僅供委員問政所需參考
不代表本院意見或立場

編號：2461

# 議題研析

## 一、題目：詐欺犯罪防制議題-歐盟打擊線上詐欺規則簡介

## 二、議題所涉法規

詐欺犯罪防制條例草案[1]（行政院研擬中）

## 三、背景說明

歐盟反詐欺局(European Anti-Fraud Office；OLAF)2022 年度報告指出，歐盟存在各類詐欺模式，包括共謀、操縱採購程序、虛報帳務、逃稅、走私和偽造。與此同時，跨境網路電子詐欺趨勢仍在持續。由於開放銀行等服務的出現，電子支付在歐盟持續成長，這些服務涉及從銀行到支付服務提供者安全共享金融資料，相關服務也帶來了新型詐欺，損害了對該行業的信任；社群媒體詐騙性廣告或資訊揭露不實或不完整，亦對消費者權益造成侵害。詐欺不僅被用來資助犯罪集團，還限制了歐盟數位單一市場的發展，使(歐盟)公民更不願意進行網上購物。我國刻正研擬「詐欺犯罪防制條例草案」之打詐專法，強化涉及金融、電信領域之反詐規範，謹介紹歐盟打擊詐欺相關規則及法制經驗，俾供參考。

## 四、探討研析

### （一）歐盟反詐欺局

歐盟除後文將簡介之相關法律及指令外，另有常設性機構-反詐欺局(OLAF)，為歐盟授權的保護歐盟金融利益的機構，於 1999 年 4

[1] 行政院刻正召集各打詐主責部會積極研擬「詐欺犯罪防制條例」（草案）內容，由內政部擔任提案領銜主責機關，通傳會（電信管理）、數位部（數位經濟管理）、金管會（金融機構管理）及法務部（刑度及刑罰執行）擔任共同辦理機關。

月 28 日根據歐盟委員會第 1999/352 號決議成立，任務為打擊影響歐盟預算的詐欺行為、制定反詐欺立法和政策。OLAF 由來自歐盟成員國的警察、海關和法律專家等 4 百多名工作人員組成[2]，透過完全獨立地進行內、外部調查來實現其使命[3]。它協調成員國合作打擊詐欺活動並提供必要之技術支援。

2014 年至 2020 年期間，歐盟委員會和成員國發現了 4,000 多起潛在的詐欺違規行為，其中一部分提交 OLAF 處理，這些違規行為涉及 15 億歐元，OLAF 保護或追回約 5 億歐元，並制止了一些走私、假冒和海關詐欺之企圖，幫助執行歐盟的貿易防禦措施，並制定了預防和打擊新形式的詐欺的戰略[4]、採取必要措施加強相關立法，例如 OLAF 近年完成挪用經費、反傾銷稅逃稅、走私菸酒、非法採伐等詐欺行為之調查。然 OLAF 進行行政調查後，無法強制要求成員國按其後續建議採取行動[5]，而有賴各成員國之自願配合。當 OLAF 結束調查時，它通常會向國家和歐洲主管機關提出建議，OLAF 請各國執法當局針對調查中發現的詐欺、貪腐或其他非法活動採取行動，以對潛在的詐欺者發揮威懾作用[6]。

## （二）數位服務法

於 2024 年 2 月 17 日正式施行之歐盟「數位服務法」(Digital

[2]European Anti-Fraud Office，維基百科。網址：https://en.wikipedia.org/wiki/European_Anti-Fraud_Office，最後瀏覽日期：2024 年 4 月 28 日。

