J M L

Jeffrey Mak Law Firm
麦振兴律师事务所
www.jmaklegal.com

Hong Kong Licensed Corporations Alert
香港持牌法团快讯

2025.06.27

Hong Kong Securities and Futures Commission Issues Circular to Licensed Corporations on Prevention and Handling of Unauthorized Trading Incidents

Licensed corporations (LCs) in Hong Kong are facing a rising number of unauthorized trading incidents, often resulting in significant financial losses to clients. These incidents are frequently linked to sophisticated phishing attacks, where fraudsters impersonate LCs by sending SMS messages containing malicious hyperlinks. These links redirect clients to fake websites closely resembling the LCs' genuine platforms, capturing sensitive login credentials and two-factor authentication (2FA) data such as one-time passwords (OTPs) and biometric information. This enables unauthorized access to client accounts and fraudulent trading activities.

In light of these incidents, the Securities and Futures Commission (SFC) has recently issued clear regulatory expectations and practical guidance focused on three key areas: signing up for the SMS Sender Registration Scheme, raising client awareness, and enhancing internal procedures and controls.

1. Sign Up for the SMS Sender Registration Scheme

The Office of the Communications Authority (OFCA) administers a free SMS Sender Registration Scheme that enables registered participants to send SMS messages with a "#" prefix. This prefix helps recipients verify the authenticity of the sender and prevents fraudsters from impersonating your firm.

- **Action Required:** Register without delay and arrange with your telecom providers to send all SMS messages to clients with the "#" prefix.
- **Client Communication:** Inform your clients through your usual channels that:
    - All genuine SMS messages from your firm will carry the "#" prefix.
    - The firm will never send SMS messages containing hyperlinks directing clients to login pages.
    - Clients should never enter credentials or OTPs on websites or apps accessed via SMS links.
    - Clients can verify your registration status through OFCA's public register or by contacting you directly.

2. Raise Client Awareness Continuously

Educating clients is vital to reducing the risk of phishing and unauthorized trading. Your firm should regularly remind clients about the dangers of clicking on embedded hyperlinks in SMS messages and how to protect themselves.

- Display prominent warnings and educational materials on your website and mobile app.
- Remind clients to:
    - Avoid clicking on suspicious links.
    - Monitor account notifications for unusual login attempts, password reset, trade executions, or changes to client and account related information.
    - Report any suspected unauthorized trading prompt to the firm and the Hong Kong Police Force.
- Inform clients about useful tools such as Scameter, which help detect fraudulent websites and scams in real time.
- Provide links to reputable cybersecurity resources, including CyberDefender, the Anti-Deception Coordination Centre, the Investor and Financial Education Council, and the SFC's Alert List.

3. Enhance Procedures and Controls to Detect and Respond to Unauthorized Access

According to Paragraph 1.2 for Reducing and Mitigating Hacking Risks Associated with Internet Trading (Cybersecurity Guidelines), the firm should implement effective monitoring and surveillance mechanisms tailored to its business size and complexity, where LCs which serve a large number of clients or handle substantial trading volumes are expected to use automated tools in their monitoring processes.

Key red flags to watch for include:

- Sudden changes in transaction volume or patterns inconsistent with client profiles.
- Multiple clients trading in small-cap or illiquid stocks with significant daily turnover.
- Changes in login IP addresses within a short period of time.
- Multiple logins from the same or similar IPs.
- Multiple client accounts linked to the same device.

Upon detecting suspicious activity:

- Contact the client immediately to verify the legitimacy of the transactions.
- Suspend or restrict account access to prevent further unauthorized activity (Paragraph 2.1
- 2 of Schedule 7, Code of Conduct).
- File Suspicious Transaction Reports (STRs) promptly with the Joint Financial Intelligence Unit (JFIU) in line with Paragraph 7.20 of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers).
- Notify the SFC immediately of any material system failures or suspicious transactions as required by the Code of Conduct.

Under Paragraph 4.3 of the Code of Conduct, LCs are expected to have internal control procedures in place and operational capabilities reasonably expected to protect it operations and clients from financial loss arising from theft, fraud and other dishonest acts.

4. Strengthen Cybersecurity Measures

Senior management, especially the Manager-In-Charge of IT, are responsible for overseeing cybersecurity risk management in compliance with the SFC's Cybersecurity Guidelines, Code of Conduct and thematic review findings.

