HKMA Consultations on Obligations of HKMA-Licensed Stablecoin Issuers

The Hong Kong Monetary Authority (**HKMA**) issued consultation papers on 26 May 2025 on the ongoing obligations, including in respect of anti-money laundering (**AML**) and counter-financing of terrorism (**CFT**), of fiat-referenced stablecoin issuers licensed by the HKMA (**HKMA-licensed Stablecoin Issuers**) under the recently passed Stablecoins Ordinance (Cap. 656 of the laws of Hong Kong) (**Hong Kong Stablecoins Ordinance**) which will take effect on 1 August 2025.[1] For details of the Hong Kong stablecoin regime under the Stablecoins Ordinance, please see our April newsletter "Hong Kong Stablecoin Regulation".

The HKMA's proposed requirements for HKMA-licensed Stablecoin Issuers were set out in two consultation papers published on 26 May 2025:

- HKMA Consultation on the Draft Guideline on Supervision of Licensed Stablecoin Issuers (**HKMA Stablecoins Guideline Consultation**) which sets out how the HKMA expects HKMA-licensed Stablecoin Issuers to comply with the requirements of Schedule 2 to the Hong Kong Stablecoins Ordinance (**Schedule 2 SO**); and

- HKMA Consultation Paper on the Proposed AML/CFT Requirements for Regulated Stablecoin Activities (**HKMA Stablecoins AML/CFT Consultation Paper**) which consults on the proposed AML and CFT obligations of HKMA-licensed Stablecoin Issuers under the HKMA's proposed Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Stablecoin Issuers) (**HKMA AML/CFT Guideline**), set out in the Consultation Paper's Annex.

The consultation period for both consultations ended on 30 June 2025.

Draft Guideline on Supervision of Licensed Stablecoin Issuers

The draft Guideline on Supervision of Licensed Stablecoin Issuers (**HKMA Stablecoin Guideline**) sets out how stablecoin issuers are expected to meet the criteria for HKMA-licensing in Schedule 2 of the Hong Kong Stablecoins Ordinance.[2] The following provides a summary of the key licensing requirements and how the HKMA expects them to be met.

[1] Government of the Hong Kong Special Administrative Region. 6 June 2025. *"Stablecoins Ordinance to Commence Operation on August 1, 2025*. Available at: https://www.info.gov.hk/gia/general/202506/06/P2025060600275.htm

[2] Stablecoins Ordinance, section 24

Schedule 2 SO Requirement	HKMA Stablecoin Guideline Requirements
A. RESERVE ASSET MANAGEMENT	
Full asset backing *Section 5(2)*: the market value of the reserve assets pool backing each type of issued stablecoins must at all times equal or exceed the par value of the outstanding stablecoins of that type in circulation.	HKMA-licensed Stablecoins Issuers should: • implement robust measures that: o take account of the reserve assets' risk profile and ensure appropriate over-collateralisation to mitigate market risk; o adopt custodial arrangements that do not compromise full backing (e.g., account-level fees should not be deducted from accounts holding reserve assets); and o conduct ongoing monitoring and regular reconciliations between the reserve assets' market value and the par value of outstanding stablecoins in circulation to ensure compliance with the full backing requirement (paragraph 2.1.1); • adopt a consistent and prudent method for calculating the market value of reserve assets that uses reasonable, reliable data sources reflecting prevailing market prices and apply the more prudent side of bid/offer prices. Use a consistent and transparent approach to calculate the par value of outstanding stablecoins. HKMA-licensed stablecoin issuers should ensure that there is no mismatch between the valuation methods used for the reserve assets and outstanding stablecoins' par value (paragraph 2.1.2); and • have effective asset-backing arrangements for stablecoins that are temporarily restricted from circulation (e.g., due to a court order or enforcement action), but could re-enter circulation to ensure that they can meet the redemption requirements once the restrictions are removed. (Paragraph 2.1.3)
Acceptable reserve assets *Section 5(5)*: Reserve assets must be of high quality and liquidity and have minimal investment risks.	The following are acceptable forms of reserve assets: 1) bank deposits for terms not exceeding three months; 2) marketable debt securities that: o are issued or guaranteed by a government, central bank, public sector entity, qualified international organisation[3] or multilateral development bank; o have a maximum residual maturity of one year; o qualify for a 0% risk weight (under sections 55 to 58 of the Banking Capital Rules (Cap. 155L)); or are denominated in the domestic currency of a government or central bank stablecoin issuer; o are highly liquid; and o are not obligations of a financial institution or an associated entity of a financial institution, that is not a public sector entity bank; 3) cash receivable from overnight reverse repurchase agreements with minimal counterparty risk, collateralised by assets referred to under 2 above; 4) investment funds that invest in any of the above assets whose sole purpose is managing the HKMA-licensed Stablecoins Issuer's reserve assets; and/or 5) other asset types acceptable to the HKMA. (Paragraph 2.2.1)

[3] Defined as relevant international organisations as defined in section 2(1) of the Banking (Capital Rules) (Cap. 155L)

Referenced currency *Section 5(3)*: Reserve assets for each stablecoin type must be denominated in the same referenced currency as the issuer's stablecoin, unless the HKMA approves the holding of reserve assets in a different referenced asset.	Reserve assets must be denominated in the same referenced currency as the HKMA-licensed Stablecoin Issuer's stablecoins. If there are more than one referenced currency, reserve assets must be denominated in the referenced currencies in the same ratio as the stablecoins. The HKMA must give its prior written approval of a currency mismatch. The HKMA-licensed Stablecoin Issuer will need to demonstrate the need and rationale for the currency mismatch and implement measures (e.g., over-collateralisation) to manage relevant risks and prevent risks being transferred to stablecoin holders or disrupting its operations. The HKMA recognises the stability of the Hong Kong Dollar (**HKD**) under the Linked Exchange Rate System band (HKD 7.75-7.85 per United States Dollar (**USD**)). It will therefore allow HKD-referenced stablecoins to be backed by USD-denominated reserves. (Paragraphs 2.3.1 and 2.3.2)
Reserve assets segregation & safekeeping *Section 5(1)*: The reserve assets for each stablecoin must be segregated from any other reserve assets of the issuer.	HKMA-licensed Stablecoin Issuers should put in place effective trust arrangements that segregate reserve assets backing their stablecoins from their own assets to ensure that they are available to meet redemption requests at par value. Acceptable trust arrangements include appointing an independent trustee or executing a declaration of trust over the reserve assets. Before implementing a trust arrangement, HKMA-licensed Stablecoin Issuers must obtain an independent legal opinion confirming that the trust arrangement is effective, and they should submit that opinion to the HKMA. (Paragraph 2.4.2)
Section 5(4): Each pool of reserve assets must be adequately protected against claims by the issuer's other creditors and kept separate from the HKMA-licensed Stablecoin Issuer's other funds.	All income or loss generated from managing the reserve assets belong to the HKMA-licensed Stablecoin Issuer. The trust arrangement must therefore include a clear mechanism to allow the regular transfer of excess assets (i.e., those exceeding the internal target set by the HKMA-licensed Stablecoin Issuer) from the reserve assets account to the stablecoin issuer's own account. The mechanism should include a triggering mechanism and detailed procedures to ensure that only the excess assets are transferred out of the reserve assets account. (Paragraph 2.4.3)
Section 5(8): HKMA-licensed Stablecoin Issuers must implement adequate and appropriate control systems for: • assessing the risks associated with having reserve assets managed by third parties; • monitoring third parties' performance; and • managing their relationship with third parties.	HKMA-licensed Stablecoin Issuers should enter into a written contractual agreement with a qualified custodian for the reserve assets' safekeeping. Acceptable custodians include Hong Kong licensed banks and other asset custodians appointed under an arrangement that is acceptable to the HKMA. Notwithstanding the appointment of a custodian, HKMA-licensed Stablecoin Issuers remain primarily responsible and accountable for managing and safekeeping the reserve assets. (Paragraph 2.4.4)

Prohibition on interest bearing stablecoins Section 15: HKMA-licensed Stablecoin Issuers are prohibited from paying interest on their stablecoins and from allowing others to pay interest on them. “Interest” is defined to include any profit, income or other return payable to stablecoin holders based on: • how long the stablecoin has been held; or • its par value or market value.	HKMA-licensed Stablecoin Issuers should not pay interest or interest-like incentives in any form to holders of their stablecoins. They can, however, offer marketing incentives that do not amount to interest payments. Accordingly, all income or losses generated from managing the reserve assets (including interest or capital gains/losses) must be attributed solely to the HKMA-licensed Stablecoin Issuer and not to the holders.
Disclosure and reporting *Section 5(7)*: HKMA-licensed Stablecoin Issuers must make timely public disclosures of: • their reserve assets management policy; • an assessment of the risks arising from their reserve assets and their management of the risks; • the composition and market value of their reserve assets; and • the results of regular independent attestation and audit of their reserve assets.	HKMA-licensed Stablecoin Issuers should prepare daily statements of: • the par value of their outstanding stablecoins in circulation; and • the market value and composition of their reserve assets. They should report this information to the HKMA weekly and publish it on their website in a prominent position. This disclosure requirement is mandatory unless the HKMA approves different disclosure arrangements. HKMA-licensed Stablecoin Issuers should appoint a qualified independent auditor acceptable to the HKMA to regularly conduct an attestation on their reserve assets. The frequency of attestation must be agreed with the HKMA. The attestation should cover: • the market value and composition of the reserve assets; • the par value of the outstanding specified stablecoins in circulation; and • whether the reserve assets are adequate to fully back the par value of the outstanding stablecoins in circulation: (a) as at the last business day of the period covered by the auditor’s attestation report and (b) as at at least one randomly selected business day during the period. HKMA-licensed Stablecoin Issuers should submit the auditor’s attestation report to the HKMA and disclose it on their website in a reasonably prominent location.
Section 13: HKMA-licensed Stablecoin Issuers must publish a white paper for each stablecoin it issues providing comprehensive information about the stablecoin.	HKMA-licensed Stablecoin Issuers are required to publish white papers on their website in a reasonably prominent position. They must notify the HKMA before publishing or making material changes to a white paper. (Paragraph 8.23) White papers should set out: • general information about the HKMA-licensed Stablecoin Issuer; • detailed information about the stablecoins; • the arrangements for the management of the reserve assets;

