MAS Notice 626

28 March 2024

NOTICE TO BANKS
FINANCIAL SERVICES AND MARKETS ACT 2022

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM – BANKS

---

1 INTRODUCTION

1.1 This Notice is issued under section 16 of the Financial Services and Markets Act 2022 ("FSM Act") and applies to all banks in Singapore, as defined in section 2 of the Banking Act 1970 ("BA").

1.2 This Notice shall take effect from 1 April 2024.

2 DEFINITIONS

2.1 For the purposes of this Notice –

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

"Authority" means the Monetary Authority of Singapore;

"bank" means a bank in Singapore, as defined in section 2 of the BA;

"beneficial owner", in relation to a customer of a bank, 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 includes any person who exercises ultimate effective control over a legal person or legal arrangement;

"beneficiary institution" means –

(a) in relation to a wire transfer, the financial institution that receives the wire transfer from the ordering institution, directly or through an intermediary institution, and makes the funds available to the wire transfer beneficiary; or

(b) in relation to a value transfer, the financial institution that receives the value transfer from the ordering institution, directly or through an intermediary institution, and makes one or more digital tokens available to the value transfer beneficiary;

"business relations" means –

(a) the opening or maintenance of an account by the bank in the name of; or

(b) the provision of financial advice by the bank to,

a person (whether a natural person, legal person or legal arrangement);

"capital markets products" has the meaning as in section 2(1) of SFA;

"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 any director or any natural person having executive authority in the legal person;

(b) in relation to a legal person that is a partnership, means any partner or manager[1]; and

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

"COSMIC" refers to the electronic information sharing system established under section 28N(1) of the FSM Act.

"Core Principles" refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organisation of Securities Commissions, or the Insurance Core Principles issued by the International Association of Insurance Supervisors;

"cross-border wire transfer" means a wire transfer where the ordering institution and the beneficiary institution are located in different countries or jurisdictions and also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country or jurisdiction;

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

"custodian wallet service" means the service of safekeeping and administration of digital payment tokens or instruments enabling control over digital payment tokens;

"customer", in relation to a bank, means a person (whether a natural person, legal person or legal arrangement) -

(a) with whom the bank establishes or intends to establish business relations; or

(b) for whom the bank undertakes or intends to undertake any transaction without an account being opened;

"digital CMP token" means a digital representation of a capital markets product which can be transferred, stored or traded electronically;

"digital payment token" has the same meaning as defined in section 2(1) of the PS Act;

"digital payment token service" has the same meaning as defined in section 2(1) of the PS Act;

"digital payment token transfer service" means the service of accepting digital payment token from one digital payment token address or account, whether in Singapore or outside Singapore, as principal or agent, for the purposes of transferring, or arranging for the transfer of, the digital payment token to another digital payment token address or account, whether in Singapore or outside Singapore;

"digital token" means –

(a) a digital payment token; or

(b) a digital CMP token;

"digital token transaction" means –

(a) a payment service transaction; or

(b) any transaction accepted, processed, or executed by the bank in the course of its business of conducting any regulated activity under the SFA in relation to digital CMP tokens;

"domestic wire transfer" means a wire transfer where the ordering institution and beneficiary institution are located in the same country or jurisdiction and also refers to any chain of wire transfer that takes place entirely within a country or jurisdiction, even though the system used to transfer the payment message may be located in another country or jurisdiction;

“FATF” means the Financial Action Task Force;

“financial advice” means a financial advisory service as defined in section 2(1) of the Financial Advisers Act 2001 or advising on corporate finance as defined in section 2(1) of the SFA;

“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 for the application of group supervision under the Core Principles, 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;

“government entity” means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a 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;

“officer” means any director or any member of the committee of management of the bank;

“ordering institution” means –

(a) in relation to a wire transfer, the financial institution that initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the wire transfer originator; or

(b) in relation to a value transfer, the financial institution that initiates the value transfer and transfers 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;

“payment service transaction” means any transaction accepted, processed, or executed by the bank in the course of carrying on its business of providing a specified payment service;

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

"PS Act" means the Payment Services Act 2019;

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

"SFA" means the Securities and Futures Act 2001;

"specified payment service" means any of the following service:

(a) a digital payment token service;

(b) a digital payment token transfer service;

(c) a custodian wallet service;

"STR" means suspicious transaction report;

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

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

"value transfer" refers to any 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, irrespective of whether the originator and the beneficiary are the same person; and

"wire transfer" refers to any transaction carried out on behalf of a wire transfer originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary institution, irrespective of whether the originator and the beneficiary are the same person.