Recommended measures include:

- Hardening website's cybersecurity defenses against man-in-the-middle phishing attacks by blocking connections redirected from known phishing sites.
- Considering stronger client authentication methods beyond SMS OTPs.
- Displaying pop-up warnings during the 2FA process to alert clients if the authentication was not initiated by them.
- Notifying clients through separate channels when new login devices are registered or used, reminding them not to approve unauthorized requests.
- Requiring additional identity verification before trade execution, such as a dedicated password or 2FA.
- Disallowing concurrent logins to your trading platform to reduce risk.
- Proactively searching for and taking down fake websites or apps impersonating your firm, and warning clients about them.

The SFC's recent guidance highlights the urgent need for licensed corporations to adopt a multi-layered approach combining technological safeguards, client education, vigilant monitoring, and prompt reporting.

Senior management accountability is critical in driving these initiatives and ensuring compliance with regulatory expectations. We encourage all licensed corporations to review their current practices in light of this guidance and take proactive steps to safeguard their operations and clients.

Source:
https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC33

Hong Kong Securities and Futures Commission Provides Updated Guidance to Licensed Corporations Based on Findings from Review of Internal Controls regarding Client Asset Protection

Licensed corporations (LCs) in Hong Kong continue to face significant challenges in protecting client assets from misappropriation and fraud. The Hong Kong Securities and Futures Commission (SFC) recently issued a circular on June 6, 2025, highlighting key red flags and control deficiencies identified through a comprehensive review of internal controls of client accounts at selected small to medium-sized securities brokers with the assistance of KPMG Advisory (Hong Kong) Limited.

Key Observations from Recent Asset Misappropriation Cases

The SFC's review and reported cases reveal common tactics used by fraudsters and some dishonest staff to misappropriate client assets:

- **Impersonation of Clients:** Fraudsters often impersonate clients by sending counterfeit instructions via emails that closely resemble clients' legitimate email addresses or by hacking into clients' email accounts.
- **Forgery of Client Signatures:** Fraudsters submit forged written instructions through post, fax, or email, requesting amendments to client particulars or authorizing transactions.
- **Manipulation of Client Details:** Fraudulent requests involving changes in client contact information (phone numbers, email, correspondence addresses) to intercept statements and notifications.
- **Unauthorized Transfers:** Instructions requesting transfers of client securities or money to third-party accounts controlled by fraudsters.
- **Internal Control Failures:** In some reported incidents, poor safeguarding of login credentials and security tokens of authorized signers or staff members further facilitated theft.

SFC's Expected Regulatory Standards and Recommended Controls

To mitigate these risks, the SFC reminds LCs of their obligation to implement robust internal control procedures to protect their operations and clients from financial loss arising from theft, fraud and other dishonest acts in accordance to Paragraph 4.3 of the Code of Conduct for Persons Licensed by or Registered with the SFC, and regarding client assets, especially in the following areas:

a) Amendments to Client Particulars
- Verify the identity and signatures of clients requesting amendments, even if signatures appear genuine.
- Conduct independent verification with clients using alternative registered contact details, at least on a reasonable sample basis or when in doubt.
- Promptly issue acknowledgment notifications to clients' registered contact points that are not subject to change.

b) Handling of Email Requests
- Verify email addresses against official records and apply additional verification for suspicious or high-value transaction requests.
- Confirm instructions through alternative client contact methods rather than replying to the email.
- Provide staff with regular training to identify and handle email scams effectively.

c) Third-Party Deposits, Payments, and Physical Scrip Collection
- Discourage third-party deposits and payments; accept only under exceptional, legitimate circumstances with proper due diligence and management approval.
- Verify the authenticity of withdrawal requests involving third parties by confirming directly with clients.
- Verify the identities of third parties collecting physical securities on clients' behalf.

d) Operation of Bank Accounts
- Implement appropriate authorized signer arrangements, preferably requiring two or more signatories for bank payments.
- Ensure authorized signers safeguard online banking credentials on security devices securely and do not disclose them to others.

e) Dormant Accounts
- Classify accounts with no trading or asset movements initiated by the account holder for a period not exceeding 24 months as dormant.
- Monitor dormant accounts closely to prevent unauthorized trading or fraudulent activities.

Enhancing Client Awareness

The SFC also urges LCs to educate their clients on protecting their assets by:
- Safeguarding personal information such as specimen signatures, login credentials, and account details.
- Promptly informing the firm of any changes in personal particulars.
- Regularly reviewing trading documents and statements of accounts, and reporting discrepancies directly to the firm's management or independent staff rather than account executives.

