Annex to Consultation Paper

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

May 2025
(For Consultation)

Contents

1. Introduction

1.1. This Guideline is issued by the Hong Kong Monetary Authority (HKMA) under section 171 of the Stablecoins Ordinance, Cap. [-] and section 7 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (AMLO) for a stablecoin issuer which holds a licence granted under section 15 of the Stablecoins Ordinance (hereafter referred as "licensee"). A licensee is a financial institution (FI) as defined in Part 2 of Schedule 1 to the AMLO.

1.2. This Guideline provides guidance to assist a licensee to understand the money laundering and terrorist financing (ML/TF) risks associated with the regulated stablecoin activities [1] and sets out the relevant anti-money laundering and counter-financing of terrorism (AML/CFT) regulatory requirements for the licensee to address such risks. A licensee should meet these requirements in order to comply with the statutory requirements under the Stablecoins Ordinance and the AMLO.

1.3. This Guideline is intended for use by licensees, their officers and staff, taking into account the specific characteristics of the issuance, redemption and other related activities of stablecoins. Given significant differences that may exist in the organisational and legal structures of different licensees, as well as the nature and scope of their business models, the flexible approach adopted in this Guideline is a reflection of the fact that there exists no single set of universally applicable implementation measures.

1.4. Compliance with this Guideline is enforced through the Stablecoins Ordinance and the AMLO. A licensee who fails to comply with this Guideline may be subject to disciplinary or other actions under the Stablecoins Ordinance and/or the AMLO (if applicable). The HKMA is empowered to exercise various provisions under the Stablecoins Ordinance and/or the AMLO in case of non-compliance with the requirements set out in this Guideline.

1.5. Section 10 of Schedule 2 to the Stablecoins Ordinance requires a licensee to have in place and implement adequate and appropriate systems of control: (i) for preventing and combating possible ML/TF in connection with its licensed stablecoin activities; and (ii) to ensure compliance with applicable provisions of the AMLO, and any measure promulgated by the Monetary Authority (MA) in the form of rules, regulations, guidelines or otherwise, to prevent, combat or detect ML/TF. A failure to comply with any provision of this Guideline may reflect adversely on whether a licensee continues to comply with such minimum criterion.

[1] See section 5 of the Stablecoins Ordinance.

1.6. The minimum criteria set out in Schedule 2 of the Stablecoins Ordinance, and other requirements promulgated by the MA in the form of rules, regulations, guidelines or other communications apply when a licensee is granted a license and continue to apply throughout the licensee's conduct of licensed stablecoin activities. Certain requirements, particularly the record-keeping requirements under the AMLO, will continue to apply for a specified period (at least 5 years for record-keeping) after the relevant activities have taken place. In the event of licence revocation, the licensee is required to comply with these requirements for the period stipulated under applicable laws and regulations. The licensee should have in place adequate and appropriate arrangements to ensure that any time specific requirements are met. The MA reserves the right not to revoke any licence unless such arrangements are in place to the satisfaction of the HKMA.

1.7. This Guideline should be read in conjunction with the Stablecoins Ordinance, the AMLO and any rules, regulations or guidelines issued by the HKMA that are relevant to the operations of the licensee.

1.8. Terms that are not defined in this Guideline should be interpreted in accordance with the definitions provided under the Stablecoins Ordinance and the Guideline on Supervision of Licensed Stablecoin Issuers.

1.9. For the avoidance of doubt, the use of the word "must" or "should" in relation to an action, consideration or measure referred to in this Guideline indicates that it is a mandatory requirement. The content of this Guideline is not intended to be an exhaustive list of the means to meet the statutory and regulatory requirements. A licensee should therefore use this Guideline as a basis to develop measures appropriate to its structure and business activities.

2. Risk assessment

2.1. A licensee should adopt a risk-based approach (RBA) in the design and implementation of its AML/CFT policies, procedures and controls (hereafter collectively referred to as "AML/CFT Systems"). The licensee should identify, assess and understand the ML/TF risks to which it is exposed in respect of its specific stablecoin business, and take AML/CFT measures commensurate with those risks in order to manage and mitigate them effectively.

2.2. A licensee should conduct an institutional ML/TF risk assessment to identify, assess and understand its ML/TF risks taking into consideration a number of factors including but not limited to (i) customer risk factors, (ii) country risk factors, (iii) product, service or transaction risk factors and (d) delivery channel risk factors. The institutional ML/TF risk assessment forms the basis of the RBA, enabling the licensee to understand how and to what extent it is vulnerable to ML/TF.

2.3. In undertaking an institutional ML/TF risk assessment, a licensee should ensure that:

(a) the risk assessment process is appropriately structured and properly documented, covering the identification and assessment of relevant risks and supported by qualitative and quantitative analysis;

(b) the risk assessment has taken into account all the relevant risk factors before determining what the level of overall risk is and the appropriate level and type of mitigation to be applied;

(c) the approval of senior management is obtained for the assessment results;

(d) a process is in place by which the risk assessment is kept up-to-date; and

(e) appropriate mechanisms are in place to provide its risk assessment to the HKMA when required to do so.

2.4. The scale and scope of the institutional ML/TF risk assessment should be commensurate with the nature, size and complexity of a licensee's business. It should also consider risks identified in other relevant risk assessments which may be published from time to time, such as Hong Kong's jurisdiction-wide ML/TF risk assessment, as well as other higher risks notified to the licensee by the HKMA, the Joint Financial Intelligence Unit (JFIU) or other law enforcement agencies.

2.5. A licensee should identify and assess the ML/TF risks that may arise in relation to: (a) the development of new products and new business practices, including new delivery mechanisms; and (b) the use of new or developing technologies for both new and pre-existing products. The licensee should undertake the risk assessment prior to the launch of the new products, new business practices, or the use of new or developing technologies, and should take appropriate measures to manage and mitigate the risks identified.

3. AML/CFT Systems

3.1. A licensee should:

(a) have AML/CFT Systems, which are approved by senior management, to enable the licensee to effectively manage and mitigate the risks relevant to the licensee;

(b) monitor the implementation of those AML/CFT Systems referred to in (a), and to enhance them if necessary; and

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

3.2. The nature, scale and complexity of AML/CFT Systems may be simplified provided that:

(a) a licensee complies with the statutory requirements set out in Schedule 2 of the AMLO and the requirements set out in paragraphs 2.2, 2.3 and 3.1;

(b) the lower ML/TF risks which form the basis for doing so have been identified through an appropriate risk assessment (e.g. institutional ML/TF risk assessment); and

(c) the simplified AML/CFT Systems, approved by senior management, are subject to review from time to time. However, AML/CFT Systems are not permitted to be simplified whenever there is a suspicion of ML/TF.

3.3. A licensee should implement AML/CFT Systems having regard to the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses. The AML/CFT Systems should include:

(a) compliance management arrangements;

(b) an independent audit function;

(c) employee screening procedures; and

(d) an ongoing employee training programme.

Compliance management arrangements

3.4. A licensee should have appropriate compliance management arrangements that facilitate the licensee to implement AML/CFT Systems to comply with relevant legal and regulatory obligations and manage ML/TF risks effectively. Compliance management arrangements should, at a minimum, include oversight by the licensee's senior management, and appointment of a Compliance Officer (CO) and a Money Laundering Reporting Officer (MLRO)[2].

3.5. Effective ML/TF risk management requires adequate governance arrangements. The board of directors or its delegated committee (where applicable), and senior management of a licensee should have a clear understanding of its ML/TF risks and ensure that the risks are adequately managed. The senior management of the licensee should appoint a CO at the management level to have the overall responsibility for the establishment and maintenance of its AML/CFT Systems; and a sufficiently senior person as the MLRO to act as the central reference point for suspicious transaction reporting and the main point of contact with JFIU and law enforcement agencies. The CO and MLRO should be individuals with sufficient expertise and be provided with adequate resources for discharging their responsibilities.

Independent audit function

3.6. A licensee should establish an independent audit function which should have a direct line of communication to the senior management and the board of directors of the licensee. The function should have sufficient expertise and resources to enable it to carry out its responsibilities, including undertaking independent reviews of the licensee's AML/CFT Systems to ensure effectiveness.

Employee screening

3.7. A licensee should have adequate and appropriate screening procedures in order to ensure that only employees with high integrity are deployed to perform AML/CFT roles.

Ongoing employee training programme

3.8. Ongoing staff training is an important element of an effective system to prevent and detect ML/TF activities. A licensee should provide adequate training for its staff so that they have the necessary capability and are adequately trained to implement its AML/CFT Systems. The scope and frequency of training should be tailored according to the job functions, responsibilities and the level of experience of the staff of the licensee.

---

[2] Depending on the size of a licensee, the functions of CO and MLRO may be performed by the same person.

Group-wide AML/CFT Systems

3.9. Subject to paragraphs 3.12 and 3.13, a licensee with branches or subsidiary undertakings outside Hong Kong[3] that carry on the same business as an FI as defined in the AMLO should implement group-wide AML/CFT Systems to apply the requirements set out in this Guideline to all of these branches and subsidiary undertakings, where the requirements in this Guideline are relevant and applicable.

3.10. In particular, a licensee should, through its group-wide AML/CFT Systems, ensure that all of its branches and subsidiary undertakings outside Hong Kong that carry on the same business as an FI as defined in the AMLO, have procedures in place to ensure compliance with the CDD and record-keeping requirements similar to those imposed under Parts 2 and 3 of Schedule 2 to the AMLO, to the extent permitted by the laws and regulations of the jurisdictions where the branches or subsidiary undertakings operate.

