# SFC Mandates Phishing-Resistant Authentication for Internet Brokers and VATPs

On July 9th 2026, the Securities and Futures Commission (**SFC**) issued a circular to licensed corporations and SFC-licensed virtual asset service providers on implementing robust authentication methods and monitoring measures, setting out the SFC's expectations that internet brokers and SFC-licensed virtual asset service providers (**VASPs**) adopt robust, phishing-resistant authentication for client login and device binding, and implement effective monitoring and surveillance measures to identify suspicious activities in client accounts.

The circular effectively converts what the SFC had previously only strongly encouraged into a firm requirement: licensed firms must stop using one-time passwords (**OTPs**) for client login and device binding, and move instead to phishing-resistant alternatives such as passkeys and bound devices.

Phishing continues to be the most common type of reported cybersecurity incident in Hong Kong. In 2025, internet brokers and VASPs reported to the SFC large-scale SMS phishing campaigns run by fraudsters that indiscriminately targeted their clients. The fraudulent messages impersonated internet brokers and referred to purported information requests from regulators or government bodies, luring clients into entering their login credentials, including OTPs, on fake websites. The SFC suspects the fraudsters used a man-in-the-middle attack to intercept these credentials, gain access to client accounts and conduct unauthorised transactions. Phishing attacks accounted for 57% of the security incidents reported to the Hong Kong Computer Emergency Response Team Coordination Centre in 2025.

## SFC-licensed Entities covered by the Circular

The Circular applies to internet brokers and VASPs. Internet brokers are licensed corporations engaged in internet trading which are licensed for Type 1 (dealing in securities), Type 2 (dealing in futures contracts), Type 3 (leveraged foreign exchange trading) and/or Type 9 (asset management, to the extent that they distribute funds under their management through internet-based trading facilities) regulated activities. VASP currently refers only to virtual asset trading platform (VATP) operators, since only one type of virtual asset service is presently specified under Schedule 3B to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance.

## Expected Standards of Conduct

The SFC expects internet brokers and VASPs to implement robust measures across four areas: (A) prevention,

principally through strong, phishing-resistant authentication; (B) detection and surveillance of suspicious activity; (C) prompt response to and reporting of hacking incidents; and (D) enhancing client awareness of phishing and other cybersecurity risks.

**(A) Ending Reliance on OTPs**

Internet brokers and VASPs must implement robust authentication solutions for client login to internet trading accounts, and for the registration and binding of devices; existing clients are not required to rebind devices that are already bound. Firms should assess their own circumstances, including the types of internet trading platforms they offer and their risk profile, in choosing the appropriate method. As the SFC had already explained in its September 2020 and February 2025 circulars, both email OTPs and SMS OTPs carry security weaknesses. The SFC does not consider OTP a phishing-resistant authentication solution and internet brokers and VASPs should no longer use it for client login or device binding.

**Accepted Authentication Methods under SFC Circular**

The Circular's Appendix gives two examples of acceptable, phishing-resistant methods, both of which can support the "something the client has" factor required for two-factor authentication:

- **Passkeys** - password-less credentials based on public-key cryptography, where a private key stored on the client's device or a passkey manager authenticates the client without transmitting or sharing secrets. Passkeys operate only with the legitimate website or application for which they were created, are internationally recognised as phishing-resistant, and can be used across different types of internet trading platform. In use, the client authenticates the login request via the passkey stored on their device or passkey manager, typically unlocked by biometric verification or a PIN.

- **Bound devices** - a device linked to the client's account using robust verification methods, applicable to both mobile and desktop trading applications. For device binding, the client must provide an additional authentication factor, such as biometric verification or their trading account password.

Firms are also reminded that, under current requirements, clients generally should not be allowed to bind or register more than three passkeys and/or three devices to their internet trading accounts; where a client requests more, the firm should carry out an adequate assessment before approving the request.

The SFC separately reiterates its expectations, set out in the September 2020 circular and its Cybersecurity FAQs, on session timeout controls. Clients should not be permitted to disable session timeout, the idle timeout periods should generally be limited (for example, to within 30 minutes), subject to prior assessment and ongoing monitoring; a longer idle timeout may only be allowed, where justified by the client's trading needs, if the firm closely monitors the client's login, logout and trading activity. Firms should keep abreast of technological developments and regularly reassess their security controls to ensure they remain appropriate, effective and commensurate with the nature, scale and complexity of their business.

**(B) Detection and Surveillance**

Internet brokers and VASPs should promptly notify clients, through multiple channels where applicable (such as email, SMS or push notification), of successful logins and other high-risk account activities, including logins from new devices, binding of a new device and the creation or revocation of passkeys. Clients should be encouraged to report any suspicious activity immediately. Firms are also strongly encouraged to require clients to confirm authorised material account changes, or confirm they have been notified of unusual account activity, before further transactions are permitted - for example, verifying that a newly registered device genuinely belongs to the client before allowing that device to place transactions.

