2025 年 6 月 6 日

致持牌法團的通函

預防及處理未經授權交易事故

1. 證券及期貨事務監察委員會（證監會）注意到，持牌法團出現未經授權交易事故的數目有所增加，而在某些情況下更導致其客戶蒙受財務損失。本通函旨在闡述證監會對持牌法團在預防及處理其客戶帳戶的未經授權交易事故方面的監管要求。

2. 未經授權交易事故的根本原因及其作案手法因應個別情況而異。然而，就近期發生的此類事件而言，我們懷疑犯罪者利用了“中間人攻擊”的方式來作案。犯罪者向經紀行的客戶發出內含仿冒詐騙（或稱網路釣魚）超連結的短訊，誘騙他們在與持牌法團真實網站非常相似的虛假網站上，輸入其用戶資料，然後藉此截取客戶的用戶名稱、登入密碼，及在持牌法團雙重認證程序中用作驗證客戶身分的數據，包括短訊一次性密碼及生物識別數據，從而登入客戶帳戶以進行未經授權交易。

3. 有鑑於此，證監會期望持牌法團在以下方面採取適當的措施，以預防及處理未經授權交易事故：

   (a) 登記參與短訊發送人登記制；

   (b) 提高客戶的認知；及

   (c) 加強程序及監控，以識別客戶帳戶中未經授權的登入和交易。

(A) 登記參與短訊發送人登記制

4. 短訊發送人登記制（該登記制）由通訊事務管理局辦公室（通訊辦）[1] 管理，費用全免，讓已登記的參與者可以“#”號開頭發出短訊，以協助接收者核實短訊發送人的身分，及避免騙徒假冒發送人。因此，持牌法團應盡快登記參與該登記制，並與電訊服務供應商作出必要的安排，以便能夠以“#”號開頭發出短訊。

5. 成功登記參與該登記制後，持牌法團應：(i)僅以“#”號開頭向客戶發出短訊；及(ii)透過其慣常的溝通渠道通知客戶以下事項：

   (a) 它已登記參與該登記制，及所有由其發出的短訊均會以“#”號開頭；

   (b) 它不得發出內含引導客戶登入至其網站或流動應用程式的超連結的電子訊息（例如短訊及電子郵件等）[2]。因此，由持牌法團發出的真實短訊不應內含任何超連結；

[1] 詳情見 https://www.ofca.gov.hk/tc/consumer_focus/guide/hot_topics/ssrs/index.html。
[2] 2025 年 5 月 21 日的《致持牌法團的通函 — 偵測及預防仿冒詐騙》。另見關於持牌法團的網絡保安檢視的通函的附錄。

(c) 即使客戶收到以“#”號開頭的短訊，他們仍應保持警覺，及不應點擊任何內含的超連結。如客戶不慎點擊內含的超連結，及因而被引導至任何網站或流動應用程式的話，切勿輸入任何敏感或機密的個人資料，例如用作登入帳戶所需的用戶資料及一次性密碼；及

(d) 該登記制的參與者會被記錄在通訊辦所建立的登記冊[3]內，客戶可查閱該登記冊或直接聯絡其持牌法團，以核實短訊發送人的身分及短訊的真實性。

(B) 提高客戶的認知

6. 持牌法團應不時提高其客戶的認知，讓他們意識到點擊聲稱由持牌法團發出的短訊內含的超連結的危險性，以及此舉可如何導致其帳戶內出現未經授權交易。除定期向客戶發送提示，提醒他們留意上文第 5 段的要點外，持牌法團亦應加強客戶外展和溝通工作，尤其是如有關持牌法團已遇到未經授權交易事故，或者已知悉業界正發生該等事故。

7. 因此，持牌法團應：

(a) 在其網站及流動應用程式的顯眼處展示有關未經授權交易事故的警示，和有關客戶可如何保護自己[4]的提示，例如避免點擊短訊內含的超連結，以及避免在他們被引導到的網站或流動應用程式中，輸入機密的個人資料、用戶資料及一次性密碼；

