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

9 July 2026

Circular to licensed corporations and SFC-licensed virtual asset service providers

Implementing (i) robust authentication methods to reduce and mitigate hacking risks from phishing attacks and (ii) adequate monitoring and surveillance measures to identify suspicious activities

1. The Securities and Futures Commission (SFC) expects internet brokers[1] and SFC-licensed virtual asset services providers (VASPs)[2] to adopt robust authentication methods for login to clients' accounts[3] and device-binding[4] to protect clients' internet trading accounts from phishing attacks, and implement effective monitoring and surveillance measures to identify suspicious activities in clients' accounts. This circular sets out the SFC's expectations and provides examples of acceptable authentication methods for reference.

Background

2. Phishing continues to be the most common type of reported cybersecurity incidents in Hong Kong[5].

3. In 2025, among the cybersecurity incidents reported by internet brokers and VASPs to the SFC, large-scale Short Message Service (SMS) phishing campaigns were conducted by fraudsters that indiscriminately targeted internet brokers'/VASPs' clients. Specifically, fraudsters sent SMS messages containing malicious links which impersonated internet brokers and referred to purported information requests from regulators or government bodies. Clients were then lured into inputting their user credentials on fake websites. These credentials included one-time passwords (OTPs) used to authenticate the clients as part of the internet brokers' login process. It is suspected that the fraudsters executed a man-in-the-middle attack to intercept these clients' credentials, gain access to clients' accounts and conduct unauthorised transactions[6].

---

1 Internet brokers refer to licensed corporations which are engaged in internet trading and are licensed for (i) Type 1 regulated activity (dealing in securities); (ii) Type 2 regulated activity (dealing in futures contracts); (iii) Type 3 regulated activity (leveraged foreign exchange trading); and/or (iv) Type 9 regulated activity (asset management) to the extent that they distribute funds under their management through their internet-based trading facilities.

2 This currently refers to virtual asset trading platform operators as there is currently only one type of VA service under Schedule 3B to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance.

3 For the purpose of this circular, the terms "clients' internet trading accounts" and "clients' accounts" are used interchangeably.

4 Device binding is used as one of the authentication factors, where the client binds or registers and links a mobile device/a computer with the internet brokers'/VASPs' trading system and the mobile device/computer is recognised by its securely enrolled device attributes.

5 Phishing attacks accounted for 57% of the security incidents reported to the Hong Kong Computer Emergency Response Team Coordination Centre in 2025.

6 For details, please refer to (i) Circular to licensed corporations – Phishing detection and prevention dated 21 May 2025 and (ii) Circular to licensed corporations – Prevention and handling of unauthorised trading incidents dated 6 June 2025 (June 2025 Circular).

Expected standards of conduct

4. Internet brokers and VASPs should implement robust measures to protect clients' accounts and assets. This includes:

   (A) Robust prevention controls, including the use of strong and phishing-resistant authentication solutions for client login and device binding, to protect clients' accounts from phishing attacks;

   (B) Effective detection and surveillance measures to identify suspicious transactions (including trade orders and fund/virtual asset withdrawals) in clients' accounts. This should also include timely notifications to clients on their account activities, enabling them to alert the internet broker/VASP to unauthorised activities;

   (C) Prompt response and reporting procedures for hacking incidents, including measures to contain and mitigate unauthorised activities, safeguard client assets, notify affected clients and report the incident to the SFC; and

   (D) Enhance client awareness of phishing and other cybersecurity risks and corresponding protective measures, including alerts to clients on common tactics used to compromise clients' accounts and guidance on good security practices.

(A) Robust preventive controls to reduce and mitigate hacking risks from phishing

5. Internet brokers and VASPs should implement robust authentication solutions that reduce and mitigate hacking risks from phishing attacks for:

   - clients' login to internet trading accounts; and
   - clients' registration and binding of devices[7] (see Appendix). For the avoidance of doubt, internet brokers and VASPs are not required to request existing clients to rebind devices that are already bound.

6. Internet brokers and VASPs should carefully assess their own circumstances, including the types of internet trading platforms[8] offered to clients and the platforms' risk profile, and adopt the appropriate authentication method.

7. As explained in the September 2020 Circular[9] and February 2025 Circular[10], there are a number of security issues associated with the use of email OTPs and SMS OTPs. The SFC does not consider OTP to be a phishing-resistant authentication solution, and

---

7 Devices which are successfully registered and linked to the clients' accounts are referred to as "bound devices".

8 Internet trading services are typically offered through desktop trading application, mobile trading application and trading website.

9 Section A of the Circular to licensed corporation – Review of internet trading cybersecurity dated 23 September 2020 (September 2020 Circular).

10 Circular to licensed corporations - Cybersecurity review of licensed corporations dated 6 February 2025 (February 2025 Circular).

internet brokers and VASPs should not use it for the processes mentioned under paragraph 5 above.

