

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

**Hong Kong Monetary Authority
26 May 2025**

Contents

1. Foreword.....	3
2. Background.....	4
3. Proposed AML/CFT requirements	8
4. AML/CFT Requirements for activities other than issuance and redemption.....	14
5. Next steps	15

1. Foreword

1.1. The Hong Kong Monetary Authority (HKMA) is issuing this consultation paper to seek views on the proposed anti-money laundering and counter-financing of terrorism (AML/CFT) regulatory requirements for stablecoin issuers to be licensed by the HKMA for carrying out regulated stablecoin activities (hereinafter referred as “licensee”). This paper should be read in conjunction with the Stablecoins Ordinance (SO) and the proposed Guideline on Supervision of Licensed Stablecoin Issuers¹.

1.2. The HKMA invites market participants and other interested parties to submit written comments on or before 30 June 2025 on the proposals discussed in this consultation paper through the following channels:

By email to (recommended means): stablecoin_feedback@hkma.gov.hk
(Subject: Consultation Paper on the Proposed AML/CFT Requirements for Regulated Stablecoins Activities)

By mail to: -

Hong Kong Monetary Authority
55/F, Two International Finance Centre
8 Finance Street
Central, Hong Kong
(Subject: Consultation Paper on the Proposed AML/CFT Requirements for Regulated Stablecoins Activities)

1.3. Persons submitting comments on behalf of an organisation should provide details of the organisation whose views they represent.

1.4. Please note that the names of commentators and the contents of their submissions may be published on the HKMA website and/or in other documents to be published by the HKMA.

1.5. If you do not wish your name or submission to be published by the HKMA, please indicate this when you make your submission.

¹ The Guideline on Supervision of Licensed Stablecoin Issuers is proposed to be published under section 171 of the Stablecoins Ordinance.

2. Background

Local developments on virtual assets activities

- 2.1. In October 2022, the Government issued a Policy Statement on the Development of Virtual Assets (VA) in Hong Kong, setting out its commitment to enhancing the VA regulatory framework under the principle of “same activity, same risk, same regulation”. In this regard, the Government has introduced a licensing system and regulatory requirements for VA service providers, ensuring that VA trading platforms (VATP) in Hong Kong comply with relevant international requirements, including control measures for AML/CFT and investor protection. The VATP licensing regime commenced operation in June 2023 and any person engaging in VATP business is required to apply for a licence from the Securities and Futures Commission (SFC).
- 2.2. On 18 December 2024, the Government introduced the Stablecoins Bill to the Legislative Council with the aim of establishing a regulatory regime for supervision of activities involving stablecoins and providing the Monetary Authority (MA) with relevant supervisory powers. The Stablecoins Bill has been passed by the Legislative Council on 21 May 2025.

Scope of regulated stablecoins and regulated stablecoin activities

- 2.3. “Stablecoin” is defined in section 3 of the SO. Essentially, stablecoins are a type of VA², used or intended to be used, as a medium of exchange, e.g. for payments for goods or services, and which purport to maintain a stable value with reference to a single asset, or a pool or basket of assets. The definition excludes digital representations of value that are issued by central banks or government, for example central bank digital currencies.
- 2.4. The SO sets out a regulatory framework for certain activities relating to “**specified stablecoins**”, which are defined in section 4 as stablecoins that purport to maintain a stable value with reference to one to more official currencies or a digital representation of value³. For the purpose of this consultation paper, the term “stablecoin” means a stablecoin that is a specified stablecoin defined under section 4 of the SO issued by a licensee.
- 2.5. Section 5 defines “**regulated stablecoin activity**”. Essentially, these activities include (i) issuing, in the course of business, a specified stablecoin in Hong Kong; (ii) issuing, in the course of business, a specified stablecoin outside Hong Kong that is wholly or partly referenced to Hong Kong dollars; and (iii)

² As defined in section 53ZRA of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap.615.

³ Section 4 of the Stablecoins Ordinance grants the Monetary Authority the power to specify a digital representation of value, or a class of digital representations of value, as a specified stablecoin by notice published in the Gazette.

carrying on activity specified by the Monetary Authority per subsection (4) of the SO. Carrying on these activities will require a licence issued by the MA.

- 2.6. The regulatory framework in the SO encompasses a number of activities in relation to stablecoins in addition to issuance, including offering and redemption. “**Offering specified stablecoins**” is defined in section 6, while other terms relevant to stablecoin activities are explained in the Glossary to the proposed Guideline on Supervision of Licensed Stablecoin Issuers.