Senior Management Accountability

Senior management, including Responsible Officers and Managers-In-Charge, bear primary responsibility for maintaining appropriate standards of conduct, implementing effective policies and procedures, and

supervising staff diligently to protect client assets according to General Principles 8 and 9 and paragraphs 4.2, 11.1 and 14.4 of the Code of Conduct.

The SFC expresses concern over repeated control deficiencies in some LCs, which may call into question their fitness and properness to remain licensed. Failure to maintain adequate internal controls that seriously jeopardize client and firm interests may result in the SFC imposing license conditions under section 116(6) of the Securities and Futures Ordinance or taking other regulatory actions.

Source:
https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC32
https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=24EC5

Hong Kong Securities and Futures Commission Updates Requirements on Licensed Corporations regarding Phishing Detection and Prevention

Licensed corporations (LCs) in Hong Kong must remain vigilant against phishing attacks, which have recently caused significant financial losses to clients.

The Hong Kong Securities and Futures Commission (SFC) issued a circular on May 21, 2025, to remind LCs of the expected standards for phishing detection and prevention, as well as their obligation to notify the SFC under the Code of Conduct.

Several LCs reported that their clients received phishing SMS messages containing embedded hyperlinks, falsely appearing to be sent by the LCs. When clients clicked these links, they were directed to fraudulent websites or mobile apps resembling the LCs' legitimate platforms. Clients were then tricked into providing sensitive login details—including login names, biometric IDs, passwords, and SMS one-time passwords (OTPs)—which enabled unauthorized access to their accounts. These accounts were subsequently used for unauthorized transactions, sometimes involving market manipulation, resulting in financial losses.

Regulatory Expectations

Building on the cybersecurity review circular issued in February 2025, the SFC reiterates the following standards for LCs:

- **No Embedded Hyperlinks in Client Communications**: LCs must not send emails or SMS messages containing hyperlinks that direct clients to login pages or transactional platforms.
- **No Requests for Sensitive Information via Hyperlinks**: LCs should never ask clients to provide login credentials, OTPs, or other sensitive personal information through hyperlinks.
- **Regular Cybersecurity Alerts**: LCs should send frequent reminders and alerts to clients warning against phishing attacks and advising on safe practices.
- **Monitoring and Surveillance**: Implement effective systems to detect unauthorized access or suspicious activities in clients' internet trading accounts.
- **Client Education**: Inform clients clearly that LCs will not request sensitive information via hyperlinks and remind them not to disclose login details on unverified websites, no matter how genuine those sites appear.

Handling Client Reports of Phishing

If an LC receives enquiries or notifications from clients about phishing SMS or emails with embedded hyperlinks, or if clients have been defrauded:

- Advise affected clients to report the incidents promptly to the Hong Kong Police Force.
- Alert other clients as soon as practicable to raise awareness and prevent further victimization.

Risk Management and Supervisory Controls

Under paragraph 2.1 of Schedule 7 of the Code of Conduct, LCs offering internet trading must establish:

- Automated Pre-Trade Controls:
  Systems reasonably designed to prevent entry of orders that do not comply with regulatory requirements.
- Post-Trade Monitoring:
  Procedures to identify potentially manipulative or abusive order instructions and transactions.

Mandatory Notifications to the SFC

Per paragraphs 12.5(e) and 12.5(f) of the Code of Conduct, LCs must immediately notify the SFC upon:

- Any material failure, error or defect in the operation of trading, accounting, clearing, or settlement systems or equipment.
- Any material breach, infringement or non-compliance of market misconduct provisions under Parts XIII or XIV of the Securities and Futures Ordinance, providing detailed particulars and relevant documentation.

Phishing remains a significant threat to client security and market integrity. Licensed corporations must adopt a multi-layered approach combining strict communication protocols, client education, robust monitoring, and prompt regulatory reporting. Senior management should ensure these measures are embedded in operational policies and compliance frameworks.

By adhering to the SFC's guidance, LCs can better protect their clients from phishing scams and maintain confidence in Hong Kong's securities market.

Source:
https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC30
https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC7

Hong Kong Securities and Futures Commission Issues to Licensed Corporations its Expected Standards of Conduct for IPO Financing and IPO Subscription Practices

Licensed corporations (LCs) in Hong Kong engaged in IPO subscription and financing services with offering periods starting after March 20, 2025 must align their practices with the Hong Kong Securities and Futures Commission's (SFC) enhanced expectations following a recent review that identified significant risk management deficiencies.

The review highlights concern about imprudent IPO financing practices by some LCs, including acceptance of subscription orders without ensuring clients' financial capacity, over-leveraging clients based on IPO subscription levels rather than actual financial positions, and improper segregation of client subscription deposits.

