

首9月詐騙案超去年 金管局促落實三大範疇措施 「轉數快」年底前增防騙警示

「道高一尺，魔高一丈」，近年互聯網及智能手機普及，亦令到網上詐騙案呈上升趨勢，金管局今年首9個月收到涉及詐騙的銀行投訴954宗，超過去年全年總和的555宗，當中七成與信用卡交易有關，其餘涉及匯款交易、支付交易和銀行貸款等，金額最大的一宗投資騙案，涉款120萬歐元（折合約990萬港元）。金管局昨日向28間零售銀行發通告，要求銀行提供足夠的資源和專家，確保銀行業在訊息共享、交易監察和客戶警示三大範疇的打擊詐騙重點合作措施如期推出，並預料最快兩個月內推出「轉數快」可疑識別代號警示。

◆香港文匯報記者 曾業俊

金管局副總裁阮國恒昨在記者會指出，涉及信用卡交易的騙案之中，以假積分兌換計劃佔最多，騙徒發出附連結的短訊，向事主聲稱積分即將到期，要求事主支付少量金錢兌換禮品，從而套取了事主的信用卡資料。他提醒市民，進行交易或與金錢有關的活動時，「按連結是一個非常危險的動作」，強調「雖然很方便，但風險不低」；提醒市民牽涉資金調撥時要很小心，包括提供個人資料、信用卡資料、一次性密碼等，這些都是高風險動作，不要亂按連結。

對比「防騙視伏器」資料提警示

鑑於金融犯罪手法層出不窮，金管局一直密切監察相關情況及新出現的詐騙手法，從三方面落實不同措施以應對最新風險。金管局主管（金融基建發展）黎巧兒指出，在客戶警示方面，當局正推動「轉數快」可疑識別代號警示，提升對用戶的警示，在進行「轉數快」支付交易前提醒用戶相關風險。FPS參與機構若為個人用戶提供即時轉賬服務及使用FPS識別代號，都必須參與此計劃向用戶提供防騙警示，將有超過40間銀行和儲值支付工具營運商參與此計劃。各機構正積極落實相關工作（例如系統修改與測試），預計服務將在未來兩個月內推出，金管局將繼續與警方及業界進行宣傳教育工作。

黎巧兒續指，當用戶使用「轉數快」轉賬時，如果「轉數快」識別代號，包括手機號碼、電郵地址和轉數快識別碼（FPS ID），與「防騙視伏器」內標籤為「高危有伏」的資料融合，會在確認交易前向用戶發出警示。在收到警示訊息後，用戶可以選擇繼續向出現警示的「轉數快」識別代號的收款人進行交易，但需要留意有關轉賬存在高度詐騙風險。她建議，用戶每次交易前均需仔細核實付款詳情和收款人身份是否可信。如有懷疑，建議不要進行交易，免招損失。

推訊息交換平台偵測詐騙活動

金管局助理總裁（法規及打擊清洗黑錢）朱立翹表示，在訊息共享方面，該局第一個重點項目是推動「銀行間訊息交換平台（FINEST）」，有助提高銀行之間交換訊息的能力，從而更有效偵測及制止詐騙活動與傀儡戶口網絡。FINEST的第一階段已在今年6月成功推出，包括5間具本地系統重要性機構（D-SIB），並集中交換懷疑與詐騙相關洗錢活動的企業訊息。平台推出3個月來，運作大致暢順。通過此平台交換的訊息，一半涉及投資騙局，其餘與網購、網上情緣騙案有關。訊息促使參與銀行加強監察高風險賬戶，並及時識別未知的可疑賬戶，提交相關可疑交易報告協助罪案的調查工作。

28銀行已實施實時監察系統

朱立翹續指，在交易監察方面，金管局第二個重點項目為「實時監察系統」。目前28間零售銀行已按當局要求，全部實施實時詐騙監察。實時監察系統的目的是加強銀行的實時監察可疑戶口能力，並警惕騙案的潛在受害人，阻截有關騙案款項落入騙徒戶口，減少損失。當客戶進行轉賬時，如果收款賬戶與銀行根據執法機構提供騙案情報而被識別的可疑賬戶融合，銀行的內部實時詐騙監察系統會發出風險標示，跟進該筆交易。銀行職員會聯絡該客戶，提醒該筆交易的詐騙風險，讓客戶三思，再決定是否仍然進行該筆交易。