[3] 經濟部國際貿易局與歐盟反詐欺局（OLAF）於 2016 年 11 月 25 日於臺北簽署行政合作協議，雙方互相提供涉嫌偽報產地之相關資訊及協助查證，有助我國及早掌握違規轉運情資並採行防杜措施，避免後續遭歐盟反規避調查；同日財政部關務署與 OLAF 簽署臺灣海關與歐盟反詐欺局行政合作協議，共同打擊關務詐欺，詳見：財政部關務署與歐盟反詐欺局簽署行政合作協議，駐歐盟兼比利時代表處網站，2016 年 12 月 2 日，https://www.taiwanembassy.org/be/post/4871.html；另參貿易局與歐盟反詐欺局簽署行政合作協議，駐歐盟兼比利時代表處網站，2016 年 12 月 1 日，網址：https://roc-taiwan.org/be/post/4852.html，最後瀏覽日期：2024 年 5 月 7 日。

[4] Bogdan Kołcz，The activities of the European Anti-Fraud Office (OLAF) in combating corruption and ensuring the financial security of European Union funds，Lublin Academy, Higher School of Economics and Innovation，網址：https://politics-security.net/index.php/ojsdata/article/view/222，最後瀏覽日期：2024 年 4 月 30 日。

[5] 同註 2。

[6] 相關建議包含：司法建議：邀請成員國司法當局啟動刑事起訴；紀律建議：旨在製裁歐盟工作人員或歐盟機構成員的不當行為；行政建議：旨在採取不同於或超越財務追回或紀律處分的行政措施，詳見：Impact of OLAF’s investigations，OLAF，網址：https://ec.europa.eu/olaf-report/2022/impact-of-investigations/impact-of-investigations_en.html，最後瀏覽日期：2024 年 4 月 30 日。

Services Act, DSA[7]）主要規範「中介服務提供者」和「網路平台」等業者，例如線上商家、社群網路、應用程式商店等。該法新增資訊社會服務提供者(ISSP)更多的積極義務，其立法目的為：1.創建更安全的數位空間，保護所有數位服務使用者的基本權利；2.建立公平的競賽環境，促進歐洲單一市場及全球範圍的創新、成長和競爭力[8]。

根據 DSA 規定，除僱用人數少於 50 人且年營業額低於 1,000 萬歐元（約新臺幣 3.43 億元）之小型企業外，所有在歐盟擁有線上用戶之數位平臺皆必須遵守其規定。此外，DSA 也適用於託管服務以及線上中介機構[9]，重點如下：

1.非法內容控管義務：

第 14 條規定，業者須於其他平台介面提供舉報及刪除非法內容之功能，依第 19 條並賦予「受信任舉報者」(trusted flagger）優先處理其舉報內容之優先權，且須停權累犯者之平台用戶權利。

2.透明度義務：

第 15 條規定，非法內容遭舉報刪除時，平台業者須提供非法內容原作者刪除該內容之理由。又依第 13 條，平台業者須定期發布其非法內容舉報刪除狀況之報告。

3.客戶身分識別及廣告資訊揭露義務：

第 24 條規定，平台業者須確實進行客戶身分識別，並須提供用戶廣告資訊，及應清楚明確標示廣告之存在、廣告贊助商[10]，以及該廣告出現於用戶頁面之原因[11]。

---

[7] 2022 年 7 月歐洲議會完成一讀草案，2022 年 10 月 27 日《歐盟官方公報》正式公布《數位服務法》全文，並於 2022 年 11 月 16 日正式生效，並於生效日後 15 個月直接適用於整個歐盟。詳見：江雅綺，歐盟建立數位韌性的立法趨勢：從《數位服務法》、《數位市場法》、《網路犯罪法》到「人工智慧法」，台灣經濟研究月刊，第 46 卷第 10 期，2023 年 10 月，頁 65。

[8] 同前註。

[9] 歐盟《數位服務法（DSA）》正式實施，適用於歐盟所有數位平臺跨國國旗跨國，國際通傳產業動態觀測，2024 年 2 月 16 日，網址：https://intlfocus.ncc.gov.tw/xcdoc/cont?xsmsid=0J210565885111070723&sid=0O093421130135742449&sq=%E6%95%B8%E4%BD%8D%E5%B9%B3%E8%87%BA，最後瀏覽日期：2024 年 4 月 30 日。