It was revealed that selected licensed corporations exhibited significant deficiencies in IPO financing, including granting credit based on IPO subscription levels rather than clients' true financial capacity, leading to over-leveraging and heightened default risks. Many firms collected minimal upfront deposits, relying heavily on their own funds for pre-funding, which placed pressure on the firm's liquidity, especially during the critical settlement period. Additionally, improper and delayed segregation of client subscription deposits, particularly those not placed with designated banks for pre-funding confirmation in their daily client money segregation calculations, and slow refunds after balloting caused under-segregation of client monies. These practices expose both clients and firms to substantial financial risks and regulatory non-compliance.

The following outlines the SFC's key findings and provides a guide to help LCs meet the regulatory standards and safeguard both client interests and firm stability.

SFC's Expectations on IPO Subscription and Financing Services

To address these issues, the SFC expects LCs to:

- Collect minimum upfront subscription deposits from clients.
- Conduct thorough financial risk assessments for both the firm and clients.
- Properly segregate client subscription deposits.
- Adhere to investor identification requirements under the Fast Interface for New Issuance (FINI) platform.
- Prevent multiple subscriptions by the same client through different accounts.
- Comply with the Securities and Futures (Financial Resources) Rules (FRR) on liquid capital calculations.

Guide for Licensed Corporations

1. Collect Minimum Upfront Subscription Deposits
   - For IPO subscription orders not fully pre-funded by clients, collect at least 10% upfront deposit of the subscription amount.
   - Where clients' financial situations warrant, consider collecting deposits exceeding 10% to mitigate credit risk.

2. Conduct Financial and Liquidity Assessments
   - Firm-Level Assessment:
     - Evaluate the firm's financial and liquidity position before each IPO to estimate funding needs and maximum IPO financing exposure.
     - Determine whether internal funds or external borrowings will be used to finance client subscriptions.
   - Client-Level Assessment:
     - Assess each client's financial capability prior to granting IPO financing.
     - Set credit limits based on clients' actual financial positions rather than IPO subscription levels or anticipated oversubscription rates.

3. Properly Segregate Subscription Deposits
   - Segregate all upfront subscription deposits, including those not placed with designated banks

for pre-funding confirmation, in accordance with the Securities and Futures (Client Money) Rules.
- For unsuccessful IPO applications, ensure deposits are either segregated or refunded within one business day of receipt under section 4 of the Securities and Futures (Client Money) Rules.

4. Comply with FINI Investor Identification Requirements
- Submit accurate client identification data (CID) to the FINI platform, adhering to its waterfall requirements for priority of identity documents.
- Obtain client confirmations that no higher-priority identity documents exist and keep proper audit trails.
- Conduct additional verification if KYC information raises doubts about client confirmations.
- Implement controls to prevent clients from submitting multiple IPO subscription orders through different accounts within the same firm.

5. Calculate Liquid Capital Appropriately
- Account for IPO financing receivables in accordance with generally accepted accounting principles and the FRR.
- Include "amounts receivable from clients for subscription of securities" as liquid assets only after collecting the minimum upfront deposits.
- Consult certified public accountants where necessary to ensure correct accounting treatments.

6. Review and Update Policies and Procedures
- Critically review your existing IPO subscription and financing policies to ensure full compliance with the SFC's guidance.

7. Monitor and Supervise Ongoing Compliance
- Implement ongoing monitoring of IPO financing exposures and client creditworthiness.

The SFC's enhanced guidance aims to promote prudent risk management and protect investors from undue financial risks associated with IPO subscription and financing services. Licensed corporations should adopt a comprehensive approach encompassing upfront deposit collection, robust financial assessments, proper segregation of client monies, and strict adherence to investor identification rules.

Source:
https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC18

https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=23EC54

Hong Kong Securities and Futures Commission's Latest Guidelines to Licensed Corporations Following its Cybersecurity Review

On February 6, 2025, the Hong Kong Securities and Futures Commission (SFC) released a circular titled "Cybersecurity review of licensed corporations". This circular presents findings from the SFC's 2023/24 Thematic Cybersecurity Review of Licensed Corporations (LCs), focusing on compliance with the Cybersecurity Guidelines and Code of Conduct, collectively referred to as the "Cybersecurity Requirements." It also addresses eight material cybersecurity incidents reported between 2021 and 2024, setting out expected standards to mitigate risks such as phishing, end-of-life (EOL) software, remote access, third-party IT service provider management, and cloud security.

