數位經濟防詐措施之策略與執行情形

羅文庭、林青嶔、黃雅萍、林俊秀
（數位發展部數位產業署專員、組長、副署長、署長）

近年詐欺手法快速演變，社群廣告、電商及第三方支付等數位管道已成為主要散布與金流路徑，傳統以單一部門或產業為主的防制模式，已無法有效因應。本文旨在說明數位發展部在應對新型詐騙的策略與成效，主要從「法律、技術、商業」三管齊下，未來亦將持續透過 AI 技術對抗深偽、整合情資匯流與智慧分析，並強化平臺監管與追蹤。

壹、前言－數位經濟下的新型挑戰

隨著網際網路與科技的普及，數位經濟已成爲國家經濟成長的重要動力。然而，數位化帶來的便利性，也讓詐欺活動得以快速變異與擴散，特別是結合了深度僞造（Deepfake）、AI 生成內容的詐騙手法，對民眾財產安全、社會信任及政府治理構成嚴峻挑戰。爲此，數位發展部（下稱數發部）從源頭防堵與產業賦能的角度，積極推動數位經濟環境下的防詐策略與具體執行措施。

貳、關鍵方針－結合科技與產業力量建構防詐「鐵三角」

數發部將從法律、技術及商業三管齊下持續推動防詐工作。法律面已完成詐欺犯罪危害防制條例（下稱詐防條例）立法並實施廣告實名制；技術面建置「網路詐騙通報查詢網」、導入物流隱碼、DNS RPZ 及政府專屬短碼簡訊等機制；商業面則結合企業社會責任與市場形象，透過防詐作爲提升品牌信任度與社會認同的手段，讓業者在投入防詐工作時，不僅符合法規要求，也能獲得正向商業利益。

另為有效應對不斷進化的詐欺犯罪型態，行政院於 114 年 1 月起實施新世代打擊詐欺策略行動綱領 2.0 版，除原有「識詐、堵詐、阻詐、懲詐」4 大面向架構外，新增「防詐」面向，強化數位經濟產業治理，數發部為「防詐」面向主政機關，聚焦數位經濟防詐措施為核心，以「防制網路詐騙廣告」、「遏止詐騙網站」、「建立政府專屬短碼簡訊發送機制」、「加強電商業者資安維護」、「防制第三方支付詐騙」、「防制遊戲點數成為詐騙工具」等六大策略著手，期能從數位經濟產業源頭防堵詐欺犯罪危害，降低詐騙受害事件，相關措施成效說明如下：

一、透過源頭防堵，從根本上減少民眾接觸詐騙廣告的機會

（一）「強化網路廣告平臺業者之實名認證」，要求業者應驗證委託刊播者及出資者之身分，並於廣告中揭露

1. 詐防條例納管數發部所轄之「網路廣告平臺業者」，係指透過網際網路平臺或版位，提供刊登或推播廣告之服務並收取對價，且為民眾接觸之廣告最終端網路平臺業者。數發部依詐防條例之授權，訂定《一定規模之網路廣告平臺計算基準》，據以評估「平臺被用於刊登詐騙廣告之風險」與「國內使用者占比」，納管網路廣告平臺業，包括 Google LLC（Google、YouTube）、LY Corporation（LINE）、Meta Platforms, Inc（Facebook、Instagram、Threads），以及 TIKTOK PTE. LTD.（TikTok）等 4 家業者共 7 個經營平臺。
2. 要求業者進行源頭管理提出防詐作為

(1) 落實「廣告實名制」

要求業者驗證委託刊播者和出資者的身分，避免有心人士冒用或假借他人身分以躲避追查，減少詐騙集團投放廣告，避免民眾因接觸廣告而遭受到詐騙的機會。

(2) 訂定及執行「詐欺防制計畫」，並發布「透明度報告」

要求業者持續關注實務上詐欺手法及風險之變化，主動實施預防、偵測、辨識及應對，訂定相應之詐欺防制計畫，依據最新詐騙實際手法之變化為因應。並定期公布透明度報告，讓公眾能知悉網路廣告平臺業者關於詐欺防制相關具體措施與實施情形。

