

從英國因應數位詐騙線上平台變革 論我國相關措施之精進

歐陽廣、羅俊瑋

摘 要

本文深入剖析英國應對數位詐騙之法制變革，藉此檢視我國防詐政策之結構性困境與精進之道。隨生成式人工智慧（GenAI）與數位生態系統演進，詐騙已質變為具產業化特徵之國家安全威脅。英國經驗顯示，僅賴產業「自律」性質之《防範線上詐欺憲章》顯有不足，遂轉向具有法律強制力之《線上安全法》，確立平台業者對「系統性風險」之主動預防義務，並透過全球營收百分比罰鍰與高階管理人刑事責任，建構嚴格之監管框架。反觀我國，雖推動「打詐國家隊」並制定專法，惟當前仍面臨關鍵阻斷條款未施行、跨部會協調阻滯及司法懲詐效能不彰等「政策失調」與「執行斷層」之挑戰。本文主張，我國應借鏡英國「強制監管」思維，盡速施行針對網路廣告平台之流量管理措施，並建議修法改採以「全球營收」計算之罰鍰機制、整合監管權限設立單一專責機構，以及增訂高階經理人未盡防詐義務之刑事責任。藉由強化平台業者之法律歸責性，從結構面阻斷詐騙產業鏈，以完善我國數位治理法制。

關鍵字：英國、防詐政策、防範線上詐欺憲章、線上安全法、強制監管、平台責任、詐騙服務化

壹、前言

隨生成式人工智慧（GenAI）與數位科技的發展，詐騙犯罪已升級為具跨國性、產業化特徵的系統性國家安全威脅。經考察英國經驗，認為僅靠產業「自律」與自願性協議不足以對抗數位詐騙，其須轉向「強制監管」；且英國將平台作為「系統性風險」之一進行考量，引入高達全球營收 10% 的罰鍰與高階管理人刑事責任，成功建立主動預防的成果。

本文認為我國應盡速施行針對網路廣告平台的流量管理與阻斷措施，並可參酌改採以「全球營收百分比」計算之罰鍰機制、整合監管權限並設立專責機構，以及增訂高階經理人因過失未履行防詐義務之刑事責任，藉從結構面阻斷詐騙產業鏈。

貳、英國「詐騙流行病」之困境

一、詐騙威脅國家安全

英國之國民較其他國家而言係相對富裕，該國並建置有完善支付系統，曾因「詐騙流行病」（fraud epidemic）¹ 侵襲而困擾不已。其於聯合國第 16 屆《打擊跨國有組織犯罪公約》² 技術援助工作組提出相關數據指出，詐騙犯罪占英國所有犯罪 43%³（每 14 名年滿 16 歲者就有 1 人成為受害者）⁴、高達 80% 的詐騙案件為網路犯罪⁵，且近三分之二的成年人曾成為網路詐騙的目標⁶。另經分析，70% 的詐騙案件具跨國性⁷，其中 30% 係由位於海外的犯罪者實施⁸，顯示詐騙犯罪已高度「國際分工化」。因此吾人似得推論詐騙犯罪

《註 1》Kathryn Westmore, 2023/11/16, Fraud: The Emergence of a UK Epidemic, Royal United Services Institute, <https://www.rusi.org/explore-our-research/publications/commentary/fraud-emergence-uk-epidemic>, last visited: 22 Oct. 2025.

《註 2》United Nations Convention against Transnational Organized Crime.

《註 3》HM Government, 2025/05, UK Government's approach to Fraud, https://www.unodc.org/documents/treaties/WG_TA_2025/presentations/CTOC_WGTA_UK_presentation_-_criminalisation_of_fraud.pdf, last visited: 29 Oct. 2025.

《註 4》National Crime Agency (UK), Fraud, <https://www.nationalcrimeagency.gov.uk/threats-2025/nsa-fraud-2025?highlight=WyJmcmF1ZCJd>, last visited: 22 Oct. 2025.

《註 5》HM Government, *Supra* note 3.

《註 6》*Id.*

《註 7》*Id.*

《註 8》House of Commons Justice Committee (UK), Fraud and the Justice System, 2022/10/11, Fourth Report of Session 2022-23, p.6, <https://committees.parliament.uk/publications/30328/documents/175363/default/>, last visited: 23 Oct. 2025.

在英國，甚或其他各國已非單純的治安問題，其或可能已演變為系統性的國家安全威脅。

有認為英國原先應對詐騙案件的措施係「政策失調」(policy mismatch)⁹所致，即一個於 21 世紀以技術驅動之無國界犯罪，正衝撞著一個於 20 世紀以屬地管轄為基礎，並各自為政的執法體系。英國警察基金會 (The Police Foundation) 在其 2024 年所發布的《線上詐騙剖析》(“The anatomy of online fraud”) 亦曾提及，英國警方在應對線上犯罪時「舉步維艱」，係因為執法結構的「碎片化」及過度依賴受害者報案的「被動運作模式」¹⁰ 足以得見。於現今 70% 的犯罪源於境外，傳統的在地警務模式在打擊犯罪源頭時或有力不從心之感。此等結構性的失能，與其說是警務工作的失敗，不如說是「政策真空」，這種真空迫使英國政府必須尋找傳統警力之外的全新干預點。

英國政府為審慎應對犯罪率占比日

漸攀升且具跨國性的詐騙，自 2023 年 5 月起推動並執行《反詐騙策略》(“Fraud Strategy”)，以「追捕詐騙者」(如推動成立統一事權的執法單位「國家反詐騙小組」及擴大國際合作¹¹)、「阻斷詐騙」(如推動《線上安全法》(“Online Safety Act”, OSA) 的立法及建立《防範線上詐欺憲章》(“Online Fraud Charter”) 促進平台責任機制¹²) 與「賦能公眾」(如提供防詐教育及強化受害者補償機制¹³) 等策略，期將詐騙案的數量降低 10%¹⁴。

二、威脅的演變——從網路釣魚到生成式人工智慧

這場詐騙流行病的獨特性不僅在於其規模巨大，更在於威脅的演變速度；即詐騙者利用網路數位生態系統的特性——匿名性和加密技術，助長其「隱匿身分進行犯罪活動」，使執法部門難以追查¹⁵。當前詐騙手法，依英國警察基金會之報告可歸納為如下三大類：

《註 9》Nicholas Ryder, 2025/11/20, Successive UK governments keep failing on fraud – and the problem is only getting worse, The conversation, <https://doi.org/10.64628/AB.euqr9gwna>, last visited: 25 Nov. 2025.

《註 10》Michael Skidmore, 2024/04, The Anatomy of Online Fraud, The Police Foundation, p.8-9, https://www.police-foundation.org.uk/wp-content/uploads/2010/10/perspectives_online_fraud.pdf, last visited: 23 Oct. 2025.

《註 11》HM Government, Fraud Strategy: Stopping Scams and Protecting the Public, 2023/05, p.14-25.

《註 12》HM Government, *Supra* note 11 at 26-36.

《註 13》HM Government, *Supra* note 11 at 37-42.

《註 14》HM Government, *Supra* note 11 at 3.

《註 15》Michael Skidmore, *Supra* note 10 at 8.

（一）利用社會關係與線上欺詐

此類型利用人類心理弱點，如網路釣魚（phishing，即指駭客利用電子郵件來騙取使用者或企業資訊的社交工程技巧）和情感詐騙（romance fraud）¹⁶。

（二）與個人資訊有關之犯罪

此類型以外洩的個人資訊進行非法利用進而獲利，如「無卡交易」（card-not-present）詐欺¹⁷。

（三）駭客攻擊

此類型採惡意軟體或入侵個人帳戶以獲取數據，作為身分盜用的切入點¹⁸。

從前揭英國政府的「反詐騙策略」可知，當前威脅或僅係冰山一角。詐騙者正濫用「尖端技術」，特別是「人工智慧大型語言模型」（如 ChatGPT、Bing 和 Bard）製造出史無前例更具說服力的詐騙通訊、電子郵件和語音通話¹⁹，令受害者在不知情之情況下受害。此外，Bottomline²⁰ 與

Themis²¹ 合作調查北美和英國 90 多名銀行專業人士後所發布的《2025 年詐騙趨勢》（“Themis 2025 Fraud Trends”）報告中顯示，逐日高升的詐騙威脅實質影響經濟層面，茲說明如下：

1. 營運成本與詐騙數量提升呈正相關

超過四分之一的調查受訪者認為，2024 年至少有 10% 的銀行運營損失歸因於欺詐。此外，50% 的受訪者表示，其服務之銀行在 2024 年欺詐案件大幅增加²²。

2. AI 使詐騙威脅加劇及巨額損失

50% 的受訪者認為，以生成式人工智慧進行詐欺是 2025 年對銀行之最大威脅，其中基於深度偽造的詐欺在多種類型案件出現之頻率愈來愈高。近 40% 的受訪者認為，合成身分（Synthetic identities）詐欺將成為 2025 年對銀行構成最嚴重之威脅，凸顯此等技術在生物識別驗證協議帶來的複雜挑戰²³。

而生成式人工智慧除被用於執行更複雜的網路釣魚、惡意軟體外²⁴，亦增

《註 16》*Id.*

《註 17》*Id.*

《註 18》*Id.*

《註 19》HM Government, *Supra* note 11 at 11.

