SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

2026 年 7 月 9 日

致持牌法團及獲證監會發牌的虛擬資產服務提供者的通函

實施(i)穩健的認證方法以降低及紓減來自仿冒詐騙攻擊的黑客入侵風險及(ii)充足的監察及監督措施以識別可疑活動

1. 證券及期貨事務監察委員會（證監會）要求互聯網經紀行[1]及獲證監會發牌的虛擬資產服務提供者（虛擬資產服務提供者）[2]就客戶帳戶[3]的登入以及裝置綁定[4]採取穩健的認證方法，以保障客戶的互聯網交易帳戶免受仿冒詐騙（或稱網絡釣魚）攻擊，並實施有效的監察及監督措施，以識別客戶帳戶中的可疑活動。本通函載列證監會的要求及提供可接受的認證方法的例子，以供參考。

背景

2. 仿冒詐騙仍然是香港最常被匯報的網絡保安事故類型[5]。

3. 在互聯網經紀行及虛擬資產服務提供者於 2025 年向證監會匯報的網絡保安事故中，騙徒進行大規模的短訊仿冒詐騙活動，無差別地針對互聯網經紀行／虛擬資產服務提供者的客戶。具體而言，騙徒發出含有惡意連結的短訊，冒充互聯網經紀行，並聲稱應監管機構或政府機關的要求而索取資料。客戶隨後被誘使在虛假網站上輸入其用戶登入資料，當中包括在互聯網經紀行的登入程序中用作認證客戶身分的一次性密碼。我們懷疑騙徒利用了“中間人攻擊”的方式來作案，以截取這些客戶的登入資料，從而登入客戶帳戶以進行未經授權交易[6]。

應達到的操守標準

4. 互聯網經紀行及虛擬資產服務提供者應實施穩健的措施，以保障客戶帳戶及資產。這些措施包括：

   (A) 穩健的預防性監控措施，包括就客戶登入及裝置綁定採用高強度且可防止仿冒詐騙的認證解決方案，以保障客戶帳戶免受仿冒詐騙攻擊；

---

1 互聯網經紀行指從事互聯網交易並就以下活動獲發牌的持牌法團：(i)第 1 類受規管活動（證券交易）；(ii)第 2 類受規管活動（期貨合約交易）；(iii)第 3 類受規管活動（槓桿式外匯交易）；及／或(iv)第 9 類受規管活動（提供資產管理），惟以那些以其互聯網為基礎的交易設施分銷所管理的基金者為限。

2 該詞目前指虛擬資產交易平台營運者，原因是在《打擊洗錢及恐怖分子資金籌集條例》附表 3B 下，現時只有一類虛擬資產服務。

3 就本通函而言，“客戶的互聯網交易帳戶”及“客戶帳戶”這兩個詞彙交替使用。

4 裝置綁定被用作其中一項認證元素，即客戶在互聯網經紀行／虛擬資產服務提供者的交易系統內綁定或註冊並連結某台流動裝置／電腦，使有關流動裝置／電腦可藉其經安全登記的裝置特徵而被辨識。

5 在 2025 年向香港網絡安全事故協調中心匯報的保安事故中，仿冒詐騙攻擊佔 57%。

6 詳情請參閱(i)日期為 2025 年 5 月 21 日的《致持牌法團的通函——偵測及預防仿冒詐騙》，及(ii)日期為 2025 年 6 月 6 日的《致持牌法團的通函——預防及處理未經授權交易事故》（《2025 年 6 月的通函》）。

(B) 有效的偵測及監督措施，以識別客戶帳戶中的可疑交易（包括交易指示及資金／虛擬資產的提取），同時亦應包括就客戶的帳戶活動及時通知有關客戶，讓他們能夠就未經授權活動向互聯網經紀行／虛擬資產服務提供者示警；