金管局表示，在多管齊下的措施推出後，當局收到涉及詐騙的銀行投訴個案升幅有所放緩，從今年首季較去年同期上升約1.7倍，放緩至今年第三季較去年同期上升約1.3倍，而警務處錄得的詐騙案升幅亦同樣有所放緩。



◆阮國恒（中）表示，涉及信用卡交易的騙案之中，以假積分兌換計劃佔最多。左為朱立翹，右為黎巧兒。

金管局打擊詐騙未來工作重點

「轉數快」可疑識別代號警示

- 推動零售銀行和儲值支付工具持牌人使用「防騙視伏器」以及向客戶發出「轉數快」(FPS)支付交易的警示，料逾40間銀行和儲值支付工具營運商參與；
- 相關落實工作(包括系統開發與改造)正在進行中，預計今年底前推出；
- 金管局和警方正在籌備有關宣傳教育工作，希望更全面傳遞相關的防騙訊息。

銀行間訊息交換平台(FINEST)

- 進一步提高銀行交換可疑相關訊息的能力。據現有資料，牽涉詐騙的傀儡戶口約10%屬於企業客戶，因此金管局將與銀行業界和持份者持續檢視和優化交換平台，期望推進FINEST下一階段擴展工作，包括涵蓋個人戶口，讓更多銀行參與，以及分享包括以貿易進行洗錢活動等其他金融罪行的相關訊息；
- 金管局將繼續與業界和持份者溝通，爭取共識和訂立具體時間表；
- 參考財務行動特別組織(FATF)的指引及國際經驗、擴大金融罪行類別(例如貿易相關的洗錢活動)；
- 在未來一至兩個月內就提升銀行間訊息交換擴展至個人戶口的发展諮詢業界和公眾。

實時監察系統

- 所有零售銀行已在2023年9月底前採用一致及協調的方式建立實時詐騙監察；
- 要求銀行逐步加入更多資料，例如採用網絡分析工具及非傳統數據，務求可以發現及監察更多可疑戶口及網絡，提醒客戶不要轉錢入騙徒戶口，盡量在源頭堵截騙案發生；
- 最近金管局已展開傀儡戶口網絡分析的反洗錢監管科技試驗，測試來自8間銀行的數據以及科技應用，以助進一步加強應付系統性層面的傀儡戶口網絡風險，金管局會就有關經驗和成果適時與業界分享；
- 在金管局協助下，銀行發展網絡分析技術的進度理想，具備網絡分析技術能力的零售銀行已覆蓋接近九成的零售銀行客戶。

製表：香港文匯報記者 曾業俊

金管局對詐騙近期採取的措施



未來兩個月內推出可疑識別代號警示



註：用戶每次交易前無論是否收到警示均需仔細核實付款詳情和收款人身份。

資料來源：金管局

今年首8月香港的騙案2.55萬宗



今年首9月涉及詐騙的銀行投訴954宗



資料來源：金管局

騙案金額小 市民易中招

WhatsApp 香港文匯報訊（記者 曾業俊）詐騙並非香港獨有，手法也不時創新。金管局收到的個案林林總總，包括有市民收到聲稱積金到期及帶有超連結的訊息。金管局副總裁阮國恒昨表示，近期香港出現全新詐騙手法，金管局最近一個月接獲10多宗市民舉報，指手機遭不法分子入侵，對方假冒機主身份，利用即時通訊軟件WhatsApp向機主電話簿內的朋友發出求救短訊，並附上轉賬連結，向對方訛稱「急需用錢」、「按這連結，替我入一些錢」、「我很急」等等，要求機主朋友轉賬。受害人因為相信短訊是由自己朋友發出而受騙，按下連結後做一些即時轉賬交易，款項被立即匯走。

金管局助理總裁（法規及打擊清洗黑錢）朱立翹補充指，有關WhatsApp騙案投訴每宗涉案金額介乎幾千至十萬元，由於牽涉金額較小，令市民容易降低戒心。她提醒市民要小心，強調市民收到類似信息要先與對方核實。

正為穩定幣建立監管制度

被問及最近的JPEX事件和穩定幣發展進度，阮國恒表示，金管局正為穩定幣建立監管制度，相關設計工作仍在進行，完成後會徵詢市場意見再正式立法。他認為，香港發展虛擬資產業務更多的是講求技術帶來的可能性，相信分布式分類賬技術（DLT）等技術，可為整個金融市場的運作帶來很多好處，但新技術同時有一定風險，因此須妥善管理這些風險。

阮國恒續指，近期發生的JPEX事件亦凸顯香港需要一套有效的監管制度，市民應該小心部分聲稱將會申請牌照的平台。別有用心的人可能將部分交易透過科技包裝成不受規管的產品，有關交易的營運未必合法，投資者要特別小心。