Section 13: HKMA-licensed Stablecoin Issuers must publish a white paper for each stablecoin it issues providing comprehensive information about the stablecoin.	• the mechanisms for issue, redemption and distribution covering the procedures, redemption rights, timeframe and any conditions and fees involved; • the technology underlying the stablecoins; and • the risks associated with using the stablecoins (Paragraph 8.24).
Section 6.5: HKMA-licensed Stablecoin Issuers must publicly disclose the redemption rights attaching to their stablecoins, including any redemption fee payable, any conditions for exercising the redemption right, the procedures for redemption and the processing time for redemption requests.	The information required to be provided to holders by section 6.5 of Schedule 2 to the Stablecoins Ordinance should be set out in the white paper for the stablecoins together with the terms and conditions applicable to the stablecoins. (Paragraph 3.5.1)
Reporting to the HKMA	HKMA-licensed Stablecoin Issuers must submit to the HKMA their annual audited financial statements which should include an audit of the reserve assets backing their issued stablecoins. (Paragraph 8.25) They should also conduct regular audits to check compliance with their own issuance, redemption and distribution policies, and applicable regulatory requirements. Audit outcomes—including any material findings—must be reported to the HKMA promptly, with the audit report and supporting documents provided upon request. Any breach of statutory/regulatory requirements or material non-compliance with policies on issuance, redemption and distribution must be reported to the HKMA immediately. (Paragraph 3.5.3)
B. ISSUE, REDEMPTION & DISTRIBUTION OF STABLECOINS	
Issue requirements Section 11: An HKMA-licensed Stablecoin Issuer's issue of a stablecoin must be prudent, having regard to its purpose, business model and operational arrangement.	HKMA-licensed Stablecoin Issuers should maintain an effective stablecoin issuance mechanism. In practice, they should only issue stablecoins to their customers and issues should be made promptly after receiving the funds and a valid request for issue. The currency of funds received from customers should be the same as the stablecoin's referenced currency (or currencies, and in the same ratio if more than one). Crucially, every stablecoin minted must be matched by an immediate and equivalent increase in the relevant reserve assets pool.
Distribution requirements *Section 11*: See above.	Although HKMA-licensed Stablecoin Issuers will have different business models and operational arrangements, if an issuer enters into arrangements with a third party for the distribution of its stablecoins, it needs to ensure that these arrangements will not negatively impact the prudence and soundness of the issue. HKMA-licensed Stablecoin Issuers therefore need to consider the legal and regulatory requirements in the jurisdictions in which their stablecoins will be distributed and the licensing status of any third party distributor. If stablecoins will be offered in Hong Kong, any distributor must be a permitted offeror under the Stablecoins Ordinance. In conducting the necessary risk assessments and due diligence on third parties, HKMA-licensed Stablecoin Issuers must take into account (among others):

Distribution requirements *Section 11*: See above.	• their size, capabilities, expertise, track record and reputation; and • the adequacy of the third party's governance, conduct standards, risk management, and internal controls. For secondary market liquidity providers, HKMA-licensed Stablecoin Issuers must assess the need for their engagement, and the extent and scope of their engagement given their business model and operations. HKMA-licensed Stablecoin Issuers need to ensure that the arrangements prioritise maintaining a stable value for the stablecoins in the secondary markets, and that all potential and/or actual conflicts of interest have been identified and mitigated.
Redemption *Section 6(1) and (2)*: HKMA-licensed Stablecoin Issuers must redeem stablecoins at par on receipt of a valid redemption request from holders. They must not impose any unduly onerous condition on redemption or charge fees beyond what is reasonable. Valid redemption requests must be honoured as soon as practicable and holders should be paid the par value less any reasonable redemption fee in the stablecoin's referenced currency or currencies. *Section 6(4)*: HKMA-licensed Stablecoin Issuers must provide stablecoin holders with rights in the event of their insolvency to: • direct the disposal of the reserve assets pool to redeem all outstanding stablecoins of the same type pro rata; and • claim against the HKMA-licensed Stablecoin Issuer for any shortfall if the proceeds from the disposal of the reserve assets is not enough to redeem all the outstanding stablecoins in full.	HKMA-licensed Stablecoin Issuers should obtain an independent legal opinion to confirm that they provide stablecoin holders with the rights required by section 6 of the Stablecoins Ordinance. That legal opinion must be submitted to the HKMA and an updated legal opinion will be required if there is any material change to these rights. (Paragraph 3.2.2) HKMA-licensed Stablecoin Issuers should also maintain effective redemption procedures for the stablecoins they issue. Holders' redemption requests must be honoured within one business day of their receipt, unless the HKMA's prior written approval has been obtained. (Paragraph 3.2.3) Relevant factors in determining whether redemption fees are reasonable include (without limitation) whether the fees are proportional to the HKMA-licensed Stablecoin Issuer's operational costs of redeeming the stablecoins and how they compare with prevailing industry practices. (Paragraph 3.2.4) The assessment of whether a condition is unduly burdensome will consider, among others, whether: • fulfilment of the condition is reasonably practicable; • the condition is required due to legal or regulatory obligations of the HKMA-licensed Stablecoin Issuer; and • the condition will cause undue hardship to stablecoin holders. (Paragraph 3.2.4) In honouring redemption requests, HKMA-licensed Stablecoin Issuers should transfer the par value of the stablecoins received from the holder to the holder after deducting their reasonable redemption fee. Funds must be denominated in the stablecoin's referenced currency, and if there is more that one referenced currency, in those currencies in the same ratio referenced by the stablecoins. Each draw-down of reserve assets for honouring a redemption request must coincide with a corresponding decrease in the par value of the outstanding stablecoins in circulation. (Paragraph 3.2.5)

Customer on-boarding	HKMA-licensed Stablecoin Issuers must implement robust customer on-boarding policies and procedures for the issue and redemption of stablecoins. Where applicable, they should conduct customer due diligence on potential stablecoin holders before issue and redemption as required by the HKMA AML/CFT Guideline. They must also comply with all relevant laws and regulations in the jurisdictions in which they will offer stablecoins. which should be implemented by policies and procedures that: • block issuance in jurisdictions where it is illegal to do so (e.g., by verifying customer IDs, geolocation lookup via Internet Protocol addresses, access blocking); • ensure compliance with regulations applicable to its operations and marketing activities in relevant jurisdictions; and • actively monitor regulatory changes affecting stablecoins in order to make appropriate changes to its operations. Additionally, HKMA-licensed Stablecoin Issuers must have controls to mitigate the risk of location spoofing (e.g., use of VPNs) during remote customer on-boarding and in the course of their business operations. For example, VPN use can be detected by implementing controls that can examine network protocols and device configurations, and by verifying IP addresses against those of commercial VPN providers.
C. BUSINESS ACTIVITIES IN RELATION TO ISSUANCE OF SPECIFIED STABLECOINS IN HONG KONG	
Restrictions on business activities *Section 12*: HKMA-licensed Stablecoin Issuers must: • have sufficient resources for conducting stablecoin activites; • obtain HKMA consent for the conduct of any business activity other than a licensed stablecoin activity (**Other Business Activities**); • implement controls to ensure that: (a) any other business activity approved by the HKMA does not cause significant risk to its stablecoin activities; and (b) conflicts of interest (actual or potential) can be properly managed and mitigated.	HKMA-licensed Stablecoin Issuers will need to: • implement governance arrangements for the conduct of other HKMA-approved business activities; and • carry out a risk assessment to identify risks and implement controls to manage and mitigate the risks identified. The restrictions related to Other Business Activities do not apply to HKMA-licensed Stablecoin Issuers that are authorised institutions under the Banking Ordinance.

Issuance of more than one type of specified stablecoins	HKMA-licensed Stablecoin Issuers can issue more than one type of stablecoin under their licence, but should consult the HKMA before issuing a new type of stablecoin (e.g., a stablecoin referencing different official currencies). The issuer will need to demonstrate to the HKMA that: • it has adequate capabilities and resources to manage the issue of different types of stablecoins; and • that the issue of an additional type of stablecoin will not adversely impact its existing stablecoin operations.
D. FINANCIAL RESOURCES OF HONG KONG STABLECOINS ISSUERS	
Minimum paid-up share capital *Section 4*: HKMA-licensed Stablecoin Issuers must have paid-up share capital of HKD 25 million (or its equivalent in a currency freely convertible into Hong Kong dollars) or other financial resources in an equivalent amount approved by the HKMA. *Section 17 Stablecoins Ordinance*: The HKMA may impose higher financial resources requirements under licence conditions.	Financial resources meeting these requirements must be used solely for business activities and cannot be diverted to dealing with related parties (shareholders, directors, affiliated companies or senior management). Authorised institutions are exempt from these requirements but must comply with the requirements under the Banking Ordinance.
E. RISK MANAGEMENT	
Risk governance	HKMA-licensed Stablecoin Issuers must establish robust risk governance frameworks defining clear responsibilities for the board, senior management and any specialised committees to monitor their adherence to risk appetite and risk limits, and identify, measure, manage and control risks. This should involve implementing a three-line defence model with distinct roles for: 1. business units which conduct ongoing risk identification, assessment, management and reporting; 2. the independent risk management and compliance functions which are responsible for risk identification, assessment, monitoring, reporting, control and mitigation and management of the compliance risk, respectively; and 3. an independent internal audit function. The risk management, compliance and internal audit functions must have adequate authority and resources and unfettered access to information, and be independent of the front-line operations. The risk management and compliance functions should generally report directly to senior management while the internal audit function should report to the board or a board committee. The risk management function should also have direct access to the board, and the compliance function must be able to report matters directly to the board where necessary. (Paragraph 6.2)
Risk management framework and internal control system	HKMA-licensed Stablecoin Issuers must establish a comprehensive, board-approved risk management framework with documented policies and procedures to identify, monitor, report and manage all material risks—including credit, liquidity, market, technology, operational, reputation, and AML/CFT risks. This framework must clearly define accountability and authority while enabling:

