

防制身分冒用

身分冒用係指掠取消費者個人資料，包括姓名、地址、信用卡或社會安全碼等，並以此開立新帳戶、訂購商品或進行借貸等行為，其影響範圍及於消費者、企業及經濟全體。為此，美國於 1998 年訂定“身分冒用與假冒嚇阻法”〈Identity Theft and Assumption Deterrence Act〉，修正美國法典第 18 議題第 1028 條，將未經合法授權，移轉或使用他人身分證明，意圖從事、幫助或教唆任何違反聯邦法律或任何構成州、地方法律重罪之非法活動，均定義為聯邦犯罪。

美國財政部於本年 3 月 15、16 日在 Washington DC 召開“防制身分冒用高峰會議”，集合政府官員、商業界代表、消費者團體及聯邦、州和地方執法單位，研商如何防制身分冒用及減低受害者損失。美國聯邦交易委員會〈簡稱 FTC〉受國會指派為身分冒用資料清算中心，負責消費者教育及身分冒用申訴資料處理。FTC 訂定措施，包括提供受害者免費諮詢服務、開發申訴網站、及利用文宣教導大眾如何處理身分被冒用，讓受害者可充分獲取所需資訊與政府協助。另一方面，FTC 亦將個人資料建置於安全資料庫，並於適當情況下，與其他經法律授權之機關共享資訊。

經濟犯罪研究中心〈National Fraud Center, NFC〉發現詐欺類型眾多，如信用卡詐欺、銀行詐欺等，而部分類型確為身分冒用實例。NFC 在會議中發表白皮書，指出專業詐欺案件，多採阻力較少、風險較低而有相對高報酬率等方式。伴隨科技發達，身分冒用案件亦隨之增加，如九〇年代詐欺行為多為電話行銷詐欺〈telemarketing fraud〉，近年來則透過網際網路方式進行。以後者為例，除新商業契機不斷產生外，在無須露面即可進行信用交易環境下，遂成為詐欺者利用匿名方式與電子傳輸，盜用他人身分之溫床，降低消費者經網際網路進行商業交易之意願，弱化網際網路豐沛商機。舉凡任何防範身分冒用之解決方案，皆有賴政府執法單位、私人企業、隱私權支持者及消費者共同合作，方可達成。任何機構於取得、儲存、傳送個人資料時，需有適當暨安全程序為先決條件，以防範未經授權資料存取；此外，監控資料使用亦有助於防止身分冒用。

至於偵測與預防身分盜用方法，NFC 列舉如下：一、數位認證/數位簽章法：於電子傳輸時，提供資料接收者判讀傳送者身分之服務，確保傳送過程中，資料未經不當修改。數位簽章包含於加密軟體內，需配合密碼與簽章公鑰，由憑證機構〈certificate authorities, 簡稱 CA〉核發數位認證，CA 存有各組身分與其所對應簽章鑰匙之配對資料。二、生物鑑定法：以生理外貌來辨識消費者身分，如指紋及瞳孔虹膜辨識等。三、一般鑑定法：使用商業或消費者個人資料判別其身分真偽，此法適用於當事人親辦或網路交易。為有效防止身分冒用，有關單位應協助私人企業，於身分認證過程中，取得所須辨識資料，但該企業亦應擔負維護經辨識資料之安全。