《註 20》總部位於英國，提供金融科技解決方案的軟體公司。

《註 21》總部位於英國，協助企業識別和管理金融犯罪風險的公司。

《註 22》Themis/Bottomline, 2025, *Fraud Trends 2025*, p.4, <https://www.wearethemis.com/uk/resources/publications/fraud-trends-2025>, last visited: 8 Apr. 2025.

《註 23》Themis/Bottomline, *Supra* note 22 at 6.

《註 24》Themis/Bottomline, *Supra* note 22 at 19-20.

加兩種詐騙類型的威脅度——「帳戶盜用」(Account Takeover, ATO)²⁵和「商業電子郵件入侵」(Business Email Compromise, BEC)²⁶。這兩種詐騙類型，使美國在2023年分別損失近130億美元及29億美元，後者更使全球損失達67億美元，為消費者遭受詐騙總損失的15%²⁷。

三、詐騙即服務——「企業化」和「服務化」

前揭報告指出，「詐騙服務化」(Fraud-as-a-Service, FaaS)²⁸模式的興起，即不肖集團開發專為執行欺騙的工具以供詐騙者購買使用，使缺乏經驗的潛在犯罪者也能輕鬆發動複雜攻擊，這使得80%以上的案件與FaaS有關²⁹。如FaaS的興起，代表詐騙「服務化」讓詐騙更像產業鏈，而模組化攻擊套組(Modular attack kits，指網路釣魚工具、外洩之用戶資料、洗錢服務或帳戶接管服務等)則讓詐騙操作規模

化，而致成「企業化」之趨勢³⁰。

犯罪「企業化」，意味打擊策略必須從追捕個別詐騙者，轉向打擊「犯罪的賦能者」，因此英國政府除從打擊詐騙基礎設備著手，自2025年4月起以立法方式成為歐洲第一個禁止國民持有或供應SIM卡農場³¹(SIM farms，即集中大量SIM卡並透過稱為「貓池」的伺服器進行大規模簡訊發送或撥打電話的設備)的國家。其針對電信公司、金融機構，以及最重要的——社群媒體採取全方位應對，而《防範線上詐欺憲章》便是這場新戰略的第一槍。

參、防範線上詐欺憲章

一、《2023年反詐騙策略》的政策產物

前揭英國《反詐騙策略》中最優先之工作即為與科技公司達成新的《防範線上詐欺憲章》³²，其被視為至關重要的原因，

《註 25》Themis/Bottomline, *Supra* note 22 at 27-28.

《註 26》Themis/Bottomline, *Supra* note 22 at 29-30.

《註 27》*Id.*

《註 28》Themis/Bottom line, *Supra* note 22 at 42.

《註 29》Kennedy Meda, 2025/02/21, Fraud-as-a-Service: Creating a new breed of fraudsters, Thomson Reuters, <https://www.thomsonreuters.com/en-us/posts/corporates/faas-new-fraudsters/>, last visited: 26 Oct. 2025.

《註 30》Amy Lurie & Tomer Naor, 2025/07/16, Top Fraud Trends for 2024-2025, AU10TIX, <https://www.au10tix.com/blog/top-fraud-trends-for-2024-2025/>, last visited: 26 Oct. 2025.

《註 31》HM Government, 2025/04/24, Major step for fraud prevention with landmark ban on SIM farms, <https://www.gov.uk/government/news/major-step-for-fraud-prevention-with-landmark-ban-on-sim-farms>, last visited: 6 Oct. 2025.

《註 32》HM Government, *Supra* note 11 at 29.

在於犯罪者濫用尖端 AI 技術使威脅不斷增長。本憲章核心目標是確保所對應的「每個部分」，特別是「產業界」得以嚴肅態度因應詐騙³³。

《防範線上詐欺憲章》的訂定為英國政府高層意志的展現，其係在內政部（Home Office）和唐寧街 10 號（No.10 Downing Street，即現英國首相官邸，常為英國首相之代稱）的共同努力下，與科技產業密切談判達成的。在經歷六個月詳細討論後，這份文件最終於 2023 年 11 月 30 日，由時任內政大臣 James Cleverley 主持的儀式上正式簽署³⁴。

二、自願性的盟約：公私部門的夥伴關係

《防範線上詐欺憲章》係作為公私部門夥伴關係的「自願性協議」（Voluntary agreement）³⁵。全球科技產業巨頭均將簽

署這份憲章內容，包含亞馬遜（Amazon）、eBay、Google（含 YouTube）、Meta（含 Facebook 及 Instagram）、LinkedIn、Match Group、微軟（Microsoft）、Snap Inc.、TikTok 及 X（前 Twitter）等³⁶。從該憲章所載引言可知，其目的係為讓關鍵科技公司認知「橫行於其平台的詐騙活動所致的金融剝削對英國公眾構成的風險，並承諾致力解決相關議題」，同時也展示其與政府合作的雄心和意願³⁷。

英國政府採取由私部門自願參與的策略，乃反映當時的政治現實。首先，應對詐騙危機需要立即展現行動，而《防範線上詐欺憲章》從策略提出（2023 年 5 月）到簽署（2023 年 11 月）僅用六個月即達成，這只有在「自願」而非「強制立法」的前提下始得以實現³⁸。而憲章的問世，使當時保守黨政府能迅速召開新聞發布會，宣稱在「反詐戰爭」中取得重大勝利，英國也成為世界上第一個採取行動對抗線

《註 33》*Id.*

《註 34》TechUK, 2023/12/01, Leading the Charge Against Fraud: techUK Works to Deliver New Online Fraud Tech Charter, <https://www.techuk.org/resource/leading-the-charge-against-fraud-techuk-works-to-deliver-new-online-fraud-tech-charter.html>, last visited: 28 Oct. 2025.

《註 35》HM Government, 2023/11/30, Online Fraud Charter 2023 (accessible), <https://www.gov.uk/government/publications/online-fraud-charter-2023/online-fraud-charter-2023-accessible#definitions>, last visited: 28 Oct. 2025.

《註 36》*Id.*

《註 37》*Id.*

《註 38》Douglas Blakey, 2023/11/30, Online Fraud Charter: UK government claims world first agreement to tackle online fraud, Retail Banker International, <https://www.retailbankerinternational.com/news/uk-launches-online-fraud-charter-with-11-large-tech-firms/?cf-view>, last visited: 29 Oct. 2025.

上詐騙的國家³⁹。

其次，憲章旨在界定產業可接受的最低行動標準⁴⁰，其內容充滿「合作性」的語言，並採用許多平台已在進行的防詐作為，且未設定懲罰機制。其係產業為對即將到來並有更嚴厲的強制性法規（即《線上安全法》）採取的策略性妥協⁴¹。

三、《防範線上詐欺憲章》的內容

《防範線上詐欺憲章》的核心是關鍵平台同意採取應對線上詐騙的具體化行動，其分為九部分，故有將其稱為「九大承諾」（Nine Commitments），簽署者將按其商業模式戮力施行⁴²。按《防範線上詐欺憲章》之九大承諾及其行動針對所有公司依其特性訂有不同行動需求，彙整如下頁表 1：

《防範線上詐欺憲章》的九大承諾之第

4 項「廣告」為最具關鍵性和爭議性，因為它要求平台主動驗證廣告商身分，特別是交叉核對金融行為監管局的授權名單，這實質上讓平台自願承擔部分金融監管角色⁴⁵。在此之前，科技平台作為中立管道對廣告內容無負擔事先審核義務。此項承諾代表科技產業的重大妥協，很可能是當時為換取即將實施的《線上安全法》中的更寬鬆條款，或至少展現合作意願，以影響未來監管之架構。

此外，第 5 項「執法」與第 6 項「情報分享」類於警務功能「外包」的現象，因為在國家執法機構承認其反應遲緩且資源短缺的背景⁴⁶，本憲章要求擁有全球數據資源、即時監控技術及先進 AI 偵測系統的科技平台，承擔第一線的犯罪偵測責任。當然，這項設計連結私部門的技術

《註 39》HM Government, 2023/11/30, World first agreement to tackle online fraud, <https://www.gov.uk/government/news/world-first-agreement-to-tackle-online-fraud>, last visited: 29 Oct. 2025.

《註 40》UK Parliament, 2023/12/18, Written evidence submitted by techUK, <https://committees.parliament.uk/writtenevidence/126140/html/>, last visited: 30 Oct. 2025.

《註 41》Helena Wood, 2023/11/09, The Online Safety Act: Landmark legislation on online fraud, Cifas, <https://www.cifas.org.uk/insight/fraud-risk-focus-blog/online-safety-bill-landmark-legislation>, last visited: 31 Oct. 2025.

《註 42》HM Government, *Supra* note 35.

《註 43》Financial Conduct Authority, FCA.

《註 44》HM Government, *Supra* note 35.