Risk management framework and internal control system	• Risk identification and assessment, including the evaluation of exposure to material risks associated with their businesses taking into account internal factors (business model, operations) and external factors (market trends, target sectors); • Risk monitoring and reporting: ongoing surveillance of risk profiles and material exposures using qualitative and quantitative metrics for early warnings, with timely, actionable reports incorporating audit findings and feedback provided to senior management and the board; and • Risk control and mitigation employing robust internal controls ensuring operational integrity, fraud and error prevention, data security, and compliance with laws and policies, supported by verification processes and consequences for non-compliance.
Credit, liquidity and market risk management *Section 5(6)(a)*: HKMA-licensed Stablecoin Issuers are required to implement comprehensive risk management policies and procedures to ensure reserve assets are properly managed and valid redemption requests are promptly honoured.	For Credit Risk: Measures should be implemented to manage credit risk exposures to counterparties by setting and enforcing internal limits based on their creditworthiness. Issuers should also establish breach response procedures which include promptly notifying the HKMA of prolonged breaches (e.g., of more than one business day). For Liquidity Risk: Measures should be put in place to project and monitor redemption demand under normal and stressed conditions. Policies to manage the reserve assets' liquidity profile (e.g., managing allocation according to instrument types, maturities, counterparties) should also be put in place to ensure timely payouts to meet valid redemption requests, considering factors such as the liquidity of instruments, settlement times, term and early withdrawal options and concentration risks. HKMA-licensed Stablecoin Issuers must also set and enforce internal limits for liquidity indicators (e.g., cash ratios and conversion of reserve assets within certain time limits), with breach procedures and HKMA notification for prolonged breaches of internal limits. For Market Risk: HKMA-licensed Stablecoin Issuers should set and enforce internal limits for market risk indicators, with breach procedures and HKMA notification protocols for prolonged breaches (e.g., exceeding one business day). Issuers should also apply appropriate over-collateralisation for reserve assets to cover market risk. Stress testing: Quarterly stress testing should be carried out using strict but plausible scenarios to assess the robustness of reserve assets and the adequacy of risk management measures against credit, liquidity and market stress. Methodologies, data sources and results must be submitted promptly to the board and the HKMA. Scenarios and assumptions require regular review and board approval for material changes.
Technology risk management	HKMA-licensed Stablecoin Issuers must maintain and implement a technology risk management framework to ensure the adequacy of controls over their information technology operations, the quality and security of their technologies and the safety and efficiency of their operations. The HKMA requires the technology risk management framework to cover at least the following: • **Token management**

Technology risk management	The HKMA expects the technology risk management framework to document the token standards and distributed ledgers used and the smart contract architecture for each stablecoin type. HKMA-licensed Stablecoin Issuers should adopt a suitable level of authorisation requirements and conditions depending on the level of risk of each of the operations throughout the stablecoins' lifecycle. Additionally, HKMA-licensed Stablecoin Issuers should implement specific authorisation controls such as multi-signature requirements for high-risk lifecycle operations and impose additional security measures such as velocity limits on transactions, restrictions on minting, time locks and pre-signed transactions for certain operations, off-chain simulation, and check signed transactions where applicable to ensure that operational execution is robust and secure. Staffing plans, staff screening and training are also required together with policies to ensure adequate segregation of duties to ensure checks and balances. Auditing of smart contracts is required annually and whenever there are upgrades to the smart contracts. Reporting protocols must also be put in place for material changes or incidents. • **Wallet and private key management** HKMA-licensed Stablecoin Issuers must apply stringent controls to the full lifecycle of cryptographic keys (from generation to usage to destruction), with elevated standards for "Significant Seeds and/or Private Keys" involved in the deployment or upgrade of smart contracts in relation to stablecoins, role management and operations that materially affect the stablecoins' supply. The HKMA Stablecoins Guideline Consultation sets out in detail the HKMA's expectations on the controls to be implemented for each aspect involved in wallet and private key management including: (i) hardware and software management; (ii) key generation; (iii) key distribution; (iv) key storage; (v) physical security of key storage; (vi) key inventory; (vii) key usage; (viii) key rotation and destruction; (ix) key compromise; (x) key back-up; (xi) key recovery; and (xii) logs. • **Account management** Effective procedures must be adopted to maintain a communication channel with customers and authenticate customer identity using secure methods (e.g., two-factor authentication) during on-boarding, performing account operations and conducting transactions. Fund and stablecoin transfers to and from customers should be restricted to pre-registered accounts/wallets. HKMA-licensed Stablecoin Issuers must also implement measures to conduct transaction monitoring, fraud detection, and audit trails. Customer account security measures and reminders should also be imposed. Additionally, measures should be put in place to detect and block unauthorised access to customers' accounts and fraudulent transactions and to advise customers on security precautions if needed. Further measures should also be imposed where customers are given programmable access to their accounts. HKMA-licensed Stablecoin Issuers must also document audit trails and all details of customer transactions, and provide information on past transactions to customers for their review. • **Security management**

Technology risk management	HKMA-licensed Stablecoin Issuers must implement measures to ensure a high level of security of IT assets covering: (i) system security settings; (ii) authentication and access control with a security administration function; (iii) security monitoring; (iv) security patch management; (v) physical and personnel security, especially when third party service providers are given access to critical information processing facilities; and (vi) endpoint security and end-user computing. • **Information management** Measures managing the security of information collected by HKMA-licensed Stablecoin Issuers must at least cover: (i) information ownership assignment and classification; (ii) encryption of information when in storage and in transmission; and (iii) information retention and disposal. • **IT services and operations** HKMA-licensed Stablecoin Issuers must ensure that IT services and operations are effective and robust. The HKMA expects that the policies and procedures on IT services and operations should cover: (i) IT operations management and support; (ii) IT incident and problem management; (iii) capacity and performance of IT assets; and (iv) IT facilities and equipment maintenance. • **Project and change management** The framework for managing technology-related projects and the risk management and internal control framework should: (i) adopt a full project life cycle methodology approach; (ii) use a formal testing and acceptance process before adopting systems; (iii) segregate development, testing and production environments; (iv) implement change management to plan, schedule, apply, distribute and track changes to IT assets, including emergency changes and approval procedures for these changes. • **Network management** HKMA-licensed Stablecoin Issuers must designate competent expertise to manage and continuously monitor the network for failures, overload and intrusions. Controls and procedures for using networks and network services must also be put in place with secure network infrastructure, applicable encryption and other network security measures. • **Cybersecurity** HKMA-licensed Stablecoin Issuers must implement robust cybersecurity measures to identify and mitigate cyber risks. This includes conducting regular risk assessments to identify threats from internal and external operations, monitoring threat intelligence to detect emerging risks, and deploying tools like antivirus software to detect vulnerabilities. Regular vulnerability scans, penetration testing, and simulated cyberattack drills should be performed to evaluate security defences in place. Additionally, an incident response plan must be established to detect, contain and recover from cyber incidents, with clear escalation procedures and forensic analysis to prevent recurrence. • **Disaster recovery** An IT disaster recovery plan is required to be included in the incident management framework and business continuity plan.

Technology risk management	• **Management of technology service providers** HKMA-licensed Stablecoin Issuers must ensure that third-party technology service providers are able to meet their cybersecurity standards and have restrictions on outsourcing critical technology services. Service contracts should also define performance, ownership and accountability. Diversifying providers and having contingency plans may also reduce dependency risks.
Operational risk management	Regular review procedures should be put in place to identify operational risks that emerge from time to time and suitable risk assessment matrices should be adopted for each identified risk. In terms of third-party risk management, the HKMA recommends the adoption of the following measures: • **Pre-engagement assessment** Identify and assess risks of third-party arrangements, including the impact on business operations, and in particular, evaluating the criticality of services and the reasons for outsourcing, and the effect on risk profile. Risks of operational disruption should also be considered when formulating the HKMA-licensed Stablecoin Issuers' incident management framework and business continuity plan and implementing applicable contingency plans. Due diligence on third parties should be conducted covering areas such as cost, service quality, financial stability, reputation and technical capabilities, compliance with regulations, long-term capacity, industry expertise and innovation adaptability. • **Contractual agreements** Written contracts must specify the service scope, performance standards, operational/subcontracting arrangements, contingency plans, termination rights, fees, data access rights and data handling (storage, backup, confidentiality and deletion upon contract expiry). • **Ongoing monitoring and review** Continuous monitoring of third-party performance and service availability and conducting regular risk assessments and quality reviews to ensure compliance. Depending on market standards and business needs, the arrangements may need to be re-negotiated and updated. • **Regulatory and data access compliance** Ensure that authorities (e.g., the HKMA) and auditors can access data without obstruction and measures should be put in place to allow on-site/off-site examinations (announced/unannounced) of third-party operations. • **Comply with Personal Data (Privacy) Ordinance (Chapter 486 of the law of Hong Kong) and privacy guidelines** Data access by third-party service providers should be restricted to authorised personnel only. HKMA-licensed Stablecoin Issuers must also ensure data return or destruction upon termination of the services.

