



Stablecoin Regulation in Hong Kong Part 2

February 2026

Julia Charlton, Charltons

Today's Focus

- Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) obligations for licensed stablecoin issuers, including Travel Rule compliance
- Restrictions on offering Specified Stablecoins
- The process for applying for a stablecoin issuer licence from the HKMA
- Overview of key offences under the Stablecoins Ordinance

AML & CFT Framework

Licensed Stablecoin Issuers are "financial institutions" under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) and must comply with Schedule 2 requirements and all HKMA guidance

AMLO Compliance

Implement controls to prevent and combat money laundering and terrorist financing

HKMA Guideline

Follow the Guideline on Anti-money Laundering and Counter-financing of Terrorism for Licensed Stablecoin Issuers (AML/CFT Guideline)

Continuing Eligibility

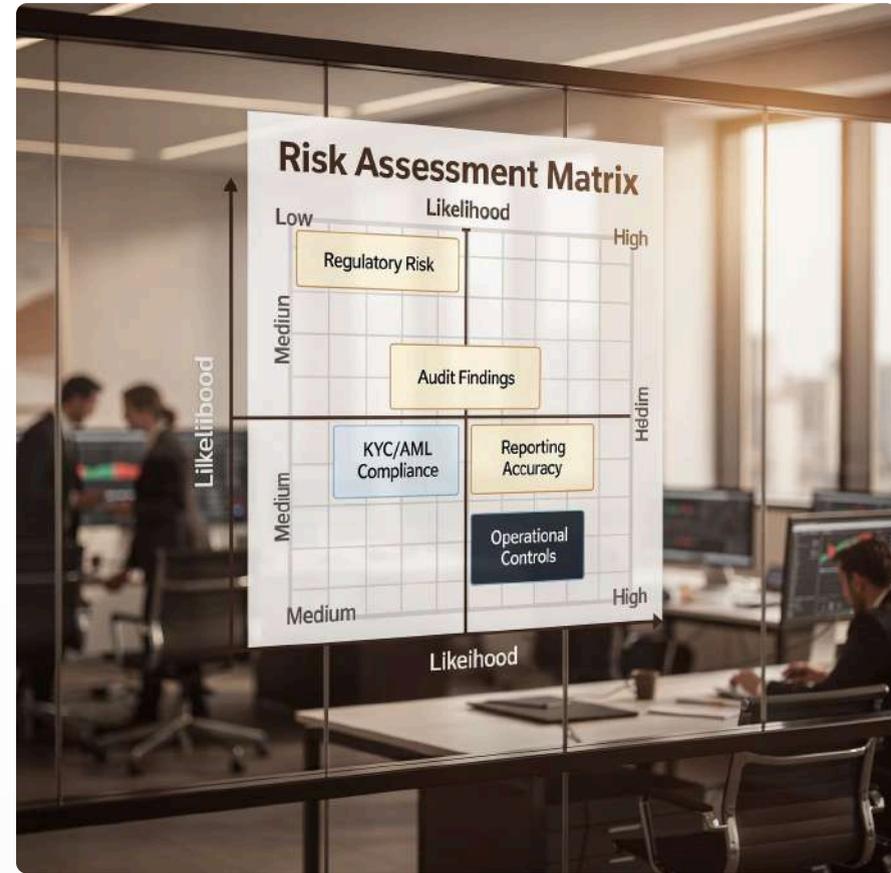
Maintain compliance as a licensing criterion under Section 10 of Schedule 2 to the Stablecoins Ordinance



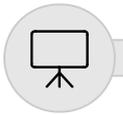
Risk-Based Approach

Assessment Requirements

- Conduct institutional risk assessment
- Identify customer, country, product and delivery channel risks
- Keep risk assessment up-to-date
- Implement systems to manage and mitigate risks



Governance Structure



Board & Senior Management

Approve AML/CFT systems and understand ML/TF risks



Compliance Officer

Overall responsibility for establishing and maintaining AML/CFT systems



MLRO

Money Laundering Reporting Officer acts as central reference point for suspicious transaction reporting

Compliance Management



Independent Audit Function

Review AML/CFT systems to ensure effectiveness



Employee Screening

Appoint individuals with high integrity to AML/CFT roles



Staff Training

Ongoing, role-specific training tailored to responsibilities and experience levels