(3) 詐騙廣告下架處理

檢警調單位或相關主管機關可通知業者下架詐騙廣告，減少詐欺廣告在平臺上的存續時間，降低民眾接觸到詐騙廣告的風險；經檢警調或主管機關通知後，業

者應於 24 小時內移除、限制瀏覽或停止播送詐騙廣告，如業者未依通知處理，將對業者開罰，如仍不改善，將按次處罰，促使業者配合。

3. 針對未納管之網路廣告平臺業者，數發部持續鼓勵並輔導業者採行適當之身分驗證機制，以降低投放詐欺網路廣告之風險，並持續關注實務上詐欺風險變化，以及網路廣告平臺業者規模之更迭，與詐騙目標轉移之可能性，檢討更新納管業者名單，降低詐欺廣告擴散及移轉。

（二）開發「網路詐騙通報查詢網」，即時通報，安心查詢

1. 爲防止詐騙集團利用網路廣告接觸民眾進行誘騙，數發部開發《網路詐騙通報查詢網》，並已於 114 年 5 月 15 日正式上線營運，透過民眾通報與 AI 偵測技術蒐集可疑網路廣告，由遭僞冒之公眾人物或主管機關協助驗證可疑廣告眞僞，並迅速通報網路廣告平臺業者下架涉及詐欺之網路廣告，並將處理進度公告於系統，以利社會大眾提高警覺。

2. 自 113 年 9 月 30 日至 114 年 9 月 30 日止，共有 34,413 位民眾下載使用，有 7,676 人使用 APP 通報過案件，總計通報了 345,731 則疑似詐騙訊息。其中 181,978 則經由被僞冒的公眾人物本人或主責的政府機關確認爲詐騙訊息，平均每個月有超過 1 萬則詐騙訊息經數發部通知要求下架。

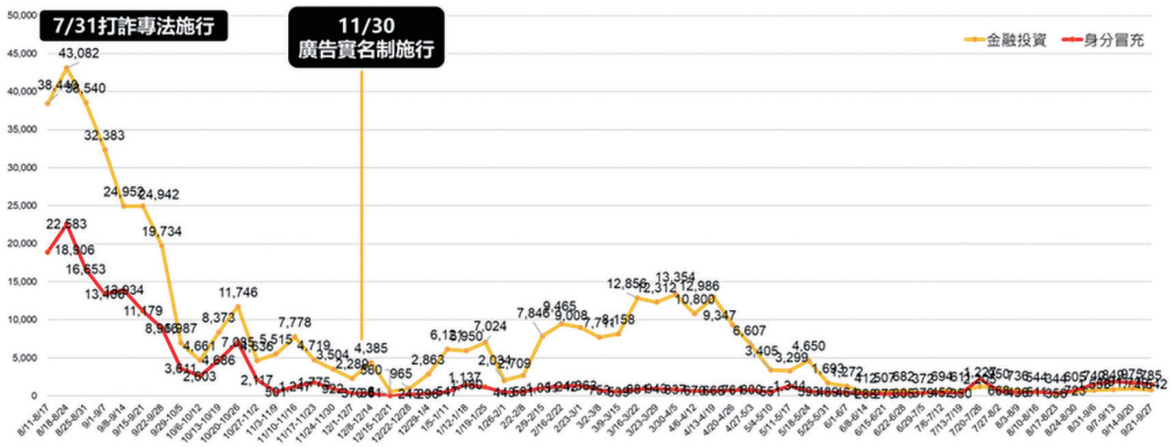
3. 整體高風險金融投資廣告掃獲案件數已自 113 年單週最高 77,484 件，下降至 114 年 9 月平均每週約 837 件，降幅達 99%。身分冒充詐騙廣告掃獲案件數已自 113 年單週最高 38,139 件，下降至 114 年 9 月平均每週約 1,685 件，降幅達 96%（圖 1）。

二、建立 DNS RPZ 機制，遏止詐騙網站

數發部督管之財團法人台灣網路資訊中心（TWNIC）基於服務其會員目的，已建立 DNS RPZ 自律機制停止解析惡意或不當的網域名稱，如各目的事業主管機關或司法警察機關依詐防條例第 42 條規定，令網際網路接取服務提供者（IASP）停止解析或限制接取，TWNIC 將協調加入 DNS RPZ 自律機制之 IASP，停止解析該網域名稱。經統計透過 DNS RPZ 自律機制攔阻詐騙網域件數，110 至 113 年共 6 萬 8,428 件、114 年截至 9 月底已攔阻 3 萬 9,949 件。