Operational risk management	• **Cross-border arrangements** If overseas third-party service providers are engaged, an assessment should be conducted regarding additional risks considering the governing law of the relevant service agreement. HKMA-licensed Stablecoin Issuers should also take note of foreign authorities' access to licensee data and notify the HKMA where applicable. • **Reporting and notification** Third-party arrangements should be classified by materiality (e.g., custody, stablecoin distribution, critical IT) and the HKMA should be notified before commencing material third-party arrangements.
Reputation Risk Management	HKMA-licensed Stablecoin Issuers must manage reputation risks by identifying, monitoring and minimising reputation risks that may arise considering the size and complexity of their business activities, and mitigating the potential impacts in a timely manner. These measures also require reporting protocols to notify the HKMA of any material issues. The HKMA also emphasised the importance of implementing measures to detect potential fraud in relation to its business and stablecoins.
Incident Management, Business Continuity and Exit *Section 16(1)*: HKMA-licensed stablecoin issuers must have in place and implement adequate and appropriate systems of control for appropriate planning to support timely recovery and continuity of critical functions in relation to their licensed stablecoin activities when there is a significant operational disruption. *Section 16(2)*: HKMA-licensed stablecoin issuers must have in place and implement adequate systems of control to ensure: (a) an orderly wind-down of its licensed stablecoin activities could be implemented; and (b) redemption of stablecoins could be honoured in an orderly manner.	The incident management framework should enable timely responses to material incidents affecting business operations, assets, reputation or regulatory compliance. This framework requires: • clear criteria for classifying incident severity that would trigger response procedures across multiple risk domains (i.e. credit/liquidity, technology, operational, de-pegging, reputational, legal etc.); • containment strategies for incidents threatening reserve asset backing or redemption capabilities, such as liquidity stress protocols; • operational continuity plans for stablecoin issuance and redemption during disruptions, with specific measures regarding third-party services; • technology failure protocols such as data back-ups for facilitating recovery and redemption pathways for irrecoverable ledger failures; and • post-incident actions including forensic evidence preservation, root cause analysis, and corrective measures. HKMA-licensed Stablecoin Issuers must put in place a business continuity plan which must: • be overseen by senior management; • be documented and outline critical operations, dependencies, escalation procedures and key personnel contacts, with copies stored off-site; • include regular business impact analyses, monitoring mechanisms, classification of essential critical services and recovery strategies (e.g., maximum tolerable downtime, recovery time and recovery point objectives); • require regular back-ups of essential data at secure off-site locations, using real-time mirroring for high-availability records where applicable; • designate geographically separate alternate sites for business and IT recovery, equipped to meet operational needs within required timeframes; and • avoid over-reliance on third parties for recovery services; if used, risks must be managed per third-party risk guidelines.

Incident Management, Business Continuity and Exit *Section 16(1)*: HKMA-licensed stablecoin issuers must have in place and implement adequate and appropriate systems of control for appropriate planning to support timely recovery and continuity of critical functions in relation to their licensed stablecoin activities when there is a significant operational disruption. *Section 16(2)*: HKMA-licensed stablecoin issuers must have in place and implement adequate systems of control to ensure: (a) an orderly wind-down of its licensed stablecoin activities could be implemented; and (b) redemption of stablecoins could be honoured in an orderly manner.	A business exit plan is also required to ensure the orderly wind-down of stablecoin activities where necessary. This plan must cover scenarios triggering wind-down, with monitoring mechanisms and include detailed procedures for: • liquidating reserve assets (maximising proceeds, minimising market impact); • facilitating redemption claims by stablecoin holders; • distributing proceeds to holders; and • managing third-party arrangements. Sufficient time and resources should be reserved for an orderly wind-down when needed, and the legal certainty and operational feasibility of the business exit procedures must also be considered. HKMA-licensed Stablecoin Issuers must review and update their incident management framework, business continuity plan, and exit plan annually or after any activation. Identified shortcomings must be promptly addressed in updated documents. Annual testing and simulations of all plans should be carried out and reported to the board and senior management to ensure that relevant staff are familiar with their roles and responsibilities, and the plans should be updated accordingly to fix identified gaps. HKMA-licensed Stablecoin Issuers must also comply with the following reporting obligations to the HKMA: • submission of contact details of key personnel for plan implementation and notify changes promptly; • immediate reporting if scenarios triggering incident response, continuity recovery, or exit plans materialise or are anticipated; and • obtain HKMA's written consent before delaying stablecoin redemptions beyond one business day under any plan.
F. CORPORATE GOVERNANCE	
Corporate governance *Section 13*: HKMA-licensed stablecoin issuers must have in place and implement adequate and appropriate risk management policies and procedures to identify, prevent, manage and disclose potential and actual conflicts of interest between themselves and stablecoin holders.	In connection with the requirement to implement adequate and appropriate risk management policies and procedures, the HKMA emphasises the need for good corporate governance with clear organisational roles, documented decision-making procedures and internal reporting lines to ensure effective decision-making. • **Board Responsibilities** The board is responsible for the operations of the HKMA-licensed stablecoin issuer. At least one-third of the board should be independent non-executive directors (**INEDs**) to ensure checks and balances, and HKMA pre-approval is required for director appointments (except for authorised institutions which should comply with the requirements under the Banking Ordinance). In addition to documenting clearly defined responsibilities, authorities, composition requirements and arrangements, the board's responsibilities also include: o setting business objectives/strategies; o establishing a corporate structure with defined responsibilities; o delegating members to specialised committees (e.g., audit, remuneration); o appointing/supervising senior management;

Corporate governance *Section 13*: HKMA-licensed stablecoin issuers must have in place and implement adequate and appropriate risk management policies and procedures to identify, prevent, manage and disclose potential and actual conflicts of interest between themselves and stablecoin holders.	o overseeing risk governance, internal controls and policy approval; and o setting corporate values, standards and remuneration policies. • **Senior Management** Senior management (i.e. chief executives, the stablecoin manager, senior executives) should report to the board and should be guided by clearly defined responsibilities, performance assessments and accountability mechanisms. Their key duties include: o proposing and implementing board-approved business strategies; o establishing corporate structure with documented roles and reporting lines; o ensuring staff competency via recruitment, appraisal and development programs; o implementing risk management frameworks and internal controls; and o establishing management information systems for accurate reporting. • **Compliance and internal audit** These functions must be performed by competent professionals, be independent, adequately resourced and separate from the business units. They must also have sufficient authority and unfettered data access. In particular, the compliance function should manage compliance risk and ensure adherence to laws and regulations. It should also be responsible for developing board-approved compliance policies and report to senior management with rights to report to the board directly. The internal audit function should generally be responsible for conducting impartial assessments of internal systems and controls and proposing enhancements accordingly. Its operations should be guided by an audit charter approved by the board and it should report to the board or a board committee directly. • **Corporate governance measures** The HKMA recommends adopting a code of conduct for the board, senior management and staff members with integrity standards covering the fitness/ propriety of directors, managers and stablecoin managers; and prohibiting certain behaviour such as conflicts of interest and bribery (aligned with the Prevention of Bribery Ordinance). To comply with the conflict management requirements under section 13(3) of Schedule 2 Hong Kong Stablecoins Ordinance, policies to identify and prevent conflicts (e.g., segregation of duties, information barriers) should be adopted. Additionally, a remuneration policy commensurable with HKMA-licensed Stablecoin Issuers' business strategies and long-term interests should be put in place. The remuneration policy for chief executives, stablecoin managers and control function heads should be overseen by the board. The remuneration policies for internal control functions should also be separated from those for staff of the front-line business units.

Fitness and propriety (Sections 37, 39, 53, 58, 66 Hong Kong Stablecoins Ordinance, sections 7 and 8 of Schedule 2 Hong Kong Stablecoins Ordinance)	Hong Kong stablecoins issuers must ensure that their controllers, directors, chief executives, stablecoin managers and managers meet stringent fitness and propriety standards and have suitable knowledge and expertise to carry out their respective duties. Key roles that require HKMA pre-approval include chief executives, directors and controllers (of non-authorised institutions) and stablecoin managers (of authorised institutions). The appointment or appointment cessation of managers of HKMA-licensed Stablecoin Issuers must be notified to the HKMA within 14 days. To evaluate whether a proposed chief executive, stablecoin manager, director, controller or manager meets the fitness and propriety requirements, the HKMA will generally consider their: 1. integrity: o clean criminal record and regulatory history in Hong Kong and other jurisdictions; o absence of past disqualifications; o financial soundness (absence of risks to operations and specified stablecoins holder confidence); 2. competence: o relevant experience, qualifications, and leadership ability; o demonstrated time commitment and ability to work with other functions and staff; o absence of conflicts of interest; o for INEDs, independence from the Hong Kong stablecoin issuer and its significant shareholders For managers, HKMA-licensed stablecoin issuers must also clearly define the required skills and knowledge for each managerial position and implement structured procedures for managers including: • rigorous selection and appointment protocols; • performance appraisals and disciplinary mechanisms; • temporary coverage plans for vacancies; • ongoing training and development programs; and • internal audit reviews of control systems to ensure that managers are fit and proper to hold their respective positions.
G. BUSINESS PRACTICES AND CONDUCT	
Information & accounting systems	HKMA-licensed Stablecoin Issuers should establish effective information and accounting systems with back-up facilities and disaster recovery arrangements to accurately and timely record all business activities, including both on-chain and off-chain data, and generate quality management information for operational efficiency and maintain audit trails.

Information & accounting systems	Additionally, compliant books, accounts and financial statements must be maintained in accordance with Hong Kong's regulatory standards and accounting requirements. HKMA-licensed Stablecoin Issuers should also adopt comprehensive record-keeping policies to retain accurate documentation of business activities and decisions for a legally mandated duration. If these systems are located outside Hong Kong, the HKMA and other authorised parties must be provided with unimpeded access to conduct both announced and unannounced on-site examinations or off-site reviews.
Personal data protection	HKMA-licensed Stablecoin Issuers should observe and comply with the PDPO and all relevant publications on personal data protection by the Office of the Privacy Commissioner for Personal Data.
Complaints handling *Section 14*: HKMA-licensed Stablecoin Issuers must ensure that holders have access to complaints handling and redress mechanisms that are fair, timely and efficient.	As HKMA-licensed Stablecoin Issuers are required to implement mechanisms to ensure segregation of duties, complaints should be handled by competent staff not involved in the subject matter. Formal policies must be established to cover complaint acknowledgment, investigation, escalation, remediation, resolution, response, closure and follow-up on systemic issues. Records of complaints should be kept confidential. The complaint system should also be publicly accessible with processes and timeframes disclosed prominently on the Hong Kong Stablecoin Issuer's website. If third-party entities are engaged to distribute stablecoins, procedures for third-party entities' handling of complaints should also be implemented.