3.11. To the extent permitted by the laws and regulations of the jurisdictions involved and subject to adequate safeguards on the protection of confidentiality and use of information being shared, including safeguards to prevent tipping off, a licensee should also implement measures, through its group-wide AML/CFT Systems, for:

(a) sharing information required for the purposes of CDD and ML/TF risk management; and

(b) provision to the licensee's group-level compliance, audit and/or AML/CFT functions, of customer, account, and transaction information from its branches and subsidiary undertakings outside Hong Kong that carry on the same business as an FI as defined in the AMLO, when necessary for AML/CFT purposes[4].

3.12. If the AML/CFT requirements in the jurisdiction where the branch or subsidiary undertaking of a licensee is located (host jurisdiction) differ from those relevant requirements referred to in paragraph 3.9, the licensee should require that branch or subsidiary undertaking to apply the higher of the two sets of requirements, to the extent that the host jurisdiction's laws and regulations permit.

3.13. If the host jurisdiction's laws and regulations do not permit the branch or subsidiary undertaking of a licensee to apply the higher AML/CFT requirements,

---

[3] A licensee should contact the HKMA at an early stage to discuss its intention to establish a branch or subsidiary undertakings outside Hong Kong.

[4] This should include information and analysis of transactions or activities which appear unusual (if such analysis is done); and may include a suspicious transaction report, its underlying information, or the fact that a suspicious transaction report has been submitted. Similarly, branches and subsidiary undertakings should receive such information from the group-level functions when relevant and appropriate to risk management.

particularly the CDD and record-keeping requirements imposed under Parts 2 and 3 of Schedule 2 to the AMLO, the licensee should:

(a) inform the HKMA of such a situation; and

(b) take additional measures to effectively mitigate ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the requirements.

4. Customer due diligence

4.1. The term "stablecoin holder" in this Guideline refers to a person who has possession of the specified stablecoin issued by a licensee. A person should be treated as a customer of the licensee if (i) a business relationship[5] has been established between the person and the licensee; or (ii) the licensee carries out an occasional transaction[6] for a person (both (i) and (ii) hereafter referred to as "customer" or "customer stablecoin holders"). Other stablecoin holders that are not the licensee's customers are referred to as "non-customer stablecoin holders".

4.2. A licensee should apply an RBA when conducting customer due diligence (CDD) measures so that the extent of CDD measures is commensurate with the ML/TF risks associated with its customers (see paragraph 4.18).

What CDD measures should be applied

4.3. The following are CDD measures applicable to a licensee:

(a) identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source[7];

(b) where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity;

(c) obtain information on the purpose and intended nature of the business relationship (if any) established with the licensee unless the purpose and intended nature are obvious; and

(d) if a person purports to act on behalf of the customer:
   (i) identify the person and take reasonable measures to verify the person's identity using documents, data or information provided by a reliable and independent source; and
   (ii) verify the person's authority to act on behalf of the customer.

5 The term "business relationship" is defined in section 1 of Part 1 of Schedule 2 to the AMLO.
6 The term "occasional transaction" is defined in section 1 of Part 1 of Schedule 2 to the AMLO.
7 The list of reliable and independent source is outlined in section 2, Part 2 of Schedule 2 to the AMLO.

When CDD measures should be carried out

4.4. A licensee should carry out CDD measures in the following circumstances:

(a) before establishing a business relationship with a customer;

(b) before carrying out an occasional transaction (e.g. issuance and redemption of stablecoin) involving an amount equal to or above $8,000 for a customer;

(c) when the licensee suspects that the customer or the customer's account is involved in ML/TF; or

(d) when the licensee doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

4.5. A licensee may, exceptionally, verify the identity of a customer and any beneficial owner of the customer after establishing the business relationship, provided that:

(a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed;

(b) it is necessary not to interrupt the normal conduct of business with the customer; and

(c) verification is completed as soon as reasonably practicable.

Identification and verification of identity – customer

4.6. A licensee should identify the customer and verify the customer's identity by reference to documents, data or information provided by a reliable and independent source[8].

4.7. As part of the CDD, a licensee should identify the customer by obtaining at least the following identification information:

(a) For a customer that is a natural person:
  (i) full name;
  (ii) date of birth;
  (iii) nationality;
  (iv) residential address; and
  (v) unique identification number (e.g. identity card number or passport number) and document type.

[8] For the avoidance of doubt, a licensee should not establish business relationships or conduct occasional transactions for customers in fictitious names.

(b) For a customer that is a legal person;
   (i) full name;
   (ii) date of incorporation, establishment or registration;
   (iii) place of incorporation, establishment or registration (including address of registered office);
   (iv) unique identification number (e.g. incorporation number or business registration number) and document type; and
   (v) principal place of business (if different from the address of registered office).

4.8. In verifying the identity of a customer that is a natural person, a licensee should verify the name, date of birth, unique identification number and document type of the customer by reference to documents, data or information provided by a reliable and independent source[9], examples of which include:

(a) Hong Kong identity card or other national identity card;

(b) valid travel document (e.g. unexpired passport); or

(c) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).

4.9. In verifying the identity of a customer that is a legal person, a licensee should normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the legal person by reference to documents, data or information provided by a reliable and independent source, examples of which include[10]:

(a) certificate of incorporation;

(b) record in an independent company registry;

(c) certificate of incumbency;

(d) certificate of good standing;

(e) record of registration;

(f) partnership agreement or deed;

---

[9] The identification document should contain a photograph of the customer. In exceptional circumstances where a licensee is unable to obtain an identification document with a photograph, the licensee may accept an identification document without a photograph if the associated risks have been properly assessed and mitigated.

[10] In some instances, a licensee may need to obtain more than one document to meet this requirement. For example, a certificate of incorporation can only verify the name and legal form of the legal person in most circumstances but cannot act as a proof of current existence.

(g) constitutional document; or

(h) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).

4.10. Where a licensee's business model involves identifying and verifying the identity of a natural person via non-physical / non-face-to-face channels (e.g. through an electronic channel such as mobile applications or internet), a licensee should:

(a) verify the identity of the customer on the basis of data or information provided by a digital identification system that is a reliable and independent source recognised by the HKMA; or

(b) employ appropriate technology solutions to mitigate the risks, particularly for impersonation risks, when identifying and verifying the identity of a natural person customer. The technology solutions adopted by the licensee should cover the following two aspects:
   (i) identity authentication – where the natural person customer's identity is obtained through electronic channels, the licensee should take appropriate technology measures to ensure reliability of the document, data or information obtained for the purpose of verifying the customer's identity; and
   (ii) identity matching – the licensee should use appropriate technology to link the natural person customer incontrovertibly to the identity provided in (i).

4.11. A licensee should obtain additional customer information that enables it to identify, manage and mitigate the ML/TF risks associated with its delivery channels. Such additional customer information may include but not limited to: IP address(es) with an associated time stamp, geo-location data, device identifiers, wallet addresses, transaction hashes and other electronic identifiers.

Connected parties

4.12. Where a customer is a legal person, a licensee should identify all the connected parties[11] of the customer (e.g. a director of the customer that is a corporation) by obtaining their names.

Identification and verification of identity – beneficial owner

[11] For the avoidance of doubt, if a connected party also satisfies the definition of a customer, a beneficial owner of the customer or a person purporting to act on behalf of the customer, a licensee has to identify and verify the identity of that person with reference to relevant requirements set out in this Guideline.

4.13. A beneficial owner refers to the natural person(s) who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. A licensee should identify any beneficial owner in relation to a customer, and take reasonable measures to verify the beneficial owner's identity so that the licensee is satisfied that it knows who the beneficial owner[12] is.

4.14. For a customer that is a legal person, a licensee should identify any natural person who ultimately has a controlling ownership interest (i.e. more than 25%) in the legal person and any natural person exercising control of the legal person or its management, and take reasonable measures to verify their identities. If there is no such natural person, the licensee should identify the relevant natural persons who hold the position of senior managing official, and take reasonable measures to verify their identities.

Ownership and control structure

4.15. Where a customer is not a natural person, a licensee should understand its ownership and control structure, including identification of any intermediate layers (e.g. by reviewing an ownership chart of the customer). The objective is to follow the chain of ownership to the beneficial owners of the customer. Where a customer has a complex ownership or control structure, the licensee should obtain sufficient information for the licensee to satisfy itself that there is a legitimate reason behind the particular structure employed.

Identification and verification of identity – person purporting to act on behalf of the customer (PPTA)

4.16. A licensee should identify and verify the identity of the PPTA in line with the identification and verification requirements for a customer that is a natural person or a legal person, as appropriate. The licensee should also verify the authority of each PPTA by obtaining appropriate documentary evidence (e.g. board resolution or similar written authorisation).

Purpose and intended nature of business relationship

4.17. A licensee should understand the purpose and intended nature of the business relationship. In some instances, this will be self-evident, but in many cases, the licensee may have to obtain information in this regard. The information obtained by the licensee to understand the purpose and intended nature should be commensurate with the risk profile of the customer and the nature of the business relationship. In addition, where a customer is not a natural person, a licensee should also understand the nature of the customer's business.

Risk-based approach to CDD

[12] Beneficial owner in relation to a corporation is defined in section 1, Part 1 of Schedule 2 to the AMLO.

4.18. A licensee should in general carry out all four CDD measures set out in paragraph 4.3 before establishing a business relationship with a customer or before carrying out a specified occasional transaction for a customer. The licensee should determine the extent of the four CDD measures following an RBA. The licensee should apply enhanced due diligence (EDD) measures where the ML/TF risks are high[13]. The licensee may apply simplified due diligence (SDD) measures where low ML/TF risks are identified. The EDD or SDD measures applied should be commensurate with the nature and level of ML/TF risk[14] identified by the licensee which should be supported by an adequate analysis of ML/TF risks.

4.19. SDD measures should not be applied or continue to be applied, where:

(a) a licensee's risk assessment changes and it no longer considers that there is a low degree of ML/TF risk;

(b) where the licensee suspects ML or TF; or

(c) where there are doubts about the veracity or accuracy of documents or information previously obtained for the purposes of identification or verification.