[10] 根據歐盟《數位服務法（Digital Services Act, DSA）》規定，為加強數位平臺之安全與可信度，社群媒體影響者須明確標示出商業廣告貼文。歐盟執委會（European Commission, EC）與 22 個成員國的國家消費者保護機構於 2024 年 2 月 14 日共同發布社群媒體影響者貼文調查結果，發現有 97%的社群媒體影響者曾發布商業內容，然僅 20%公開表明其為商業廣告。另外，成員國主管機關將進一步調查 358 名社群媒體影響者，並要求違法者遵守現行規則，若後續有必要，將採取執法行動，詳見：歐盟執委會（EC）與成員國的國家消費者保護機構共同發布社群媒體影響者貼

4. 風險評估義務：

第 33 條至第 43 條規定，每年應自費請獨立機關就是否含有不法內容進行風險評估、接受執委會審查、提供監管所需數據資料、聘僱法遵人員等[12]

## （三）第三版支付服務指令

歐盟執委會（European Commission； EC)於 2023 年 6 月 28 日提出第三版支付服務指令（Third Payment Services Directive, PSD3）草案及新支付服務法規（new Payment Services Regulation；PSR）草案，預計於 2024 年底前通過最終版本並於 2026 年施行。相較第二版支付服務指令（PSD2)，PSD3 強化歐盟電子、數位支付和金融服務規範，加強現有的法律框架，擴大金融資料的存取範圍，並為使用者提供更高的安全性、保護與促進創新（Innovation)，建立更適合歐盟的支付架構，旨在保護消費者權益和個人資訊，改善支付產業競爭環境，提高消費者對資料掌控度，促進創新金融產品服務發展。PSD3 修正重點歸納如下[13]：

1. 交易保護及支付系統安全性：

強化對未經授權交易之保護，完善支付詐欺或支付錯誤之賠償方案，減少消費者潛在損失。強化客戶身分認證（Strong Customer Authentication, SCA)，促進支付過程的透明度（Transparency）與安全性（Security)。支付服務提供者(payment service providers；PSP）應將付款收款人的姓名和唯一識別碼之間的任何差異通知支付服務使用者( Payment Service User；PSU)。PSD3 規定，授權支付提供者須投保保險(insurance)，以承擔其因詐欺性存取或詐欺性使用支付帳

---

文調查結果，國際通傳產業動態觀測， 2024 年 2 月 14 日，網址：https://intlfocus.ncc.gov.tw/xcdoc/cont?xsmsid=0J210565885111070723&sid=0O088634821271007782&sq ，最後瀏覽日期：2024 年 4 月 30 日。

[11] 劉徑綸，歐盟數位服務法與數位市場法草案初探，科技法律透析，第 33 卷第 3 期，2021 年 3 月，頁 53。

[12] 同註 7，頁 66。

[13] Rudrani Djwalapersad，PSD3 and PSR: regulatory uniformization for enhanced protection，EY(building a better working world)，2024 年 2 月 22 日，網址：https://www.ey.com/en_nl/cybersecurity/psd3-and-psr-regulatory-uniformization-for-enhanced-protection，最後瀏覽日期：2024 年 4 月 30 日。

戶資訊服務而承擔的責任。

2. 開放銀行：

持續推動開放銀行（Open Banking）發展，透過加強規範第三方支付服務提供者(Third party payment provider, TPP)與提供更標準化與更安全的應用程式介面（Application Programming Interface, API)，促進創新金融產業服務發展。

