整的防詐規範體系：

一、金流監管與非法所得沒收：

《支付服務法》規範支付業者的反詐與反洗錢義務，為金流追蹤建立第一道防線。《貪腐、販毒與其他嚴重犯罪（沒收利益）法》則提供法律依據，讓執法單位能追蹤、凍結並沒收與詐騙相關之所得，特別針對人頭帳戶運用情形設下新罪名與量刑指南，提供追回不法所得之工具。

數位身份與工具濫用處罰：

《電腦濫用法》修法後，新增條文針對交出數位個人身分（Singpass）[19]等行為予以入罪，嚇阻並懲罰明知或疏忽地讓詐騙集團利用自己數位個人身分從事詐騙之犯罪協力者。

二、網路平台治理與預防性封鎖：

19 新加坡「數位個人身分」是新加坡政府推出的官方數位身份認證系統。它允許新加坡公民和永久居民，透過單一安全的方式登入超過 2,700 項政府和私人機構的數位服務。使用者透過 新加坡數碼個人身分應用程式完成指紋或臉部識別等身分驗證，即可連結公共服務或線上交易，係新加坡人之數位身分憑證。

線上犯罪危害法》賦予政府權力對高風險網路服務平台（如Meta、Telegram、旋轉拍賣）發出命令，要求其落實偵測機制、移除詐騙帳號與提供年報揭露，開創了東南亞少見的「反詐平台責任制度」。

三、實體通訊工具濫用打擊：

雜項犯罪法》修正後，將人頭SIM卡的轉讓、非法註冊與販售設為刑事犯罪，處罰不實申請者、中介者與業者三方，是針對詐團利用新加坡電話號碼申請網路平台人頭帳號，或以貓池、卡池[20]機房濫發詐騙電話之制度性補強。

四、即時介入與轉帳限制：

《詐騙防治法》因應「自願轉帳無法即時阻止」的執法瓶頸，創設限制令制度，賦予警方在高風險情境下，可要求銀行暫停潛在受害者個人交易，以爭取時間進行干預與說服，防止金錢流出境外。

五、納鞭刑為詐欺犯刑罰：

有鑑於詐欺犯罪在新加坡的氾濫程度，新加坡政府為回應民眾加重對詐欺犯罪的處罰力度之呼聲[21]，新加坡政府於2025年11月完成修法三讀，將詐欺相關犯罪納入鞭刑刑責，期提升威嚇效果。

20 「貓池」（Modem Pool）係能同時插入多張SIM卡的電信通訊設備，用於大量收發簡訊、通話或接收驗證碼。「卡池」則是「貓池」設備中實際用來放置SIM卡的部分。貓池因其能夠一次處理大量電話和簡訊的特性，常被詐騙集團用來進行犯罪活動。

21 https://www.mha.gov.sg/mediaroom/parliamentary/second-reading-of-the-criminal-law-miscellaneous-amendments-bill-wrap-up-speech

圖7、新加坡近期防詐立法作為

資料來源：駐新加坡代表處繪製

3.1《支付服務法》（2024年4月修訂生效）

3.1.1 修法背景：支付市場變化快速，法律需更新應對

2010年代中期，新加坡的支付生態系統快速發展，出現電子錢包、電子支付平台及加密貨幣等新型態服務。金融管理局為維持金融市場穩定，避免支付系統遭濫用於洗錢及資助恐怖主義，亦盼建立靈活而有包容性之監管框架，鼓勵創新支付方式，同時保障消費者利益與系統安全。因此，於2019年立法通過《支付服務法》，並於2020年1月28日正式生效。

自2020年《支付服務法》上路後，新加坡支付版圖迅速擴張，尤其是「數位支付代幣」（Digital Payment Token）相關活動與跨境匯款模式仍有監管。配合防制洗錢金融行動工作組織對虛擬資產服務業者的最新指引，以及2023年爆發的30億新幣洗錢案，金融管理局決定修正《支付服務法》，並自2024年4月4日起全面擴大管制範圍，並針對數位支付代幣業者制定用戶保護與金融穩定措施的法源。

3.1.2 法令內容

《支付服務法》以「模組化」的方式設計，針對不同類型的支付服務實施分級監

管。

主要內容包括：

一、涵蓋七大支付活動

（一）帳戶發行服務

（二）國內匯款服務

（三）跨境匯款服務

（四）商業支付接受服務

（五）電子貨幣發行服務

（六）數位支付代幣服務

（七）貨幣兌換服務

二、兩級執照制度

（一）標準支付機構：規模較小，需符合一般監管標準。

（二）大型支付機構：規模大（如年交易量、客戶資金額度超過門檻），須遵守更嚴格的資本充足、隔離資金等要求。

三、加強反洗錢與資助恐怖主義規範

所有受規範機構必須遵守「反洗錢及打擊資恐通則」。

四、保護消費者

（一）要求業者保障用戶資金（如：隔離帳戶、信託安排）。

（二）必須妥善處理爭議與退費機制。

五、靈活的監管授權

金融管理局可依市場變化，規定新的支付服務或更新規範。

3.1.3 成效與案例

一、加強對支付服務提供者的監管，防止成為詐騙工具

（一）執照制度

（二）《支付服務法》要求所有提供支付服務（如電子錢包、跨境匯款、加密貨幣交易）者必須取得執照。金融管理局於發照時將審查公司之背景、資本能力及反詐騙措施等，過濾可疑或不合規業者。

（三）適用持續監管與檢查

（四）金融管理局可持續監督支付服務業者，包括其交易記錄、內部控制、異常交易監控機制等。若業者未能妥善防範詐騙風險，可能遭吊銷或暫停執照。

二、要求業者建立反洗錢與反資恐制度，加快詐騙資金凍結、調查及追蹤流程

交易監測義務：所有受監管的支付服務業者必須建立交易異常偵測系統，如：

（一）大額交易異常

（二）頻繁小額轉帳異常

（三）非典型地理位置/客戶行為異常

1. 可疑交易申報若懷疑有詐騙、洗錢、資恐行為，支付業者必須主動向新加坡警方的商業事務局或反詐騙中心通報。

三、提升消費者保護，減少個人受騙損失

（一）資金保護要求：大型支付機構必須將用戶資金隔離於獨立帳戶（如：信託帳戶），即使業者破產，客戶資金也能安全返還。

（二）投訴與爭議解決機制：《支付服務法》要求業者設立明確的客訴與調解機制，若消費者因詐騙或未經授權交易受損，能及時處理與補救。

四、擴大監管至加密貨幣服務，防止虛擬詐騙

（一）《支付服務法》納管加密貨幣交易所、加密錢包提供者，要求其進行客戶盡職調查、資金流監控，並規定托管、轉移及兌換等服務皆須持有相關證照方能營運。

（二）防止詐騙集團利用加密貨幣匿名性進行資金轉移與洗錢。

表7、《支付服務法》內容與成效

功能項目	具體說明	防詐效果
執照審查	過濾不良或風險業者	阻斷詐騙平台
反洗錢與反資恐機制	交易監測與可疑交易申報	快速查凍資金流
資金保護	資金隔離、消費者投訴機制	減少被害損失
虛擬貨幣納管	管控加密資產交易所，托管、轉移及兌換等服務皆須持照	防範虛擬詐騙

資料來源：駐新加坡代表處整理

3.1.4 實際案例、成果及展望

2023年7月至2024年12月期間，多家金融機構因未能遵守反洗錢與反資恐規定，金融管理局因而處以總計超過1,500萬新幣之罰款[22]。這些違規行為包括未能進行充分的客戶盡職調查、未能監控異常交易活動，以及未能維護適當的交易記錄。前述措施旨在防止金融系統被用於洗錢及資助恐怖活動，從而間接打擊詐騙行為。

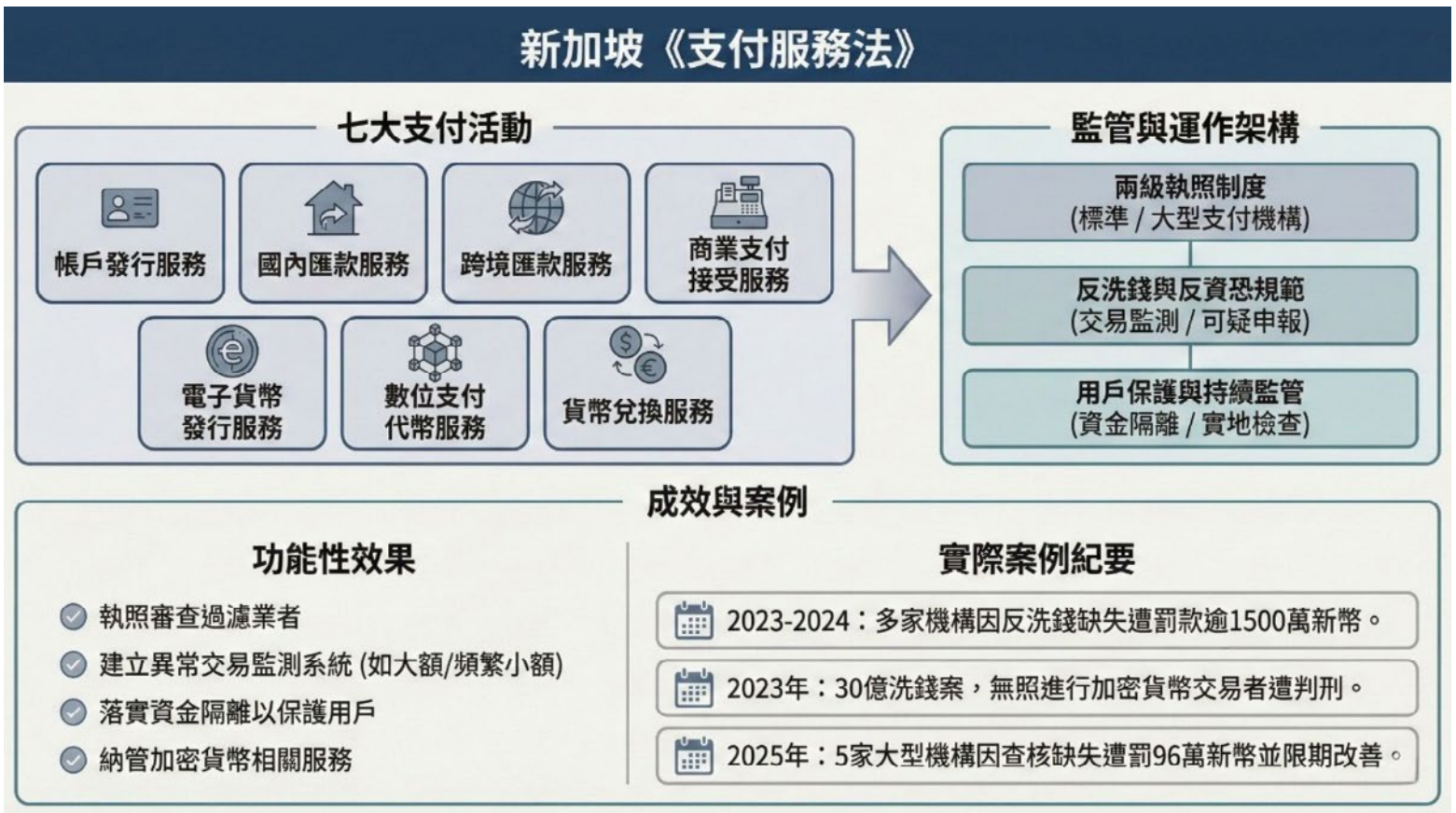
2023年8月，新加坡警方偵破高達30億新幣之洗錢案，逮捕10名中國福建幫嫌犯，被扣押的資產範圍涵蓋現金、豪宅、名車、奢侈品、黃金及加密貨幣等。其中4名涉案人員因未持有在新加坡經營任何類型支付服務業務之牌照，卻進行大量加密貨幣交易，違反《支付服務法》及反洗錢相關法規，分別遭判4週至20個月不等有期徒刑[23]。

2025年6月，新加坡5家大型支付機構因未對客戶及匯款關係人進行洗錢及資恐之資訊查核，以及善盡匯款透明度調查，金融管理局首度對前述機構開罰合計96萬新幣，另同步發布分析報告，列舉常見缺失並要求相關機構於六個月內完成改善[24]。

上述案例顯示，金融管理局透過《支付服務法》對支付服務提供者進行嚴格監管，有效整合過去分散的監管架構，並對違規行為採取果斷執法行動，進而達到維護新加坡金融體系完整性及安全性之目的。

22 Monetary Authority of Singapore, Enforcement Report 2023-2024 (Singapore: Moentary Authority of Singapore, 2025), p. 7
23 Ministry of Finance, Virtual Assets Risk Assessment Report Singapore 2024 (Singapore: MOF 2025), p. 28
24 Kenneth Lo, “Payment service providers under the radar: MAS imposes composition penalties on five major payment institutions for AML/CFT Breaches,” Bird & Bird, 30 June, 2025, https://www.twobirds.com/en/insights/2025/singapore/payment-service-providers-under-the-radar-mas-imposes-composition-penalties-on-five-major-payment-in

圖8、《支付服務法》內容與成效



資料來源：駐新加坡代表處繪製

3.2《電腦濫用法》修訂（2024年2月修訂生效）

3.2.1 修法背景：詐騙產業結構轉變下的協力犯罪問題

在詐騙犯罪高度組織化的趨勢下，2024年超過82.4%的詐騙案件受害人屬「自願轉帳」而受害，高比例的自願轉帳詐騙，其背後仰賴大量協力者支援，包括人頭帳戶或身分出借者、SIM卡代辦與數位個人身分提供者，使詐騙集團得以合理化其運作，降低受害人戒心，也使警方難以追查。

新加坡「數位個人身分」係2003年由新加坡政府資訊通信發展管理局推出，用於認證登入政府網站，讓民眾能方便、安全地使用各項電子化政府服務。2014年新加坡啟動「智慧國家」戰略，「數位個人身分」升級為一全面性的數位身分憑證系統，連接各項政府與私人部門數位服務。截至2024年，「數位個人身分」已具有以下幾個核心功能：

一、可登入超過2,700項政府與企業服務（例如稅務、教育補助、銀行業務等）；

二、支援雙重認證與生物辨識登入；

三、可用於「數位簽名」，具有法律效力；

四、支援轉接服務：如開立公司、設立銀行帳戶或電子錢包時，使用者可透過數位個人身分完成身份驗證程序。

「數位個人身分」現已成為新加坡民眾進行重要法律與金融行為的數位入口，濫用他人「數位個人身分」帳戶或將帳戶交給他人使用，可能導致個人身分被盜用、資

金被挪用，亦淪為詐騙集團之工具。然而在修法前，司法機關需證明濫用或提供數位個人身分的協力者「明知」其行為係幫助詐欺犯罪，方得以刑法詐欺罪論處。為補上此一缺漏，新加坡政府2023年對「電腦濫用法」進行重大修法，將濫用或提供數位個人身分之協力者納入刑事處罰體系，其法規內容說明如下。

3.2.2 修法內容概述

2023年修訂之《電腦濫用法》於2024年2月8日正式生效。本次修法新增下列具體罪名：

一、明知或應合理知情而交付帳號（電腦濫用法第8A條）：若個人在明知或有合理理由相信他人將利用其數位個人身分從事犯罪，或在客觀情況下應合理知道該帳號密碼將被濫用，仍提供者，即構成犯罪。

二、濫用他人身分憑證罪（電腦濫用法第8B條）：獲取、持有、傳輸、供應他人數位個人身分，以供犯罪使用，即便為報酬極低或未獲利，亦構成犯罪。

3.2.3 成果及展望

新法實施後，新加坡警方已以新法查獲相關犯罪，《2024年度詐騙與網路犯罪年報》案例顯示：有被告因新幣2,400元報酬，交出其數位個人身分，供他人註冊開立兩組銀行帳戶，兩組銀行帳戶接收了至少21名新加坡受害人共計超過11萬新幣之款項。法院依修法新罪名判處被告8個月有期徒刑，並命其交還不法所得。《電腦濫用法》之修訂，從協力者的面向為數位詐騙防制打下基礎，尤其降低了協力者主觀構成要件之舉證門檻，也與3.4節《新加坡雜項犯罪法》針對濫用SIM卡之犯罪行為互為補充。

圖9、《電腦濫用法》內容與成效

資料來源：駐新加坡代表處繪製

3.3《網路犯罪危害法》（2024年2月生效）

3.3.1 立法背景

隨著科技快速進步，網路環境成為詐騙、惡意活動與其他犯罪行為的重要溫床，新加坡政府意識到現有法律架構已無法充分應對跨境及匿名性強的網路犯罪威脅。為此，新加坡於2022年進行「網路犯罪與線上安全法令檢討」，並廣泛徵詢業界、民間團體及學界意見，最終於2023年7月5日通過《網路犯罪危害法》。新加坡內政部於2024年1月30日發布新聞稿，正式宣布《網路犯罪危害法》將自2024年2月1日起分階段生效，藉由賦權執法機關及主管部門迅速介入犯罪性網路活動，強化民眾保護及國家安全。

3.3.2 立法條文概述

《網路犯罪危害法》引入一系列措施，使新加坡政府能夠更有效地應對具有犯罪性質的網路活動。該法案相關資訊如下：

一、重點措施：

（一）針對已經發生的、或正準備發生於網路上的犯罪行為，對網路服務業者發出「

指令」，限制其平台上新加坡用戶接觸犯罪活動的可能性；

1. 對不遵守規範的網路服務平台進行進一步限制，以限制犯罪活動的露出；
2. 具有要求業者提供資訊以執行指令、協助調查及刑事訴訟程序的權力；
3. 制定業務規範及指示，加強與網路服務業者的合作，打擊詐騙及惡意網路活動。

（二）有關「指令」之種類、發動條件及效果（見圖10）：

1. 指令種類：包含「停止通訊」、「內容封鎖」、「帳戶限制」、「網路封鎖」及「應用程式下架」等以下5種指令：
   (1) 停止通訊指令：要求指令的接收者停止向新加坡民眾傳播特定的網路內容（包括本質相似的內容）。指令的接收者可以是傳達此類網路內容的個人及實體。
   (2) 內容封鎖指令：要求提供網路服務業者屏蔽其服務中的特定內容（如：發文或網頁），其中可能包含相同內容的副本。
   (3) 帳戶限制指令：要求提供網路服務業者停止使用其服務的帳戶在新加坡進行通訊，或與新加坡民眾聯繫。
   (4) 網路封鎖指令：要求提供網路服務業者阻止新加坡民眾訪問特定網路位置。
   (5) 應用程式下架指令：要求應用程式商場從其新加坡頁面中刪除指定應用程式，避免新加坡民眾繼續下載該程式。
2. 發動條件：當有合理懷疑網路活動有助於實施特定犯罪時，指定官員即可向任何提供網路服務業者、實體或個人發出指令。
3. 指令範圍：該法案將允許政府向任何可能進行犯罪活動的網路服務發布「指令」。
4. 效果：
   (1) 對於詐騙及惡意網路活動，發出指令的門檻較低。當懷疑或有理由相信正在進行的任何網路活動是為準備、實施詐騙或惡意網路活動犯罪時，指定官員即可發出指令。此政策將可使政府能夠在民眾成為受害者之前主動打擊詐騙及惡意網路活動。
   (2) 若網路服務業者未遵守業務規範，主管當局可以發出指令，以限制對該服務或部分服務部分的連線，以限制新加坡民眾進一步遭該犯罪活動影響或受害。

（三）要求資訊的權力：

1. 指定官員、主管當局或被授權官員可以要求接收指令或命令的任何人提供為執行該法案所需的任何資訊。
2. 當合理懷疑發生了特定犯罪行為時，警察及執法官員可要求提供網路服務業者或網域持有者提供相關資訊，以協助調查及刑事訴訟的進行。

3. 上揭權力亦適用於海外實體及儲存於海外之資料。

（四）而針對詐欺在內的犯罪行為，本法第四部份另設計預防性措施，主管機關可向網路服務業者提出包括行為準則、糾正通知或實施指令，概述如次：

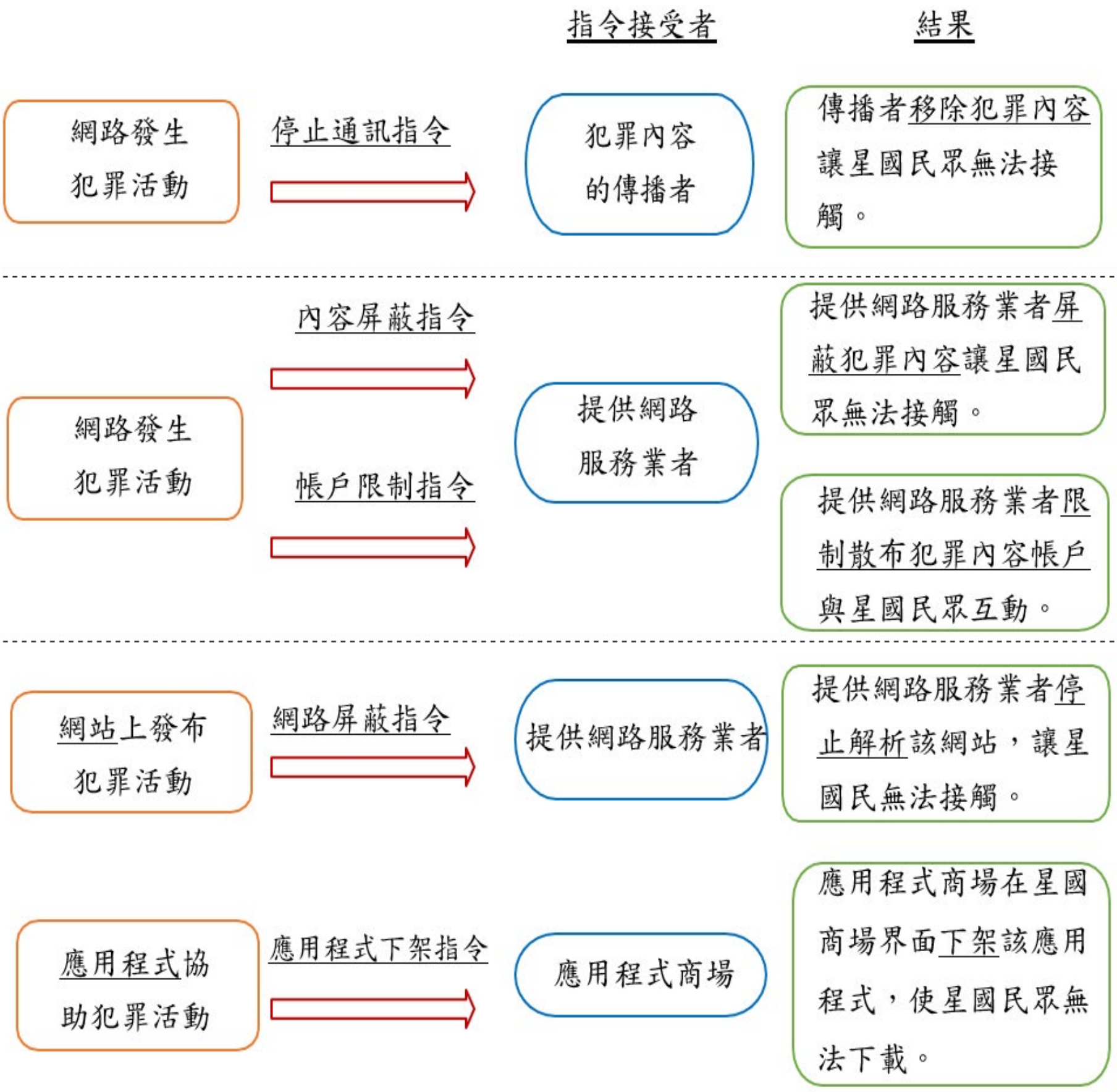
1. 行為準則：由主管機關發布的一套指導原則、最佳實踐或標準要求，規定指定服務提供者應當採取的一般性或特定措施，以預防或應對在其服務上發生的相關犯罪。

