New SFC Custody Requirements for VATPs & Investor Warnings re. Stablecoin Market Movements

New custody requirements have been imposed on SFC-licensed virtual asset trading platforms (**VATPs**) in the Circular to licensed virtual asset trading platform operators on custody of virtual assets[1] published by Hong Kong's Securities and Futures Commission (**SFC**) on 14 August 2025.

On the same day, the SFC and Hong Kong Monetary Authority (**HKMA**) issued a Joint statement on stablecoin-related market movements[2] warning investors about volatility in stablecoin prices that it says may be driven by speculation about plans for certain stablecoins to seek licensing under the recently implemented Stablecoins Ordinance (Cap. 615).

The following provides a summary of the custody standards now expected of SFC-licensed VATPs and the contents of the SFC/HKMA statement on market movements in stablecoins.

SFC Circular to Licensed Virtual Asset Trading Platforms on Custody of Virtual Assets

The SFC's latest circular sets out the minimum custody obligations of SFC-licensed virtual asset (**VA**) trading platform operators and their associated entities (together, **VATP Operators**) and gives examples of best practices which, while not compulsory, provide ways of meeting the new minimum obligations. The new standards elaborate on the obligations on VATP Operators under the SFC Guidelines for Virtual Asset Trading Platform Operators[3] (**VATP Guidelines**) in relation to: senior management responsibilities; client cold wallet infrastructure and operation; wallet solutions (including third party wallet solutions); ongoing real time threat monitoring; and staff training and awareness.

These standards will also form the baseline compliance criteria for SFC-licensed virtual asset custodian service providers on implementation of the proposed licensing regime set out in the SFC/FSTB Public Consultation on Legislative Proposal to Regulate Virtual Asset Custodian Services,[4] which is under consultation until 29 August 2025. For a summary of the proposed licensing regime, please see our newsletter, SFC & FSTB Consult on Regulation of Virtual Asset Custodians.[5]

1 SFC. 15 August 2025. "Circular to licensed virtual asset trading platform operators on custody of virtual assets"
2 SFC. 15 August 2025. *"Joint statement by the SFC and the HKMA on stablecoin-related market movements"*
3 SFC. (June 2023). *"Guidelines for Virtual Asset Trading Platform Operators"*
4 SFC and FSTB. *"Public Consultation on Legislative Proposal to Regulate Virtual Asset Custodians"*
5 Charltons. 5 August 2025. *"SFC & FSTB Consult on Regulation of Virtual Asset Custodians"*

The impetus for the VA custody obligations were significant financial losses recently suffered by overseas VA trading platforms due to cybersecurity incidents. These apparently revealed weaknesses in wallet systems and the associated controls irrespective of custody methods, including vulnerabilities in hot and cold wallet systems and weaknesses in platforms' day-to-day management, internal controls, third party oversight and threat monitoring.

In February 2025, the SFC published its ASPIRe regulatory roadmap[6] for Hong Kong's VA market which recognised the evolution in VA custody technologies and noted plans to *"explore transitioning to more technology-neutral, outcome based standards"*. It stated, in particular that VATPs *"may possibly adopt more innovative solutions, provided that they demonstrate robust asset protection measures and maintain a secure, auditable control environment"*. An SFC investigation into SFC-licensed VATPs' VA custody controls apparently revealed some inadequacies. The latest circular on VATPs' required VA custody arrangements is intended to set the required minimum standards that must be met before the SFC will consider allowing VATPs to transition to more advanced custody technologies.

The table below provides a summary of the existing requirements under the SFC's VATP Guidelines and the additional obligations imposed by the SFC's Circular to licensed virtual asset trading platform operators on custody of virtual assets (**SFC Circular on VATPs' Custody Obligations**).

The SFC expects VATP Operators to critically assess their VA custody framework, procedures and controls to ensure compliance with the new standards. Compliance with these requirements should also be part of VATP Operators' annual external compliance and technology assessment.

	VATP Guidelines' Requirements	SFC Circular on VATPs' Custody Obligations
1	**SFC-licensed VATP Operators: Senior Management Responsibilities**	
	Effective corporate governance, risk management, internal controls and compliance are fundamental to VATP Operators' competence.[7] Senior management are accountable for upholding operational standards and ensuring compliance with proper procedures.[8]	Senior management are required to ensure that: • effective policies, procedures and internal controls are implemented; and • adequate senior management oversight and governance is provided by suitably qualified and experienced individuals. In addition, VATP Operators should designate at least one Responsible Office or Manager-in-Charge to oversee the matters referred to sections 2 to 6 below.
2	**SFC-licensed VATP Operators: Client Cold Wallet Infrastructure**	
	Paragraph 10.8 requires VATP Operators to enforce robust internal controls and governance frameworks for private key management. This includes ensuring the secure generation, storage and backup of all cryptographic seeds and private keys. Whenever feasible, these should be created offline and safeguarded in a certified secure environment—such as a Hardware Security Module (**HSM**)—throughout their lifecycle.	VATP Operators must: • conduct thorough due diligence when selecting an HSM provider and carry out regular ongoing assessments to ensure its continued reliability; • when evaluating HSM providers, VATP Operators must verify the vendor's ability and ongoing commitment to: maintain security standards through effective patch management; and promptly validate the patched HSM and update its certification after applying any necessary security patches; and • to reduce exposure to online threats, cold wallet systems should avoid including smart contracts on public blockchains.
3	**SFC-licensed VATP Operators: Client Cold Wallet Operation**	