《註 45》Financial Conduct Authority, 2025/02/07, FCA steps up action against misleading financial adverts, <https://www.fca.org.uk/news/press-releases/fca-steps-action-against-misleading-financial-adverts>, last visited: 31 Oct. 2025.

《註 46》Rasha Kassem, Umut Turksen, “Beyond resources: understanding police attitudes to fraud and the barriers to prioritisation”, *Policing: An International Journal*, Vol.49, Issue 1, 2026, p.8-9.

表 1 《防範線上詐欺憲章》之九大承諾及對應

序號	承諾名稱	詳細描述
1	阻擋 (Blocking)	所有公司 簽署者應設置檢測措施並阻擋潛在的詐騙材料，如確保反詐騙作為列入營運條款、標記並移除可疑內容和帳戶，及提供符合國家網路安全中心建議的登入方式，並鼓勵用戶採用兩步驟驗證。 獨立的線上約會平台 簽署者應提供驗證措施，用戶理解他們是與真人互動，並允許用戶選擇只與經過驗證者互動。 社群媒體及用戶可直接交換資訊 (Peer-to-Peer, P2P) 進行交易的社群 簽署者應提供交易指引以提升使用者對潛在高風險交易的認知。 電商、社群媒體及用戶可直接交換資訊 (Peer-to-Peer, P2P) 進行交易的社群 簽署者應提供賣家驗證和安全支付機制。
2	報告 (Reporting)	所有公司 簽署者應負提供簡易且迅速報告途徑的義務，以利用戶通報詐騙材料、盡速處理用戶的申訴、為執法機關及可信賴夥伴設立專屬的直接報告流程及指導用戶向執法單位或銀行舉報詐騙事件。 社群媒體 簽署者應於未知用戶聯繫用戶時，標示潛在詐騙風險的提示。 獨立的線上約會平台 簽署者應發送警報給曾與已被通報為詐騙警示戶互動之用戶，並提供其教育資源。
3	移除 (Takedowns)	所有公司 簽署者應立即刪除詐騙內容，對涉嫌詐騙的用戶採取及時且適當的行動與建立恢復受害用戶帳戶的機制。
4	廣告 (Advertising)	所有公司 簽署者應保護公眾免受詐騙廣告之侵害。 付費廣告平台 簽署者應設置針對新投放者的驗證機制、確認英國金融服務公司經金融行為監管局⁴³授權、辨識廣告內嵌連結導向網站之合法性，及承諾用戶可以在廣告頁面點擊兩次內瞭解平台的反詐騙機制。
5	執法 (Law enforcement)	所有公司 簽署者應設立專門聯絡人以回應執法機關之請求，提供必要資訊以支持調查，並於執法單位有需求時提供培訓或借調人員予執法單位。
6	情報分享 (Intelligence sharing)	所有公司 簽署者應與國家網路安全中心 (NCSC)、資訊專員辦公室 (ICO)、執法單位及產業夥伴合作並參與快速分享詐騙情報之計畫，內容包含分析內外部資料以識別及預防詐騙與分享案例。

7	透明度 (Transparency)	所有公司 簽署者應提供平台具有詐騙風險之資訊，以及相應之應對措施。
8	溝通 (Comms)	所有公司 簽署者應提供公眾迅速辨識並避免受線上詐騙的簡易措施，如持續向用戶傳達詐騙風險。
9	前瞻性評估 (Horizon scanning)	所有公司 簽署者應評估自有平台和服務於應對頂尖技術時是否存在技術漏洞，並預先設置干預點以阻止詐騙遂行。

資料來源：《防範線上詐欺憲章》之九大承諾⁴⁴。

優勢與公部門的執法權力，建立更高效率之合作管道，從而彌補公共資源的不足⁴⁷。

四、《防範線上詐欺憲章》的缺失

(一)「自願性」造成的阿基里斯之踵⁴⁸

就《防範線上詐欺憲章》有認為其自願性即為缺點，即其認為國家政策的《反詐騙策略》過度依賴自願性措施為不可行，而且從「歷史上看，自願主義從來

不是改善社群媒體安全的有效策略」⁴⁹。英國保險業協會⁵⁰也表達同樣的擔憂，其論及憲章的「自願性……不足以促使 (incentivise) 這些公司立即採取減少其平台上發生詐騙的行動」⁵¹。英國國防與安全智庫——皇家聯合研究所⁵²則指出，考量憲章施行後，仍有三分之二的授權轉帳詐欺源自網路，而不得不認為這份自願憲章僅具「遮羞布」之作用⁵³。

《註 47》City of London Police, 2023/11/30, City of London Police welcomes Government's Online Fraud Charter, <https://www.cityoflondon.police.uk/news/city-of-london/news/2023/november/city-of-london-police-welcomes-governments-online-fraud-charter/>, last visited: 31 Oct. 2025.

《註 48》按希臘神話之延伸，阿基里斯之踵即指弱點。

《註 49》Clean Up The Internet, 2024/01/10, Written evidence submitted by Clean Up The Internet, p.13, <https://committees.parliament.uk/writtenevidence/125734/pdf/>, last visited: 1 Nov. 2025.

《註 50》Association of British Insurers, ABI.

《註 51》Jonathan Purvis, 2024/09/27, Change? How the new government can show it's serious about tackling fraud, Association of British Insurers, <https://www.abi.org.uk/news/blog-articles/2024/9/change-how-the-new-government-can-show-its-serious-about-tackling-fraud/>, last visited: 1 Nov. 2025.

《註 52》Royal United Services Institute, RUSI.

《註 53》Helena Wood, 2024/05/23, Tackling the Silent Threat of Fraud: Amplifying the UK's Response, Royal United Services Institute, <https://www.rusi.org/explore-our-research/publications/commentary/tackling-silent-threat-fraud-amplifying-uks-response>, last visited: 1 Nov. 2025.

（二）金融業與科技業的利益衝突

就《防範線上詐欺憲章》自願性質的批評，不僅源於公共安全考量，更反映英國兩大經濟支柱——金融業與科技業間之利益衝突，即雙方責任分配不均衡⁵⁴。其引爆點涉及受害者被誘導自願轉帳，長期處於監管灰色地帶的授權推送支付（Authorised Push Payment, APP）之詐騙類型。此類詐騙因具備「消費者自行授權」的特性，使銀行常據此主張免責，或因舊有的「自願守則」（CRM Code）對過失認定標準不一，導致補償成效有限⁵⁵。然自 2024 年 10 月 7 日起施行的新規定「快速支付系統補償規則」（FPS Reimbursement Rules）徹底扭轉此一局勢，確立了「強制補償」原則⁵⁶。按財團法人金融消費評議中心主任委員羅俊瑋教授於詳細研究該

機制後即指出⁵⁷，依據新規，銀行及其他支付服務提供者（PSPs）被強制要求在收到通報後的五個工作日內（例外可延長至三十五個工作日），返還至高 85,000 元英鎊予 APP 詐騙受害者⁵⁸。更具關鍵性的是，新制引入「責任分攤機制」，規定由「付款銀行」與「收款銀行」各承擔 50% 的賠償責任⁵⁹。此機制旨在利用財務壓力，迫使金融機構（特別是過往責任較輕的收款行）必須更積極地利用科技偵測異常交易與人頭帳戶，以從源頭阻斷詐欺金流。相較於金融業面臨如此嚴格的強制賠償與技術升級壓力，科技業者目前仍僅受自願性憲章約束，此更加凸顯兩大產業間在防詐責任與成本分擔上的顯著落差。

據英國金融協會（UK Finance）報告指出，2025 年上半年詐騙損失額達 6.293 億英鎊，並以 APP 詐騙居多⁶⁰，這代表金

《註 54》Helena Wood, 2025/01/31, From words to action: The outlook on fraud in the UK in 2025, Cifas, <https://www.cifas.org.uk/insight/fraud-risk-focus-blog/uk-fraud-outlook-2025>, last visited: 1 Nov. 2025.

《註 55》羅俊瑋、符懋佑，〈英國金融詐欺補償制度對我國之啓示〉，《存款保險資訊季刊》，第 38 卷，第 2 期（2025 年 6 月），頁 36-47。本文對於英國金融詐欺補償制度有較為充分之說明與討論，讀者可進一步就此自行參閱。

《註 56》Payment Systems Regulator (UK), Deadlines for firms, <https://www.psr.org.uk/our-work/app-scams/deadlines-for-firms/>, last visited: 1 Nov. 2025.

《註 57》羅俊瑋、符懋佑，同《註 55》，頁 36-37。

《註 58》Payment Systems Regulator (UK), 2024/10/07, APP fraud reimbursement protections, <https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections>, last visited: 1 Nov. 2025.

《註 59》羅俊瑋、符懋佑，同《註 55》，頁 45。

《註 60》UK Finance, 2025/10/24, Half Year Fraud Report 2025, <https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/half-year-fraud-report-2025>, last visited: 1 Nov. 2025.