Consultation Paper on the Proposed AML/CFT Requirements for Regulated Stablecoin Activities

The HKMA's proposed AML/CFT framework for HKMA-licensed Stablecoin Issuers aim to address unique money laundering and terrorist financing (**ML/TF**) risks while aligning with the Financial Action Task Force (**FATF**) standards. Considering the potential risks in relation to stablecoin activities, stablecoins share vulnerabilities with virtual assets, including anonymity risks from transactions involving unhosted wallets, which may bypass AML/CFT controls and enable illicit activities. Jurisdictional gaps in regulating virtual asset service providers further exacerbate these risks, as stablecoins may circulate through non-compliant entities. Internationally, AML/CFT obligations often rest on the financial institutions providing financial services to their customers. Given that stablecoin issuers act as intermediaries during redemption, custody or transaction facilitation, they will be classified as "financial institutions" under Hong Kong's Anti-Money Laundering Ordinance (Cap. 615 of the Laws of Hong Kong) (the **AMLO**), applying the principle of "*same activity, same risk, same regulation*". However, minting, creating and burning virtual assets may not fall within the scope of an intermediary's activities. Accordingly, HKMA-licensed Stablecoin Issuers will be required to implement tailored AML/CFT controls detailed in the draft HKMA AML/CFT Guideline, which target stablecoin-specific ML/TF threats.

The AML/CFT policies should at least cover: (i) the adoption of a risk-based approach and conducting institutional ML/TF risk assessments; (ii) governance, senior management oversight, internal audit and staff training; (iii) controls to combat terrorist financing, financial sanctions and proliferation financing; (iv) suspicious transaction reporting; and (v) record keeping.

The main requirements under the draft HKMA AML/CFT Guideline and the specific issues the HKMA consulted on under the HKMA Stablecoins AML/CFT Consultation Paper are summarised below.

A. Risk assessment

HKMA-licensed Stablecoin Issuers must implement a risk-based approach to formulating their AML/CFT systems, beginning with a comprehensive institutional ML/TF risk assessment tailored to their specific stablecoin operations. This assessment must evaluate risks across four key dimensions: (i) customer profiles, (ii) jurisdictional, (iii) product, service or transaction specific, and (iv) delivery channels. The process requires rigorous documentation with qualitative and quantitative analysis, consideration of all relevant risk factors prior to determining the overall risk level and mitigation measures, senior management approval, and regular updates to reflect evolving threats. HKMA-licensed Stablecoin Issuers should also be prepared to submit the results to the HKMA upon request. Risk levels must also align with the HKMA-licensed Stablecoin Issuer's business scale and complexity, incorporating external inputs like Hong Kong's jurisdiction-wide risk assessments or risks observed by the HKMA and the Joint Financial Intelligence Unit. Additionally, new products, technologies or business practices demand pre-launch risk evaluations with commensurate mitigation measures.

B. AML/CFT systems

AML/CFT systems must be implemented and approved by senior management with continuous monitoring protocols and enhanced measures when higher risks are identified. Simplified systems are permitted only if: (i) statutory AMLO Schedule 2 requirements and paragraphs 2.2, 2.3 and 3.1 under the HKMA AML/CFT Guideline are met in full; (ii) the HKMA-licensed Stablecoin Issuer is subject to lower ML/TF risks which are validated through institutional risk assessments, noting that simplified systems are not permitted if there is a suspicion of ML/TF; (iii) senior management approves the simplified systems; and (iv) the simplified systems are regularly reviewed.

In particular, the AML/CFT systems should cover guidance on the following:

i. **Compliance Management**:

The ML/TF risks must be monitored by senior management familiar with the applicable ML/TF risks. A Compliance Officer should be appointed to establish and maintain AML/CFT systems, and a Money Laundering Reporting Officer should be appointed to act as the central point for suspicious transaction reporting and law enforcement liaison. Both the Compliance Officer and Money Laundering Reporting Officer must have sufficient expertise and resources to perform their duties, and these roles can be performed by the same person depending on the size of the HKMA-licensed Stablecoin Issuer.

ii. **Independent Audit**:

There should also be an independent audit function directly reporting to senior management and the board and possessing sufficient expertise and adequate resources to review AML/CFT system effectiveness.

iii. **Employee Screening**

HKMA-licensed Stablecoin Issuers are also advised to adopt rigorous procedures to ensure high-integrity staff in AML/CFT roles.

iv. **Continuous training**

Ongoing, role-specific programs tailored to the responsibilities of different positions and experience levels should be available for staff members.

v. **Group-wide requirements**

HKMA-licensed Stablecoin Issuers with overseas branches and/or subsidiaries conducting activities as a financial institution (as defined in the AMLO) must implement group-wide AML/CFT systems extending Hong Kong standards to these overseas branches and/or subsidiaries where applicable. Specifically, these branches and/or subsidiaries must also comply with AMLO-equivalent customer due diligence and record-keeping (parts 2 and 3 of Schedule 2 to the AMLO) to the extent permissible, including measures for sharing information and group-level compliance, audit and/or AML/CFT functions. Where the foreign jurisdiction also imposes AML/CFT requirements, the HKMA AML/CFT Guideline advises applying the stricter standard, where permitted. However, if the laws of the foreign jurisdiction prohibit Hong Kong standards, the HKMA-licensed Stablecoin Issuer must notify the HKMA immediately and implement compensatory measures to mitigate ML/TF risks.

C. Customer due diligence

The requirements relate to customers of the HKMA-licensed Stablecoin Issuers, which include persons who have a business relationship (defined in section 1 of Part 1 of Schedule 2 to the AMLO) with the HKMA-licensed Stablecoin Issuer and persons with whom the HKMA-licensed Stablecoin Issuer conducts occasional transactions involving an amount of HK$8,000 or more. HKMA-licensed Stablecoin Issuers should not establish a business relationship or conduct occasional transactions with a customer if the Customer Due Diligence measures cannot be satisfied, and suspicious transaction reports must be submitted to the Joint Financial Intelligence Unit where necessary.

HKMA-licensed Stablecoin Issuers must perform Customer Due Diligence measures in four situations:

1) before establishing a business relationship;

2) prior to executing occasional transactions (e.g., stablecoin issuance/redemption) involving HK$8,000 or more per customer;

3) when ML/TF is suspected; or

4) if they doubt the accuracy of customer information previously obtained.

Exceptionally, verification post-establishment of the business relationship is permitted only if the ML/TF risks resulting from the delay are manageable, immediate verification would disrupt normal business operations with the customer, and identity confirmation is completed as soon as reasonably practicable.

The Customer Due Diligence measures should include the following steps.

Verifying the identity of customers using reliable independent sources	Customer identities must be verified using reliable independent sources, prohibiting fictitious names. For natural persons, verification requires confirming the full name, date of birth, unique identification number (e.g., ID card/passport) and document type by obtaining photo-bearing documents such as HKID cards or passports, with exceptions only in special circumstances. For legal persons such as entities and corporates, verification must establish the entity's name, legal form, current existence, other corporate information (e.g. registered and principal business address, company number and document type) and authorities to bind the legal entity, using independent sources such as certificates of incorporation, company registeries' certificates and records, or partnership agreements. More than one document may be required to verify all the information. For non-face-to-face identity verification methods, HKMA-licensed Stablecoin Issuers must either use HKMA-recognised digital ID systems or deploy technology solutions ensuring both identity authentication (validating document and data reliability) and identity matching (linking the person conclusively to the identity provided). Additionally, HKMA-licensed Stablecoin Issuers must collect supplementary data for digital delivery channels, including IP addresses, geolocation, device IDs and wallet addresses, to manage ML/TF risks. **Connected parties** Connected persons of legal persons such as directors of corporate clients must also be identified by name.
Identifying and verifying beneficial owners	HKMA-licensed Stablecoin Issuers must identify and verify the identity of any beneficial owner, who is a natural person(s) who ultimately owns or controls the customer, or for whom a transaction or activity is conducted. Verification measures must achieve the purpose of definitively identifying the beneficial owner's identity. For legal person customers, HKMA-licensed Stablecoin Issuers must thoroughly understand the ownership and control structure by mapping all intermediate layers, such as through organisational charts, to trace the chain of ownership up to the ultimate beneficial owner(s). In cases involving complex ownership or control arrangements, sufficient documentation must be obtained to validate legitimate business justifications for these structures. Additionally, anyone with a controlling ownership interest above 25% or control over the management or the operations must be identified and their identities verified. If no such person exists, the identity of the senior managing official(s) should be identified and verified.
Understanding the purpose and intended nature of the business relationship	This is necessary to evaluate the risk profile of the customer and identify any potential ML/FT risks. Information on the business nature of customers who are not natural persons, such as entities or corporations, should also be obtained.

Validating representatives acting on behalf of customers to confirm both the representative's identity and authorisation through trustworthy documentation or data	HKMA-licensed Stablecoin Issuers must verify the identity and authority of any person purporting to act on behalf of the customer using standard customer due diligence procedures and obtain proper authorisation documents.

Risk-based approach to the customer due diligence exercise

The extent of the customer due diligence to be conducted on a customer must be determined using a risk-based approach. Enhanced Due Diligence is required for high ML/TF risk cases, while simplified due diligence can be applied in low-risk scenarios, provided the level of due diligence aligns with the identified risks and is supported by thorough risk analysis using the risk assessment criteria set out in section A "Risk assessment" above. However, simplified due diligence cannot be used if the risk assessment changes to indicate higher risks, ML/TF is suspected, or if there are doubts about previously obtained identification documents or information. Additionally, senior management approval is mandatory for initiating or continuing business relationships presenting high ML/TF risks.

