

政府企業共同擔責 追討賠償用戶損失

電騙集團肆虐全球 多國立法加強監管

電騙案追蹤

香港文匯報訊 電騙集團近年肆虐全球各地，手法層出不窮，令不少民眾受害，為此多國均立法打擊及加強監管。分析多國防電騙法例顯示，愈來愈多政府要求企業同時承擔反電騙責任，尤其銀行、金融機構、電訊營銷商和數碼平台不得事不關己，需要積極配合追蹤個案，違者需賠償受害人損失。

英國支付系統監管機構去年10月頒布新政策，應對用戶授權支付欺詐個案（APP Fraud）。這項新政策適用於英國所有合資格金融機構和銀行，若用戶在授權支付期間遭到詐騙，用戶所屬銀行要賠償被詐騙的費用，最高賠償金額為8.5萬英鎊（約80.2萬港元）。過去銀行可以選擇自願賠償，新規要求銀行強制實施。

英前年累計損失逾40億

英國當局頒布的《金融年度詐欺報告》顯示，英國民眾是2023年遭授權支付欺詐，累計損失近4.6億英鎊（約43.4億港元）。英國金融服務機構向當局報告的授權支付欺詐個案，2023年累計超過23.2萬宗，較2020年急增12%。新政策規定，如果客戶明確授權銀行等支付服務提供商（PSP）進行可疑付款，其後蒙受欺詐損失，PSP無需承擔責任，但PSP仍有追討責任，即銀行方面留意到可疑行為，必須配合當局調查、設法追回被騙款項。

歐盟建議詐騙責任轉移銀行

歐盟反詐騙辦公室近年提出設立詐騙責任轉移制度，如果銀行等機構未能完善客戶身份驗證等程序，令客戶蒙受欺詐損失，銀行需要擔責。客戶遭騙徒冒用金融機構名義詐騙個案中，相關金融機構若未及時預警，也需承擔部分責任。美國聯邦貿易委員會（FTC）考慮頒布類似措施，若客戶遭冒用金融機構名義的詐騙，可以向銀行尋求補償。

新加坡本月初通過新法案，擴大警方打擊電騙權力，如果有證據顯示有民眾疑似正被詐騙，警方有權無須事先通知，即凍結這些人士的銀行賬戶、暫停可疑交易。泰國計劃本月頒布行政命令，要求銀行和電訊運營商承擔預防電騙責任，如果使用其服務的用戶遭詐騙，相關企業需賠償損失。

網絡安全事務專家指出，現時多地電騙猖獗、手段多樣，各地政府都意識到僅靠單方面力量，無法獨立承擔打擊詐騙的責任，也無法顯著提升防詐騙效率。預防電訊詐騙需要政府、企業與相關機構共同擔責，提升民眾防詐騙意識，共同面對潛在威脅。



●英規定用戶所屬銀行要賠償被詐騙費用。圖為英國一間滙豐分行。 網上圖片



●新加坡公積金反電騙團隊定期舉行公眾教育活動。 網上圖片

部分國家防電騙法規及漏洞

國家	法規	漏洞
英國	當地監管機構規定，若用戶在授權支付（APP）期間遭到詐騙，相關銀行和金融機構需強制賠償用戶損失，最高賠償金額為8.5萬英鎊（約80.2萬港元）。英國所有合資格金融機構需承擔追討責任。	該規定涵蓋的授權支付僅限英國用戶透過轉數快（FPS）及自動支付清算系統（CHAPS）兩種在英國賬戶之間的交易方式。用戶透過其他支付系統、信用卡、現金或支票等跨國交易遭到詐騙，都無法得到賠償。
新加坡	當局要求落實網絡通訊服務和電子商務服務守則，除銀行機構外，電訊商和社媒需配合打擊電騙。當局可要求指定電訊及網絡服務商建立可主動攔截惡意網絡活動的系統，違規者等同觸犯刑事罪名。	該守則規定打擊的電騙僅限於網絡釣魚詐騙，且難以追蹤來自新加坡境外的電騙。
澳洲	澳洲要求銀行、電訊公司、網絡服務供應商和社媒合作，與當局建立防電騙情報共享網絡。任何一方發現疑似電騙行為，都需及時報警並跟進，未能及時攔截電騙的企業可被處罰。	網絡專家指出，詐騙分子經常透過暗網等隱秘途徑，收集潛在目標的個人資料或私隱等，專家認為當局應要求金融和網絡機構，加強保護用戶個人資料避免外洩。

星法案成全球首例：警方有權凍結受騙人賬戶

香港文匯報訊 新加坡國會上周二（1月7日）通過《防詐騙保障法案》，授權警方合理懷疑有民眾遭到詐騙、可能向騙徒匯款時，向銀行發出限制令，凍結受騙人銀行賬戶並限制交易。法新社報道，新加坡相信是全球首個透過立法，限制詐騙受害人進行銀行交易的國家。

該法案規定，警方如果掌握確鑿證據，證明某人即將從銀行賬戶向騙徒匯款，即使是自願行為，警方與負責調查金融犯罪的新加坡商業事務局均有權要求銀行，暫停此人所有銀行交易。受限服務包括從自動櫃員機提款、信用卡交易、私人貸款、銀行轉賬和操作手機銀行等。

法案規定每次限制令最長持續30天，最多延長5次，意味針對個人的限制令最多可持續180天。受限人士如需從賬戶提取資金，繳納醫療費用或生活開支，可向警方申請並提供證明。

