FSM Notice FSM-N27

Last revised on DD MM 2025
(Refer to endnotes for history of amendments)

Notice to licensed digital token service providers
FINANCIAL SERVICES AND MARKETS ACT 2022

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM – HOLDERS OF DIGITAL TOKEN SERVICE LICENCE

1 INTRODUCTION

1.1 This Notice is issued under section 16 of the Financial Services and Markets Act 2022 ("FSM Act") and applies to a holder of a licence granted under section 138 of the FSM Act ("digital token service provider").

1.2 This Notice takes effect from XX Month XXXX.

2 DEFINITIONS

2.1 For the purposes of this Notice –

"AML/CFT" means anti-money laundering[1] and countering the financing of terrorism;

"Authority" means the Monetary Authority of Singapore;

"bank" has the same meaning as section 2(1) of the Banking Act 1970;

"bank in Singapore" has the same meaning as in section 2(1) of the Banking Act 1970;

"bearer negotiable instrument" means –

(a) a traveller's cheque; or

(b) a negotiable instrument that is in bearer form, indorsed without any restriction, made out to a fictitious payee or otherwise in a form that title thereto passes upon delivery,

and includes a negotiable instrument that has been signed but with the payee's name omitted;

"beneficial owner", in relation to a customer of a digital token service provider, means the natural person who ultimately owns or controls the customer or the natural person on whose behalf a transaction is conducted or business relations are established, and

[1] In this Notice, money laundering includes proliferation financing, and all references in this Notice to money laundering (including money laundering risks) shall be construed accordingly.

includes a person who exercises ultimate effective control over a legal person or legal arrangement;

"beneficiary institution" means the financial institution that receives the value transfer from the ordering institution mentioned in limb (a) of the definition of "ordering institution", directly or through an intermediary institution, and makes one or more digital tokens available to the value transfer beneficiary;

"business day" means a calendar day other than a Saturday, Sunday, public holiday or bank holiday;

"business relations" means the opening or maintenance of an account by the digital token service provider for the purposes of accepting, processing or executing a transaction in the name of a person (whether a natural person, legal person or legal arrangement), in the course of carrying on its business of providing a digital token service;

"cash" means currency notes and coins (whether of Singapore or of a foreign country or jurisdiction) which are legal tender and circulate as money in the country or jurisdiction of issue;

"CDD measures" or "customer due diligence measures" means the measures required by paragraph 6;

"CDSA" means the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992;

"connected party" –

(a) in relation to a legal person (other than a partnership), means a director or a natural person having executive authority in the legal person;
(b) in relation to a legal person that is a partnership, means a partner or manager[2]; and

(c) in relation to a legal arrangement, means a natural person having executive authority in the legal arrangement;

"customer", in relation to a digital token service provider, means a person (whether a natural person, legal person or legal arrangement) –

(a) with whom business relations are established or with whom the digital token service provider intends to establish business relations; or

(b) for whom the digital token service provider undertakes or intends to undertake a transaction without an account being opened;

"FATF" means the Financial Action Task Force;

[2] In the case of a limited liability partnership or a limited partnership.

"financial group" means a group that consists of a legal person or legal arrangement exercising control and coordinating functions over the rest of the group, and its branches and subsidiaries that are financial institutions as defined in section 2 of the FSM Act or the equivalent financial institutions outside Singapore;

"FX counterparty", in relation to an FX transaction entered into by the digital token service provider, means the person on whose behalf the FX transaction is conducted;

"FX transaction" means a transaction (not being a money-changing transaction) for the purchase or sale of foreign currency without the use of foreign currency notes;

"government entity" means a government of a country or jurisdiction, a ministry within that government, or an agency specially established by that government through written law;

"legal arrangement" means a trust or other similar arrangement;

"legal person" means an entity other than a natural person that can establish a permanent customer relationship with a financial institution or otherwise own property;

"merchant bank" has the same meaning as in section 2(1) of the Banking Act 1970;

"merchant bank in Singapore" has the same meaning as in section 2(1) of the Banking Act 1970;

"officer" –

(a) in relation to a digital token service provider that is a legal person (other than a partnership), means a director or a member of the committee of management of the legal person;

(b) in relation to a digital token service provider that is a partnership, means a partner or manager; and

(c) in relation to a digital token service provider that is a legal arrangement, means a member of the committee of management of the legal arrangement;

"ordering institution" means the financial institution that:-

(a) initiates the value transfer and transfers one or more digital tokens; or

(b) arranges for the value transfer of one or more digital tokens,

upon receiving the request for a value transfer on behalf of the value transfer originator;

"partnership" means a partnership, a limited partnership within the meaning of the Limited Partnerships Act 2008 or a limited liability partnership within the meaning of the Limited Liability Partnerships Act 2005;

"personal data" has the same meaning as defined in section 2(1) of the Personal Data Protection Act 2012;

"reasonable measures" means appropriate measures which are commensurate with the level of money laundering or terrorism financing risks;

"recipient" –

(a) in relation to a digital token service provider that carries on a business of providing a digital token service, means a person (whether a natural person, legal person or legal arrangement) to whom the digital token service provider pays out funds in cash or cash equivalent and the person on behalf of whom the funds are received; or

(b) means an FX counterparty;

"relevant FX counterparty" is a FX counterparty that is not –

(a) a financial institution as defined in section 2 of the FSM Act; or

(b) a financial institution incorporated or established outside Singapore that is subject to, and supervised for compliance with, AML/CFT requirements consistent with standards set by the FATF;

"SFA" means the Securities and Futures Act 2001;

"STR" means suspicious transaction report;

"STRO" means the Suspicious Transaction Reporting Office, Commercial Affairs Department of the Singapore Police Force;

"transaction" means a transaction accepted, processed, or executed by the digital token service provider in the course of carrying on its business of providing a digital token service;

"trust relevant party" has the same meaning as defined in paragraph 2.1 of MAS Notice TCA-N03;

[MAS Notice FSM-N27 (Amendment) 2025]

"TSOFA" means the Terrorism (Suppression of Financing) Act 2002; and

"value transfer" refers to a transaction carried out on behalf of a value transfer originator through a financial institution with a view to making one or more digital tokens available to a beneficiary person at a beneficiary institution, whether or not the originator and the beneficiary are the same person.

2.2 A reference to a threshold or value limit expressed in S$ includes a reference to the equivalent amount expressed in any other currency and in any digital token. The equivalent amount in digital tokens is determined based on the conversion rates prevailing at the time of the digital token service provider's compliance with the relevant threshold or value limit, either as published by the digital token service provider in the

course of its business or offered by the digital token service provider to its customer in relation to the transaction.

2.3 Except where defined in this Notice or if the context otherwise requires, the expressions in this Notice have the same meanings as in the FSM Act.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which serves as a guide for a digital token service provider in the conduct of its operations and business activities:

(a) A digital token service provider must exercise due diligence when dealing with customers, natural persons appointed to act on the customer's behalf, connected parties of the customer and beneficial owners of the customer.

(b) A digital token service provider must conduct its business in conformity with high ethical standards, and guard against establishing any business relations or undertaking any transaction, that is or may be connected with, or facilitates or may facilitate money laundering or terrorism financing.

(c) A digital token service provider must, to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore to prevent money laundering and terrorism financing.

4 ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH

Risk assessment

4.1 A digital token service provider must take appropriate steps to identify, assess and understand, its money laundering and terrorism financing risks[3] in relation to –

(a) its customers;

(b) the countries or jurisdictions its customers are from or in;

(c) the countries or jurisdictions the digital token service provider has operations in;

(d) the products, services, transactions and delivery channels of the digital token service provider; and

(e) its branches and subsidiaries, including those outside Singapore.

4.2 The appropriate steps mentioned in paragraph 4.1 include –

(a) documenting the digital token service provider's risk assessments;

[3] For the avoidance of doubt, money laundering risks include proliferation financing risks.

(b) considering all the relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation to be applied;

(c) keeping the digital token service provider's risk assessments up-to-date; and

(d) having appropriate mechanisms to provide its risk assessment information to the Authority.