For clients from high-risk jurisdictions specified by the Financial Action Task Force, Enhanced Due Diligence measures or other countermeasures must be implemented. The HKMA can also issue written notices requiring HKMA-licensed Stablecoin Issuers to apply Enhanced Due Diligence measures, as outlined in section 15 of Schedule 2 AMLO, or specific countermeasures detailed in a notice, which are proportionate to the nature of the risks or deficiencies present in the relevant jurisdiction.

Politically exposed persons

HKMA-licensed Stablecoin Issuers are also required to have in place effective procedures to identify whether a customer or their beneficial owner is a Politically Exposed Person (**PEP**), including non-Hong Kong PEPs, Hong Kong PEPs, and international organisation PEPs. For non-Hong Kong PEPs, their source of wealth and source of funds must be ascertained, and senior management approval must be obtained before establishing a business relationship, or before continuing an existing relationship if the PEP status is discovered later. These requirements are also applicable to Hong Kong PEPs and international organisation PEPs who pose high ML/TF risks. Regarding former PEPs, HKMA-licensed Stablecoin Issuers may decide, following a Risk-Based Approach assessment, to not apply these enhanced measures if the individual no longer presents a high ML/TF risk.

Customer due diligence through intermediaries

HKMA-licensed Stablecoin Issuers are allowed to outsource some of their Customer Due Diligence obligations to specific intermediaries provided that the requirements of section 18 of Schedule 2 AMLO and requirements under the HKMA AML/CFT Guideline are met. Under these requirements, HKMA-licensed Stablecoin Issuers must: (a) obtain the intermediary's written agreement specifying the Customer Due Diligence tasks they will perform; and (b) ensure the intermediary can promptly provide copies of all Customer Due Diligence documents and information upon request.

After the intermediary completes a Customer Due Diligence task, HKMA-licensed Stablecoin Issuers must also:

1) obtain the data or information collected by the intermediary;

2) if the intermediary holds the records, obtain an undertaking that they will store all underlying Customer Due Diligence information for the duration of the business relationship plus at least five years after it ends (or as specified by the HKMA);

3) ensure that the intermediary will supply copies promptly upon request within the record-keeping period under the AMLO;

4) obtain an undertaking from the intermediary to pass on all underlying documents if the intermediary ceases trading or ceases to act as an intermediary; and

5) conduct sample tests regularly to verify the intermediary's ability to produce documentation promptly.

HKMA-licensed Stablecoin Issuers should ask for all underlying documents when they terminate their relationship with intermediaries and should re-perform necessary Customer Due Diligence when in doubt about the intermediary's past Customer Due Diligence.

D. Requirements in relation to wallets

The HKMA proposes to require HKMA-licensed Stablecoin Issuers to take reasonable steps to manage ML/TF risks associated with customer wallets before issuing stablecoins or completing redemption requests from clients.

Under the proposed requirements in the HKMA AML/CFT Guideline, HKMA-licensed Stablecoin Issuers must identify each customer's wallet address and classify its type, which may be custodial or unhosted. HKMA-licensed Stablecoin Issuers are also required to verify the customer's ownership or control of the address through technical validation (e.g., micropayment transfers or message signing tests specified by the licensee), obtaining documentary evidence, or other effective measures. To streamline future transactions, licensees may optionally whitelist verified wallet addresses after confirming ownership.

Specific requirements for the two different types of wallets are summarised below:

Custodial wallets Wallets managed by a third-party financial institution or a virtual asset service provider.	HKMA-licensed Stablecoin Issuers must conduct at least the following due diligence on the third-party financial institution or a virtual asset service provider: • collect information to understand their business nature; • determine the provider's reputation and assess the quality of AML/CFT regulation/supervision in its operating jurisdictions using publicly available information; • evaluate the adequacy and effectiveness of the provider's AML/CFT controls; and • secure senior management approval before engagement. The extent of the due diligence exercise should be determined using a risk-based approach, taking into account the product and service type, the customer type, the geographical exposures, the relevant AML/CFT regime, and the adequacy and effectiveness of the AML/CFT controls. These requirements are similar to the due diligence measures SFC-regulated virtual asset trading platforms are required to adopt before transferring virtual assets to a counterparty.
Unhosted wallets Wallets with private keys that are held or controlled by the client themselves.	According to the HKMA AML/CFT Guideline and the HKMA Stablecoins AML/CFT Consultation Paper, given the decentralised nature allowing peer-to-peer transactions that bypass intermediary involvement and the heightened ML/TF risks associated with these wallets, HKMA-licensed Stablecoin Issuers are required to adopt additional controls, including: • conducting enhanced monitoring of stablecoin transfers; • restricting transfers to to/from unhosted wallets previously assessed as reliable based on transaction and wallet address screening; and • impose transaction limits where appropriate. The HKMA clarified that if a customer using an unhosted wallet is itself an entity subject to AML/CFT requirements (e.g., a financial institution), due diligence measures for custodial wallets should be applied instead.

The HKMA specifically sought comments in the HKMA Stablecoins AML/CFT Consultation Paper on the above proposals on due diligence requirements in relation to custodial or unhosted wallets before stablecoin issuance and redemption respectively.

E. Ongoing monitoring requirements

The HKMA acknowledged that HKMA-licensed Stablecoin Issuers differ from traditional financial intermediaries (like banks) as their primary activity involves issuing and redeeming stablecoins. On the other hand, the HKMA is of the view that ongoing monitoring is fundamental for effective AML/CFT systems to prevent stablecoins (including stablecoins in the secondary market) being used for illicit purposes. It is therefore proposing to require HKMA-licensed Stablecoin Issuers to implement measures for ongoing monitoring. The approach to monitoring suspicious activities must be tailored to the HKMA-licensed Stablecoin Issuer's specific business activities, operating structure, and corresponding ML/TF risks.

It is proposed that HKMA-licensed Stablecoin Issuers must continuously monitor customer relationships in two key ways:

1) **ongoing Customer Due Diligence**: including regularly reviewing existing customer documents, data and information to ensure they remain current and relevant, based on a risk-based approach involving periodic reviews and trigger events defined in clear policies; and

2) **risk-based transaction monitoring**: such as scrutinising customer transactions to check for transactions that are not compatible with the client's business, risk profile and source of funds. Steps should also be taken to identify and document transactions that are complex, unusually large, exhibit unusual patterns, lack an apparent economic or lawful purpose or involve transactions with wallets that have been listed as having connections with illicit or suspicious activities or persons. For transactions with the above redflags, further measures such as detailed investigation into the transaction background and additional customer due diligence is required to detect any grounds for suspicion warranting further reporting and investigation.

   To effectively track and monitor stablecoin flows at issuance and redemption, issuers must implement effective systems and use appropriate technological solutions (e.g. blockchain analytics tools to trace on-chain history) to track stablecoin transaction history and screen transactions and associated wallet addresses against those linked to illegal or suspicious activities or designated parties.

   The HKMA clarified that HKMA-licensed Stablecoin Issuers remain fully responsible for AML/CFT compliance even when using third-party tech solutions. Accordingly, thorough due diligence on the solution's effectiveness, data quality (i.e., coverage, accuracy and reliability of the underlying database), and limitations (e.g., limited reach or lack of capability to handle wallets that use anonymity-enhancing tech) should be conducted before implementation.

HKMA-licensed Stablecoin Issuers should also monitor supplementary data (IP addresses, geolocation, device IDs, metadata etc.) to identify suspicious activity. If monitoring measures reveals heightened ML/TF risks, HKMA-licensed Stablecoin Issuers must apply enhanced customer due diligence and ongoing monitoring, and take additional risk-mitigation measures and preventive controls.

Stablecoins in circulation

While HKMA-licensed stablecoin issuers are not required to perform Customer Due Diligence on non-customer holders of their stablecoins, they must implement adequate and proportionate ongoing monitoring measures to prevent the stablecoins being used for illicit purposes. The inherent traceability of all on-chain stablecoin transactions recorded on the blockchain may also help identify illicit activities and associated wallet addresses.

Examples of systems and controls include:

- restricting primary issuance and redemption to regulated financial intuitions and virtual asset service providers;

- using technological tools to continuously monitor stablecoin transactions and wallet addresses beyond the initial distribution point.

- blacklisting wallet addresses identified as sanctioned or linked to illicit activities;
- whitelisting approved wallet addresses; or
- adopting a closed-loop system restricting circulation to regulated entities.

HKMA-licensed Stablecoin Issuers must conduct further investigation into any illicit or suspicious activity and report any transactions suspected to involve ML/FT to the Joint Financial Intelligence Unit and take suitable follow-up actions under Chapter 8 of the HKMA AML/CFT Guideline.

Relevant consultations in relation to ongoing monitoring requirements

In the HKMA Stablecoins AML/CFT Consultation Paper, the HKMA also sought feedback on whether HKMA-licensed stablecoin issuers should be required to implement measures to prevent or combat ML/TF abuse associated with stablecoin transactions to or from unhosted wallets or unregulated wallets and further suggestions on risk mitigating measures applicable to these stablecoin transactions with reference to the various stakeholders involved in the transfer process.

Additionally, the HKMA asked for comments on the level of responsibility HKMA-licensed stablecoin issuers should bear for monitoring stablecoin transactions in secondary markets, and suggestions on how should these monitoring controls be implemented.

F. Stablecoin transfer

Section 13A to Schedule 2 AMLO sets out the special requirements applicable to various stakeholders involved in the virtual asset transfer process which is defined as: a transaction carried out by the “ordering institution” on behalf of an originator by transferring any virtual assets with a view to making the virtual asset available to the recipient at a “beneficiary institution” whether or not one or more other “intermediary institutions” are involved in the completion of such transfer.

The HKMA is of the view that HKMA-licensed Stablecoin Issuers may assume the roles of an “ordering institution”, a “beneficiary institution” or a “intermediary institution” depending on the business model of the HKMA-licensed Stablecoin Issuer and therefore proposed that HKMA-licensed Stablecoin Issuers should also be subject to section 13A to Schedule 2 AMLO.