2. 糾正通知：當主管當局認為指定網路服務業者沒有遵守適用於其服務的行為準則時，發出此通知，要求他們在規定的時限內糾正不遵守的行為之強制通知。

3. 實施指令：主管機關確信某個特定的流程或措施對於達成打擊指定罪行的目的是必要或有利時，以此指令要求網路服務業者在規定的時限內實施該措施。

（五）前開糾正通知及實施指令對於網路服務業者均有強制力，業者如不遵從，第一次可處最高100萬元新幣罰款，持續不遵從者，可連續處罰每日10萬元新幣罰款。

圖10、網路犯罪危害法指令運作方式



資料來源：駐新加坡代表處整理

3.3.4 實際案例、成果及展望

《網路犯罪危害法》自2024年2月1日起分階段生效後，警方已開始運用法案的相關權力，積極打擊網路詐騙及其他惡意活動。首先針對詐騙網站和嚴重的網路活動發出指令，以優先處理詐騙及惡性犯罪行為，並逐步擴展至其他指定犯罪活動。

新加坡內政部兼國家發展部高級政務次長孫雪玲於2025年3月指出，新加坡警方向社群平台發出「下架指令」，要求24小時內移除或限制接觸特定冒充政府官員之假帳號，已多次獲平台業者配合；另於2024年阻斷逾17萬組詐騙相關之電話線路、網站與社媒帳號[25]，其中部分亦為使用《網路犯罪危害法》指令之成效[26]；在此之前，阻斷詐騙相關之電話線路、網站與社媒帳號之數據僅約6.75萬組。

此外，《網路犯罪危害法》賦予新加坡警方在合理懷疑某項網路活動涉及犯罪時，對網路服務提供者、其他實體或個人發出指令之權力，藉以限制犯罪網路活動的影響範圍，防止新加坡用戶進一步接觸到這些有害內容，展現政府打擊網路犯罪之強硬立場。

2025年9月，新加坡內政部及家庭發展部政務部長吳培銘宣布，新加坡警察部隊依《網路犯罪危害法》對META發布「實施指令」，這是該法通過後新加坡政府首次發出之執行指令。此係因在星國詐騙案件使用的社群平台與通訊軟體中，Meta旗下之臉書、WhatsApp及Instagram即佔案件數的37.3%，是最主要的聯繫管道。該指令要求Meta須在同月底前，採取措施打擊詐騙廣告、強化人臉辨識，並優先處理新加坡用戶的檢舉；若未能在期限內採取足夠改進措施，平台可能面臨高達100萬新幣的罰款。而TikTok因使用人數崛起，也依該法列入線上服務商之列，被要求在2026年2月28日前制定反詐相關措施[27]。

針對電子商務與通訊軟體的漏洞，政府亦持續加強監管。2025年11月，內政部指出，雖然電子商務平台整體詐騙案件較前一年下降約36%，但特定類型詐騙仍有增長。因此，二手交易平台旋轉拍賣承諾於2026年1月31日前實施多項新措施，包括引入通行密鑰（Passkeys）與生物辨識登入，以及將涉及詐騙的「數位個人身分」憑證列入黑名單，禁止其驗證新帳號，以防範已驗證帳號遭濫用[28]。

另新加坡警方發現多起利用蘋果簡訊（iMessage）與Google簡訊（Messages）冒充新加坡郵政及政府機構（gov.sg）的詐騙案例，這類透過網路數據傳輸的訊息一度成為原有簡訊防護機制的漏洞。警方亦於2025年11月進一步依據《網路犯罪危害法》

25 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p.12.
26 “Committee of Supply Debate 2025 on Working Together to Fight Scams – Speech by Ms Sun Xueling, Minister of State, Ministry of Home Affairs and Ministry of Social and Family Development,” MHA, 04 March, 2025, https://www.mha.gov.sg/mediaroom/media-detail/committee-of-supply-debate-2025-on-working-together-to-fight-scams/
27 https://www.zaobao.com.sg/news/singapore/story20250903-7455027
28 https://www.zaobao.com.sg/realtime/singapore/story20251121-7851158

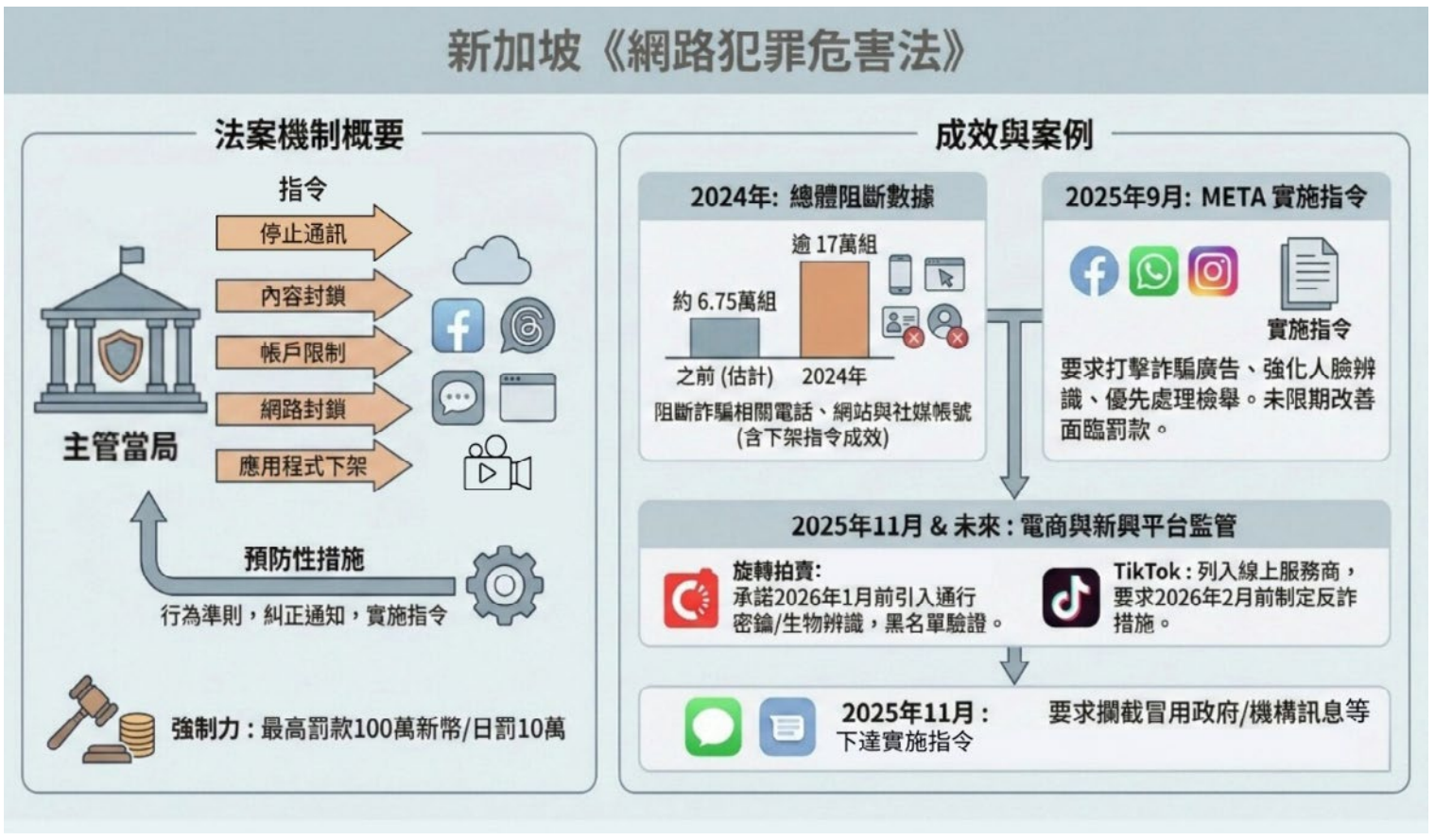
向蘋果及谷歌發出「實施指令」，要求兩大科技巨頭落實防範措施。請業者須攔截顯示冒用政府名稱的帳號或群組訊息，並確保陌生寄件人的名稱顯示不比電話號碼醒目，以協助民眾辨識詐騙訊息[29]。亦可見在法律授權下，政府可針對不同平台特性與新興犯罪手法，對打擊詐欺採取更積極且具強制力之手段。

表8、2023年至2024年政府阻斷詐騙相關標的數量及增幅

阻斷標的	2023年	2024年	年增幅
行動電話門號	＞ 9, 200	＞ 57, 700	＞ 527%
WhatsApp號碼	＞ 29, 200	＞ 40, 500	＞ 38%
網路帳號與廣告	＞ 4, 100	＞ 33, 600	＞ 719%
網站	＞ 25, 000	＞ 44, 900	＞ 79%

資料來源：駐新加坡代表處整理[30]

圖11、《網路犯罪危害法》內容與成效



資料來源：駐新加坡代表處繪製

3.4《新加坡雜項犯罪法》（2025年1月生效）

3.4.1 修法背景

新加坡警察部隊指出，詐騙集團廣泛透過本地合法註冊之SIM卡，進行社群詐騙帳號註冊、即時通訊詐欺、雙重身分驗證接收（如：一次性密碼）、以及電子支付詐

29 https://udn.com/news/story/6811/9161656

30 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 12.

騙金流的接收與轉移[31]。詐騙集團大量以Telegram、WhatsApp帳號引誘受害人加入虛構投資或工作群組，並配合指定的電子支付帳戶完成詐騙流程，而從警方封鎖的龐大電話號碼數量亦可窺知，SIM卡流通管理上確存在漏洞，但過去缺乏直接刑事法律依據可追訴這樣的行為。

此外，本次修法前，對於提供SIM卡的中介人，即便警方能證明其提供的SIM卡最終被用於詐騙通訊，若無法證明中介者「明知SIM卡將用於犯罪」，便難以依舊法課以刑責。同樣，協助詐騙者大量申辦SIM卡的零售業者與店員，也欠缺特別條文對其行為加以規範。即便警方2024年大量封鎖逾五萬筆之詐騙手機號碼，但若無法遏止SIM卡來源，詐騙集團仍可迅速更換號碼、持續作案。

3.4.2 修法內容及條文概述

新加坡政府於2024年修訂《雜項犯罪法》，新增第6A部分，首度明確將「濫用SIM卡」定義為刑事犯罪，建立個人與中介者的刑事責任。新增條文主要包含以下核心罪名類型，分述如下：

一、非法持有他人SIM卡罪

任何人如持有未以其本人身分登記之SIM卡，除非能合理解釋來源與用途，即構成犯罪。該規定設有推定條款：只要非本人註冊卡數量過多、來源可疑，即可推定其行為有不當目的，由被告自負提出反證之責。此設計目的在於快速壓縮SIM卡黑市中轉售行為空間。

二、非法提供個資協助註冊

針對「提供個人資料供他人註冊SIM卡」的行為，修法亦明定構成刑事責任。亦即行為人出售或出借自己的身份證號碼、個人照片或住址證明，讓他人可用其身分完成SIM卡註冊，進而逃避通訊實名制監管。過去這種手法難以歸責，僅能依違反電信合約進行行政處理。

三、非法中介、轉讓或提供SIM卡罪

針對「協助他人取得SIM卡」者，無論是否收費，只要未經授權協助他人開卡、轉讓、提供使用，即可構成犯罪。行為人包含人頭、代購商、零售商等。特別的是，條文明文指出：無論該SIM卡是否實際被用於詐騙，均構成犯罪，體現立法者欲切斷詐騙工具之供應鏈的思維。

31 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 9.

四、非法協助註冊罪

針對協助註冊者（例如電信零售門市或便利店人員）之行為增設刑責。條文明定，若電信服務提供者或其員工在未確實完成實名查驗下，協助第三人註冊SIM卡，即屬違法，可對公司與個人分別課以刑責與罰金。

五、非法使用他人SIM卡罪

針對行為人明知或應知SIM卡非經其本人實名登記，卻仍加以使用。此類行為在詐騙犯罪中極為普遍，詐騙犯嫌為規避責任，常透過管道取得註冊於他人名下之SIM卡，並用於開設即時通訊帳號（如WhatsApp、WeChat）、接收一次性簡訊密碼、註冊金融帳戶或進行與詐騙金流相關的其他操作，過往此類行為若無證據顯示使用者亦參與核心詐騙行為，難以構成刑責。

透過新增罪名補足刑事上對SIM卡濫用行為之規範空白，涵蓋「供應－註冊－轉交－使用」的SIM卡濫用行為鏈，更透過推定與舉證責任轉移，打破過往執法端「難以證明主觀知情」的高門檻困境。此外，條文中對不論「SIM卡是否實際被用於犯罪」之立場，顯示此次修法係重在預防性規範，而非單純回應既有犯罪後果。

3.4.3 實務案例、成果及展望

前述《雜項犯罪法》針對SIM卡供應鏈管制修法部分，於2024年修訂後，於2025年1月實施，2025年3月間新加坡警察部隊即依據新法查獲電信門市店員因以盜用之顧客資料註冊大量電話卡之案件，2025年7月間又再以新法逮捕44名涉及提供偽冒註冊之SIM卡與不法集團之案例[32]。

本法因新修正通過，尚無數據資料，然依照圖5所示，以與手機門號相關之通訊工具施行詐騙案件，包含通訊軟體、社群媒體、撥打電話或簡訊等，占詐騙犯罪中之絕對多數，該法修正之處確補足新加坡原先存在的打詐漏洞，有助於在詐騙犯罪之前端建立制度性防火牆。

32 https://www.police.gov.sg/media-room/news/20250728_44_persons_investigated_for_suspected_involvement_in_fraudulently_registering_sim_cards

圖12、新加坡《雜項犯罪法》內容與成效

資料來源：駐新加坡代表處繪製

3.5《貪腐、販毒與其他嚴重犯罪（沒收利益）法》修訂（2024年2月生效）

3.5.1 修法背景

為因應詐騙與洗錢犯罪手法日益複雜化、分工化的趨勢，新加坡於2024年2月8日正式修訂《貪污、販毒與其他嚴重犯罪（沒收利益）法》，這是該國打擊金融犯罪體系中的重要一環。在2024年修正前，雖已透過該法第54條與第55條初步建立針對洗錢行為的刑事處罰框架，惟實務上仍存有兩大明顯不足：其一，主觀構成要件之門檻過高，偵察機關於實務上難以舉證；其二，無條文涵蓋日益常見的人頭帳戶等協力者。

修法前，《貪污、販毒與其他嚴重犯罪（沒收利益）法》第54條在雖已規範行為人不得隱匿、轉移、持有或使用來自犯罪所得之財產，構成要件為「明知或有合理理由相信」該財產與犯罪有關，然而實務上舉證此項主觀認知難度較高。對資金來源存在可疑跡象卻選擇不查證的收款人，或聲稱只是代收、轉帳而不知情者，檢方往往難以舉證其主觀知情程度，致使洗錢案無法入罪，成為法律打擊之盲區。

其次，舊法亦未有專屬條文處理那些未實際接觸資金，但卻提供帳戶、密碼予他人的犯罪者。例如帳戶出租人、讓他人操作自己網銀帳戶的人頭，或未查明對方身分與資金來源即協助完成資金轉移者，在缺乏專屬條文情況下，往往難以追訴。這類協力角色雖未實際參與詐騙過程，卻常是詐騙金流能順利運作的關鍵節點，若未加以法律規範，將致執法效果大打折扣。

3.5.2 修法內容與條文概述

一、增設「魯莽」與「過失」構成之洗錢罪（新增第54條第3A項）

修法新增第54條第3A項，納入非故意洗錢行為，針對「魯莽」與「過失」處理犯罪利益之行為課以刑責。其中，所謂「魯莽」，指在可預見風險之下，仍選擇不查證行為，屬於主觀上不顧後果的冒險行為；而「過失」指涉行為人未能履行合理注意義務，在法律上雖不具主觀故意，仍應負起刑事責任。

二、協助他人保留犯罪所得罪（新增第55A條）

2024年修法中新設條文，針對協助他人持有、操作、安排犯罪資金之行為進行入罪設計。不同於第54條規範實際持有或處理犯罪財產者，第55A條針對的是人頭帳戶提供者、代操作者、轉帳協助者等未實際接觸金流的協助者。

在客觀構成要件上包含了「協助安排」（第55A條第1項）例如：安排資金由他人控制、使用帳戶幫他人保留資金、以他人之利益進行財產投資等，及「執行可疑金流操作」（第55A條第2項），被告並負有對特定客觀事實要件的查證義務，包含以下情形：財產價值與收入來源顯不相稱；未合理查證對方身分或資金來源；未查用途即讓對方使用帳戶。當上述情形發生，舉證責任即發生轉移，被告必須證明自己採取了合理之查證步驟

3.5.3 實務案例、成果及展望

新加坡警方指出，該法施行後即有一名被告因收取1,000馬幣的報酬，允許他人使用其網路銀行帳戶，且未採取合理步驟查證用途，導致其帳戶被用於超過16萬新幣之洗錢犯罪。法院最終依據新法對「魯莽」處理犯罪利益的罪名，判處該被告6個月有期徒刑，並命其歸還不法所得。這個案例凸顯了新法核心精神：即便行為人聲稱對犯罪不知情，只要未能履行合理的注意義務，也將面臨刑事責任。

另於2024年新加坡警察部隊發動之25次全國性的打擊詐欺行動中，超過660名詐欺集團成員及提供人頭帳戶者遭起訴，其中110名即係依據新修訂的《貪污、販毒與其他嚴重犯罪（沒收利益）法》及《電腦濫用法》[33]，可見修法之成效。

33 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 11.