3. 交易監控機制：

PSR 強制 PSP 建立交易監控機制，以降低詐欺風險。此外，如果存在詐欺性支付交易的實質證據，PSP 可能會與另一個 PSP 交換資訊。

4. 跨境支付與支付創新與多元化：

加強跨境支付措施與降低成本，推動歐盟市場一體化，導入區塊鏈或其他更先進的即時支付系統。

5. 因應新型詐欺及強化監管：

導入新規定與工具對抗日益增加的網路詐欺風險；制定更明確的法規，加強各方監管，確保市場公平與穩定[14]。

## （四）歐盟 2019 年之 713 號指令

2019 年 4 月 17 日歐洲議會和理事會關於打擊詐欺和偽造非現金支付手段之 2019/713 號指令取代 2001/413/JHA 指令[15]，重點歸納如下：

1. 技術中立：

由於新的支付技術涉及使用新型支付工具，這在為消費者和企業創造新機會的同時也增加了詐欺的機會。因此，法律框架必須在技術中立(technology-neutral)的基礎上與時俱進[16]。

2. 虛擬資產與其它支付方式均應受同等之保護：

該指令應鼓勵會員國在其國內法中確保各國央行發行之

[14] 歐盟發布第三版支付服務指令（PSD3）草案，強化消費者保護與改善產業環境，科技法律研究所，2024 年 2 月，網址：https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9121，最後瀏覽日期：2024 年 5 月 1 日。

[15] 原文為 DIRECTIVE (EU) 2019/713 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019。

[16] DIRECTIVE (EU) 2019/713 指令第 6 條。

虛擬資產將享有與一般非現金支付手段受同等程度之防詐欺犯罪保護[17]。

3. 成員國間對犯罪構成要件之趨同性：

有效的刑法措施對於保護非現金支付手段免受詐欺和假冒至關重要。對於犯罪行為的構成要件需採取共同的刑法處遇。收集和擁有支付工具以意圖進行詐欺的行為，例如透過網路釣魚、略讀或引導或重定向支付服務使用者到仿製網站，以及散布該等工具，例如在互聯網上出售信用卡資訊，不待實際上詐欺性使用支付手段本身就應定為刑事犯罪。對詐欺和偽造非現金支付手段的制裁和處罰應在整個歐盟範圍內有效、相稱和具有勸阻作用[18]。

4. 快速回饋以保全電子證據：

歐盟有其機制，使國家執法當局能夠為調查和起訴犯罪而交流資訊。鑑於該指令所涵蓋的犯罪具有跨境性及電子證據的不穩定性，成員國應能夠迅速處理來自網路的緊急請求，並在8小時內提供回饋。在非常緊急和嚴重的情況下，會員國應通知歐盟執法合作署(the European Union Agency for Law Enforcement Cooperation)即歐洲刑警組織(Europol)[19]。

## (五)結語

因應科技與消費型態的日新月異，行銷與各類支付系統隨之發展，詐欺的模式也有別以往。數位服務法及第三版支付指令等法令，即是對這些詐欺行為的回應，試圖透過提高支付的安全性和可靠性以及改善消費者資訊和權利來重新建立信任，其增加了監管範圍，要求更多的支付服務提供者打擊支付詐欺，減少對繁瑣技術資料介面的依賴，從整體上消除支付提供者和消費者安全使用支付服務的障礙。相關做法除了實體與非實體金流(線上支付及虛擬資產)同等重視、快速

[17] 同前指令第10條。

[18] 同前指令第13條。另有關於後續執行，該指令不妨礙根據案件情況和國家刑法的一般規則對處罰和判決的個別化和適用以及刑罰的執行(第17條)；由於該指令規定了最低限度的規則，成員國可以自由地通過或維持關於欺詐和偽造非現金支付手段的更嚴格的刑法規則，包括更廣泛的犯罪定義(第18條)；管轄權規則應確保本指令中提到的罪行得到有效起訴。一般而言，犯罪行為最好由犯罪發生國的刑事司法系統處理(第20條)。

[19] 同前指令第26條。

回饋以保全電子證據、非法內容舉報及控管、增加透明度及資訊揭露、強化支付服務提供者建立交易監控及通報機制，以降低詐欺風險等作法值得我國借鏡參考。

撰稿人：楊蕙如