8. Examples of robust authentication solutions are set out in the Appendix to this circular. These include authentication using:

   - passkeys, which are password-less authentication credentials based on public-key cryptography, whereby a private key securely stored on, among other things, a user's device or passkey manager is used to authenticate without transmitting or sharing secrets; passkeys are designed to operate only with the legitimate website or application for which they are created and registered, and are recognised internationally[11] as a phishing-resistant authentication method, which can be adopted across different types of internet trading platforms; and

   - bound devices, where the device is linked to the clients' account using robust verification methods; this method is applicable to both mobile and desktop trading applications.

9. Both passkeys authentication and bound devices can support the "what the client has" factor required under the two-factor authentication[12] process for logging into clients' accounts:

   - for passkey authentication, the client authenticates the login request using passkey stored on their device or passkey manager, typically by unlocking it through biometric verification or a PIN; and

   - for device binding, the client is required to provide an additional authentication factor, such as biometric verification or the password for the internet trading account.

10. Internet brokers and VASPs are also reminded that, under the current requirements[13], generally, they should not allow clients to bind or register more than three passkeys and/or three devices for their internet trading accounts. Where a client requests to bind or register more than three passkeys and/or three devices, internet brokers and VASPs should conduct adequate assessment before approving such request.

11. The SFC also reiterates its expectations set out in its September 2020 Circular[14] and the Cybersecurity FAQs[15] in relation to session timeout controls, where internet brokers and VASPs should not allow clients to disable session timeout and should limit the idle timeout period, for example, to within 30 minutes, subject to prior assessments and ongoing monitoring. Where a longer idle timeout period is justified by the client's trading

---

11 For example, by National Institute of Standards and Technology (US), Cybersecurity and Infrastructure Security Agency (US), Australian Cyber Security Centre and National Cyber Security Centre (UK).

12 Paragraph 1.1 of the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (Cybersecurity Guidelines) and paragraph 12.12(b) of the Guidelines for Virtual Asset Trading Platform Operators (VATP Guidelines).

13 Section A of the September 2020 Circular and answer to question 6 of the frequently asked questions on cybersecurity for virtual asset trading platform operators updated on 31 May 2024 (Cybersecurity FAQs).

14 Section D of the September 2020 Circular.

15 Answer to question 10 of the Cybersecurity FAQs.

needs, the internet broker or VASP may only allow a longer idle timeout period if it monitors closely the client's login and logout records and trading activities.

12. Internet brokers and VASPs should stay abreast of latest technological developments and trends, take into account the particular type of internet trading platform they operate, together with the relevant technological developments associated with such platform, and regularly assess their existing security controls, to ensure that their cybersecurity controls remain appropriate, effective, and commensurate with the nature, scale, and complexity of their business and operations.

(B) Effective detection and surveillance measures to identify suspicious transactions

13. Internet brokers and VASPs should notify clients promptly of successful login to their internet trading accounts and other high-risk account activities, including logins from new devices, binding of new device and creation or revocation of passkeys. Such notifications should be made through multiple communication channels, where applicable, such as email, SMS or other push notifications.

14. Internet brokers and VASPs should remind clients to notify them immediately upon the identification of any suspicious activities in the client accounts so as to facilitate them in stopping the unauthorised activities, where applicable.

15. Internet brokers and VASPs are also strongly encouraged to require clients to confirm that they have authorised certain material changes or have been notified of unusual account activities before further transactions are permitted in the account. For example, when a newly registered device is used to access a client's account, internet brokers and VASPs may consider verifying with the client whether the new device genuinely belongs to the client before allowing transactions to be placed with this device.

16. Internet brokers and VASPs should implement effective monitoring and surveillance measures[16] to identify suspicious login and abnormal trading activities in their client accounts and promptly follow-up on any irregularities, including verifying directly with the clients on the transactions conducted and suspending the client accounts (where appropriate). This includes:

    (a) *Transaction monitoring:* Identify abnormal trading activities using predefined thresholds and analyse red flags associated with suspicious transactions. For example:

        - Predefined thresholds should be set with reference to the client's profile, historical trading behaviour, account activity, device usage and login patterns as appropriate; and

        - Potential red flags include:

            ➢ transactions that are inconsistent with the client's previous trading patterns, transactions initiated at unusual hours having regard to the client's normal

[16] Paragraph 1.2 of the Cybersecurity Guidelines, paragraph 12.12(h) of the VATP Guidelines and section (C) of the June 2025 Circular.

trading pattern, or transactions resulting in significant losses within a short period of time;

- sudden and unusually large numbers of transactions in highly illiquid or small-cap stocks; and/or

- unusual transactions conducted shortly after a password reset, change in contact details or binding of a new device; and

(b) *System login and device binding monitoring*: Maintain sufficient logs, including device IDs captured during system login and device binding, and review them on a timely basis to detect irregular events, such as binding requests from unusual geographic locations, instances where multiple client accounts are bound to the same device, logins from multiple locations within a short period and unusually long login sessions.

