June 30, 2025

ripple

Digital Finance Division
Monetary Management Department
Hong Kong Monetary Authority
55/F, Two International Finance Centre
8 Finance Street
Central
Hong Kong

Email: stablecoin_feedback@hkma.gov.hk

Dear Sir or Madam,

Ripple Labs Inc. ("Ripple") welcomes the opportunity to comment on the Consultation Paper on the Proposed AML/CFT Requirements for Regulated Stablecoin Activities ("AML/CFT Consultation") published by the Hong Kong Monetary Authority (the "HKMA") on May 26, 2025.[1]

Ripple is also grateful for the opportunity to comment on the Discussion Paper on Crypto-assets and Stablecoins (the "HKMA Discussion Paper") published by the HKMA on January 12, 2022[2] as well as the consultation paper on the Legislative Proposal to Implement the Regulatory Regime for Stablecoin Issuers in Hong Kong (the "Legislative Proposal") jointly published by the Financial Services and the Treasury Bureau (the "FSTB") and the HKMA on December 27, 2023.[3]

Ripple responded to the HKMA Discussion Paper on March 31, 2022 and the Legislative Proposal on February 29, 2024, and we request HKMA read the two responses in conjunction with this comment letter.

[1] *See* https://www.hkma.gov.hk/media/eng/regulatory-resources/consultations/20250526_Consultation_Paper_on_the_Proposed_AMLCFT_Reg_for_Regulated_Stablecoin_Activities.pdf, *Consultation Paper on the Proposed AML/CFT Requirements for Regulated Stablecoin Activities.*
[2] *See* https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2022/20220112e3a1.pdf, *Hong Kong Monetary Authority Discussion Paper on Crypto-assets and Stablecoins.*
[3] See https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2023/20231227e4a1.pdf, *Legislative Proposal to Implement the Regulatory Regime for Stablecoin Issuers in Hong Kong.*

Additionally, Ripple also responded to the Draft Guideline on Supervision of Licensed Stablecoin Issuers ("Draft Guideline") published by the Hong Kong Monetary Authority (the "HKMA") on 30 June, 2025[4] and we request that the response is also read in conjunction with this comment letter.

Ripple would like to thank the HKMA for both the in-depth and comprehensive analysis that has been undertaken to date, and for the opportunity to provide our comments. We respectfully request you take them into consideration as you consider the policy direction and scope of the intended AML/CFT requirements for regulated stablecoin activities in Hong Kong. We welcome the opportunity for further engagement with the HKMA on this AML/CFT Consultation and any other related consultations as may be appropriate.

As a global leader in enterprise blockchain solutions and the issuer of RLUSD, a U.S. dollar-backed stablecoin, Ripple is committed to fostering a secure, transparent, and compliant digital asset ecosystem. Ripple strongly supports the HKMA's initiative to establish a robust and forward-looking regulatory framework for fiat-referenced stablecoins (FRS) in Hong Kong. We commend the HKMA for its thoughtful approach in addressing risks while fostering innovation.

Ripple supports a technology-neutral, proportionate, and risk-sensitive approach to AML/CFT obligations. Given the growing institutional interest in stablecoins and tokenized financial instruments, clear and consistent AML/CFT expectations are essential to support responsible innovation and prevent regulatory arbitrage. Therefore, Ripple strongly agrees with the HKMA's recognition of the need for a regulatory framework that is aligned with international standards while being responsive to local market dynamics.

To support the industry in meeting the HKMA's expectations, Ripple suggests the following:

1. **Industry Engagement and Sandboxes**

We encourage the HKMA to establish a regulatory sandbox or working group focused specifically on AML/CFT controls for stablecoin use. This would allow licensees and vendors to test advanced compliance tooling and share feedback on technical feasibility and efficacy.

[4] *See* https://www.hkma.gov.hk/media/eng/regulatory-resources/consultations/20250526_Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, *Consultation Draft Guideline on Supervision of Licensed Stablecoin Issuers.*

2. **Safe Harbor for Known Risks**

In certain situations, such as low-risk transfers or transactions between trusted parties, licensees should be afforded a safe harbor where intensive screening requirements may be relaxed based on contextual analysis and prior transaction history.