三、建立政府專屬短碼簡訊平臺，供政府部門發送簡訊

圖 1　詐騙廣告投放趨勢



資料來源：作者整理。

為提升政府簡訊識別度，避免有心人士偽冒政府簡訊詐騙民眾，數發部提供 111 政府專屬短碼簡訊服務，透過共同供應契約提供各機關（構）、公營事業等機關單位，如有簡訊業務需求之機關單位，可逕行採購使用。本項服務已有 500 個機關單位使用，114 年截至 9 月底累計發送逾 7,000 萬則簡訊。

四、加強電商業者資安維護

（一）因電商業者之經營特性，屬蒐集並保有大量消費者個人資料，在個資蒐集、處理、保存及利用的過程中，都有可能發生外洩風險。為提升電商業者對消費者個資保護及資安防護的重視，並落實個人資料保護以維護民眾隱私，數發部積極強化與電商業者的聯繫及督導，具體作為包含持續辦理行政檢查、資安技術輔導及法制宣導，相關作為已大幅強化電商業者個資法遵及資安意識，自 112 年 10 月至 114 年 9 月底，內政部警政署於 165 全民防騙網中所公告之高風險賣場名單中，已無數發部主管之大型電商業者，辦理成果如下：

1. 舉辦資訊安全課程活動

強化網路服務相關從業人員資安風險意識、個資法遵及其資安技能。自 111 年 8 月 27 日成立迄 114 年 9 月底止共舉辦 8 場。

2. 輔導業者進行資安技術性檢測

針對網站及主機弱點等進行檢測，輔導業者持續強化資安防護措施，使其瞭解並願意改善風險，提升資安防護基本能量。自 111 年 8 月 27

日成立迄 114 年 9 月底止，共計協助 40 家業者進行資安檢測。

3. 針對重大矚目、高風險或保有大量個資業者辦理行政檢查

督導業者強化個人資料保護及資安防護，落實法遵。自 111 年 8 月 27 日成立迄 114 年 9 月底止，已辦理 49 次行政檢查。

另為強化技術層面的防護，已推動 8 家電商業者導入隱碼技術，未來將持續與電信業者合作，並擴及其他領域應用。

（二）App Store 卡阻詐措施

數發部定期邀集臺灣高等檢察署、內政部警政署刑事警察局與蘋果公司共同研商阻詐及精進措施，截至 114 年 9 月已召開 11 次聯防會議，目前蘋果公司已推出防詐措施如下：

1. 運用 AI 技術分析 Apple ID 儲值與詐騙態樣。
2. AI 監控並鎖定異常儲值帳號。
3. 導入超商端銷售限額及關懷相關措施，在第一線防堵民眾受騙。
4. AppleCare 客服可依受害者通報，協助鎖定受騙序號，以減少民眾財損。

五、跨部會串聯檢警調及公私協力產業聯防，共同防堵第三方支付遭濫用

（一）訂定「第三方支付服務業能量登錄制度」（下稱三支能量登錄），啓動第三方支付服務業防制洗錢聯防查核作業

1. 數發部於 112 年 7 月啓動三支能量登錄，要求申請第三方支付服務業者（下稱三支業者）提出洗錢防制及法遵聲明書始能登錄，並審查其人力配置與素質、實績、執行管理能力、財務狀況等項目。與金融監督管理委員會達成部會聯防共識，未完成三支能量登錄通過之三支業者，銀行在其開戶時就不會受理；若是銀行現有客戶，未申請三支能量登錄通過之三支業者，銀行將會視為高風險不再提供虛擬帳戶服務；與經濟部達成部會聯防共識，四大超商業者於合作契約簽訂前審核檢視，如為三支業者應檢附三支能量登錄通過之證明文件。
2. 依據洗錢防制法第 6 條第 1 項規定，第三方支付服務之事業或人員未向中央目的事業主管機關完成洗錢防制、服務能量登記或登錄者，不得提供第三方支付服務。同條第 4 項規定，違反第 1 項規定者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 500 萬元以下罰金。三支能量登錄已屬類特許制度，未完成能量登錄之三支業者不得提供第三方支付服務；截至 114 年