(C) 針對黑客入侵事故的迅速反應及匯報程序，包括實施措施以遏止和減少未經授權活動，保障客戶資產，通知受影響客戶，及向證監會匯報有關事故；及

(D) 提高客戶對仿冒詐騙和其他網絡保安風險以及相應保護措施的認知，包括警惕客戶提防常被用以盜用客戶帳戶的手段，並提供良好保安作業方式的指引。

(A) 穩健的預防性監控措施以降低及紓減來自仿冒詐騙的黑客入侵風險

5. 互聯網經紀行及虛擬資產服務提供者應就以下各方面實施穩健的認證解決方案，以降低及紓減來自仿冒詐騙攻擊的黑客入侵風險：

- 客戶登入互聯網交易帳戶；及
- 客戶註冊及綁定裝置[7]（見附錄）。為免生疑問，互聯網經紀行及虛擬資產服務提供者無須要求現有客戶重新綁定已綁定的裝置。

6. 互聯網經紀行及虛擬資產服務提供者應審慎評估自身情況，包括向客戶提供的互聯網交易平台類型[8]及平台的風險狀況，並採用適當的認證方法。

7. 如《2020 年 9 月的通函》[9]及《2025 年 2 月的通函》[10]所詳述，多個保安問題都與使用經電郵及短訊傳送的一次性密碼有關。證監會認為，一次性密碼並非可防止仿冒詐騙的認證解決方案，因此互聯網經紀行及虛擬資產服務提供者不應將之用於上文第 5 段所述的程序。

8. 穩健的認證解決方案的例子載於本通函附錄。這些例子包括利用以下各項進行的認證：

- 通行密鑰（passkey），一種以公鑰加密技術為基礎且無需密碼的認證資料，安全儲存於（除其他位置外）用戶裝置或通行密鑰管理工具的私鑰會被用作認證，而無須傳送或分享機密信息；通行密鑰的設計令它只能與其創建和註冊時所對應的合法網站或應用程式配合使用，且通行密鑰是國際公認[11]可防止仿冒詐騙的認證方法，並可於不同類型的互聯網交易平台上採用；及
- 綁定裝置，即採用穩健的核實方法與客戶帳戶建立連結的裝置；此方法同時適用於流動及桌面交易應用程式。

---

7 成功註冊並連結至客戶帳戶的裝置稱為“綁定裝置”。

8 互聯網交易服務一般透過桌面交易應用程式、流動交易應用程式及交易網站提供。

9 日期為 2020 年 9 月 23 日的《致持牌法團的通函——互聯網交易網絡保安檢視》（《2020 年 9 月的通函》）A 節。

10 日期為 2025 年 2 月 6 日的《致持牌法團的通函——持牌法團的網絡保安檢視》（《2025 年 2 月的通函》）。

11 例如，獲美國國家標準技術研究所（National Institute of Standards and Technology）、美國網絡安全與基礎設施安全局（Cybersecurity and Infrastructure Security Agency）、澳洲網絡安全中心（Australian Cyber Security Centre）及英國國家網絡安全中心（National Cyber Security Centre）認可。

9. 通行密鑰認證及綁定裝置均可支援就客戶帳戶登入所實施的雙重認證程序下所指的“客戶所有的”元素[12]：

- 至於通行密鑰認證，客戶在利用儲存於其裝置或通行密鑰管理工具的通行密鑰來就登入要求進行認證時，一般會透過生物識別數據核實或以個人身分識別碼（PIN）來解鎖；及

- 至於裝置綁定，客戶須提供額外的認證元素，例如生物識別數據核實或互聯網交易帳戶密碼。

10. 互聯網經紀行及虛擬資產服務提供者亦應注意，根據目前的要求[13]，一般而言，不應容許客戶就其互聯網交易帳戶綁定或註冊超過三個通行密鑰及／或三部裝置。當客戶要求綁定或註冊超過三個通行密鑰及／或三部裝置時，互聯網經紀行及虛擬資產服務提供者應在批准有關要求前進行充足的評估。

11. 證監會亦重申其於《2020 年 9 月的通函》[14]及《網絡保安常見問題》[15]所載，有關網頁超時監控措施的要求，即互聯網經紀行及虛擬資產服務提供者不應容許客戶關閉網頁超時監控功能，並應限制閒置超時時限（例如在 30 分鐘以內），但須事先作出評估及持續進行監察。如因客戶的交易需要而有充分理由延長閒置超時時限，互聯網經紀行或虛擬資產服務提供者只可在密切監察該客戶的登入和登出紀錄及交易活動的情況下，容許較長的閒置超時時限。