(C) Prompt response and reporting procedures for hacking incidents

17. Internet brokers and VASPs should establish procedures to promptly respond to hacking incidents. This includes immediate measures to halt unauthorised activities, safeguard client assets, notify affected clients, and prevent further compromise.

18. Internet brokers and VASPs should also report hacking incidents to the SFC immediately[17]. They should conduct root cause analysis to identify any potential internal control weakness or system vulnerabilities which led to the incident, maintain detailed incident reports and implement appropriate remedial actions to strengthen controls and prevent the recurrence of similar incidents.

(D) Enhance client awareness of phishing and other cybersecurity risks and corresponding protective measures

19. Internet brokers and VASPs should take reasonable steps to alert and remind clients of the risks of phishing and other cybersecurity risks. In particular, internet brokers and VASPs should:

- alert clients of common attack scenarios, including fraudulent emails, text messages or phone calls impersonating the firm, fake websites or mobile applications designed to harvest login credentials, and social engineering tactics intended to induce clients to disclose passwords, OTPs or other security information; and

- remind clients that the compromise of their account credentials, including usernames, passwords, and authentication codes or devices, may result in unauthorised access to their accounts, and they should not disclose their credentials and authentication information to any third party under any circumstances and should remain vigilant in safeguarding their accounts.

[17] Paragraph 12.5(e) of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct) and paragraphs 16.7(b) and (c) of the VATP Guidelines.

20. Internet brokers and VASPs should also remind clients regularly to adopt sound security practices to reduce the risk of unauthorised access and transactions in their accounts. Such practices include using strong and unique passwords, setting appropriate trading controls and limits, activating alerts for key account activities, and promptly reviewing and reporting any suspicious or unauthorised transactions.

Implementation timeline

21. Internet brokers and VASPs are expected to:

    (a) review their client notification, monitoring and surveillance measures, and response and reporting procedures (as mentioned under sections (B) to (C) above) and make the necessary enhancements immediately to meet the expected standards of conduct. Nevertheless, the SFC recognises that some internet brokers/VASPs may need time to update their systems to meet these requirements and the SFC will take a pragmatic approach when assessing their compliance;

    (b) enhance clients' awareness on phishing and other cybersecurity risks and corresponding protective measures (as mentioned under section (D) above) as soon as practicable; and

    (c) implement robust authentication solutions that can reduce and mitigate hacking risks from phishing attacks (as mentioned under section (A)) as soon as practicable and in any event, no later than 8 July 2027 (ie, within 12 months from the date of this circular) (referred to as "the 12-month implementation period") and large internet brokers are expected to implement these solutions immediately.

22. During the 12-month implementation period, internet brokers and VASPs should:

    - enhance their internet trading systems by incorporating robust authentication methods and ensure they are adequately tested before deployment;
    - roll out the robust authentication methods to all clients as soon as practicable; and
    - communicate the changes to clients, and provide appropriate guidance and support on the implementation and use of the new authentication solutions.

    Internet brokers and VASPs are also reminded of, among other things, the phishing risk associated with the continued use of OTP for authentication purpose during this 12-month implementation period. In this connection, internet brokers and VASPs should implement enhanced measures to identify suspicious activities in clients' accounts, including irregular logins and unauthorised trading activities. Upon the identification of any such suspicious or potentially fraudulent activities, internet brokers and VASPs must take immediate action to suspend or restrict account access.

23. Should any internet broker or VASP anticipate any difficulty in meeting the 12-month implementation period, it should immediately notify its case officer-in-charge.

Management responsibilities

24. Internet brokers and VASPs are reminded that their senior management, in particular, the Manager-in-Charge of Overall Management and Oversight and Manager-in-Charge of Information Technology, are ultimately responsible for overseeing the implementation of the abovementioned enhancements and ensuring that client accounts are properly protected. Internet brokers and VASPs should seek advice and assistance from their system vendors and IT security experts as necessary.

25. Internet brokers and VASPs are also reminded of their obligation to implement adequate internal controls and operational capabilities to protect its operations and clients from financial loss arising from theft, fraud and other dishonest acts under paragraph 4.3 of the Code of Conduct and paragraph 11.10 of the VATP Guidelines. If the internet broker/VASP fails to implement adequate measures to prevent, detect and stop large-scale unauthorised transactions conducted through client accounts following hacking incidents, the SFC will hold the relevant firm accountable for the losses suffered by its clients.

26. Should you have any queries regarding this circular, please contact your case officers-in-charge or Ms Kammy Kwok on 2231 1455.

Intermediaries Division
Securities and Futures Commission

Enclosure

End

SFO/IS/021/2026