Factors taken into consideration

- 2.7. In formulating the proposed AML/CFT regulatory framework for licensed stablecoin issuers, the HKMA has taken into account a number of factors, such as the potential risks associated with stablecoin activities and current international AML/CFT standards.

(i) Potential risks associated with stablecoin activities

- 2.8. Stablecoins share many of the same money laundering and terrorist financing (ML/TF) vulnerabilities as other forms of VAs, by virtue of their potential for anonymity, global reach and potential use in layering of illicit funds. Specific risks arise if the VAs and stablecoins can be transacted with unhosted wallets⁴ (sometimes also referred to as self-hosted or self-custody wallets) which allow VAs, including stablecoins, to be transacted peer-to-peer without the involvement of an intermediary and proper AML/CFT controls. Unhosted wallets can also be transferred physically which allow them to be operated by another person, effectively transferring ownership of the VAs without being recorded on the blockchain. The Financial Action Task Force (FATF), the international standard setting body for AML/CFT, has highlighted the potential risks associated with unhosted wallets based on the anonymity and mobility associated with VAs transacted through such devices⁵. As transactions to and from unhosted wallets may not involve AML/CFT-obliged intermediaries, they exhibit certain vulnerabilities which may be attractive to illicit actors seeking to obscure their financial activities⁶.
- 2.9. Furthermore, the VA landscape is evolving globally, and the pace of legal and regulatory developments for VA and virtual asset service providers⁷ (VASPs) varies among jurisdictions. As a result, stablecoins can be transacted among VASPs that are not yet licensed, registered or supervised for AML/CFT

⁴ Prevailing market practices showed that an unhosted wallet is a software or a hardware that enables a person to store and transfer VA, including stablecoins, on his own behalf, and in relation to which the private key is controlled or held by that person. The software provider of wallet or hardware wallet manufacturers may not be an AML/CFT-obliged entity for compliance of AML/CFT requirements.

⁵ Having similar characteristics to anonymous bearer instruments.

⁶ [Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers](#)

⁷ This refers to “virtual asset service provider” defined in the FATF Glossary.

purposes so long as they continue to circulate in the market and similarly may be attractive for illicit uses due to potential challenges in managing the associated ML/TF risks.

- 2.10. At the same time, VAs, including stablecoins, offer certain advantages that go some way towards mitigating ML/TF risks. All stablecoin transactions on-chain are recorded instantaneously and automatically on the blockchain on which they take place, including details such as time, date, transaction hash, and wallet addresses. As these records on the distributed ledger are irreversible and transparent, stablecoin transactions are inherently traceable. While there are tools, including mixers and tumblers, which may obfuscate the origins and owners of the funds, VA transactions are generally more traceable than traditional assets on traditional platforms. This can aid in the identification of transactions and wallets addresses involved in such activities.

(ii) International AML/CFT standards

- 2.11. International standards on AML/CFT generally place obligations on intermediaries between individuals and the financial system, such as financial institutions providing financial services to their customers. The act of minting/creation (i.e. creation of token contract) and the burning of VA (i.e. remove token from circulation on blockchain), will not fall in the scope of an intermediary under the international AML/CFT standards. That said, a stablecoin issuer becomes an intermediary when it undertakes functions such as offering and redemption of stablecoins to a customer in exchange with fiat currencies, provision of stablecoin custodian services, or facilitating transactions involving stablecoin etc.
- 2.12. Given that the development of stablecoins is still at an early stage and the associated ML/TF risks are evolving, the HKMA considers that there is a need for stablecoin issuers to comply with certain AML/CFT controls having regard to the nature of activities being carried out and the ML/TF risks associated with those activities. In particular, as described above, stablecoins (and other VAs) have certain unique features which give rise to ML/TF risks and therefore some additional controls are proposed to address these risks.
- 2.13. As a stablecoin issuer will undertake activities which results in it acting as an intermediary, it is intended that the stablecoin issuers will be included in the definition of “financial institution” in Schedule 1 of the Anti-Money Laundering and Counter-terrorist Financing Ordinance (Cap. 615) (AMLO) following the principle of “same activity, same risk, same regulation”.

Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Stablecoin Issuers) (the draft Guideline)

- 2.14. The proposed AML/CFT requirements for stablecoin issuers are set out in the draft Guideline, which is enclosed in the ***Annex***. To assist understanding, the next section summarizes key proposed AML/CFT requirements, the policy thinking behind those requirements and the questions on which the HKMA is seeking input from market participants and other interested parties.