4.20. A licensee should obtain approval from its senior management to establish a business relationship that presents a high ML/TF risk, or continue an existing business relationship where the relationship subsequently presents a high ML/TF risk.

Politically exposed persons (PEPs)

4.21. A licensee should establish and maintain effective procedures for determining whether a customer or a beneficial owner of a customer is a PEP[15].

4.22. Where a customer or a beneficial owner of a customer is a non-Hong Kong PEP[16], a licensee should take reasonable measures to establish the customer's

---

13 The ML/TF risks include a situation by its nature presenting a high ML/TF risk or a situation specified by the HKMA in a notice in writing given to the licensee.

14 A licensee can take into account customer risk factors; country risk factors; and product, service, transaction or delivery channel risk factors in assessing the level of ML/TF risks; and applied SDD requirements following section 4, Schedule 2 to the AMLO or EDD requirements following section 15, Schedule 2 to the AMLO.

15 Including non-Hong Kong PEPs, Hong Kong PEPs and international organisation PEPs.

16 A non-Hong Kong PEP is defined as:
(a) an individual who is or has been entrusted with a prominent public function in a place outside Hong Kong and
(i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;

or the beneficial owner's source of wealth and the source of the funds before (i) establishing a business relationship; or (ii) continuing an existing business relationship where the customer or the beneficial owner is subsequently found to be a non-Hong Kong PEP. The licensee should also obtain approval from its senior management for establishing or continuing such business relationship with a non-Hong Kong PEP. The same requirements apply to Hong Kong PEPs[17] and international organisation PEPs[18] when the licensee has a business relationship with such a person and identifies a higher risk of ML/TF.

4.23. Following an RBA, a licensee may decide not to apply, or not to continue to apply, the measures set out in paragraphs 4.22 to a former PEP who no longer presents a high risk of ML/TF after stepping down from the position that led to them being regarded as a PEP[19]. To determine whether a former PEP no longer presents a high risk of ML/TF, the licensee should conduct an appropriate assessment of the ML/TF risk associated with the previous PEP status.

(ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual falling within paragraph (a).

17 A Hong Kong PEP is defined as:

(a) an individual who is or has been entrusted with a prominent public function in Hong Kong

(i) includes head of government, senior politician, senior government or judicial official, senior executive of a government-owned corporation and an important political party official;

(ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual falling within paragraph (a).

18 An international organisation PEP is defined as:

(a) an individual who is or has been entrusted with a prominent function by an international organisation, and

(i) includes members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions;

(ii) but does not include a middle-ranking or more junior official of the international organisation;

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual falling within paragraph (a)

19 The handling of a former non-Hong Kong PEP should be based on an assessment of risk and not merely on prescribed time limits.

Reliance on CDD performed by intermediaries

4.24. A licensee may rely upon an intermediary[20] to perform any part of the CDD measures[21] set out in paragraphs 4.3 subject to the applicable criteria set out in section 18 of Schedule 2 to the AMLO, and has measures in place to ensure compliance with the CDD and record keeping requirements under this Guideline. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the licensee.

4.25. When relying on an intermediary, a licensee should:

(a) obtain written confirmation from the intermediary that the intermediary agrees to act as the licensee's intermediary and perform which part of the CDD measures specified in section 2 of Schedule 2 to the AMLO; and

(b) be satisfied that the intermediary will on request provide a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out the CDD measures without delay.

4.26. A licensee that carries out a CDD measure by means of an intermediary should, immediately after the intermediary has carried out that measure, obtain from the intermediary the data or information that the intermediary has obtained in the course of carrying out that measure, but nothing in this paragraph requires the licensee to obtain at the same time from the intermediary a copy of the document, or a record of the data or information, that is obtained by the intermediary in the course of carrying out that measure.

4.27. Where these documents and records are kept by the intermediary, a licensee should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the licensee's business relationship with the customer and for at least five years beginning on the date on which the business relationship of a customer with the licensee ends or until such time as may be specified by the HKMA. The licensee should ensure that the intermediary will, if requested by the licensee within the period specified in the record-keeping requirements of the AMLO, provide to the licensee a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out that measure as soon as reasonably practicable after receiving the request. The licensee should also obtain an undertaking from the intermediary to supply copies of all underlying CDD information in circumstances where the intermediary is about to cease trading or does not act as an intermediary for the licensee anymore. The licensee should

[20] A list of permitted intermediaries is specified in section 18(3) of Schedule 2 to the AMLO.

[21] For the avoidance of doubt, a licensee cannot rely on an intermediary to continuously monitor its business relationship with a customer for the purpose of complying with the requirements in section 5 of Schedule 2 to the AMLO.

conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay.

4.28. Whenever a licensee has doubts as to the reliability of the intermediary, it should take reasonable steps to review the intermediary's ability to perform its CDD duties. If the licensee intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the licensee has any doubts regarding the CDD measures carried out by the intermediary previously, the licensee should perform the required CDD as soon as reasonably practicable.

Failure to satisfactorily complete CDD

4.29. Where a licensee is unable to comply with relevant CDD requirements set out in this Chapter, it should not establish a business relationship or carry out any occasional transaction with that customer, or should terminate business relationship as soon as reasonably practicable (where applicable), and where there is relevant knowledge or suspicion, should make a suspicious transaction report (STR) to the JFIU.

Jurisdictions subject to a call by the Financial Action Task Force (FATF)

4.30. A licensee should apply EDD measures (see paragraph 4.18), proportionate to the risks, to business relationships and transactions with natural and legal persons (including FIs) from jurisdictions for which these are called for by the FATF.

4.31. Where mandatory EDD or countermeasures[22] are called for by the FATF, or in other circumstances independent of any call by the FATF but considered to be of higher risk, the HKMA may also, through a notice in writing:

(a) impose a general obligation on a licensee to comply with the requirements to apply EDD measures set out in section 15 of Schedule 2 to the AMLO; or

(b) require the licensee to undertake specific countermeasures described in the notice.

The type of measures in paragraph (a) and (b) should be proportionate to the nature of the risks and/or deficiencies existing in the AML/CFT regime of the relevant jurisdiction.

[22] For jurisdictions with serious deficiencies in applying the FATF Recommendations and where inadequate progress has been made to improve their positions, the FATF may recommend the application of countermeasures.

Risk management of customers' wallets

4.32. While a licensee is expected to focus primarily on the issuance and redemption of stablecoins, reasonable actions should be taken in respect of wallets used by customers to hold the stablecoins issued by the licensee. Subject to the operating model of the licensee, wallets used by customers to hold stablecoins for the purpose of issuance or redemption may be custodial wallets managed by another FI or virtual asset service provider (VASP); or unhosted wallets (sometimes also referred to as self-hosted or self-custody wallets).

4.33. A licensee should properly manage any ML/TF risks associated with the wallets used by its customers to receive stablecoins from the licensee at issuance and return the stablecoin(s) to the licensee at redemption.

4.34. A licensee should identify a 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:

(a) using appropriate confirmation methods to test the ownership (e.g. requesting the customer to perform a micropayment test (i.e. by effecting a transfer of a small amount specified by the licensee) or message signing test (i.e. by signing a message specified by the licensee which is then verified by the licensee);

(b) obtaining evidence from the customer, such as statements of account issued by the VASP or the wallet provider; or

(c) other appropriate and effective measures.

4.35. To facilitate prompt identification, a licensee may whitelist a customer's wallet address which it has assessed to be owned or controlled by the customer, having regard to the requirements set out in paragraph 4.34[23].

Custodial wallets

4.36. If a customer's wallet is a custodial wallet, a licensee should conduct due diligence measures on the FI or the VASP providing the custodial wallet to the customer (hereafter collectively referred to as "custodial wallet providers"). The licensee should conduct the due diligence measures before the stablecoin is transferred to the customer at issuance or the stablecoin is transferred from the customer back to the licensee at redemption.

---

[23] In general, a licensee can whitelist a customer's wallet address if (i) the customer's wallet is a custodial wallet; (ii) the customer is an entity subject to AML/CFT requirements; or (iii) the customer's wallet is an unhosted wallet and subject to controls set out in paragraph 6.42 in relation to ascertaining the ownership of the unhosted wallet on a periodic and risk sensitive basis.

4.37. A licensee should adopt an RBA in applying the following due diligence measures on a custodial wallet provider[24]:

(a) collect sufficient information about the custodial wallet provider to enable the licensee to understand fully the nature of the custodial wallet provider's business[25];

(b) determine from publicly available information the reputation of the custodial wallet provider and the quality and effectiveness of the AML/CFT regulation and supervision over the custodial wallet provider by authorities in the jurisdictions in which it operates and/or is incorporated which perform functions similar to those of the Relevant Authorities defined in the AMLO;

(c) assess the AML/CFT controls of the custodial wallet provider and be satisfied that they are adequate and effective; and

(d) obtain approval from its senior management.

4.38. A licensee does not need to undertake due diligence for each stablecoin transfer at issuance or at redemption when dealing with custodial wallet providers on which it has previously conducted due diligence measures, unless there is suspicion of ML/TF or when the licensee is aware of any heightened ML/TF risks from its ongoing monitoring of transactions with the custodial wallet provider.

Unhosted wallets

4.39. An unhosted wallet refers to software or hardware that enables a person to store and transfer virtual assets (VAs), including stablecoins, on the person's own behalf, and in relation to which the private key is held or controlled by that person. Unhosted wallets can allow VAs to be transacted peer-to-peer without the involvement of an AML/CFT-obliged intermediary. This decentralised

---

[24] In applying RBA, the following risk factors may be taken into account: (a) the types of products and services offered by the custodial wallet provider; (b) the types of customers to whom the custodial wallet provider provides services; (c) geographical exposures of the custodial wallet provider and its customers; (d) the AML/CFT regime in the jurisdictions in which the custodial wallet provider operates and/or is incorporated; and (e) the adequacy and effectiveness of the AML/CFT controls of the custodial wallet provider.