(b) 提醒客戶定期查核與其帳戶有關的任何異常活動，例如查閱他們獲發送的有關系統登入、密碼重置、交易執行或客戶和帳戶相關資料變更的通知，藉以識別攻擊者試圖進行未經授權交易（不論成功與否）的跡象；

(c) 如客戶已選擇不接收交易執行或系統登入通知，便要定期（至少每年）提醒客戶警惕相關風險，並告知客戶可選擇接收該等通知及有關啟用通知的流程；

(d) 提醒客戶如懷疑（或確定）其帳戶曾發生未經授權交易，應立即聯絡持牌法團，並告知客戶可使用的通訊渠道或聯絡單位；

(e) 鼓勵客戶就任何未經授權交易事故立即向香港警務處（警方）舉報；

(f) 告知客戶並鼓勵他們使用“防騙視伏器”和流動應用程式“防騙視伏 App”[5]。例如，用戶可在“防騙視伏器”的數據庫中進行搜索，以查核某網站、電話號碼、電郵等是否可能涉及欺詐。“防騙視伏 App”如偵測到用戶嘗試瀏覽可能涉及欺詐的網站，更可實時向用戶發出警示[6]；

[3] 見 https://app2.ofca.gov.hk/apps/ssrs/onlineEnquiry?lang=zh_HK。
[4] 《證券及期貨事務監察委員會持牌人或註冊人操守準則》（《操守準則》）第 5 項一般原則。
[5] 詳情見 https://cyberdefender.hk/scameter/。
[6] 用戶亦可透過“防騙視伏 App”向警方舉報可疑的網站、電話號碼、電郵地址及仿冒連結，以使詐騙行為可被識別及被載入一個可供公眾查閱的數據庫中。

(g) 在其網站及流動應用程式中提供接達值得信賴或可靠的資源的連結，例如守網者[7]、反詐騙協調中心[8]、投資者及理財教育委員會[9]的網站及證監會的警示名單[10]，以教育客戶關於網絡保安威脅及詐騙的訊息。

(C) 加強程序及監控，以識別客戶帳戶中未經授權的登入及交易

8. 持牌法團應實施有效的監察及監督機制，以偵測未經授權而登入客戶帳戶的情況[11]。持牌法團所採用的工具及機制應與其業務規模及複雜程度相稱[12]。

9. 持牌法團應保持警覺，識別那些可能顯示出現未經授權而登入客戶帳戶的情況或客戶帳戶內發生未經授權交易的預警跡象。潛在的預警跡象包括：

(a) 客戶帳戶內進行的交易數量、模式或類型突然有變，而有關變化與持牌法團根據其“認識你的客戶”紀錄或客戶過往交易歷史所了解到的客戶情況並不相符。例如，之前主要投資於藍籌股的客戶突然將其投資組合轉向細價股，或之前不活躍的帳戶突然頻繁買賣細價股；

(b) 多名客戶買賣細價股或流通性低的股票，而其交易佔每日成交額的相當大部分；

(c) 用於登入客戶帳戶的 IP 地址在短時間內由一個地點轉為另一個地點；

(d) 從相同或相似的 IP 地址登入多個客戶帳戶；及

(e) 多個客戶帳戶被綁定到同一設備以進行交易。

10. 持牌法團應設有內部監控程序及操作能力，而按照合理的預期，這些程序和能力足以保障其運作及客戶，以免其因偷竊、欺詐及其他不誠實的行為而招致財政損失[13]。除本通函(A)及(B)節所述的措施外，持牌法團應加強其現有政策、程序及內部監控，以便更有效地保護客戶帳戶以免出現未經授權交易及減低其影響。