3. Proposed AML/CFT requirements

3.1. General

3.1.1 As licensed and regulated financial institutions, we propose that every licensee⁸ should implement appropriate and effective AML/CFT policies, procedures and controls with a view to managing and mitigating ML/TF risks associated with its stablecoin business operations, including relating to the following minimum criteria for application (and, if a licence is granted, continuing requirements for maintaining the licence). The design and implementation of AML/CFT policies, procedures and controls should follow a risk-based approach. AML/CFT policies, procedures and controls should at a minimum cover the following aspects:

- (a) adoption of risk-based approach and conducting institutional ML/TF risk assessments (see Chapter 2 of the draft Guideline);
- (b) governance, senior management oversight, internal audit and staff training (see Chapter 3 of the draft Guideline);
- (c) controls to combat terrorist financing, financial sanctions and proliferation financing (see Chapter 7 of the draft Guideline);
- (d) suspicious transaction reporting (see Chapter 8 of the draft Guideline); and
- (e) record-keeping (see Chapter 9 of the draft Guideline).

3.1.2 In addition to the general requirements set out in paragraph 3.1.1 above, a licensee should comply with specific AML/CFT requirements appropriate to the activities it conducts. As stablecoins can be circulated and used in various circumstances, there is no one-size-fits-all AML/CFT framework that can be applied to different kinds of business models adopted by each licensee. In general, a licensee is responsible for issuance⁹ and redemption¹⁰ of stablecoin. The following paragraphs provide an overview of the specific AML/CFT requirements in relation to the activities of issuance and redemption.

⁸ Licensee is a person who is licensed to carry on a regulated stablecoin activity.

⁹ Issuance is explained in the Glossary to the proposed Guideline on Supervision of Licensed Stablecoin Issuers.

¹⁰ Redemption is explained in the Glossary to the proposed Guideline on Supervision of Licensed Stablecoin Issuers.

3.2. **Stablecoin issuance**

- 3.2.1. Minting of stablecoins refers to the creation of new stablecoins on a blockchain. By reference to current industry practices, minting can generally be classified into two models: “pre-minted model” (i.e. creating the tokens before they are transferred to another party) and “minted-on-demand model” (i.e. creating the token only when they are transferred to another party). Regardless of the minting models, a licensee should conduct customer due diligence (CDD) measures on its customers, including a person who has a business relationship with the licensee and a person who conducts an occasional transaction involving an amount equal to or above \$8,000 with the licensee.
- 3.2.2. Broadly speaking, a stablecoin holder may instruct the licensee to transfer the stablecoin to a custodial wallet provided by a VASP that holds or keeps the stablecoin on behalf of the holder, or to an unhosted wallet. The licensee should identify the customer’s wallet address and determine if the wallet address is a custodial wallet address or an unhosted wallet address. The licensee should also ascertain that the customer owns or controls the wallet address by appropriate confirmation methods to test the wallet ownership (see paragraphs 4.34 to 4.35 of the draft Guideline).
- 3.2.3. If a custodial wallet is used, the licensee should ascertain the identity of the institution providing such custodial wallet, and conduct due diligence measures on the institution before issuance of stablecoin. We propose that the due diligence measures should be similar to the VA transfer counterparty due diligence measures imposed by the SFC on VATPs¹¹ (see paragraphs 4.36 to 4.38 of the draft Guideline).
- 3.2.4. To mitigate additional vulnerabilities associated with unhosted wallets as stated in paragraph 2.8 above, we propose that if a stablecoin holder uses an unhosted wallet to receive the stablecoin from a licensee during the issuance process, the licensee should implement the additional controls before the stablecoin is transferred to the unhosted wallet (see paragraphs 4.39 to 4.41 of the draft Guideline):
- (a) conduct enhanced monitoring of stablecoin transfers with the unhosted wallet;
 - (b) transfer stablecoins only to the unhosted wallets that the licensee has assessed to be reliable, having regard to the screening results of the stablecoin transactions and the associated wallet addresses; and
 - (c) (where appropriate) impose transaction limits.

¹¹ Paragraph 12.13 of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers).

Q1: Do you agree with the proposed regulatory approach in relation to stablecoin issuance, including the need for (i) due diligence measures for the institution (e.g. financial institution or VASP) providing the custodial wallet for the stablecoin holder; and (ii) additional controls to mitigate the risks of unhosted wallets?