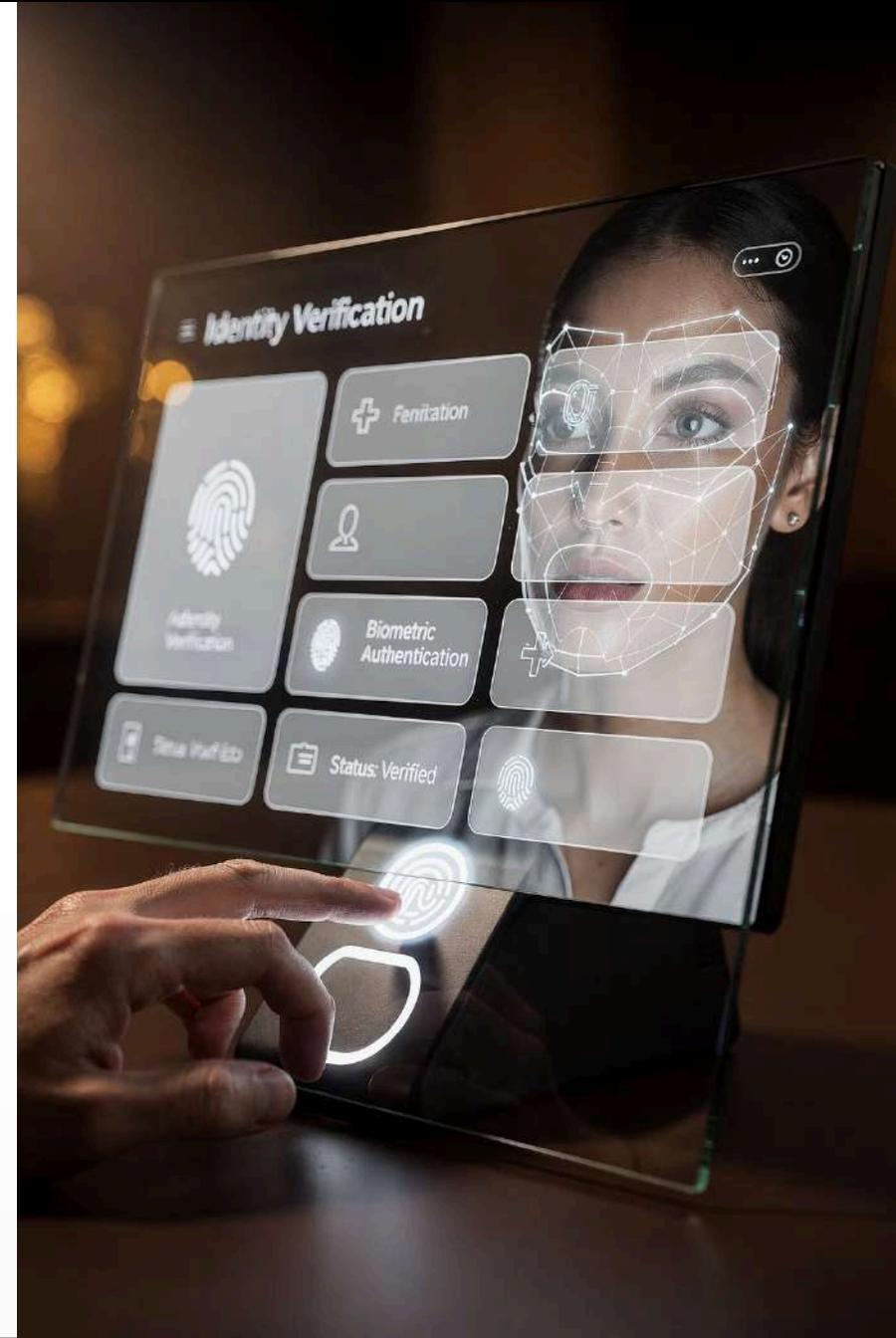


Customer Due Diligence (CDD)

Stablecoin Holders = holders of Specified Stablecoins

Licensed issuers must treat as customers:

- Persons with whom they have a business relationship
- Persons conducting occasional transactions (e.g., issuance and redemption of Specified Stablecoins) (Paragraph 4.1 AML/CFT Guideline)



When CDD Must Be Conducted

1

Before Business Relationship

Prior to establishing relationship
with customer

2

Occasional Transactions

Before transactions (including
Specified Stablecoin issue and
redemption) involving HK\$8,000 or
more

3

Suspicion Arises

When ML/TF suspected or doubts
about identification information

Paragraph 4.4 AML/CFT Guideline

Four Fundamental CDD Measures



Identify & Verify Customer

Using reliable, independent source documents, data or information



Beneficial Owners

Identify and take reasonable measures to verify their identities



Purpose & Nature

Obtain information on purpose and intended nature of business relationship



Representative Authority

Verify identity and authority of person(s) acting on behalf of customer

Paragraph 4.3 AML/CFT Guideline



Customer Identification Requirements

Natural Persons

- Full name
- Date of birth
- Nationality
- Residential address
- Unique identification number
- Document type (HKID, passport)

Legal Persons

- Full name
- Date and place of incorporation
- Registered office address
- Unique identification number
- Current existence and powers that regulate it

Paragraphs 4.6-4.9 AML/CFT Guideline

Non-Face-to-Face Onboarding

Remote customer identification requires either:

Digital ID System

Use HKMA-recognised digital identification system

Technology Verification

Appropriate technology ensuring document authenticity and linking person to authenticated identity

Supplementary Data

IP addresses, geo-location, device identifiers, wallet addresses, transaction hashes

Paragraphs 4.10 and 4.11 AML/CFT Guideline



Connected Parties & Beneficial Owners of Legal Entity Customers

01

Identify Connected Parties

Obtain names of all connected parties (e.g., directors of corporate customers)

03

Senior Managing Officials

If no beneficial owner identified, verify identity of senior managing officials

Paragraphs 4.12 and 4.15 AML/CFT Guideline

02

Beneficial Owners

Natural persons with controlling ownership interest (>25%) or exercising control over management

04

Ownership Structure

Understand customer's ownership and control structure; verify legitimate reasons for complexity

Enhanced vs Simplified Due Diligence

Enhanced Due Diligence

Required for high ML/TF risk cases, complying with section 15 of Schedule 2 to AMLO

Senior management approval needed for high-risk relationships

Paragraph 4.18 AML/CFT Guideline

Simplified Due Diligence

Permitted in low-risk scenarios under section 4 of Schedule 2 to AMLO

Cannot be used if risks increase, ML/TF suspected, or doubts about identification

Compliance Risk Level Scale





Politically Exposed Persons (PEPs)

Non-Hong Kong PEPs

Establish source of wealth and funds before relationship; senior management approval required

Hong Kong PEPs

Enhanced measures when higher ML/TF risk identified

International Organisation PEPs

Risk-based enhanced measures apply

Former PEPs

Enhanced measures can cease if no longer high risk after assessment

Paragraphs 4.22-4.24 AML/CFT Guideline

Third Party Distributors

When appointing third-party entities to distribute Specified Stablecoins, licensed issuers must:

- Treat as Customer**
Conduct full CDD on the distributor
- Understand Business**
Collect sufficient information on the third-party's business operations
- Assess Reputation**
Determine reputation and quality of AML/CFT regulation in operating jurisdiction
- Evaluate Controls**
Assess adequacy and effectiveness of third-party's internal AML/CFT controls
-

Paragraph 4.21 AML/CFT Guideline



CDD Failure Consequences

Required Actions

- Cannot establish business relationship
- Cannot carry out occasional transaction
- Must terminate existing relationship as soon as reasonably practicable
- Consider filing Suspicious Transaction Report with Joint Financial Intelligence Unit (JFIU)

Paragraph 4.30 AML/CFT Guideline



Wallet Risk Management



Custodial Wallets

Provided by custodial wallet providers (financial institutions or VASPs)