融業或因「待歸還損失」而有可觀的潛在負債。此外，約 70% 的 APP 詐騙源於線上平台（如社群媒體和搜尋引擎）並導致 29% 的損失額⁶¹，凸顯科技業在詐騙傳播中的角色。

這種明顯的不平衡局面使得金融業（以銀行業為首）深感此乃不公平之情事⁶²，即金融業受強制規定約束，須為詐騙損失「買單」，包括退款及相關合規成本。然而作為詐騙源頭（廣告和假帳戶來源）的科技業，卻僅受自願性且缺乏強制執行機制的憲章約束。

是以金融遊說團體如英國保險業協會（Association of British Insurers, ABI）即紛紛呼籲英國政府加速審查憲章進展，以藉此迫使科技業提高防詐層級⁶³。來自金融業的強大遊說壓力，已成為推動英國政府超越憲章、轉向更嚴格立法的關鍵因素，例如延遲發布的國家詐騙策略預計將強化對科技業的監管⁶⁴。

（三）《防範線上詐欺憲章》為《線上安全法》的銜接協議

英國政府或許自始即未將《防範線上詐欺憲章》定位為終極解決方案，而視其為「政策性橋梁」。即在《線上安全法》經歷其冗長且爭議之立法與實施程序期間，將憲章作為穩定公共秩序與承諾金融產業需求的協議⁶⁵，此設計表現立法者對時效性之考量，更反映出在數位治理領域，公權力如何透過自願協議鋪設強制規範之基礎。

英國保險業協會的公開聲明即論及：「《線上安全法》將強化消費者保護，惟該等措施需時始能生效，故《防範線上詐欺憲章》將在此過渡期間擔任關鍵角色（an important role）⁶⁶」。此不僅確認憲章之暫時性質，更凸顯其作為法規施行前的緩衝機制。因此從立法角度觀察，或許《防範線上詐欺憲章》並非一項「政策失誤」，而

《註 61》UK Finance, 2025/05/28, Fraud continues to pose a major threat with over £1 billion stolen in 2024, <https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2025-press-release>, last visited: 2 Nov. 2025.

《註 62》Eleanor Myers, 2025/10/22, Banks furious as UK shies away from making Big Tech pay for fraud, Politico, <https://www.politico.eu/article/keir-starmer-big-tech-banks-fraud/>, last visited: 2 Nov. 2025.

《註 63》UK Parliament, 2024/01/10, Written evidence submitted by the Association of British Insurers, p.2-3, <https://committees.parliament.uk/writtenevidence/125834/pdf/>, last visited: 2 Nov. 2025.

《註 64》Francesca Washtell & John Crowley, 2025/11/03, Publication of UK fraud strategy pushed back to next year, The Banker, <https://www.thebanker.com/content/be64a19d-2eb0-4587-af88-ce97ec691412>, last visited: 4 Nov. 2025.

《註 65》Helena Wood, *Supra* note 41.

《註 66》Jonathan Purvis, *Supra* note 51.

為精湛的「立法策略操作」，宛若「立法特洛伊木馬（Legislative Trojan Horse）」，透過看似溫和的自願協議，但卻可達成如下關鍵之目的：

1. 建立原則

政府使科技巨頭公開承諾與遵守其監管原則⁶⁷，如主動審查廣告商身分並對照金融行為監管局之授權名單，縱其為自願性質的承諾，卻為後續的法規解釋或將之轉化為法規提供基礎。

2. 建立基準

憲章為政府樹立「政策基準線」，即允許其援引金融業及倡議團體對自願性之批評⁶⁸，順勢主張「鑑於自願措施未能充分激勵產業，現須將這些已獲產業原則同意之原則，轉化為《線上安全法》下之強制性義務」。此舉不僅得以化解政治阻力，更強化立法之正當性。

最終，簽署憲章的科技業已在《線上安全法》針對細項的談判上，明顯喪失關鍵談判籌碼，因為其已經原則上同意自己有責任審核平台上的詐騙資訊⁶⁹，從而難以抗拒接受更嚴格的法定義務。

肆、自願性協議到具法律強制力的法規

一、《線上安全法》

在眾多科技龍頭簽署憲章的前一個月，英國立法機關早已完成真正的補強，即為保護兒童與成人線上安全而設計的《線上安全法》。本法於 2023 年 10 月 26 日獲得英國政府批准而正式成為法律，並由英國通訊管理局（Office of Communications, Ofcom）作為獨立監管機構辦理相關作為。線上安全法與憲章的問世時序至關重要，前者於 10 月 26 日生效，而科技巨頭則於 11 月 30 日簽署後者（這證明憲章的從屬地位）。即英國政府先是通過強制性法規，再拿著這把槍（違規者將受 1,800 萬英鎊或全球營收 10% 的罰款⁷⁰）「邀請」科技業簽署「自願」的憲章，而科技業為在即將到來的執法細則中爭取有利條件，只好「自願」合作。因此，科技業實質上是在 Ofcom 的強制細則正式施行前，提前履行 OSA 的核心原則（即憲章的九大承諾），以向監管機關展示善意，並試圖影響未來細則的制定。

《註 67》HM Government, *Supra* note 35.

《註 68》Jonathan Purvis, *Supra* note 51.

《註 69》陳穎萱，2024/05，〈英國與 13 家科技公司簽署《防範線上詐欺憲章》，建立網際網路防詐之重要里程碑〉，財團法人資訊工業策進會科技法律研究所，<https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9171>，最後瀏覽日期：2025 年 11 月 12 日。

《註 70》Latham & Watkins, 2024/08/19, UK Online Safety Act 2023, p.2, <https://www.lw.com/admin/upload/SiteAttachments/UK-Online-Safety-Act-2023.pdf>, last visited: 1 Nov. 2025.

二、從「被動反應」到「主動預防」

線上安全法被視為是對《防範線上詐欺憲章》的根本性補強，其主要在於實現監管典範的轉移，從傳統被動模式（即平台僅在接到通知後才需移除非非法內容，無須主動干預）轉向主動預防（即要求平台自主作為以保護用戶因非法內容受害）⁷¹。

此為一種全新的風險管理模型，因為平台必須進行風險評估，並主動緩解其服務被用於犯罪的風險⁷²，其可避免總是等到傷害達到危機點才進行立法干預的被動局面，從而建立更有效的預防機制，強化整體數位安全治理。

三、將「詐欺廣告」定為非法內容

線上安全法得以較完整填補《防範線上詐欺憲章》在「詐欺」議題上的法律空白⁷³。即線上安全法賦予平台新的法定職責，要求受規範的網路服務提供者（如

社群媒體、搜尋引擎）識別、減輕並管理非法內容所帶來的風險，且採取適當措施防止其傳播並迅速移除⁷⁴。有關非法內容載於第 59 條，其規範則在同法之附表 7（“Schedule 7”），包含《2006 年詐欺法》（“Fraud Act 2006”）相關規定，如虛假陳述詐欺、製造或供應用於詐欺的物品及參與獨資經營者等經營的詐欺業務等。

其次，則是最關鍵的線上安全法第五章，其針對大型「使用者對使用者」平台服務提供者及大型「搜尋引擎」⁷⁵，就「詐欺廣告」分別課予各種具體義務及提供相關詐欺廣告定義。針對大型「使用者對使用者」平台服務提供者，其義務有三項⁷⁶：

- （一）防止個人透過該服務接觸到包含欺詐性廣告的內容。
- （二）盡量縮短任何此類內容存在的時間。
- （三）若服務提供者接獲任何人對此類內容存在的通報，或以其他方式察覺其存

《註 71》Nath Solicitors, 2023/10/26, Top Ten FAQs on the Online Safety Bill: An In-Depth Analysis, <https://www.nathsolicitors.co.uk/2023/10/26/top-ten-faqs-on-the-online-safety-bill/>, last visited: 2 Nov. 2025.

《註 72》John Woodhouse, 2025/02/25, Research Briefing: Implementation of the Online Safety Act, House of Commons Library, <https://commonslibrary.parliament.uk/research-briefings/cdp-2025-0043/>, last visited: 2 Nov. 2025.

《註 73》HM Government, 2025/04/24, Online Safety Act: explainer, <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>, last visited: 4 Nov. 2025.

《註 74》Legislation (UK), 2023, Online Safety Act 2023, <https://www.legislation.gov.uk/ukpga/2023/50>, last visited: 4 Nov. 2025.

《註 75》Legislation (UK), 2025, The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025, <https://www.legislation.gov.uk/ukdsi/2025/9780348267174>, last visited: 4 Nov. 2025.

《註 76》Legislation (UK), *Supra* note 74, § 38.