[25] While a licensee should determine on a risk-sensitive basis the amount of information to collect about the custodial wallet provider to enable it to understand the nature of the custodial wallet provider's business, the licensee should, among other things, endeavour to identify and verify the identity of the custodial wallet provider using documents, data or information provided by a reliable and independent source; and take reasonable measures to understand the ownership and control structure of the custodial wallet provider, with the objective to follow the chain of ownerships to its beneficial owners.

nature and lack of regulatory oversight may particularly attractive to illicit actors or money launderers.

4.40. When a customer uses an unhosted wallet to receive stablecoins from a licensee at issuance or return stablecoins to a licensee at redemption, the licensee should conduct additional control measures before completing the respective issuance or redemption processes:

(a) conduct enhanced monitoring of stablecoin transfers with the unhosted wallet;

(b) transfer stablecoin only to or from unhosted wallets that the licensee has assessed to be reliable[26], having regard to the screening results of the stablecoin transactions and the associated wallet addresses (see paragraphs 5.4, 5.5, 5.7 and 5.8); and

(c) (where appropriate) impose transaction limits[27].

4.41. For the avoidance of doubt, if a customer that is an entity subject to AML/CFT requirements uses an unhosted wallet to hold stablecoins, a licensee should, instead of conduct additional control measures set out in paragraph 4.40, apply the due diligence measures set out in paragraph 4.37.

[26] For example, a licensee may implement controls to prevent the relevant stablecoins from an unhosted wallet being made available to its customer, or putting the transfer to an unhosted wallet on hold, unless the licensee is satisfied that the relevant unhosted wallet is reliable.

[27] For example, a license may place appropriate limits on the amount of stablecoin transfers or transfers of stablecoins with unhosted wallets.

5. Ongoing monitoring

5.1. Ongoing monitoring is an essential component of effective AML/CFT Systems. Unlike other FIs (e.g. banks or SFC-licensed VA trading platforms) which serve as intermediaries to conduct various financial transactions on behalf of their customers, a licensee's main activities revolve around the issuance and redemption of stablecoins. The approach to ongoing monitoring of suspicious activities may vary from licensee to licensee, depending on their business and operating models, and the associated ML/TF risks.

5.2. A licensee should continuously monitor its business relationship with a customer in two aspects:

(a) **ongoing CDD**: reviewing from time to time documents, data and information relating to the customer that have been obtained by the licensee for the purpose of complying with the requirements imposed under this Guideline and Part 2 of Schedule 2 to the AMLO to ensure that they are up-to-date and relevant; and

(b) **transaction monitoring**:
   (i) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the licensee's knowledge of the customer, the customer's business, risk profile and source of funds; and
   (ii) identifying transactions that (i) are complex, unusually large in amount or of an unusual pattern; and (ii) have no apparent economic or lawful purpose, and examining the background and purposes of those transactions and setting out the findings in writing.

5.3. To ensure documents, data and information of a customer obtained are up-to-date and relevant[28], a licensee should undertake reviews of existing CDD records of customers on a regular basis and/or upon trigger events following an RBA. Clear policies and procedures should be developed, especially on the frequency of periodic review or what constitutes a trigger event.

5.4. A licensee should also 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. 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 stablecoin to or from customers) and the associated

[28] Keeping the CDD information up-to-date and relevant does not mean that a licensee has to re-verify identities that have been verified (unless doubts arise as to the veracity or adequacy of the information previously obtained for the purposes of customer identification and verification).

wallet addresses. In particular, the licensee should adopt appropriate technological solutions (e.g. blockchain analytic tools[29]) to:

(a) track the transaction history of stablecoins to more accurately identify the source[30] 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[31], or designated parties.

5.5. Where a licensee employs a technological solution provided by an external party to conduct screening of stablecoin transactions and the associated wallet addresses, the licensee remains responsible for discharging its AML/CFT obligations. The licensee should conduct due diligence on the solution before deploying it, taking into account relevant factors such as:

(a) the quality and effectiveness of the tracking and detection tools;

(b) the coverage, accuracy and reliability of the information maintained in the database that supports its screening capability (e.g. whether the list of wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources, or designated parties, is subject to timely review and update); and

(c) any limitations (e.g. limited reach of the blockchain analytical tools; or inability to deal with VA or wallet addresses involving the use of anonymity-enhancing technologies or mechanisms such as anonymity-enhanced VAs, mixers or tumblers).

5.6. A licensee should (where applicable) monitor the additional information (i.e. IP addresses with associated time stamps, geo-location data, device identifiers, metadata and other electronic identifiers) obtained by the licensee on an ongoing basis to identify suspicious transactions and activities as well as take appropriate follow-up actions.

---

29 Blockchain analytic tools typically enable their users to trace the on-chain history of specific virtual assets. These tools support a number of common virtual assets and compare transaction histories against a database of wallet addresses connected to illicit or suspicious activities/sources, and flag identified transactions.

30 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.

31 Illicit activities include, for example, ransomware, fraud, identity theft, phishing, and other cybercrimes; and suspicious activities/sources include, for example, darknet marketplaces, online gambling services, peel chains and use of anonymity-enhancing technologies or mechanisms (e.g. mixers, tumblers, privacy wallets). In addition, any wallet addresses owned or controlled by customers with which the licensee has decided not to establish or continue business relationships due to suspicion of ML/TF should be included as those associated with suspicious sources.

5.7. A licensee should take appropriate steps (e.g. examining the background and purposes of the transactions; making appropriate enquiries to or obtaining additional CDD information from a customer) to identify if there are any grounds for suspicion, when:

(a) the customer's transactions are not consistent with the licensee's knowledge of the customer, the customer's business, risk profile or source of funds;

(b) the licensee identifies transactions and series of transactions that (i) are complex, unusually large in amount or of an unusual pattern, and (ii) have no apparent economic or lawful purpose[32]; or

(c) the licensee identifies transactions and series of transactions involving wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources, or designated parties.

5.8. Where a licensee becomes aware of any heightened ML/TF risks from ongoing monitoring of business relationship with its customers and screening of stablecoin transactions and the associated wallet addresses, the licensee should apply enhanced customer due diligence and ongoing monitoring, and take other additional preventive or mitigating actions as necessary to mitigate the ML/TF risks involved.

Ongoing monitoring for stablecoins in circulation

5.9. Unlike some types of VA that may lack an identifiable issuer, a licensee, as an AML/CFT-obligated entity, has a responsibility for maintaining effective functioning of the stablecoins and guarding against the risk of their misuse for unlawful purposes. Ongoing monitoring of stablecoins in circulation is crucial for the licensee to discharge its AML/CFT responsibilities. The extent of such ongoing monitoring should be proportionate to the associated ML/TF risks identified in the licensee's institutional risk assessment (see paragraph 2.2), taking into account the nature of the licensee's business model (e.g. open or closed-loop).

5.10. While a licensee is not required to conduct CDD on non-customer stablecoin holders in possession of the stablecoins in circulation, all on-chain stablecoin transactions [33] are recorded instantaneously and automatically on the blockchains on which they take place, and such records provide some traceability of transactions which can aid in identification of potential illicit activities, as well as wallet addresses involved in such activities. A licensee should therefore take adequate and proportionate ongoing monitoring measures

[32] A licensee should examine the background and purposes of the transactions and set out its findings in writing.

[33] For example, time, date, transaction hash and wallet addresses.

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.

5.11. If a licensee identifies any stablecoin transactions and the associated wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources, or designated parties, the licensee should promptly undertake further investigations and analyses. If there are any grounds for suspicion; the licensee should report the suspicious transactions to the JFIU and take appropriate follow-up actions as stated in Chapter 8 of this Guideline.

6. Stablecoin transfers

6.1. This Chapter provides guidance on how a licensee should comply with the requirements with regard to stablecoin transfers set out in section 13A of Schedule 2 to the AMLO, in circumstances where the transfer of stablecoins issued by a licensee falls under the definition of stablecoin transfer (see paragraph 6.3).

6.2. To prevent criminals and terrorists from having unfettered opportunities to move their assets through stablecoin transfers and to detect such misuse when it occurs, a licensee must take all reasonable measures to ensure that proper safeguards exist to mitigate the ML/TF risks associated with stablecoin transfers. In particular, a licensee should establish and maintain effective procedures to ensure compliance with:

(a) the stablecoin transfers requirements under paragraphs 6.5 to 6.24 (also called the travel rule[34]); and

(b) other relevant requirements under paragraphs 6.25 to 6.42,

to enable it to effectively carry out sanctions screening and transaction monitoring procedures on all relevant parties involved in a stablecoin transfer.

Stablecoin transfers between a licensee and another institution

6.3. A stablecoin transfer is a transaction carried out:

(a) by an institution (the ordering institution) on behalf of a person (the originator) by transferring any stablecoin; and

(b) with a view to making the stablecoin available:
  (i) to that person or another person (the recipient); and
  (ii) at an institution (the beneficiary institution), which may be the ordering institution or another institution,

whether or not one or more other institutions (intermediary institutions) participate in completion of the transfer of the stablecoins.

[34] The travel rule refers to the application of the wire transfer requirements set out in FATF Recommendation 16 in a modified form in the context of virtual asset transfers (in particular, the requirements to obtain, hold, and submit required and accurate originator and required recipient information immediately and securely when conducting virtual asset transfers), recognising the unique technological properties of virtual assets.

6.4. Depending on its business model, a licensee may act as an ordering institution, an intermediary institution or a beneficial institution in a stablecoin transfer. The licensee should follow the relevant requirements set out in this Chapter with reference to its role in a stablecoin transfer.