6 SFC. 19 February 2025. *"A-S-P-I-Re" for a brighter future SFC's regulatory roadmap for Hong Kong's virtual asset market"*
7 Paragraphs 3.4 and 3.7
8 Paragraph 5.1

	Under paragraph 10.10, VATP Operators must: • adopt procedures for VA deposits and withdrawals that protect against losses due to fraud, theft, professional misconduct etc.; • implement safeguards to prevent fraudulent/forced requests and controls to prevent unauthorised transfers by employees; and • ensure destination addresses for client withdrawal instructions cannot be altered before transactions are signed and broadcast to the blockchain.	VATP Operators must: • ensure that generation and safeguarding of seeds and private keys are conducted on air-gapped cold wallet devices; • regularly evaluate potential security threats, particularly prior to significant operational changes (e.g., updates to systems, processes, or authorised personnel); • implement multi-layered integrity checks across transaction phases, ensuring end-to-end protection from transaction initiation to blockchain submission. Clear role segregation must be enforced to mitigate risks; • implement effective controls to block unauthorised cold wallet transactions. Key measures include: whitelist controls to prevent VA transfers to unapproved wallet addresses; controls and oversight of changes to the cold wallet whitelist; and automatic verification of transactions to confirm their legitimacy and detect any irregularities; • transaction approval must be conducted on dedicated devices with minimal network exposure and reduced functionality. These devices must be physically segregated from standard workstations to minimise vulnerability; • critical transaction data integrity checks must be conducted using air-gapped devices stored in a cold vault. All code modifications to these devices should require physical access to maintain verification integrity; • for transactions requiring manual approval before signing, all details must be presented in a clear, easily understandable format to allow signers to review the information before signing. The good practices outlined include the following: (1) A cold wallet system including an air-gapped HSM and a signing terminal within the cold wallet vault. Key features are: • **a controlled access system**: entry to the secured area requires multi-factor authentication, and comprehensive logging of all entries and exits; and • **continuous surveillance**: the vault is continuously monitored by surveillance cameras; and • **signing restrictions**: if a displayed transaction does not correspond to the intended transaction, the signing terminal will halt the process and alert the signers via a screen notification. (2) Use of dedicated hardware devices only for review and approval of transactions. The devices are used only for wallet operations and ensure clear segregation from the approvers' usual activities. (3) Use of a final stage pre-broadcast data validation check as an additional layer of end-to-end verification. Before broadcasting a signed blockchain transaction, the system performs an integrity check by cross-verifying the signed transaction with its original unsigned version. Any detected inconsistencies prevent the signed transaction from being broadcast to the network.