圖13、《貪腐、販毒與其他嚴重犯罪（沒收利益）法》內容與成效

資料來源：駐新加坡代表處繪製

3.6《防詐騙保障法》（2025年7月新法生效）

3.6.1 立法背景

自2018年至2024年間，新加坡詐騙案件數量增加逾六倍，從約6,234件增加至約51,500件，僅2024年度，詐騙財損金額即高達約11億新幣。

政府與銀行業合作實施一系列保護民眾之措施，包括「緊急止付」機制，允許客戶在懷疑其帳戶遭盜用時凍結帳戶，以及「資金鎖定」，讓客戶將一部分資金設定為無法通過網路方式轉出。

雖有上揭保護措施及反詐宣導，被害人自願轉帳給詐騙集團（自主轉帳）的案件仍然居高不下。2024年所有詐騙案件中，高達82.4%涉受害人自主轉帳，亦即歹徒並未直接控制被害人的帳戶，而是透過操控被害人來進行資金轉移。

其中有些案例，警方、銀行或家人已告知被害人其正遭詐騙，然被害人仍然執意轉帳，這些包括造成極高財損的投資及假冒政府官員類型詐騙，而警方之前並無權阻止堅持轉帳的被害人。

3.6.2 立法條文概述

一、限制令：

本法案目的在於保護正遭詐騙之目標群體，賦予警方權力向銀行發出限制令，倘

合理相信特定民眾將轉帳予詐騙歹徒，即可避免發生財損。

二、限制令核發流程：

（一）限制令核發由個別員警根據每個案件的事實及情況進行評估，例如民眾或其家人提供的相關事實來作出決定。

（二）員警可於下列情況向銀行發出限制令：

1. 合理相信特定民眾將轉帳予詐騙歹徒；以及

2. 限制令對保護特定民眾是必要之手段。限制令僅在其他說服選項無效後作為最後手段發出。

三、 限制令效力範圍：

（一）警方僅會對詐騙案件發出限制令，主要針對藉由數位或電信管道（如電話、簡訊或網路通話）進行的詐騙案件。傳統的真人詐騙（如支付不誠實的裝修承包商或家人、朋友）不在限制令效力範疇。

（二）被發出限制令的對象可預期以下銀行服務將受到限制：

1. 將資金從銀行帳戶轉出到其他賬戶（包括網路銀行App、現金電子支付及臨櫃）；

2. 自動提款機服務；

3. 所有信用服務（如信用卡交易、個人貸款服務）。

四、倘限制令發出，將直接適用於新加坡7家國內系統重要銀行34。若有合理懷疑民眾將從非國內系統重要銀行帳戶轉帳給詐騙歹徒，限制令也可發出給非國內系統重要銀行。

五、降低限制令造成的不便：將設立讓受限制令限制的對象可因合法理由（如日常生活開銷、支付帳單）申請使用其資金之機制，此類申請將採個案評估。

六、限制令效期：

（一）限制令最長效期為30日。若需更多時間以實施必要的干預措施，警方每次可延長最多30天，最多可延長五次。

（二）倘評估認為對象不再有被詐騙的風險，警方可在30日期限前撤銷限制令。

34 指對新加坡金融系統穩定性具有重大影響的銀行。包括新加坡本地銀行之星展銀行、華僑銀行、大華銀行，外商銀行之花旗銀行、馬來亞銀行、渣打銀行以及滙豐銀行。

七、訴願機制：對象可向警察總監對發出限制令的決定提出訴願。由於限制令在訴願審查期間仍將有效，內政部將確保訴願過程迅速進行；警察總監的決定將為最終裁定。

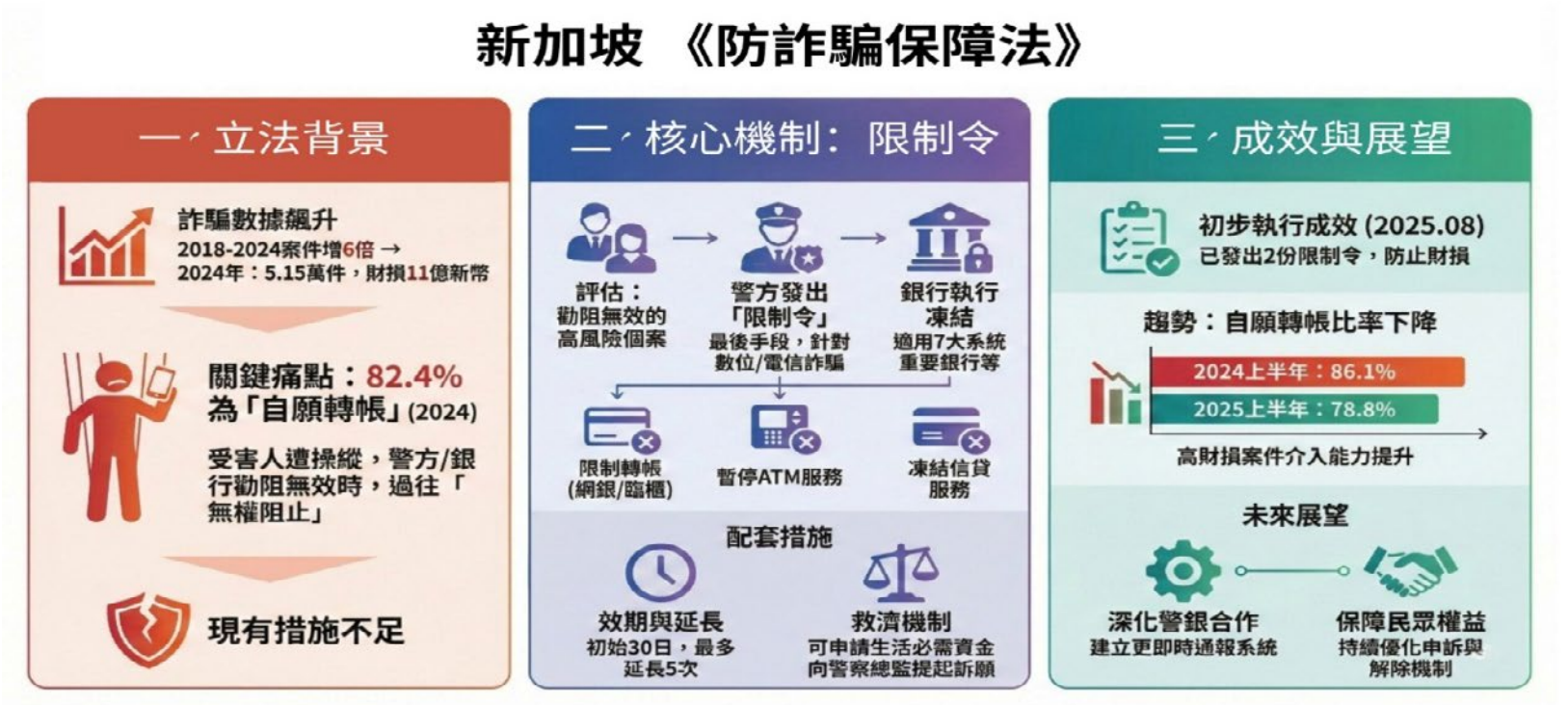
3.6.3 實際案例、成果及展望

隨著防詐騙保障法正式生效，警方將有明確法律依據在必要時主動介入，直接下令凍結可疑資金，特別是面對堅持轉帳的高風險受害人，將可有效降低財損案件。預期可顯著降低高金額自主轉帳詐騙案件，特別是投資詐騙及冒充政府官員詐騙案件的受害比率。

截至2025年8月20日，警方已對2位民眾發出限制令，限制其銀行交易，以防止詐騙損失；另一方面，從整體統計趨勢觀察，自願性轉帳在詐騙案件中的占比已出現下降跡象。2024年上半年與2025年上半年數據相較，自願性轉帳案件比率已自86.1%下降至約78.8%[35]。此數據顯示過往居高不下的被害人自願性轉帳現象已有趨緩，特別是在投資詐騙及假冒政府官員詐騙等高財損類型中，警方與銀行的介入能力正逐步提升。

此外，內政部表示未來將與金融業者進一步合作，以建立更即時的銀行間通報系統，加速應對詐騙資金流動。同時，為保障民眾權益，將持續優化限制令申請解除及申訴機制，確保符合比例原則與程序正義。

圖14、《防詐騙保障法》內容與成效



資料來源：駐新加坡代表處繪製

35 SPF, Mid-Year Scam and Cybercrime Brief 2025 (Singapore: SPF, 2025), p. 3 & p. 9

3.7《刑事法（雜項修正）法案》

3.7.1 立法背景

有鑑詐騙問題日益嚴重，新加坡民間前已有要求政府對詐騙犯施以鞭刑的呼聲，2025年3月，時任新加坡國會議員陳有明在國會發言正式建議政府修法，將詐騙相關犯罪納入鞭刑範疇，2025年10月14日，新加坡國會一讀通過對刑事法檢討修正之《刑事法（雜項修正）法案》，其中最引起討論的，即是正式將詐騙相關條文列入鞭刑，該法案於亦隨即於同年11月4日正式三讀通過。

3.7.2 修法概述

新加坡係國際間少數保有鞭刑刑罰之國家之一，適用於數十項嚴重罪行，根據嚴重程度，區分為強制鞭刑與酌情鞭刑二類，強制性鞭刑意即法律規定某些罪名一經定罪必須施以最低限度的鞭刑；典型例子包括持械或結夥搶劫、強姦、販毒（達特定數量）、非法放貸、蓄意破壞公共財產（塗鴉破壞等）等。酌情性鞭刑則係法官可根據案件嚴重程度決定是否加判鞭刑，例如嚴重傷害、敲詐勒索等罪行。

截至本次修法前，新加坡法律共明列161項罪名可附加鞭刑（其中65項強制、96項酌情）。修法檢討後，星國將161項罪名中的22項取消或降級，然最受社會與國際間矚目的，仍是首次納入鞭刑範疇的詐欺相關犯罪。

依照該法案，詐騙集團主謀、集團成員與招募者將為強制鞭刑，罪名成立後將施以最少6下、最多24下的鞭刑。至於協力者，例如上開《貪腐、販毒與其他嚴重犯罪（沒收利益）法》中的協助洗錢者、人頭帳戶提供者，或《電腦濫用法》、《雜項犯罪法》中以提供數位身分密碼或SIM卡之協力者，則為最高可施以12下的酌情鞭刑。

3.7.3 成效及展望

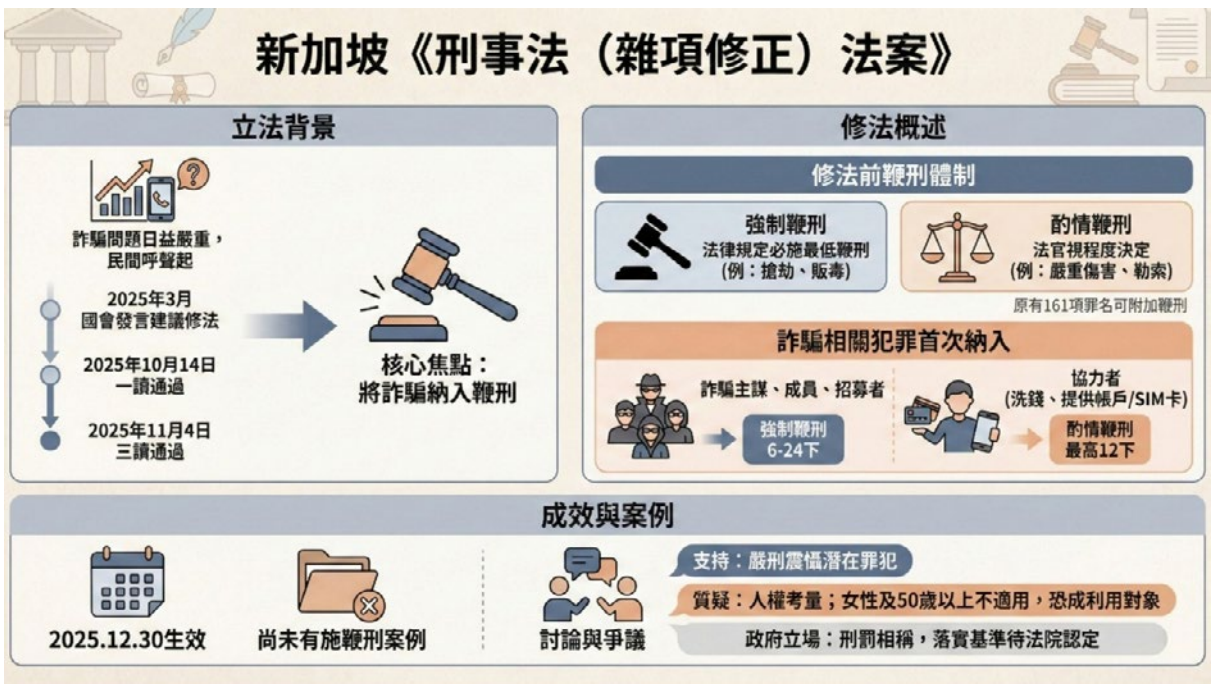
雖此法案自2025年12月30方正式生效，尚未有因詐騙犯罪遭施鞭刑之案例，惟被認為係基於治亂世用重典下的嚴厲刑罰，輿論支持者多認為得震懾潛在罪犯，而反對者則多自人權角度提出質疑，或認為詐騙相關鞭刑，仍不及於女性及50歲以上之行為人，此一族群恐成未來遭詐騙集團主要利用的對象等。

新加坡外交部暨內政部政務部長沈穎於國會答覆有關此次修法時強調，星國內政部係整體考量所有涉鞭刑的罪名，並評估與詐騙類似性質犯罪等多項因素，認為鞭刑係與詐騙犯罪相稱的刑罰，惟其落實之基準與比例原則仍有待法院認定[36]，尤其新加坡新加坡前開關於洗錢、數位身分及SIM卡犯罪都生效未久，甚麼情結下應施予鞭

36 https://www.mha.gov.sg/mediaroom/parliamentary/second-reading-of-the-criminal-law-miscellaneous-amendments-bill-wrap-up-speech

刑、如何鞭刑，均有待評估。

圖15、《刑事法（雜項修正）法案》內容與成效



資料來源：駐新加坡代表處繪製

3.8 小結：法制面向之綜整與成效

綜觀新加坡自2020年起至2025年間的法制改革工程，可發現其打詐策略從事後追懲轉而更強調事前預防與阻斷協力，並透過不同面向之法案與刑法修正，試圖提升法規範密度。填補傳統刑法在面對數位犯罪時的構成要件漏洞，更提升了執法機關介入的時效性與強制力。

3.8.1 立法策略核心

一、 金流監管與阻斷：透過《支付服務法》與《貪腐、販毒與其他嚴重犯罪（沒收利益）法》，將監管觸角延伸至加密貨幣與跨境支付，並降低洗錢罪的主觀犯意門檻，解決「車手」與「人頭帳戶」難以定罪的困境。

二、 數位工具與帳號源頭管理：利用《電腦濫用法》與《雜項犯罪法》，將出借數位個人身分與濫用SIM卡的行為直接入罪，從源頭切斷詐騙集團獲取犯罪工具的供應鏈。

三、 平台責任與強制介入：藉由《網路犯罪危害法》與《防詐騙保障法》，賦予政府直接命令平台移除內容的權力，以及在緊急時刻凍結受害者資金的強制力，解決境外平台叫不動與受害者勸不聽的實務難題。

四、 高強度威嚇：透過《刑事法（雜項修正）法案》，將鞭刑納入詐騙犯罪的刑罰選項，對犯罪集團核心與協力者形成強大的心理威嚇。

3.8.2 立法主要內容、預期成效與具體成果摘要

表9彙整了本節所述各項法案之核心規範與截至目前的具體執法成果：

表9、新加坡防詐法律體系綜整與成效表

法律名稱	核心規範內容	預期成效	具體成果與案例
支付服務法	納管加密貨幣與跨境匯款，強制業者落實反洗錢監測與資產隔離。	阻斷非法資金流動，防止支付機構淪為洗錢管道。	1. 2025年6月對5家大型支付機構開罰96萬新幣；另有多家機構因合規不足遭罰逾1,500萬新幣。 2. 30億新幣洗錢案中，無照經營加密貨幣者遭判刑。
電腦濫用法	將「明知或應合理知情」而交付數位個人身分之行為入罪。	遏止民眾隨意出借數位身分，減少人頭帳戶供給。	1. 成功依新法起訴交付數位個人身分供開戶者，判處8個月有期徒刑。 2. 配合CDSA修法，2024年共有110名相關協力者遭起訴。
網路犯罪危害法	賦予政府發布「指令」（如停止通訊、封鎖內容、下架App）的權力，要求平台移除詐騙資訊，。	快速清除網路詐騙廣告與假帳號，降低民眾接觸風險。	1. 2024年阻斷逾17萬組詐騙電話、網站與社群帳號。 2. 2025年向Meta發出實施指令，並與Google合作阻擋意圖側載的惡意App。
雜項犯罪法	將濫用SIM卡（非法註冊、轉讓、持有）列為刑事犯罪，並引入推定過失條款。	打擊黑市SIM卡供應鏈，使詐騙集團難以取得通訊工具。	2025年新法上路後，3月即查獲電信門市店員盜用個資註冊案；7月逮捕44名涉嫌偽冒註冊SIM卡者。
貪腐、販毒與其他嚴重犯罪法	增訂「魯莽」與「過失」洗錢罪，以及「協助他人保留犯罪所得罪」。	降低洗錢罪舉證門檻，即使聲稱「不知情」但未盡查證義務仍可定罪。	1. 2024年全國打詐行動起訴逾660人，其中110人係援引本法新增條款。 2. 有被告因「魯莽」借用帳戶遭判刑6個月。
防詐騙保障法	賦予警方發布「限制令」，可強制凍結堅持轉帳之潛在受害者帳戶最長30天。	針對「自願轉帳」案件進行強制止損，爭取冷靜期。	1. 截至2025年8月已對2名民眾發出限制令。 2. 自願性轉帳案件佔比從86.1%下降至約78.8%。
刑事法（雜項修正）	將詐騙主謀、成員（強制鞭刑）及協力者（情節鞭刑）納入鞭刑適用範圍。	對潛在犯罪者形成極高之心理嚇阻，展現國家嚴打決心。	法案於2025年11月通過，預期將對跨國詐騙集團成員及本地車手產生強大震懾效果。

第四章 新加坡打擊詐騙犯罪的措施：科技面向

4.1 ScamShield應用程式（2020年推出）

4.1.1 前言

新加坡政府早於2014年即因意識到詐騙犯罪的嚴重性而推出防詐資訊網站ScamAlert，由國家預防犯罪理事會與新加坡警察部隊共同營運，旨在為民眾提供有系統的詐騙類型資訊、案例警示與舉報管道，透過資訊公開以降低詐騙風險。

ScamAlert作為新加坡政府防詐策略數位化的第一次嘗試，其功能設計圍繞三個核心目標：一、公眾教育、二、警示提醒、三、案件通報。網站內容涵蓋超過20種常見詐騙手法的分類介紹與應對建議，例如：貸款詐騙、網戀詐騙、投資騙局、釣魚連結、冒充政府官員等；並有「受害者經歷分享」與「線上檢舉表單」，供民眾提供可疑訊息或號碼，由警方整合入情資系統作為研判參考。平台亦支援四種語言（英語、華語、馬來語、淡米爾語），提升資訊可及性，並設有1800-722-6688 與報警通道，為警方與民眾聯繫之橋樑。

然而，隨著詐騙犯罪技術提升與通訊平台的多元化發展，ScamAlert 難以回應詐騙犯罪帶來的挑戰。首先，ScamAlert屬於靜態平台，由使用者主動進入查詢，無法於詐騙發生時即時提出警示。其次，雖然設有線上舉報管道，但填寫流程不夠直覺，加上缺乏 App整合或行動通知功能，民眾多半將其視為資訊網站，而非實質的防詐工具。第三，當年尚未導入主動分析機制，詐騙資訊研判仍多依賴民眾回報，回應速度與精準度有限。

在此背景下，政府決定強化防詐科技部署，啟動了多項反詐騙科技工具與制度改革，開發主動攔截型數位工具ScamShield。該工具由國家預防犯罪理事會與政府科技局合作推出，為一款於自動過濾手機詐騙簡訊與來電之軟體。

隨著詐騙樣態快速演化、平台多元化，以及社會參與需求升高，ScamShield的功能也歷經數次更新與強化。以下將系統性回顧 ScamShield的誕生背景、初始設計目標與功能限制，分階段詳述其演進過程，直至2024年功能更完整之ScamShield「套裝版」推出，評估其對整體詐騙防治政策的影響與未竟挑戰。

4.1.2 ScamShield 的誕生

一、2018年起之詐騙趨勢變化

2018至2020年間新加坡的詐騙案件數與金額倍增，而以下三個現象是當時警方打擊詐騙遭遇之難題：

（一）詐騙訊息多冒用政府機構、銀行或物流商名義，透過SMS簡訊發送；

（二）詐騙來電多使用網路電話偽裝新加坡本地號碼，誤導性極強；

（三）民眾面對真假難辨的來電與訊息，無從分辨，且缺乏可靠快速的查證管道。

二、面對此一趨勢，新加坡政府推出ScamShield應用程式，旨在建立一個可自動識別與封鎖詐騙電話的機制，其設計初衷在於減輕警方與金融機構的調查與處理壓力，並預防民眾受騙，核心功能如下：

（一）自動過濾：透過AI建立簡訊過濾模型，自動識別詐騙簡訊，並加以分析；

（二）阻擋黑名單來電：該應用程式可在背景自動運作，封鎖來自已知詐騙號碼的來電與簡訊；

（三）資料回傳：ScamShield應用程式會自動將被過濾的詐騙簡訊和來電資訊匿名回傳給新加坡警察部隊。這些資料有助於警方分析詐騙趨勢，更新黑名單號碼，並提升詐騙偵測的準確性。

然而，初代的ScamShield功能有一定限制，如僅支援iOS裝置，Android用戶無法使用；其次，過濾模型無法處理Telegram、WhatsApp或Messenger等即時通訊軟體訊息；第三，雖提供使用者主動檢舉及回傳功能，但設定複雜，使用者介面不夠直覺等，且無法查詢特定號碼是否為詐騙電話。

至2022年推出Android版本前，ScamShield約有31萬5,000次下載量，封鎖逾580萬條詐騙簡訊及2萬9,000組門號，顯示出一定效用。2022年9月ScamShield推出Android 版本，終於將使用範圍擴大至所有智慧型手機使用者。

4.1.3 ScamShield 套裝版的誕生：2024年全面升級與轉型

2024年9月，國家預防犯罪理事會與政府科技局正式推出ScamShield套裝版，標誌該工具正式從一款工具型應用程式升級為多模組平台，整合查詢、識別、推播、通報、教育於一體之綜合型打詐平台。

一、新增四大核心模組

（一）ScamShield應用程式強化版：新增「主動查詢」與「主動舉報」功能，用戶可複製貼上訊息、電話號碼或網站，系統以AI分類協助比對來電及訊息之可疑程度，用戶亦可匿名通報可疑訊息及電話。

（二）將ScamShield. gov. sg網頁建構為全國性防詐資訊平台，內含熱點地圖、案例與查詢引擎。

（三）在Telegram與WhatsApp上建構ScamShield Alert頻道，定期推播新型詐騙手法並即時通報案例。

（四）ScamShield熱線（1799）：整合並縮短原先的報案熱線，全年無休電話服務中心，提供即時語音協助，供民眾在受騙疑慮下可電話詢問。

二、此次功能擴充重點在於「全民參與」、「資料回饋」、「跨平台互通」三大面向，改變過往僅靠警方與政府科技機關主導的模式。

4.1.4 結語

ScamShield作為新加坡政府針對詐騙問題的數位治理實驗，其從簡單工具演化為整合式公共服務平台的歷程，展現了政策從點狀部署到系統型整合的進程。

此一過程中亦可觀察出ScamShield漸次普及化並發揮效益，舉例而言，ScamShield於2021年上線前半年的下載量約11萬9, 000次，攔阻約72萬則疑似詐騙簡訊、5, 537組疑似詐騙號碼[37]。2022年底，因Android版上市，下載量迅速成長至近50萬次，累計通報詐騙簡訊逾740萬則、攔阻超過47, 000組門號[38]，均以倍數成長。