Unhosted Wallets

Self-hosted wallets where private key is held and controlled by owner

Paragraph 4.33 AML/CFT Guideline



Wallet Verification Process

01

Identify Wallet Address

Licensed issuer must identify each customer's wallet address used to receive or return Specified Stablecoins from/to issuer

03

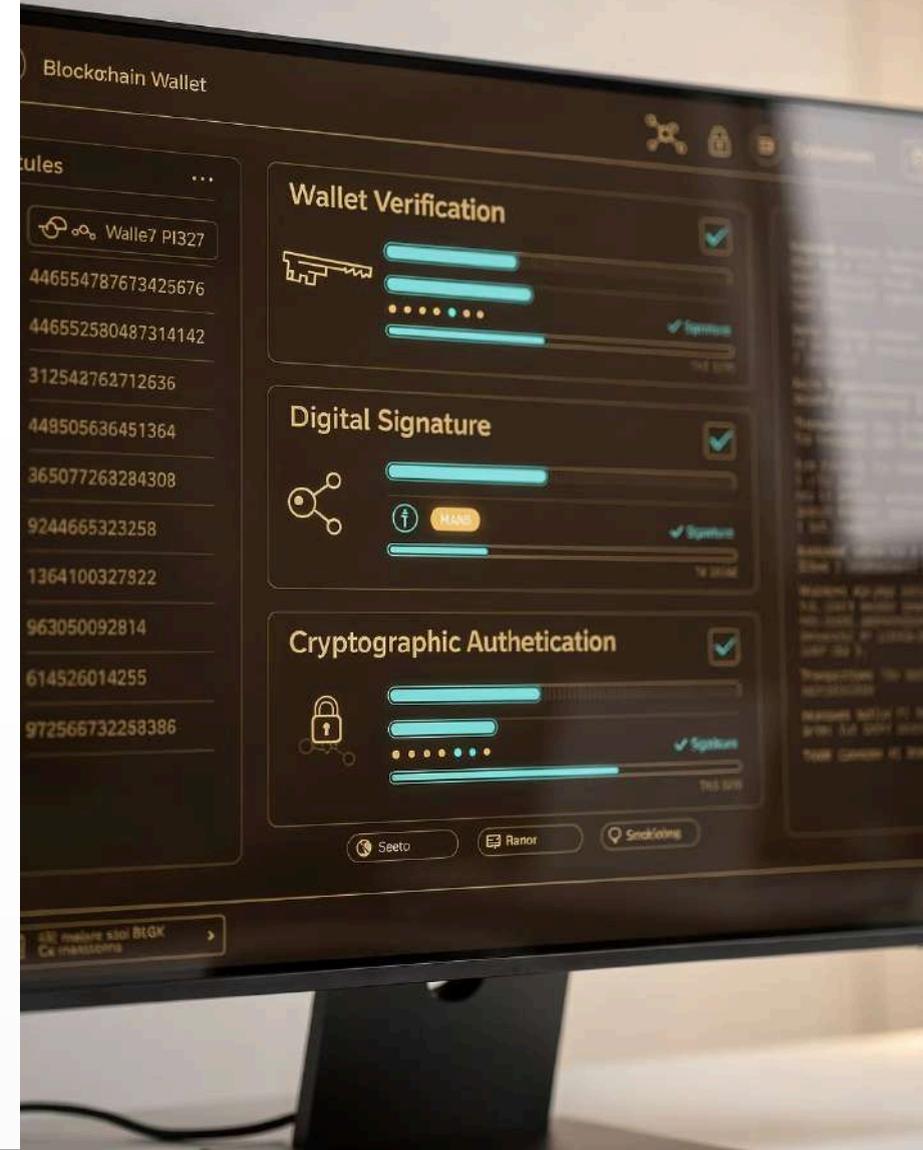
Conduct Due Diligence

To assess ML/TF risks based on wallet type

02

Verify Ownership

Confirm customer owns or controls wallet via micropayment test, message signing, or documentary evidence



Custodial Wallet Due Diligence

For wallets provided by custodial wallet providers or self-hosted wallets used by financial institutions/VASPs, issuer must conduct CDD on custodial wallet provider or self-hosted wallet owner

Business Understanding

Collect information to understand nature of their business

Reputation Assessment

Assess reputation and quality of AML/CFT regulation in operating jurisdictions

Controls Evaluation

Evaluate adequacy and effectiveness of AML/CFT controls

Due diligence extent determined using risk-based approach; not repeated for every transfer unless ML/TF suspicion arises

Paragraphs 4.37 and 4.38 of AML/CFT Guideline



Unhosted Wallet Requirements

Screening Obligation

Screen wallet address to identify transactions associated with:

- Illicit or suspicious activities
- Suspicious sources
- Designated parties

Enhanced Controls

If higher ML/TF risk identified, before issuing or redeeming Specified Stablecoins, must implement additional controls such as:

- Enhanced monitoring of stablecoin transfers with unhosted wallet
- Transaction limits

Paragraph 4.39 AML/CFT Guideline

Ongoing Monitoring Requirements

Ongoing CDD

Review customer documents, data and information to ensure they remain up-to-date and relevant

Transaction Monitoring

Scrutinise transactions for compatibility with customer's business, risk profile and source of funds

Red Flag Detection

Identify complex, unusually large, or unusual pattern transactions and those lacking apparent economic or lawful purpose

Paragraphs 5.1 to 5.3 AML/CFT



Transaction Monitoring Systems

Licensed issuers must implement effective risk-based transaction monitoring on issue & redemption of Stablecoins including:



Blockchain Analytics

Tools to screen transfers and track transaction history



Transfer Tracking

Detect destination on issuance and source on redemption



Illicit Activity Detection

Identify wallet addresses linked to illicit or suspicious activities



Additional Data Monitoring

Monitor IP addresses, geo-location, device IDs and metadata

Paragraph 5.4 AML/CFT Guideline

Technology Due Diligence

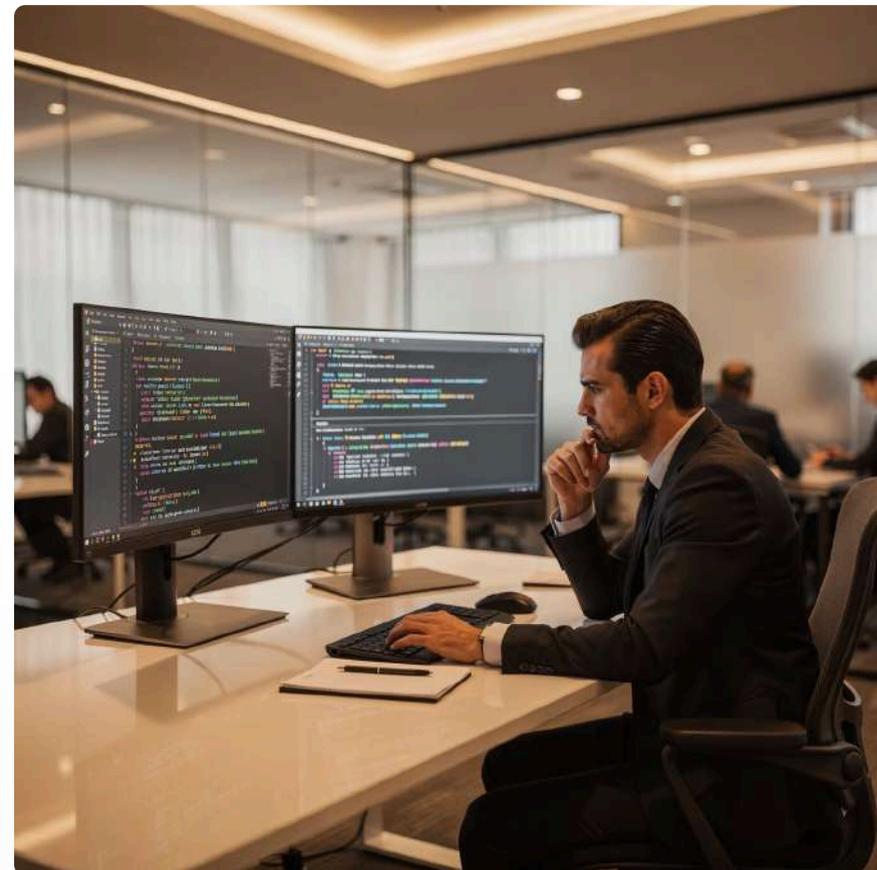
Issuer Responsibility

Licensed issuers remain fully responsible for AML/CFT compliance when using third-party technology solutions

Must conduct thorough due diligence on:

- Solution's effectiveness
- Data quality (coverage, accuracy, reliability)
- Limitations and constraints

Paragraph 5.5 AML/CFT Guideline





Monitoring Stablecoins in Circulation

Licensed issuers must implement ongoing monitoring to prevent stablecoins in circulation from being used for illicit purposes:

- Blockchain Analytics**
Screen stablecoin transactions and wallet addresses beyond initial distribution
- Blacklisting**
Blacklist wallet addresses identified as sanctioned or linked to illicit activities
- Freezing Capability**
Freeze stablecoins if requested by regulator, law enforcement or court order

Paragraph 5.9 AML/CFT Guideline

Peer-to-Peer Transfer Requirements Between Unhosted Wallets

Cautious Approach Required

Unless issuer proves to HKMA's satisfaction that risk-mitigating measures effectively prevent ML/TF, the issuer must:

Verify identity of each stablecoin holder even without customer relationship

Paragraph 5.11 AML/CFT Guideline

Alternative

Stablecoin holder's identity can be verified by:

- Regulated financial institution
- VASP
- Reliable third party

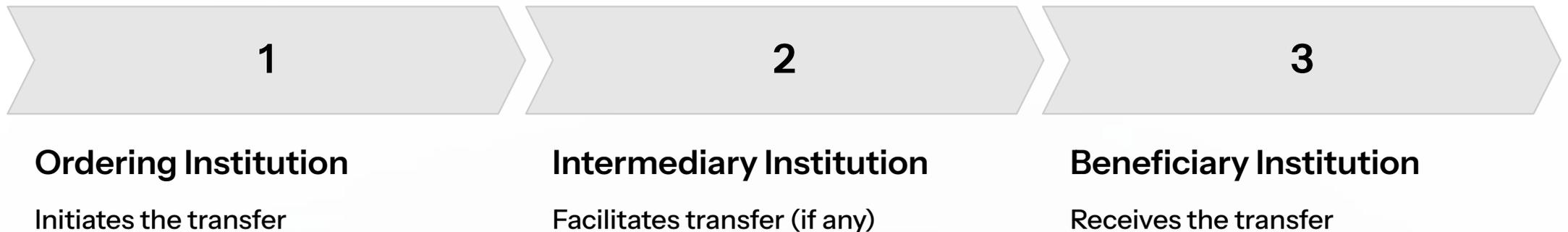


Travel Rule Compliance

Chapter 6 of AML/CFT Guideline

What is a Stablecoin Transfer?

A transfer of Specified Stablecoin by an "ordering institution" on behalf of an "originator" to a "recipient" at a "beneficiary institution", whether or not "intermediary institutions" are involved





Ordering Institution Obligations

01

Obtain Information

Name, account/wallet address or unique reference number of originator and recipient

02

Additional Data (\geq HK\$8,000)

Originator's address, customer ID number or ID number, date and place of birth (individuals)

03

Verify Identity (\geq HK\$8,000)

Verify originator's identity and ensure accuracy of required information

04

Submit Information

Submit required information to beneficiary institution before or simultaneously with transfer