Risk Mitigation

4.3 A digital token service provider must –

(a) develop and implement policies, procedures and controls, which are approved by senior management, to enable the digital token service provider to effectively manage and mitigate the risks that have been identified by the digital token service provider or notified to it by the Authority or other relevant authorities in Singapore;

(b) monitor the implementation of those policies, procedures and controls, and enhance them if necessary;

(c) perform enhanced measures if higher risks are identified, to effectively manage and mitigate those higher risks; and

(d) ensure that the performance of measures or enhanced measures to effectively manage and mitigate the identified risks addresses the risk assessment and guidance from the Authority or other relevant authorities in Singapore.

5 NEW PRODUCTS, PRACTICES AND TECHNOLOGIES

5.1 A digital token service provider must identify and assess the money laundering and terrorism financing 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 existing products.

5.2 A digital token service provider must undertake the risk assessments, before the launch or use of the products, practices and technologies mentioned in paragraph 5.1 (to the extent the use is permitted by this Notice), and must take appropriate measures to manage and mitigate the risks.

5.3 A digital token service provider must, in complying with the requirements of paragraphs 5.1 and 5.2, pay special attention to –

(a) new products and new business practices, including new delivery mechanisms; and

(b) new or developing technologies,

that favour anonymity.

6 CUSTOMER DUE DILIGENCE ("CDD")

Anonymous or Fictitious Account

6.1 A digital token service provider must not open or maintain an anonymous account or an account in a fictitious name.

If There Are Reasonable Grounds for Suspicion before the Establishment of Business Relations or Undertaking a Transaction without opening an Account

6.2 Before a digital token service provider establishes business relations or undertakes a transaction without opening an account, if the digital token service provider has reasonable grounds to suspect that the assets or funds of a customer are proceeds of drug dealing or criminal conduct as defined in the CDSA, or are property related to the facilitation or carrying out of a terrorism financing offence as defined in the TSOFA, the digital token service provider must –

(a) not establish business relations with, or undertake a transaction for, the customer; and

(b) file an STR[4], and extend a copy to the Authority ~~for information~~ upon request.

[MAS Notice FSM-N27 (Amendment) 2025]

When CDD is to be Performed

6.3 A digital token service provider must perform the measures as required by paragraphs 6, 7 and 8 when –

(a) the digital token service provider establishes business relations with a customer;

(b) the digital token service provider undertakes a transaction for a customer who has not otherwise established business relations with the digital token service provider;

(c) the digital token service provider effects the sending of, receives, or arranges for the transfer of, one or more digital tokens by value transfer, for a customer who has not otherwise established business relations with the digital token service provider;

[4] Please note in particular section 57 of the CDSA on tipping-off.

(d) there is a suspicion of money laundering or terrorism financing, even though the digital token service provider would not otherwise be required by this Notice to perform the measures as required by paragraphs 6, 7 and 8; or

(e) the digital token service provider has doubts about the veracity or adequacy of information previously obtained.

6.4 If a digital token service provider suspects that two or more transactions are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for in this Notice, the digital token service provider must treat the transactions as a single transaction and aggregate their values for the purpose of this Notice.

(I) Identification of Customer

6.5 A digital token service provider must identify each customer.

6.6 For the purposes of paragraph 6.5, a digital token service provider must obtain at least the following information:

(a) where the customer is a natural person, his or her –

~~(a)~~(i) full name, including any aliases;

~~(b)~~(ii) unique identification number (such as an identity card number, birth certificate number or passport number~~, or where the customer is not a natural person, the incorporation number or business registration number)~~;

~~(c)~~(iii) ~~the customer's~~ residential address;

~~(i) residential address; or~~

~~(ii) registered or business address, and if different, principal place of business,~~

~~as may be appropriate;~~

~~(d)~~(iv) date of birth~~, constitution, incorporation or registration (as may be appropriate)~~; ~~and~~

~~(e)~~(v) nationality~~, place of incorporation or place of registration (as may be appropriate).~~; and

(b) where the customer is a legal person or legal arrangement –

(i) its full name;

(ii) its incorporation number, business registration number or tax identification number or its equivalent;

(iii) its registered or business address, and if different, its principal place of business;

(iv) its date of constitution, incorporation or registration;

(v) its place of incorporation or registration;

(vi) a copy of the trust deed (or its equivalent)(if any);

(vii) the purpose for which the legal person or legal arrangement was set up;

(viii) the place from where the legal person or legal arrangement is administered; and

(x) the legal form, constitution, and powers that regulate and bind the legal person or legal arrangement.

[MAS Notice FSM-N27 (Amendment) 2025]

6.7 ~~If the customer is a legal person or legal arrangement, the digital token service provider must, apart from identifying the customer, also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement.~~

Deleted with effect from DD MM 2025.

[MAS Notice FSM-N27 (Amendment) 2025]

6.8 If the customer is a legal person or legal arrangement, the digital token service provider must identify the connected parties of the customer, by obtaining at least the following information of each connected party:

(a) full name, including any aliases; and

(b) unique identification number (such as an identity card number, birth certificate number or passport number of the connected party).

6.9 If the digital token service provider –

(a) has assessed that the money laundering and terrorism financing risks in relation to the customer are not high; and

(b) is unable to obtain the unique identification number of the connected party after taking reasonable measures,

the digital token service provider may obtain the date of birth and nationality of the connected party, in lieu of the unique identification number.

6.10 The digital token service provider must document the results of the assessment in paragraph 6.9(a) and the measures taken under paragraph 6.9(b).

(II) Verification of Identity of Customer and information relating to the Legal Arrangement

6.11 A digital token service provider must verify the identity of the customer using reliable, independent source data, documents or information. If the customer is a legal person or legal arrangement, a digital token service provider must verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable, independent source data, documents or information.

(III) Identification and Verification of Identity of Natural Person Appointed to Act on a Customer's Behalf

6.12 If a customer appoints one or more natural persons to act on the customer's behalf in establishing business relations with a digital token service provider ~~or the customer is not a natural person~~, the digital token service provider must –

(a) identify the natural persons who act or are appointed to act on behalf of the customer by obtaining at least the following information of each natural person:

(i) full name, including any aliases;

(ii) unique identification number (such as an identity card number, birth certificate number or passport number);

(iii) residential address;

(iv) date of birth;

(v) nationality; and

(b) verify the identity of the natural persons using reliable, independent source data, documents or information.

[MAS Notice FSM-N27 (Amendment) 2025]

6.13 A digital token service provider must verify the due authority of each natural person appointed to act on behalf of the customer by:-

(a) obtaining appropriate documentary evidence authorising the appointment of each natural person by the customer to act on the customer's behalf; and

(b) verifying that each natural person is the person authorised to act on the customer's behalf, through methods which include obtaining the person's specimen signature or electronic means of verification.

6.14 If the digital token service provider –

(a) has assessed that the money laundering and terrorism financing risks of the customer are not high; and

(b) is unable to obtain the residential address of a natural person who acts or is appointed to act on behalf of the customer after taking reasonable measures,

the digital token service provider may obtain the business address of this natural person, in lieu of the residential address.

6.15 If the digital token service provider has obtained the business address of the natural person mentioned in paragraph 6.14, the digital token service provider must take reasonable measures to verify the business address using reliable, independent source data, documents or information.

6.16 The digital token service provider must document the results of the assessment in paragraph 6.14(a) and the measures taken under paragraph 6.14(b).

6.17 If the customer is a Singapore government entity, the digital token service provider is only required to obtain the information as may be required to confirm that the customer is a Singapore government entity as asserted.

(IV) Identification and Verification of Identity of Beneficial Owner

6.18 Subject to paragraph 6.21, a digital token service provider must inquire if there exists a beneficial owner in relation to a customer.

6.19 If there is one or more beneficial owners in relation to a customer, the digital token service provider must identify the beneficial owners ~~and take reasonable measures to verify the identities of the beneficial owners using the relevant information or data obtained from reliable, independent sources. The digital token service provider must~~, as follows–

(a) for customers that are legal persons –

(i) identify the natural persons (whether acting alone or together) who ultimately own the legal person;

(ii) to the extent that there is doubt under subparagraph (i) whether the natural persons who ultimately own the legal person are the beneficial owners or if no natural persons ultimately own the legal person, identify the natural

persons (if any) who ultimately control the legal person or have ultimate effective control of the legal person; and

(iii) if no natural persons are identified under subparagraphs (i) or (ii), identify the natural persons having executive authority in the legal person, or in equivalent or similar positions;

(b) for customers that are legal arrangements –

(i) for trusts, identify the ~~settlors, the trustees, the protector (if any), the beneficiaries (including beneficiaries that fall within a designated characteristic or class)[5], and natural persons exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership)~~ trust relevant parties; and

(ii) for other types of legal arrangements, identify persons in equivalent or similar positions, as ~~those~~ described under subparagraph (i).