3. **Global Regulatory Alignment**

Stablecoins frequently operate across borders. Ripple urges the HKMA to engage in international coordination, particularly with regulators in the EU, Singapore, Japan, and the U.S., to support cross-jurisdictional consistency in monitoring and enforcement standards.

4. **Technology-Driven Compliance Innovation**

Ripple continues to advocate for compliance-by-design architectures, including:

- On-chain identity and credentialing frameworks (e.g., decentralized identifiers or verifiable credentials);
- Smart contract-based controls for pre-approved transaction routing; and
- Zero-knowledge proofs to allow compliance checks without revealing personal data.

We urge the HKMA to encourage licensees to experiment with such tools to stay ahead of evolving ML/TF threats while preserving the efficiency and privacy benefits of blockchain-based systems.

We commend the HKMA's proactive approach in establishing a comprehensive regulatory framework that balances innovation with financial integrity.

We welcome HKMA's commitment to engaging with industry participants and look forward to continued collaboration. With the right safeguards and policy clarity, Hong Kong is well-positioned to become a leader in compliant, innovation-driven digital asset adoption.

***

With this overview, Ripple respectfully submits the following responses to the proposals in the AML/CFT Consultation in the attached Appendix.

Ripple appreciates the opportunity to provide feedback on the AML/CFT Consultation as the HKMA studies these important issues, and we would encourage and support further dialogue with all stakeholders.

Should you wish to discuss any of the points raised in this letter, please do not hesitate to contact Rahul Advani (Global Co-Head of Policy) at radvani@ripple.com and Caren Tso (Policy Manager, APAC) at ctso@ripple.com.

Sincerely,

Ripple Labs Inc.

APPENDIX

Ripple respectfully submits the following responses to the proposals in the AML/CFT Consultation.

Question 1: 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?

Ripple is broadly supportive of the proposed regulatory approach in relation to stablecoin issuance, and we believe the proposals are risk-based and proportionate. We are also supportive of the proposed due diligence measures for custodial wallet providers and enhanced controls related to unhosted wallets.

We believe these measures are broadly appropriate and aligned with global efforts to mitigate AML/CFT risks while enabling responsible innovation in the use of stablecoins. However, we believe the following recommendations could help provide further clarification to licensees and align the proposals in the AML/CFT Consultation with global best practices.

a. Due diligence for custodial wallet providers

Ripple agrees that when a stablecoin is issued to a custodial wallet, the licensee should identify and conduct due diligence on the custodial institution - especially where the licensee does not have a direct relationship with the end user. This is consistent with established regulatory principles under the Financial Action Task Force ("FATF") Recommendation 16 (i.e., the "Travel Rule") and similar measures implemented by the Securities and Futures Commission ("SFC") for virtual asset trading platforms ("VATP"s). However, given the diversity of service providers in the stablecoin ecosystem, we suggest that the HKMA:

- Provide clarity on the types of custodial institutions that meet acceptable due diligence thresholds (e.g. regulated financial institutions, licensed VATPs, trust companies etc.);
- Allow risk-based adjustments based on jurisdictional equivalence (e.g. if the custodial provider is regulated in a jurisdiction with AML/CFT standards deemed equivalent to Hong Kong);
- Offer a mechanism for licensees to maintain an internal whitelist or register of approved custodial wallet providers to streamline compliance and ensure consistency.

These steps will ensure that AML/CFT obligations are met without overly restricting operational efficiency or excluding reputable foreign custodians.

b. Additional controls for unhosted wallets

Ripple also supports HKMA's recognition of the unique challenges posed by unhosted (i.e., non-custodial) wallets. Ripple has long advocated for a balanced approach that recognizes the legitimate use cases of self-hosted wallets, while addressing the potential for misuse in illicit finance.

The proposed requirements, including enhanced monitoring, reliability assessment of wallet addresses, and imposing transaction limits where appropriate, are reasonable and consistent with emerging best practices from regulators globally (including FATF's guidance on peer-to-peer transactions).

