

英App詐騙猖獗銀行卸責

警方不作為玩謝受害人

制度多缺陷追討過程痛苦 奧斯卡影帝前妻公司破產

香港文匯報訊 英國《金融時報》報道，當地的「授權支付」（App）詐騙情況猖獗，然而受害者飽受警方不作為、監管漏洞，以及大型金融機構對用戶不同處理標準所困擾，以致輾轉求助無門。英國雖於去年推出新規，金融機構和支付公司須對受害者作出賠償，但《金融時報》訪問十多名騙案受害者和專家，指出制度存在諸多缺陷。

授權支付詐騙是指客戶受騙後，授權將資金轉移到他們以為由合法收款人持有、但其實由騙徒控制的賬戶。英國現時是此類詐騙案的熱點，原因是該國擁有快速的支付系統，加上人工智能（AI）技術複製網站、製造「深度偽造」（Deepfake）影片或冒充銀行和稅務機關信息，令詐騙案更頻密發生。然而智庫「皇家聯合研究所」（RUSI）資深研究員韋斯特摩爾形容，受害人拿回錢財的過程與被騙一樣痛苦。

哥連費夫前妻花百萬打官司

曾奪得奧斯卡影帝的英國影星哥連費夫的前妻弗斯，是詐騙案的受害者之一。她經營的的諮詢公司遭遇App詐騙，騙徒模仿客戶的電郵地址並插入虛假發票，導致一名員工直接將逾32萬英鎊（約314萬港元）轉入騙徒賬戶。短短數日間，騙徒繞過銀行的查詢，將全部款項匯入餘額為2.62英鎊（約25.7港元）的賬戶。弗斯希望追討失款，她耗時11個月、花費10萬英鎊（約98.2萬港元）律師費仍不得要領，最終公司宣布破產。弗斯批評在過程中警察不作為，以及銀行處事方式令人震驚，稱「我們基本上被這個系統搞垮」。

新規定銀行須賠償最高83萬

《金融時報》指出，英國去年推出新規，若客戶成為App詐騙的受害者，金融機構和支付公司須向客戶償還最多

8.5萬英鎊（約83.5萬港元），使英國成為全球首個引入此類計劃的國家。專家表示，新規定在特定情況下提供了賠償保障，但不能解決日益嚴重的騙案問題。新規則列明若客戶被視為「嚴重疏忽」，他們將無權獲得賠償，但《金融時報》指出，「嚴重疏忽」尚未有明確定義。韋斯特摩爾認為「嚴重疏忽」是灰色地帶，銀行有很多逃避方法，「如果忽略5次彈出的警告，這算是嚴重疏忽嗎？」

此外，英國支付監管機構將App詐騙，定義為從一個英國銀行賬戶到另一個英國銀行賬戶的授權轉賬，但這一定義不包含部分常見騙案，例如透過加密錢包轉移資金，此類詐騙的受害者沒有資格獲賠償。幫助受害者追回資金的調查公司Refundee創始人艾爾斯稱，加密貨幣騙案目前佔該公司每年約5,000宗案件的37%。



●英國影星哥連費夫前妻弗斯是App詐騙案的受害者。 網上圖片



●英國去年推出新規定，銀行須向App詐騙的受害者償還最多8.5萬英鎊。 網上圖片

去年上半年逾9.7萬宗 損失21億元

香港文匯報訊 根據英國金融行業協會（UK Finance）的數據，英國去年上半年共發生97,344宗授權支付詐騙，合計損失2.14億英鎊（約21億港元）。該協會經濟犯罪部門負責人唐納森表示，「騙案持續對這個國家構成重大威脅，除影響經濟外，這種犯罪還會對受害者造成嚴重心理傷害。這場鬥爭只依靠我們是無法取得勝利。」

據該協會發表的2023年報告，該年度英國授權支付詐騙造成的損失近4.6億英鎊（約45.1億港元），共發生逾23萬宗，受害者合共取回2.87億英鎊（約28.8億港元）被騙款項，佔總損失約62%。報告還指出，76%的授權支付詐騙案來自網上，傾向於例如購物詐騙案等低價值騙案，此類騙案總損失佔整體30%。另有16%個案涉及電訊詐騙，涉及詐騙金額較高，形式包括假冒身份等，佔總損失的43%。

專家：反詐騙須跨部門資料共享

香港文匯報訊 英國《金融時報》引述專家應對詐騙危機的建議，指出跨部門資料共享的重要性，以及應讓科技公司和電訊公司承擔責任。《金融時報》指新加坡和澳洲是防範詐騙的標杆，澳洲於2023年成立國家反詐騙中心，將政府、執法部門和私營部門聯繫在一起。新加坡的主要銀行則於去年建立共享數據平台，監管機構要求電訊公司承擔部分損失。英國金融行業協會經濟犯罪部門負責人唐納森表示，「目前在英國有很多這樣的信息，但這些信息都是孤立的。我們需要網上服務和電訊行業在金融服務和執法方面發揮更多作用。」內政部負責反欺詐事務的高官漢森亦承認，政府、執法部門和業界需採取統一及協調的應對措施，指出工黨去年的大選宣言承諾採取「新的擴大

反詐騙戰略」，但沒有提供有關該戰略將包含哪些內容，以及何時宣布的更多細節。

應當面或電話查核支付請求

另一方面，針對個人防範授權支付詐騙，專家建議應直接確認支付請求，最好是當面或透過電話查核，以確認指示的真實可信。人們應使用已知的正確號碼確認付款，而非直接使用電子郵件中提供的聯繫方式。同時還需要留意付款指示的電郵地址是否與真實相符合，以及電子郵件中是否包含異常語句，又或異於發件人以往風格的撰寫方式。此外，企業應建立內部流程，處理有關支付或授權支付的所有請求。