[MAS Notice FSM-N27 (Amendment) 2025]

6.19A For the purposes of paragraph 6.19, the digital token service provider shall obtain at least the following information:

(a) where the beneficial owner is a natural person, his or her –

(i) full name, including any aliases;

(ii) unique identification number (such as an identity card number, birth certificate number or passport number);

(iii) residential address;

(iv) date of birth; and

(v) nationality.

(b) where the beneficial owner is a legal person or legal arrangement –

(i) its full name;

(ii) its incorporation number, business registration number or tax identification number or its equivalent;

~~[5] In relation to a beneficiary of a trust designated by characteristics or by class, the digital token service provider shall obtain sufficient information about the beneficiary to satisfy itself that it will be able to establish the identity of the beneficiary –~~

~~(a) before making a distribution to that beneficiary; or~~

~~(b) when that beneficiary intends to exercise vested rights.~~

(iii) its registered or business address, and if different, its principal place of business;

(iv) its date of constitution, incorporation or registration;

(v) its place of incorporation or registration;

(vi) a copy of the trust deed (or its equivalent)(if any);

(vii) the purpose for which the legal person or legal arrangement was set up;

(viii) the place from where the legal person or legal arrangement is administered; and

(ix) the legal form, constitution and powers that regulate and bind the legal person or legal arrangement.

[MAS Notice FSM-N27 (Amendment) 2025]

6.19B A digital token service provider shall verify the identity of each beneficial owner using reliable, independent source data, documents or information. Where the beneficial owner is a legal person or legal arrangement, a digital token service provider shall verify the legal form, proof of existence, constitution and powers that regulate and bind the beneficial owner, using reliable, independent source data, documents or information.

[MAS Notice FSM-N27 (Amendment) 2025]

6.20 If the customer is not a natural person, the digital token service provider must understand the nature of the customer's business and its ownership and control structure.

6.21 A digital token service provider is not required to inquire if there exists a beneficial owner, in relation to a customer that is –

(a) an entity listed and traded on the Singapore Exchange;

(b) an entity listed on a stock exchange outside of Singapore that is subject to –

(i) regulatory disclosure requirements; and

(ii) requirements relating to adequate transparency in respect of its beneficial owners (imposed through stock exchange rules, law or other enforceable means);

(c) a financial institution set out in Appendix 1;

(d) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; or

(e) an investment vehicle where the managers are financial institutions –

(i) set out in Appendix 1; or

(ii) incorporated or established outside Singapore but are subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF,

unless the digital token service provider has doubts about the veracity of the CDD information, or suspects that the customer, business relations with, or transaction for the customer, may be connected with money laundering or terrorism financing.

6.22 For the purposes of paragraphs 6.21(d) and 6.21(e)(ii), a digital token service provider must document the basis for its determination that the requirements in those paragraphs have been duly complied with.

(V) Information on the Purpose and Intended Nature of Business Relations and Transaction Undertaken without an Account being Opened

6.23 A digital token service provider must, when processing the application to establish business relations, or undertaking a transaction without an account being opened, understand and as appropriate, obtain from the customer information as to the purpose and intended nature of business relations or transaction.

(VI) Review of Transactions Undertaken without an Account being Opened

6.24 If a digital token service provider undertakes one or more transactions for a customer without an account being opened ("current transaction"), the digital token service provider must review the earlier transactions undertaken by that customer to ensure that the current transaction is consistent with the digital token service provider's knowledge of the customer, its business and risk profile and if appropriate, the source of funds.

6.25 If a digital token service provider establishes business relations with a customer, the digital token service provider must review transactions undertaken before the business relations are established, to ensure that the business relations are consistent with the digital token service provider's knowledge of the customer, its business and risk profile and if appropriate, the source of funds.

6.26 A digital token service provider must pay special attention to all complex, unusually large or unusual patterns of transactions undertaken without an account being opened that have no apparent or visible economic or lawful purpose.

6.27 For the purposes of reviewing transactions undertaken without an account being opened as required by paragraph 6.24, a digital token service provider must put in place and implement adequate systems and processes, commensurate with the size and complexity of the digital token service provider to –

(a) monitor its transactions undertaken without an account being opened for customers; and

(b) detect and report suspicious, complex, unusually large or unusual patterns of transactions undertaken without an account being opened.

6.28 A digital token service provider must, to the extent possible, inquire into the background and purpose of the transactions in paragraph 6.26 and document its findings with a view to making this information available to the relevant authorities should the need arise.

6.29 If there are reasonable grounds for suspicion that a transaction for a customer undertaken without an account being opened is connected with money laundering or terrorism financing, and if the digital token service provider considers it appropriate to undertake the transaction, the digital token service provider must substantiate and document the reasons for undertaking the transaction.

(VII) Ongoing Monitoring

6.30 A digital token service provider must monitor on an ongoing basis, its business relations with customers.

6.31 A digital token service provider must, during the course of business relations with a customer, observe the conduct of the customer's account and scrutinise transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with the digital token service provider's knowledge of the customer, its business and risk profile and if appropriate, the source of funds.

6.32 A digital token service provider must perform enhanced risk mitigation measures if the transaction involves a transfer of one or more digital tokens to or a receipt of one or more digital tokens from an entity other than:

(a) a financial institution as defined in section 2 of the FSM Act; or

(b) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

6.33 A digital token service provider must pay special attention to all complex, unusually large or unusual patterns of transactions, undertaken throughout the course of business relations, that have no apparent or visible economic or lawful purpose.

6.34 For the purposes of ongoing monitoring, a digital token service provider must put in place and implement adequate systems and processes, commensurate with the size and complexity of the digital token service provider to –

(a) monitor its business relations with customers; and

(b) detect and report suspicious, complex, unusually large or unusual patterns of transactions undertaken throughout the course of business relations.

6.35 A digital token service provider must, to the extent possible, inquire into the background and purpose of the transactions in paragraph 6.33 and document its findings with a view to making this information available to the relevant authorities should the need arise,

6.36 A digital token service provider must ensure that the CDD data, documents and information obtained in respect of customers, natural persons appointed to act on behalf of the customers, connected parties of the customers and beneficial owners of the customers, are relevant and kept up-to-date by undertaking reviews of existing CDD data, documents and information, particularly for higher risk categories of customers.

6.37 If there are reasonable grounds for suspicion that existing business relations with a customer are connected with money laundering or terrorism financing, and if the digital token service provider considers it appropriate to retain the customer –

(a) the digital token service provider must substantiate and document the reasons for retaining the customer; and

(b) the customer's business relations with the digital token service provider must be subject to commensurate risk mitigation measures, including enhanced ongoing monitoring.

6.38 If the digital token service provider assesses the customer or the business relations with the customer mentioned in paragraph 6.37 to be of higher risk, the digital token service provider must perform enhanced CDD measures, which must include obtaining the approval of the digital token service provider's senior management to retain the customer.

CDD Measures for Non-Face-to-Face Business Relations or Non-Face-to-Face Transactions Undertaken without an Account Being Opened

6.39 A digital token service provider must develop policies and procedures to address specific risks associated with non-face-to-face business relations with a customer or non-face-to-face transactions undertaken without an account being opened for a customer ("non-face-to-face business contact").

6.40 A digital token service provider must implement the policies and procedures mentioned in paragraph 6.39 when establishing business relations with a customer and when conducting ongoing due diligence.

6.41 If there is no face-to-face contact, the digital token service provider must perform CDD measures that are at least as robust as those that would be required to be performed if there was face-to-face contact.

6.42 Where a digital token service provider conducts its first non-face-to-face business contact, the digital token service provider must, at the digital token service provider's own expense, appoint an external auditor or an independent qualified consultant to assess the effectiveness of the policies and procedures mentioned in paragraph 6.39, including the effectiveness of technology solutions used to manage impersonation risks.

6.43 The digital token service provider must submit to the Authority a report of the assessment no later than one year after conduct of the digital token service provider's non-face-to-face business contact.