Cybersecurity Incidents

Between 2021 and 2024, LCs reported eight significant cybersecurity incidents that caused substantial disruptions:

- **Ransomware Attacks**: Two LCs experienced ransomware attacks, potentially initiated through phishing, which impacted all IT systems, including internet trading, settlement, and back-office systems, leading to severe operational disruptions.
- **Vendor Network Compromise**: One LC faced back-office service disruptions due to a compromised vendor network, exacerbated by an inadequate contingency plan.
- **Unauthorized Access**: Several incidents involved fraudsters exploiting security loopholes to access trading systems, alter client data, and execute unauthorized transactions.

The SFC noted that some incidents were linked to the use of EOL software, such as Windows Server 2008 and 2012, which no longer receive security updates, increasing vulnerability to attacks. LCs are urged to remain vigilant, identify system vulnerabilities, and implement proactive measures to protect against cyber threats.

Deficiencies in Cybersecurity Requirements

Compared to the 2020 review, the SFC observed improvements in compliance with certain Cybersecurity Requirements, particularly in mobile security. However,

significant deficiencies remain in critical areas, exposing LCs, especially internet brokers, to cybersecurity risks. These include:

- **Unqualified Two-Factor Authentication**: Weak authentication methods for system logins.
- **Lax Security Configurations**: Open unnecessary service ports (e.g., File Transfer Protocol, Secure Shell) and overly permissive firewall access control lists.
- **Delayed Patch Management**: Slow implementation of security patches and hotfixes.
- **Weak Encryption**: Use of inadequate encryption algorithms for sensitive data and insufficient protection for data-in-transit and data-at-rest.
- **Excessive User Access**: Overly broad access to system admin accounts for critical systems and databases.
- **Lack of Audit Trails**: Absence of logs in key systems, hindering monitoring and investigation of incidents.

These shortcomings underscore the need for LCs to strengthen their cybersecurity frameworks to protect systems, client accounts, and data.

Expected Standards

The SFC outlined specific areas where LCs must implement robust cybersecurity controls to meet regulatory expectations. These standards aim to address both existing deficiencies and emerging threats.

Key Areas for Compliance

Area	Expected Standards
Network Security	Implement controls to prevent and detect unauthorized intrusions, disable unnecessary service ports, and conduct annual cybersecurity reviews, including vulnerability scanning and penetration testing.
Patch Management	Monitor and implement security patches within one month of testing.
Data Encryption	Use strong encryption algorithms for sensitive data, including client particulars and credentials, for both data-in-transit and data-at-rest.
User Access Rights	Grant access on a need-to-have basis, limit admin account usage, and log and monitor activities.
Audit Logs	Retain and review logs for critical servers, network devices, and databases to detect suspicious activities.
Client Account Monitoring	Implement mechanisms to detect unauthorized access, monitor IP addresses, and review changes to client particulars for red flags (e.g., multiple clients using the same phone number).

Emerging Threats and Risks

The SFC highlighted several emerging cybersecurity challenges:

- **Phishing**: A common attack vector, potentially linked to ransomware incidents.
- **EOL Software**: Use of unsupported software increases vulnerability to attacks.
- **Remote Access**: Unpatched virtual private network (VPN) solutions pose risks.
- **Third-Party IT Service Providers**: Potential breaches by providers could lead to system disruptions and data leakage.
- **Cloud Security**: Cloud-hosted systems require specific security measures distinct from on-premises environments.

Detailed Standards for Emerging Threats

To address these emerging threats, the SFC has provided detailed standards in the appendix to the circular. These standards are essential for LCs to strengthen their cybersecurity frameworks.

The key standards are summarized below:

Topic	Key Standards
Phishing Detection and Prevention	Deploy anti-malware solutions, update malware signatures timely, avoid embedded hyperlinks in emails/SMS for transactions, stay informed about latest attacks, provide regular cybersecurity training, send client alerts, and ensure incident handling covers phishing scenarios.
End-of-Life (EOL) Software Management	Develop IT asset management policies, maintain and review IT asset inventory annually, monitor software validity, maintain an up-to-date EOL list, plan

	software replacement/upgrade, cease EOL software use on critical systems, and mitigate risks for other systems.
Remote Access	Develop policies for remote access management, grant access on a "least privileged" basis, review user lists annually, implement VPN and multi-factor authentication, set session timeouts, log Third Party Provider activities, and comply with the SFC's operational resilience report.
Third Party Provider Management	Develop policies for due diligence, selection, and monitoring, maintain a provider list, conduct due diligence, enter service level agreements (SLAs) with cybersecurity measures, review SLAs regularly, monitor performance, set security configurations, and include providers in contingency plans.
Cloud Security	Develop policies for access, encryption, logging, and backups, conduct due diligence on providers, secure network infrastructure, control root account access, manage credentials on a "least privilege" basis, ensure daily immutable backups, and collaborate with providers for contingency drills.