追蹤到騙徒身份地址 警卻告知無能為力

香港文匯報訊 英國「授權支付詐騙」層出不窮，然而受害者向當局尋求幫助時，警方卻不斷將案件轉交不同部門，受害人如同被當作「人球」。被詐騙逾32萬英鎊（約314萬港元）的弗斯追蹤到騙徒的身份和地址，但卻被警方告知「無能為力」，她痛斥「（警方）正在使洗錢和詐騙合法化」。

案件多重轉交不了了之

英國警方設有網絡犯罪國家報告中心 Action Fraud，該機構本身並不調查案件，而是將報告轉交給另一個警察部門國家詐騙情報局。國家詐騙情報局負責交叉核對案件，並在適當的情況下轉給當地警方。然而《金融時報》指出，在絕大多數情況下，受害者會被告知警方不會採取進一步行動。根據2023年的國會報告，詐騙佔英國記錄在案犯罪的40%以上，但其僅佔警務資源的1%。由於大多數案件涉及海外因素，這進一步增加了調查的複雜程度。Action Fraud每年收到的報告中，僅有不足2%會導致刑事指控或起訴。英國內政部和倫敦警方正合作建設新的報告中心，以取代 Action Fraud，該中心原定計劃去年啟動，但推遲至今年，專家半開玩笑地稱該中心為「Inaction Fraud」（詐騙不作為）。經營電動車生意的一名女企業家去年損失8.5萬英鎊（約83.5萬港元），自稱來自金融科技企業Revolut的騙徒誘騙她的商業夥伴交出登入驗證碼。她追蹤到倫敦東部的一個付款地址，但 Action Fraud 卻發來郵件稱「不會採取進一步行動」。她表示「損失如此巨額金錢，警方卻表示無能為力，實在令人震驚」。《金融時報》訪問其他數名受害人，他們亦有同樣的感受。



●英國網上詐騙受害者舉牌抗議，要求賠償。 網上圖片

銀行不滿獨力承擔賠償 促Meta等科企分攤責任



●Meta與英國銀行NatWest及Metro Bank建立合作夥伴關係，分享社交平台發生的欺詐活動情報。 資料圖片

香港文匯報訊 隨著網絡詐騙日益猖獗，英國的銀行、支付業者及社交媒體公司，正在為誰該對受害人負上賠償責任爭吵不休。從去年10月開始，英國的銀行須對「授權支付詐騙」案件的受害人最高賠償8.5萬英鎊（約83.5萬港元），由於這對銀行來說是一項不少的財務責任，因此引起部分銀行業人士不滿，認為社媒也應分攤詐騙案的賠償責任，特別是詐騙往往始於社交平台。

「Meta沒動力打擊詐騙」

英國數碼銀行Revolut公開批評當局的政策，指責社媒Facebook（fb）母公司Meta未有採取足夠措施打擊詐騙行為。Revolut金融犯罪部門主管馬魯夫說，Meta和其他社媒應承擔詐騙案受害人的賠償費，指出「由於不用分擔這項責任，他們就沒有動力為此採取行動」。英國國家經濟犯罪中心主任瓊斯亦批評科企對詐騙行為打擊不力，稱目前缺少的部分是大型社媒主動刪除與詐騙有關的嫌疑賬號，承認改變科企在打擊詐騙方面的慣性做法仍充滿挑戰。事實上，銀行和科企的關係一直緊張，由於數碼支付和社媒平台興起，近年來授權支付詐騙案件急劇增加。據《金融時報》去報道，工黨已草擬提案，強迫科企對其平台發生的詐騙案受害人作出賠償，但一直未成為政策。英國銀行和監管機構長期以來一直在推動社媒公司與零售銀行進行更多合作，以幫助應對急速增長且形態不斷演變的詐騙威脅，關鍵在於科企分享有關犯罪分子如何濫用其平台的情報。Meta去年10月宣布與英國銀行NatWest及Metro Bank建立合作夥伴關係，分享在其平台發生的欺詐活動情報，但拒絕科技業應對授權支付詐騙受害人負上賠償責任的建議。Meta稱，可以透過詐騙情報互惠交換計劃，使用來自大銀行的即時情報來協助阻止欺詐，並發展和改進其機器學習和人工智能（AI）檢測系統，Meta還呼籲政府鼓勵更多這類跨產業合作，指出欺詐是一個跨產業問題，只能透過合作來解決。

冒充合作方或公司高層 授權轉移資金至假賬戶

話你知

授權支付（Authorized Push Payment，簡稱App）指客戶指示銀行從他們的賬戶向另一賬戶支付款項，而授權支付詐騙是指客戶受騙後，授權將資金轉移到他們以為由合法收款人持有、但其實由騙徒控制的賬戶。授權支付詐騙大致分為兩類，「款項轉移詐騙」及「行政總裁/企業電子郵件盜用詐騙」。「款項轉移詐騙」是看似來自熟識的承包商/第三方的電郵，或是來自供應商的偽造信函，聲稱其賬戶號碼已更改，並指示客戶以後將所有款

項轉至新賬戶。「行政總裁/企業電子郵件盜用詐騙」是指看似自身組織高級管理人員（如行政總裁或財務總監）的電郵，要求支付緊急款項。此類電郵通常要求保密，指示員工或收件人切勿與他人談及此事。總體而言，此類詐騙難以察覺，因網絡犯罪分子使用的軟件可操控電郵特徵（包括發件人地址），使之看似真實可信。這意味著詐騙電郵都會與來自同一聯繫人的一般電郵一樣，以相同方式顯示在收件人的收件匣中。騙徒甚至可能非法侵入特定用戶的真實電郵賬戶，直接從該電子信箱發出電郵。