However, we offer the following refinements for HKMA's consideration:

- Enhanced monitoring should be risk-calibrated: Stablecoin transfers to long-standing self-hosted wallets of known customers (e.g. institutional clients, fintech partners) may not carry the same risk as newly created or previously flagged addresses. Licensees should be able to apply differentiated monitoring rules based on behavioural patterns, source of funds, and user profile.
- Defining "reliable" wallets: The AML/CFT Consultation refers to assessing "wallet reliability". Ripple recommends that this include criteria such as transaction history, blockchain analytics scoring (e.g. via providers like Chainalysis or TRM Labs), and association with previously verified identities.
- Transaction limits: Limits should be guided by the results of the risk assessment, not applied arbitrarily. For example, small-value transfers to self-hosted wallets used by retail users should not be subject to disproportionate restrictions.
- Encouraging technical safeguards: In addition to transaction monitoring, the HKMA could encourage the use of technical methods such as address whitelisting, on-chain attestations, or cryptographic ownership verification (e.g. signing messages from the wallet) to validate control and reduce reliance on off-chain verification methods.

Ripple believes the application of AML/CFT controls should remain technology-neutral. The use of self-hosted wallets is not inherently riskier than custodial services, provided licensees can demonstrate control, verification, and transaction monitoring. As such, we urge the HKMA to allow for the use of compliance innovation - such as privacy-preserving tools, decentralized identity systems, and verifiable credentials - to enhance oversight without undermining user rights or innovation.

We believe the measures outlined above will help strike an appropriate balance between managing financial crime risk and supporting the development of a compliant and competitive stablecoin ecosystem in Hong Kong.

Question 2: 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?

Ripple supports the HKMA's commitment to establishing a robust AML/CFT framework for stablecoin redemption, and broadly agrees with the proposed approach as outlined in Section 3.3 of the AML/CFT Consultation. Redemption is a key lifecycle event for stablecoins, and should be subject to appropriate risk-based safeguards. We particularly endorse the emphasis on verifying wallet ownership, performing counterparty due diligence, and applying enhanced measures where necessary. However, we believe the following recommendations could help provide further clarification to licensees and align the proposals in the AML/CFT Consultation with global best practices.

a. Due diligence measures for custodial wallet providers

Ripple agrees that when redemption requests involve custodial wallets, it is essential for the licensee to identify the institution providing the wallet service and conduct appropriate due diligence on that entity. This requirement is consistent with the principle of KYC and aligns with international expectations for VASP interactions under the FATF's Travel Rule.

To support clarity and consistency in application, we recommend the HKMA consider the following refinements:

- Risk-tiered diligence: The intensity of due diligence measures should be aligned with the risk profile of the custodial institution. For example, custodians licensed in jurisdictions with strong AML/CFT oversight could be subject to simplified due diligence, while less regulated or opaque entities should trigger enhanced measures.
- Jurisdictional equivalence: To streamline cross-border activity, the HKMA could publish or endorse a list of jurisdictions whose regulatory frameworks are deemed equivalent for the purposes of AML/CFT obligations. This would encourage alignment and reduce compliance friction.
- Whitelist option: Licensees should be permitted to maintain an internal list of vetted custodial wallet providers based on pre-established risk criteria. This will ensure efficiency and consistency in repeated redemption processes involving frequent counterparties.

b. Additional controls for unhosted wallets

Ripple also agrees with the proposed requirement for licensees to apply additional controls when processing redemptions involving unhosted wallets. The characteristics of unhosted wallets - namely, their ability to operate outside of

regulated financial intermediation - may warrant enhanced monitoring and safeguards. The proposed measures from section 3.2.4 (referenced again in 3.3.3) are reasonable and proportionate. However, Ripple once again believes the application of AML/CFT controls should remain technology-neutral. The use of self-hosted wallets is not inherently riskier than custodial services, provided licensees can demonstrate control, verification, and transaction monitoring. As such, we urge the HKMA to allow for the use of compliance innovation - such as privacy-preserving tools, decentralized identity systems, and verifiable credentials - to enhance oversight without undermining user rights or innovation.

We also suggest the HKMA consider how its guidance aligns with international best practices and regulatory developments in peer jurisdictions (e.g. the EU's MiCA regime, Singapore's Payment Services Act). Greater convergence will support efficiency in cross-border stablecoin flows and reduce regulatory arbitrage risks.

Question 3: Do you agree that the licensees should conduct ongoing monitoring for its customers to detect potential illicit activities for their specified stablecoins?