The SFC also noted concerns with SMS one-time passwords (OTPs) due to interception risks and encourages LCs to adopt more secure authentication methods, such as biometrics or software tokens.

Senior Management Responsibility

The SFC emphasizes that senior management, particularly the Manager-In-Charge of Information Technology (MIC-IT), is ultimately responsible for managing cybersecurity risks. Key responsibilities include:

- **Resource Allocation**: Ensuring qualified staff and adequate technology and financial resources are deployed.
- **Policy Review**: Regularly reviewing and approving cybersecurity risk management policies to address evolving threats.
- **Cybersecurity Reviews**: Conducting regular system reviews and ensuring remedial actions are implemented.
- **Contingency Planning**: Establishing and testing contingency plans to address cybersecurity scenarios, with updates based on operational changes and risk exposure.

These responsibilities highlight the critical role of leadership in fostering a robust cybersecurity culture within LCs.

Recognizing the increasing reliance on technology across all LCs, not just internet brokers, the SFC plans to review existing Cybersecurity Requirements in 2025 and develop an industry-wide cybersecurity framework. This initiative aims to provide comprehensive guidance to help all LCs manage cybersecurity risks effectively, addressing the growing sophistication of cyber threats.

The circular underscores the critical importance of cybersecurity for licensed corporations in Hong Kong's financial sector. By addressing deficiencies, implementing expected standards, and preparing for emerging threats, LCs can enhance their resilience against cyber-attacks. The SFC's pragmatic approach allows some flexibility for system updates, but immediate action is essential to protect operations and client interests. LCs are encouraged to consult the full circular, including its appendix, for detailed guidance on meeting these expectations.

Source:
https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC7
https://apps.sfc.hk/edistributionWeb/api/circular/openAppendix?lang=EN&refNo=25EC7&appendix=0

Hong Kong Securities and Futures Commission Provides Updated Guidance to Intermediaries on Acceptable Account Opening Approaches

On May 30, 2025, the Hong Kong Securities and Futures Commission (SFC) issued a circular titled "Updates to Acceptable Account Opening Approaches" . The circular updates the five acceptable non-face-to-face (NFTF) account opening approaches published on the SFC's designated webpage, addressing the increasing digitalization and automation in intermediaries' operations. The updates cover certification services, the iAM Smart platform, and an expanded list of eligible jurisdictions for remote onboarding of overseas individual clients.

These measures ensure compliance with the Securities and Futures Ordinance (Cap. 571) (SFO), the Code of Conduct for Persons Licensed by or Registered with the SFC, and the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT Guideline).

The circular provides LCs with guidance to implement secure and efficient NFTF onboarding processes while meeting regulatory requirements.

Certification Services

Certification services, recognized under the Electronic Transactions Ordinance (Cap. 553), are listed as approach number 2 on the SFC's designated webpage for client identity verification in NFTF account opening. These services, detailed on the Digital Policy Office (DPO) website, utilize smartphones with Near Field Communication (NFC) functionality for remote authentication. The Personal (Remote) ID-Cert Class 12, issued by Digi-Sign Certification Services Limited, enables overseas investors holding ePassports compliant with International Civil Aviation Organization (ICAO) standards to subscribe remotely. Over 100 jurisdictions have issued ICAO-compliant ePassports, with public keys stored in the ICAO public key repository.

The process for using certification services is summarized below:

I. Arrange system setup, integration, and testing with the designated service provider (SP) of a recognized Certification Authority (CA).
II. Receive an account opening application from an overseas investor with an ICAO-compliant ePassport.
III. Collect personal information for client due diligence and know-your-client (KYC) procedures.
IV. Obtain applicant's consent to use the SP's certification service to verify identity via NFC technology from the ePassport and issue a digital certificate.
V. Submit account opening documents to the SP for digital signing by the applicant using their digital certificate.
VI. Review the applicant's profile and signed documents to approve the application per internal policies.
VII. Complete client onboarding upon successful verification and approval.

iAM Smart

Introduced by the Hong Kong Special Administrative Region (HKSAR) Government in December 2020, iAM Smart is a digital services platform recognized under paragraph 4.2.1 of the AML/CFT Guideline for client identity verification. Newly added as an acceptable NFTF account opening approach on the SFC's designated webpage, iAM Smart (including iAM Smart+ with digital signing via Hongkong Post iAM Smart-Cert) supports authentication and electronic agreement execution. The SFC has accepted iAM Smart for account opening since its launch, with some LCs already implementing it and others testing its application.