9 月 30 日，已通過能量登錄業者共 53 家，廢止登錄 20 家。

3. 為精進三支能量登錄，防範犯罪集團進入產業並取得能量登錄資格，已強化以下精進作法：

(1) 事前防範

於「提供第三方支付服務之事業或人員洗錢防制及服務能量登錄辦法」第 3 條訂定「第三方支付服務業者之公司、有限合夥或商業負責人、合夥人或實質受益人不得犯有組織犯罪、詐欺、貪污治罪、金融犯罪等相關犯罪紀錄」。三支能量登錄申請者應檢附公司、有限合夥或商業負責人、合夥人及實質受益人無違反第 3 條規定情事之聲明書。

(2) 事中查證

發函法務部確認前述聲明書是否屬實，並辦理現場審查確認公司經營現況，且同步啓動企業徵信，針對公司是否遭拒絕往來、退票（含退票理由）、支票戶、動產擔保等情形進行徵信，強化審查財務報表。

(3) 事後查核

邀集法務部調查局、財政部國稅局持續辦理第三方支付服務業防制洗錢及打擊資恐跨部會聯合查核，要求業者落實內部控制與稽核制度，強化客戶身分確認（KYC：Know Your Customer）；並修訂「提供第三方支付服務之事業或人員防制洗錢及打擊資恐辦法」，規範三支業者應要求賣方客戶保留網路實質交易相關憑證並定期查驗、落實確認賣方客戶實質受益人。第三方支付服務業者如違反相關規定，數發部將依據規定落實行政裁罰，自 114 年 1 月 1 日至 9 月 30 日止已查核 45 家，廢止登錄 3 家，裁罰 8 家，金額總計 273 萬元。

（二）數發部建置「第三方支付服務業虛擬帳號查詢平臺」，與檢警調單位合作快速圈存受詐款項

1. 因檢警調單位對於受詐民眾第一時間提供之虛擬帳號，無法得知所屬之第三方支付業者，須先請銀行查詢，再由銀行回報所屬業者後，檢警調單位方能再通知所屬業者就受詐款項進行流向回報及圈存，受詐款項於查詢期間可能已遭犯罪集團提領，無法追回。數發部已建置「第三方支付服務業虛擬帳號查詢平臺」，協助檢警調單位更快速查找虛擬帳號所屬第三方支付業者。自 113 年 3 月上線後，整體流程由原本 7 至 30 天，縮短為 1

至3天，已有效協助檢警調單位辦案，加速圈存受詐款項，降低民眾損失。截至114年9月30日已累計查詢3萬8千餘筆。

2. 因應虛擬帳號納管後，不法集團改以超商條（代）碼繳費作爲詐騙、洗錢工具，目前亦已於虛擬帳號查詢平臺納入第三方支付業者所屬超商條（代）碼資訊，俾利檢警調快速查詢。

（三）建置「第三方支付服務業產業聯防平臺」，與產業共享情資，快速識別並防堵來自高風險商家的詐騙行為

爲協助三支業者落實防制洗錢聯防，數發部已建置「第三方支付服務業產業聯防平臺」，由三支業者上傳涉嫌違法之買方、賣方客戶資訊。系統已於113年8月30日上線，供三支業者自律使用，鼓勵產業聯防，共同防堵詐騙及洗錢案件。同時亦提供網頁偵測工具，協助業者落實審查客戶網站（URL）義務及確認實質交易內容，以降低三支業者被利用於博弈洗錢、詐欺等不法犯罪之工具。