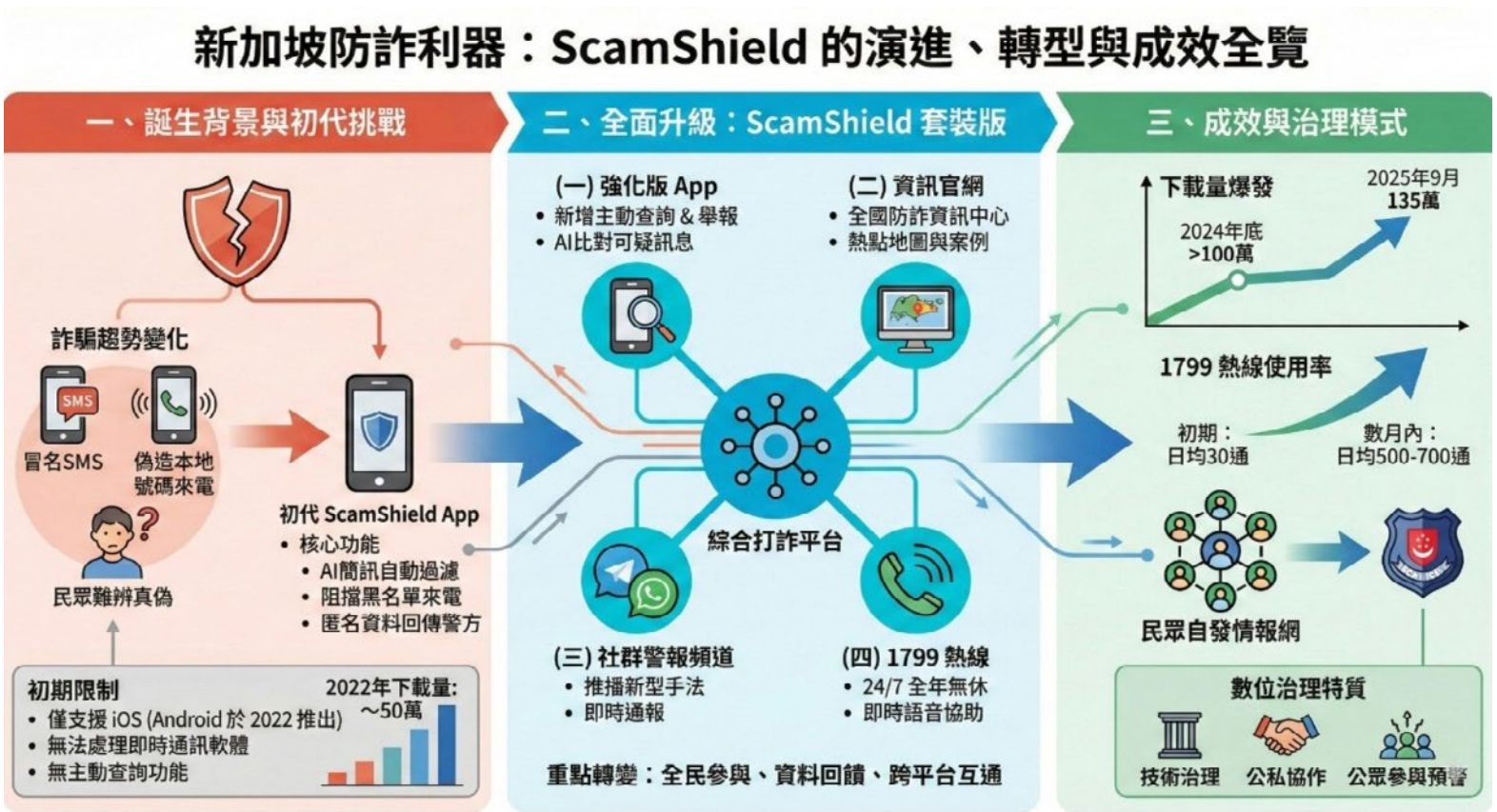
2024年ScamShield套裝版上市不久，同年底下載數累計突破百萬次，至2025年9月達135萬次。且因線上檢舉系統運作順暢，目前的ScamShield更像是民眾自發形成的情報網，發揮更大反詐功能[39]。

而搭配ScamShield套裝版推出之1799熱線，初期每日僅約30通求助來電，但因宣傳和知名度提高，在數月內日均來電量飆升至500至700通。截至2025年9月中旬，1799熱線已累計處理了超過12萬8, 000通電話和線上諮詢，防阻多起潛在的詐騙案件[40]。

ScamShield之發展過程中涵蓋多項治理特質：技術治理、公私協作、公眾參與與風險預警，系一防詐政策數位治理的實踐案例。ScamShield的演進歷程不僅回應了科技犯罪對制度韌性的挑戰，也為數位時代社會信任之重構提供了可供參照的範例。

37 https://mothership.sg/2021/05/scamshield-blocks-scams/
38 https://www.gasa.org/post/anti-scam-centre-of-the-singapore-police-force-fighting-scams-is-a-community-effort#:~:text=The%20results%20are%20impressive%3A%20Between,Scam%20Centre
39 https://cnalifestyle.channelnewsasia.com/women/scamshield-fighting-scams-singapore-470861
40 https://www.asiaone.com/singapore/scamshield-helpline-expands-ops-daily-calls-jump-30-700-last-year

圖16、新加坡防詐利器：ScamShield 的演進、轉型與成效全覽



資料來源：駐新加坡代表處繪製

4.2 詐騙分析及戰術性介入系統（2023年推出）

4.2.1 系統推出前的新加坡面對的打詐困境

在面對詐騙快速數位化與生成式 AI 大規模應用的壓力下，新加坡政府於2023年推出「詐騙分析及戰術性介入系統」（Scam Analytics and Tactical Intervention System，SATIS），作為一項融合人工智慧、即時介入與公私協力的政策工具。「詐騙分析及戰術性介入系統」的設計回應了過去反詐措施在偵測速度、平台整合與用戶行為介入等方面的侷限，也標誌著新加坡從事後補救走向預警的防詐治理轉型。

在「詐騙分析及戰術性介入系統」推出前，新加坡既有的防詐騙機制深受三大問題困擾：首先，是偵測能力落後於詐騙技術演進。詐騙網站與假帳號可在數小時內生成並傳播，然而警方仰賴民眾通報與人工研判，導致應對時間延遲、行動滯後。其次，資訊管道分散，尤其部分境外通訊軟體配合度低，即時刪除訊息與凍結帳號的能力因而受限。最後，詐騙手法由電話與簡訊轉為社交平台主導，並進一步結合生成式 AI 技術，利用深偽影片、假語音與圖像廣告操弄受害者的信任，傳統黑名單與靜態風險模型無法因應這些高度擬真的內容。

自2018年以來，新加坡詐騙案件不僅逐年攀升，透過社交平台或通訊軟體發生的詐騙亦佔多數，全球反詐騙聯盟報告顯示，全球有38%的詐騙案件涉及 AI 生成內容，

包含深偽語音與影像廣告等技術[41]。這些趨勢與執行挑戰，促使新加坡政府必須建立一套整合技術與制度的防詐系統，具備跨平台偵測與即時干預能力，從源頭阻斷詐騙行為的生成與傳播。

4.2.2「詐騙分析及戰術性介入系統」系統之核心功能

「詐騙分析及戰術性介入系統」作為新加坡首個引入人工智慧的反詐科技系統，由政府科技局與內政科技局共同開發。其核心機制為 遞迴式機器評分引擎，每日掃描逾十萬個網站，假陽性率低於千分之一，可靠性極高[42]。透過文字內容、網頁結構與關鍵字自動分類潛在詐騙風險，如屬高風險，「詐騙分析及戰術性介入系統」可即時通報警方，並透過與 Google網路風險檢測服務整合，使惡意網站在支援該應用程式介面介接的瀏覽器與應用程式中遭封鎖。雖然網路風險檢測服務由 Google 提供，但其封鎖效力不限於 Google自家產品（如 Chrome瀏覽器），只要第三方應用程式或安全防護系統串接網路風險檢測服務應用程式介面，例如火狐瀏覽器、Safari瀏覽器 或企業防火牆系統，也能即時獲得該惡意網址的風險回應與封鎖指令。

「詐騙分析及戰術性介入系統」亦被納入反詐騙指揮處[43]的標準作業程序，並整合進反詐騙指揮處與META、蝦皮、旋轉拍賣等合作平台，以協助識別可疑網站與帳號。平台方依據通報結果執行內容審查與移除，縮短處置時間，平台技術人員並進駐反詐騙指揮處與警方在特定聯合行動中曾緊密協作。整體而言，「詐騙分析及戰術性介入系統」成為跨部門協作平台中的重要機制，角色更為重要，此部分將於本報告第五章公私協力部分詳加描述。

4.2.3 成果與未來展望

「詐騙分析及戰術性介入系統」是新加坡反詐體系中結合AI技術、公私協力與制度化作業的一體化架構，試圖解決偵測時效與數據通報的瓶頸，也成為打詐治理體系不可缺的一部分。統計2024年，共封鎖44, 900個詐騙網站與40, 500個WhatsApp號碼，較2023年封鎖25, 000個網站及29, 200個WhatsApp號碼，分別有79%及38%之成長[44]。此外，透過「詐騙分析及戰術性介入系統」系統，也促進反詐騙指揮處與平台業者之公私協力及處置效率，使協力業者得以更迅速接收「詐騙分析及戰術性介入系統」分析結果並採取行動。

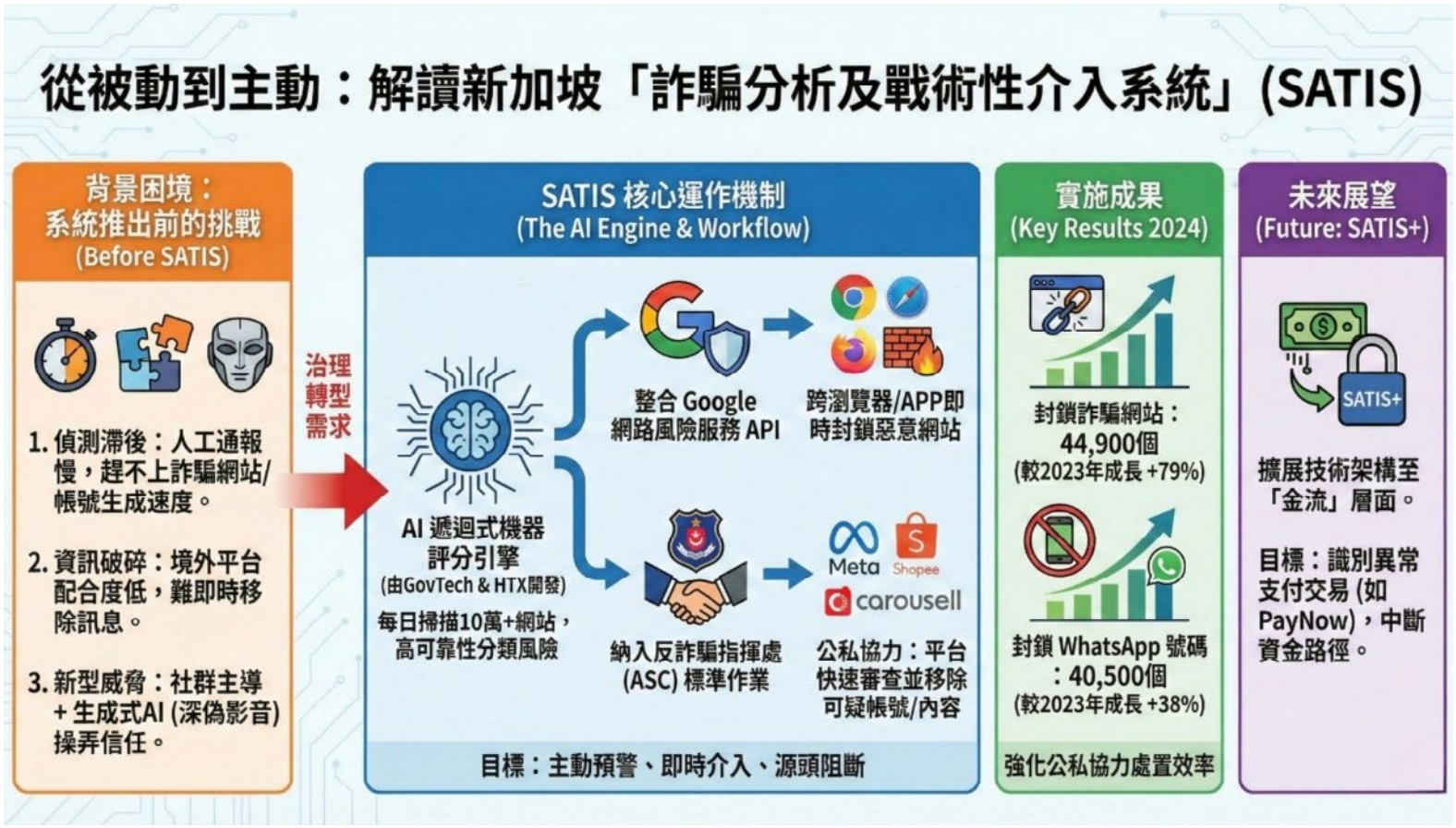
在目前「詐騙分析及戰術性介入系統」基礎下，新加坡政府力求持續擴展反詐科

41 Global Anti-Scam Alliance (GASA) in collaboration with Feedzai, The State of Scams in Singapore 2024 (Singapore: GASA, 2024), p. 6.
42 https://www.tech.gov.sg/products-and-services/for-citizens/scam-prevention
43 反詐騙指揮處(ASCom)即原反詐騙中心(ASC)，係2022年改制升格。
44 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 12.

技領域之技術架構。新計畫命名為「詐騙分析及戰術性介入系統+」，功能預計將拓展至處理與詐騙活動相關的支付管道，以期識別並中斷金流路徑。儘管該系統仍正開發中，未來若能應用於如 PayNow即時轉帳服務[45]或其他數位支付的異常交易偵測，有望補足現行「詐騙分析及戰術性介入系統」在阻斷金流層面應用的限制。

整體而言，儘管在打詐科技面上仍有如Telegram 與境外詐騙管道仍等難題，但就現階段成果而言，應可認為「詐騙分析及戰術性介入系統」已發揮應有之功能。

圖17、解讀「詐騙分析及戰術性介入系統」



資料來源：駐新加坡代表處繪製

4.3 小結：科技防詐之策略轉型與具體成效

綜觀新加坡自 2020 年至 2024 年的科技反詐進程，可發現其治理思維出現了重大轉折：從早期被動的「資訊公告（ScamAlert）」，轉型為利用人工智慧與自動化技術進行「主動偵測」與「即時阻斷」。並由「用戶端防護（ScamShield）」與「系統端偵測（SATIS）」組成落實，不僅強化了政府對詐騙的反應速度，更將防線推前至詐騙接觸到受害者之前。

一、新加坡科技反詐主要做法與預期成效

新加坡的科技反詐策略旨在解決傳統執法人力有限的挑戰，其具體做法與預期成效如下：

45 新加坡於 2017 年推出的即時轉帳服務，直接與使用者金融帳戶連結，只要使用手機號碼、身分證字號或者掃描QR code等方式，即可於用戶間即時轉帳或付款。

（一）用戶端：透過ScamShield套裝版係政府予民眾自動過濾簡訊與封鎖來電的護盾，該軟體在歷次更新中提升了回報機制，即時更新黑名單，並結合1799熱線提供全天候的諮詢服務，解決民眾「求助無門」的恐慌。

（二）系統端：透過「詐騙分析及戰術性介入系統」，政府利用AI每日自動掃描逾10萬個網站，識別釣魚連結與假冒平台，在詐騙網站大規模傳播前實現源頭阻斷，此外，透過與科技公司的合作機制，自瀏覽器端直接封鎖，並自動通報社群平台下架內容，大幅縮短從發現到處置的時間差。

二、具體成果與數據

根據 2024 年至 2025 年的最新數據，這套科技體系攔阻效果如次：

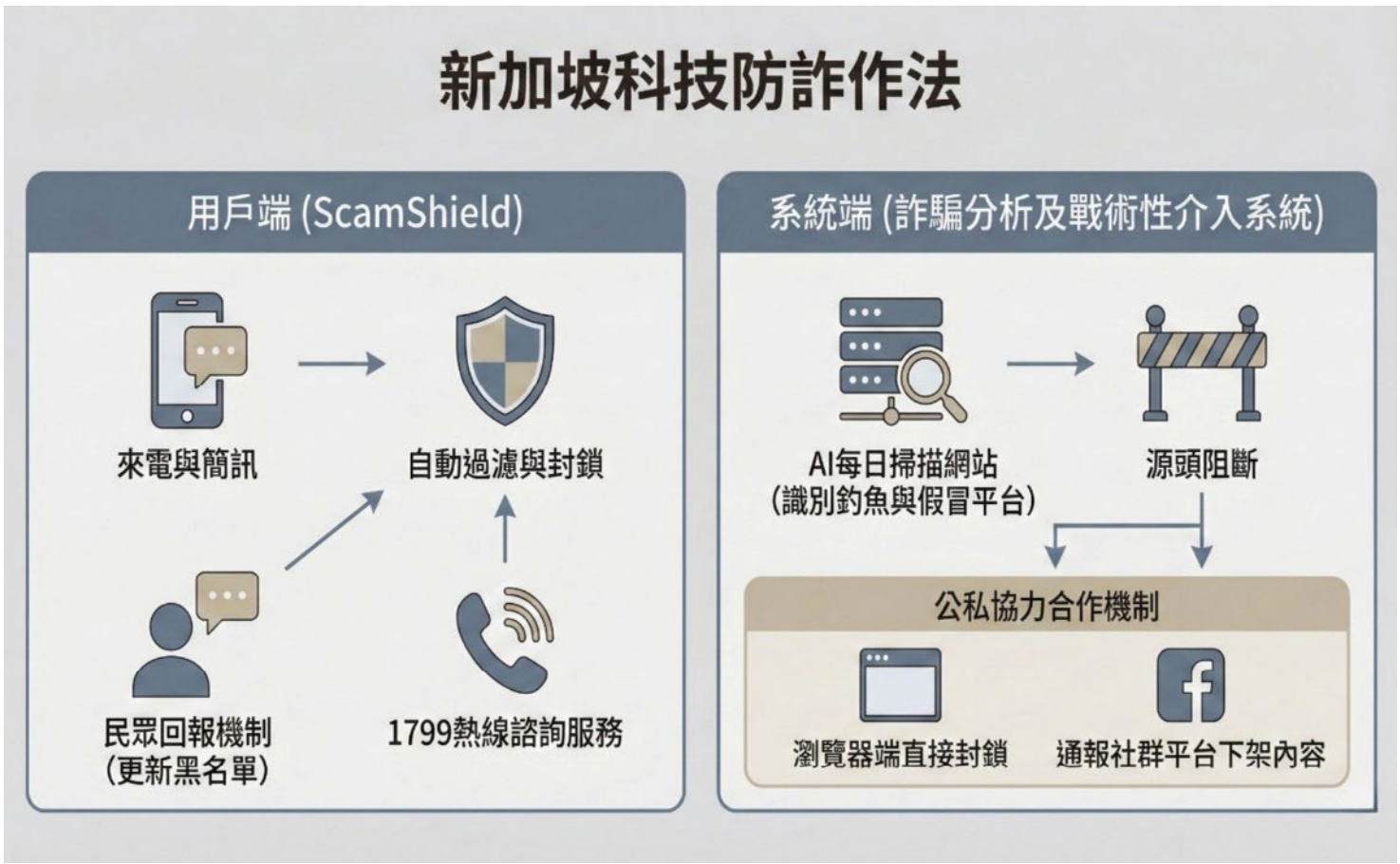
（一）公眾覆蓋率與參與度提升：ScamShield的下載量從2021年初期的11.9萬次，增加至2025年9月的135萬次。隨著功能完善，民眾的主動參與度亦提高，1799熱線的日均來電量從初期的30通提高至500通，此等科技工具已成功建立民眾的信賴感與使用習慣。

（二）攔阻效能倍數成長：在AI輔助下，「詐騙分析及戰術性介入系統」攔阻效率亦向上成長。2024年共封鎖44,900個詐騙網站與40,500個WhatsApp帳號，相較於2023年分別成長了79%與38%。

三、綜合評估

透過ScamShield與「詐騙分析及戰術性介入系統」，新加坡構建動態的數位防禦生態系。然而，科技工具僅是手段，要將這些攔阻資訊轉化為更強大的打擊力量，仍需仰賴下一章所述的「公私協力」機制，將科技偵測到的情資，迅速轉化為銀行凍結與平台下架的實際行動。

圖18、科技防詐之策略轉型與具體成效



資料來源：駐新加坡代表處繪製

第五章 新加坡打擊詐騙犯罪的措施：公私協力

隨著數位經濟的迅速發展與全民網路滲透率的提升，新加坡社會面臨日益嚴峻的詐騙威脅。從網路釣魚、假投資平台、社群假帳號、冒充公務員至跨境洗錢詐騙，新型態詐騙層出不窮，受害者遍及各年齡層與社會階層。顯示詐騙已非單一刑事問題，而是一項跨部門、跨產業、跨社群的綜合治理挑戰。

面對詐騙的高度科技化與組織化，新加坡政府深知僅憑警察單一力量難以全面防堵。因此，新加坡的反詐政策強調政府與民間機構共同承擔風險防控的責任，將警政、金融、科技、通訊與社區組織等不同領域的關鍵群體整合為防詐網絡。

2019年新加坡警察部隊於商業事務局下成立反詐騙中心46，以作為政府部門與私部門合作應變的樞紐平台。此中心能快速處理通報案件、凍結可疑帳戶、分析詐騙趨勢，並連接銀行、電信與網路平台業者共同打擊詐欺金流與網路詐術。

銀行業在新加坡反詐體系中亦扮演重要角色。不僅主動升級防詐驗證機制，更與警方簽署通報協議，實施高風險交易延遲處理及用戶警示機制，減少即時轉帳損失。這類措施充分體現金融機構作為把關資金流動最後一道防線的角色。

社群媒體與科技平台同樣是防詐合作的重要環節。新加坡政府要求META、蝦皮及旋轉拍賣等大型平台與警方配合，設立快速下架通報機制，防堵假訊息與假廣告流傳；同時也推動平台加強用戶實名認證與詐騙內容識別功能，冀使科技平台成為反詐之共同防線。

最後，新加坡政府也同時強化社區防詐意識，「社區警政」制度由社區聯絡警員定期與居民、學校、宗教團體等舉辦反詐宣導活動，同時透過如前章介紹之ScamShield應用程式等工具強化全民識詐能力。以這類公眾參與的基層機制，延伸風險預警，也望強化社會韌性。

綜合上述，新加坡以「公私協力」為核心精神，試圖形塑出一套跨部門且持續演進的反詐策略。以下將以成立反詐中心、銀行合作、社群平台管理與社區合作等四個面向，進一步詳述新加坡的反詐具體作法與成效。

5.1 成立反詐騙中心

5.1.1 成立背景：面對跨境數位詐騙的挑戰

46 反詐騙中心(ASC)後於2022年改制升格為反詐騙指揮處(ASCom)