The iAM Smart Sandbox Program, launched by the DPO and Cyberport, provides documentation, training videos, simulated APIs, and support for API integration, security checklists, and privacy impact assessments. LCs can apply through the SFC, while registered institutions should contact the Hong Kong Monetary Authority.

The following process for iAM Smart account opening is summarized below:

I. Join the iAM Smart Sandbox Program (via the Digital Policy Office and Cyberport) to design, develop, and test system integration, including APIs, security checklists, and privacy impact assessments, with ongoing security reviews every two years.
II. Receive an account opening application and obtain authorization from the iAM Smart account holder to verify their identity.
III. Direct the applicant to the iAM Smart app to authorize sharing of personal data (e.g., name, Hong Kong identity card number, date of birth, gender) for identity verification.
IV. Collect identity information and, if authorized, additional details (e.g., address, email) via the iAM Smart form-filling function.
V. Gather further information to conduct client due diligence and know-your-client (KYC) procedures.
VI. Review the applicant's profile and approve the application in accordance with internal policies and the SFC's AML/CFT Guideline.
VII. Obtain a signed client agreement via electronic signature or iAM Smart-Cert digital signing.
VIII. Complete client onboarding upon successful verification and approval.

Eligible Jurisdictions for Remote Onboarding

The SFC maintains a list of eligible jurisdictions for remote onboarding of overseas individual clients, where clients hold bank accounts for initial and ongoing fund movements, as outlined in approach number 5 on the designated webpage. Based on Financial Action Task Force (FATF) mutual evaluations, 15 additional jurisdictions have been added effective immediately: Argentina, Brazil, France, Germany, Greece, India, Indonesia, Japan, Korea, Luxembourg, Netherlands, New

Zealand, Saudi Arabia, South Africa, and Turkey. The updated list is available on the SFC's designated webpage.

LCs must consider restrictions imposed by domestic regulatory authorities, such as the China Securities Regulatory Commission, which may limit services for mainland China clients. Cybersecurity measures are required to protect client accounts and data from threats like phishing and ransomware. LCs are encouraged to participate in the iAM Smart Sandbox Program to access resources and support for implementation.

The circular sets forth updated standards for NFTF account opening, mandating that LCs adopt certification services, iAM Smart, or the expanded list of eligible jurisdictions to ensure secure and compliant client onboarding. These approaches, detailed in the circular's appendices, are aligned with the SFO, the Code of Conduct, and the AML/CFT Guideline, reinforcing regulatory compliance in a digital financial landscape. LCs are required to implement these methods expeditiously, adhere to cybersecurity and jurisdictional obligations, and consult professionals for comprehensive guidance.

Source:
https://apps.sfc.hk/edistributionWeb/api/circular/openFile?lang=EN&refNo=25EC31
https://apps.sfc.hk/edistributionWeb/api/circular/openAppendix?lang=EN&refNo=25EC31&appendix=0
https://apps.sfc.hk/edistributionWeb/api/circular/openAppendix?lang=EN&refNo=25EC31&appendix=1

Hong Kong Securities and Futures Commission Issues Circular to Licensed Corporations and Virtual Asset Service Providers on Latest Findings from Inspections and Standards for Virtual Asset Trading Platforms

On January 16, 2025, the Hong Kong Securities and Futures Commission (SFC) issued a circular to Licensed Corporations (LCs), SFC-licensed Virtual Asset Service Providers, and Associated Entities. The circular addresses findings from on-site inspections of deemed-to-be-licensed virtual asset trading platform (VATP) applicants and establishes mandatory standards of conduct to ensure compliance with the Guidelines for Virtual Asset Trading Platform Operators (VATP Guidelines). The inspections evaluated cybersecurity measures, client asset protection, and know-your-client (KYC) processes, identifying deficiencies that require immediate corrective action. The circular urges operators to align with these standards promptly to ensure robust systems and client safety.

Regulatory Context

The SFC regulates VATPs to ensure investor protection and market integrity in the virtual asset sector. The inspections reflect the SFC's commitment to enforcing the VATP Guidelines, which set out licensing and operational requirements for VATPs operating in or targeting Hong Kong investors. The circular builds prior guidance, emphasizing the need for VATP operators to maintain effective systems, employ qualified staff, and deploy adequate resources to meet regulatory requirements.