在，則須迅速移除該內容。

而針對大型「搜尋引擎」亦有其三項重要義務⁷⁷，即：

- (一) 防止個人於該服務的搜尋結果或透過該服務的搜尋結果接觸到包含詐騙廣告。
- (二) 若該服務的搜尋結果或透過該服務的搜尋結果可能接觸到任何此類內容，則儘量縮短此種情況持續的時間。
- (三) 若服務提供者接獲任何人對可能接觸到相類內容事實的通報，或以其他方式察覺該事實，則須迅速確保個人不再能夠於該服務的搜尋結果或透過該服務的搜尋結果接觸到相類內容。

綜上，可將網路服務提供者的防詐騙義務精簡為三項要旨，即為「預防用戶接觸詐騙廣告」、「最短化詐騙廣告存在期」及「迅速移除該類廣告」，相關條款等於是

將《防範線上詐欺憲章》中關於廣告的「自願承諾」（如核實 FCA 授權），原封不動地轉化為具有法律強制力的法定義務⁷⁸。

有別於憲章的寬鬆設計，線上安全法排除業者可自行衡量「核實成本」與「廣告收益」而導致執行落差與利益衝突的可能性，且課予業者必須將詐騙廣告視為「系統性風險」並導入管理層面的法定義務⁷⁹。據分析，Ofcom 將平台出現詐騙廣告一事視為「平台審核機制的失靈」而非「內容錯誤」⁸⁰，故監管機關得以藉此審查平台的廣告商上架流程、驗證機制與其演算法設計，監管焦點亦從「廣告本身」轉向「允許該廣告出現的平台系統」，展現出更深入且技術導向的監管模式⁸¹。此等制度轉型提升平台的法律責任，也反映英國政府在數位治理上由「自律」向「法制」的根本性轉變。

《註 77》Legislation (UK), *Supra* note 74, § 38.

《註 78》HM Government, 2022/03/08, Major law changes to protect people from scam adverts online, <https://www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online>, last visited: 4 Nov. 2025.

《註 79》Ofcom, 2022/07/06, Online Safety Bill: Ofcom's roadmap to Regulation, P.15, <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/roadmap/online-safety-roadmap.pdf?v=328170>, last visited: 5 Nov. 2025.

《註 80》Alexandros Antoniou & Lorna Woods, 2025/06/13, Advertising and the Online Safety Act 2023, p.10-11, https://www.onlinesafetyact.net/documents/564/Advertising_and_the_Online_Safety_Act_2023.pdf, last visited: 5 Nov. 2025.

《註 81》Ofcom, 2024/12/16, Online Safety Enforcement Guidance, p.12-16, <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/online-safety-enforcement-guidance.pdf?v=391925>, last visited: 5 Nov. 2025.

四、Ofcom 的執法權力

線上安全法不僅提供平台防止詐騙義務的法律依據，其更賦予 Ofcom 各種強制性執法工具，包含：

（一）資訊權與調查權

Ofcom 擁有強制的資訊請求權，可要求平台提供其行使職能所需的資訊。Ofcom 亦可啟動調查，並有權訪談相關人員、進入場所、進行檢查與「演算法審計」⁸²。

（二）處違規者高額金融罰鍰

Ofcom 有權對違規公司處以高達 1,800 萬英鎊或其全球年營收 10% 的罰鍰（以較高者為準）⁸³。此機制顯然是針對大型跨國科技公司所設計，使其面臨潛在的重大財務損失，則公司將因違規成本遠高於合規成本，從而提供強大的法律遵循動機。

（三）追究違規者窗口的刑事責任

每一受規範公司均須指派一位高階經理人擔任窗口確保該公司作為合規，若 1. 服務提供者實體犯下特定罪行（如未遵守通報要求或提供虛假資訊）；且 2. 該窗口未能採取所有合理步驟防止該罪行發

生，則將面臨刑事究責⁸⁴。此條款將責任從公司擴展至個人，透過使高階經理人在特定情況下將面臨個人刑事責任之風險，從而提高企業內部的問責性。

（四）發出改善令或要求強制作為

Ofcom 可在發現違規行為後對違規公司發出改善令，且可針對改善期限屆滿後未改善者，要求該公司採取指定作為（如要求使用特定類型的主動預防技術）以改正其違規行為⁸⁵。

（五）中斷業務權

Ofcom 可於經法院同意後採取「服務限制」或「訪問限制」措施，即 Ofcom 可要求其他網路服務供應商、支付服務商或廣告商停止為違規平台提供服務，實質上阻斷其在英國的營運⁸⁶。

（六）連帶責任

Ofcom 的執法權可擴及受規範公司集團內的其他實體，或對該公司具有重大影響力的「控制人」，以確保問責之全面性⁸⁷。

綜上，英國的策略採取雙軌並進，其先以《防範線上詐欺憲章》作為自願性舉措，聚焦產業合作原則，隨後透過《線上安全法》建立強制性法律架構，並賦予

《註 82》Latham & Watkins, *Supra* note 70 at 14.

《註 83》*Id.*

《註 84》*Id.*

《註 85》*Id.* at 15.

《註 86》*Id.*

《註 87》*Id.*

Ofcom 一系列強大監管工具(從系統審核、高額罰款至高階經理個人責任)以彌補自願協議的固有局限。

伍、我國「打詐國家隊」的現況與挑戰

一、2025 年的政策失調與執行斷層

我國近年來亦面臨嚴峻的詐騙犯罪挑戰，為此行政院於 2022 年 7 月 15 日訂頒「新世代打擊詐欺行動綱領」，以「識詐」(宣導及公眾教育)、「堵詐」(防堵資通犯罪工具)、「阻詐」(阻截詐騙贓款)及「懲詐」(懲追詐騙集團)四大面向⁸⁸遏制詐騙。而為精進四大面向期使全面降低詐騙事件，更於 2023 年 5 月通過「新世代打擊詐欺策略行動綱領 1.5 版」⁸⁹(下稱綱領 1.5 版)，運用公私協力推動各項防詐作為，達成「減少接觸，減少誤信，減少損害」三減目標，更於 2024 年 11 月再通過新增「防詐」面向的打詐綱領 2.0 版⁹⁰。

然而，截至 2025 年 11 月 15 日，我國的打詐行動仍有政策失調與效能危機之疑慮。

據立法院公報資料顯示，我國 2025 年前七個月因詐騙損失總額高達 565.5 億元，一舉超越 2024 年整年詐騙損失總額計 502 億元⁹¹(惟財損數據之顯著攀升，與內政部警政署為強化報案流程及數據整合以降低「犯罪黑數」而於 2024 年 12 月 1 日推出之「165 打詐儀表板」之措施仍有一定關聯)，此資訊證實平均每日遭詐騙 2 至 3 億元的嚴峻事實。然行政院在同場會議卻提出，若以《詐欺犯罪危害防制條例》公布施行後的第一個月對比最新一個月的數據，則詐騙案受理件數實則下降 22.5%，財物損失實則下降 37.7%。根據全球防詐聯盟(Global Anti-Scam Alliance, GASA)、Whoscall 與 ScamAdviser 攜手發布的《2025 亞洲詐騙調查報告：台灣篇》更揭露我國 72% 成年人在 2024 年曾遭遇詐騙，且 61% 更因詐騙遭致財物損失⁹²。

《註 88》中華民國法務部，2022/07/15，〈新世代打擊詐欺策略行動綱領〉，頁 12，<https://www.moj.gov.tw/media/26646/%E6%96%B0%E4%B8%96%E4%BB%A3%E6%89%93%E6%93%8A%E8%A9%90%E6%AC%BA%E7%AD%96%E7%95%A5%E8%A1%8C%E5%8B%95%E7%B6%B1%E9%A0%98.pdf?mediaDL=true>，最後瀏覽日期：2025 年 11 月 5 日。

《註 89》中華民國行政院，2023/05/17，〈新世代打擊詐欺策略行動綱領 1.5 版〉，<https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/d6bb7d87-3e54-44ca-a4ad-3f11d329338d>，最後瀏覽日期：2025 年 11 月 5 日。

《註 90》中華民國行政院，2024/11/28，〈新世代打擊詐欺策略行動綱領 2.0 版〉，<https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/c93637bd-ddc2-4447-8829-246a5ca0befc>，最後瀏覽日期：2025 年 11 月 5 日。

《註 91》中華民國立法院，《立法院公報》，第 114 卷，第 71 期，2025 年 8 月，頁 185。

《註 92》GASA, State of Scams in Taiwan 2025 Report, Global Anti-Scam Alliance, p.8, <https://www.gasa.org/research>, last visited: 17 Nov. 2025.