Ripple supports the HKMA's proposal to require licensees to conduct ongoing monitoring of stablecoin activity. As a regulated issuer of a USD-backed stablecoin (RLUSD), Ripple recognizes that stablecoins - because of their wide applicability in payments, remittances, and settlement - could pose unique AML/CFT risks. However, they also offer a higher degree of transparency and traceability than traditional financial instruments when implemented responsibly.

We agree with the HKMA that the existence of a known legal issuer and the traceable nature of blockchain transactions position stablecoins uniquely for effective AML/CFT oversight. Ongoing monitoring obligations, when risk-based and technology-enabled, can significantly enhance the detection and mitigation of illicit finance risks.

Ripple fully supports the requirement that licensees implement effective, risk-based transaction monitoring systems and processes to detect:

- The destination of stablecoins at issuance, and
- The source of stablecoins at redemption.

This dual-sided visibility helps build a comprehensive understanding of transactional behavior, user intent, and associated risks. By monitoring wallet address behavior over time, especially those involved in higher-value or high-frequency flows, licensees can better identify patterns indicative of money laundering, sanctions evasion, or other illicit activities.

However, we suggest that the HKMA incorporate the following best practices and clarifications in implementing this requirement:

a. Use of blockchain analytics tools

We agree with the HKMA's encouragement for licensees to adopt blockchain analytics tools. Tools offered by blockchain analytics firms (e.g., Chainalysis, TRM Labs) can support the following objectives:

- On-chain wallet profiling (associating wallets with known entities or typologies);
- Transaction risk scoring (e.g., proximity to illicit actors, mixer usage, darknet connections);
- Sanctions screening (against OFAC, UN, EU lists), and
- Behavioral pattern detection (e.g., structuring, layering).

Ripple currently uses blockchain analytics to monitor on-chain activity related to RLUSD and supports the industry-wide adoption of similar solutions.

b. Wallet address screening

We support the HKMA's proposal that licensees should screen both the sender and recipient wallet addresses of stablecoin transactions. This aligns with global AML/CFT standards and helps prevent tainted funds from entering or exiting the regulated ecosystem. However, to avoid excessive false positives, screening systems should allow for contextual risk weighting, e.g.:

- Distinguishing between direct and indirect exposure to high-risk addresses;
- Considering the proportion and timing of exposure, and
- Taking into account the overall risk profile of the user.

c. Risk-based calibration

Ripple recommends that licensees be permitted to calibrate monitoring intensity based on transaction characteristics, such as:

- Transaction value and frequency;
- Wallet behavior history;
- Jurisdictional risk exposure;
- User type (retail vs. institutional).

A tiered monitoring model will ensure that regulatory resources are focused where risks are most concentrated, and compliance obligations remain proportionate.

Ripple believes that stablecoins, when supported by strong compliance programs, can actually enhance the transparency and auditability of financial flows. Unlike cash or certain off-chain instruments, blockchain-based assets create immutable transaction records that are available for real-time analysis. These features support law enforcement and regulatory oversight while enabling innovation in payments and tokenized finance. By encouraging licensees to implement

best-in-class transaction monitoring and wallet screening, the HKMA is laying the groundwork for a secure and scalable stablecoin ecosystem in Hong Kong.

Question 4: 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?

Ripple supports the consistent application of the AML/CFT requirements under section 13A of Schedule 2 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance ("AMLO") to regulated stablecoin activities, provided that implementation remains risk-based, technology-neutral, and aligned with international standards. We recommend that the HKMA incorporate the following best practices and clarifications in implementing these requirements:

We agree that licensees involved in stablecoin transfers, whether as ordering institutions, beneficiary institutions, or intermediaries, should comply with the relevant obligations set out in section 13A of Schedule 2 of the AMLO. This includes collecting, transmitting, and receiving originator and beneficiary information in accordance with the transaction's role and routing. However, it is critical that the application of these rules:

- Distinguishes between regulated and unregulated counterparties: For example, when a licensee transfers stablecoins to or from another regulated institution within Hong Kong or a FATF-aligned jurisdiction, information-sharing mechanisms should be streamlined. Conversely, higher scrutiny should apply to transfers involving unregulated or entities in non-FATF jurisdictions.
- Exempts certain low-risk or low-value transfers: The HKMA should consider providing thresholds or exemptions for de minimis transactions, which are unlikely to pose material ML/TF risks. This is consistent with the FATF's allowance for thresholds (e.g., USD/EUR 1,000) in its Travel Rule guidance.
- Allows for reasonable reliance on counterparties: Licensees should be permitted to rely on counterparties' compliance programs (subject to risk assessment) when they are dealing with other regulated institutions, to avoid duplicative compliance burdens.