2010年代後期，新加坡社會加速邁入數位化，伴隨網路支付、數位銀行與社群媒體廣泛普及，詐騙犯罪逐年攀升。根據新加坡警察部隊統計，自2017年起詐騙案件已顯著增加，由2017年的5,147件成長至2018年的6,234件，再至2019年已達9,545件，年增率分別為21%與53%。而詐騙損失金額亦從2017年的新幣1.27億元，增至2018年的1.51億元，呈現明顯上升趨勢。

詐騙手法快速進化，涵蓋假網購平台、社群釣魚連結、投資詐騙、冒充政府機關與跨境洗錢等，手段更具組織性與跨境性，令傳統調查模式與資金追回機制難以即時應對。

在此背景下，新加坡內政部與警察部隊意識到，僅依賴單一執法機構難以全面防堵詐騙風險。因此，於2019年6月正式成立反詐騙中心，並於2022年3月22日進一步升格成立反詐騙指揮處，將反詐騙中心結合七個地區警署之詐騙打擊小組，打造全國性、即時性、高密度反詐協調平台。目標在於整合全政府與民間資源，建立一套高效率、科技導向的跨部門反詐協調機制，提升對詐騙資金流與行動的即時偵測與應對能力，並以打造新加坡為「無詐騙之地」為願景。

5.1.2 策略架構及核心功能

新加坡反詐騙中心以五個英文字首組成之「SCAMS」（詐騙）作為打擊詐騙的策略架構，強調將以「詐騙」對抗詐騙，其五個英文字分別代表意義如下：

一、資訊感知（Sense-making）：運用數據分析與情資研判掌握詐騙趨勢。

二、跨部門合作（Collaboration）：整合銀行、電信、科技業、政府部門與海外執法單位。

三、社會意識（Awareness）：透過全國宣導與APP工具提升全民識詐能力。

四、降低損害（Mitigation）：快速凍結資金、終止廣告與通訊管道，降低損害。

五、快速執法（Swift Enforcement）：透過警方之反詐騙小組與跨境執法合作加強打擊與逮捕效率。

此外，反詐騙中心運作方式可歸納為六個「I」之六大核心功能，用以阻斷詐騙集團運作及減少被害人金錢損失

一、資訊管理（Information Management）

反詐騙中心運用科技，追蹤全國詐騙趨勢並分析每日大量的犯罪資料，識別詐騙活動中所使用之電話號碼、WhatsApp帳號及網路帳號，藉此破壞詐騙分子之運作。

二、即時介入（Intervention）

反詐騙中心與來自公私部門的利害關係人攜手合作，打擊詐騙。透過「資金追回行動小組」，反詐騙中心與超過80家機構合作，包括金融機構、金融科技公司、電信商與網路電商，藉此縮短凍結詐騙帳戶的處理時間，並加速追回轉入詐騙者手中的資金。新加坡警察部隊在與新加坡金融管理局合作上，將星展銀行、華僑銀行、大華銀行、渣打銀行、匯豐銀行、聯昌國際及GXS等七家大型銀行的員工共同進駐反詐騙中心，強化即時凍結帳戶與追查資金流向的能力。

根據官方統計資料，2024年警方共凍結超過21,000個銀行帳戶，並成功回收逾1.82億新幣之詐騙財產損失[47]；相較之下，2023年約凍結20,000個銀行帳戶，追回約1億新幣受害款項[48]。相關數據顯示，銀行人員實質進駐反詐騙中心並與執法機關即時合作，已對資金攔阻與回收產生實質成效。

此外，反詐騙中心亦與電信業者與網路電商密切合作，終止涉詐手機門號、舉報WhatsApp帳號，以及下架可疑的網路帳號與廣告。

三、調查（Investigation）

快速對接各地區警察機關進行線索分析與拘捕行動。反詐騙中心積極針對詐騙嫌犯與車手展開執法行動。車手的犯罪樣態包括協助詐騙集團轉帳、出借銀行帳戶，或提供數位個人身分、開立人頭帳戶或申請人頭門號等。

四、創新（Innovation）

反詐騙中心積極利用科技打擊網路詐騙。例如與政府機關「政府公開產品」部門合作推出「ScamShield」App，該應用程式分別於2020年11月與2022年9月推出iOS與Android版本。ScamShield可透過機器學習與演算法辨識並過濾詐騙簡訊，也能封鎖曾涉詐騙的電話號碼。

ScamShield於2021年上線前半年的下載量約11萬9,000次，攔阻約72萬則疑似詐騙簡訊、5,537組疑似詐騙號碼；2022年底，下載量迅速成長至近50萬次，累計通報詐騙簡訊逾740萬則、攔阻超過47,000組門號；2023年則成功封鎖3.9億通疑似詐騙電話[49]。

2024年ScamShield套裝版上市不久，在年中的下載次數已達95萬次，同年底下載人次更超過118萬次，同年與電信監管部門合作，成功封鎖了約1.17億通電話及5,000萬則簡訊。

47 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 12
48 SPF, Annual Scams and Cybercrime Brief 2023 (Singapore: SPF, 2024), p. 31
49 “Whole of Government Efforts,” Scamshield, accessed 10 Aug. 2025, https://www.scamshield.gov.sg/whole-of-government-effort/

五、公眾教育（Inculcation）

提升民眾識詐能力是最有效的防詐策略，新加坡警察部隊自2023年起推動全國反詐倡議「我可以對抗詐騙」（I Can ACT Against Scams），號召全民採取行動，保護自己與親友。該行動分為三步驟「A. C. T」：A – Add（強化安全）：加裝ScamShield應用程式，設立網路銀行交易限額，啟用個人帳戶的雙重認證。C – Check（查證資訊）：保持警覺，留意詐騙跡象，確認交易平台與對象是否真實可信。T – Tell（主動通報）：向警方與相關機構通報詐騙經歷，通報越快，可減少他人受害風險；同時與親友分享詐騙手法，共設立社會防線。此外，民眾亦可透過ScamShield網站（www. scamshield. gov. sg） 或撥打1799熱線查詢詐騙資訊。

六、國際合作（International Cooperation）

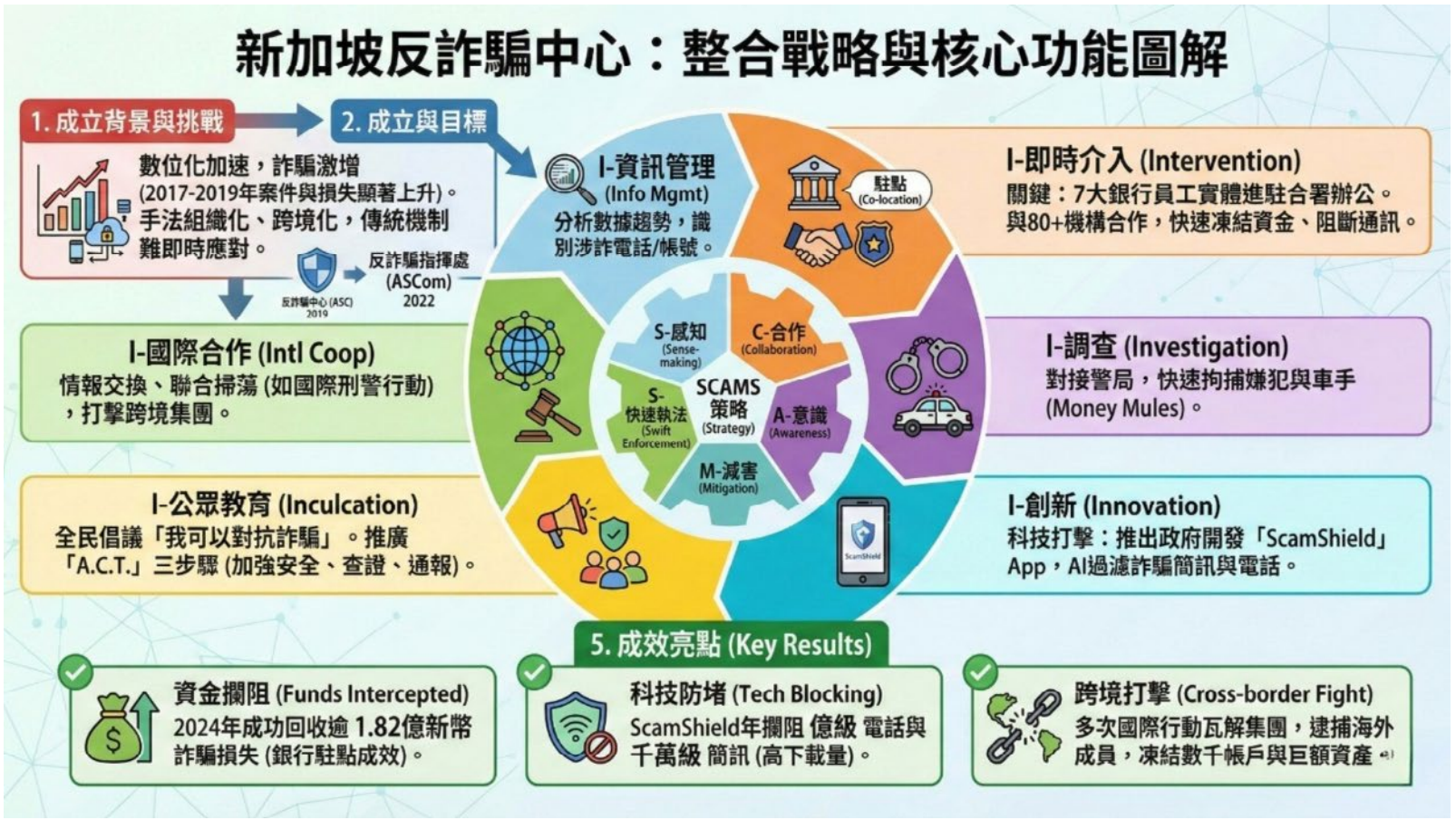
新加坡的詐騙案件多源自境外，警察部隊持續與外國執法單位進行合作，包括情報交換、聯合調查與同步掃蕩行動。在2022年，與海外執法機關的緊密合作成功瓦解13個詐騙集團，其中包括6個求職詐騙集團、3個假冒政府官員詐騙集團、2個釣魚詐騙集團及2個網戀詐騙集團。共有超過70名海外成員遭到逮捕，涉及超過280起案件。

2023年，新加坡警方參與國際刑警組織「曙光行動」，該行動共有超過76個國家共同合作。新加坡警方調查超過2, 000人，並在本地凍結超過5, 300個銀行帳戶，成功追回逾1, 150萬新元。此外，反詐指揮處亦查扣總值超過3, 000萬新元之虛擬資產。同年之「HAECHI行動」計有32個國家參與，星方總計調查超過800名涉嫌詐騙及洗錢成員；並在新加坡封鎖逾4, 900個銀行帳戶，並查扣超過1, 640萬新元。另一方面，亦封鎖超過300個虛擬帳戶，並由反詐指揮處扣押超過50萬新元之虛擬資產。

2024年，與來西亞皇家警察等海外執法機關的緊密合作下，成功瓦解16個跨國詐騙集團，共150多名海外成員被捕，總計涉及2, 300多起跨國詐騙案件，受害金額逾5, 800萬新元。此外，星國警方亦參與了國際刑警組織的「HAECHIV行動」，調查超過1, 600名涉案人士，凍結逾5, 100個銀行帳戶，扣押資金逾5, 480萬新元；另封鎖1, 000多個加密貨幣帳戶，查扣加密貨幣資產約79. 8萬新元[50]。

50 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p. 13

圖19、新加坡反詐騙中心：整合戰略與功能圖解



資料來源：駐新加坡代表處繪製

5.2 銀行

在打擊日益嚴重的網路詐騙問題上，新加坡政府積極推動「公私協力」模式，特別是在銀行業領域，透過金融機構的直接參與，強化全民防詐網路的安全防護。以下是具體的政策與措施：

5.2.1 淘汰一次性簡訊密碼驗證，全面推動數位認證

一、背景：釣魚詐騙的嚴重威脅

根據新加坡警察部隊統計，2023年僅網路釣魚詐騙即造成至少新幣1,420萬元（約合新台幣3.43億元）財損，顯示該類詐騙手法對民眾財產安全威脅極大。新加坡金融管理局為保護民眾避免遭網路釣魚而受騙上當，於2023年7月開始要求各消費金融銀行逐步淘汰一次性簡訊密碼驗證作為高風險交易的唯一認證方法，以對此類詐騙手法進行系統性防堵。

二、措施內容

金融管理局及銀行公會於2024年7月9日共同發布公告表示，新加坡的主要消費金

融銀行（包括星展銀行、華僑銀行及大華銀行等，另新加坡花旗銀行則早於2023年已淘汰一次性簡訊密碼），將於未來逐步讓已使用數位認證的用戶停止使用一次性簡訊密碼登錄網路銀行帳戶，而須透過瀏覽器或手機應用程式發送之數位認證登錄。此方式可直接檢核民眾的登錄身分，而不需輸入一次性密碼。

三、 成效展望

傳統的一次性簡訊密碼較易透過手機間諜軟體或社交工程方式遭詐騙集團攔截取得，再加上現代的社交工程手法已更加精進與複雜，如建立與真實網站非常相似的假銀行網站，讓民眾落入網路釣魚的陷阱、在不自覺的情形下遭歹徒獲取一次性簡訊密碼。致一次性簡訊密碼未能達防範網路釣魚攻擊之理想效果，為改善此情形，金融管理局盼透過最新的數位認證措施強化民眾登錄網路銀行的安全防護，在民眾未親自透過以手機或平板等裝置授權下，詐騙者更難登入其網銀。

此外，新加坡各大銀行也加強了銀行應用程式的反惡意軟體功能，當手機或平板裝置被偵測到存在惡意程式時，系統將禁止該裝置登入網銀，形成第二道防線，進一步降低受害風險。這種主動偵測與封鎖的設計，不僅提升了用戶端的防護層級，也反映出新加坡打詐政策中由產業界主動承擔技術防詐責任」的治理理念。

5.2.2 以「共同責任架構」追究金融機構與電信業者在釣魚詐騙案件之責任

一、背景

由於近期新加坡釣魚詐騙案件層出不窮，新加坡政府於2024年12月16日起實施「共同責任架構」，倘發現金融機構及電信業者失責，須對詐騙案件共同承擔責任，賠償受害者損失；消費者自身亦須隨時保持警惕，不點擊任何未經請求的可疑連結。因詐騙類型繁多，考量銀行及電信業者相關措施的防詐能力有其限制，該架構並未涵蓋所有詐騙案，例如投資、愛情交友及惡意軟體詐騙案等。

二、究責方式

「共同責任架構」依據「瀑布模式」追究責任：發生釣魚詐騙案件時，銀行須負起第一層把關責任，倘發現未採取適當措施，即須賠償受害者損失。若確認銀行履行所有責任，繼而審查第二層把關的電信業者，倘發現失責即須賠償。若銀行及電信業者均未失責，則應由消費者承擔損失。倘消費者對調查結果不滿，可向「金融業爭議調解中心」提出申訴。

三、業者相關責任及消費者申請賠償流程

（一）金融機構：

1. 確保消費者啟用密碼生成器須至少12個小時才能生效；
2. 啟用密碼生成器及出現高風險交易須通知消費者；
3. 提供全天候管道及自助功能讓消費者可立即阻止線上轉帳交易；
4. 必須實施即時詐騙監控，當消費者帳戶被迅速提走大量資金時，必須封鎖或凍結該筆交易（含之後的交易）至少24小時。

（二）電信業者：

1. 確保僅獲授權之供應商能發送顯示發送者身分的簡訊；
2. 阻斷來自未取得授權供應商的簡訊；
3. 實施反詐騙過濾，阻斷含有釣魚連結的簡訊。

（三）消費者申請賠償流程：

1. 申請賠償階段：被害人報警並向負有責任的金融機構申請賠償，該金融機構將評估賠償案件是否屬共同責任架構範圍，並在適用前揭架構的情況下，通知負有責任的電信公司；另帳戶持有人應儘快向負有責任的金融機構報告任何未經授權的交易活動，不得超過在察覺交易似已獲授權的30日。
2. 調查階段：負有責任的金融機構及負有責任的電信公司應依據按照前開指南之相關規定進行調查。
3. 結果階段：負有責任的金融機構將調查結果通知帳戶持有人。
4. 申訴階段：若帳戶持有人對結果不滿意，可另透過諸如「金融業爭議調解中心」或「資訊、通訊及媒體發展管理局」等途徑進行申訴。

四、成效

「共同責任架構」的推行，強化金融機構與電信業者的法律責任與防詐義務，也有效推動業者升級其詐騙攔阻技術與客戶安全通知機制。自制度實施以來，新加坡各大銀行相繼調整其數位安全機制，例如各大銀行從2025年10月15日起，針對餘額至少5萬新幣的儲蓄或聯名帳戶，實施「24小時轉帳冷靜期」。一旦單筆或24小時內累計轉帳金額超過帳戶餘額的50%，該筆交易將被自動延遲24小時或拒絕，以給予可能受騙的客戶緩衝思考時間。這些措施已逐步出現成效，僅2025年首七個月，各大銀行安全措施便成功阻止了7,800萬新幣的詐騙財損[51]。

再者，新加坡政府為所有政府機構統一採用單一的簡訊識別ID「gov.sg」，取代

51 “拥至少5万元储蓄或联名账户 本月15日起线上转移银行户头逾半金额自动延后24小时,” Zaobao, 4 Oct. 2025, https://www.zaobao.com.sg/news/singapore/story20251003-7611981

大多數原本各別機關自行使用的ID。此舉在於協助民眾更容易辨識真正的政府簡訊，並防範冒充政府官員的詐騙，電信商亦需阻擋任何假冒的類似字樣。該政策自2024年7月1日上路至2025年6月，透過「gov. sg」ID發送之簡訊達1. 81億則，其中並未發現任何詐騙簡訊，使用「gov. sg」的機關已增加至66, 140個，達93%的民眾能辨識「gov. sg」為官方簡訊，並獲得民眾84. 3%的正向滿意度評分[52]。

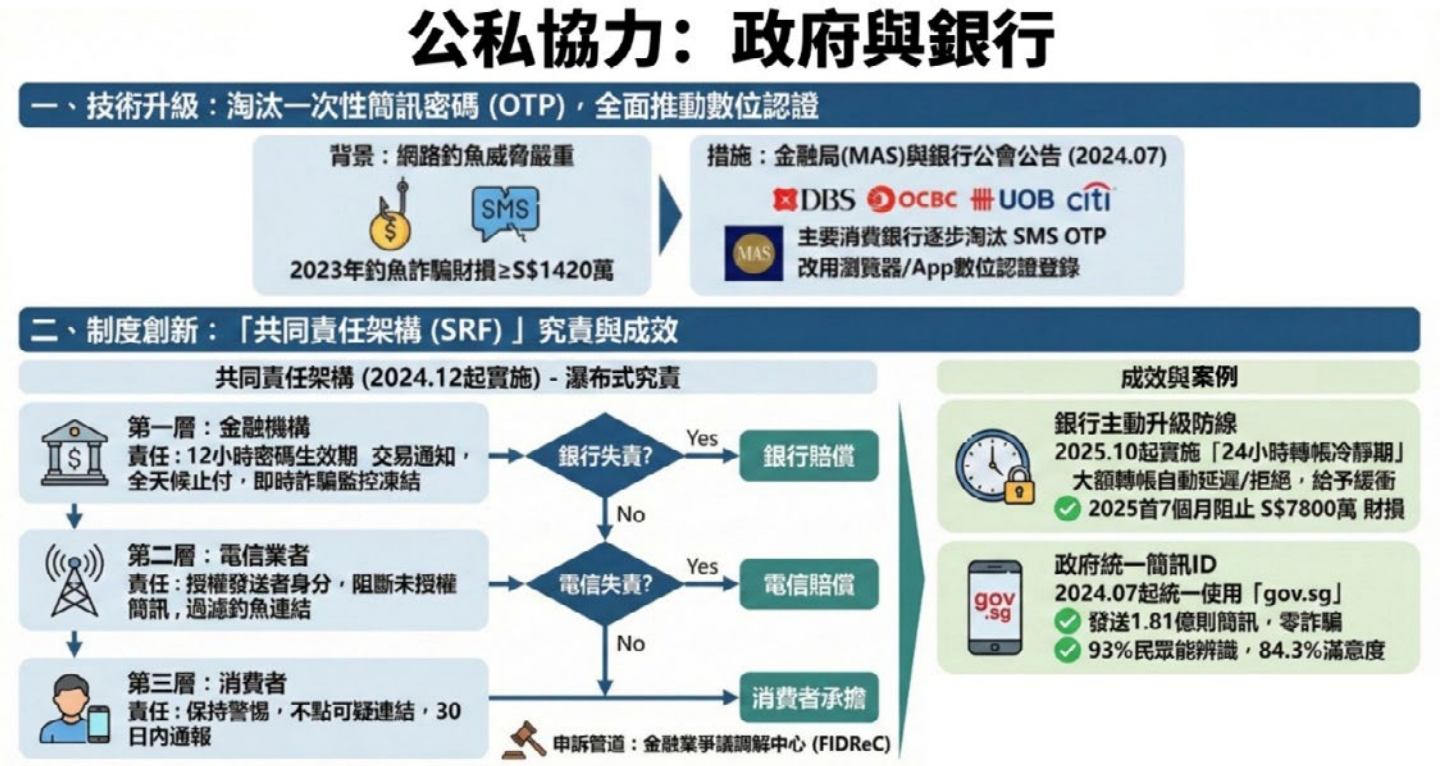
五、結語

「共同責任架構」在於承認詐騙防制並非單一機構的責任，而應由上下游共負。透過「瀑布式責任追究機制」，新加坡政府將「資訊基礎設施提供者」（銀行與電信業者）納入法律義務者，使其在日常業務中主動升級防詐機制，並提升對潛在詐騙風險的應變能力，最新的「24小時冷靜期」措施便是金融業強化自身防線的具體展現。

此一制度亦不忽略消費者的責任，強調用戶在面對詐騙連結、可疑簡訊時的基本警覺與通報義務。值得注意的是，新制度排除某些詐騙型態如投資詐騙、戀愛詐騙及惡意程式詐騙，未來是否擴大涵蓋範圍仍需審慎觀察與政策評估。