6.44 If there has been a substantial change in the policies and procedures mentioned in paragraph 6.39, the digital token service provider must appoint an external auditor or an independent qualified consultant to carry out an assessment of the new policies and procedures, and must submit the report of the assessment to the Authority no later than one year after the implementation of the change in policies and procedures.

Reliance by Acquiring Digital Token Service Provider on Measures Already Performed

6.45 When a digital token service provider ("acquiring digital token service provider") acquires, either in whole or in part, the business of another financial institution (whether in Singapore or elsewhere), the acquiring digital token service provider must perform the measures as required by paragraphs 6, 7 and 8, on the customers acquired with the business at the time of acquisition except if the acquiring digital token service provider has –

(a) acquired at the same time the corresponding customer records (including CDD information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and

(b) conducted due diligence enquiries that have not raised doubt on the part of the acquiring digital token service provider as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring digital token service provider, and document the enquiries.

Measures for Non-Account Holder

6.46 A digital token service provider that undertakes a transaction for a customer who does not otherwise have business relations with the digital token service provider must –

(a) perform CDD measures as if the customer had applied to the digital token service provider to establish business relations; and

(b) record adequate details of the relevant transaction so as to permit the reconstruction of the transaction, including the nature and date of the transaction, the type and amount of currency involved, the value date, and the details of the payee or beneficiary.

Timing for Verification

6.47 Subject to paragraphs 6.48 and 6.49, a digital token service provider must complete verification of the identity of a customer as required by paragraph 6.11, natural persons appointed to act on behalf of the customer as required by paragraph 6.12(b) and beneficial owners of the customer as required by paragraph 6.19B –

(a) before the digital token service provider establishes business relations with the customer;
(b) before the digital token service provider undertakes a transaction for the customer, if the customer has not otherwise established business relations with the digital token service provider; or

(c) before the digital token service provider effects the sending of, receives, or arranges for the transfer of, one or more digital tokens by value transfer for the customer, if the customer has not otherwise established business relations with the digital token service provider.

[MAS Notice FSM-N27 (Amendment) 2025]

6.48 A digital token service provider may establish business relations with a customer before completing the verification of the identity of the customer as required by paragraph 6.11, natural persons appointed to act on behalf of the customer as required by paragraph 6.12(b) and beneficial owners of the customer as required by paragraph 6.19B if –

(a) the deferral of completion of the verification is essential in order not to interrupt the normal conduct of business operations; and

(b) the risks of money laundering and terrorism financing can be effectively managed by the digital token service provider.

[MAS Notice FSM-N27 (Amendment) 2025]

6.49 If the digital token service provider establishes business relations with a customer before verifying the identity of the customer as required by paragraph 6.11, natural persons appointed to act on behalf of the customer as required by paragraph 6.12(b), and beneficial owners of the customer as required by paragraph 6.19B, the digital token service provider must –

(a) develop and implement internal risk management policies and procedures concerning the conditions under which the business relations may be established before verification; and

(b) complete the verification as soon as is reasonably practicable.

[MAS Notice FSM-N27 (Amendment) 2025]

If Measures are Not Completed

6.50 If the digital token service provider is unable to complete the measures as required by paragraphs 6, 7 and 8, it must not commence or continue business relations with a customer, or undertake a transaction for a customer.

6.51 If the digital token service provider is unable to complete the measures as required by paragraphs 6, 7 and 8, the digital token service provider must consider if the circumstances are suspicious so as to warrant the filing of an STR.

6.52 For the purposes of paragraphs 6.50 and 6.51, completion of the measures means the situation where the digital token service provider has obtained, screened and verified (including by delayed verification as allowed under paragraphs 6.48 and 6.49) all necessary CDD information required under paragraphs 6, 7 and 8, and if the digital token service provider has received satisfactory responses to all the inquiries in relation to the necessary CDD information.

Joint Account

6.53 In the case of a joint account, a digital token service provider must perform CDD measures on all of the joint account holders as if each of them is an individual customer of the digital token service provider.

Existing Customers

6.54 Where a digital token service provider has a Pre-License Customer, the digital token service provider must perform the measures as required by paragraphs 6, 7 and 8 in relation to the Pre-Licence Customer within a time period to be determined by the Authority, from the date the digital token service provider obtained its licence under section 138 of the FSM Act. For the purpose of this paragraph 6.47, a “Pre-Licence

Customer" means a customer who had established business relations with the digital token service provider prior to the digital token service provider holding a licence under section 138 of the FSM Act, and who continues to be a customer upon the digital token service provider obtaining its licence under section 138 of the FSM Act.

6.55 Where there is any subsequent revision to this Notice resulting in a change in the measures as required under paragraphs 6, 7 and 8, a digital token service provider must perform the measures as required by paragraphs 6, 7 and 8 in relation to its existing customers, based on its own assessment of materiality and risk, taking into account any previous measures applied, the time when the measures were last applied to such existing customers and the adequacy of data, documents or information obtained.

Screening

6.56 A digital token service provider must screen a customer, natural persons appointed to act on behalf of the customer, connected parties of the customer and beneficial owners of the customer against relevant money laundering and terrorism financing information sources, as well as lists and information provided by the Authority and other relevant authorities in Singapore for the purposes of determining if there are any money laundering or terrorism financing risks in relation to the customer.

6.57 A digital token service provider must screen the persons mentioned in paragraph 6.56 –

(a) when, or as soon as reasonably practicable after, the digital token service provider establishes business relations with a customer;

(b) before the digital token service provider undertakes a transaction for a customer who has not otherwise established business relations with the digital token service provider;

(c) before the digital token service provider effects the sending of, receives, or arranges for the transfer of, one or more digital tokens by value transfer, for a customer who has not otherwise established business relations with the digital token service provider;

(d) on a periodic basis after the digital token service provider establishes business relations with the customer; and

(e) when there is any change or update to –

(i) the lists and information provided by the Authority and other relevant authorities in Singapore to the digital token service provider; or

(ii) the natural persons appointed to act on behalf of a customer, connected parties of a customer or beneficial owners of a customer.

6.58 A digital token service provider must screen the value transfer originator and value transfer beneficiary as defined in paragraph 14, against lists and information provided by the Authority and other relevant authorities in Singapore for the purposes of determining if there are any money laundering or terrorism financing risks in relation to the person.

6.59 The results of screening and assessment by the digital token service provider must be documented.

7 SIMPLIFIED CUSTOMER DUE DILIGENCE

7.1 Subject to paragraph 7.4, a digital token service provider may perform simplified CDD measures in relation to a customer, a natural person appointed to act on behalf of the customer and a beneficial owner of the customer (other than a beneficial owner that the digital token service provider is exempted from making inquiries about under paragraph 6.21) if it is satisfied that the risks of money laundering and terrorism financing are low.

7.2 The assessment of low risks must be supported by an adequate analysis of risks by the digital token service provider.

7.3 The simplified CDD measures must be commensurate with the level of risk, based on the risk factors identified by the digital token service provider.

7.4 A digital token service provider must not perform simplified CDD measures –

(a) if one or more transactions undertaken, whether in the course of business relations or otherwise, by the digital token service provider for a customer in any one year period cumulatively exceeds S$20,000[6];

(b) if a customer or a beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures;

(c) if a customer or a beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the digital token service provider for itself, or notified to digital token service providers generally by the Authority, or other foreign regulatory authorities; or

(d) if the digital token service provider suspects that money laundering or terrorism financing is involved.

7.5 Subject to paragraphs 7.2, 7.3 and 7.4, a digital token service provider may perform simplified CDD measures in relation to a customer that is a financial institution set out in Appendix 2.

[6] Please note paragraph 6.4 of the Notice.

7.6 If the digital token service provider performs simplified CDD measures in relation to a customer, a natural person appointed to act on behalf of the customer and a beneficial owner of the customer, it must document –

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

7.7 To avoid doubt, the term "CDD measures" in paragraph 7 means the measures required by paragraph 6.

8 ENHANCED CUSTOMER DUE DILIGENCE

8.1 For the purposes of paragraph 8 –

"close associate" means a natural person who is closely connected to a politically exposed person, either socially or professionally;

"domestic politically exposed person" means a natural person who is or has been entrusted domestically with prominent public functions;

"family member" means a parent, step-parent, child, step-child, adopted child, spouse, sibling, step-sibling and adopted sibling of the politically exposed person;

"foreign politically exposed person" means a natural person who is or has been entrusted with prominent public functions in a foreign country or jurisdiction;

"international organisation" means an entity established by formal political agreements between member countries or jurisdictions that have the status of international treaties, whose existence is recognised by law in member countries or jurisdictions and which is not treated as a resident institutional unit of the country or jurisdiction in which it is located;

"international organisation politically exposed person" means a natural person who is or has been entrusted with prominent public functions in an international organisation;

"politically exposed person" means a domestic politically exposed person, foreign politically exposed person or international organisation politically exposed person; and

"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil or public servants, senior judicial or military officials, senior executives of state owned corporations, senior political party officials, members of the legislature and senior management of international organisations.