However, Ripple notes several practical and technical challenges in complying with the Travel Rule for stablecoin transfers, particularly across different networks and jurisdictions:

- Lack of interoperable messaging standards: The digital asset industry continues to face fragmentation in how originator and beneficiary data is transmitted. Although messaging standards like IVMS 101 have gained traction, technical implementation varies widely. The HKMA could support the development of interoperable protocols and industry-wide sandboxes

for testing Travel Rule compliance in cross-chain and cross-jurisdictional scenarios.

- Counterparty identification and onboarding: In some cases, especially where transfers involve unhosted wallets or new VATPs, collecting beneficiary data may be operationally difficult or raise privacy and security concerns. The HKMA should issue practical guidance on how to handle unhosted wallet interactions and counterparty due diligence when full originator/beneficiary data is unavailable; and
- Timing and sequencing of data transmission: Some blockchain-based stablecoin transfers occur instantaneously, which can challenge pre-validation of Travel Rule data. HKMA could adopt a phased or "as soon as technically feasible" approach, as suggested by the FATF, to allow institutions time to align infrastructure with regulatory obligations.

Ripple also encourages the HKMA to work closely with regional and global regulators to ensure alignment in the interpretation and implementation of Travel Rule obligations. Divergent standards across jurisdictions can lead to compliance uncertainty, increase operational costs, and reduce the competitiveness of Hong Kong as a global digital asset hub. We also recommend that the HKMA explore frameworks for mutual recognition of equivalent Travel Rule compliance systems, particularly with jurisdictions that have adopted robust digital asset regulations (e.g. Singapore, the EU under MiCA, and the U.S. where applicable).

Question 5: 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?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?

Ripple supports the HKMA's principle-based approach to monitoring and mitigating ML/TF risks associated with the circulation of stablecoins in secondary markets. We agree that licensees must implement appropriate systems and controls to address these risks, particularly where stablecoins are transacted with unhosted wallets or wallets managed by unregulated entities.

However, we also encourage the HKMA to ensure that any such controls remain proportional, technologically feasible, and flexible enough to support ongoing innovation, especially given the evolving state of both stablecoin usage and compliance technology.

Stablecoins, by design, are transferable peer-to-peer, making secondary market circulation both inevitable and vital to their utility. As such, Ripple agrees that regulatory frameworks must extend beyond issuance and redemption to include

monitoring of post-issuance activity, including transfers to and from unhosted or unregulated wallets. We believe that licensees should be required to implement ongoing monitoring protocols that include:

- Use of blockchain analytics tools to trace stablecoin movement across the public ledger;
- Screening wallet addresses against sanctions and watchlists; and
- Blacklisting and whitelisting mechanisms to manage counterparty risk.

These tools allow for the real-time detection of suspicious patterns, and licensees can take pre-emptive action such as freezing transfers, suspending redemption, or flagging transactions for regulatory reporting.

We provide the following feedback on the HKMA's suggested controls:

a. Confine primary issuance/redemption to regulated entities

Ripple supports the idea of restricting issuance and redemption functions to financial institutions and licensed VATPs that meet AML/CFT standards. However, we caution that such limitations should not extend to the secondary use of stablecoins, which would defeat their core utility and programmability. Restricting who may hold, use, or transfer stablecoins after issuance - particularly in retail or DeFi contexts - would undermine interoperability and financial inclusion.

b. Blockchain analytics tools

We strongly endorse the adoption of blockchain analytics solutions to:

- Map transactional flows;
- Monitor wallet behavior; and
- Score risk exposure to illicit actors.

Ripple uses such tools in connection with our enterprise products and with RLUSD, and believes they represent the most effective method of post-distribution monitoring in open systems.