4	**SFC-licensed VATP Operators: Use of wallet solution and third party provider**	
	Under paragraphs 12.8 and 12.10, VATP Operators must: • **rigorously test** all system changes – including new implementations or upgrades – prior to live deployment; • **conduct periodic audits** of their platforms to ensure sustained system integrity, operational reliability, security robustness and performance capacity; • **implement strong contingency plans** to address potential disruptions or failures;	**Mandatory Role Separation**: Strict segregation of duties and oversight mechanisms must be maintained for wallet code management, irrespective of whether the codebase is developed internally or externally. **Multi-Layered Security Protocols**: Controls must include gatekeeping procedures such as code reviews, testing, software supply chain management, management approvals and secure deployment practices. **Comprehensive Documentation**: Audit trails must be maintained for all code management activities. **Procedure Access Controls**: Administrator access to production systems must be strictly controlled according to principles of least privilege and privilege separation and recognised industry standards. **Third Party Wallets**: Assessments of third parties must include independent code reviews and understanding the wallet provider's software development and release processes before onboarding or making material changes. When utilising third party wallet solutions, VATP Operators must perform thorough due diligence during provider selection and continuously monitor the provider's adherence to the VATP Guidelines. This includes regularly assessing the provider's security controls, operational protocols, incident reporting practices, and regularly testing its disaster recovery readiness. Additionally, VATP Operators should regularly evaluate inherent risks tied to third party dependencies, implement measures to address vulnerabilities, and conduct independent cybersecurity audits of the deployed system as stipulated in paragraph 12.13 of the VATP Guidelines to ensure sustained compliance and risk mitigation. VATP Operators must also implement ongoing emergency preparedness protocols, including regular testing of business continuity plans (BCPs) through comprehensive drills. These exercises should involve third-party providers to validate that recovery timelines align with SFC requirements.
5	**SFC-licensed VATP Operators: Ongoing Real-time Threat Monitoring**	
	Paragraphs 12.12(f) and 12.14 require VATP Operators to implement robust security controls over their platform infrastructure, which includes setting up a Security Operations Centre (**SOC**) or similar unit responsible for overseeing all monitoring systems and coordinating incident detection. Additionally, they are required to develop formal, documented protocols that clearly define escalation procedures for both potential and confirmed cybersecurity incidents.	VATP Operators must ensure continuous, real-time alignment between on-chain client asset records and ledger balances. In the event of any unexplained transaction discrepancies, the SOC or designated monitoring team must immediately receive automated alerts and coordinate swift corrective measures to resolve the issue. The SOC must collaborate with specialists in wallet management, operations, and technology to regularly evaluate and optimise alert systems and their settings. Senior management must supervise this process to ensure that alert thresholds are calibrated for early identification of potential issues. Additionally, VATP Operators need to implement strong detection systems to identify unauthorised access or breaches targeting critical wallet infrastructure—such as cold wallet vaults, signing devices, databases, production binaries, and code repositories—and ensure comprehensive protection across all sensitive components.

	Paragraphs 12.12(f) and 12.14 require VATP Operators to implement robust security controls over their platform infrastructure, which includes setting up a Security Operations Centre (**SOC**) or similar unit responsible for overseeing all monitoring systems and coordinating incident detection. Additionally, they are required to develop formal, documented protocols that clearly define escalation procedures for both potential and confirmed cybersecurity incidents.	VATP Operators must implement comprehensive monitoring processes that encompass not only their custody systems but also all associated dependencies—such as third-party vendors, underlying technologies, blockchain protocols, encryption algorithms and common libraries—to ensure the ongoing security of client assets. Additionally, the monitoring framework should proactively account for major industry security incidents and publicly identified security vulnerabilities that could compromise the safety of the custody system. Security monitoring must be continuously conducted, i.e., 24/7 and during holidays. Sufficient resources must be allocated to addressing contingency issues and procedures for mobilising additional resources for incidents occurring outside normal business hours. A structured framework must be in place to handle security alerts and manage incidents according to their degree of severity. Good practice recognised in the Circular refers to firms implementing a 24/7 monitoring function which successfully identified an industry incident immediately after it appeared on social media around midnight in Hong Kong. While the incident did not directly affect the firms' custody arrangements, it prompted the security team to escalate the matter to senior management without delay. A response team with the appropriate mix of senior management, technology and security staff was quickly assembled to thoroughly assess the incident's potential impact on the firm's custody systems.
6	**SFC-licensed VATP Operators: Staff Training and Awareness**	
	Paragraph 12.5 of the VATP Guidelines requires VATP Operators to allocate appropriately qualified staff and sufficient expertise, technological resources and financial support to the design, development, operation and modification of their platforms. Section III(3) of the Internal Control Guidelines additionally provides that management must ensure that staff receive adequate training tailored to their specific roles, both at the outset and on an ongoing basis.	VATP Operators must: • ensure that transaction signers receive comprehensive training to fully understand the verification requirements and appropriate procedures in the case of any exception or uncertainty concerning a transaction; and • implement controls to prevent blind signing and ensure effective manual transaction review or approval. As an example of good practice, the SFC cited a firm which, in addition to providing general security awareness training, also trains staff on transaction verification, with specific focus on procedures to prevent errors during manual verification.

SFC and HKMA Joint Statement on Stablecoin-related Market Movements

In their Joint Statement on Stablecoin-related Market Movements, the SFC and HKMA warn investors about recent, abrupt movements in the market relating to stablecoins, which they say appear to be linked to corporate announcements, news reports and social media posts or speculation suggesting intentions to apply for a stablecoin issuer licence under Hong Kong's Stablecoin Ordinance or engage in related activities. The statement notes that some of these have included claims to have met with Hong Kong's financial regulators.

The SFC and HKMA reiterate that the licensing of stablecoin issuers requires them to meet stringent criteria, and that a licence application or an expression of interest in applying for a stablecoin issuer licence provide no indication of whether or not the entity will be successful in obtaining a licence.

The regulators urge investors to avoid making investment decisions based only on market hype or price momentum and encourage them to carry out thorough research and exercise caution when making investments.

The SFC and HKMA also caution market participants against making statements that could mislead investors or result in unrealistic expectations.

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