8.2 A digital token service provider must implement appropriate internal risk management systems, policies, procedures and controls to determine if a customer, a natural person appointed to act on behalf of the customer, a connected party of the customer or a

beneficial owner of the customer is a politically exposed person, or a family member or close associate of a politically exposed person.

8.3 A digital token service provider must, in addition to performing CDD measures (specified in paragraph 6), perform at least the following enhanced CDD measures if a customer or a beneficial owner of the customer is determined by the digital token service provider to be a politically exposed person, or a family member or close associate of a politically exposed person under paragraph 8.2:

(a) obtain approval from the digital token service provider's senior management to establish or continue business relations with the customer or undertake transactions without an account being opened for the customer;

(b) establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer and the beneficial owners of the customer; and

(c) conduct, during the course of business relations with the customer, enhanced monitoring of the business relations with the customer. In particular, the digital token service provider must increase the degree and nature of monitoring of the business relations with and transactions for the customer, in order to determine whether they appear unusual or suspicious.

8.4 A digital token service provider may adopt a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for –

(a) domestic politically exposed persons, their family members and close associates;

(b) international organisation politically exposed persons, their family members and close associates; or

(c) politically exposed persons who have stepped down from their prominent public functions, taking into consideration the level of influence the persons may continue to exercise after stepping down from their prominent public functions, their family members and close associates,

except in cases where their business relations with the digital token service provider or transaction without an account being opened by the digital token service provider present a higher risk for money laundering or terrorism financing.

Other Higher Risk Categories

8.5 A digital token service provider must implement appropriate internal risk management systems, policies, procedures and controls to determine if business relations with or

transactions undertaken without an account being opened for a customer present a higher risk for money laundering or terrorism financing.

8.6 For the purposes of paragraph 8.5, circumstances where a customer presents or may present a higher risk for money laundering or terrorism financing include but are not limited to the following:

(a) if a customer or a beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures, the digital token service provider must treat any business relations with or transactions for the customer as presenting a higher risk for money laundering or terrorism financing;

(b) if a customer or a beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the digital token service provider for itself, or notified to digital token service providers generally by the Authority or other foreign regulatory authorities, the digital token service provider must assess whether the customer presents a higher risk for money laundering or terrorism financing; and

(c) if a customer is a legal person for which the digital token service provider is not able to establish if it has any –

(i) ongoing, apparent or visible operation or business activity;

(ii) economic or business purpose for its corporate structure or arrangement; or

(iii) substantive financial activity in its interactions with the digital token service provider,

the digital token service provider must assess whether the customer presents a higher risk for money laundering or terrorism financing.

8.7 A digital token service provider must perform the appropriate enhanced CDD measures in paragraph 8.3 for business relations with, or transactions for a customer –

(a) who the digital token service provider determines under paragraph 8.5; or

(b) the Authority or other relevant authorities in Singapore notify to the digital token service provider,

as presenting a higher risk for money laundering or terrorism financing.

8.8 A digital token service provider must, in taking enhanced CDD measures to manage and mitigate any higher risks that have been identified by the digital token service provider, or notified to it by the Authority or other relevant authorities in Singapore, ensure that the enhanced CDD measures take into account the requirements of laws, regulations or

directions administered by the Authority, including but not limited to the regulations or directions issued by the Authority under section 192 read with section 15(1)(b) of the FSM Act, and section 15(1)(a) of the FSM Act, respectively.

9 FOREIGN CURRENCY EXCHANGE TRANSACTIONS

9.1 If the value of an FX transaction is equal to or exceeds S$20,000 (or its equivalent in a foreign currency), a digital token service provider must comply with paragraphs 6, 7, and 8 in relation to an FX transaction as if the references to a customer and transaction in those paragraphs were references to a relevant FX counterparty and the FX transaction respectively.

9.2 For the purposes of paragraph 9 read with paragraphs 6, 7 and 8 –

"business relations" means the opening or maintenance of an account by the digital token service provider in the name of a person (whether a natural person, legal person or legal arrangement).

9.3 In addition to performing CDD measures, a digital token service provider must, to the extent possible, inquire into the background and purpose of every FX transaction the value of which is equal to or exceeds S$20,000 (or its equivalent in a foreign currency) and document its findings with a view to making this information available to the relevant authorities should the need arise.

10 ISSUANCE OF BEARER NEGOTIABLE INSTRUMENTS AND RESTRICTION OF CASH PAYOUT

Prohibition of Issuance of Bearer Negotiable Instruments

10.1 A digital token service provider must not in the course of carrying on its business to provide a digital token service or an FX transaction make payment for a sum of money in the form of a bearer negotiable instrument to a recipient or to a person appointed to act on behalf of a recipient.

Restriction on Cash Payouts by Digital Token Service Providers

10.2 A digital token service provider must not, in respect of a payment transaction processed, accepted, or executed in the course of carrying on its business to provide a digital token service, or an FX transaction, pay cash in an amount that is equal to or exceeds S$20,000 to a recipient or person appointed to act on behalf of a recipient

10.3 If a digital token service provider suspects that two or more payment transactions or FX transactions, as the case may be, are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for in paragraph 10.2, the digital token service provider must treat

the payment transactions or FX transactions, as the case may be, as a single transaction and aggregate their value for the purposes of paragraph 10.2.

10.4 A digital token service provider may make a payment of S$20,000 and above by cheque if the following conditions are complied with:

(a) the cheque is crossed and made payable to a customer who is an account holder with a bank in Singapore;

(b) the digital token service provider maintains a register of all crossed cheques issued with the corresponding transaction reference numbers.

11 RELIANCE ON THIRD PARTIES

11.1 For the purposes of paragraph 11, "third party" means –

(a) a financial institution set out in Appendix 2;

(b) a financial institution which is subject to and supervised by a foreign authority for compliance with AML/CFT requirements consistent with standards set by the FATF (other than a foreign FI); and

(c) the parent entity, the branches and subsidiaries of the parent entity, and other related corporations, of a digital token service provider (other than an Entity X).

(d) For the purposes of sub-paragraphs (b) and (c) –

"Foreign FI" means a financial institution which (i) is subject to and supervised by a foreign authority for compliance with AML/CFT requirements consistent with standards set by FATF; (ii) holds a licence equivalent to a payment services license under the Payment Services Act or a digital token service provider license under the FSM Act; and (iii) does not hold any other financial services licence other than the licence mentioned in (ii) .

"Entity X" means an entity which (i) holds a payment services license under the Payment Services Act or a digital token service provider license under the FSM Act, or equivalent licences; and (iii) does not hold any other financial services licence other than the licence mentioned in (i).

11.2 Subject to paragraph 11.3, a digital token service provider may rely on a third party to perform the measures as required by paragraphs 6, 7 and 8 if the following requirements are complied with:

(a) the digital token service provider is satisfied that the third party it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate AML/CFT measures in place to comply with those requirements;

(b) the digital token service provider takes appropriate steps to identify, assess and understand the money laundering and terrorism financing risks particular to the countries or jurisdictions that the third party operates in;

(c) the third party is not one which digital token service providers have been specifically precluded by the Authority from relying upon; and

(d) the third party is able and willing to provide, without delay, upon the digital token service provider's request, data, documents or information obtained by the third party with respect to the measures applied on the digital token service provider's customer, which the digital token service provider would be required or would want to obtain.

11.3 A digital token service provider must not rely on a third party to conduct ongoing monitoring of business relations with customers.

11.4 If a digital token service provider relies on a third party to perform the measures as required by paragraphs 6, 7 and 8, it must –

(a) document the basis for its satisfaction that the requirements in paragraphs 11.2(a) and (b) have been complied with, except if the third party is a financial institution set out in Appendix 2; and

(b) immediately obtain from the third party the CDD information which the third party had obtained.