整體而言，「共同責任架構」已成為全球數位金融治理中的重要參考案例，創新性地導入跨產業連帶責任機制，也提供平衡使用者權益與產業營運風險的新型框架，未來或可推廣至更多類型詐騙情境，成為打擊數位金融詐欺之重要策略。

圖20、銀行在反詐騙活動的課責與成效



資料來源：駐新加坡代表處繪製

52 SPF, Mid-Year Scam and Cybercrime Brief 2025 (Singapore: SPF, 2025), p. 35

5.3「星空智速反詐」計畫

一、前言

面對日益嚴峻的跨境詐騙威脅，新加坡警察部隊致力從「事後打擊」轉向「事前預警」與「即時阻斷」，以降低民眾財產損失與強化整體反詐防線。在此思維下，反詐騙指揮處[53]於實務推展上導入科技輔助與主動介入概念，啟動「星空智速反詐」（Automation of Scam-fighting Tactics & Reaching Out，A.S.T.R.O.）計畫。該專案透過與新加坡三大銀行（大華銀行、華僑銀行及星展銀行）合作、導入「機器人流程自動化」與大規模簡訊通報機制，對可疑轉帳進行即時干預，迅速提醒潛在受害者，成為新加坡落實「以民為本、科技為輔」反詐政策的重要典範。

二、運作模式

「星空智速反詐」（A.S.T.R.O.）計畫係一項以主動預警與即時介入為核心的反詐騙協作機制，由新加坡警方反詐騙指揮體系與多家金融機構共同推動。其運作重點不在於個案事後偵辦，而是透過跨機構協作與科技輔助，於詐騙行為發展初期即介入提醒，降低後續財務損失風險。

在整體架構上，警方與合作銀行依既有法制與合作框架，針對可疑金流或異常交易行為進行風險辨識與研判。當系統偵測到可能涉及詐騙風險之交易型態時，警方與銀行即透過自動化工具與既定通報流程，啟動以被害人為核心的預警機制。

其中，大量簡訊警示（SMS　alerts）為對外可見且最具代表性的介入手段。警方會向可能面臨詐騙風險的帳戶使用人發送官方警示簡訊，提醒其注意可疑交易，並建議立即停止進一步金錢移轉、主動向銀行或警方查證。許多民眾正是在接獲此類簡訊後，才即時察覺異常並中止交易行為。

此一模式透過科技自動化、跨部門資訊協調與規模化通報，形成可重複運作的防護循環，使反詐騙工作由傳統的「事後追查」轉為「事前阻斷」，有效強化整體金融安全與民眾防詐韌性。

三、成效及展望

（一）階段性成果

1. 2023年透過六次聯合行動，共發送超過68,000則簡訊，提醒超過28,500名被害人，成功避免超過1.48億新幣的潛在損失[54]。

53　反詐騙指揮處(ASCom)即原反詐騙中心(ASC)，係2022年改制升格。
54　SPF, Annual Scams and Cybercrime Brief 2023 (Singapore: SPF, 2025), p.17

2. 2024年透過六次聯合行動，共發送超過77,100則警示簡訊。成功預警並通知超過55,600名潛在被害人，大多數被害人於接獲簡訊後，便意識到詐騙風險並停止轉帳。估計此系統2024年協助攔阻總計超過4.2億新幣的潛在詐騙損失[55]。

3. 2025年上半年透過三次聯合行動，共發送超過19,800則簡訊，提醒超過14,200名被害人。這種主動、以被害人為核心的做法成功避免超過1.45億新幣的潛在損失[56]。

（二）制度優勢：

1. 提升凍結款項效率：從發現、分析到警示可自動化快速完成，大幅提升資金凍結與止損效率。

2. 規模可擴展：透過機器人流程自動化機制可快速處理大量交易資料，未來可與更多銀行、電信商或支付平台擴大合作。

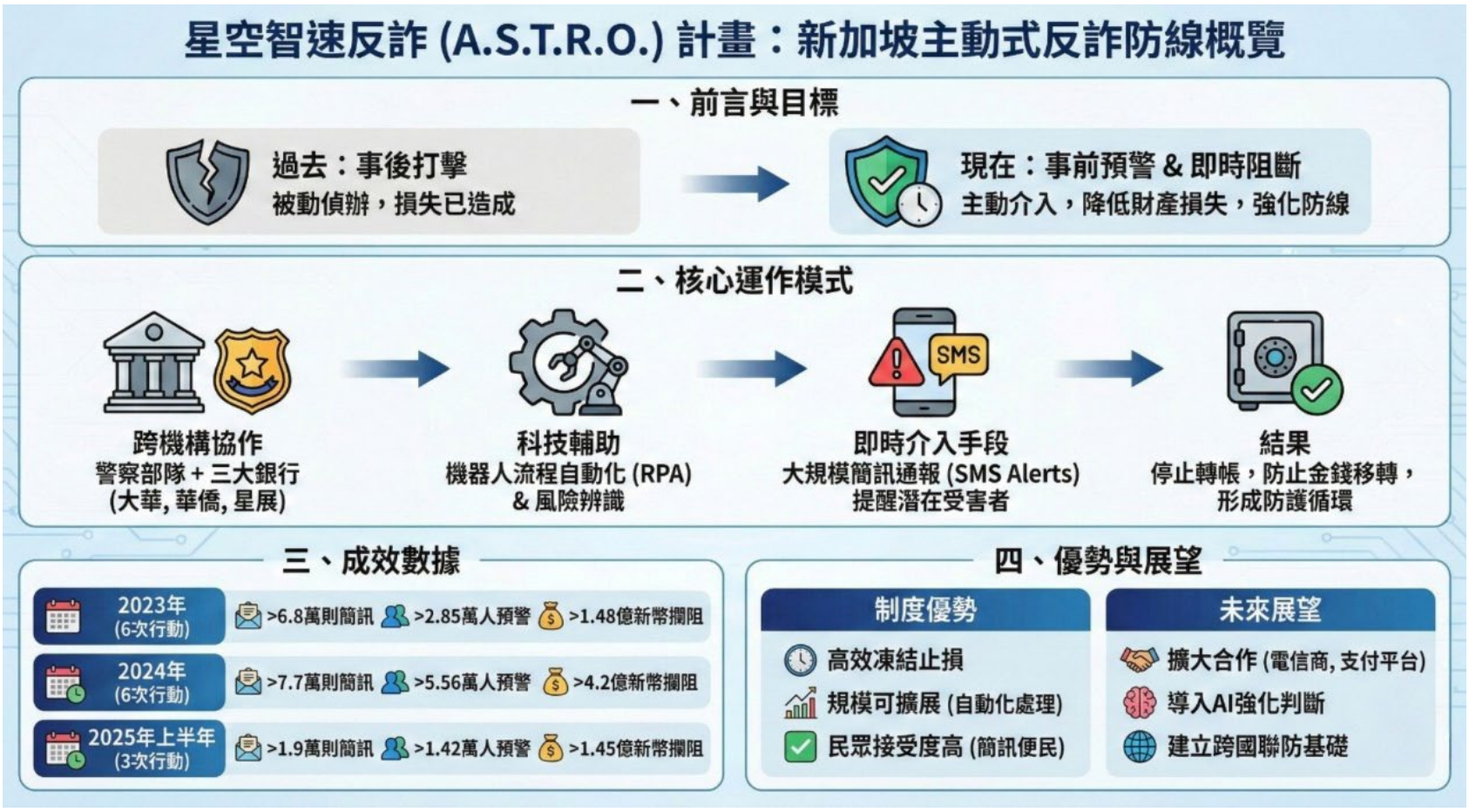
3. 民眾接受度高：採用SMS簡訊通報形式，可直接接觸手機使用者，簡便且即時。

四、小結：

「星空智速反詐」計畫展現新加坡政府在數位防詐策略上的積極作為與技術整合能力，透過與金融機構的深度合作與自動化簡訊預警機制，大幅提升對潛在詐騙受害者的即時防護。在現有基礎上，該機制可望進一步擴展合作對象，涵蓋更多銀行與電信業者，實現更全面的金流監測與通報。另一方面，倘導入人工智慧強化風險判斷與精準警示能力，也將使系統運作更具彈性與效率。

55 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p.14
56 SPF, Mid-Year Scam and Cybercrime Brief 2025 (Singapore: SPF, 2025), p. 28

圖21、「星空智速反詐」計畫內容與成效



資料來源：駐新加坡代表處繪製

5.4 社群媒體

5.4.1 背景

據新加坡警方統計，約60%詐騙案件乃透過社群媒體及即時通訊平台進行傳播與誘導。2024年社群平台詐騙案增加至近1.5萬件。其中透過臉書接觸者有59.8%、透過Instagram 接觸者有18%、利用TikTok 接觸者占13.2%。平台的匿名性與廣告投放機制，使詐騙內容能在短時間內大規模擴散；Telegram 更因強調隱私而成高風險溫床，該平台通報案件在 2024 年幾乎倍增。

政府因而將社群業者納入「公私協力」反詐體系，並在2023年至2025年間推出新法規與技術對接方案，以因應詐騙案件結構變化，利用前端防堵與跨部門合作等方式，盼有效抑制透過網路平台傳播的詐騙活動。

5.4.2 措施與成效

表10、新加坡警方與社群平台業者合作措施及成效

政府或警方措施	平台配合動作	主要成效
《網路犯罪危害法》：對指定網路服務發布「停止傳播／停用帳號」等指示，並要求落實身分驗證。	Meta等平台業者須向高風險賣家實施證件驗證，並定期向內政部報告[57]。 旋轉拍賣承諾於2026年1月31日前實施多項新措施，包括引入通行密鑰與生物辨識登入，以及將涉及詐騙的Singpass憑證列入黑名單，禁止其驗證新帳號，以防範已驗證帳號遭濫用[58]。	2024年6月至12月間，旋轉拍賣的電商詐騙數量下降約 11%。雖然幅度不大，但仍呈下降趨勢。 2024年5月至11月間，臉書市集的電商詐騙數下降約 55%[59]（年度資料請參考表3-4）。 2025年上半年電子商務詐騙案件數大幅下降，自2024年上半年的7, 224件降至3, 237件，減少55. 2%；整體財損也從2024年同期約850萬新幣減少至約760萬新幣，下降10. 7%[60]。
政府邀請主要社群平台建立專線或進駐反詐中心，以期更有效率地下架可疑網路帳號與廣告[61]。	旋轉拍賣、Meta及蝦皮等平台業者依專案需求進駐反詐中心。	警方歷年與平台業者合作下架數量，於2024年至2025年上半年間有顯著增長： 2021年：1, 300件 2022年：3, 100件 2023年：4, 100件 2024年：33, 600件 2025上半年：21, 600 件
Google公司率先與新加坡網路安全局於2024年2月合作推出「阻擋側載高風險App」機制[62]。	Google Play商店在新加坡先行封鎖要求敏感權限的側載App。	2024年2月至7月阻擋了90萬次安裝嘗試；惡意程式詐騙案件降至 95件。[63] 此措施之後陸續擴展至巴西、香港、印度、肯亞、奈及利亞、菲律賓、南非、泰國及越南等國，2024年總計成功阻擋了3, 600萬次、20萬款不同應用程式的安裝嘗試，防止這些潛在惡意應用程式滲透1, 000萬部Android系統裝置。[64]

資料來源：駐新加坡代表處整理

57 “Singapore Introduces Codes of Practice under the Online Criminal Harms Act 2023,” Perspectives, Reed Smith LLP, accessed 10 Aug. 2025, https://www.reedsmith.com/en/perspectives/2024/06/singapore-introduces-codes-of-practice-under-the-online-criminal-harms

58 “平台骗案去年同比下降近四成 旋转拍卖明年再推更多防诈措施,” Zaobao, 21 Nov. 2025, https://www.zaobao.com.sg/realtime/singapore/story20251121-7851158

59 “Assessment of Carousell’s and Meta’s Enhanced Verification Measures Under the E-commerce Code of the Online Criminal Harms Act,” MHA, 10 Mar. 2025, https://www.mha.gov.sg/mediaroom/press-releases/assessment-of--and-meta-enhanced-verification-measures-under-the-e-commerce-code-of-the-online-criminal-harms-act/

60 SPF, Mid-Year Scam and Cybercrime Brief 2025 (Singapore: SPF, 2025), p. 19

61 SPF, Mid-Year Scam and Cybercrime Brief 2024 (Singapore: SPF, 2024), p. 16

62 “Singapore Android Users to Be Blocked from Installing Certain Unverified Apps as Part of Anti-Scam Trial,” CNA, 7 Feb. 2024, https://www.channelnewsasia.com/singapore/google-android-devices-malware-scam-unverified-apps-sideloading-4102991

63 “Android Users in Singapore Tried to Install Unverified Apps Nearly 900,000 Times in Past 6 Months.” CNA, 16 Aug. 2024, https://www.channelnewsasia.com/singapore/android-users-install-malware-unverified-apps-google-fund-anti-scam-4550026

64 BÎZGĂ, Alina. “Google Blocks 2.3 Million Malicious Apps from Play Store in 2024: What You Need to Know.” Hot for Security, 4 Feb. 2025, https://www.bitdefender.com/en-us/blog/hotforsecurity/google-blocks-2-3-million-malicious-apps-from-play-store-in-2024-what-you-need-to-know

表11、2023年至2024年主要電子商務平台的詐騙數據變化

	2023年		2024年	
平台	詐騙案件數	於電子商務詐騙案比例	詐騙案件數	於電子商務詐騙案比例
臉書	4, 550	46. 5%	4, 368	37. 4%
旋轉拍賣	2, 476	25. 3%	1, 987	17. 0%

資料來源：駐新加坡代表處整理[65]

5. 4. 3 小結

在「公私協力」框架下，新加坡透過法規、驗證機制及即時通報（進駐反詐中心）等策略，把社群平台從「內容載體」轉為「共同防線」。政府賦予平台驗證、封鎖與資料回報義務；平台則提供即時通報窗口、專責團隊與廣告審查，形成「警方快速舉報、平台即時處置、用戶風險降低」的快速反應操作流程。隨著跨國詐騙持續升溫，新加坡下一步將評估把Telegram等高風險即時通訊平台納入強制性身分驗證與合規對象，並推動與周邊國家進行跨境聯防計畫，進一步提升區域整體的社群媒體反詐韌性。

圖22、社群媒體在反詐騙活動的角色與成效

資料來源：駐新加坡代表處繪製

65 “Number of E-commerce Scams by Approach Modality,” MHA, 10 Mar. 2025, https://www.mha.gov.sg/docs/default-source/default-document-library/annex-b-number-of-e-commerce-scams-by-approach-modality.pdf?sfvrsn=96c277c9_1

5.5 社區合作

5.5.1前言

面對日益嚴峻的詐騙犯罪數字，新加坡政府近年將「公私協力」作為反詐核心戰略之一，而社區合作是其中最貼近民眾並落實到日常生活中的環節。本節綜整「速訊滅詐計畫」、「我可以對抗詐騙」全國運動、「安全家園」組屋入戶宣導計畫，以及「樂齡防詐計畫」，剖析警方如何把防詐宣導教育結合新加坡組屋社區網絡，並評估其成效與未來方向。

5.5.2 措施與成效

一、「速訊滅詐計畫」

（一）運作方式：由反詐騙指揮處[66]製作30秒至60秒的短影音及圖卡，依最新騙術快速改版，發布於ScamShield網站的「詐騙佈告欄」及官方、民間社群網站。

（二）社區連結：利用警察及政府公務員個人社群、風險相關公司員工進行二次轉傳，再搭配每個月的「詐騙佈告欄」刊物，形成熟人圈的提醒效果。

（三）主要成效： 新加坡警察部隊經常根據最新詐騙趨勢製作30秒至1分鐘左右的宣導短影片，並透過WhatsApp及Telegram等平台進行推廣。鑑於詐騙分子最常使用這兩大通訊平台聯絡目標，新加坡警察部隊便以同樣媒介發佈短影音，內容含詐騙訊息截圖及警方提醒，影片觸及率達將近百萬名民眾[67]。

二、「我可以對抗詐騙」（I Can ACT Against Scams）倡議：

（一）運作方式：該倡議以「A. C. T.」（行動）作為框架簡化防詐流程，每個字代表意義如下：

1. ADD －「加」：強化安全防護

(1) 下載「ScamShield」或其他合法攔阻詐騙之應用程式。

(2) 調整社群軟體（如：Telegram、臉書、Instagram、TikTok、LinkedIn）隱私設定，限制或禁止他人查看自己之動態。

(3) 啟用兩步驟或多重步驟驗證，為社群、銀行及其他重要帳戶增設額外驗證方式。

(4) 更新裝置與軟體安全設定，確保系統與防毒程式為最新版本。

(5) CHECK －「查」：多方核實確認

(6) 確認金融交易透過正規平台、對象真實可信。

66 反詐騙指揮處(ASCom)即原反詐騙中心(ASC)，係2022年改制升格。

67 SPF, Annual Scams and Cybercrime Brief 2022 (Singapore: SPF, 2023), p.13.

(7)向官方來源與可信親友查證詐騙跡象與趨勢（如：新加坡警察部隊、Scam Alert、網路安全局、全國犯罪預防理事會等網站）。

(8)自我檢視行為與情緒狀態：遇到使人感到壓力或不確定之要求，先暫停回覆、冷靜思考。

2. TELL –「報」：立即通報分享

(1)無論是遭遇詐騙或已成為被害人，第一時間通報相關官方單位（銀行、平台、警方等）。

(2)向親友與社群分享詐騙徵兆、趨勢與自身經驗，協助周遭親朋好友提高警覺。

(3)回報相關官方單位與社區，共同累積資訊、傳播警示。

（二）社區連結

1. 國家犯罪預防理事會、警察部隊與ScamShield平台於電視、大眾運輸及社群媒體等投放宣導廣告[68]。

2. 設置ACT體驗攤位巡迴校園與鄰里中心，示範　ScamShield、「緊急止付」等工具[69]。

（三）主要成效：相關宣傳影片累計超過100萬瀏覽次數，超過七成受訪者能正確說出至少一項ACT行動[70]。

三、「安全在家」組屋入戶防詐宣導計畫：

（一）運作方式：由宏茂橋警署發起之社區安l全方案。員警、國民服役警員與志工走訪組屋，逐戶發放防詐手冊，並邀請居民關注鄰里警局之社群帳號，以及註冊「警民即時警訊服務」以獲取最新犯罪動態。

（二）社區連結：宏茂橋警區六個鄰里警局之員警將逐戶拜訪宏茂橋、後港、榜鵝、盛港及實龍崗等區之居民，宣導最新詐騙手樣，並告知民眾如何保護自己及家人免受詐騙，並結合居民委員會活動以Instagram直播「安全在家」實況節目[71]。

（三）主要成效：自2022年7月發起以來，9個月內已拜訪2, 400座組屋，面對面接觸超過95, 000名居民[72]。

四、「樂齡防詐計畫」

（一）運作方式

68　Joanna Octavia, “Online Fraud and Scams in Singapore,” Safer Internet Lab, p. 8

69 “Police Community Roadshows 2023,” accessed 10 Aug. 2025, https://ncpc.org.sg/news-and-events/event-news/police-community-roadshow-2023/.