We recommend the HKMA clarify that licensees may select from a range of qualified providers and should not be required to adopt a specific vendor or framework, provided the tools meet baseline requirements.

c. Blacklisting and whitelisting

The blacklisting of wallet addresses linked to illicit activity is a reasonable requirement and consistent with global AML practices. Licensees should be expected to maintain internal watchlists and integrate these with analytics tools and transaction monitoring systems.

Whitelisting, on the other hand, can be more restrictive. While suitable in closed-loop or permissioned ecosystems, enforcing whitelisting across open,

public blockchains can raise significant operational and inclusion-related challenges. We suggest that whitelisting remain optional or only be required for specific use cases, such as stablecoin usage in tokenized securities or enterprise-grade closed-loop payment networks.

Question 6: 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?

Ripple supports a nuanced, role-based approach to mitigating the risks associated with stablecoin transactions involving unhosted wallets. While unhosted wallets play a legitimate role in enabling self-custody, financial inclusion, and decentralized innovation, they could also present challenges in terms of customer due diligence ("CDD"), transaction monitoring, and traceability. The appropriate mitigation tools and responsibilities will vary based on the nature and function of the regulated entity within the ecosystem.

We have outlined role-specific risk mitigation strategies below, emphasizing proportionality, technological feasibility, and regulatory interoperability.

a. Role-specific risk mitigation measures

i. Stablecoin issuers

Issuers, while often not directly engaged in peer-to-peer transfers involving unhosted wallets, can support risk mitigation in the following ways:

- KYC at entry and exit points: Ensure robust CDD at the time of issuance and redemption, even where intermediaries are involved.
- Wallet ownership verification: Use technical methods (e.g., signature verification, whitelisting, or nonce challenges) to confirm that an unhosted wallet is controlled by the intended recipient.
- Reserve controls: Link redemption rights strictly to verifiable identity or wallet control to prevent anonymous exits from the system.
- Monitoring via blockchain analytics: Deploy tools to trace post-issuance wallet activity and flag interactions with high-risk addresses (e.g., mixers, darknet entities, sanctioned parties).

ii. Intermediaries (VATPs, wallet providers, payment processors)

Intermediaries serve as the most frequent touchpoint between users and the stablecoin ecosystem and are best placed to implement front-line controls such as:

- Transaction screening: Integrate blockchain intelligence tools to assess risk of unhosted wallet addresses (e.g., proximity to illicit funds, velocity, or behavioral anomalies).

- Risk scoring and tiered controls: Assign risk scores to wallet interactions and calibrate controls accordingly (e.g., enhanced due diligence, transfer limits, or transaction freezing for high-risk scores).
- Enhanced Due Diligence ("EDD"): For frequent or high-value transfers to/from unhosted wallets, collect additional customer information (e.g., source of funds, wallet provenance).
- Threshold-based triggers: Establish monetary or frequency-based thresholds that trigger manual review, suspicious transaction reporting, or wallet deactivation.
- Educational campaigns: Inform customers about safe wallet usage and the regulatory risks of engaging with high-risk wallets.

iii. Banks and regulated financial institutions

While banks may not directly facilitate stablecoin transactions today, they will increasingly interact with crypto-native services via custody partnerships, payment facilitation, or banking-as-a-service models.

Therefore, we recommend that banks:

- Apply consistent AML/CFT controls across fiat and digital interfaces, ensuring the origin/destination of funds can be linked to a verifiable identity.
- Participate in ecosystem-wide monitoring networks, e.g., via shared watchlists or suspicious activity signaling mechanisms for wallet addresses flagged by peers or regulators.
- Implement dynamic risk assessment models that take into account blockchain transaction data alongside traditional financial intelligence.

b. Cross-cutting Recommendations

Regardless of role, Ripple recommends the following shared approaches:

- Adopt open standards: Use interoperable formats like IVMS 101 to facilitate information exchange when interacting with other VASPs.
- Leverage privacy-preserving compliance tools: Encourage the development of solutions such as zero-knowledge proofs, verifiable credentials, and decentralized identifiers to allow wallet users to attest to compliance attributes without compromising privacy.
- Maintain a registry of known wallet behaviors: Promote industry-wide data sharing (e.g., through a regulator-supported whitelist/blacklist registry) to harmonize assessments of wallet risks.