11.5 To avoid doubt, despite the reliance upon a third party, the digital token service provider remains responsible for its AML/CFT obligations in this Notice.

12 CORRESPONDENT ACCOUNTS

12.1 Paragraph 12 applies to a digital token service provider when either of the following occurs:

(a) it provides correspondent account services or other similar services to a financial institution that is operating in or outside Singapore; or

(b) it engages a financial institution that is operating in or outside Singapore to provide or to facilitate the provision of correspondent account services or other similar services, if such financial institution is not –

(i) a bank in Singapore; or

(ii) a merchant bank in Singapore.

12.2 For the purposes of paragraph 12 –

"correspondent account services" means:

(a) the provision of digital token services by a digital token service provider to a respondent financial institution, whether for the respondent financial institution as principal or for that respondent financial institution's customers;

(b) the provision of digital token services, or the facilitation thereof, by a correspondent financial institution to a digital token service provider, whether for the digital token service provider as principal or for that digital token service provider's customers;

"correspondent financial institution" means a financial institution that provides or facilitates the provision of correspondent account services or other similar services to the digital token service provider;

"payable-through account" means an account maintained with the digital token service provider by the respondent financial institution for the provision of correspondent account services, but which is accessible directly by a third party to effect transactions on its own behalf;

"respondent financial institution" means a financial institution to which correspondent account services or other similar services are provided by a digital token service provider;

"shell financial institution" means a financial institution incorporated, formed or established in a country or jurisdiction where the financial institution has no physical presence and which is unaffiliated with a financial group that is subject to effective consolidated supervision; and

"similar services" include:

(a) services undertaken for transactions or funds transfers, for the respondent financial institution, whether as principal or for its customers; and

(b) services undertaken for transactions or funds transfers, for the digital token service provider for whom a correspondent financial institution provides correspondent account services to, whether as principal or for its customers.

12.3 A digital token service provider in Singapore must perform the following measures, in addition to CDD measures as required by paragraphs 6, 7 and 8, when providing correspondent account services or other similar services:

(a) assess the suitability of the respondent financial institution by taking the following steps:

(i) gather adequate information about the respondent financial institution to understand fully the nature of the respondent financial institution's business,

including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;

(ii) determine from available sources the reputation of the respondent financial institution and the quality of supervision over the respondent financial institution, including whether it has been the subject of money laundering or terrorism financing investigation or regulatory action; and

(iii) assess the respondent financial institution's AML/CFT controls and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent financial institution operates;

(b) clearly understand and document the respective AML/CFT responsibilities of the digital token service provider and the respondent financial institution; and

(c) obtain approval from the digital token service provider's senior management before providing correspondent account services or similar services to a new respondent financial institution.

12.4 If the provision of correspondent account services or similar services by the digital token service provider involve a payable-through account, the digital token service provider must be satisfied that –

(a) the respondent financial institution has performed appropriate measures at least equivalent to those specified in paragraph 6 on the third party having direct access to the payable-through account; and

(b) the respondent financial institution is able to perform ongoing monitoring of its business relations with that third party and is willing and able to provide CDD information to the digital token service provider upon request.

12.5 A digital token service provider in Singapore must perform the following measures, in addition to CDD measures as required by paragraphs 6, 7 and 8, when receiving correspondent account services or other similar services:

(a) assess the suitability of the correspondent financial institution by taking the following steps:

(i) gather adequate information about the correspondent financial institution to understand fully the nature of the correspondent financial institution's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;

(ii) determine from available sources the reputation of the correspondent financial institution and the quality of supervision over the correspondent

financial institution, including whether it has been the subject of money laundering or terrorism financing investigation or regulatory action; and

(iii) assess the correspondent financial institution's AML/CFT controls and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the correspondent financial institution operates;

(b) clearly understand and document the respective AML/CFT responsibilities of the digital token service provider and the correspondent financial institution; and

(c) obtain approval from the digital token service provider's senior management before receiving correspondent account services or similar services from a new financial institution.

12.6 The digital token service provider must document the basis for its satisfaction that the requirements in paragraphs 12.3 to 12.5 are complied with.

12.7 A digital token service provider must not enter into or continue correspondent account services or other similar services relationship with another financial institution that does not have adequate controls against money laundering or terrorism financing activities, is not effectively supervised by the relevant authorities or is a shell financial institution.

12.8 A digital token service provider must also take appropriate measures when establishing correspondent account services or other similar services relationship, to satisfy itself that its respondent or correspondent financial institutions do not permit their accounts to be used by shell financial institutions.

12.9 A digital token service provider must maintain a current list of the financial institutions that it provides or receives correspondent account services or other similar services. The digital token service provider must make the list accessible to the Authority and to other relevant authorities in the countries or jurisdictions where the financial institutions operate, upon request.

13 AGENCY ARRANGEMENTS

13.1 For the purposes of paragraph 13, "agent" means a natural person or legal person (that is not a financial institution) that contracts with or is under the direction of the digital token service provider to assist in the provision of digital token service, but does not itself carry on the business of digital token service.

13.2 A digital token service provider must not appoint an agent unless the following requirements are complied with:

(a) the agency arrangement is documented in writing and approved by the senior management of the digital token service provider;

(b) the digital token service provider takes appropriate steps to identify, assess and understand the money laundering or terrorism financing risks particular to the countries or jurisdictions that the agent operates in;

(c) the agent is not one which digital token service providers have been specifically precluded by the Authority from appointing; and

(d) the digital token service provider includes all its agents in its AML/CFT programme and monitors them for compliance with its programme.

13.3 The digital token service provider must document the basis for its satisfaction that the requirements in paragraph 13 are complied with.

13.4 The digital token service provider must maintain a current list of its agents that it engages and must make the list accessible to the Authority and to other relevant authorities in the countries or jurisdictions where the agents operate, upon request.

14 VALUE TRANSFERS

14.1 Paragraph 14 applies to a digital token service provider when it:

(a) effects the sending of one or more digital tokens by value transfer on the account of the value transfer originator;

(b) receives one or more digital tokens by value transfer on the account of the value transfer beneficiary; or

(c) arranges for the value transfer of one or more digital tokens;

but does not apply to a transfer and settlement between the digital token service provider and another financial institution if the digital token service provider and the other financial institution are acting on their own behalf as the value transfer originator and the value transfer beneficiary.

14.2 For the purposes of paragraph 14 –

"batch transfer" means a transfer comprising a number of individual value transfers that are sent by a value transfer originator to the same financial institutions, whether or not the individual value transfers are intended ultimately for one or more value transfer beneficiaries;

"intermediary institution" means the financial institution that receives and transmits a value transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution;

"straight-through processing" means payment transactions that are conducted electronically without the need for manual intervention;

"unique transaction reference number" means a combination of letters, numbers or symbols, determined by the digital token service provider or ordering institution, in

accordance with the protocols of the payment and settlement system or messaging system used for the value transfer, and which permits the traceability of the value transfer;

"value transfer beneficiary" means the natural person, legal person or legal arrangement who is identified by the value transfer originator as the receiver of the digital tokens transferred; and

"value transfer originator" means the account holder who allows the value transfer from that account, or if there is no account, the natural person, legal person or legal arrangement that places the value transfer order with the ordering institution to perform or arrange the value transfer.

Responsibility of the Ordering Institution

(I) Identification and Recording of Information

14.3 Before effecting or arranging for a value transfer, a digital token service provider that is an ordering institution must –

(a) identify the value transfer originator and take reasonable measures to verify the value transfer originator's identity, as the case may be (if the digital token service provider has not already done so by virtue of paragraph 6); and

(b) record adequate details of the value transfer so as to permit its reconstruction, including but not limited to, the date of the value transfer, the type and value of digital token(s) transferred and the value date.

(II) Value Transfers Below or Equal To S$1,500

14.4 Subject to paragraph 14.5, in a value transfer where the amount to be transferred or arranged to be transferred is below or equal to S$1,500, a digital token service provider which is an ordering institution must include in the message or payment instruction that accompanies or relates to the value transfer the following:

(a) the name of the value transfer originator;

(b) the value transfer originator's account number (or unique transaction reference number if no account number exists);

(c) the name of the value transfer beneficiary; and

(d) the value transfer beneficiary's account number (or unique transaction reference number if no account number exists).