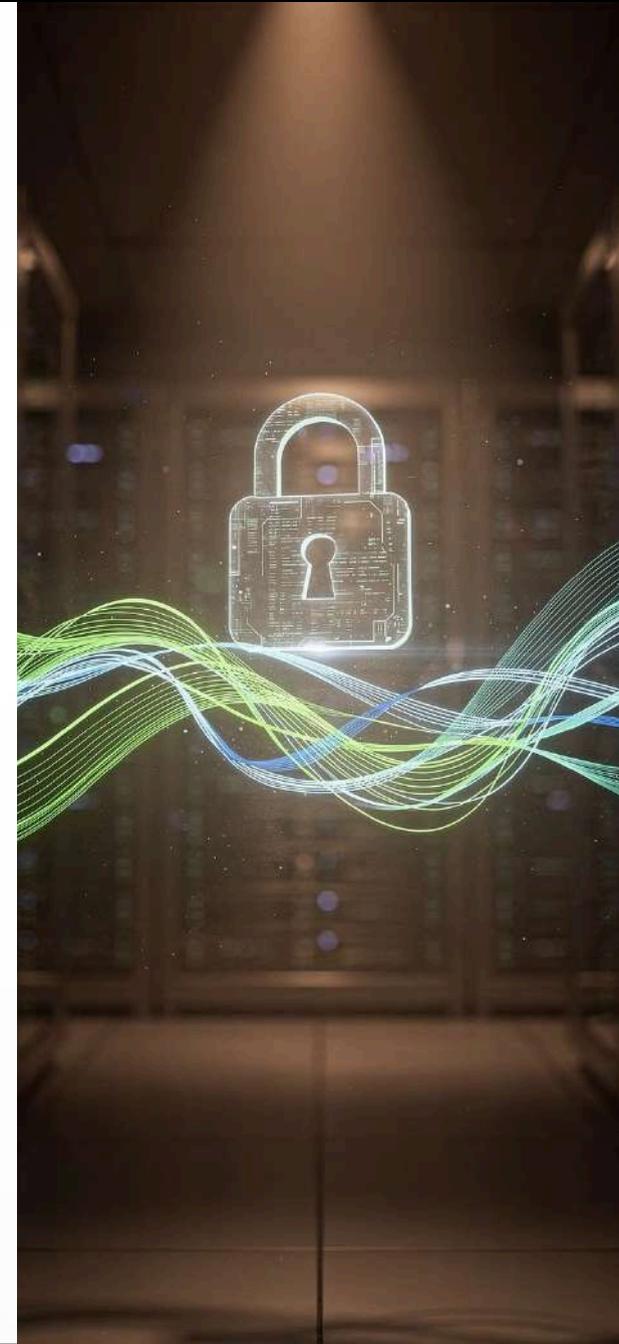
Secure Information Transfer

Security Requirements

- Ensure information integrity
- Protect from unauthorised disclosure
- Can be sent directly or indirectly
- Need not be attached to transfer itself

Safeguards

- Formal agreements with counterparties
- Strong encryption during transmission
- Robust information security controls
- Counterparty due diligence on beneficiary or intermediary institution to ensure they can protect information



Intermediary Institution Duties



Retain Information

Retain all originator and recipient information



Transmit Complete Dataset

Transmit complete dataset intact to next institution



Secure Submission

Ensure immediate, secure submission of required information to intermediary or beneficiary institution



Beneficiary Institution Requirements

- Obtain & Record Information**
Obtain and record all required originator and recipient information
- Counterparty Due Diligence**
Conduct counterparty due diligence on ordering institution and intermediary institutions
- Verify Recipient (\geq HK\$8,000)**
Verify recipient's identity if not previously verified by CDD process
- Cross-Check Information**
Cross-check recipient's name and account number; take risk mitigation measures if discrepancies found

Handling Non-Compliant Transfers

Beneficiary and intermediary institutions must establish procedures to identify and handle transfers without required information:

Monitoring Measures

Detect non-compliant transfers with missing information

Risk-Based Protocols

Determine whether to execute, suspend, or return transfers with missing data

Obtain Missing Information

Take steps to obtain information from sending institution

Relationship Actions

Restrict or terminate relationship with non-compliant institutions or mitigate ML/TF risks

Technology Solutions for Travel Rule

Licensed issuers remain ultimately responsible for compliance when using technological solutions

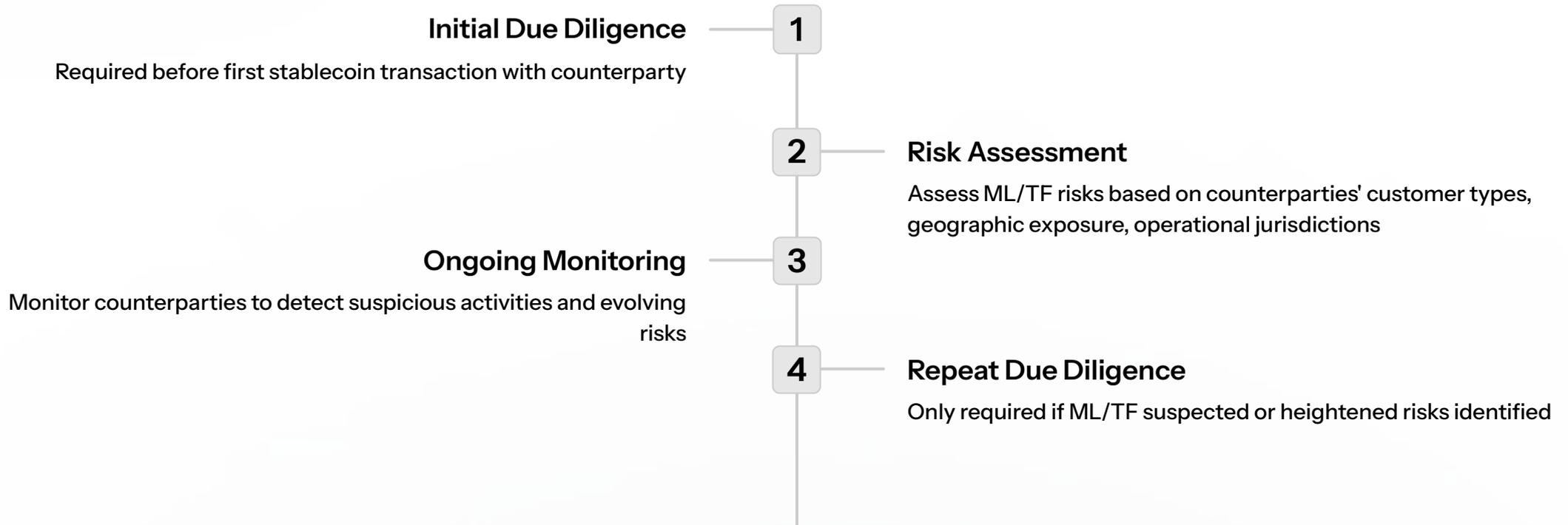
Due diligence must confirm solution can:

- Identify stablecoin transfer counterparties (i.e., ordering, intermediary or beneficiary institutions)
- Submit required information immediately and securely
- Receive required information
- Detect incomplete or missing information
- Support suspicious transaction monitoring and sanctions compliance
- Facilitate counterparty due diligence and record-keeping



Stablecoin Transfer Counterparty Due Diligence

"**Stablecoin Transfer Counterparty**" = An institutional counterparty (i.e. the ordering or beneficiary institution or an intermediary institution) that is the counterparty in a stablecoin transfer





Counterparty Due Diligence Exercise

Identify Counterparty

Determine if transaction involves Stablecoin Transfer Counterparty (i.e. institutional counterparty) or unhosted wallet; verify Stablecoin Transfer Counterparty's identity using reliable sources

Understand Business

Collect information on Stablecoin Transfer Counterparty's nature of business; analyse transaction characteristics and volumes

Assess Regulation

Assess reputation and quality of AML/CFT regulation and supervision

Evaluate Controls

Evaluate sufficiency of Stablecoin Transfer Counterparty's AML/CFT controls

Obtain senior management approval

Counterparty's Travel Rule Compliance

Licensed Stablecoin Issuers must conduct due diligence to ensure Stablecoin Transfer Counterparties can meet Travel Rule requirements:

Travel Rule Capability

Assess the counterparty's ability to comply with Travel Rule obligations

Jurisdictional Comparability

Verify if the counterparty operates under comparable Travel Rule requirements in its jurisdiction

Effective AML/CFT Controls

Evaluate the counterparty's AML/CFT controls for their effectiveness in ensuring Travel Rule compliance

Data Privacy & Security

Confirm the counterparty's data privacy and security controls adequately protect originator and recipient information

Higher Risk Counterparty Indicators



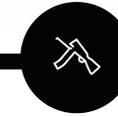
High-Risk Jurisdiction

Operates or incorporated in jurisdiction with weak AML/CFT regulation



Unregulated Entity

Not subject to AML/CFT regulation and supervision



Inadequate Systems

Failure to maintain adequate AML/CFT systems for Travel Rule compliance



Insufficient Data Protection

Failure to implement sufficient data protection safeguards



Illicit Associations

Associations with ML/TF or other illicit activities

Managing Counterparty ML/TF Risks

01

Evaluate Impact

Assess potential impact of identified risks on operations

02

Implement Measures

Enhanced due diligence, closer monitoring, transaction limits

03

Assess Relationship

Continuously evaluate whether to maintain, restrict or terminate relationship

04

Prohibition

Refrain from transfers if risks cannot be mitigated; never deal with shell VASPs or shell financial institutions



Unhosted Wallet Transfers

Enhanced controls required for transfers to/from unhosted wallets

To Unhosted Wallet

Required information:

- Originator's name, account/unique reference number
- Originator's address, customer ID number, date/place of birth
- Recipient's name and wallet address

From Unhosted Wallet

Required information:

- Originator's name, wallet address
- Originator's address, customer ID number, date/place of birth
- Recipient's name, account/unique reference number

Originator's address, ID number, date/place of birth **not** required for transfers of < HK\$8,000



Terrorist Financing & Sanctions

Licensed stablecoin issuers must implement controls to comply with legal/regulatory requirements on terrorist financing, financial sanctions and proliferation financing including staff training and maintaining comprehensive database (Chapter 7 AML/CFT Guideline)

- Database Requirements

Database Contents

Hong Kong Gazette lists, CEDB website, UN Security Council Resolutions, sanctions lists, HKMA-specified lists

Maintenance

Promptly update when changes occur; ensure readily accessible to relevant staff

Third-Party Services

Can subscribe to third-party database but must ensure completeness and accuracy via periodic testing

Delegation

Can delegate to overseas office but ultimate responsibility remains with issuer

Screening Mechanism

Licensed issuers must implement effective screening to prevent relationships or transactions with:

- Terrorist suspects and designated persons/entities
- Anyone acting on their behalf or at their direction
- Entities owned or controlled by prohibited parties

Screening required irrespective of customer's risk profile



When to Screen

Stablecoin Issuance & Redemption

Screen customers and beneficial owners against current database

1

2

3

4

Before Transfers

Screen parties to stablecoin transfer before execution

New Designations

Screen against new or updated designations as soon as practicable

Incoming Transfers

Implement risk-mitigation measures if prior screening not completed

Handling Screening Hits

Enhanced Investigation

When possible name matches identified:

- Conduct enhanced investigation to confirm genuine hits
- Document all relevant records and results
- Report any suspicions to JFIU



Suspicious Transaction Reporting: Ch. 8 AML/CFT Guideline

Statutory obligation to file suspicious transaction report (STR) with Joint Financial Intelligence Unit if knowledge or suspicion that property:

Proceeds of Crime

Represents proceeds of drug trafficking or indictable offence

Used in Offences

Was used or intended for use in connection with offences

Terrorist Property

Constitutes terrorist property

Failure to report: Maximum 3 months' imprisonment and HK\$50,000 fine



Tipping Off Prohibition

Criminal Offence

Revealing information that might prejudice an investigation (including internal suspicions not yet reported) constitutes "tipping off"

Strictly prohibited: Notifying customer of STR filing

Permitted: Legitimate customer enquiries made in good faith (to extent they don't tip off customer)



STR System Requirements



MLRO Appointment

Main point of contact for internal reporting and JFIU communications



Policies & Procedures

Internal reporting, JFIU reporting, post-reporting risk mitigation, preventing tipping-off



Staff Guidance

Detecting suspicious circumstances and recognising ML/TF indicators



Ongoing Monitoring

Ensure systems meet regulatory requirements and remain effective



Post-STR Actions

01

File Report Promptly

File with supporting information as soon as reasonably practicable; ensure high quality incorporating JFIU and HKMA feedback

02

Review Relationship

Conduct immediate review of relevant business relationship

03

Implement Measures

Implement risk-mitigating measures (e.g., freeze stablecoins if required by law enforcement)