（四）發布「第三方支付服務業疑似涉詐客戶認定及控管措施處理辦法」

要求三支業者發現涉詐客戶後延後撥款或拒絕業務關係合作，並透過保存紀錄與同業聯防通報，以防堵犯罪者持續利用第三方支付服務從事詐欺活動。

六、以公私協力方式推動，並定期檢視遊戲點數阻詐成效

數發部爲加強遊戲點數詐騙防制，要求業者自律配合四大阻詐措施，包含「點數業者端」導入不定期OTP驗證機制、「線上遊戲端」監控異常情形、「四大超商端」依營業額規模進行限額並設置警語、「線上客服端」增加客服處理人力；並提出線上遊戲事業防制詐騙暨洗錢指引作爲自律措施，輔導重點業者推出延遲入點與線上鎖卡機制，強化阻詐措施與保護民眾財產；另邀請行政院洗錢防制辦公室、臺灣高等檢察署、內政部警政署刑事警察局與5大遊戲點數業者定期召開阻詐執行成效會議，檢視阻詐成效及要求業者自律配合提出阻詐措施，經公私部門共同協力下，整體遊戲點數詐騙案件數已自112年之7,163件，下降至113年之1,895件，成功降低約7成遊戲點數詐騙案件，單月案件數也自112年單月最高1,600件，下降至114年9月約300餘件。此外，遊戲點卡業者113年協助攔阻詐騙金額經統計逾新臺幣1.45億元，114年截至9月底攔阻總金額也已超過1.1億元。

參、其他防詐措施

一、打造線上線下整合機制，全民防詐廣宣升級防詐韌性

數發部建立「線上＋實體」整合式防詐宣導體系，透過多元管道傳遞即時資訊，結合社群平臺、數據圖表與視覺化設計，促使全民主動參與，強化社會整體防詐韌性。

（一）為集中防詐訊息、減少民眾受害，於數發部數位產業署官網設置「斥詐人生」專區，針對轄管數位經濟相關產業，提供最新詐騙樣態及防詐作為。防詐資訊包括：「防詐快訊」，每周更新高風險廣告、網頁、商品及關鍵字等；「現場直擊」第一線詐騙案例，以及「遊戲點數防詐」、「防詐工具箱」、「斥詐法典」和「行政處分」等主題，提升使用者體驗和資訊吸收效率。

（二）在實體場域，設計出貼近實務情境、具備預警效果的宣導內容。從校園巡迴到樂齡族群、從市集到大型展會，走遍全臺全方位活動，依宣導群體設計不同的互動式宣導模式，讓年輕人學會看穿「車手」的風險、長者理解「AI 變聲」與「假檢警」的話術陷阱。同時設計防詐理解度評估，收回數據後作為未來宣導素材翻新之依據，讓每一場宣導都更精準。

113 年台北資訊月

資料來源：作者拍攝。

114 年 TGS 台北國際電玩展

資料來源：作者拍攝。

校園宣導活動

資料來源：作者拍攝。

二、數發部與網路廣告平臺公私協力防詐作為

（一）Google

數發部與 Google 共同盤點常見的詐騙手法，於民眾資金充裕、詐騙好發的農曆年間，由 YouTube 號召共 11 位領域創作者響應「# 甘五摳零」防詐宣導活動，除了在影片中分享識詐觀念外，也發揮創意推出豐富影音內容，向更多受眾傳遞反詐知識。

（二）Meta

1. 自 113 年 12 月起，Meta 在全球啟動一項重大試驗計畫，預計招募約五萬名公眾人物參與，透過比對其臉書（Facebook）與 Instagram 個人資料照片和涉嫌用於詐騙廣告的影像進行比對，以精準偵測並自動移除詐騙內容。數發部積極與 Meta 展開合作，提供名人白名單並共享相關資源，促成此項試驗的推行，更將有效提升平臺對詐騙廣告的防禦能力，保護廣大用戶免受其害。
2. 數發部與 Meta 合作，推出互動教育遊戲《眞的假的？》（圖 2），以遊戲化與情境化的學習方式，呈現常見的詐騙手法，包括網路購物、假冒身份、釣魚簡訊、投資詐騙等，讓識詐教育生動有趣，引導玩家從模擬對話、留言與廣告中，辨識可疑訊息，找出關鍵詐騙話術與用詞，並在互動過程中學習判斷與應對的方法，強化識詐力。

（三）LINE

1. 研議強化用戶帳號安全機制

就民眾所使用 LINE 帳號遭盜取情形，數發部已協調 LINE 推出「再次登入」功能，一旦帳號被盜用後，於詐團未變更帳號及密碼的情況下，

圖 2　真的假的

資料來源：Meta 提供。

只要即時發現都可使用「再次登入」功能搶回自己的帳號，讓用戶保住帳號，還能完整還原聊天紀錄，期望能更有效地保障用戶的LINE帳號安全，降低帳號被盜用及資料遺失的風險。