Firms should implement effective monitoring and surveillance to identify suspicious login and abnormal trading activity, and promptly follow up on irregularities, including verifying transactions directly with clients and suspending accounts where appropriate. This covers:

- **Transaction monitoring** - setting predefined thresholds by reference to the client's profile, historical trading behaviour, account activity, device usage and login patterns, and watching for red flags such as transactions inconsistent with the client's normal trading pattern, transactions at unusual hours or resulting in significant losses in a short period, sudden large volumes of transactions in illiquid or small-cap stocks, or unusual transactions shortly after a password reset, change of contact details, or binding of a new device.

- **System login and device binding monitoring** - maintaining sufficient logs, including device IDs captured during login and device binding, and reviewing them in a timely manner to detect irregularities such as binding requests from unusual demographic locations, multiple client accounts bound to the same device, logins from multiple locations within a short period, or unusually long login sessions.

**(C) Responding to and Reporting Hacking Incidents**

Firms should establish procedures to respond promptly to hacking incidents, including immediate measures to halt unauthorised activity, safeguard client assets, notify affected clients and prevent further compromise. Hacking incidents must be reported to the SFC immediately. Firms should conduct root cause analysis to identify any internal control weaknesses or system vulnerabilities that contributed to the incident, maintain detailed incident reports, and implement appropriate remedial action to prevent recurrence.

**(D) Client Awareness**

Internet brokers and VASPs should take reasonable steps to alert and remind clients of phishing and other cybersecurity risks, including alerting clients to common attack scenarios (fraudulent emails, text messages or calls impersonating the firm, fake websites or apps designed to harvest credentials and social engineering tactics), and reminding clients that compromised credentials, passwords or authentication codes or devices may lead to unauthorised account access, that credentials should never be disclosed to any third party, and that clients should remain vigilant. Firms should also regularly remind clients to adopt sound security practices, such as using strong and unique passwords, setting appropriate trading controls and limits, activating alerts for key account activities, and promptly reviewing and reporting suspicious or unauthorised transactions.

## SFC Circular's Implementation Timeline

Internet brokers and VASPs are expected to:

- Review their client notification, monitoring and surveillance measures, and response and reporting procedures (items (B) and (C) above), and make the necessary enhancements immediately; the SFC recognises that some firms may need time to update their systems and will take a pragmatic approach in assessing compliance;

- Enhance client awareness of phishing and other cybersecurity risks (item (D) above) as soon as practicable; and

- Implement robust, phishing-resistant authentication solutions (items (A) above) as soon as practicable and in any event no later than 8 July 2027, being 12 months from the date of the Circular (the **12-month implementation period**); large internet brokers are expected to implement these solutions immediately.

During the 12-month implementation period, internet brokers and VASPs should enhance their internet trading systems to incorporate robust authentication methods and ensure these are adequately tested before deployment, roll out the new authentication methods to all clients as soon as practicable, and communicate the changes to clients with appropriate guidance and support. Firms are also reminded of the continuing phishing risk associated with OTPs during this transitional period, and should implement enhanced measures to identify suspicious activity, including irregular logins and unauthorised trading, taking immediate action to suspend or restrict account access on identifying any suspicious or potentially fraudulent activity. Any internet broker or VASP that anticipates difficulty meeting the 12-month implementation period should notify its case officer-in-charge immediately.

## SFC Licensed Corporations' Senior Management Responsibility

Senior management, in particular the Manager-in-Charge of Overall Management and Oversight and the Manager-in-Charge of Information Technology, are reminded that they are ultimately responsible for overseeing implementation of the enhancements described in the Circular and for ensuring that client accounts are properly protected; firms should seek advice and assistance from their system vendors and IT security experts as necessary. Firms are also reminded of their obligation, under paragraph 4.3 of the Code of Conduct for Persons Licensed by or Registered with the SFC and paragraph 11.10 of the Guidelines for Virtual Asset Trading Platform Operators, to implement adequate internal controls and operational capabilities to protect their operations and clients from financial loss arising from theft, fraud, and other dishonest acts. Where a firm fails to implement adequate measures to prevent, detect and stop large-scale unauthorised transactions conducted through client accounts following a hacking incident, the SFC will hold that firm accountable for the resulting client losses.

## SFC Reminder to Investors

The SFC has also reminded investors to stay vigilant in safeguarding their trading accounts and credentials, including using strong and unique passwords, keeping credentials and devices secure and up to date, and accessing accounts only through the official websites or mobile applications of their licensed corporations or VATPs. Investors should monitor their accounts regularly, promptly review account statements, transaction records and notifications for suspicious activity, and, if they suspect their credentials have been compromised or identify unauthorised transactions, contact their licensed corporation or VATP immediately, secure their accounts and report the matter to the relevant authorities.

CHARLTONS
易周律师行

Hong Kong Office

Dominion Centre 12th Floor
43-59 Queen's Road East Hong Kong

enquiries@charltonslaw.com

www.charltonslaw.com
Tel: + (852) 2905 7888
Fax: + (852) 2854 9596