Ordering institutions

6.5. Before carrying out a stablecoin transfer involving an amount not less than $8,000, an ordering institution must obtain and record the following originator and recipient information[35]:

(a) the originator's name;

(b) the number of the originator's account maintained with the ordering institution and from which the stablecoin is transferred (i.e. the account used to process the transaction) or, in the absence of such an account, a unique reference number assigned to the stablecoin transfer by the ordering institution;

(c) the originator's address [36], the originator's customer identification number[37] or identification document number or, if the originator is an individual, the originator's date and place of birth;

(d) the recipient's name; and

(e) the number of the recipient's account maintained with the beneficiary institution and to which the stablecoin is transferred (i.e. the account used to process the transaction) or, in the absence of such an account, a unique reference number assigned to the stablecoin transfer by the beneficiary institution.

---

35 For the avoidance of doubt, in relation to stablecoin transfers carried out for a customer, a licensee is not required to obtain the originator information from a customer that is the originator before carrying out every individual stablecoin transfer (unless doubts arise as to veracity or adequacy of the information previously obtained for the purposes of customer identification and verification).

36 The originator's address refers to the geographical address of the originator (i.e. residential address of an originator that is a natural person; or the address of the registered office (or principal place of business if different from the registered office) of an originator that is a legal person, a trust or other similar legal arrangement).

37 Customer identification number means a number which uniquely identifies the originator to the ordering institution and is a different number from the unique transaction reference number referred to in paragraph 6.8. The customer identification number must refer to a record held by the ordering institution which contains at least one of the following: the customer's address, identification document number, or date and place of birth.

6.6. Before carrying out a stablecoin transfer involving an amount less than $8,000, an ordering institution must obtain and record the following originator and recipient information:

(a) the originator's name;

(b) the number of the originator's account maintained with the ordering institution and from which the stablecoins are transferred or, in the absence of such an account, a unique reference number assigned to the stablecoin transfer by the ordering institution;

(c) the recipient's name; and

(d) the number of the recipient's account maintained with the beneficiary institution and to which the stablecoins are transferred (i.e. the account used to process the transaction) or, in the absence of such an account, a unique reference number assigned to the stablecoin transfer by the beneficiary institution.

6.7. Where applicable, the number of the account maintained with the ordering institution or beneficiary institution from or to which the stablecoins are transferred referred to in paragraphs 6.5 and 6.6 could mean the wallet address of the originator or recipient maintained with the ordering institution or beneficiary institution and used to process the transaction.

6.8. The unique reference number assigned to the stablecoin transfer by the ordering institution or beneficiary institution referred to in paragraphs 6.5 and 6.6 should permit traceability of the stablecoin transfer.

6.9. An ordering institution must submit the required originator and recipient information obtained and held under paragraphs 6.5 and 6.6 (hereafter referred to as "required information") to the beneficiary institution securely (see paragraph 6.12).

6.10. In addition, the ordering institution must submit the required information to the beneficiary institution immediately (see paragraph 6.13).

6.11. For the avoidance of doubt, the required information may be submitted either directly or indirectly to the beneficiary institution provided that it is submitted in accordance with the requirements set out in paragraphs 6.9 and 6.10. This means that it is not necessary for the required information to be attached directly to, or be included in, the stablecoin transfer itself.

6.12. "Securely" means that the ordering institution should store and submit the required information in a secure manner to protect the integrity and availability of the required information for facilitating record-keeping and the use of such

information by the beneficiary institution and, where applicable, the intermediary institution, in fulfilling its AML/CFT obligations[38]; and protect the information from unauthorised access or disclosure. To ensure that the required information is submitted in a secure manner, an ordering institution should[39]:

(a) undertake the stablecoin transfer counterparty due diligence measures as set out in paragraphs 6.28 to 6.39 to determine whether the beneficiary institution and, where applicable, the intermediary institution can reasonably be expected to adequately protect the confidentiality and integrity of the information submitted to it; and

(b) take other appropriate measures and controls, for example:

(i) entering into a bilateral data sharing agreement with the beneficiary institution and, where applicable, the intermediary institution and/or (where applicable) a service-level agreement with the technological solution provider for travel rule compliance (see paragraphs 6.25 to 6.27) which specifies the responsibilities of the institutions involved and/or of the provider to ensure the protection of the confidentiality and integrity of the information submitted;

(ii) using, or ensuring the technological solution adopted for travel rule compliance (where applicable) uses, a strong encryption algorithm to encrypt the information during the data submission; and

(iii) implementing adequate information security controls to prevent unauthorised access, disclosure or alteration.

For the avoidance of doubt, an ordering institution should not execute a stablecoin transfer unless it can ensure that the required information can be submitted to a beneficiary institution, and where applicable, an intermediary institution, in a secure manner having regard to the above guidance and the stablecoin transfer counterparty due diligence results.

6.13. "Immediately" means that the ordering institution should submit the required information prior to, or simultaneously or concurrently with, the stablecoin transfer (i.e. the submission must occur before or when the stablecoin transfer is conducted)[40].

---

38 AML/CFT obligations include, among others, identifying and reporting suspicious stablecoin transfers, taking freezing actions and prohibiting stablecoin transfers with designated persons and entities.

39 An ordering institution should give due regard to the laws and regulations on privacy and data protection of the jurisdictions in which the ordering institution operates and/or is incorporated.

40 Where an intermediary institution is involved in a stablecoin transfer, an ordering institution should undertake the stablecoin transfer counterparty due diligence measures as set out in paragraphs 6.28 to 6.39 to determine if the intermediary institution can submit the required information immediately

6.14. An ordering institution should keep records and relevant documents so that it can demonstrate to the relevant authority whether and how the required information is submitted to a beneficiary institution in accordance with the requirements set out in paragraphs 6.9 and 6.10[41].

6.15. For a stablecoin transfer involving an amount not less than $8,000, an ordering institution must ensure that the required originator information submitted with the stablecoin transfer is accurate[42].

6.16. For an occasional stablecoin transfer involving an amount not less than $8,000, an ordering institution must verify the identity of the originator[43]. For an occasional stablecoin transfer involving an amount less than $8,000, the ordering institution is in general not required to verify the originator's identity, except when several transactions are carried out which appear to the ordering institution to be linked and amount to not less than $8,000, or when there is a suspicion of ML/TF.

6.17. The ordering institution should not execute a stablecoin transfer unless it has ensured compliance with the requirements in paragraphs 6.5 to 6.16.

Intermediary institutions

6.18. An intermediary institution must ensure that all originator and recipient information as set out in paragraphs 6.5 and 6.6 which the intermediary institution receives in connection with the stablecoin transfer is retained with the required information submission, and is transmitted to the institution to which it passes on the transfer instruction[44].

---

to the beneficiary institution, or where applicable, another intermediary institution and should not execute the stablecoin transfer if the intermediary institution is unable to do so.

41 For the avoidance of doubt, where technological solution is adopted for travel rule compliance, the ordering institution should keep any records or relevant documents of its due diligence on the technological solution. In addition, where an intermediary institution is involved in a stablecoin transfer, the ordering institution should keep records and relevant documents that demonstrate whether and how the required information is submitted to the beneficiary institution through the intermediary institution in accordance with the requirements set out in paragraphs 6.9 and 6.10.

42 "Accurate" in this context means information that has been verified for accuracy as part of its CDD process. For example, if the originator's address is part of the required information to be submitted by the ordering institution, the ordering institution should ensure that the originator's address is accurate having regard to the CDD information obtained pursuant to Chapter 4 as appropriate.

43 For the avoidance of doubt, where the originator is a customer of a licensee, the licensee does not need to re-verify the identity of the customer that has been verified (unless doubts arise as to veracity or adequacy of the information previously obtained for the purposes of customer identification and verification).

44 An intermediary institution should undertake the stablecoin transfer counterparty due diligence measures on the ordering institution and, where applicable, another intermediary institution(s), as set out in paragraphs 6.28 to 6.39.

6.19. As with the submission of required information by an ordering institution, an intermediary institution should transmit the aforesaid information to another intermediary institution or the beneficiary institution in accordance with the manner set out in paragraphs 6.12 to 6.13 and the requirement set out in paragraph 6.14[45].

Beneficiary institutions

6.20. A beneficiary institution must obtain and record the required information submitted to it by the institution from which it receives the transfer instruction[46].

6.21. For a stablecoin transfer involving an amount not less than $8,000, a beneficiary institution should verify the identity of the recipient if the identity has not been previously verified as part of its CDD process. The beneficiary institution should also confirm whether the recipient's name and account number obtained from the institution from which it receives the transfer instruction match with the recipient information verified by it, and take reasonable measures as set out in paragraph 6.24 where such information does not match.

Identification and handling of incoming stablecoin transfers lacking the required information

6.22. A beneficiary institution or an intermediary institution (hereafter referred to as "instructed institution") must establish and maintain effective procedures for identifying and handling incoming stablecoin transfers that do not comply with the relevant requirements on required originator or recipient information, which include:

(a) taking reasonable measures (e.g. real-time or post-event monitoring) to identify stablecoin transfers that lack the required information; and

(b) having risk-based policies and procedures for determining: (i) whether and when to execute, suspend (i.e. prevent the relevant stablecoins from being made available to the recipient) a stablecoin transfer lacking the required information or, where appropriate, return the relevant stablecoins to the account of the ordering institution or another intermediary institution (hereafter referred to as "instructing institution") from which the instructed institution receives the transfer instruction[47]; and (ii) the appropriate follow-up action.

---

45 For the purpose of paragraph 6.19, any reference to "ordering institution" and "the intermediary institution" in paragraphs 6.12 to 6.14 refers to "intermediary institution" and "another intermediary institution" respectively.