14.5 In a value transfer where the amount to be transferred or arranged to be transferred is below or equal to S$1,500, a digital token service provider which is an ordering institution may, in the message or payment instruction that accompanies or relates to the value transfer to an intermediary institution in Singapore, include only the unique transaction

reference number and the value transfer beneficiary information set out in paragraphs 14.4(c) and (d), provided that –

(a) the unique transaction reference number will permit the transaction to be traced back to the value transfer originator and value transfer beneficiary;

(b) the ordering institution must provide the value transfer originator information and value transfer beneficiary information set out in paragraphs 14.4(a) to (d) within 3 business days of a request for the information by the intermediary institution in Singapore, the Authority or other relevant authorities in Singapore;

(c) the ordering institution must provide the value transfer originator information and value transfer beneficiary information set out in paragraphs 14.4(a) to (d) immediately upon request for the information by law enforcement authorities in Singapore; and

(d) the ordering institution must provide the value transfer originator information and value transfer beneficiary information set out in paragraphs 14.4(a) to (d) to the beneficiary institution.

(III) Value Transfers Exceeding S$1,500

14.6 Subject to paragraph 14.8, in a value transfer where the amount to be transferred or arranged to be transferred exceeds S$1,500, a digital token service provider which is an ordering institution must identify the value transfer originator and verify the value transfer originator's identity, and include in the message or payment instruction that accompanies or relates to the value transfer the information required by paragraphs 14.4(a) to 14.4(d) and any of the following:

(a) the value transfer originator's –

(i) residential address, or

(ii) registered or business address, and if different, principal place of business,

as may be appropriate;

(b) the value transfer originator's unique identification number (such as an identity card number, birth certificate number or passport number, or if the value transfer originator is not a natural person, the incorporation number or business registration number); or

(c) the date and place of birth, incorporation or registration of the value transfer originator (as may be appropriate).

14.7 If several individual value transfers from a single value transfer originator are bundled in a batch file for transmission to value transfer beneficiaries, a digital token service provider must ensure that the batch transfer file contains –

(a) the value transfer originator information required by paragraph 14.6[7] and which has been verified; and

(b) the value transfer beneficiary information required by paragraph 14.6[8],

which are fully traceable within the beneficiary country or jurisdiction.

14.8 In a value transfer where the amount to be transferred or arranged to be transferred exceeds S$1,500, a digital token service provider which is an ordering institution may, in the message or payment instruction that accompanies or relates to the value transfer to an intermediary institution in Singapore, include only the unique transaction reference number and the value transfer beneficiary information required by paragraph 14.6[9], provided that:

(a) the unique transaction reference number will permit the transaction to be traced back to the value transfer originator and value transfer beneficiary;

(b) the ordering institution must provide the value transfer originator information and value transfer beneficiary information set out in paragraph 14.6[10] within 3 business days of a request for the information by the intermediary institution in Singapore, the Authority or other relevant authorities in Singapore;

(c) the ordering institution must provide the value transfer originator information and value transfer beneficiary information set out in paragraph 14.6[11] immediately upon request for the information by law enforcement authorities in Singapore; and

(d) the ordering institution must provide the value transfer originator information and value transfer beneficiary information set out in paragraph 14.6 to the beneficiary institution

14.9 All value transfer originator and value transfer beneficiary information collected by the ordering institution must be immediately and securely submitted to the beneficiary institution.

14.10 All value transfer originator and value transfer beneficiary information collected by the ordering institution must be documented.

14.11 If the ordering institution is unable to comply with the requirements in paragraphs 14.3 to 14.10, it must not execute or arrange for the value transfer.

Responsibility of the Beneficiary Institution

---

[7] Please note the references to paragraphs 14.4 (a) and (b) in paragraph 14.6.
[8] Please note the references to paragraphs 14.4 (c) and (d) in paragraph 14.6.
[9] Please note the references to paragraphs 14.4 (c) and (d) in paragraph 14.6.
[10] Please note the references to paragraphs 14.4 (a) to (d) in paragraph 14.6.
[11] Please note the references to paragraphs 14.4 (a) to (d) in paragraph 14.6.

14.12 A digital token service provider that is a beneficiary institution must take reasonable measures, including post-event monitoring or real-time monitoring if feasible, to identify value transfers that lack the required value transfer originator or required value transfer beneficiary information.

14.13 For value transfers where the beneficiary institution pays out the transferred digital token(s) in cash or cash equivalent to the value transfer beneficiary, a beneficiary institution must identify and verify the identity of the value transfer beneficiary if the identity has not been previously verified.

14.14 A digital token service provider that is a beneficiary institution must implement appropriate internal risk-based policies, procedures and controls for determining –

(a) when to execute, reject, or suspend a value transfer lacking required value transfer originator or value transfer beneficiary information; and

(b) the appropriate follow-up action.

14.15 For a digital token service provider that controls both the ordering institution and the beneficiary institution, it must –

(a) take into account all the information from both the ordering institution and the beneficiary institution in order to determine whether an STR has to be filed; and

(b) if applicable, file an STR in a country or jurisdiction affected by the value transfer, and make transaction information available to the relevant authorities.

Responsibility of the Intermediary Institution

14.16 A digital token service provider that is an intermediary institution must retain all the information accompanying the value transfer.

14.17 If a digital token service provider that is an intermediary institution effects a value transfer to another intermediary institution or a beneficiary institution, the digital token service provider must immediately and securely provide the information accompanying the value transfer, to that other intermediary institution or beneficiary institution.

14.18 If technical limitations prevent the required value transfer originator or value transfer beneficiary information accompanying a value transfer from remaining with a related value transfer, a record must be kept, for at least five years, by the receiving intermediary institution of the information received from the ordering institution or another intermediary institution.

14.19 An intermediary institution must take reasonable measures, which are consistent with straight-through processing, to identify value transfers that lack the required value transfer originator or value transfer beneficiary information.

14.20 An intermediary institution must implement appropriate internal risk-based policies, procedures and controls for determining –

(a) when to execute, reject, or suspend a value transfer lacking required value transfer originator or value transfer beneficiary information; and

(b) the appropriate follow-up action.

15 RECORD KEEPING

15.1 A digital token service provider must, in relation to all data, documents and information that the digital token service provider is required to obtain or produce to comply with this Notice, prepare, maintain and retain records of the data, documents and information.

15.2 A digital token service provider must perform the measures as required by paragraph 15.1 such that –

(a) the requirements imposed by law (including this Notice) are complied with;

(b) an individual transaction undertaken by the digital token service provider can be reconstructed (including the amount and type of currency involved) so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) the Authority or other relevant authorities in Singapore and the internal and external auditors of the digital token service provider are able to review the digital token service provider's business relations, transactions, records and CDD information and assess the level of compliance with this Notice; and

(d) the digital token service provider can satisfy, within a reasonable time or a more specific time period imposed by law or by the requesting authority, an enquiry or order from the relevant authorities in Singapore for information.

15.3 Subject to paragraph 15.5 and other requirements imposed by law, a digital token service provider must, for the purposes of record retention under paragraphs 15.1 and 15.2 and when setting its record retention policies, comply with the following record retention periods:

(a) for CDD information relating to the business relations, value transfers, transactions undertaken without an account being opened as well as account files, business correspondence and results of an analysis undertaken, a period of at least 5 years following the termination of the business relations or completion of the value transfers or transactions; and

(b) for data, documents and information relating to a transaction, including information needed to explain and reconstruct the transaction, a period of at least 5 years following the completion of the transaction.

15.4 A digital token service provider may retain data, documents and information as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

15.5 A digital token service provider must retain records of data, documents and information on all its business relations with or transactions for a customer pertaining to a matter which is under investigation or which has been the subject of an STR, in accordance with a request or order from STRO or other relevant authorities in Singapore.

16 PERSONAL DATA

16.1 For the purposes of paragraph 16, "individual" means a natural person, whether living or deceased.

16.2 Subject to paragraph 16.3 and for the purposes of complying with this Notice, a digital token service provider is not required to provide an individual customer, an individual appointed to act on behalf of a customer, an individual connected party of a customer or an individual beneficial owner of a customer, with —

(a) access to personal data about the individual that is in the possession or under the control of the digital token service provider;

(b) information about the ways in which the personal data of the individual under subparagraph (a) has been or may have been used or disclosed by the digital token service provider; and

(c) aright to correct an error or omission of the personal data about the individual that is in the possession or under the control of the digital token service provider.