Inspection Findings

The SFC's inspections of deemed-to-be-licensed VATP applicants revealed significant deficiencies in key operational areas, necessitating immediate improvements. The observed issues include:

Area	Deficiencies Identified
Cybersecurity	Inadequate network segmentation, outdated encryption algorithms, weak access controls, and insufficient monitoring systems.
Client Asset Protection	Improper segregation of client and operational funds, non-compliance with the 98/2 cold-to-hot wallet ratio, wallet management issues, and inadequate insurance coverage (failing to cover 50% of cold wallet assets and 100% of hot wallet assets).
KYC and Client Access	Unauthorized access from restricted jurisdictions, lack of robust geolocation tools, and insufficient client identity verification procedures and Inadequate due diligence on VPN and proxy detection tools.
Client Money Handling	Indirect deposit of client funds, increasing exposure to risks and Inappropriate bank account signatory arrangements, allowing single-person payments

These findings indicate that many VATP applicants lack the necessary operational and technical capabilities to ensure client safety and regulatory compliance, necessitating immediate corrective actions.

Expected Standards of Conduct

The circular establishes mandatory standards for all VATP operators, including SFC-licensed platforms, deemed applicants, and other applicants, effective immediately.

These standards, which supplement the VATP Guidelines, address cybersecurity, client virtual asset protection, and platform access controls. The following table provides a detailed overview:

Category	Standard	Details
Cybersecurity	Network Access and Segmentation	Segregate critical systems and sensitive data using cloud-native or micro-segmentation techniques.
	Privileged Access Management	Implement a governance framework, manage privileged accounts, ensure transparency, and approve usage.
	Encryption	Use strong encryption for data storage and transmission, with ongoing threat monitoring and algorithm review.
	Security Monitoring Arrangement	Deploy 24/7 security operations centers (SOC) for continuous monitoring and prompt incident handling.
	Detection of Unauthorized Access	Use real-time automated solutions to monitor and identify suspicious access to client accounts.
	Internet Access Control	Grant access to the Internet based on staff duties, implement URL whitelisting to minimize phishing risks.
Client Virtual Assets	Handling of Client Virtual Assets	Allow handling of assets only to authorized personnel (e.g., Responsible Officers), use wallet address whitelisting, and secure keys in Hong Kong.
	Segregation of Client Virtual Assets	Prevent commingling with operator assets in client-designated wallets.
	98/2 Cold/ Hot Wallet Asset Ratio	Apply The "98/2 Requirement", 98% of client virtual assets to be held in cold storage to minimize hacking risks, with prompt transfers to comply if breached.
	Large Withdrawals/ Deposits	Implement protocols for transactions exceeding 2% of client assets to maintain the 98/2 ratio.
	Storage and Access to Seeds and Private Keys	Store in secure environments (e.g., certified Hardware Security Modules) in Hong Kong, with stringent access controls.
	Contingency and Recovery Plans	Develop comprehensive plans for disruptions, restore services within 12 hours, and maintain equivalent backup facilities.
	Insurance Arrangement	Ensure coverage for 50% of cold wallet assets and 100% of hot wallet assets, reviewing exclusions and deductibles.
	Handling of Client Money	Deposit client funds directly into segregated bank accounts, with dual signatory controls to prevent fraud, in compliance with the Client Money FAQs (issued May 31, 2023) for financial management.
Access to Platform Services	Access to Services	Conduct due diligence with advanced geolocation, VPN, and proxy detection to prevent access from restricted jurisdictions (include sanctioned regions and those prohibiting virtual asset trading).

The SFC reminds all VATP operators to review their policies, procedures, systems, and processes against the established standards and address identified deficiencies promptly. Operators must deploy adequately qualified staff with relevant professional qualifications, training, or experience, as well as sufficient technology and financial resources, per paragraphs 11.6, 11.7, and 12.5 of the VATP Guidelines. Operators are advised to contact their SFC case officers for clarification and consult the detailed guidance available on the SFC's website. The requirement for external assessments, such as penetration tests and vulnerability assessments,

emphasizes the importance of operational resilience and client protection.

Source:
https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC3
https://apps.sfc.hk/edistributionWeb/api/circular/openAppendix?lang=EN&refNo=25EC3&appendix=0
https://apps.sfc.hk/edistributionWeb/api/circular/openAppendix?lang=EN&refNo=25EC3&appendix=1

Information in this alert is for reference only and should not be relied on as legal advice.