

## 議題研析

### 一、題目：網路刷卡詐騙爭議之法制研析

### 二、議題所涉法規

銀行法、電子簽章法、信用卡業務機構管理辦法、信用卡定型化契約應記載及不得記載事項

### 三、背景說明<sup>1</sup>

據報載<sup>2</sup>，一頁式網購詐騙氾濫，民眾在網路刷卡交易，遭詐騙集團截取個資及 OTP（一次性密碼）後盜刷高價商品，向銀行投訴卻被認定非屬爭議款。金融監督管理委員會（下稱金管會）指出，經與國際信用卡組織及銀行業者會商，該組織表示持卡人輸入 OTP 即參與交易完成，不能列為爭議款；惟金管會認為消費者因資訊不確實被誤導，不應認為參與交易，以免不公。為排解信用卡交易使用 OTP 遭盜刷之消費爭議，金管會銀行局爰要求銀行業者應落實協助客戶申列爭議款，並於發送 OTP 簡訊時標示清楚內容<sup>3</sup>。

### 四、探討研析

#### （一）信用卡交易疑義有關規範

按銀行法第47條之1規定，經營信用卡業務之機構，應經中央主管機關之許可，相關管理辦法另由中央主管機關洽商中央銀行定之。依信用卡業務機構管理辦法第47條第1項規定，發卡機構訂定之信用卡定型化契約條款，其內容應遵守信用卡定型化契約應記載及不

<sup>1</sup> 本研析關於年分之使用，涉及外國法制或立法例部分，採西元紀年表述，其餘以民國紀年表述。

<sup>2</sup> 戴瑞瑤、黃于庭，OTP 盜刷 金管會定調三方向 銀行協助客戶爭取爭議款、OTP 簡訊資訊要清楚、不符日常行為模式可不給 OTP，Q2上路，工商時報，113年3月26日，第 A11版。

<sup>3</sup> 朱漢崙，阻詐騙廣告盜刷 銀行須落實3原則，聯合報，113年3月26日，第 A7版。

得記載事項之規定，且對消費者權益之保障，不得低於主管機關發布之信用卡定型化契約範本內容。

查信用卡定型化契約應記載及不得記載事項第1點、第8點規定：「……發卡機構應以善良管理人之注意，……依持卡人約定之指示方式為持卡人處理使用信用卡交易款項之清償事宜。」、「持卡人與特約商店發生消費糾紛時，發卡機構應予協助，有疑義時，並應為有利於消費者之處理。持卡人……如對帳單所載之交易明細有疑義，得檢具理由及證明文件通知發卡機構協助處理，……。」另信用卡定型化契約範本第9條及第18條規定，以網際網路、行動裝置訂購商品而使用信用卡付款，發卡機構得以密碼、電話確認等可辨識當事人同一性及確認持卡人意思表示之方式代之，無須使用簽帳單或當場簽名；持卡人信用卡如有遭他人冒用之情形，持卡人應儘速通知發卡機構辦理停卡及換卡手續，停卡及換卡前被冒用所發生之損失，概由發卡機構負擔。準此，民眾於網路刷卡購買商品，發卡機構得不依簽名，而以密碼辨識及確認當事人之同一性與意思表示；對於刷卡交易疑義，民眾得檢具理由及證明文件通知發卡機構協助處理。

按司法實務<sup>4</sup>認為信用卡契約兼具委任契約及消費借貸契約之法律性質，查民法第546條第1項規定：「受任人因處理委任事務，支出之必要費用，委任人應償還之，並付自支出時起之利息。」論者指出，發卡機構依持卡人委託就其刷卡簽帳款項予以支付，該依信用卡契約代付之款項乃委任契約之必要費用。惟發卡機構若無法證明刷卡帳單確由真正持卡人簽署，應認刷卡交易非依信用卡契約之委任意旨所為，該代付款項即非屬必要費用而不得請求償還<sup>5</sup>。從而，民眾利用網際網路刷卡消費，遭截取 OTP 密碼後盜刷交易，發卡機構若無法證明該交易確屬真正持卡人所為之意思表示，似不宜逕認輸入 OTP 即係參與交易，而與信用卡契約之委任意旨相符。爰建議主管機關或可修正信用卡定型化契約應記載及不得記載事項，將