70 “Chairman’s Message,” accessed 10 Aug. 2025, https://ncpc.org.sg/chairman/

71 “Launch Of SAFE@Home By Member Of Parliament (MP) For Pasir Ris-Punggol GRC, Ms Yeo Wan Ling At Punggol Plaza On 23 July 2022,” SPF, http://www.police.gov.sg/Media-Room/News/20220723_launch_of_safehome_by_mp_for_pasir_ris_punggol_grc

72 “Change Of Command At Ang Mo Kio Police Division.” SPF, accessed 10 Aug. 2025, http://www.police.gov.sg/Media-Room/News/20230530_change_of_command_at_ang_mo_kio_police_division

1. 宏茂橋警署與新加坡銀髮志工組織聯合推出的樂齡防詐倡議，透過同儕志工之力量，把最新防詐資訊送進銀髮社群。

2. 由宏茂橋警署社區警務組提供培訓講師及最新詐騙趨勢資訊，與銀髮志工組織共同培訓及任命「樂齡防詐志工」。志工在接受半日之最新詐騙概況與溝通技巧課程後，於社區中心、醫療院所及「與警察喝咖啡」等活動中擔任主持人、講座，或於活動攤位上向年齡相仿之長者宣導防詐知識及安裝ScamShield軟體等，縮短與年長者間之距離，並以相同語言進行交流。

（二） 社區連結

1. 採「樂齡對樂齡」同儕模式，於20多個組屋城鎮間巡迴，每月固定出隊[73]。

2. 志工同時是「社區守望計畫」成員，可透過該計畫通訊群組，即時接收並分享警方發布的最新犯罪資訊與防範訊息。

（三）主要成效[74]

1. 計畫自2022年啟動至2024年，已培訓超過200名樂齡志工，辦理120場以上防詐講座，觸及超過11, 180位長者。

2. 2023年9月，兩名樂齡防詐志工在盛港活動中心成功勸阻一名長者匯款，避免其遭假警察詐騙而蒙受損失。

3. 2024年10月，一名樂齡防詐志工於社區防詐講座結束後，成功說服受害者停止與網戀詐騙集團接觸，避免其在損失10萬新元後繼續匯款。

5.5.3 小結

近年來，新加坡以「社區合作」為公私協力打詐的突破口，建構線上、線下與同儕互助交織的多層防線。為避免民眾警覺性隨時間而下降，而在詐騙手法更新後再次受騙，反詐宣導必須不斷更新教材與內容。

速訊滅詐計畫以短影音搶占民眾注意力，提高民眾警覺；「我可以對抗詐騙」倡議讓「加、查、報」三步驟則把反詐觀念簡化，讓民眾易於執行；「安全在家」計畫由員警逐戶敲門直接與民眾互動，深化彼此理解；「樂齡防詐計畫」則由銀髮志工向銀髮族解說，藉同齡語言建立信任。上述措施建立了「警訊、行動及陪伴」的正向循環。從宣傳短片近百萬的觀看數，員警在社區超過9萬戶觸及率，樂齡志工在第一線阻止多起民眾的高額損失，凸顯新加坡政府在社區反詐工作之滲透力與效果。

73 PRAISE (Police RSVP Anti-Scam Engagement), C3A, accessed 10 Aug. 2025, https://www.c3a.org.sg/volunteerism/praise-police-rsvp-anti-scam-engagement

74 “Police-RSVP Anti-Scam Engagement (Praise) Advocate Appointment Ceremony.” SPF, accessed 10 Aug. 2025, http://www.police.gov.sg/Media-Room/News/20240715_policersvp_antiscam_engagement_praise_advocate_appointment_ceremony

圖23、社區合作在反詐騙活動的角色與成效

資料來源：駐新加坡代表處繪製

5.6 小結：公私協力之聯防體系與成效

綜觀新加坡自2019年推動與銀行、電信業、電商與社群媒體及社區等之協力防詐作為，著重打破以政府為唯一的打詐主體的框架，透過共同責任架構與實體進駐，將銀行、電信商、社群平台與社區串連成共同防護體系。

5.6.1 公私協力反詐主要做法

除了資訊交換外，新加坡政府另強調實體整合與責任分擔，其主要運作策略如下：

一、實體進駐：以反詐騙指揮處為核心，邀請七大系統性銀行（如星展、華僑、大華等）與主要電商平台（如旋轉拍賣、蝦皮）派員實體進駐反詐騙指揮處。減少公文往返的時程，實現跨機構的即時溝通與決策。

二、金融防線的責任升級：推動「共同責任架構」，確立了銀行與電信商在詐騙案件中的賠償責任（瀑布式究責）。銀行端推行資金鎖定、緊急止付以及淘汰一次性簡訊密碼，從被動防禦轉為主動風險控管。

三、 數位平台的源頭治理：要求社群與電商平台落實身分驗證，並與 Google合作在應用程式商店端直接阻擋高風險的側載App，從源頭減少惡意軟體的入侵機會。

四、社區鄰里的延伸推廣：將防詐觸角延伸至家戶，透過「安全在家」與「銀髮志工」計畫，利用同儕與鄰里警局的力量，針對高風險族群進行面對面宣導。

5.6.2 預期成效與成果

這套公私協力機制，在2024年至2025年間具體成效數據如下表所示：

表12、新加坡公私協力反詐具體成果一覽表

協力面向	策略及作法	具體成果與數據
組織面	反詐騙指揮處：銀行派員駐點，即時凍結資金。	1. 2024年成功追回逾1. 82億新幣 之受害款項。 2. 透過快速介入，額外攔阻了4. 83億新幣的潛在損失。
金融防線（銀行端）	星空智速反詐計畫(A. S. T. R. O.)：自動化偵測潛在受害者並發送警示。	1. 2024年發送逾7. 7萬則警示簡訊，觸及5. 5萬名潛在受害者。 2. 成功避免約4. 2億新幣的潛在轉帳損失。
資產保全（客戶端）	資金鎖定：用戶可鎖定部分資金，僅臨櫃可動用。	截至2025年6月，已有超過37萬名客戶啟用，鎖定資產總額超過 300億新幣，有效降低遭駭後的損失規模。
平台治理（科技端）	下架機制與技術聯防：平台進駐與Google防側載合作。	1. 2024年協助下架 33, 600件詐騙帳號與廣告，較2023年成長顯著。 2. Google機制在半年內阻擋 90萬次 高風險側載安裝，使惡意軟體詐騙案降至95件。
電信防護（通訊端）	單一政府簡訊ID（gov. sg）：統一發送來源，杜絕假冒。	截至2025年6月，發送1. 81億則簡訊，未出現任何假冒詐騙簡訊，民眾辨識度達93%。

第六章 結論：新加坡打詐作法及成效總結

6.1 新加坡打詐作法

綜合前面各章的打詐政策，可知新加坡面對現有個詐騙犯罪挑戰，將作法聚焦於「法律治理、組織佈局、科技偵查、公私協力、社區參與及跨境合作」六大面向，各面向內容摘要整理如下：

一、法制作為

（一）「支付服務法」（2024年修訂）

1. 將加密貨幣交易所、錢包與跨境匯款一併納管，要求落實洗錢及反資恐監控、客戶資金隔離及可疑交易申報，並賦予警察部隊商業事務局與反詐騙中心即時凍結可疑金流權限。
2. 違規案例：2023年30億新幣洗錢案中，有4名嫌犯因未持有牌照仍大量兌換加密貨幣，遭判處4週至20個月不等有期徒刑。

（二）「電腦濫用法」（2024年修訂）

新增第 55A 條「協助可疑金流」罪，行為人未盡合理查證即該當要件，成功降低執法機關「人頭帳戶及數位個人身分」之舉證門檻。

（三）「網路犯罪危害法」（2024年2月生效）

設置五大「指令」：停止通訊、內容屏蔽、帳戶限制、域名封鎖及應用程式下嫁指令。平台通常會在指令發出後24小時內配合移除。2024年，新加坡警方藉此措施阻斷逾15萬組詐騙相關之電話線路、網站與社媒帳號。

（四）「雜項犯罪法」（2025年1月生效）

針對「人頭SIM卡」相關行為態樣新設刑責，對不實申請、中介、轉讓及使用者究責，預防性規範SIM卡濫用導致之詐騙犯罪。

（五）《貪污、販毒與其他嚴重犯罪（沒收利益）法》（2024年2月修訂）

1. 增設「魯莽」與「過失」構成之洗錢罪及「協助他人保留犯罪所得罪」，針對協助詐團洗錢或提供洗錢帳戶者，即使未實際接觸金流，只要未盡合理查證義務，即可追究刑事責任。
2. 成效：2024年警方發動之全國性打詐行動中，超過660名詐欺集團成員及人頭帳戶提供者遭起訴，其中有110名即係依據此新修訂法案起訴。

（六）「防詐騙保障法」（2025年7月生效）

引入限制令措施：警方得在「明顯高風險」情況下凍結被害人帳戶最長180

天，阻止自願轉帳型之大額詐騙財損。

（七）《刑事法（雜項修正）法案》（2025年11月生效）

首次將詐騙相關犯罪納入鞭刑範疇，對詐騙集團主謀、成員與招募者實施強制鞭刑（6下至24下）。對於協力者，如協助洗錢者、人頭帳戶提供者等，則可酌情處以最高12下之鞭刑，藉由嚴厲的刑罰，建立強大的威懾力。

二、組織佈局：反詐騙指揮處及聯合戰情室

自反詐騙中心（2019年）擴展成反詐騙指揮處(2022年)：整合七大地方警署的詐騙打擊小組及「跨境資金追回行動小組」的國際合作網絡，藉星展銀行、華僑銀行、大華銀行、渣打銀行、匯豐銀行、聯昌國際及GXS等七家系統性銀行人員進駐合署辦公，跨行凍結時間從數日縮短至同日內即可完成凍結。

「SCAMS」與「六I」策略：反詐騙指揮處以資訊感知、跨部門合作、社會意識、降低損害、快速執法五項策略為總綱，再衍生資訊管理、即時介入、調查、創新、公眾教育及國際合作等六大核心功能，藉以應對每日平均140件以上之詐騙案件通報。

三、科技偵查：AI-機器人流程自動化-簡訊形成之「迅速阻斷金流防線」

（一）ScamShield 套裝版（2024年）

2024年升級為「應用軟體、網站、Telegram/WhatsApp警訊、1799熱線」的「四合一」工具組後，歷年成效比較如下：

1. 2021年，下載量約25萬7,000次，攔阻約370萬則疑似詐騙簡訊、15,500組疑似詐騙號碼。
2. 2022年，下載量近50萬次，累計通報詐騙簡訊逾740萬則、攔阻超過47,000組門號。
3. 2023年，下載量成長至近85萬次，累計通報詐騙簡訊逾790萬則、攔阻超過80,000組門號。
4. 2024年ScamShield套裝版上市不久，同年底下載數累計突破百萬次，至2025年9月已達135萬次。
5. 「1799」熱線於2023年開辦時，每天電話僅約14通，自行2024年推出ScamShield套裝版，24小時的救助專線（1799），每天接聽電託增加至約500通。

（二）「詐騙分析及戰術性介入系統」、「詐騙分析及戰術性介入系統+」（AI網路巡邏）

1. 利用遞迴式機器評分引擎，每日掃描逾10萬個網站，2023年封鎖25,000個網站及29,200個WhatsApp號碼，2024年則總計封鎖44,900個詐騙相關網站

與40, 500個WhatsApp帳號，數字分別有79%及38%之成長。

2. 與Google網路風險檢測服務界面整合後，可在任何支援瀏覽器即時警示有詐欺風險網站。此外，「詐騙分析及戰術性介入系統+」正評估延伸至PayNow即時轉帳與電子支付異常偵測，預計本（2026）年上線。

（三）「星空智速反詐」計畫（機器人自動化流程、SMS簡訊預警）

1. 2023年透過六次聯合行動，共發送超過68, 000則簡訊，提醒超過28, 500名被害人，成功避免超過1. 48億新幣的潛在損失75。

2. 2024年透過六次聯合行動，共發送超過77, 100則警示簡訊。成功預警並通知超過55, 600名潛在被害人，大多數被害人於接獲簡訊後，便意識到詐騙風險並停止轉帳。估計此系統2024年協助攔阻總計超過4. 2億新幣的潛在詐騙損失76，成效大幅上升。

3. 流程全自動：包含報案、銀行凍結、大數據回溯清查、SMS簡訊群發及發現、促請潛在被害人報案等步驟，再循環找出更多詐騙人頭帳戶。

（四）緊急止付、資金鎖定與惡意 App偵測

1. 金管局要求銀行從2022年10月底前實施緊急止付（自助凍結帳戶功能）作為網路銀行安全的標準措施。至2023年底，警方已可透過銀行以緊急止付功能幫助民眾在帳戶可能被入侵時暫停凍結，以防止未經授權的交易活動。

2. 各銀行於2023年11月開始陸續推出資金鎖定功能，用戶可一鍵凍結帳戶或將存款鎖定為「僅臨櫃可提」。2024年2月時，約61, 000個帳戶設置資金鎖定，鎖定存款總額超過54億新幣。同(2024)年10月時，已有181, 000客戶使用資金鎖定功能，鎖定資金總額約158億新幣。截至2025年6月，共有超過370, 000客戶使用資金鎖定，被鎖定資金超過300億新幣77。

3. Google公司與新加坡網路安全局於2024年2月合作推出「阻擋側載高風險App」機制；Google Play商店半年間(2024年2月至7月)擋下90萬次側載安裝，惡意程式詐騙案降至95件。

四、公私協力：「共同責任架構」與社群媒體、電商平台派員駐點

（一）「共同責任架構」與瀑布式責任追究：

新加坡政府於2024年12月16日正式實施「共同責任架構」，針對層出不窮的釣魚詐騙案件，建立金融機構、電信業者與消費者三層責任的「瀑布式」究責模式。其核心設計在於：

1. 金融機構：承擔第一層把關責任，例如延後密碼生成器生效時間、在高風險交易發生時即時通知客戶、提供24小時自助阻斷轉帳服務，以及強化即時詐騙監控。

75 SPF, Annual Scams and Cybercrime Brief 2023 (Singapore: SPF, 2025), p.17
76 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p.14
77 “Over 370,000 Singapore bank customers used the money lock feature,” Asian Banking and Finance, accessed 24 Sep. 2025 https://asianbankingandfinance.net/news/over-370000-singapore-bank-customers-used-money-lock-feature

2. 電信業者：確保僅有授權供應商能發送簡訊、阻斷未授權簡訊來源，並攔截含有釣魚連結的簡訊。配合「簡訊發送者識別碼註冊制度」，未註冊的簡訊會被標註為「可能為詐騙」。

3. 消費者：保持警覺，不點擊可疑連結，並及時通報未經授權的交易（30日內）。若對調查結果不滿，可透過「金融業爭議調解中心」等管道申訴。

制度實施後，相關成效逐步顯現：

1. 各大銀行已全面升級數位安全機制，強化高風險交易的即時防護能力。

2. 電信商配合政府，自2024年7月1日起統一使用「gov. sg」作為政府簡訊識別碼，避免不同單位各自使用ID而導致混淆。截至2025年6月，已透過「gov. sg」發送1. 81億則簡訊，未出現任何詐騙簡訊；93%用戶能辨識「gov. sg」為官方簡訊，並獲得84. 3%的民眾滿意度。

（二）平台聯防：社群與電商業者駐點合作

為有效遏止電商與社群平台上的詐騙活動，新加坡政府透過《網路犯罪危害法》，向指定網路服務業者發布「停止傳播」及「停用帳號」等指令，並要求業者落實身分驗證措施。

在執行層面，政府與警方邀請主要平台，如Meta、旋轉拍賣及蝦皮，派遣技術團隊進駐反詐騙指揮處，建立專線加速合作處理個案。平台也須針對高風險賣家進行證件驗證，並定期向內政部報告。此舉搭配「詐騙分析及戰術性介入系統」的通報機制，使得假賣家帳號與詐騙廣告的下架時間由過去的數天縮短至數小時。相關成效如下：

1. 詐騙案件下降：

(1) 2024年5月至11月間，臉書市集電商詐騙數量下降約55%；

(2) 2024年6月至12月間，旋轉拍賣的電商詐騙數下降約11%，雖幅度有限，但顯示趨勢改善。

2. 合作下架可疑帳號及廣告成效（2024年至2025上半年間件數速成長）：

(1) 2021年：下架 1, 300件

(2) 2022年：下架 3, 100件

(3) 2023年：下架 4, 100件

(4) 2024年：下架 33, 600件

(5) 2025上半年：下架21, 600件

五、社區參與：短影音及敲門行動的「鄰里防詐網」

（一）「速訊滅詐計畫」：由反詐騙指揮處依最新詐騙趨勢製作30至60秒短影音及圖卡，透過ScamShield網站、「詐騙佈告欄」及官方、民間社群網站發布，再由

警察、公務員與相關企業員工二次轉傳。特別是在WhatsApp與Telegram等詐騙最常用的通訊平台進行推廣，單支影片觸及率近百萬，形成去中心化的熟人圈提醒效果。

（二）「我可以對抗詐騙」運動：以「加」「查」「報」三步驟簡化防詐流程，透過電視、公共運輸與社群媒體廣告，以及校園與鄰里中心的ACT體驗攤位，示範ScamShield、「緊急止付」等工具。相關宣導影片瀏覽量累計逾百萬，調查顯示超過七成受訪者能正確說出至少一項ACT行動，顯示宣導成效顯著。

（三）「安全在家」計畫：由宏茂橋警署發起，員警、國民服役警員與志工逐戶走訪宏茂橋、後港、榜鵝、盛港與實龍崗等區，共拜訪2, 400座組屋，面對面接觸超過95, 000名居民，並結合居民委員會活動以Instagram直播「安全在家」節目，提升社區即時互動與防詐意識。

（四）「樂齡防詐計畫」：採「樂齡對樂齡」模式，透過200名培訓銀髮志工巡迴20多個組屋城鎮，每月固定出隊，兩年間已辦理120場以上防詐講座，觸及逾11, 180名長者。2023年與2024年分別成功勸阻長者遭遇假警察與網戀詐騙，避免高額損失，顯示對60歲以上高風險族群的精準防護成效。

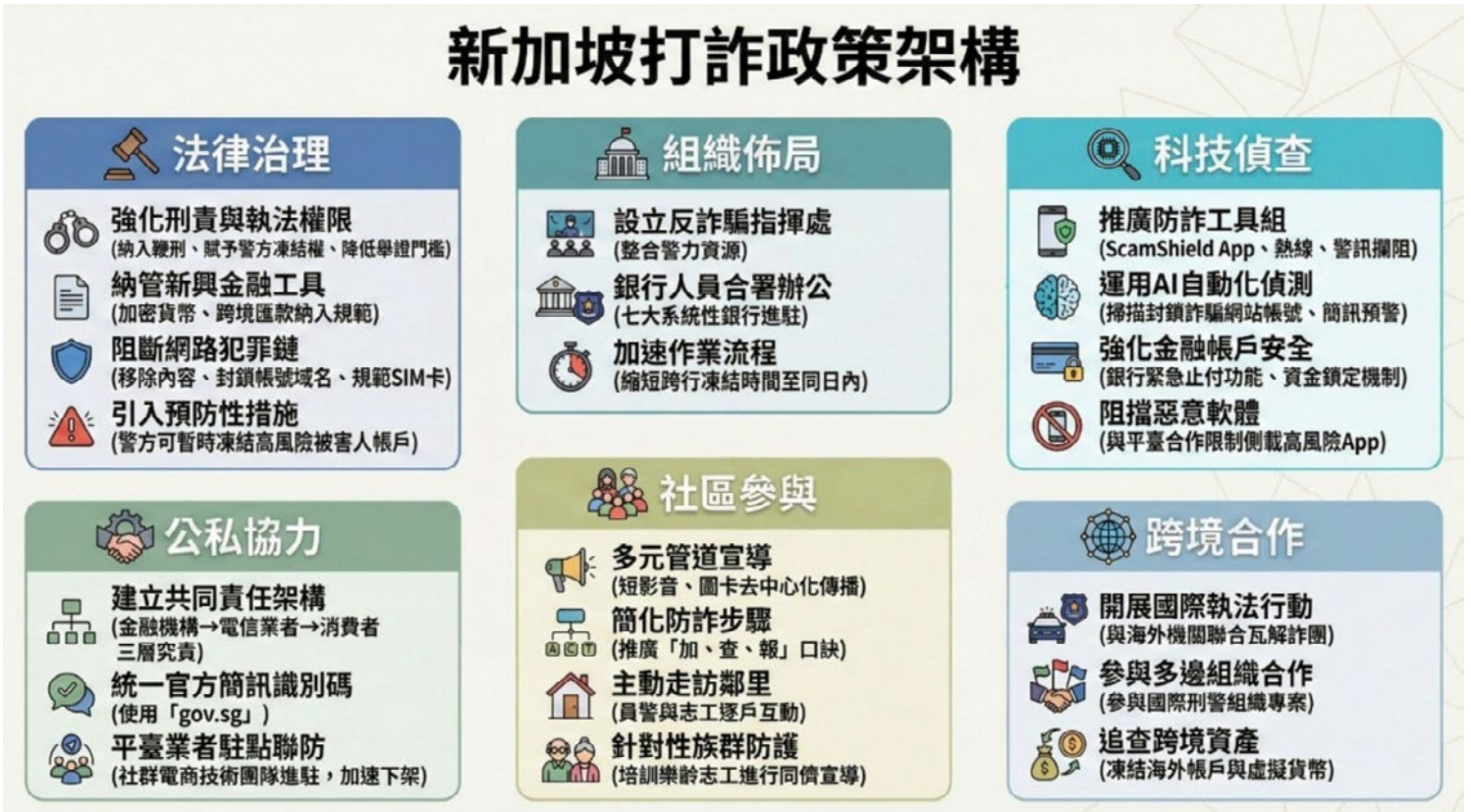
六、跨境合作：區域聯繫與資產凍結

（一）2022年，新加坡警方與海外執法機關緊密合作，成功瓦解13個詐騙集團，包括6個求職詐騙、3個假冒政府官員詐騙、2個釣魚詐騙及2個網戀詐騙，共逮捕超過70名海外成員，涉及280餘起案件。

（二）2023年，參與國際刑警組織的「曙光行動」，與76個國家共同合作，調查超過2, 000人，凍結本地5, 300個銀行帳戶、追回逾1, 150萬新幣，並扣押總值3, 000萬新幣之虛擬資產。另於「HAECHI反詐騙專案行動」中，調查逾800名涉案成員，封鎖4, 900個銀行帳戶與300個虛擬帳戶，並扣押資金與虛擬資產合計超過1, 690萬新幣。

（三）2024年，與馬來西亞皇家警察等海外執法機關合作，瓦解16個跨國詐騙集團，共逮捕150餘人，涉及2, 300多起案件，受害金額逾5, 800萬新幣。並參與國際刑警組織「HAECHI V」行動，調查超過1, 600人，凍結5, 100個銀行帳戶及1, 000個加密錢包，扣押資金5, 480萬新幣及約79. 8萬新幣加密貨幣。2024年與馬來西亞警方聯手瓦解16個跨國詐團，逮捕 150 人、追回5, 800萬新幣。

圖24、新加坡打詐政策架構



資料來源：駐新加坡代表處繪製

6.2 新加坡打詐成效

新加坡政府在過去五年間把「打擊詐騙」視為維護人民安全的重要一環，並將之與反恐、反洗錢同列為國家級議題[78]，進而整合各政府機關效能、強化公私部門合作，藉以規劃全方位的反詐架構。

首先，新加坡政府從法律基礎著手，修訂《支付服務法》、《電腦濫用法》、《網路犯罪危害法》、《雜項犯罪法》、《貪腐、販毒與其他嚴重犯罪（沒收利益）法》及《防詐騙保障法》等法案，奠定政府機關介入干預之權限。再經由政府技術局及內政部科技局等資訊單位提供技術支援，最後透過銀行、電信及電商平台同時進場，形成從法律面嚇阻犯罪分子、技術面強化反詐能力，以及教育面提升反詐意識的完整策略。

在此一整合式戰略下，新加坡政府在「降低平均財損」、「攔阻速度」、「資金追回」、「預防偵測」、「中介機制」及「防止詐團取得人頭帳戶及電話門號」等方面均有顯著成效；惟在當前科技日新月異的時代背景下，詐騙集團手法呈現技術化、跨境化及時事化的趨勢，再輔以逐漸進化的AI模擬技術及去中心化的加密貨幣金流等各種新型態詐欺挑戰；未來若要鞏固成效，相信仍需不斷精進反詐政策，以及拓展跨國合作聯防機制，方能持續創造良好打詐成果。

78 “HomeTeamNS Awards 2025 – Speech by Mr K Shanmugam, Minister for Home Affairs and Minister for Law.” Ministry of Home Affairs, accessed 10 Aug. 2025, https://www.mha.gov.sg/mediaroom/speeches/hometeamns-awards-2025/