Ripple believes that managing risks related to unhosted wallets is not about banning or restricting legitimate self-custody but about developing tiered, data-driven, and collaborative safeguards tailored to each actor in the ecosystem. By assigning responsibilities based on capabilities and exposure - and supporting innovation in compliance tools - the HKMA can ensure that Hong Kong's stablecoin regime balances risk mitigation with global competitiveness.

Question 7: 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.)?

Ripple broadly agrees that licensees should be held accountable for implementing reasonable, risk-based monitoring of stablecoin transactions in the secondary market. However, accountability must be clearly defined, proportionate to the licensee's role and technical capacity, and supported by realistic expectations around scope, analytics frequency, and operational feasibility.

Stablecoins - by design - are intended to circulate beyond their primary issuance and redemption environment. As such, while licensees should play a role in preventing illicit use, they cannot and should not be made solely responsible for all activity in open secondary markets, especially for peer-to-peer transactions beyond their visibility or control.

Therefore, Ripple recommends a layered accountability model, based on the licensee's control over and proximity to the transaction. Primary accountability should apply to issuance and redemption events, and to on-platform transfers where the licensee retains custody or clear visibility into customer identity and wallet usage.

Secondary accountability should apply to:

- Known or recurring customer wallet addresses (e.g., whitelisted self-hosted wallets);
- Transfers facilitated via the licensee's infrastructure (e.g., APIs or smart contracts); and
- High-risk or high-volume transactions involving flagged counterparties.

Tertiary or limited accountability should apply where:

- The licensee has no custodial relationship or technical control over the stablecoin flow;
- The transaction occurs entirely off-platform or between third parties, and
- Compliance tools cannot realistically provide deterministic wallet ownership attribution.

Ripple supports the principle that licensees should be accountable for what they can monitor, influence, or control, not for all downstream activity on public blockchains.

To guide effective and fair implementation, Ripple recommends the following parameters for secondary market monitoring:

a. Scope of analytics

Focus on transfers to/from external wallet addresses, particularly:

- First-hop transactions after issuance;
- Last-hop transactions before redemption; and
- Known risky destinations (e.g., mixers, flagged exchanges).

Monitor for exposure to sanctioned entities, proximity to high-risk transaction clusters, and involvement in typologies associated with money laundering or fraud.

b. Analytics frequency

Real-time or near-real-time screening should be applied to transactions that are part of the issuance/redemption flow, involve known suspicious wallet addresses, and/or exceed value or frequency thresholds.

Periodic batch analysis (e.g., daily or weekly) can be used for general transaction monitoring and wallet behavior profiling, while event-triggered review should apply when new risk indicators emerge (e.g., new OFAC sanctions, hack reports, or law enforcement requests).

c. Control measures

Based on analytics output, licensees should have pre-defined escalation actions, such as:

- Flagging or blocking redemption from high-risk wallets;
- Conducting EDD on suspicious transfers;
- Filing suspicious transaction reports ("STR"s); and
- Blacklisting and/or de-prioritizing engagement with repeat-offender wallets.

These control measures should be documented in internal policies, subject to regular review, and be proportional to the entity's size, technology, and customer risk profile.

Ripple recommends that the HKMA issue detailed guidance clarifying expectations for "reasonable monitoring" and thresholds for compliance action, and also supports flexibility in implementation, allowing licensees to choose and integrate blockchain analytics providers best suited to their business model and risk exposure.

The HKMA could also encourage compliance innovation through sandboxes or supervised pilot programs, particularly for tools involving on-chain identifiers, privacy-preserving compliance protocols, or automated compliance scoring, and

foster public-private collaboration to share typologies, wallet risk lists, and best practices for cross-platform monitoring.

To reduce regulatory fragmentation and promote global scalability, Ripple urges the HKMA to align its expectations with those of other leading jurisdictions (e.g., FATF guidance, EU MiCA requirements, MAS stablecoin regime). Mutual recognition of monitoring and enforcement protocols will improve operational efficiency and cross-border cooperation in combating illicit finance.

Ripple supports holding licensees accountable for risk-based, technologically enabled monitoring of secondary market stablecoin activity within the bounds of their visibility and control. Therefore, we recommend a tiered model of accountability, calibrated expectations for analytics and control, and a collaborative approach to industry-wide compliance innovation.