The table below sets out the proposed requirements under the HKMA AML/CFT Guideline with respect to each of the roles before executing a stablecoin transfer to ensure compliance with section 13A to Schedule 2 AMLO, also called the “Travel Rule”:

Ordering institutions	For transactions equivalent to HK$8,000 or more, HKMA-licensed stablecoin issuers must obtain the following information from the originator and the recipient: (i) name; (ii) for originators, the account number (this could also mean the wallet address) or the unique reference number that is assigned to the stablecoins transfer (the transfer must be traceably by this reference number) maintained with the ordering institution or the beneficiary institution, as the case may be; and (iii) for originators, their address, customer identification number or ID number, date and place of birth (if applicable). Further verification of the originator’s identity and information provided by the originator with regards to the documents obtained during Customer Due Diligence by the HKMA-licensed stablecoin issuers is required to ensure accuracy of the information provided. For transactions below HK$8,000, except for item (iii) all other information set out above must also be obtained. For these transactions, further verification of the information for accuracy is not strictly required, verification of identity of the originator is required only where the HKMA-licensed stablecoin issuers detects that there may be ML/TF involved.

Ordering institutions	*Information transfer requirements* Ordering institutions are required to store the information collected securely and pass them to the beneficiary institution and/or the intermediary intuition in a direct or indirect manner (i.e. not attached to the stablecoin transfer itself) immediately and safely to ensure integrity of the information and data safety. To ensure safe transfer of the information, ordering institutions should conduct counterparty due diligence to confirm that the beneficiary or intermediary institutions can protect data confidentiality and integrity and implement other appropriate safeguards such as entering into formal agreements with counterparties or solution providers specifying data protection responsibilities, using strong encryption during data transmission, and adopting robust information security controls against unauthorised access or alteration. An ordering institution must not proceed with a stablecoin transfer unless it can guarantee secure data submission based on the above safeguards and due diligence findings. The HKMA also emphaised that the such submission of information should be done before or at the time of the stablecoin transfer. It is also important for ordering institutions to keep a paper trail of the submission of documents and provide relevant records to the authorities when required.
Intermediary institutions	Intermediary institutions must retain all originator and recipient information associated with stablecoin transfers and transmit this complete dataset intact to the next institution in the chain (whether another intermediary or the beneficiary institution). This transmission must also comply with the "Information transfer requirements" applicable to ordering institutions as set out above. Intermediary institutions are also required to conduct counterparty due diligence with respect to the ordering institution and other intermediary institutions.
Beneficiary institutions	Beneficiary institutions must obtain and record all required originator and recipient information submitted with stablecoin transfers. For transfers of HK$8,000 or more, they must: • verify the recipient's identity if not previously confirmed by Customer Due Diligence; • cross-check the recipient's name and account number against their own records; and • take reasonable mitigation measures if discrepancies are found.

Guidance on handling stablecoin transfers without the requisite originator or recipient information

Beneficiary or intermediary institutions must establish procedures to identify and handle transfers that lack the required originator or recipient information. These include:

- implementing monitoring measures to detect non-compliant transfers;
- developing risk-based protocols to decide whether and when to execute, suspend, or return stablecoin transfers with missing data and take other appropriate actions;
- promptly obtaining missing information from the sending institution; and
- if the information remains unavailable, restricting or terminating the business relationship with the instructing institution or taking reasonable ML/TF mitigation measures.

When provided with incomplete or meaningless information, beneficiary or intermediary institutions must also implement risk mitigation actions per their established procedures set out in the second point above.

Using technological solutions to comply with the "Travel Rule"

Where technological solutions are used, HKMA-licensed Stablecoin Issuers remain ultimately responsible for AML/CFT compliance and must implement robust safeguards to ensure the secure and compliant transmission of required information on stablecoin transfers. First, they must conduct thorough counterparty due diligence to verify the solution's effectiveness. This requires confirming that the solution is able to:

- identify stablecoin transfer counterparties; and
- perform immediate and secure submission or retrieval of the required information, for instance whether it is able to identity missing or incomplete information arising from differences in regulations across jurisdictions, and whether it can protect data confidentiality and integrity against unauthorised access, disclosure or alteration.

Additionally, HKMA-licensed Stablecoin Issuers must evaluate whether the technology is able to: (a) be compatible with counterparties' systems to ensure seamless data exchange; (b) securely process high-volume transfers across multiple institutions with stability; (c) allow effective suspicious transaction monitoring and sanctions compliance including freezing prohibited transfers to designated parties; (d) facilitate counterparty due diligence and supplemental information requests; and (e) support proper record-keeping of required data.

Counterparty due diligence requirements

In the HKMA AML/CFT Guideline, the HKMA noted that HKMA-licensed Stablecoin Issuers conducting stablecoin transfers may face ML/TF risks from counterparties (ordering, intermediary or beneficiary institutions), and these risks may vary according to the counterparty's product, service and customer types, their geographic exposure and operational jurisdictions, and the adequacy of AML/CFT controls. To ensure compliance with AML/CFT requirements and the Travel Rule, HKMA-licensed Stablecoin Issuers are required to conduct due diligence on counterparties before executing stablecoin transfers with a relevant counterparty. Specifically for counterparties based in different jurisdictions but belonging to the same corporate group, the HKMA clarified that although due diligence should be conducted on counterparties as independent entities, an overall assessment should also be conducted on the basis of the related companies as part of the same group.

The table below summarises the counterparty due diligence requirements under the HKMA AML/CFT Guideline.

Procedures in the due diligence exercise	The aims and typical procedures involved in the conduct of counterparty due diligence include: (i) verifying whether the transaction involves a regulated counterparty or an unhosted wallet; (ii) identifying counterparties by reference to the list of licensed or registered financial institutions or virtual asset services providers; and (iii) assessing counterparty eligibility for both conducting transactions and receiving required originator or recipient information.
Due diligence measures	To carry out the procedures set out above, HKMA-licensed Stablecoin Issuers are required to adopt a risk-based approach when: (i) collecting comprehensive business information about the counterparty's business, including its ownership and control structure by reference to reliable and independent sources; (ii) analysing transaction characteristics and projected transaction volumes to ascertain the risk profile of expected transfers; (iii) evaluating the counterparty's reputation and assessing the quality of its jurisdiction's AML/CFT regime and regulatory supervision standards; (iv) evaluating the sufficiency of the counterparty's AML/CFT controls; and (v) obtaining senior management approval.
Compliance with the Travel Rule	Specifically, HKMA-licensed Stablecoin Issuers must also evaluate whether the counterparty is able to comply with the Travel Rule with reference to the following criteria: (i) whether the counterparty is bound by equivalent Travel Rule obligations in its jurisdiction;

Compliance with the Travel Rule	(ii) whether the counterparty's AML/CFT controls are effective in ensuring compliance; and (iii) whether the counterparty's data privacy and security measures can sufficiently protect the originator and recipient information.
Counterparties with higher ML/TF risks	The HKMA also set out factors it considers to be indicators that the counterparties may pose higher ML/TF risks, including where the counterparty: (i) operates or is incorporated in a high-risk jurisdiction with a weaker AML/CFT regime; (ii) lacks proper licensing, registration or AML/CFT supervision by a competent authority in its operating jurisdiction; (iii) is unable to maintain adequate AML/CFT systems, including failures in Travel Rule compliance; (iv) is unable to implement sufficient data protection safeguards to ensure personal information confidentiality and integrity; or (v) has documented associations with money laundering, terrorist financing or other illicit activities.
Ongoing monitoring of counterparties	HKMA-licensed Stablecoin Issuers must implement ongoing, risk-based monitoring of stablecoin transfer counterparties to detect suspicious activity and assess evolving risks. This involves two key processes: (1) continuously scrutinising transactions for unusual patterns or risk profile changes with reference to the ongoing monitoring requirements set out above; and (2) periodically reviewing counterparty due diligence information, either on a scheduled basis or when triggered by risk events like adverse media, sanctions listings or regulatory investigations. Based on these monitoring results, HKMA-licensed Stablecoin Issuers must make risk-sensitive determinations about whether to continue relationships with these counterparties, the level of AML/CFT measures to apply, and whether to maintain information sharing.
Mitigating and managing counterparty ML/TF risks	Upon identifying ML/TF risks through counterparty due diligence, HKMA-licensed Stablecoin Issuers must evaluate the potential impact of these risks on their operations and implement proportionate risk mitigation measures. For counterparties presenting higher risks, these measures include conducting enhanced or frequent due diligence reviews, closely monitoring relevant stablecoin transfers and/or imposing transaction limits where necessary. HKMA-licensed Stablecoin Issuers must continuously assess whether to maintain, restrict or terminate relationships with high-risk counterparties. If ML/TF risks cannot be effectively mitigated, HKMA-licensed Stablecoin Issuers must refrain from executing or facilitating any stablecoin transfers involving the relevant counterparties. Specifically, under no circumstances may HKMA-licensed Stablecoin Issuers conduct stablecoin transfers with shell virtual asset services providers or shell financial institutions.

Stablecoin transfers to and/or from unhosted wallets

As the HKMA considers that transactions involving unhosted wallets present elevated ML/TF risks due to participant anonymity and absence of intermediary oversight, the HKMA proposed to require the implementation of enhanced controls for these transactions, including:

1) **Mandatory information collection** – Before executing transfers to or from an unhosted wallet for the first time, HKMA-licensed Stablecoin Issuers must obtain and record:

   o For *outbound transfers*, the originator's name, account or unique reference number, address, identification details, date and place of birth and the recipient's name and wallet address; or

   o For *inbound transfers*, the originator's name, wallet address, address, identification details; and the recipient's name and account or unique reference number.

The originator's address, identification number, date and place of birth are not required for transactions that are under HK$8,000.