此看似矛盾的資訊，揭示政府「政治敘事」與「危機現實」之間的巨大鴻溝。當前的挑戰，本文認為應係源於三大系統性失能：其一是關鍵法律的「分階段施行」困境，其二是跨部會「五大支柱」協作阻滯，最後則是司法體系在「懲詐」環節上的結構性無力。

（一）「分階段施行」的防詐困境

首於 2024 年 7 月 31 日三讀通過的《詐欺犯罪危害防制條例》被視為「打詐國家隊」的核心法律武器，然而其在執行層面卻存在「分階段施行」所導致策略性挑戰。即涉及網路平台前端用戶 KYC（用戶身分核對及留存）於同年 11 月 30 日施行，使其配套子法（即《電信事業使用指定資料庫核對用戶身分查詢辦法》）亦同時生效。但在後端攔阻、針對網路廣告平台業者的干預工具（第 39 條第 2 至 5 項及第 40 條第 1 項第 6 款）的施行日期卻待行政院定之⁹³。

這使得要阻斷我國 75% 詐騙發生在具備「直接訊息功能」的平台一事⁹⁴有如緣木求魚，且毋寧為政府手持新通過的法律利器，卻選擇將其束之高閣，凸顯立法與

行政部門在打詐策略上的協調落差。

（二）五大支柱協作阻滯

「新世代打擊詐欺行動綱領 2.0」建立一個由五大部會分工的跨部會作戰體系，彙整如下頁表 2。

我國打詐策略自 2022 年 7 月訂頒「新世代打擊詐欺策略行動綱領 1.0 版」起，即確立「識詐、堵詐、阻詐、懲詐」四大面向，分別由內政部、國家通訊傳播委員會、金融監督管理委員會、法務部分別統籌，再於 2023 年 5 月推出 1.5 版延續四大面向架構，並於 2024 年升級為 2.0 版及於同年 7 月三讀通過《詐欺犯罪危害防制條例》，建立「識詐、堵詐、防詐、阻詐、懲詐」五大支柱架構。

然而，作為打詐國家隊，主責政策協調、情資研判、統計分析、涉詐金流通報及涉詐平台通報等關鍵任務的核心幕僚機關「詐欺犯罪防制中心」，在實際運作上卻因「工作量因各項重大計畫推進而倍增」，然而「中心仍屬任務編組，缺乏穩定人力與法定職掌，難以支撐迅速擴張的偵防需求」⁹⁵（詐欺犯罪防制中心於 2025 年 11

《註 93》全國法規資料庫，2024/07/31，《詐欺犯罪危害防制條例》，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=D0080226>，最後瀏覽日期：2025 年 11 月 6 日。

《註 94》GASA, *Supra* note 92 at 13.

《註 95》中華民國內政部警政署刑事警察局，2025/11/28，〈詐欺犯罪防制中心法制化啓航 跨部會合作、公私協力再升級〉，<https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1887&serno=ec05985f-e77c-4906-835a-50416dd85dae>，最後瀏覽日期：2025 年 11 月 30 日。

表 2 五大部會打擊詐欺行動分工

面向	主辦機關
識詐	內政部
堵詐	國家通訊傳播委員會
防詐	數位發展部
阻詐	金融監督管理委員會
懲詐	法務部

資料來源：行政院新世代打擊詐欺策略行動綱領2.0版。

月 7 日完成法制化修正發布並生效實施，不僅從臨時編組升級為常設法制單位擴大組織編制，亦新設詐欺偵查隊⁹⁶，標誌政府對該系統性失能的重大制度改革。雖此改革值得稱慶，惟本文認為雖然詐防中心完成法制化，但該改革的實際成效仍有待後續觀察。法制化本身雖解決組織編制與人力資源的結構性困境，但跨部會協調的深層問題仍須透過配套的業務流程改善與文化調整才能真正克服）。

其次則是資訊整合與情資共享機制闕如，即縱打詐綱領明定建立 165 反詐騙資料庫、金融資料線上平台、虛擬通貨 AI 分析平台等數位工具，但各部會資料格式不一、調閱程序冗長、回覆時間延宕等問題持續存在，使得跨部會協作淪為紙上談兵⁹⁷。以上顯示五大支柱在協作流暢度有

極大改善空間。

（三）懲詐失靈導致的低犯罪成本

司法體系作為打詐策略「懲詐」面向的最後防線，卻呈現結構性的懲罰無力，使詐騙犯罪淪為「高獲利，低風險」的投資保障。此困境具體展現在量刑輕刑化、緩刑比率過高，以及執行效能不彰三大層面。

首先，根據審計部 113 年度中央政府總決算審核報告，據司法院統計自 2019 至 2024 年（截至 8 月底止）各級法院依刑法第 339-4 條之「加重詐欺罪」處之刑期多未及三年，處三年以上刑期者均低於 5%，亦即每千名詐欺犯中僅不到 5 人被判處相對較重刑期⁹⁸。此種量刑分布嚴重偏離立法意旨，使得法律規定的「加重」效果形同虛設。

《註 96》劉建邦，2025/11/28，〈刑事局詐防中心法制化啟航 新設偵查隊專責打詐〉，中央社，<https://www.cna.com.tw/news/asoc/202511280106.aspx>，最後瀏覽日期：2025 年 11 月 30 日。

《註 97》中華民國審計部，《112 年度中央政府總決算審核報告》，第 2 冊，頁丙 332 至 337。

《註 98》中華民國審計部，《113 年度中央政府總決算審核報告》，第 2 冊，頁丙 148 至丙 150。

其次，緩刑比率過高削弱嚇阻效果。2017 至 2021 年詐欺罪案件裁判確定有罪 6 萬 9,741 人中，判處有期徒刑六月以下者占 43% 最多⁹⁹。由於我國刑法規定，六個月以下有期徒刑得易科罰金，二年以下有期徒刑且具備法定條件者得宣告緩刑，導致大量詐騙犯獲得緩刑或易科罰金，無須實際入監服刑，忽略詐欺犯罪的組織性與再犯風險。

再者，執行面的結構性問題亦使懲詐環節形同虛設，因為《詐欺犯罪危害防制條例》雖然將詐欺刑度提高至最重十二年，並提高假釋門檻，擴大不法利得沒收範圍，但這些規定在司法實務運作中效果有限。一方面，辦案困難導致多數被捕者為車手、提供帳戶的幫助犯等基層成員，真正的集團首腦與幕後金主難以緝捕。另一方面，即便查獲集團成員，贓款追回率極低，被害人財物損失難以填補。而法務部雖建置全國反電信詐騙資料庫、查調金融資料 AI 分析平台等工具，但調閱金融資料程序冗長、虛擬通貨追查困難等問題持續存在¹⁰⁰，使得「懲詐」效能大打折扣。

二、針對數位經濟之關鍵防詐規定

為有效阻斷他人利用網路廣告平台從

事詐欺造成不特定多數人受害，《詐欺犯罪危害防制條例》於第三章「數位經濟防詐措施」訂有明確規範，其核心架構可歸納為下列四大重點：

（一）平台管理與在地代表（第 27-31 條）

要求具一定規模之網路廣告平台須設置「法定代表」，以利我國司法文書送達與緊急聯絡，並落實用戶身分核對（KYC）。

（二）廣告審核與快速下架（第 32-34 條）

網路廣告須標示資助者資訊，若內容涉及投資或虛擬資產，業者須負事前審查義務；經通報為詐騙廣告者，業者應於二十四小時內下架，否則須負損害賠償責任。

（三）異業協作與免責機制（第 35-38 條）

明訂第三方支付、電商、網路遊戲業者應建立疑似詐騙帳號之預警機制。為鼓勵民間參與，法律賦予業者配合執行攔阻時之民事免責權。

（四）行政罰鍰與技術封鎖（第 39-42 條）

主管機關對違規業者可處最高 2,500 萬元罰鍰；情節重大者，得採取封鎖網域等干預手段。

《註 99》中華民國立法院，《議案關係文書》，第 11 屆第 3 會期第 5 次會議，院總第 20 號，委員提案第 11009501 號。

《註 100》中華民國審計部，《113 年度中央政府總決算審核報告》，第 2 冊，頁丙 339 至丙 340。

陸、結論與建議

綜上之討論，本文提出以下數點之建議：

一、自願主義的局限與強制監管的必要性

英國從 2023 年的自願性《防範線上詐欺憲章》到同年強制性《線上安全法》的政策框架演進，堪稱全球數位治理的典範轉變，凸顯產業自願自律承諾的本質局限性，無法強迫數位平台優先消滅詐騙而放棄其龐大廣告收益。

實證評估顯示，儘管主要科技公司承諾偵測、報告並迅速移除詐騙內容，但次年仍有 74% 的詐騙受害者在簽署平台如 Facebook、Google 及 Amazon 上遭遇詐騙¹⁰¹，此凸顯自願措施無法打破廣告驅動模式下的既得利益。相較之下，《線上安全法》對平台施加具約束力的義務，包括風險評估、主動減輕詐騙風險及移除非內容，從而透過監管強制彌補這些缺失。

據此，我國於 2024 年選擇跳過與產業龍頭簽署公示的自願性協議階段，直接制定《詐欺犯罪危害防制條例》，此一策略決定在法律上堪稱審慎且合理，與英國轉向強制規範的軌跡相符。該條例要求金

融機構、電信業者及大型線上廣告平台實施全面反詐措施，包括廣告主身分驗證、迅速移除欺瞞內容，以及源頭預防策略以阻斷詐騙於萌芽階段——這些規定呼應英國《線上安全法》的風險導向義務。

然而，英國經驗同時揭示一項關鍵警示，即單靠立法不足以奏效，尚須強化執行架構及罰則設計。是以該法賦予 Ofcom 作為獨立監管機構調查權力，並得對不遵守的平台課以高達其全球營收 10% 或 1,800 萬英鎊的罰鍰，乃至對高階主管追究刑事責任，此舉證明強制的法律義務在促使遵守方面至關重要，而專責監督機構亦有助確保抑制數位欺騙的效能。

二、對我國防詐政策的具體建議

基於上述對英國經驗的分析，茲對我國防詐策略提出以下六點具體政策建議：

（一）盡速施行關鍵未竟條款

英國《線上安全法》的核心在於強制平台承擔系統性攔阻義務，而我國對應的網路攔阻機制（詐欺犯罪危害防制條例第 39 條第 2 至 5 項有關流量管理措施、停止解析與限制接取處置部分）迄今尚未全面施行，導致執法處於「法律真空」狀態，無法有效應對跨國數位威脅。故建議行政

《註 101》Ash Strange, 2024/12/18, A Year On from the Online Fraud Charter, which?, <https://www.which.co.uk/policy-and-insight/article/a-year-on-from-the-online-fraud-charter-aeFbu4h2Pre8>, last visited: 17 Nov. 2025.