3.3. Stablecoin redemption

- 3.3.1. The SO makes it a condition for the grant of a licence that the MA must be satisfied that the licensee will meet all applicable minimum criteria if a licence is granted¹². One of the minimum criteria is that a licensee must provide a stablecoin holder a right to redeem the stablecoin on receiving a valid redemption request. A stablecoin holder, whether an individual or a legal person, can therefore redeem stablecoins directly from the licensee. We propose that before a licensee exercises a redemption request, the licensee should conduct CDD measures on the customer, including a person who has a business relationship with the licensee and a person who conducts an occasional transaction involving an amount equal to or above \$8,000 with the licensee, and ensure that the redemption request complies with all applicable legal and regulatory requirements.
- 3.3.2. Similar to issuance, before carrying out the redemption request, a stablecoin holder may transfer the stablecoin from a custodial wallet or from an unhosted wallet. A licensee should identify the customer's wallet address and confirm the ownerships of the wallet (see paragraphs 4.34 to 4.35 of the draft Guideline). If a customer's wallet is a custodial wallet, the licensee should conduct due diligence measures on the institution providing custodial wallet services (see paragraphs 4.36 to 4.38 of the draft Guideline).
- 3.3.3. We propose that if a stablecoin holder uses an unhosted wallet to return the stablecoin to a licensee during the redemption process, the licensee should also implement the additional controls set out in paragraph 3.2.4 above before the licensee carries out the redemption request.

Q2: Do you agree with the proposed regulatory approach in relation to stablecoin redemption, including the need for (i) due diligence measures for the institution (e.g. financial institution or VASP) providing the custodial wallet for the stablecoin holder; and (ii) additional controls to mitigate the risks of unhosted wallets?

¹² See section 15 of the SO; and Schedule 2 of the SO for the minimum criteria.

3.4. Ongoing monitoring

- 3.4.1. In light of the ML/TF risks noted in paragraphs 2.8 and 2.9 and given that stablecoins, unlike some other forms of VA, have an identifiable legal person as issuer, a licensee should take adequate measures to guard against the risk of the stablecoin it has issued for its customers being used for illicit purposes. To achieve this, a licensee should implement effective risk-based transaction monitoring systems and processes to detect the destination of the stablecoin transactions at issuance and the source of the stablecoin transactions at redemption, in order to identify and report suspicious transactions as well as take appropriate follow-up actions. It is noted that certain technologies are available which provide solutions to enable the tracking of stablecoins on the blockchain.
- 3.4.2. In this connection, a licensee should establish and maintain adequate and effective systems and controls to conduct screening of stablecoin transactions (i.e. transfer of stablecoins to or from customers) and the associated wallet addresses. In particular, the licensee should adopt appropriate technological solutions (e.g. blockchain analytic tools) to:
- (a) track the transaction history of stablecoins to more accurately identify the source¹³ and destination of these stablecoins; and
 - (b) identify transactions involving wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources, or designated parties.

(See paragraphs 5.4 and 5.5 of the draft Guideline)

Q3: Do you agree that the licensees should conduct ongoing monitoring for its customers to detect potential illicit activities for their specified stablecoins?

¹³ For the avoidance of doubt, a licensee does not need to identify the source of the stablecoin at issuance as the source is from the licensee.

3.5. Stablecoin transfers

- 3.5.1. Section 13A of Schedule 2 of the AMLO provides the special requirements for VA transfers (a.k.a. the Travel Rule), which apply to a licensee when it carries out a transfer of stablecoin¹⁴. The AMLO defines a VA transfer as:

“a transaction carried out –

- (a) by an institution (**ordering institution**) on behalf of an originator by transferring any virtual assets; and*
- (b) with a view to making the virtual assets available –*
 - (i) to that person or another person (**recipient**); and*
 - (ii) at an institution (**beneficiary institution**), which may be the ordering institution or another institution,*

*whether or not one or more other institutions (**intermediary institutions**) participated in completion of the transfer of the virtual assets.”*

- 3.5.2. We are of the view that a licensee may act as an ordering institution, an intermediary institution or a beneficiary institution in a stablecoin transfer depending on the business model. The licensee should follow the relevant requirements set out in this Chapter 6 of the draft Guideline with reference to its role in a stablecoin transfer.