表13、新加坡打詐措施總表

工具	政策	效果
法律面向		
《支付服務法》	1. 採兩級執照制度及模組化納管七大類支付活動。 2. 強制客戶盡責調查、反洗錢及反資恐監測，以及提交可疑交易報告。 3. 加密貨幣託管、轉移、兌換服務需全面持有執照；並將用戶資金隔離於獨立帳戶。	1. 2023年至2024年間，多家機構因客戶盡責調查監測不足遭處分超過1,500萬新幣。 2. 2025年6月：5家大型支付機構遭罰款96萬新幣並限期改善反洗及反資恐查核。 3. 30億新幣洗錢案涉未持照加密貨幣交易，違反者遭判刑4週至20個月不等刑期。
《電腦濫用法》	1. 新增8A及8B條款：交付帳號、濫用他人數位身分入罪。 2. 降低主觀「明知」門檻（應合理知情）。	1. 交付數位個人身分供開戶之被告判刑（並追繳不法所得）。 2. 形成對自願轉帳型詐騙「協力者」之處罰工具
《網路犯罪危害法》	1. 五類指令：停止通訊、內容屏蔽、帳戶限制、網路屏蔽及App下架。 2. 警方合理懷疑即可發布指令；另可要求平台提供資訊及遵守相關守則。	1. 2024年阻斷逾17萬組電話線路、網站與社媒帳號（較2023年的6.75萬組大幅提升）。 2. 多起移除冒充政府官員之假帳號於24小時內完成。
《雜項犯罪法》	1. 新增第6A款：SIM卡非法供應、註冊、轉交、使用全部入罪。 2. 推定條款與舉證責任轉移；對零售商及店員違法協助課以刑責。	1. 2025年3月查獲門市盜資註冊案；同年7月逮捕44名偽冒註冊SIM卡供應者。 2. 壓縮詐團門號供應鏈，補強通訊工具面之防火牆。
《貪腐、販毒與其他嚴重犯罪（沒收利益）法》	1. 第54條第3A項：「魯莽與過失」洗錢入罪。 2. 第55A條：協助他人保留犯罪所得入罪；未盡合理查證亦構成罪責。	2024年全國性打詐行動起訴超過660人，其中110人乃援引本法案新增條款。

《防詐騙保障法》	1. 警方「限制令」：可暫停高風險對象之轉帳、ATM及信用服務。 2. 30天效期、可續最多5次；附帶訴願機制，且必要開支不在此限。	1. 截至2025年8月20日，警方已對2位民眾發出限制令。 2. 2024年上半年與2025年上半年數據相較，自願性轉帳案件比率已自86.1%下降至約78.8%。 3. 促進警察與銀行即時聯動與通報常態化。
刑事法（雜項修正）法案》	1. 將詐騙相關犯罪納入鞭刑範疇，對詐騙集團主謀、成員與招募者實施強制鞭刑（6下至24下）。 2. 對於協力者，如協助洗錢者、人頭帳戶提供者等，則可處以最高12下鞭刑。	本法自2025年11月方上路，實際成效尚待觀察。
科技面向		
ScamShield套裝版(整合App功能、Scam-Shield.gov.sg網站、警示頻道及1799熱線）	1. 主動攔截及黑名單封鎖：AI簡訊過濾、來電封鎖，及匿名回傳情資。 2. 全民參與及跨平台：App查詢及檢舉、網站查詢、Telegram/WhatsApp警示頻道推播最新詐騙手法及24小時的1799防詐熱線。	1. 2021年上半年：下載約11.9萬次；攔阻約72萬則疑詐簡訊、5,537組疑似詐騙號碼。 2. 2022年：下載近50萬次；累計通報詐騙簡訊逾740萬，攔阻超過47,000組門號。 3. 2024年：下載破百萬次；2025年9月：累計約 135 萬次。 4. 1799熱線：日均約500通；迄2025年9月累計處理 超過128,000通求助及諮詢電話。
詐騙分析及戰術性介入系統	1. AI風險評分引擎：每日掃描超過10萬個網站，即時通報高風險標的。 2. 與Google網路風險檢測服務界面介接；第三方瀏覽器或安全防護系統可同步封鎖風險網站。	1. 2024年：封鎖44,900個詐騙網站、40,500個 WhatsApp號碼（較2023 年各增加79%及38%）。 2. 建立跨部門與平台的即時處置鏈，縮短行偵測、下架到封鎖的時程。
公私協力		

反詐騙中心	1. 「SCAMS」（資訊感知、跨部門合作、社會意識、降低損害、快速執法）架構及六「I」（資訊管理、即時介入、調查、創新、公眾教育、國際合作）。 2. 與超過80家金融、金科、電信、電商合作；大型銀行員工進駐，快速凍結與追資。 3. 科技導向：納入ScamShield、詐騙分析及戰術性介入系統。 4. 跨境聯手各國反詐中心及國際刑警組織。	1. 2022年：瓦解13個跨境詐騙集團；海外逮捕超過70人，涉超過280個詐騙案。 2. 2023年：參與國際刑警組織「曙光」與「HAECHI」行動；本地凍結超過5,300個帳戶、追回超過1,150萬新元；封鎖逾4,900帳戶、查扣逾1,640萬新元與30萬加密貨幣資產。 3. 2024年：聯手馬來西亞等國破獲16個詐騙集團、超過150人被捕、涉及2,300案。
銀行合作（數位認證及共同責任架構）	1. 淘汰高風險交易之一次性簡訊密碼，改用數位憑證；App 反惡意程式偵測與封鎖。 2. 共同責任架構：分為銀行、電信業者及使用者之三層瀑布式究責；全天候緊急止付功能、約定帳戶12小時生效延遲、高風險交易凍結24小時。 3. 政府整合簡訊ID政策：政府簡訊統一以「gov.sg」識別；電信業者必須阻擋仿冒政府ID者。	1. 制度上路後，各銀行啟用即時通報與止付機制、提升釣魚防堵成效。 2. 2024年7月至2025年6月：「gov.sg」發送1.81億則簡訊；93%民眾能辨識官方簡訊；平台機關使用者增至66,140個；此政策滿意度達84.3%。
社群媒體與平台合作	1. 依《網路犯罪危害法》對指定平台下達停止傳播、帳號限制、下架等指令；要求高風險賣家證件驗證與年報揭露。 2. 主要平台（Meta、旋轉拍賣、蝦皮）進駐反詐中心，加速下架。 3. Google與網路安全局合作：先行封鎖高風險側載App。	1. 2025上半年：與平台合作下架可疑帳號及廣告21,600件（2024年同期：2,700件）。 2. 2024年6月至12月：旋轉拍賣電商詐騙下降約11%；另2024年5月至11月：臉書市集電商詐騙下降約55%。 3. 2024年2月至7月：阻擋側載安裝90萬次，當地惡意程式詐騙降至95件；機制後續擴至多國、全年阻擋3,600萬次安裝嘗試。

社區合作	1. 速訊滅詐：30至60秒短影音、圖卡即時推播；同通訊軟體頻道（WhatsApp/Telegram）觸及。 2. 「我可以對抗詐騙」倡議：加、查、報三步驟；巡迴體驗攤位示範ScamShield及緊急止付功能。 3. 「安全在家」計畫：員警與志工逐戶宣導。 4. 「樂齡防詐」計畫：同儕志工受訓、定期出隊。	1. 速訊滅詐影片觸及近百萬人次。 2. 「我可以對抗詐騙」影片累計超過100萬次觀看，超過70%受訪者能說出至少一項行動。 3. 「安全在家」計畫：警方9個月走訪2,400座組屋、接觸超過95,000名居民。 4. 「樂齡防詐」計畫：培訓超過200志工、舉辦超過120場活動、觸及11,180名長者；多起現場即時勸阻高額匯款成功案例。

資料來源：駐新加坡代表處整理

一、整體趨勢：數量雖未逆轉，但增長趨勢已趨緩

回顧2018年至2024年的整體趨勢，新加坡詐騙案件數自2018年的6,730件，逐年攀升，至2024年已達51,501件，累計增幅高達665%，顯示詐騙問題在過去六年持續惡化。若進一步檢視各年度增幅，可觀察到早期上升幅度極為迅猛，例如2020年至2021年的年增率曾達近五成以上，2021年至2022年亦維持在高成長區間。

然而，近兩年情勢已有緩和。2022年至2023年的增幅下降至46.8%，而2023年至2024年的年增率更進一步收斂至10.6%，僅為前期水準的三分之一。顯見在新加坡政府積極推動的多項打詐政策與跨部門合作下，已逐漸對詐騙集團產生抑制效果。

儘管增速減緩，然整體案件量仍處於高檔。官方統計數據顯示，2024年警方平均每10分鐘就會收到一件詐騙報案；網路購物、求職、網路釣魚及投資等前四大類型的詐騙案件，仍維持每日破百件的報案量，足見詐騙犯罪活動在新加坡持續活躍。研判可能原因乃詐騙集團犯罪手法亦不斷推陳出新，讓民眾防不勝防；另一方面，許多打詐政策方推出不久，如「防詐騙保障法」等，尚需一段時間方能產生明顯成效。

二、財損狀況：大部分案件平均財損金額降低

2024年新加坡的詐騙財損金額首次突破11億新幣（約264.2億臺幣），年增率高達70.6%。雖此增幅數字驚人，但實際上有7成以上損失金額集中在僅3.3%之千萬級巨額個案，此類個案多發生在惡意軟體詐騙、商務電子郵件詐騙及網路釣魚詐騙等型態，如某一惡意軟體詐騙即造成被害人1.25億新幣之損失，凸顯少數巨額案件拉高整

體財損總額之現象。

倘排除這些極端值，2024年的中位數損失金額反而從1,590新幣降至1,389新幣；顯示許多政府與銀行合作的早期介入措施，如「星空智速反詐」計畫，或有發揮成效，讓被害人提早發現騙局而停止匯款。使受騙金額不至持續擴大，有效降低單一案件的財損數字。

此外，值得警覺的是，近期加密貨幣已逐漸成為詐騙集團用來交易及洗錢的主要工具之一。依據星國警方統計，2024年與加密貨幣相關之財損高達1.805億新幣，與2023年僅佔總體財損6.8%相較，迅速躍升3倍以上來到24.3%[79]。去中心化的區塊鏈資金交易具匿名性與快速移轉性，使傳統追蹤金流方式面臨新挑戰。各國執法機關除積極培養加密貨幣金流分析人才外，亦需加強與加密貨幣交易所之合作關係。

三、總結

近年來，新加坡政府在打詐措施上持續精進。警方反詐騙指揮處透過合署辦公模式，2024年全年為受害者追回逾1.82億新幣，並及時攔阻潛在損失4.83億新幣；同年在「星空智速反詐」行動中，更成功發送超過77,100則簡訊，提醒超過55,600名潛在受害者，避免約4.2億新幣的財損。

在科技防詐方面，「詐騙分析及戰術性介入系統」於2024年攔阻44,900個詐騙相關網站及40,500個WhatsApp帳號，比前一年大幅提升。ScamShield平台則升級為「四合一」版本，至2025年9月下載量已突破135萬次，1799熱線每日接聽量增至約500通，顯示民眾防詐參與度與警覺性顯著提升；此外，政府自2024年7月起全面導入「gov.sg」單一簡訊識別碼，截至2025年6月已發送1.81億則簡訊且未遭偽冒，有效杜絕假冒官方的詐騙簡訊。

進入2025年，隨著多項關鍵法律生效與政策工具落地，新加坡的防詐體系更趨完備。在金融監理上，繼2024年銀行引入「資金鎖定」與冷卻期功能後，金管局於2025年6月首度依《支付服務法》對5家大型支付機構開罰，延續了前一年對合規不足機構處以逾1,500萬新幣罰款的監管力度。

在法制創新方面，多部新法於2025年正式投入實戰：警方於3月依據甫生效的《雜項犯罪法》查獲電信門市員工盜用客戶資料註冊人頭SIM卡的案件，從源頭打擊黑市供應鏈；9月內政部首度依《網路犯罪危害法》對Meta發出「實施指令」，強制平台移除詐騙廣告與落實身分驗證；《防詐騙保障法》賦予警方發布「限制令」的權限，截至2025年8月已實際運用於凍結潛在受害者帳戶，使得自願轉帳案件比率由86.1%顯著下降至78.8%；同年11月通過的刑法修正案更將詐騙相關犯罪納入鞭刑範

79 SPF, Annual Scams and Cybercrime Brief 2024 (Singapore: SPF, 2025), p.2.

疇，大幅提升法律威嚇力。

整體而言，新加坡的反詐政策在2024年透過科技偵測與銀行把關取得具體成效後，2025年更進一步透過填補法律漏洞與強化刑罰，完成了「源頭治理（SIM卡與數位身分）、中段攔阻（限制令與資金鎖定）、後端嚴懲（鞭刑與沒收）」的法制拼圖。這套結合科技、金融與高密度法規的綜合治理模式，不僅抑制了詐騙集團的猖獗，也為新加坡建構長期且具韌性的社會防詐防線奠定堅實基礎。

圖25、新加坡打詐成效總覽

資料來源：駐新加坡代表處繪製

6.3 新加坡經驗總結：政策成效的背景因素

本文前開分析之新加坡打詐政策，其推動與落實，與該國獨特的文化、社會、法治、政治及人文環境等因素，亦有密不可分之關聯。以下歸納六項背景因素，說明它們如何與前述法律、科技與公私協力等措施相互呼應，促成星國防詐架構之運作及成效。

一、跨機關整合與即時執行

新加坡採單一院制國會，執政黨長期掌握多數，部長同時兼任民選議員，形成立法行政合一的精簡決策鏈。這種集中式體制安排在實務運作中，立法與行政部門間之跨部門協調得以在較短的程序路徑下完成。

例如，「詐騙分析及戰術性介入系統」係由內政科技局與政府科技局聯手為新加坡警察部隊開發之人工智慧平台，自2023年推出以來，每日能掃描十萬個可疑網域，

並在數小時內通報平台或阻斷存取，2024年更已封鎖近45, 000個詐騙網站與逾40, 000個WhatsApp帳號。成功輔助警方快速分類、評估並封鎖詐騙網站，展現出跨部門研發與即時部署之高效能。

2024年「ScamShield 升級版」推出後，短短三個月內下載數即增加至118萬次，並成功與警方1799熱線與資料庫串連，讓詐騙簡訊、惡意來電號碼、人頭帳戶可在數小時內同步攔截或凍結，整合科技與執法效能

此外，金融管理局與電信主管機關於2023年10月公開徵詢「共同責任架構」倡儀後，2024年12月即正式施行，強制銀行與電信業者承擔賠償責任，推動其升級防詐技術，將政策檢討、民意徵詢至政策落實的程序快速完成。

綜上，新加坡之政治體制強調立法效率，亦有助促成行政部門與金融、電信、社群平台建立合作機制，讓政策工具、科技系統與實務操作在短時間即可上路實施，形成靈活的打詐治理架構。

二、高普及率的數位基礎與公民識能

新加坡得以快速推廣各項即時預警及攔阻凍結的反詐工具，全國近乎無死角的上網覆蓋率是重要基礎。據資料顯示，新加坡全國網路使用率已達96%[80]，等於約530萬人隨時在網上；智慧型手機更是人手一支，使得官方發送的警示簡訊、「詐騙分析及戰術性介入系統」黑名單更新或ScamShield推廣，不但觸及率廣、速度快，也幾乎能覆蓋所有年齡層。如此高密度的上網人口，讓政府得以把防詐宣導教材及自學課程放在網路上，而不必擔心民眾會有資訊落差。

同時，實名化的數位個人身分，已發出逾450萬組帳號，涵蓋約97%的公民及永久居民人口。這代表從報稅、醫療，至開立銀行帳戶、註冊電子錢包等，都繫於同一把「數位鑰匙」。在法律上，新修訂《電腦濫用法》以第8A、8B條將「出租或濫用數位個人身分」直接入罪，為警方鎖定協力者提供明確方向。

此外，PayNow即時轉帳服務已成為新加坡轉帳的單一平台，數位化之金流可輕易追蹤溯源，銀行的12小時冷卻期與警方的凍結指令才有制度與技術的落實空間。換言之，在高度數位化之金融環境裡，防詐訊息可以直接傳達到民眾手機裡的應用程式、網銀QR碼介面，政府與業者所需的執行成本遠低於仍依賴現金的社會環境。

三、高信任度社會與守法文化

2024年度「艾德曼信任晴雨表」[81]顯示，新加坡民眾對政府的信任度高達77%，在

80 “Digital 2024: Singapore.” DataReportal – Global Digital Insights, 21 Feb. 2024, https://datareportal.com/reports/digital-2024-singapore.

81 「艾德曼信任晴雨表」（Edelman Trust Barometer）是一項由國際公關公司艾德曼（Edelman）自2001年起每年發布的全球信任度調查，主要透過問卷方式，衡量公眾對政府、企業、非政府組織（NGO）、媒體等四大機構的信任程度，並分析不同國家與地區的變化趨勢。

全球28個受訪國家中位居第四[82]，顯示政府在公共議題上的專業與廉潔形象獲得高度肯定。

這份「結構性信任」首先體現在對強制性防詐措施的支持上。新加坡政府近年推出的限制令（凍結帳戶）及「12 小時冷卻期」等強制延遲轉帳要求，雖然直接影響民眾取款之便利性，卻鮮少在社會輿論中遭到強烈反彈；多數銀行亦都能落實金融管理局推動「共同責任架構」中有關冷卻期與即時交易警示之規定，顯示對政府的高信任度大幅降低政策推行的困難度[83]。

同樣的信任感亦提升民眾「共同防詐」的參與度。如官方研發的ScamShield應用程式下載量已突破百萬次；用戶主動回報可疑來電、簡訊與連結，使系統可在後端快速標記並封鎖新的詐騙號碼與網站。再加上政府技術局與警察部隊共同運作的「詐騙分析及戰術性介入系統」，這些來自民眾的第一手回報資訊可為AI模型提供即時訓練數據，形成政策、科技及民眾共同合作的正向循環。

四、金融體系集中、易於監管

新加坡的零售金融市場高度集中，僅星展銀行、華僑銀行及大華銀行三家本地銀行，即可覆蓋大多數存款與支付需求。政府並透過政策目標，維持銀行至少50%以上為本地住戶存款佔比，以確保系統穩定並降低監理難度84。再加上金融管理局同時兼具中央銀行與金融監理機關的雙重身分，使政策指令能在單一窗口快速執行。

以政令施行為例，金融管理局與新加坡銀行公會於2024年7月宣布將於三個月內全面淘汰一次性簡訊密碼，改以裝置綁定的數位憑證進行驗證，藉此封堵釣魚網站竊取簡訊碼之風險。三大本地銀行皆於統一時程內完成系統改版與用戶教育，正是市場集中與監管直接的綜合成果。

此外，行政規範亦與執法體系緊密銜接。自2020年《支付服務法》生效後，任何提供跨境匯款、電子錢包或數位支付代幣服務的業者，都須取得金融管理局執照並遵守客戶盡責調查及反洗錢交易監測要求；違規即可能遭到吊銷執照或高額罰款。2025年6月，金融管理局便依《支付服務法》規範對5家支付機構裁罰共96萬新幣，理由包括未充分過濾受益帳戶持有人與缺乏即時監控機制，顯示監管者可透過執照與罰鍰雙軌，強制業者與警方系統對接，第一時間舉報偵查可疑金流。

五、數位競爭力與創新氛圍

82 2024 Edelman Trust Barometer, p. 42

83 “At a Glance: Duties of Telcos and Banks under Singapore’s Scam Liability Framework.” The Straits Times, 24 Oct. 2024, https://www.straitstimes.com/singapore/at-a-glance-duties-of-telcos-and-banks-under-singapores-scam-liability-framework

84 Chan Jia Hui and Elaine Chan, “In Brief: Ownership and Acquisition of Banks in Singapore.” Lexology, 11 Mar. 2025, https://www.lexology.com/library/detail.aspx?g=4d5d89ba-7918-47fc-b3ce-ef8826c373c3

新加坡在瑞士洛桑管理學院「2024世界數位競爭力排名」所有受評鑑的67個全球經濟體中脫穎而出，高居全球第1；該報告特別指出其「人才儲備」、「法規框架」及「資訊科技整合」等評選指標中皆名列第一85。這代表星國科研與技術專業人才充沛，政府能在智慧財產及資訊治理方面提供明確且友善的制度支撐，形成厚實的創新後盾。

在此堅實基礎上，新加坡每年仍透過「智慧國家」計畫投入逾30億新幣的公共資通訊基礎建設預算，用以提升全國網路安全及促進公私合作86。這些助力也推動政府科技局開發了「詐騙分析及戰術性介入系統」，利用遞迴式機器評分引擎，每日可過濾十萬個網址並自動標記詐騙網站；除1799反詐熱線外，ScamShield網站則以聊天機器人即時分流民眾求助需求。這些工具讓法規、執法與民眾服務得以同步升級，減少人力浪費，同時增強反詐成效及量能。

六、公私協力與社區動員文化

新加坡自1960年代以來即推行「三方合作」：政府、企業與工會共同決策與執行公共議題。政府將此模式視為國家的關鍵競爭優勢，強調用非對抗、協商的方式追求公共利益與經濟發展，同時培養企業對政策配合的高度默契87。

這種結構性的安排，使金融業成為防詐協力的第一線。新加坡三大本地銀行（星展、華僑及大華）不僅各自成立24小時監控部門，還把員工直接派駐至警方的反詐指揮處，與執法人員共同即時追蹤可疑交易、凍結帳戶與追回款項。類似的合作也延伸到電商與網路平台，如蝦皮、Meta、旋轉拍賣等業者也都派員進駐指揮處，充分展現星國公私協力的優良傳統。

在三方合作的文化背景下，跨機構合作由臨時專案性質進化為常態制度：企業派駐專員、即時資料交換與快速下架流程皆已內化為日常運作模式。這種高度自動化、低摩擦的合作結構，正是新加坡能夠面對詐騙威脅持續升級時，仍能保持高效率應對及社會高度信任政府的重要因素之一。

85 IMD World Digital Competitiveness Ranking 2024, p. 40

86 “FY24: Government to Spend More than $3B to Modernise ICT Infrastructure and Develop Digital Services.” Government Technology Agency (GovTech), accessed 10 Aug. 2025, https://www.tech.gov.sg/media/fy24-government-to-spend-more-than-3b-on-infrastructure-and-digital-services/

87 “What Is Tripartism. “Singapore’s Ministry of Manpower” , accessed 10 Aug. 2025, https://www.mom.gov.sg/employment-practices/tripartism-in-singapore/what-is-tripartism

圖26、新加坡防詐經驗總結

資料來源：駐新加坡代表處繪製