<sup>4</sup> 參最高法院89年台上字第1628號民事判決。

<sup>5</sup> 張志朋，〈信用卡法律關係及盜刷之風險分擔〉，《律師雜誌》，第349期，97年10月，頁80。

OTP 密碼使用相關事項納入規範，以杜爭議。

## (二) 導入網站認證機制

網站詐騙案件頻傳，不但危害社會秩序，亦影響國家經濟發展。考量「信任環境」之重要，歐盟於2016年施行「電子身分識別暨信任服務規則」(Electronic Identification and Trust Services Regulation，下稱eIDAS)，將原電子簽章指令之應用規範，擴大為「電子信任服務機制」(Electronic Trust Services)之建構，並導入「網站認證」(Website Authentication)機制，藉由相關法制之調適，建立可信任之網路服務環境<sup>6</sup>。

不同於電子簽章之自然人確認機制，歐盟eIDAS規範之「網站/網路資訊確認」，性質上屬對物之驗證。依eIDAS之定義<sup>7</sup>，網站認證憑證係指可得認證特定網站，並將該網站與受核發認證憑證之自然人或法人加以聯繫之證明。由是，透過網站認證憑證之規範，網路使用者得藉以驗證網站及其連結資訊之真實性，提升民眾對於網路服務之信任度及電子商務之交易安全。

網路應用環境之信任度，勢將影響電子商務與數位產業之發展。經查我國電子簽章法自90年制定後迄未修正<sup>8</sup>，恐已不敷當前數位經濟發展需要及國際立法趨勢。爰建議主管機關可從「信任服務」角度，參考歐盟eIDAS有關規範，建立網站認證憑證機制，以強化網路服務環境之可信任性，促進數位產業與國家經濟之發展。

## (三) 強化競價式廣告監理

網路詐騙方式眾多，變造短網址混淆訛騙之「釣魚」網站讓民

---

<sup>6</sup> 郭戎晉，〈國際電子簽章法制發展趨勢與我國因應之道〉，《國立中正大學法學集刊》，第81期，112年10月，頁62。

<sup>7</sup> eIDAS Article 3 (38)：‘certificate for website authentication’ means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued. 網址：<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32014R0910#d1e2805-73-1>，最後瀏覽日期：113年4月8日。

<sup>8</sup> 按行政院已擬具「電子簽章法修正草案」，並於113年2月29日以院臺經字第1135004183號函送請本院審議（院總第20號，政府提案第11000980號，113年3月6日印發）。經查上開草案尚無網站認證機制有關規範。

眾防不勝防。透過「競價式廣告」，詐騙假網站即可經由演算法以最快速度優先排列在網頁前方，甚至超前真正官網。據媒體報導<sup>9</sup>，民眾為前往加拿大旅遊，透過網路關鍵字搜尋該國官網，自行申請加拿大電子旅行證（ETA），卻因誤入假網站，遭民間機構以自設ETA網站收取數倍額外費用，再代辦申請ETA，引發網站詐騙與消費糾紛。

英國政府為有效約制網路搜尋引擎業者，已於2023年公布「線上安全法案」（Online Safety Act 2023）<sup>10</sup>明定有關規範，要求大型社群媒體平臺及搜尋引擎等中介服務提供者，應負防止付費詐騙廣告優先出現在政府官網前面之義務，並須建立應對系統及流程，以避免或減少疑似詐騙廣告誤導民眾<sup>11</sup>。經查我國現行法制仍乏關於網路中介服務之一般性規範，爰建議主管機關參酌上開外國先進立法，針對網路中介服務定明相關法律義務，藉由合理有效之網路監理法制，防制層出不窮的網路詐騙廣告。

撰稿人：彭文暉

---

<sup>9</sup> 劉慶侯，誤上簽證釣魚網站／被詐16倍費用 全家出國也泡湯，自由時報，113年3月3日，網址：<https://news.ltn.com.tw/news/society/paper/1633650>，最後瀏覽日期：113年4月8日。

<sup>10</sup> 網址：<https://www.legislation.gov.uk/ukpga/2023/50/enacted>，最後瀏覽日期：113年4月9日。

<sup>11</sup> 林書立，《專家傳真》競價式廣告 助長假網站橫行，工商時報，113年3月14日，第A8版。