46 A beneficiary institution should undertake the stablecoin transfer counterparty due diligence measures on the ordering institution and, where applicable, the intermediary institution(s), as set out in paragraphs 6.28 to 6.39.

47 An instructed institution should consider preventing the stablecoin from being made available to the recipient until the missing information is obtained or, where appropriate, returning the stablecoin

6.23. In respect of the risk-based policies and procedures referred to in paragraph 6.22, if an instructing institution does not submit all of the required information in connection with the stablecoin transferred to the instructed institution, the instructed institution must as soon as reasonably practicable obtain the missing information from the instructing institution. If the missing information cannot be obtained, the instructed institution should either consider restricting or terminating its business relationship with the instructing institution in relation to stablecoin transfers, or take reasonable measures to mitigate the risk of ML/TF involved.

6.24. If the instructed institution is aware that any of the information submitted to it that purports to be the required information is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved having regard to the procedures set out in paragraph 6.22(b).

Stablecoin transfers – Technological solutions for travel rule compliance

6.25. A licensee may adopt any technological solution to submit and/or obtain the required information for a stablecoin transfer provided that the solution enables the licensee to comply with the travel rule as set out in paragraphs 6.5 to 6.24, when it acts as an ordering institution, an intermediary institution or a beneficiary institution.

6.26. Where a licensee chooses to use a technological solution to ensure travel rule compliance, it remains responsible for discharging its AML/CFT obligations in relation to travel rule compliance. The licensee should conduct due diligence to satisfy itself that the solution enables it to comply with the travel rule in an effective and efficient manner. In particular, the licensee should consider whether the solution enables it to:

(a) identify stablecoin transfer counterparties; and

(b) submit the required information immediately and securely (i.e. whether the solution could protect the submitted information from unauthorised access, disclosure or alteration), and obtain the required information[48].

---

to the account of the instructing institution when there is no suspicion of ML/TF, taking into account the results of the stablecoin transfer counterparty due diligence (see paragraphs 6.28 to 6.39) and screening of the stablecoin transactions and the associated wallet addresses in relation to the stablecoin transfers (see paragraphs 5.4, 5.5, 5.7 and 5.8). Please also refer to risk mitigating measures in paragraph 7.8.

[48] In considering whether the solution enables the licensee to obtain the required information, the licensee should take into account whether it could identify situations where the required information provided by ordering institutions is incomplete or missing, which may result from slight differences in travel rule requirements across the laws, rules and regulations of other jurisdictions, before conducting stablecoin transfers.

6.27. In addition, a licensee should consider a range of factors as appropriate when conducting due diligence on the technological solution for travel rule compliance, such as:

(a) the interoperability of the solution with other similar solution(s) adopted by the stablecoin transfer counterparties that the licensee may deal with;

(b) whether the solution allows the required information for a large volume of stablecoin transfers to be submitted immediately and securely to and/or obtained from multiple stablecoin transfer counterparties in a stable manner;

(c) whether the solution enables the licensee to implement measures or controls for the effective scrutiny of stablecoin transfers to identify and report suspicious transactions (as set out in paragraphs 5.4, 5.5, 5.7 and 5.8), and screening of stablecoin transfers to meet the sanctions obligations (i.e. taking freezing actions and prohibiting stablecoin transfers with designated persons and entities) (as set out in paragraphs 7.5, 7.6, 7.7 and 7.8);

(d) whether the solution facilitates the licensee in conducting stablecoin transfer counterparty due diligence (see paragraphs 6.28 to 6.39) and requesting additional information from the stablecoin transfer counterparty as and when necessary; and

(e) whether the solution facilitates the licensee in keeping the required information (see paragraph 9.6).

Stablecoin transfer counterparty due diligence and additional measures

6.28. When a licensee conducts a stablecoin transfer referred to in paragraphs 6.5 to 6.24, the licensee will be exposed to ML/TF risks associated with the counterparty institution which may be the ordering institution, intermediary institution or beneficiary institution involved in the stablecoin transfer (hereafter collectively referred to as "stablecoin transfer counterparty"). The ML/TF risks associated with the stablecoin transfer counterparty may vary depending on the following factors:

(a) the types of products and services offered by the stablecoin transfer counterparty;

(b) the types of customers to which the stablecoin transfer counterparty provides services;

(c) geographical exposures of the stablecoin transfer counterparty and its customers;

(d) the AML/CFT regime in the jurisdictions in which the stablecoin transfer counterparty operates and/or is incorporated; and

(e) the adequacy and effectiveness of the AML/CFT controls of the stablecoin transfer counterparty.

6.29. To avoid sending or receiving stablecoins to or from illicit actors or designated parties that have not been subject to the appropriate CDD and screening measures undertaken by a stablecoin transfer counterparty and to ensure compliance with the travel rule, a licensee should conduct due diligence on the stablecoin transfer counterparty to identify and assess the ML/TF risks associated with the stablecoin transfers to or from the stablecoin transfer counterparty and apply appropriate risk-based AML/CFT measures.

6.30. A licensee should conduct due diligence measures on a stablecoin transfer counterparty before conducting a stablecoin transfer or making the transferred stablecoins available to the recipient. If a licensee conducts stablecoin transfers with several stablecoin transfer counterparties located in different jurisdictions but belonging to the same group, the licensee, whilst conducting due diligence on each of the stablecoin transfer counterparties independently, should also take into account that these counterparties belong to the same group in order to holistically assess the ML/TF risks posed by the counterparties.

6.31. A licensee does not need to undertake the stablecoin transfer counterparty due diligence process for every individual stablecoin transfer when dealing with stablecoin transfer counterparties that it has previously conducted counterparty due diligence on, unless when there is a suspicion of ML/TF or when the licensee is aware of any heightened ML/TF risks from its ongoing monitoring of stablecoin transfers with stablecoin transfer counterparties (see paragraph 6.36).

6.32. Stablecoin transfer counterparty due diligence typically involves the following procedures:

(a) determining whether the stablecoin transfer is or will be with a stablecoin transfer counterparty or an unhosted wallet;

(b) where applicable, identifying the stablecoin transfer counterparty (e.g. by making reference to lists of licensed or registered VASPs or FIs in different jurisdictions); and

(c) assessing whether the stablecoin transfer counterparty is an eligible counterparty to deal with and to send the required information to (see paragraphs 6.33 to 6.35).

6.33. A licensee should adopt an RBA in applying the following due diligence measures on a stablecoin transfer counterparty, taking into account relevant factors such as those set out in paragraph 6.28:

(a) collect sufficient information about the stablecoin transfer counterparty to enable it to understand fully the nature of the stablecoin transfer counterparty's business[49];

(b) understand the nature[50] and expected volume and value of stablecoin transfers with the stablecoin transfer counterparty;

(c) determine from publicly available information the reputation of the stablecoin transfer counterparty and the quality and effectiveness of the AML/CFT regulation and supervision over the stablecoin transfer counterparty by authorities in the jurisdictions in which it operates and/or is incorporated which perform functions similar to those of the RAs;

(d) assess the AML/CFT controls of the stablecoin transfer counterparty and be satisfied that the AML/CFT controls of the stablecoin transfer counterparty are adequate and effective; and

(e) obtain approval from its senior management.

6.34. As part of the stablecoin transfer counterparty due diligence measures in relation to its AML/CFT controls, a licensee should assess whether the stablecoin transfer counterparty can comply with the travel rule, taking into account relevant factors such as:

(a) whether the stablecoin transfer counterparty is subject to requirements similar to the travel rule imposed under section 13A of Schedule 2 to the AMLO and this Chapter in the jurisdictions in which the stablecoin transfer counterparty operates and/or is incorporated; and

(b) the adequacy and effectiveness of the AML/CFT controls that the stablecoin transfer counterparty has put in place for ensuring compliance with the travel rule.

---

[49] While a licensee should determine on a risk-sensitive basis the amount of information to collect about the stablecoin transfer counterparty to enable it to understand the nature of the stablecoin transfer counterparty's business, the licensee should, among other things, endeavour to identify and verify the identity of the stablecoin transfer counterparty using documents, data or information provided by a reliable and independent source; and take reasonable measures to understand the ownership and control structure of the stablecoin transfer counterparty, with the objective to follow the chain of ownerships to its beneficial owners.

[50] For example, the extent to which any of the stablecoin transfers and relevant underlying customers (who may be the originator or recipient of a stablecoin transfer) are assessed as high risk by the stablecoin transfer counterparty.

In addition, the licensee should assess whether the stablecoin transfer counterparty can protect the confidentiality and integrity of personal data (e.g. the required originator and recipient information), taking into account the adequacy and robustness of data privacy and security controls of the stablecoin transfer counterparty[51].

6.35. When assessing the ML/TF risks posed by a stablecoin transfer counterparty, a licensee should take into account relevant factors that may indicate a higher ML/TF risk, for example, a stablecoin transfer counterparty that:

(a) operates or is incorporated in a jurisdiction posing a higher risk or with a weak AML/CFT regime;

(b) is not (or is yet to be) licensed or registered and supervised for AML/CFT purposes in the jurisdictions in which it operates and/or is incorporated by authorities which perform functions similar to those of the RAs;

(c) does not have in place adequate and effective AML/CFT Systems, including measures for ensuring compliance with the travel rule;

(d) does not implement adequate measures or safeguards for protecting the confidentiality and integrity of personal data; or

(e) is associated with ML/TF or other illicit activities.