2) **Risk-based mitigation measures** – HKMA-licensed Stablecoin Issuers must assess transaction-specific risks and implement proportionate controls including:

   - enhanced monitoring of all unhosted wallet transactions;
   - restricting transfers only to or from pre-vetted wallets verified through unhosted wallet screening results and the evaluation of its ownerships and control structure; and
   - imposing transaction limits on, for example, the amount of stablecoin transfers.

G. Terrorist financing, financial sanctions and proliferation financing

HKMA-licensed Stablecoin Issuers must implement measures to detect transactions suspected of being connected to terrorist financing, financial sanctions and proliferation financing activities, comply with relevant regulatory requirements and provide relevant training to staff members on the legal and regulatory obligations. To support this, HKMA-licensed Stablecoin Issuers must maintain an accurate, comprehensive and up-to-date database consolidating the names and particulars of individuals and entities from relevant sanctions lists. This database must specifically include:

- lists published in the Hong Kong Gazette or on the Commerce and Economic Development Bureau website;
- any UN Security Council Resolutions (UNSCRs) or sanctions lists related to terrorism, terrorism financing and proliferation financing; and
- lists specified by the HKMA.

The database must be promptly updated whenever changes occur and be readily accessible to relevant staff. HKMA-licensed Stablecoin Issuers have the option to subscribe to a third-party service provider's database, but must implement appropriate measures, such as periodic sample testing, to verify its completeness and accuracy. An HKMA-licensed Stablecoin Issuer may also delegate the maintenance of the database or the screening process to its overseas office. However, the ultimate responsibility for ensuring full compliance with all relevant regulations and legislation will still rest with the HKMA-licensed Stablecoin Issuer itself.

To prevent establishing business relationships or conducting transactions with prohibited parties, licensees must implement an effective screening mechanism. This requirement explicitly applies to: (i) designated persons or entities; (ii) persons or entities acting on behalf of, or at the direction of, designated parties; (iii) entities owned or controlled by any of the previous two types of persons or entities; (iv) connected parties of customers (using a risk-based approach); and (v) persons purporting to act on behalf of the customer (using a risk-based approach).

The screening mechanism must cover:

1) initial customer and beneficial owner screening at issuance and redemption;

2) customer and beneficial owner screening against all new entries and updates to the database as soon as practicable after those updates occur; and

3) screening of parties to a transaction before execution of a stablecoin transaction.

Originator and recipient information obtained during counterparty due diligence should also be subject to this screening mechanism. If an incoming stablecoin transfer occurs without prior screening, or if the required originator or recipient information is missing, HKMA-licensed Stablecoin Issuers must implement appropriate risk-mitigation measures based on their business practice, such as withholding stablecoins until the screening is complete, and adequately document the measures taken.

When screening identifies possible name matches, HKMA-licensed Stablecoin Issuers must conduct enhanced investigation to confirm if they are genuine hits and document all relevant records and results. Where suspicions of terrorist financing, proliferation financing or sanctions violations arise during screening or enhanced checks, HKMA-licensed Stablecoin Issuers must report relevant cases to the Joint Financial Intelligence Unit.

H. Suspicious transaction reports

HKMA-licensed Stablecoin Issuers have a statutory obligation under section 25A(1) Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405 of the Laws of Hong Kong) and the Organized and Serious Crimes Ordinance (Cap. 455 of the Laws of Hong Kong), and section 12(1) of the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575 of the Laws of Hong Kong), which require that a person who knows or suspects that any property:

1) represents proceeds of drug trafficking or an indictable offence (in whole or part, directly or indirectly);

2) was used in connection with such offences;

3) is intended for such use; or

4) constitutes terrorist property,

must file a suspicious transaction report with the Joint Financial Intelligence Unit as soon as reasonably practicable, disclosing all supporting information. Failure to report carries a maximum penalty of three months' imprisonment and a HK$50,000 fine under these ordinances.

Tipping off

Revealing information to other persons that might prejudice an investigation (including internal suspicions not yet reported) constitutes the criminal offence of "tipping off". Accordingly, notifying a customer of a suspicious transaction report filing is strictly prohibited as it compromises investigations. However, legitimate good-faith customer inquiries are permitted to the extent it does not tip off the customer.

To fulfil reporting obligations and manage ML/TF risks, HKMA-licensed Stablecoin Issuers must implement AML/CFT Systems including:

- appointing a Money Laundering Reporting Officer as the central point for internal reporting and the contact person with the Joint Financial Intelligence Unit and enforcement authorities;
- establishing clear policies/procedures for internal reporting, Joint Financial Intelligence Unit reporting, post-suspicious transaction report risk mitigation, and tipping-off prevention;
- providing guidance to staff on recognition of ML/TF indicators and forming suspicions; and
- maintaining records of internal reports and suspicious transaction reports.

Actions after filing of suspicious transaction reports

Suspicious transaction reports must be filed immediately after the suspicion arises and should be of high quality, incorporating feedback from the Joint Financial Intelligence Unit and HKMA. Upon filing a suspicious transaction report, HKMA-licensed Stablecoin Issuers must:

- conduct an immediate review of the relevant business relationship;
- implement risk-mitigating measures, such as freezing stablecoins pursuant to law enforcement requests;
- not continue the relationship without risk reassessment and controls; and
- escalate to senior management to determine further action and capacity to mitigate legal or reputational risks.

HKMA-licensed Stablecoin Issuers must establish clear policies and procedures to respond to law enforcement requests (e.g., warrants, production, restraint or confiscation orders) effectively and promptly. This includes allocating sufficient resources and designating a dedicated point of contact. When receiving crime-related requests regarding a customer or business relationship, HKMA-licensed Stablecoin Issuers are required to promptly assess the risks involved and review the business relationship for potential points of suspicion while keeping in mind that the customer may also be a victim.

I. Record-keeping

Maintaining comprehensive records is crucial for creating documentary records to detect, investigate and confiscate criminal or terrorist property or funds and allowing investigative authorities to establish financial profiles of suspects, trace illicit property or funds and examine historical transactions to determine criminal or terrorist links. Additionally, records also serve as documentary evidence of HKMA-licensed Stablecoin Issuers' compliance with the AMLO, the HKMA AML/CFT Guideline and HKMA directives.

HKMA-licensed Stablecoin Issuers must retain all necessary Customer Due Diligence information, transaction records and supporting documentation proportionate to their business' nature, size and complexity. These records should be kept in a manner that creates a clear and complete audit trail for all customer-related funds and stablecoin transactions, is readily available to the HKMA, authorities and authorised auditors, is able to indicate compliance with sections 20 and 21 of Schedule 2 AMLO on the duty to keep records and recording keeping requirements and all relevant HKMA guidelines.

Types of documents that should be kept by HKMA-licensed stablecoin issuers

HKMA-licensed Stablecoin Issuers must keep originals or copies of the following with data records for at least five years after completion of the relevant transaction regardless of whether the transaction is an occasional transaction and whether the business transaction will terminate after completion:

- data and information record and relevant documents in relation to verifying the identity of customers, beneficial owners, beneficiaries, persons who purport to act on behalf of the customer and/or other connected parties of the customer;
- documents obtained during Customer Due Diligence (including simplified or enhanced due diligence) and ongoing monitoring;
- original or copies of documents evidencing the purpose and nature of the business relationship;
- original or copies of significant account records and material business correspondence (including those in relation to the Customer Due Diligence conducted and major changes to the accounts' operations);
- analysis results, for instance evaluations of complex or unusual transactions;
- information obtained by ordering institutions during counterparty due diligence pursuant to the Travel Rule; and
- information and documents obtained before stablecoin transactions involving an unhosted wallet.

Manner and location of keeping records

The HKMA clarified that documents should be kept either as originals or as copies in microfilm or digital format, while data or information must be stored in microfilm or digital format on a computer database, which aligns with section 21 of Schedule 2 AMLO.

Documents and records must generally be kept for at least five years after the completion of the transaction. However, the HKMA may issue written notices requiring documents and records to be kept for a longer period if the records are related to special purposes such as a criminal or other investigation that is in progress.

Keeping records of suspicious transaction reports

HKMA-licensed Stablecoin Issuers are required to maintain a register of all ML/TF reports submitted to the Money Laundering Reporting Officer which should include:

- the reporting date;
- staff involved in preparing the report;

- assessment outcomes;
- whether a suspicious transaction report is filed with the Joint Financial Intelligence Unit; and
- references to locate supporting documentation.

Similarly, a register recording suspicious transaction reports filed with the Joint Financial Intelligence Unit must contain the filing date, identity of the reporting staff member, and locational details for related documents. These registers may be consolidated into a single system where operationally appropriate.

Record-keeping requirements regarding information and documents held by intermediaries

The HKMA clarified that even when customer identification and verification documents are retained by intermediaries, HKMA-licensed Stablecoin Issuers are ultimately responsible for complying with all record-keeping requirements. Accordingly, they must ensure that the intermediary maintains systems compliant with AMLO and the HKMA AML/CFT Guidelines, and will transfer requested documents and records promptly upon receipt of a request to do so from the HKMA-licensed Stablecoin Issuer. The HKMA reiterated that where HKMA-licensed Stablecoin Issuers engage intermediaries to conduct Customer Due Diligence, relevant information and data obtained must be passed to the HKMA-licensed Stablecoin Issuer and all documents and records should be transferred to the HKMA-licensed Stablecoin Issuer when the intermediary ceases to provide relevant services.

J. Next steps

The HKMA is currently developing supplementary AML/CFT guidelines for digital asset activities (including stablecoin offerings and digital asset custodial services) conducted by Authorised Institutions and HKMA-licensed Stablecoin Issuers and aim to conduct consultations on these guidelines in 2025.

This newsletter is for information purposes only

Its contents do not constitute legal advice and it should not be regarded as a substitute for detailed advice in individual cases. Transmission of this information is not intended to create and receipt does not constitute a lawyer-client relationship between Charltons and the user or browser. Charltons is not responsible for any third party content which can be accessed through the website.

If you do not wish to receive this newsletter please let us know by emailing us at **unsubscribe@charltonslaw.com**

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