近期詐騙手法

- 信用卡積分兌換騙局** 騙徒發出附連結的短訊，聲稱事主的信用卡積分即將到期，要求事主補付少量金錢兌換禮品，從而套取事主的信用卡號碼及密碼等資料。
- WhatsApp「扮Friend」** 騙徒入侵事主手機，偽冒事主身份，利用WhatsApp向事主的朋友發出附有轉賬連結的求救短訊，訛稱「急需用錢」，要求對方轉賬。
- 求職騙局** 騙徒聲稱提供職位，騙取事主的信用卡及賬戶資料，用作非法活動。
- 問卷調查** 騙徒在即時通訊軟件向事主發送問卷調查，聲稱完成問卷後可獲獎金，藉此騙取事主的信用卡及賬戶資料。
- 投資騙局** 騙徒假冒名人騙取事主信任，誘騙事主投資。

製表：香港文匯報記者 曾業俊

本報專訪

應對無卡化新風險 33措施優化信用卡保障

香港文匯報訊（記者 曾業俊）近年，支付卡從實體發展至現在的無卡交易，令市民日常購物更方便快捷，然而新的信用卡支付模式亦帶來了新的安全風險。金管局助理總裁（銀行操守）區毓麟早前接受香港文匯報專訪時表示，除了以往的盜用實體信用卡個案外，因為信用卡資料被盜取而引致的詐騙交易也愈來愈多。詐騙手法亦由偽冒電話、欺詐網站及流動應用程式、釣魚短訊，擴展至偽冒郵遞取件、零售商及商場會員積分計劃等電子訊息。這些訊息經常附有偽冒網頁的超連結，企圖欺騙受害人提供個人或信用卡等資料。

聯手業界推防詐騙約章

區毓麟指出，金管局一直要求發卡銀行採取有效措施，確保信用卡交易的安全性，以保障客戶的利益。因應信用卡的發展和相關騙案的趨升，金管局自去年下半年開始與銀行業界積極研究完善信用卡保障措施，及如何更有效處理有關信用卡欺詐交易的情況。金管局在今年4月底和6月

向業界發出新指引，要求銀行推行一系列措施優化信用卡客戶的保障，當中包括四大範疇合共33項措施。新措施將在年內分階段落實。金管局和銀行業界會繼續與其他持份者緊密聯繫，確保相關保安及消費者保障的措施持續有效。

他續指，因應騙案手法層出不窮，金管局與銀行不時更新宣傳教育，提醒公眾在使用網上銀行服務進行交易時必須妥善保管和處理個人敏感資料和認證密碼，加強公眾的網絡保安意識，例如審慎查閱網頁及信息的真偽，小心保管個人敏感資料和核實一次性密碼短訊的內容才輸入一次性密碼授權進行交易。今年，金管局首度與零售、電訊、餐飲、交通及物流等不同行業的大型商戶聯手，推出《保障消費者防詐騙約章》（《約章》），參與簽署《約章》的機構包括全港23間發卡銀行及15間大型商戶。參與機構承諾不會透過任何即時電子訊息（如手機短訊、WhatsApp、微信等）向客戶發送超連結要求他們於線上提供個人和信用卡資料，並會通過各種渠道向公眾傳遞「提防騙案」的訊息。各參與機構亦承諾提供合適渠道讓



客戶查證訊息真偽，並加強員工培訓，以體現《約章》承諾，更有效處理客戶查詢。

緊記「撇Link前再三思」

金管局提醒客戶在進行信用卡交易時，應透過銀行和商戶的官方網站或流動應用程式（例如直接輸入商戶的網址或使用從官方管道下載的官方流動應用程式）處理。若收到任何商戶要求提供個人或信用卡資料的即時電子訊息，應小心核實訊息發送者的身份等，並要緊記「撇Link前，要三思」。

金管局要求銀行推行的優化信用卡保障主要措施

- 鼓勵商戶使用流動支付終端機，令客戶可以卡不離手；
- 客戶能夠按自己需要選擇是否以信用卡進行無卡交易(如網上交易)及調整相關交易限額；
- 客戶在交易時可以選擇SMS一次性密碼以外的替代認證方法(如生物認證)；
- 客戶就較高風險持卡交易收到通知；
- 在客戶遇上懷疑信用卡被盜用時可以「一鍵鎖卡」；
- 銀行設立團隊專責處理懷疑未經授權交易個案等。