

數位發展部  
針對堵詐、阻詐成效（第四季）  
書面報告

數位發展部  
中華民國114年1月

## 壹、案由

根據警政署資料，今年1到5月詐騙案件相較去年同期激增21%，來到1萬3,363件，然而仔細翻查了數發部的預算以及打詐綱領等相關資料後發現，數發部毫無存在感，只不斷強調技術支援的角色，完全不符合人民對數發部成立的期待，據網路民調統計，民眾對數發部不滿意度達81%，是各部會間最高。以新制定的打詐綱領1.5版為例，統計各部會在綱領中被提及的次數，可以大致代表其工作負擔以及政策細緻程度，內政部出現了127次、法務部99次、金管會25次、NCC16次，數發部居然只有10次，甚至連外交部負責在外館網站轉貼防詐訊息出現次數都高過數發部，唯一讓人有印象的僅為建置政府短碼簡訊公用平臺，故要求數發部每一季應提供針對堵詐、阻詐作為以及相關具體成效之書面報告，並公告於官網供民眾查閱。

## 貳、說明如下：

依行政院「新世代打擊詐欺策略行動綱領1.5版」跨部會分工事項，數位發展部（以下簡稱數發部）主辦「加強電商業者資安維護」、「防制第三方支付詐騙」及「防制遊戲點數成為詐騙工具」等策略，相關措施及執行成效說明如下：

## 一、加強「電商」資安與個資保護措施

### (一) 推動作法：

#### 1. 強化輔導電商資安防護能力：

提供資安檢測資源，與無店面公會合作，推動電商業者加入 TWCERT/CSIRT；另規劃辦理法制宣導說明會，透過公協會通知會員，作資安及法遵的宣導，促進業者瞭解相關法規規範。此外，本部與電信業者、電商業者持續溝通導入物流隱碼技術，以保護民眾個資，減少詐騙發生。

#### 2. 推動電商業者導入隱碼技術：

為避免電商消費者個資在物流配送過程中外洩，增加遭受詐騙可能性，因此推動物流隱碼機制。將收貨人的聯絡電話轉為代碼，藉由物流隱碼，物流士撥打代表號即可與收貨人聯繫。目前已有8家主要電商業者成功導入物流隱碼服務。



圖1 隱碼技術實例

#### 3. 辦理電商業者行政檢查作業：

自111年8月27日起至113年12月31日止，針對重大個資外洩或高風險、保有大量個資業者加強行政

檢查，共辦理41次行政檢查。

## **(二) 重點成效：**

依據警政署統計民眾報案解除分期付款詐騙案件資料，自112年第三季起，數發部接獲通報電商業者的案件數已大幅下降。自113年迄今，數發部所轄大型電商平台已未被列為警政署165全民防騙網公告之高風險業者。

## **二、強化第三方支付管理措施**

為精進第三方支付服務業能量登錄制度，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：

### **(一) 事前防範：**

1. 與經濟部協防超商條（代）碼詐騙、洗錢案件：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. 發布《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 條規定：「不得充任第三方支付服務業者之公司或商業負責人、合夥人或實質受益人之消極資格條件。」
3. 公司負責人應檢附消極資格切結書，公司應檢附洗錢防制法令遵循聲明書。

### **(二) 事中查證：**

1. 發函法務部確認切結書是否屬實。
2. 辦理現場查核確認公司經營現況。
3. 同步啟動企業徵信，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。

### **(三) 事後查核**

1. 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）。
  2. 截至 113 年 12 月 31 日止，已查核 75 家，其中 24 家查核後均已完成改善符合規定、4 家查核後廢止能量登錄、1 家查核後否准能量登錄審查、46 家補充資料中。113 年已就通過能量登錄業者達成 100% 查核覆蓋率。
- (四) 113年3月上線「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：平臺自113年3月上線後，檢警調單位已可由查詢平臺直接查詢並通知三支業者，如民眾遭到詐騙報案，檢警調單位於確認虛擬帳號所屬三支業者後，可加速通知銀行圈存受詐民眾款項。整體流程由原本7至30天，縮短為1至3天，截至113年12月10日已累計查詢3萬餘筆。平臺上線後縮短查詢時間，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。因應虛擬帳號納管後，不法集團改以超商條（代）碼繳費作為詐騙、洗錢工具，已規劃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。
- (五) 協助三支業者落實防制洗錢聯防，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，將疑似洗錢或資恐交易之名單資訊上傳平臺系統。數發部協助建置平臺，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，共同防堵洗錢案件。產業聯防平臺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。

- （六）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》：要求第三方支付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。

### 三、精進遊戲點數防治

#### （一）推動作法：

與點數卡、遊戲及超商業者合作推出四大自律措施：點數業者端完成導入 OTP 驗證機制；線上遊戲端督促業者針對遊戲帳號進行儲值監控及遊戲異常行為監控；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與偵察機關建立通報機制。另促使重點業者推出點數儲值延遲入點，並搭配點數防詐鎖卡服務，當玩家察覺遭詐騙可進行點數鎖定後，至原購買店家退費

#### （二）重點成效：

據統計，整體遊戲點數詐騙案件數已自112年單月最高1,600件，下降至113年12月約100餘件。

### 四、推出政府專屬「111」短碼簡訊服務

為降低民眾遭到簡訊詐騙的風險，本部已提供政府專屬短碼簡訊服務，透過電信業者協助檢核，確保該組短碼無法仿造，建立具有公信力的簡訊機制，各適用

機關可於共同供應契約逕行下單採購，經統計至113年12月底已有376個機關單位使用，累計發送逾6,436萬則簡訊。

## 五、一頁式詐騙網站降觸及

本部依財團法人法監督之財團法人台灣網路資訊中心（TWNIC），已建立 DNS RPZ 自律機制配合各目的事業主管機關（金融、電信、數位經濟相關產業、法務等）及司法警察機關合法處分協調自願加入該機制之網際網擄接取服務提供者（IASP）屏蔽詐騙網站，113年度透過 DNS RPZ 自律機制協處屏蔽涉及詐騙偽冒網站計30,914個。

## 六、本部「網路詐騙通報查詢網」通報機制

為整合各社群媒體平臺偽冒訊息檢舉管道，本部規劃「網路詐騙通報查詢網」，供民眾即時查詢或通報可疑網路詐騙訊息，透過系統介接，將可疑訊息交由政府或民間各單位處理，並隨時將處理進度公告於該查詢網。

本部《網路詐騙通報查詢網》App 前於113年9月30日上架至 Android 及 iOS 平臺，經公測結束並蒐集民眾的回饋與建議後，已達成 App 公測的階段性任務。為加速系統開發與測試，本部暫先下架 App，並於113年12月底推出新版本，刻正進行內外部測試（alpha test、beta test）確認改善成效，規劃於系統更趨完善後再開放民眾下載使用，後續再依測試情形決定114年對外正式上線期程，繼續守護網路環境的安全。