16.3 A digital token service provider must, as soon as reasonably practicable, upon the request of an individual customer, an individual appointed to act on behalf of a customer, an individual connected party of a customer or an individual beneficial owner of a customer, provide the requesting individual with the right to —

(a) access the following types of personal data of that individual, that is in the possession or under the control of the digital token service provider:

(i) the individual's full name, including any alias;

(ii) the individual's unique identification number (such as an identity card number, birth certificate number or passport number);

(iii) the individual's residential address;

(iv) the individual's date of birth;

(v) the individual's nationality;

(vi) subject to sections 21(2) and (3) read with the Fifth Schedule to the Personal Data Protection Act 2012, other personal data of the respective individual provided by that individual to the digital token service provider; and

(b) subject to section 22(7) read with the Sixth Schedule to the Personal Data Protection Act 2012, correct an error or omission in relation to the types of personal data set out in subparagraphs (a)(i) to (vi), provided the digital token service provider is satisfied that there are reasonable grounds for the request.

16.4 For the purposes of complying with this Notice, a digital token service provider may, whether directly or through a third party, collect, use and disclose personal data of an individual customer, an individual appointed to act on behalf of a customer, an individual connected party of a customer or an individual beneficial owner of a customer, without the respective individual's consent.

17 SUSPICIOUS TRANSACTIONS REPORTING

17.1 A digital token service provider must keep in mind the provisions in the CDSA[12] and in the TSOFA that provide for the reporting to the authorities of transactions suspected of being connected with money laundering or terrorism financing and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all employees and officers are instructed to promptly refer all transactions suspected of being connected with money laundering or terrorism financing, for possible referral to STRO via STRs; and

(b) keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them.

17.2 A digital token service provider must promptly submit reports on suspicious transactions (including attempted transactions), regardless of the amount of the transaction, to STRO, and extend a copy to the Authority for information.

17.3 A digital token service provider must consider if the circumstances are suspicious so as to warrant the filing of an STR and document the basis for its determination, including if –

(a) the digital token service provider is for any reason unable to complete the measures as required by paragraphs 6, 7 and 8; or

[12] Please note in particular section 57 of the CDSA on tipping-off.

(b) the customer is reluctant, unable or unwilling to provide any information requested by the digital token service provider, or decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

17.4 If a digital token service provider forms a suspicion of money laundering or terrorism financing, and reasonably believes that performing any of the measures as required by paragraphs 6, 7 or 8 will tip-off a customer, a natural person appointed to act on behalf of the customer, a connected party of the customer or a beneficial owner of the customer, the digital token service provider may stop performing those measures. The digital token service provider must document the basis for its assessment and file an STR.

18 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

18.1 A digital token service provider must develop and implement adequate internal policies, procedures and controls, taking into consideration its money laundering and terrorism financing risks and the size of its business, to help prevent money laundering and terrorism financing and communicate these to its employees.

18.2 The policies, procedures and controls must comply with this Notice.

Group Policy

18.3 For the purposes of paragraphs 18.3 to 18.10, a reference to "digital token service provider" means a digital token service provider incorporated in Singapore.

18.4 A digital token service provider must develop a group policy on AML/CFT to comply with this Notice and extend this to all the branches and subsidiaries within its financial group.

18.5 If a digital token service provider has a branch or subsidiary in a host country or jurisdiction –

(a) in relation to which the FATF has called for countermeasures; or

(b) known to have inadequate AML/CFT measures, as determined by the digital token service provider for itself, or notified to digital token service providers generally by the Authority or other foreign regulatory authorities,

the digital token service provider must ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

18.6 Subject to the digital token service provider putting in place adequate safeguards to protect the confidentiality and use of information that is shared, the digital token service provider must develop and implement group policies and procedures for all the branches and subsidiaries within its financial group, to share information required for the purposes of CDD and for money laundering and terrorism financing risk management, to the extent

permitted by the law of the countries or jurisdictions that its branches and subsidiaries are in.

18.7 The policies and procedures mentioned in paragraph 18.6 must include the provision, to the digital token service provider's group-level compliance, audit, and AML/CFT functions, of customer, account, and transaction information from its branches and subsidiaries within the financial group, when necessary for money laundering and terrorism financing risk management purposes.

18.8 For the purposes of paragraph 18.7, the information to be shared within the digital token service provider's financial group must include information and analysis of transactions or activities that appear unusual[13].

18.9 If the AML/CFT requirements in the host country or jurisdiction differ from those in Singapore, the digital token service provider must require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

18.10 If the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the digital token service provider must apply additional appropriate measures to manage the money laundering and terrorism financing risks, report this to the Authority and comply with further directions as may be given by the Authority.

Compliance

18.11 A digital token service provider must develop appropriate compliance management arrangements, including at least, the appointment of an AML/CFT compliance officer, at the management level.

18.12 A digital token service provider must ensure that the AML/CFT compliance officer, as well as other persons appointed to assist the AML/CFT compliance officer, is suitably qualified and, has adequate resources and timely access to the customer records and other relevant information which the AML/CFT compliance officer requires to discharge the AML/CFT compliance officer's functions.

Audit

18.13 A digital token service provider must maintain an audit function that is adequately resourced and independent, and that is able to regularly assess the effectiveness of the digital token service provider's internal policies, procedures and controls, and its compliance with regulatory requirements.

[13] Subject to section 57 of the CDSA on tipping-off, information shared may include an STR, the underlying information of the STR, or the fact that an STR was filed.

Employee hiring

18.14 A digital token service provider must have in place screening procedures to ensure high standards when hiring employees and appointing officers.

Training

18.15 A digital token service provider must take all appropriate steps to ensure that its employees and officers (whether in Singapore or elsewhere) are regularly and appropriately trained on –

(a) AML/CFT laws and regulations, and in particular, CDD measures, and detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and terrorism financing; and

(c) the digital token service provider's internal AML/CFT policies, procedures and controls, and the roles and responsibilities of employees and officers in combating money laundering and terrorism financing.

Endnotes on History of Amendments

1. MAS Notice FSM-N27 (Amendment) 2025 with effect from DD MM 2025.

Appendix 1

1. Financial institutions that are licensed, approved, registered (including a fund management company registered under paragraph 5(1)(i) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations (Rg. 10)) or regulated by the Authority but does not include a person (other than a person mentioned in paragraphs 2 and 3) who is exempted from licensing, approval or regulation by the Authority under an Act administered by the Authority, including a private trust company exempted from licensing under section 15 of the Trust Companies Act 2005 read with regulation 4 of the Trust Companies (Exemption) Regulations (Rg. 1).

2. Persons exempted under section 20(1)(g) of the Financial Advisers Act 2001 read with regulation 27(1)(d) of the Financial Advisers Regulations (Rg. 2).

3. Persons exempted under section 99(1)(h) of the SFA read with paragraph 7(1)(b) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations.

Note: To avoid doubt, the financial institutions set out in Appendix 2 fall within Appendix 1.

Appendix 2

1. Banks in Singapore licensed under the Banking Act 1970.

2. Merchant banks in Singapore licensed under the Banking Act 1970.

3. Finance companies licensed under section 6 of the Finance Companies Act 1967.

4. Financial advisers licensed under section 6 of the Financial Advisers Act 2001 except those which only provide advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning an investment product.

5. Holders of a capital markets services licence under section 82 of the SFA.

6. Fund management companies registered under paragraph 5(1)(i) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations (Rg. 10).

7. Persons exempted under section 20(1)(g) of the Financial Advisers Act 2001 read with regulation 27(1)(d) of the Financial Advisers Regulations (Rg. 2) except those which only provide advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product.

8. Persons exempted under section 99(1)(h) of the SFA read with paragraph 7(1)(b) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations.

9. Approved trustees approved under section 289 of the SFA.

10. Trust companies licensed under section 5 of the Trust Companies Act 2005.

11. Direct life insurers licensed under section 11 of the Insurance Act 1966.

12. Insurance brokers registered under the Insurance Act 1966 which, by virtue of the registration, are exempted under section 20(1)(c) of the Financial Advisers Act 2001 except those which only provide advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning an investment product.