內政部長孫雪玲

表示，新加坡現有防詐騙措施還不完善，難以阻止受害人深陷騙局時自行轉賬。去年1月至9月間，新加坡所有電騙案件中，自行轉賬佔比達86%，損失金額佔整體達94%。孫雪玲舉例說，有長者深陷「殺豬盤」騙局難以自拔，被騙徒騙取40萬坡元（約226.7萬港元），直至耗盡積蓄才醒悟，再想追回被騙款項為時已晚。

旨在爭取時間說服受騙人

新加坡部分議員建議法案允許受限制者自行解除限制，但孫雪玲表示此舉風險極高。她強調新法案旨在保護民眾免受傷害，亦尊重民眾自主選擇，限制令是警方萬不得已才會採取的措施，旨在爭取時間說服受騙人，尋求其家人協助，令其認清遭到詐騙的事實。

法案另外規定，如果受騙人願意授權可親親友監控自己的銀行賬戶，警方會考慮不強制發出限制令。但若受騙人在限制令180天期滿後仍執迷不悟，繼續向騙徒轉賬，所有損失都要由受騙人自行承擔。



●星警有權限制受騙人銀行交易。 網上圖片

澳專家促企業機構完善個人資料保護機制

香港文匯報訊 澳洲政府去年11月公布新版防電騙法案草案，考慮賦予澳洲競爭和消費者委員會更大權力，允許該部門要求銀行、電訊企業和社媒平台加大打擊電騙力度，保護消費者權益。澳洲多名網絡專家建議當局在法案基礎上，敦促各間企業和機構完善個人資料保護機制，避免用戶資料外洩，增加電騙風險。

澳洲軟件公司AvePoint產業與政策主管莫里斯表示，電騙騙徒現時變得更為狡詐，僅靠當局施壓企業及機構加強防範，並非應對電騙的萬靈丹。莫里斯認為在網絡發達的時代，防止詐騙的有效策略需以保護個人資料和私隱為基礎，令騙徒沒有聯絡誘騙潛在受害人的可乘之機。

阻詐騙團夥篩選潛在對象

莫里斯指出，詐騙團夥通常會收集大量網絡用戶的個人資料，從中篩選潛在電騙對象，再針對性展開網絡釣魚攻擊，不論是銀行、企業還是社媒平台，保護用戶的敏感資料，加強安保和防範改措施，才能最大限度地降低電騙風險。

對於澳洲政府的新草案，莫里斯建議當局完善監管措施，要求企業和機構主動提供保護用戶個人資料和機密數據的方案，培訓員工學會識別數據外洩漏洞，或由當局檢查資料儲存設施的運作情況及其安全性。莫里斯認為這些做法能夠從根本上降低詐騙風險，保護用戶私隱。

美國軟件公司Diligent副總裁兼亞太區經理伯格倫德認為，澳洲企業可以主動加強治理網絡安全，包括定期進行風險評估、修復數據外洩漏洞，安排員工接受網絡安全培訓等。企業配合當局主動加強網絡安保措施，也有助提高打擊電騙的效率。



●AvePoint認為防止詐騙需以保護個人資料和私隱為基礎。圖為該公司的培訓活動。 網上圖片

國際刑警警告電騙園犯案 亞洲多國籲民眾提高警惕

香港文匯報訊 國際刑警組織去年11月向195個成員國發布橙色通知，警告東南亞部分地區的電騙園區正擴大規模，實施有組織的人口販運犯罪，受害人主要來自亞洲，亦陸續有歐洲或非洲國家居民受騙。國際刑警組織強調，犯罪團夥以高薪工作等虛假承諾引誘受害人，目標從教育程度較低的低收入群體，逐步轉向受過良好教育的年輕人。韓國和新加坡等國家都發出警告，呼籲民眾警惕。

國際刑警組織人口販運和非法移民部門署理協調員埃斯皮諾薩稱，電騙園區犯罪團夥的目標，已轉向擁有大學學位、熟練使用網絡，甚至精通資訊科技（IT）技術的年輕人。埃斯皮諾薩解釋稱，犯罪團夥利用年輕人急於搵工心態，宣稱提供門檻較低、報酬豐厚的工作，包括翻譯、編程、文書、客服或模特兒等。受害

人被騙入園區後，便會被沒收護照，被迫從事電騙。

埃斯皮諾薩建議，求職者在瀏覽網站或社媒招聘時，需留意相關職位薪酬是否異常高，企業辦公地點是否位於東南亞或部分中東國家等高危地區。如果僱主聲稱應聘者要赴海外面試，或面試地點與實際工作地點不同，很可能涉及電騙，求職者應提高警惕。

韓求助個案同期增四成

韓國外交部去年2月警告，韓國國民遭電騙被綁架至東南亞國家的個案有所增加，當局去年1月收到38宗求助個案，較此前一年同期增加四成。韓國外交部稱，當局發現多數受害者被誘騙赴泰工作，隨後被綁架進入緬甸和柬埔寨等地的園區。韓國政府已頒布針對泰國邊境地區的旅行禁令，並發布特別旅行警告，呼籲前往泰國等地旅客留意。

新加坡、馬來西亞、印尼、印度、巴基斯坦、孟加拉、菲律賓和摩洛哥等國家，都陸續發布警告，提醒民眾不要輕信赴泰國等國家從事高薪工作的說法，若遇到危險需及時報警求助。



●國際刑警組織在全球打擊網絡詐騙，已破獲數百宗較大型個案。 網上圖片