6.36. A licensee should monitor the stablecoin transfer counterparties on an ongoing basis, including:

(a) adopting an RBA in monitoring stablecoin transfers with stablecoin transfer counterparties with a view to detecting any unexpected or unusual activities or transactions and any changes in the risk profiles of the stablecoin transfer counterparties, taking into account the transaction monitoring requirements in paragraphs 5.4, 5.5, 5.7 and 5.8; and

(b) reviewing the information obtained by the licensee from applying the stablecoin transfer counterparty due diligence measures under paragraph 6.33 on a regular basis and/or upon trigger events (e.g. when the licensee is aware of any heightened ML/TF risks from its ongoing monitoring of stablecoin transfers with stablecoin transfer counterparties or other information such as negative news from credible media or public information that the counterparty has been subject to any targeted financial sanction, ML/TF investigation or regulatory action) and, where appropriate, updating its risk assessment of a stablecoin transfer counterparty.

---

[51] This is to ensure that, among other things, the required information is submitted in a secure manner as mentioned in paragraph 6.12.

Based on the stablecoin transfer counterparty due diligence results, the licensee should determine if it should continue to conduct stablecoin transfers with, and submit the required information to, a stablecoin transfer counterparty, and the extent of AML/CFT measures that it should apply in relation to stablecoin transfers with the stablecoin transfer counterparty on a risk-sensitive basis.

6.37. A licensee should assess how the ML/TF risks identified from the stablecoin transfer counterparty due diligence may affect it, and take reasonable measures on a risk-sensitive basis to mitigate and manage the ML/TF risks posed by a stablecoin transfer counterparty[52], which include:

(a) perform enhanced and/or more frequent due diligence reviews;

(b) conduct enhanced monitoring of stablecoin transfers with the stablecoin transfer counterparty; and

(c) (where appropriate) impose transaction limits,

when dealing with a stablecoin transfer counterparty that presents a higher ML/TF risk.

6.38. A licensee should also determine on a risk-sensitive basis whether to restrict or continue to deal with, or refrain from executing or facilitating any stablecoin transfers to or from, a stablecoin transfer counterparty that presents higher ML/TF risks. If the licensee cannot mitigate and manage the ML/TF risks posed by a stablecoin transfer counterparty, it should refrain from executing or facilitating such stablecoin transfers.

6.39. A licensee must not conduct stablecoin transfers with a stablecoin transfer counterparty that is a shell VASP or a shell FI[53].

Stablecoin transfers involving licensee to or from unhosted wallets

6.40. Peer-to-peer transactions associated with unhosted wallets[54] may be attractive to illicit actors given the anonymity and mobility of stablecoins and that there is typically no intermediary involved in the peer-to-peer transactions to carry out AML/CFT measures such as CDD and transaction monitoring. A licensee should comply with the requirements set out in paragraphs 6.41 and 6.42 when

---

52 In particular, the licensee should implement appropriate measures to mitigate and manage the risks posed by stablecoin transfers from or to originators or recipients that are third parties.

53 For the purpose of this Guideline, a shell FI / VASP is a corporation that: (a) is incorporated in a place outside Hong Kong; (b) is authorised to carry on financial services / VA businesses in that place; (c) does not have a physical presence in that place; and (d) is not an affiliate of a regulated financial group that is subject to effective group-wide supervision.

54 Refer to paragraph 4.39 for the meaning of "unhosted wallets".

conducting stablecoin transfers to or from unhosted wallets so as to mitigate the associated ML/TF risks.

6.41. Before a licensee sends or receives stablecoins to or from an unhosted wallet on behalf of its customer (i.e. the originator or the recipient, as the case may be), the licensee should obtain and record the following originator and recipient information from the customer[55]:

(a) in relation to a stablecoin transfer to an unhosted wallet,
  (i) the originator's name;
  (ii) the number of the originator's account maintained with the licensee and from which the stablecoins are transferred or, in the absence of such an account, a unique reference number assigned to the stablecoin transfer by the licensee;
  (iii) the originator's address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth;
  (iv) the recipient's name; and
  (v) the recipient's wallet address;

(b) in relation to a stablecoin transfer from an unhosted wallet,
  (i) the originator's name;
  (ii) the originator's wallet address;
  (iii) the originator's address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth;
  (iv) the recipient's name; and
  (v) the number of the recipient's account maintained with the licensee and to which the stablecoins are transferred or, in the absence of such an account, a unique reference number assigned to the stablecoin transfer by the licensee.

6.42. A licensee should also assess the ML/TF risks associated with stablecoin transfers to or from unhosted wallets and take reasonable measures on a risk-sensitive basis to mitigate and manage the ML/TF risks associated with the transfers[56], which include:

---

[55] For the avoidance of doubt, a licensee is not required to obtain the originator information (for a stablecoin transfer to an unhosted wallet) or the recipient information (for a stablecoin transfer from an unhosted wallet) from a customer that is the originator or recipient respectively for every individual stablecoin transfer to or from an unhosted wallet (unless doubts arise as to veracity or adequacy of the information previously obtained for the purposes of customer identification and verification). For the purposes of paragraph 6.41, a licensee is not required to obtain the information in (a)(iii) and (b)(iii) set out therein for a stablecoin transfer to or from an unhosted wallet involving stablecoin that amount to less than $8,000.

[56] In particular, the licensee should implement appropriate measures to mitigate and manage the risks posed by stablecoin transfers to or from third parties.

(a) conduct enhanced monitoring of stablecoin transfers with unhosted wallets;

(b) accept stablecoin transfers only to or from unhosted wallets that the licensee has assessed to be reliable[57], having regard to the screening results of the stablecoin transactions and the associated wallet addresses (see paragraphs 5.4, 5.5, 5.7 and 5.8) and the assessment results of the ownership or control of the unhosted wallet[58] (see paragraphs 4.34); and

(c) (where appropriate) impose transaction limits[59].

---

57 For example, a licensee may implement controls to prevent the stablecoin from an unhosted wallet being made available to its customer, or putting the transfer to an unhosted wallet on hold, when the licensee is satisfied that the relevant unhosted wallet is unreliable.

58 Where stablecoin are transferred to or from an unhosted wallet that has been whitelisted in accordance with the requirements in paragraph 4.34, a licensee should ascertain the ownership or control of the unhosted wallet on a periodic and risk-sensitive basis, in particular, where the licensee becomes aware of any heightened ML/TF risks from the ongoing monitoring of stablecoin transactions and the associated wallet addresses or additional customer information (see paragraphs 5.4, 5.5, 5.7 and 5.8).

59 For example, a licensee may place appropriate limits on the amount of stablecoin transfers with unhosted wallets.

7. Terrorist financing, financial sanctions and proliferation financing

7.1. A licensee should establish and maintain effective policies, procedures and controls to ensure compliance with the relevant regulations and legislation on TF, financial sanctions and proliferation financing (PF). The legal and regulatory obligations of licensees and those of their staff should be well understood and adequate guidance and training should be provided to the latter.

7.2. It is particularly vital that a licensee should be able to identify terrorist suspects and possible designated parties, and detect prohibited transactions. To this end, a licensee should ensure that it maintains a database of names and particulars of terrorists and designated parties, which consolidates the various lists that have been made known to the licensee. Alternatively, a licensee may subscribe to such a database maintained by a third party service provider and take appropriate measures (e.g. conduct sample testing periodically) to ensure the completeness and accuracy of the database.

7.3. Whether or not a UNSCR or sanctions list has been implemented through Hong Kong legislation, there are offences under existing legislation relating to ML, TF and PF that are relevant. Inclusion of a country, individual, entity or activity in the UNSCR or sanctions list may constitute grounds for knowledge or suspicion for the purposes of relevant ML, TF and PF laws, thereby triggering statutory (including reporting) obligations as well as offence provisions. The HKMA draws to the attention to licensees from time to time whenever there are any updates to UNSCRs or sanctions lists relating to terrorism, TF and PF promulgated by the UNSC. Licensees should ensure that countries, individuals and entities included in UNSCRs and sanctions lists are included in the database as soon as practicable after they are promulgated by the UNSC and regardless of whether the relevant sanctions have been implemented by legislation in Hong Kong.

7.4. A licensee should include in its database: (i) the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau; and (ii) the lists that the HKMA draws to the attention of licensees from time to time. The database should also be subject to timely update whenever there are changes, and should be made easily accessible by relevant staff.

7.5. To avoid establishing business relationship or conducting transactions with any terrorist suspects and possible persons or entities including (i) designated persons or entities, (ii) persons or entities acting on behalf or at the direction of the designated persons or entities mentioned in (i), or (iii) entities owned or controlled by any persons or entities mentioned in (i) or (ii), a licensee should implement an effective screening mechanism[60], which should include:

[60] Screening should be carried out irrespective of the risk profile attributed to the customer.

(a) screening its customers and any beneficial owners of the customers against current database at issuance and at redemption;

(b) screening its customers and any beneficial owners of the customers against all new and any updated designations to the database as soon as practicable; and

(c) screening all relevant parties in a stablecoin transfer[61] against current database before executing the transfer.

7.6. The screening requirements set out in paragraph 7.5(a) and (b) should extend to connected parties as defined in paragraph 4.12 and PPTAs of a customer using an RBA.

7.7. For the screening requirement set out in paragraph 7.5(c), a licensee should screen the required originator and recipient information[62] referred to in:

(a) paragraph 6.5 or 6.6 in relation to a stablecoin transfer (including information which may be held separately to the stablecoin transfer itself); or

(b) paragraph 6.41 in relation to a stablecoin transfer to or from an unhosted wallet.

7.8. Where an incoming stablecoin transfer is conducted without the said screening or when any of the required originator and recipient information in relation to an incoming stablecoin transfer is missing (which renders the licensee unable to conduct screening), the licensee should take appropriate risk mitigating measures, having regard to its business practices[63]. The risk mitigating measures taken by the licensee should be documented.

7.9. When possible name matches are identified during screening, a licensee should conduct enhanced checks to determine whether the possible matches are genuine hits. In case of any suspicions of TF, PF or sanctions violations, the licensee should make a report to the JFIU. Records of enhanced checking results,

---

61 Relevant parties in a stablecoin transfer include: (i) the recipient if the licensee acts as the ordering institution or the stablecoin is transferred to an unhosted wallet; (ii) the originator if the licensee acts as the beneficiary institution or the stablecoin is transferred from an unhosted wallet; or both the originator and recipient if the licensee acts as the intermediary institution.