院應盡速公告有關措施的施行日期，賦予數位發展部必要的法律工具，終結當前權責不對等的執法困境，從而提升整體防詐效能。

（二）採納「營收百分比罰款」機制，取代固定罰款

英國《線上安全法》的 10% 全球營收罰款模式，已成為國際科技監管的典範，能有效突破巨型平台的經濟抗性。相較之下，我國現今施行法條有關網路平台業者僅可能面對最高 2,500 萬元的固定罰款，對全球營收達數千億美元的科技公司而言，此或僅屬微不足道的「營運成本」，無法產生足夠的驅動力。故建議我國於未來修法程序可考慮對具重大影響力的境外平台增訂罰鍰條款，且其上限應為其「全球年度總營收」的特定百分比，以確保違規後果與平台規模相稱。

針對在我國無分支機構之具規模境外平台，現行法雖要求其指定境內法律代表以執行防詐義務，然若平台拒不指定，僅憑罰鍰之行政處分，其震懾力恐未若「停止解析」（封網）或「限制接取」等阻斷經營手段。為彌補此執行漏洞，爰如前段，建議行政院應盡速公告有關措施之施行日期，避免法律代表制度淪為空談。

（三）採單一監管機構

英國的成功經驗在於賦予 Ofcom 獨立、資源充足且權力集中的監管角色，避免碎片化執法。然而我國實務已顯示，原

訂之「五大支柱」的多部會模式已導致協調失靈與數據孤島，削弱司法效能。

考量數位詐騙仍屬普通犯罪之延伸，爰建議仍以防制犯罪更為熟稔之內政部警政署為核心權責單位更為妥適，並採調撥分散於各部會之平台管控單位合組為一組織；甫於 2025 年 11 月 28 日法制化之詐欺犯罪防制中心即與此概念相似，如進一步賦予其類似 Ofcom 的單一監管權力，或可提高其整合跨部門數據與執法資源之治理效率。

（四）增訂「高階經理人個人責任」條款

英國政府正確洞察企業常將罰鍰（款）視為營運成本，而高階經理人的個人刑事責任才是轉變企業文化的關鍵槓桿。故建議在《詐欺犯罪危害防制條例》中增訂「高階經理人責任」條款，明確規定若平台因未盡「善良管理人」之履行防詐義務，其指定之高階經理人應承擔相應的刑事責任，以從內部驅動平台的主動合規。

（五）調整線上平台之監管焦點

我國《打詐專法》側重「內容管理」，要求網路平台驗證廣告商身分並移除詐騙廣告，屬「廣告監測」邏輯。惟英國《線上安全法》則採取「安全設計」（Safety by Design）邏輯，以「系統與演算法」為核心強制業者落實風險評估並主動調整演算法，從源頭防止非法內容觸及用戶。相較已產生詐騙風險之事後移除，建議得採事

前防制之監管作為。

(六) 建立強制補償詐騙受害者之機制

建議推動金融機構對詐騙受害者之「強制補償機制」(Mandatory Reimbursement)，於確認受害者無重大過失之前提下，由金融業者先行負擔部分賠償責任。此機制旨在將防詐義務「內化」

為金融機構之核心風險控管指標，透過經濟誘因驅使金融業者從被動協查轉為主動防禦。

全球實務顯示，反詐治理乃是一場與犯罪科技賽跑的制度競賽，如未能同步強化金融賠付責任、數位平台治理義務及跨部門聯防，現有制式作為將難以應對詐欺犯罪之演化速度。

(本文作者歐陽廣為中正大學法學院法律碩士、羅俊瑋為中正大學法律學系教授)

參考文獻

中文

一、期刊論文

羅俊瑋、符懋佑，〈英國金融詐欺補償制度對我國之啟示〉，《存款保險資訊季刊》，第 38 卷，第 2 期，2025 年 6 月，頁 31-65。

二、網路資料

中華民國內政部警政署刑事警察局，2025/11/28，〈詐欺犯罪防制中心法制化啟航 跨部會合作、公私協力再升級〉，<https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1887&serno=ec05985f-e77c-4906-835a-50416dd85dae>，最後瀏覽日期：2025 年 11 月 30 日。

中華民國行政院，2023/05/17，〈新世代打擊詐欺策略行動綱領 1.5 版〉，<https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/d6bb7d87-3e54-44ca-a4ad-3f11d329338d>，最後瀏覽日期：2025 年 11 月 5 日。

中華民國行政院，2024/11/28，〈新世代打擊詐欺策略行動綱領 2.0 版〉，<https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/c93637bd-ddc2-4447-8829-246a5ca0befc>，最後瀏覽日期：2025 年 11 月 5 日。

中華民國法務部，2022/07/15，〈新世代打擊詐欺策略行動綱領〉，頁 12，<https://www.moj.gov.tw/media/26646/%E6%96%B0%E4%B8%96%E4%BB%A3%E6%89%93%E6%93%8A%E8%A9%90%E6%AC%BA%E7%AD%96%E7%95%A5%E8%A1%8C%E5%8B%95%E7%B6%B1%E9%A0%98.pdf?mediaDL=true>，最後瀏覽日期：2025 年 11 月 5 日。

全國法規資料庫，2024/07/31，《詐欺犯罪危害防制條例》，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=D0080226>，最後瀏覽日期：2025 年 11 月 6 日。

陳穎萱，2024/05，〈英國與 13 家科技公司簽署《防範線上詐欺憲章》，建立網際網路防詐之重要里程碑〉，財團法人資訊工業策進會科技法律研究所，<https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9171>，最後瀏覽日期：2025 年 11 月 12 日。

劉建邦，2025/11/28，〈刑事局詐防中心法制化啓航新設偵查隊專責打詐〉，中央社，<https://www.cna.com.tw/news/asoc/202511280106.aspx>，最後瀏覽日期：2025 年 11 月 30 日。

三、政府文書

中華民國審計部，《112 年度中央政府總決算審核報告》，第 2 冊，頁丙 332 至丙 337。

中華民國審計部，《113 年度中央政府總決算審核報告》，第 2 冊，頁丙 148 至丙 150、頁丙 339 至丙 340。

中華民國立法院，《立法院公報》，第 114 卷，第 71 期，2025 年 8 月，頁 185。

中華民國立法院，《議案關係文書》，第 11 屆第 3 會期第 5 次會議，院總第 20 號，委員提案第 11009501 號。

英文

一、網路資料

Alexandros Antoniou & Lorna Woods, 2025/06/13, Advertising and the Online Safety Act 2023, p10-11, https://www.onlinesafetyact.net/documents/564/Advertising_and_the_Online_Safety_Act_2023.pdf, last visited: 5 Nov. 2025.

Amy Lurie & Tomer Naor, 2025/07/16, Top Fraud Trends for 2024-2025, AU10TIX, <https://>

- www.au10tix.com/blog/top-fraud-trends-for-2024-2025/, last visited: 26 Oct. 2025.
- Ash Strange, 2024/12/18, A Year On from the Online Fraud Charter, Which?, <https://www.which.co.uk/policy-and-insight/article/a-year-on-from-the-online-fraud-charter-aefBu4h2Pre8>, last visited: 17 Nov. 2025.
- City of London Police, 2023/11/30, City of London Police welcomes Government's Online Fraud Charter, <https://www.cityoflondon.police.uk/news/city-of-london/news/2023/november/city-of-london-police-welcomes-governments-online-fraud-charter/>, last visited: 31 Oct. 2025.
- Clean Up The Internet, 2024/01/10, Written evidence submitted to Home Affairs Committee, <https://committees.parliament.uk/writtenevidence/125734/pdf/>, last visited: 1 Nov. 2025.
- Douglas Blakey, 2023/11/30, Online Fraud Charter: UK government claims world first agreement to tackle online fraud, Retail Banker International, <https://www.retailbankerinternational.com/news/uk-launches-online-fraud-charter-with-11-large-tech-firms/?cf-view>, last visited: 29 Oct. 2025.
- Eleanor Myers, 2025/10/22, Banks furious as UK shies away from making Big Tech pay for fraud, Politico, <https://www.politico.eu/article/keir-starmer-big-tech-banks-fraud/>, last visited: 2 Nov. 2025.
- Financial Conduct Authority, 2025/02/07, FCA steps up action against misleading financial adverts, <https://www.fca.org.uk/news/press-releases/fca-steps-action-against-misleading-financial-adverts>, last visited: 31 Oct. 2025.
- Francesca Washtell & John Crowley, 2025/11/03, Publication of UK fraud strategy pushed back to next year, The Banker, <https://www.thebanker.com/content/be64a19d-2eb0-4587-af88-ce97ec691412>, last visited: 4 Nov. 2025.
- GASA, 2025, State of Scams in Taiwan 2025 Report, Global Anti-Scam Alliance, <https://www.gasa.org/research>, last visited: 17 Nov. 2025.
- HM Government, 2022/03/08, Major law changes to protect people from scam adverts online, <https://www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online>, last visited: 4 Nov. 2025.
- HM Government, 2023/11/30, Online Fraud Charter 2023 (accessible), <https://www.gov.uk/government/publications/online-fraud-charter-2023/online-fraud-charter-2023-accessible#definitions>, last visited: 28 Oct. 2025.