12. 互聯網經紀行及虛擬資產服務提供者應緊貼最新的科技發展和趨勢，考慮其本身所營運的互聯網交易平台類型和與該平台相關的技術發展，及定期評估其現有的保安監控措施，從而確保其網絡保安監控措施維持適當、有效，並與其業務和營運的性質、規模及複雜程度相稱。

(B) 有效的偵測及監督措施以識別可疑交易

13. 互聯網經紀行及虛擬資產服務提供者應就客戶互聯網交易帳戶的成功登入及其他高風險帳戶活動（包括從新裝置登入、新裝置綁定，以及通行密鑰的創建或撤銷），立即通知有關客戶。在適用的情況下，該等通知應透過多種通訊途徑發出，例如電郵、短訊或其他推播通知。

14. 互聯網經紀行及虛擬資產服務提供者應提醒客戶在發現其帳戶有任何可疑活動時立即通知它們，以便它們阻止該等未經授權的活動（如適用）。

15. 證監會亦極力鼓勵互聯網經紀行及虛擬資產服務提供者在容許帳戶進行進一步交易前，先要求客戶確認其已就若干重大變更作出授權，或已獲通知有關帳戶中的異常活動。例如，

---

12 《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 1.1 段及《適用於虛擬資產交易平台營運者的指引》（《虛擬資產交易平台指引》）第 12.12(b)段。

13 《2020 年 9 月的通函》A 節及適用於虛擬資產交易平台營運者及有關網絡保安的常見問題（於 2024 年 5 月 31 日更新）（《網絡保安常見問題》）中問題 6 的答案。

14 《2020 年 9 月的通函》D 節。

15 《網絡保安常見問題》中問題 10 的答案。

當新註冊的裝置被用以登入客戶帳戶時，互聯網經紀行及虛擬資產服務提供者可考慮在容許透過該裝置進行交易前，先向客戶核實有關的新裝置是否確實屬於該客戶。

16. 互聯網經紀行及虛擬資產服務提供者應實施有效的監察及監督措施[16]，以識別其客戶帳戶中的可疑登入及異常交易活動，並即時就任何異常情況作出跟進，包括直接向客戶核實所進行的交易及暫停客戶帳戶（如適用）。這些措施包括：

(a) *交易監察：*運用預設門檻來識別異常的交易活動，並分析與可疑交易相關的預警跡象。例如：

- 預設門檻應適當地參考客戶的概況、過往交易行為、帳戶活動、裝置使用情況及登入模式而定；及
- 潛在的預警跡象包括：
  - 與客戶先前的交易模式不一致的交易，在不尋常時間發起的交易（考慮到客戶的一般交易模式），或在短時間內造成重大損失的交易；
  - 流通性極低的股票或細價股突然出現異常大量的交易；及／或
  - 在重設密碼、更改聯絡資料或綁定新裝置後不久進行異常交易；及

(b) *系統登入及裝置綁定方面的監察：*備存足夠的紀錄（包括在系統登入及裝置綁定的過程中所採集的裝置識別資料），並適時對其進行檢視以偵測異常事件，例如從不尋常的地理位置發出裝置綁定要求，將多個客戶帳戶綁定至同一裝置，在短時間內從多個地點登入的情況，以及異常過長的登入會話。

(C) 針對黑客入侵事故的迅速反應及匯報程序

17. 互聯網經紀行及虛擬資產服務提供者應設立對黑客入侵事故迅速作出反應的程序，當中包括制止未經授權活動，保障客戶資產，通知受影響客戶及防止帳戶遭進一步盜用的即時措施。

18. 互聯網經紀行及虛擬資產服務提供者應立即向證監會匯報黑客入侵事故[17]。它們應進行根本原因分析以識別導致該事故的任何潛在內部監控缺失或系統漏洞，備存詳盡的事故報告，並實施適當的補救措施來加強監控及防止類似事故再次發生。

(D) 提高客戶對仿冒詐騙和其他網絡保安風險以及相應保護措施的認知

19. 互聯網經紀行及虛擬資產服務提供者應採取合理措施，以警惕和提醒客戶注意仿冒詐騙的風險及其他網絡保安風險。特別是，互聯網經紀行及虛擬資產服務提供者應：

---

16 《網絡保安指引》第 1.2 段，《虛擬資產交易平台指引》第 12.12(h)段，以及《2025 年 6 月的通函》(C)節。

17 《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 12.5(e)段及《虛擬資產交易平台指引》第 16.7(b)和(c)段。