Q4: To what extent do you consider licensees should comply with the special requirements for VA transfers set out in section 13A of Schedule 2 of the AMLO?

¹⁴ In circumstances where the transfer of stablecoins issued by a licensee falls under the definition of virtual asset transfer.

3.6. Additional measures for ongoing monitoring of stablecoins circulated in secondary markets

3.6.1. As set out in the Minimum Criteria for licensing¹⁵, a licensee must have in place adequate and appropriate systems of control for preventing and combating possible ML/TF in connection with its licensed stablecoin activities. Given the material risks of illicit use identified by the FATF in the secondary market¹⁶, measures in addition to those taken during issuance and redemption are required.

3.6.2. A licensee should therefore take adequate and proportionate ongoing monitoring measures to guard against the risks of stablecoins being used for illicit activities, examples of possible measures include:

- (a) confining the primary distribution and redemption of stablecoins to FIs and VASPs having adequate and effective AML/CFT controls;
- (b) adopting appropriate technological solutions (e.g. blockchain analytic tools) to screen stablecoin transactions and associated wallet addresses beyond primary distribution venue on an ongoing basis;
- (c) blacklisting of wallet addresses which are identified to be sanctioned or associated with illicit activities; and/or
- (d) any other appropriate means that can effectively mitigate the ML/TF risks arising from the stablecoins in circulation, including but not limited to whitelisting of stablecoin holders' wallet addresses or adopting a closed-loop approach by confining the stablecoin circulation to FIs and VASPs.

(See paragraphs 5.9 to 5.11 of the draft Guideline)

3.6.3. The HKMA expects that potential applicants will take into account international developments and availability of technology solutions to assist them in putting in place adequate safeguards to prevent the stablecoins from being misused for illicit purposes, including those relating to the secondary market. To balance development considerations and risk mitigation, the HKMA is open to proposals from the industry or other stakeholders as long as the licensee adheres to the above-mentioned principle.

¹⁵ Section 10 of Part 2 of Schedule 2 to the SO

¹⁶ These risks may be material if the stablecoin is allowed to be transacted peer-to-peer, unintermediated without the involvement of the licensee or any AML-obliged entities such as SFC-licensed VATPs, thereby presenting similar risks to anonymous bearer instruments.

Q5: Do you agree that a licensee should put in place adequate and appropriate systems and controls to effectively prevent or combat abuse of stablecoin transacted to or from unhosted wallets or unregulated wallets for ML/TF?

Q6: If so, do you have any suggestions as to possible risk mitigating measures for stablecoin transactions to and from unhosted wallet addresses, considering the different roles of various participants in the ecosystem, such as issuers, intermediaries and banks?

Q7: To what extent do you consider licensees should be held accountable for such monitoring of stablecoin transactions in the secondary market and how should such additional measures be implemented (e.g. scope and analytics frequency, control measures, etc.)?

4. AML/CFT Requirements for activities other than issuance and redemption

- 4.1. The HKMA is in parallel developing a supplementary AML/CFT guideline with regard to digital asset¹⁷ activities (e.g. offering stablecoins, provision of custodial services for digital assets) that may be conducted by Authorized Institutions and persons licensed to carry on a regulated stablecoin activity. Reference will be made to the relevant guidelines published by the SFC when developing the supplementary AML/CFT guidance to ensure a level playing field for financial institutions and that they are subject to the “same regulation” if they carry out “same activities”. The HKMA will consult relevant financial sectors later in 2025.

¹⁷ In the HKMA circular on Provision of Custodial Services for Digital Assets, 20 February 2024, the term “digital assets” refers to digital assets that depend primarily on cryptography and distributed ledger or similar technology, such as virtual assets as defined in section 53ZRA of the AMLO, tokenised securities and other tokenised assets. The term “digital assets” should be read to also cover the means of access to a digital asset, which generally refers to private keys, seeds or their backups.

5. Next steps

- 5.1 The HKMA seeks to adopt a balanced approach to the regulation of stablecoin issuers for AML/CFT purposes. In line with our risk-based approach to supervision, the HKMA has set out in this consultation paper the principles for the proposed AML/CFT regulatory requirements.
- 5.2 The HKMA will also carefully consider the feedback received during the consultation period and incorporate into the Guideline as appropriate. As technologies continue to advance and the VA regulatory landscape continues to evolve, the HKMA will stay abreast of international developments and also take into account feedback received from our participants in the stablecoin issuers sandbox for enhancing the draft Guideline.