- HM Government, 2023/11/30, World first agreement to tackle online fraud, <https://www.gov.uk/government/news/world-first-agreement-to-tackle-online-fraud>, last visited: 29 Oct. 2025.
- HM Government, 2025/04/24, Major step for fraud prevention with landmark ban on SIM farms, <https://www.gov.uk/government/news/major-step-for-fraud-prevention-with-landmark-ban-on-sim-farms>, last visited: 26 Oct. 2025.
- HM Government, 2025/04/24, Online Safety Act: explainer, <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>, last visited: 4 Nov. 2025.
- HM Government, 2025/05, UK Government's approach to Fraud, https://www.unodc.org/documents/treaties/WG_TA_2025/presentations/CTOC_WGTA_UK_presentation_-_criminalisation_of_fraud.pdf, last visited: 29 Oct. 2025.
- Helena Wood, 2023/11/09, The Online Safety Act: Landmark legislation on online fraud, Cifas, <https://www.cifas.org.uk/insight/fraud-risk-focus-blog/online-safety-bill-landmark-legislation>, last visited: 31 Oct. 2025.
- Helena Wood, 2024/05/23, Tackling the Silent Threat of Fraud: Amplifying the UK's Response, Royal United Services Institute, <https://www.rusi.org/explore-our-research/publications/commentary/tackling-silent-threat-fraud-amplifying-uks-response>, last visited: 1 Nov. 2025.
- Helena Wood, 2025/01/31, From words to action: The outlook on fraud in the UK in 2025, cifas, <https://www.cifas.org.uk/insight/fraud-risk-focus-blog/uk-fraud-outlook-2025>, last visited: 1 Nov. 2025.
- House of Commons Justice Committee (UK), Fraud and the Justice System, 2022/10/11, Fourth Report of Session 2022-23, p6 <https://committees.parliament.uk/publications/30328/documents/175363/default/>, last visited: 23 Oct. 2025.
- John Woodhouse, 2025/02/25, Research Briefing: Implementation of the Online Safety Act, House of Commons Library, <https://commonslibrary.parliament.uk/research-briefings/cdp-2025-0043/>, last visited: 2 Nov. 2025.
- Jonathan Purvis, 2024/09/27, Change? How the new government can show it's serious about tackling fraud, Association of British Insurers, <https://www.abi.org.uk/news/blog-articles/2024/9/change-how-the-new-government-can-show-its-serious-about-tackling->

fraud/, last visited: 1 Nov. 2025.

Kathryn Westmore, 2023/11/16, Fraud: The Emergence of a UK Epidemic, Royal United Services Institute, <https://www.rusi.org/explore-our-research/publications/commentary/fraud-emergence-uk-epidemic>, last visited: 22 Oct. 2025.

Kennedy Meda, 2025/02/21, Fraud-as-a-Service: Creating a new breed of fraudsters, Thomson Reuters, <https://www.thomsonreuters.com/en-us/posts/corporates/faas-new-fraudsters/>, last visited: 26 Oct. 2025.

Latham & Watkins, 2024/08/19, UK Online Safety Act 2023, <https://www.lw.com/admin/upload/SiteAttachments/UK-Online-Safety-Act-2023.pdf>, last visited: 1 Nov. 2025.

Legislation (UK), 2023, Online Safety Act 2023, <https://www.legislation.gov.uk/ukpga/2023/50>, last visited: 4 Nov. 2025.

Legislatio (UK), 2025, The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025, <https://www.legislation.gov.uk/ukdsi/2025/9780348267174>, last visited: 4 Nov. 2025.

Michael Skidmore, 2024/04, The Anatomy of Online Fraud, The Police Foundation, https://www.police-foundation.org.uk/wp-content/uploads/2010/10/perspectives_online_fraud.pdf, last visited: 23 Oct. 2025.

Nath Solicitors, 2023/10/26, Top Ten FAQs on the Online Safety Bill: An In-Depth Analysis, <https://www.nathsolicitors.co.uk/2023/10/26/top-ten-faqs-on-the-online-safety-bill/>, last visited: 2 Nov. 2025.

National Crime Agency (UK), Fraud, <https://www.nationalcrimeagency.gov.uk/threats-2025/nsa-fraud-2025?highlight=WyJmcmF1ZCJd>, last visited: 22 Oct. 2025.

Nicholas Ryder, 2025/11/20, Successive UK governments keep failing on fraud – and the problem is only getting worse, The conversation, <https://doi.org/10.64628/AB.euqr9gwna>, last visited: 25 Nov. 2025.

Ofcom, 2022/07/06, Online Safety Bill: Ofcom's roadmap to Regulation, p.15, <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/roadmap/online-safety-roadmap.pdf?v=328170>, last visited: 5 Nov. 2025.

Ofcom, 2024/12/16, Online Safety Enforcement Guidance, p.12-16, <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/online-safety-enforcement-guidance.pdf?v=391925>, last visited: 5 Nov. 2025.

- Payment Systems Regulator (UK), 2024/10/07, APP fraud reimbursement protections, <https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/>, last visited: 1 Nov. 2025.
- Payment Systems Regulator (UK), Deadlines for firms, <https://www.psr.org.uk/our-work/app-scams/deadlines-for-firms/>, last visited: 1 Nov. 2025.
- TechUK, 2023/12/01, Leading the Charge Against Fraud: techUK Works to Deliver New Online Fraud Tech Charter, <https://www.techuk.org/resource/leading-the-charge-against-fraud-techuk-works-to-deliver-new-online-fraud-charter.html>, last visited: 28 Oct. 2025.
- Themis/Bottomline, 2025, Fraud Trends 2025, <https://www.wearethemis.com/uk/resources/publications/fraud-trends-2025>, last visited: 8 Apr. 2025.
- UK Finance, 2025/05/28, Fraud continues to pose a major threat with over £1 billion stolen in 2024, <https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2025-press-release>, last visited: 2 Nov. 2025.
- UK Finance, 2025/10/24, Half Year Fraud Report 2025, <https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/half-year-fraud-report-2025>, last visited: 1 Nov. 2025.
- UK Parliament, 2023/12/18, Written evidence submitted by techUK, <https://committees.parliament.uk/writtenevidence/126140/html/>, last visited: 30 Oct. 2025.
- UK Parliament, 2024/01/10, Written evidence submitted by the Association of British Insurers, <https://committees.parliament.uk/writtenevidence/125834/pdf/>, last visited: 2 Nov. 2025.

二、政府文書

HM Government, Fraud Strategy: Stopping Scams and Protecting the Public, 2023/05.

三、期刊論文

Rasha Kassem, Umut Turksen, “Beyond resources: understanding police attitudes to fraud and the barriers to prioritisation”, *Policing: An International Journal*, Vol.49, Issue 1, 2026, p.8-9.

UK Online Platform Regulatory Reforms in Response to Digital Fraud: Proposals for Enhancing Taiwan's Relevant Measures

Ouyang, Kuang & Lo, Chun-Wei

Abstract

This article examines the UK's legal transition against digital fraud, offering insights for refining Taiwan's anti-fraud policies. Driven by the industrialization of fraud and GenAI, the UK shifted from the voluntary Online Fraud Charter to the mandatory Online Safety Act. This legislation imposes proactive prevention duties on platforms for "systemic risks" and establishes strict enforcement through fines based on global turnover and criminal liability for senior managers. Conversely, Taiwan's anti-fraud efforts suffer from "policy misalignment" and "implementation gaps," notably the delayed enforcement of key traffic management clauses and inadequate judicial sentencing. The article advocates that Taiwan mirrors the UK's mandatory approach: immediately enforce the law's platform blocking mechanisms; adopt a global revenue-based fine structure; and introduce criminal accountability for platform executives who neglect their preventive duties. This structural enhancement is essential for disrupting the fraud ecosystem and perfecting digital governance.

Keywords: United Kingdom, Anti-Fraud Policy, Online Fraud Charter, Online Safety Act, Mandatory Regulation, Platform Accountability, Fraud-as-a-Service (FaaS)