62 A licensee should include the names of relevant parties in the screening, and should take into consideration the address, identification document number or date and place of birth of the originator (where applicable) in the screening. In addition, the licensee should observe the requirements for ongoing monitoring of stablecoin transactions and the associated wallet addresses in paragraphs 5.4, 5.5, 5.7 and 5.8 when carrying out stablecoin transfers on behalf of its customers.

63 These may include implementing controls to prevent the relevant stablecoins from being made available to the recipient, or putting the receiving wallet on hold, until the screening is completed and confirmed that no concern is raised. Please also refer to risk mitigating measures in paragraph 6.22.

together with all screening records, should be documented, or recorded electronically.

7.10. A licensee may rely on its overseas office to maintain the database or to undertake the screening process. However, the licensee is reminded that the ultimate responsibility for ensuring compliance with the relevant regulations and legislation on TF, financial sanctions and PF remains with the licensee.

8. Suspicious transaction reports

8.1. It is a statutory obligation under sections 25A(1) of the DTROP and the OSCO, as well as section 12(1) of the UNATMO, that where a person knows or suspects that any property: (a) in whole or in part directly or indirectly represents any person's proceeds of, (b) was used in connection with, or (c) is intended to be used in connection with drug trafficking or an indictable offence; or that any property is terrorist property, the person shall as soon as it is reasonable for him to do so, file an STR with the JFIU. The STR should be made together with any matter on which the knowledge or suspicion is based. Under the DTROP, the OSCO and the UNATMO, failure to report knowledge or suspicion carries a maximum penalty of imprisonment for three months and a fine of $50,000.

8.2. It is an offence ("tipping off") to reveal to any person any information which might prejudice an investigation; if a customer is told that a report has been made, this would prejudice the investigation and an offence would be committed. The tipping off provision includes circumstances where a suspicion has been raised internally within a licensee, but has not yet been reported to the JFIU. The licensee should be aware that making enquiries to customers, when conducted properly and in good faith, will not constitute tipping off. However, if the licensee reasonably believes that it will tip off the customer, it may stop pursuing the process. The licensee should document the basis for its assessment and file an STR to the JFIU.

8.3. A licensee should implement appropriate AML/CFT Systems in order to fulfil its statutory reporting obligations, and properly manage and mitigate the risks associated with any customer or transaction involved in an STR. The AML/CFT Systems should include:

(a) appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the JFIU and law enforcement agencies (see paragraph 3.5);

(b) implement clear policies and procedures over internal reporting, reporting to the JFIU, post-reporting risk mitigation and prevention of tipping off;

(c) provide sufficient guidance to its staff enable them to form suspicion or to recognise the signs when ML/TF is taking place; and

(d) keeping proper records of internal reports and STRs (see paragraph 9.9).

8.4. A licensee should have measures in place to check, on an ongoing basis, that its AML/CFT Systems in relation to suspicious transaction reporting comply with relevant legal and regulatory requirements and operate effectively. The type and extent of the measures to be taken should be appropriate having regard to the risk of ML/TF as well as the nature and size of its business.

8.5. Once knowledge or suspicion has been formed, a licensee should file an STR which should be made as soon as reasonably practical after the suspicion was first identified. An AI should ensure STRs filed to the JFIU are of high quality taking into account feedback and guidance provided by the JFIU and the HKMA from time to time.

8.6. A licensee should conduct an appropriate review of a business relationship upon the filing of an STR to the JFIU, irrespective of any subsequent feedback provided by the JFIU, and apply appropriate risk mitigating measures (e.g. to freeze or burn relevant stablecoins in accordance with requests from law enforcement agencies). Filing a report with the JFIU and continuing to operate the relationship without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified is not acceptable. If necessary, the issue should be escalated to the licensee's senior management to determine how to handle the relationship concerned to mitigate any potential legal or reputational risks posed by the relationship in line with the licensee's business objectives, and its capacity to mitigate the risks identified.

8.7. A licensee may receive various requests from law enforcement agencies, e.g. search warrants, production orders, restraint orders or confiscation orders, pursuant to relevant legislations in Hong Kong. These requests are crucial to aid law enforcement agencies to carry out investigations as well as restrain and confiscate illicit proceeds. Therefore, a licensee should establish clear policies and procedures to handle these requests in an effective and timely manner, including allocation of sufficient resources and appointing a staff as the main point of contact with law enforcement agencies.

8.8. When a licensee receives a requirement (e.g. search warrant or production order) or other types of crime-related intelligence requests including those from a law enforcement agency (e.g. notification letter) in relation to a particular customer or business relationship, the licensee should timely assess the risks involved and the need to conduct an appropriate review on the customer or the business relationship to determine whether there is any suspicion and should also be aware that the customer subject to the request can be a victim of crime.

9. Record-keeping

9.1. Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps the investigating authorities to establish a financial profile of a suspect, trace the criminal or terrorist property or funds and assists the Court to examine all relevant past transactions to assess whether the property or funds are the proceeds of or relate to criminal or terrorist offences. Record-keeping also enables a licensee to demonstrate compliance with the requirements set out in the AMLO, this Guideline and other relevant guidance promulgated by the HKMA from time to time.

9.2. The licensee should maintain CDD information, transaction records and other records that are necessary and sufficient to meet the statutory and regulatory requirements that are appropriate to the nature, size and complexity of its businesses. The licensee should ensure that:

(a) the audit trail for funds moving through the licensee that relate to any customer or any stablecoin transactions is clear and complete;

(b) all CDD information and stablecoin transaction records are available swiftly to the HKMA, other authorities and auditors upon appropriate authority; and

(c) it can demonstrate compliance with section 20 and section 21 of Schedule 2 to the AMLO and any relevant requirements specified in other sections of this Guideline and other guidelines issued by the HKMA.

9.3. A licensee should maintain the original or a copy of the documents, and a record of the data and information, obtained in connection with each transaction the licensee carries out, both domestic and international, which should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. All these documents and records should be kept for a period of at least five years after the completion of a transaction, regardless of whether the business relationship ends during the period.

9.4. A licensee should keep:

(a) the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and, where applicable, verifying the identity of the customer and/or beneficial owner of the customer and/or beneficiary and/or persons who purport to act on behalf of the customer and/or other connected parties to the customer;
(b) other documents and records obtained throughout the CDD and ongoing monitoring process, including SDD and EDD;

(c) where applicable, the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship;

(d) the original or a copy of the records and documents relating to the customer's account and business correspondence[64] with the customer and any beneficial owner of the customer (which at a minimum should include business correspondence material to CDD measures or significant changes to the operation of the account); and

(e) the results of any analysis undertaken (e.g. inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose).

9.5. All documents and records mentioned in paragraph 9.4 should be kept throughout the continuance of the business relationship with the customer and for a period of at least five years after the end of the business relationship. Similarly, for occasional transactions, a licensee should keep all documents and records mentioned in paragraph 9.4 for a period of at least five years after the date on which the occasional transaction is completed.

9.6. A licensee should keep the required originator and recipient information set out in paragraphs 6.5 and 6.6 obtained or received by the licensee in relation to a stablecoin transfer referred to in paragraphs 6.5 to 6.24, and/or the required originator and recipient information set out in paragraph 6.41 obtained by the licensee in relation to a stablecoin transfer to or from an unhosted wallet referred to in paragraphs 6.40 to 6.42, for a period of at least five years after the completion of the transfer, regardless of whether the business relationship ends during the period.

9.7. If the record consists of a document, either the original of the document should be retained or a copy of the document should be kept on microfilm or in the database of a computer. If the record consists of data or information, such record should be kept either on microfilm or in the database of a computer. Irrespective of where CDD and transaction records are held, a licensee is required to comply with all legal and regulatory requirements in Hong Kong, especially Part 3 of Schedule 2.

9.8. The HKMA may, by notice in writing to a licensee, require it to keep the records relating to a specified transaction or customer for a period specified by the HKMA that is longer than those referred to in paragraphs 9.3, 9.5 and 9.6, where

[64] A licensee is not expected to keep each and every correspondence, such as a series of emails with the customer; the expectation is that sufficient correspondence is kept to demonstrate compliance with the AMLO.

the records are relevant to an ongoing criminal or other investigation carried out by the HKMA, or to any other purposes as specified in the notice.

Record keeping in relation to STR

9.9. A licensee should establish and maintain a record of all ML/TF reports made to the MLRO. The record should include details of the date the report was made, the staff members subsequently handling the report, the results of the assessment, whether the internal report resulted in an STR to the JFIU, and information to allow the papers relevant to the report to be located. A licensee should establish and maintain a record of all STRs made to the JFIU. The record should include details of the date of the STR, the person who made the STR, and information to allow the papers relevant to the STR to be located. This register may be combined with the register of internal reports, if considered appropriate.

Records kept by intermediaries

9.10. Where customer identification and verification documents are held by an intermediary on which a licensee is relying to carry out CDD measures, the licensee concerned remains responsible for compliance with all record-keeping requirements. The licensee should ensure that the intermediary being relied on has systems in place to comply with all the record-keeping requirements under the AMLO and this Guideline (including the requirements of paragraphs 9.4 to 9.7), and that documents and records will be provided by the intermediary as soon as reasonably practicable after the intermediary receives the request from the licensee.

9.11. For the avoidance of doubt, a licensee that relies on an intermediary for carrying out a CDD measure should immediately obtain the data or information that the intermediary has obtained in the course of carrying out that measure.

9.12. A licensee should ensure that an intermediary will pass the documents and records to the licensee, upon termination of the services provided by the intermediary.