2. 改善資料調閱機制，以符合犯罪偵查需求

由於詐騙集團大多透過 LINE 通訊軟體進行詐騙，故司法警察偵辦詐欺案件時，需大量向 LINE 進行資料調閱，而數發部作爲網路廣告平臺主管機關，扮演我國執法機關與跨國平臺 LINE 業者間的協調聯繫窗口，已與 LINE 日本母公司召開定期溝通協調會議，就「調閱量能技術輔導」及「法律遵循適用爭議」議題交換意見，成功協調 LINE 增加資料調閱處理量能、調閱條件及縮短調閱時間等，例如：原每週 100 筆帳號，自 114 年 6 月起提升至每週 375 筆帳號，針對需持搜索票調閱之資料（如對話紀錄），調閱時程由原先約 3 個月縮短至約 8 個工作天，而無需搜索票調閱之資料（如暱稱、註冊手機號碼），則可於 3 天內提供，有效改善資料調閱機制以符合司法警察實際詐騙犯罪偵查需求。

3. 打造「產業聯防平臺」即時打詐，加速可疑帳號下架

LINE 已建置「產業聯防平臺」，透過公私協力與數發部、內政部警政署及公協會合作進行快速通報，即時下架可疑帳號，攜手共同對抗詐騙、持續擴張聯防範圍。

4. 合推「防詐動態警報」官方帳號警示推播，提升全民防詐意識

數發部與 LINE 合推「防詐動態警報」官方帳號，不定期發布防詐廣宣貼文，內容涵蓋常見的詐騙手法、如何辨識詐騙訊息等，幫助民眾建立基本的防詐觀念，並密切關注當下社會熱議話題或最新詐騙案件，將其融入防詐資訊；在年節等特殊時節，亦設計結合祝福語與防詐提醒的長輩圖，希望能藉由長輩們的分享，擴大防詐資訊的廣宣效益；此外，也將整理詐騙相關數據資料，並製作成簡明易懂的數據圖表，讓民眾更瞭解當前詐騙趨勢。

5. 攜手推出防詐教育遊戲《逃離詐騙新手村》

數發部與 LINE 攜手推出防詐教育遊戲《逃離詐騙新手村》（圖 3）！玩家將進入模擬的詐騙情境中，透過遊戲角色扮演詐騙者，挑戰不同任務關卡，包含幫投票、假社群管理員、小資打工、性影像詐騙等，學習識破這些手法，成爲網路安全的守護者。

圖 3　逃離詐騙新手村

資料來源：LINE 業者提供。

三、啟動防詐實驗室，推動科技防詐應用並強化金融資安韌性

為因應詐騙手法日益翻新，數發部攜手玉山金控、金融科技產業聯盟、中華郵政、Google Cloud、LINE 業者等多元合作夥伴共同設立及推動防詐實驗室。透過共享資料資源、技術驗證與演算法優化，強化對異常交易與可疑帳戶的即時偵測能力，期在第一時間攔截與應對詐騙風險。

除技術研發外，防詐實驗室亦將扮演產業交流平臺角色，提供場域支援新創與金融機構進行測試與模擬應用，強化整體防詐量能。未來也將擴大納入更多雲端服務商、資安業者及金融新創團隊，共同建構我國可信賴之數位金融環境。

肆、結論與展望

數發部將持續透過「法律、技術、商業」三管齊下，不僅建立業者投入防詐的責任，也提供誘因與支援，確保防詐工作能具體落實並持續發揮效益。此外，鑑於深偽等新型詐騙挑戰，數發部亦將持續運用科技方法，強化防詐能量，例如：

一、開發 AI 數位技術工具，對抗深偽等新型詐騙

開發 AI 工具，除現有之文本掃描以外，將針對新興深偽檢測技術進行研究，增強對詐騙手法的防範能力。

二、情資匯流與智慧分析

整合多方情報並運用 AI，建立詐騙情資資料庫來協助政府部門更有效率地處理案件，從源頭阻斷詐騙。

三、加強對平臺的監管追蹤

對於納管平臺業者，透過科技手段追蹤詐騙廣告的下架進度進行監控與數位存證，確保平臺業者履行下架義務，有效精進監管效能。❖