04

Continue or Terminate

Only continue relationship if adequate risk mitigation and controls in place; escalate to senior management if necessary

Record-Keeping Obligations: Ch. 9 AML/CFT Guideline

Licensed issuers must maintain comprehensive records to assist in investigation/prosecution and demonstrate regulatory compliance

5

Years Minimum

Retention period after transaction completion or business relationship ends

100%

Audit Trail

Clear and complete audit trail for all funds handled



Records to be Kept

CDD Documents
Originals or copies of documents and records from customer identification, verification, beneficial owner identification, ongoing CDD

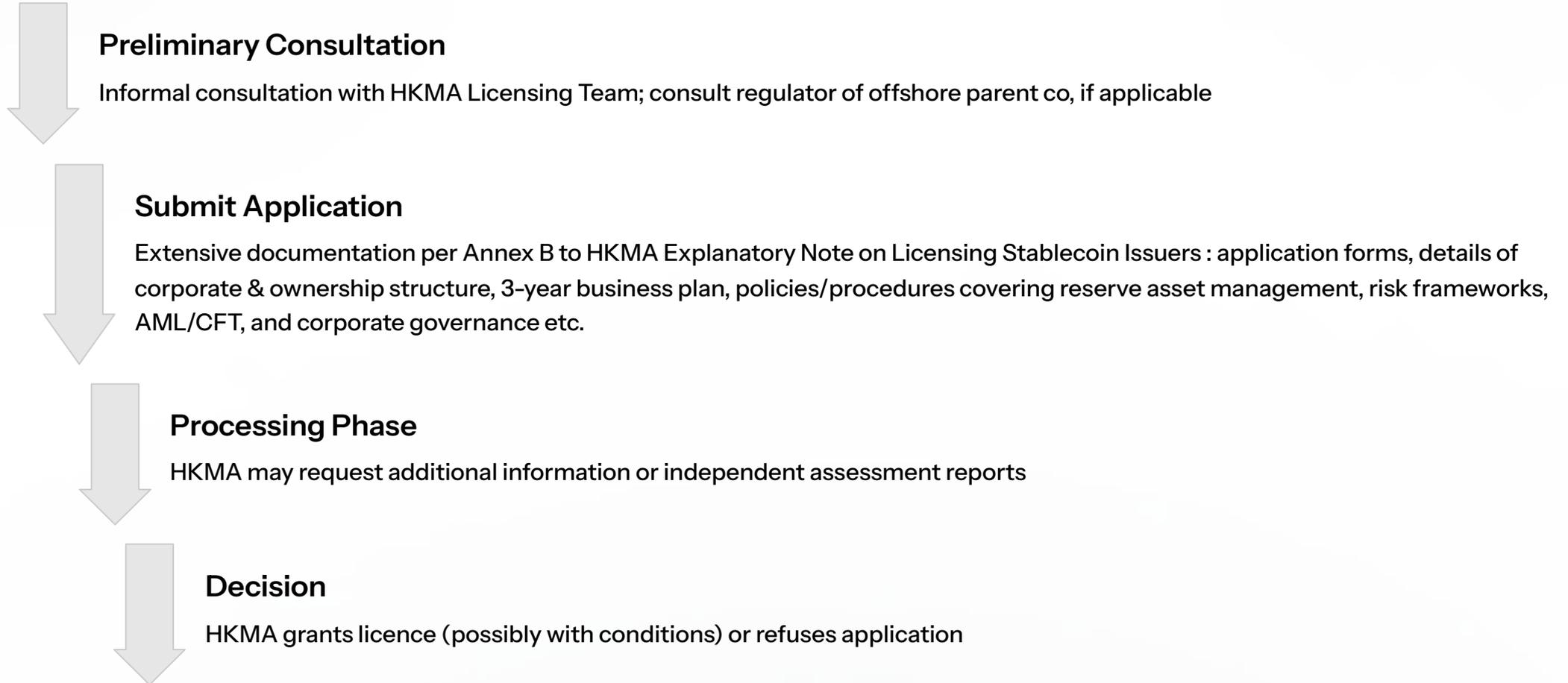
Business Relationship Records
Purpose and nature of relationship; account documents; business correspondence

Analysis Results
Results of enquiries into transactions that are complex, unusually large, have unusual pattern, or lack apparent economical/lawful purpose

Travel Rule Information
Required originator and recipient information obtained or received in complying with Travel Rule and, for transfers to/from customers' unhosted wallets, the originator and recipient information required by paragraph 6.41 AML/CFT Guideline

STR Registers
Register of reports to MLRO and register of STRs filed with JFIU

Licensing Application Steps



Post-Licence Grant

Formal Notice

HKMA provides written notice with:

- Assigned licence number
- Official effective date

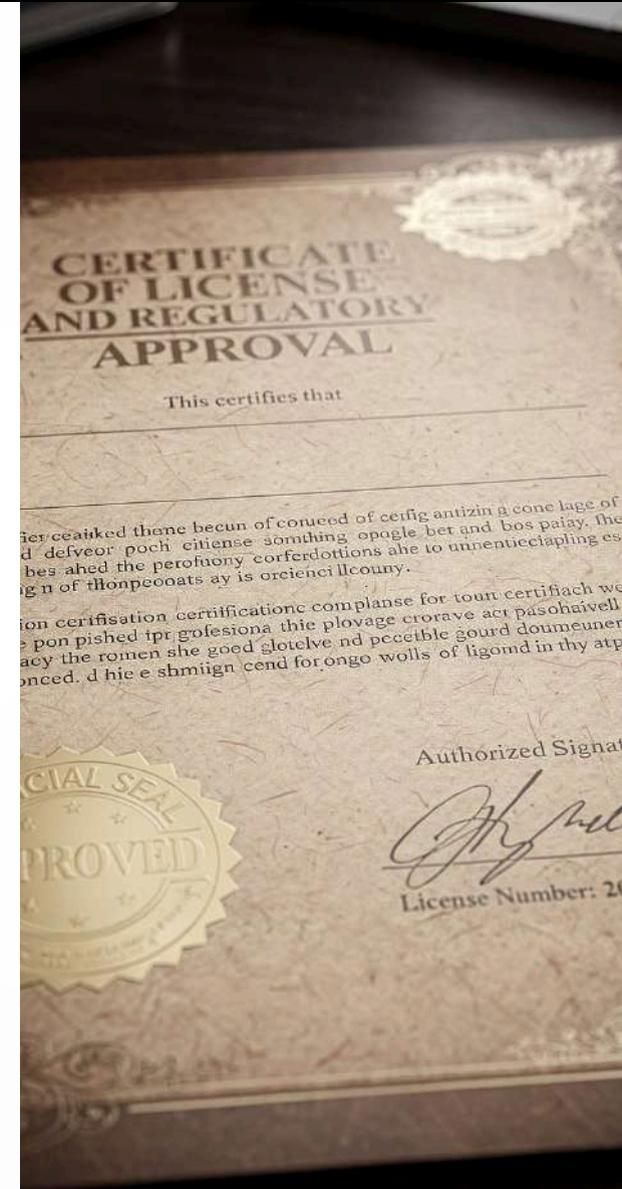
Licence remains in force until revoked

Public Register

HKMA updates official register of licensed stablecoin issuers on website

Makes licensed status publicly verifiable

- 📄 **Important:** Entities must not describe themselves as applicants or behave as such until formal application submitted (offence under section 154)



Offering Restrictions: Section 9 Stablecoins Ordinance

Only Specified Stablecoins issued by HKMA-licensed issuers can be offered to Hong Kong public, and only by "Permitted Offerors":

Licensed Stablecoin Issuer

Can offer own or another licensed issuer's Specified Stablecoins

SFC-Licensed VATP

Virtual asset trading platforms licensed under AMLO

SVF Licensee

Stored-value facility licensed under Payment Systems & Stored Value Facilities Ordinance

Type 1 Licensed Corporation

SFC-licensed corporation with Type 1 (dealing in securities) licence

Authorized Institution

HKMA-authorized institution (e.g., a bank)

Offering Restrictions

Meaning of Offering: s. 6 Stablecoins Ordinance

Making a communication in any form to another person that provides sufficient information as to:

- the Specified Stablecoin being offered
- the terms and conditions on which it is offered, and
- the channels through which it is offered,

for them to decide whether to acquire the Specified Stablecoin

Specified Stablecoins of Unlicensed Issuers - "professionals exemption"

Permitted Offerors can offer unlicensed issuers' Specified Stablecoins only to **professional investors** (as defined in Schedule 1 to SFO) if:

- Not issued in Hong Kong
- If issued outside Hong Kong, do **not** reference HK dollar

Stablecoins Ordinance (Specification of Persons for Section 9(2)(b)(iii)) Notice

Penalties for Contravention of s. 9 Stablecoins Ordinance:

HK\$5 million fine, 7 years' imprisonment, HK\$100,000 daily fine for continuing offence

Designated Stablecoin Entities: s. 101 Stablecoins Ordinance

HKMA can designate an overseas entity as a "designated stablecoin entity"



Scope of Designation

Applies to overseas entities issuing non-HK\$ Specified Stablecoins outside Hong Kong OR providing services to any stablecoin payment system wherever located



Criteria for Designation

The entity's activities are, or are likely to become, material to Hong Kong's monetary/financial stability, its role as an international financial centre, or matters of significant public interest exist



Key Requirements (s. 107)

Designated entities must have operating rules compliant with HKMA regulations, ensure operations comply with the Ordinance, and manage potential insolvency. They must also maintain adequate financial resources and systems for reserve management, disclosures, and risk management



Consequences of Non-Compliance

Failure to comply with Section 107 requirements constitutes an offence, carrying a maximum fine of HK\$400,000

Other Offences Under Stablecoins Ordinance

Advertising Offence (s.10)



Publishing advertisement holding a person out as:

- carrying on a Regulated Stablecoin Activity if person is not licensed or exempt from licensing requirement; or
- offering Specified Stablecoins, unless person is permitted to do so under section 9
- **Penalty:** 6 months' imprisonment, HK\$50,000 fine

Fraudulent or Deceptive Conduct in Specified Stablecoin Transactions (s.11)



Offence to, directly or indirectly, in transaction involving a Specified Stablecoin, either:

- employ any device, scheme, or artifice with intent to defraud or deceive, or
- engage in any act, practice, or course of business that is fraudulent or deceptive, or that would operate as a fraud or deception
- **Penalty:** HK\$10 million fine, 10 years' imprisonment, up to 5-year prohibition on involvement in Specified Stablecoin transactions

Misrepresentation (s.12)



Fraudulent or reckless misrepresentation to induce others to enter agreement to acquire, dispose of, subscribe for, or underwrite Specified Stablecoins

Penalty: 7 years' imprisonment, HK\$1 million fine

Other Offences Under Stablecoins Ordinance (continued)



False Claims (s.154, s.155)

Falsely claiming, holding out, or acting in a manner that indicates, that the person is a licence applicant or licensed issuer

Penalty: HK\$400,000 fine, 2 years' imprisonment, HK\$10,000 daily fine



False Information (s.149)

Providing false or misleading information to HKMA if person knows, or ought reasonably to know, that information is false or misleading (including by omission of material information)

Penalty: HK\$1 million, 2 years' imprisonment

HKMA's Power to Revoke Licence

HKMA can revoke a stablecoin issuer's licence on grounds specified in

Schedule 4 to the Stablecoins Ordinance including:

1

Non-Compliance with Minimum Criteria in Schedule 2 to the Ordinance

2

Breach of Licence Condition

3

Insolvency or Creditor Arrangements

Entering into arrangements with creditors, or facing insolvency, winding up, or dissolution

4

Notification of Financial Distress

Notifying HKMA of impending inability to meet obligations, insolvency, payment suspension, or business cessation

5

Actual Financial Instability

Actual inability to fulfil obligations or suspension of payments or licensed activities

6

Failure to Provide Material Information

Failing to provide the HKMA with information required under Ordinance material to the licensed issuer or its business methods

7

False or Misleading Information

Providing false, misleading, or inaccurate information to HKMA at any stage

8

Cessation of Business Activities

Ceasing licensed stablecoin business activities

9

Non-Payment of Licence Fees