11. 尤其是，持牌法團應：

(a) 如識別到客戶帳戶有任何異常活動或懷疑未經授權交易：

(i) 立即聯絡有關客戶，以核實與該帳戶有關的活動是否確實源自有關客戶；及

[7] https://cyberdefender.hk/。
[8] https://www.adcc.gov.hk/zh-hk/home.html。
[9] https://www.ifec.org.hk/web/tc/index.page。
[10] https://www.sfc.hk/TC/alert-list。
[11] 《降低及紓減與互聯網交易相關的黑客入侵風險指引》（《網絡保安指引》）第 1.2 段。
[12] 例如，持牌法團如需為大量客戶提供服務或處理龐大的交易量，應在其監察過程中使用自動化工具。
[13] 《操守準則》第 4.3 段。

(ii) 即時採取步驟防止任何異常活動繼續進行[14]，例如在適當情況下暫停帳戶；

(b) 在知悉或懷疑客戶帳戶內可能發生未經授權交易或客戶帳戶內的資產可能屬犯罪得益時，立即向聯合財富情報組（財富情報組）提交可疑交易報告以匯報該項知悉或懷疑[15]，以便有關當局可及時採取跟進行動。為免生疑問，在（懷疑）未經授權交易的另一邊的對手方持牌法團如注意到懷疑罪行，亦有責任向財富情報組提交可疑交易報告；

(c) 根據《操守準則》第 12.5 段的規定，當系統在運作或功能上出現任何重大缺失、錯誤或缺陷，或在識別出可疑交易時，立即向證監會作出匯報；及

(d) 透過訂閱來自不同可信來源（例如“防騙視伏器”）的網絡威脅情報，緊貼最新的網絡保安威脅情況，並分享本身的網絡威脅情報（例如向“防騙視伏 App”及警方匯報威脅）。

12. 持牌法團應注意，其高級管理層（特別是負責資訊科技的核心職能主管）在識別、監察及減低持牌法團所面對的網絡保安風險，及落實《網絡保安指引》、《操守準則》及《2023/24 年持牌法團網絡保安主題檢視報告》（《網絡主題報告》）所載與網絡保安有關的監管期望方面，肩負最終責任。特別是，持牌法團及其高級管理層應注意《網絡主題報告》內提到的所有措施示例和良好作業方式，並：

(a) 考慮透過阻截從已知的仿冒詐騙網站重新導向的連接嘗試等方式，加強其網站針對中間人仿冒詐騙攻擊（鑑於網站可能較流動應用程式更容易受到這種攻擊）的網絡保安防禦措施；

(b) 鑑於與短訊一次性密碼相關的保安疑慮，考慮採用更穩妥的客戶認證方法，或在適當情況下，實施監控措施以作彌補；

(c) 考慮在客戶進行持牌法團的雙重認證程序時向他們顯示彈出式訊息[16]，提醒客戶如認證程序並非由其本人發起，便不應繼續進行該程序；

(d) 當有人嘗試為客戶帳戶註冊新登入裝置時，在執行該請求前，除了要求客戶進行持牌法團的雙重認證程序外，考慮透過與用來提交該請求的渠道不同的渠道將該請求通知客戶，而向客戶發出的通知應包括提醒客戶如該請求並非由客戶提出，便不應允許該請求；

(e) 當使用新註冊的登入裝置登入客戶帳戶時，考慮在允許該裝置進行交易前，與客戶核實該新登入裝置是否確實屬於客戶；

(f) 考慮要求客戶在執行交易前再次驗證其身分，例如透過實施雙重認證或要求提供專為執行交易而設的密碼；

[14] 《操守準則》附表 7 第 2.1.2 段。
[15] 《打擊洗錢及恐怖分子資金籌集指引（適用於持牌法團及獲證監會發牌的虛擬資產服務提供者）》第 7.20 段。
[16] 持牌法團可考慮列出登入日期和時間、登入 IP 地址及登入裝置資料（例如裝置的型號和地址定位），以協助客戶作出有根據的決定。

(g) 考慮禁止客戶進行並行登入其交易平台；及

(h) 考慮定期主動搜查冒充持牌法團的假冒或欺詐網站和流動應用程式，以透過網域服務供應商及應用程式商店分別將該等網站及流動應用程式下架，並警告客戶提防該等該等網站及流動應用程式。

證券及期貨事務監察委員會
中介機構部

完

SFO/IS/018/2025