- 警惕客戶提防常見的網絡攻擊情境，包括冒充有關公司的欺詐電郵、短訊或電話，旨在騙取登入資料的虛假網站或流動應用程式，以及意圖誘使客戶披露密碼、一次性密碼或其他保安資料的社交工程手段；及

- 提醒客戶如其帳戶登入資料（包括用戶名稱、密碼及認證代碼或裝置）外洩，可能會導致其帳戶遭到未經授權的登入，且客戶在任何情況下均不應向任何第三方披露其登入資料和認證資料，並應保持警覺以保障其帳戶。

20. 互聯網經紀行及虛擬資產服務提供者亦應定期提醒客戶採取穩健的保安作業方式，以降低其帳戶出現未經授權的登入及交易的風險。有關做法包括使用高強度且獨特的密碼，設定適當的交易監控措施和限制，啟用主要帳戶活動的提示，以及迅速檢視和匯報任何可疑或未經授權的交易。

實施時間表

21. 互聯網經紀行及虛擬資產服務提供者應：

(a) 檢討其客戶通知、監察及監督措施以及反應及匯報程序（如上文(B)至(C)節所述），並立即採取必要的優化措施，以符合應達到的操守標準。然而，證監會明白，某些互聯網經紀行／虛擬資產服務提供者可能需要時間更新其系統以符合這些要求，故證監會將以務實的方式評估它們的合規情況；

(b) 在切實可行的範圍內盡快提高客戶對仿冒詐騙和其他網絡保安風險以及相應保護措施的認知（如上文(D)節所述）；及

(c) 在切實可行的範圍內盡快且無論如何不遲於 2027 年 7 月 8 日（即本通函發出日期起計 12 個月內）（下稱“12 個月的實施期間”）實施穩健的認證解決方案，以降低及紓減來自仿冒詐騙攻擊的黑客入侵風險（如(A)節所述），而大型互聯網經紀行應立即實施有關解決方案。

22. 在 12 個月的實施期間內，互聯網經紀行及虛擬資產服務提供者應：

- 採取穩健的認證方法來加強其互聯網交易系統，並確保這些方法在採用前已作充分測試；

- 在切實可行的範圍內盡快向所有客戶推出穩健的認證方法；及

- 將有關變更告知客戶，並就新認證解決方案的實施及使用提供適當的指引和支援。

互聯網經紀行及虛擬資產服務提供者亦應注意（除其他事項外），在 12 個月的實施期間內繼續使用一次性密碼以作認證用途所涉及的仿冒詐騙風險。就此而言，互聯網經紀行及虛擬資產服務提供者應實施經優化的措施，以識別客戶帳戶中的可疑活動，包括異常的登入和未經授權的交易活動。當識別到任何有關可疑或可能屬欺詐的活動時，互聯網經紀行及虛擬資產服務提供者必須立即採取行動以暫停或限制帳戶登入。

23. 如任何互聯網經紀行或虛擬資產服務提供者預計難以在 12 個月的實施期間內完成有關要求，應立即通知其個案主任。

管理層的責任

24. 互聯網經紀行及虛擬資產服務提供者應注意，其高級管理層（特別是分別負責整體管理監督及資訊科技的核心職能主管）在監督上述優化措施的實施和確保客戶帳戶得到妥善保障方面，肩負最終責任。互聯網經紀行及虛擬資產服務提供者應在有需要時向其系統供應商及資訊科技保安專家尋求意見和協助。

25. 互聯網經紀行及虛擬資產服務提供者亦應注意，根據《操守準則》第 4.3 段及《虛擬資產交易平台指引》第 11.10 段，它們有責任實施充足的內部監控及操作能力，以保障其運作及客戶免受盜竊、欺詐及其他不誠實的行為而引致的財政損失。如互聯網經紀行／虛擬資產服務提供者未有實施充足的措施，以預防、偵測及阻止在黑客入侵事故發生後透過客戶帳戶進行的大規模未經授權交易，證監會將要求有關商號就其客戶所蒙受的損失負責。

26. 如對本通函有任何疑問，請聯絡你的個案主任，或致電 2231 1455 與郭嘉慧女士聯絡。

證券及期貨事務監察委員會
中介機構部

連附件

完

SFO/IS/021/2026