2.2 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency and in any digital payment token. The equivalent amount in digital payment tokens shall be determined based on the conversion rates prevailing at the time of the bank's compliance with the relevant threshold or value limit, either as published by the bank in the course of its business or offered by the bank to its customer in relation to the payment service transaction.

2.3 The expressions used in this Notice shall, except where defined in this Notice or where the context otherwise requires, have the same meanings as in the BA.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all banks in the conduct of their operations and business activities:

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

(c) A bank shall, 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 bank shall take appropriate steps to identify, assess and understand, its money laundering and terrorism financing risks in relation to –

(a) its customers;

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

(c) the countries or jurisdictions the bank has operations in; and

(d) the products, services, transactions, including digital token transactions, and delivery channels of the bank.

4.2 The appropriate steps referred to in paragraph 4.1 shall include –

(a) documenting the bank's risk assessments;

(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 bank'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 bank shall –

(a) develop and implement policies, procedures and controls, which are approved by senior management, to enable the bank to effectively manage and mitigate the risks that have been identified by the bank 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 where 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 bank shall 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 bank shall undertake the risk assessments, prior to the launch or use of such products, practices and technologies (to the extent such use is permitted by this Notice) and shall take appropriate measures to manage and mitigate the risks.

5.3 A bank shall, in complying with the requirements of paragraphs 5.1 and 5.2, pay special attention to any -

(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 Fictious Account

6.1 No bank shall open or maintain an anonymous account or an account in a fictitious name.

Where There Are Reasonable Grounds for Suspicion prior to the Establishment of Business Relations or Undertaking any Transaction without opening an Account

6.2 Prior to a bank establishing business relations or undertaking any transaction without opening an account, where the bank has any 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 any terrorism financing offence as defined in the TSOFA, the bank shall –

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

(b) file an STR[2], and extend a copy to the Authority for information.

When CDD is to be Performed

6.3 A bank shall perform the measures as required by paragraphs 6, 7 and 8 when -

(a) the bank establishes business relations with any customer;

(b) the bank undertakes any transaction of a value exceeding S$20,000, other than any digital token transaction referred to in paragraph 6.3(c), for any customer who has not otherwise established business relations with the bank;

(c) the bank undertakes any digital token transaction for any customer who has not otherwise established business relations with the bank;

(d) the bank effects or receives any funds by domestic wire transfer, or by cross-border wire transfer that exceeds S$1,500, for any customer who has not otherwise established business relations with the bank;

(e) the bank effects or receives any digital tokens by value transfer, for any customer who has not otherwise established business relations with the bank;

(f) there is a suspicion of money laundering or terrorism financing, notwithstanding that the bank would not otherwise be required by this Notice to perform the measures as required by paragraphs 6, 7 and 8; or

(g) the bank has doubts about the veracity or adequacy of any information previously obtained.

---

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

6.4 Where a bank 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 in relation to the circumstances set out in paragraphs 6.3(b) or (d), the bank shall treat the transactions as a single transaction and aggregate their values for the purposes of this Notice.

(I) <u>Identification of Customer</u>

6.5 A bank shall identify each customer.

6.6 For the purposes of paragraph 6.5, a bank shall obtain at least the following information:

(a) full name, including any aliases;

(b) 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) the customer's –

(i) residential address; or

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

as may be appropriate;

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

(e) nationality, place of incorporation or place of registration (as may be appropriate).

6.7 Where the customer is a legal person or legal arrangement, the bank shall, apart from identifying the customer, also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement.

6.8 Where the customer is a legal person or legal arrangement, the bank shall 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).

6.8A Where the bank –

(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 bank may obtain the date of birth and nationality of the connected party, in lieu of the unique identification number.

6.8B The bank shall document the results of the assessment in paragraph 6.8A(a) and all the measures taken under paragraph 6.8A(b).

(II) Verification of Identity of Customer

6.9 A bank shall verify the identity of the customer using reliable, independent source data, documents or information. Where the customer is a legal person or legal arrangement, a bank shall 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

6.10 Where a customer appoints one or more natural persons to act on the customer's behalf in establishing business relations with a bank or the customer is not a natural person, the bank shall -

(a) identify each natural person who acts or is appointed to act on behalf of the customer by obtaining at least the following information of such 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 each natural person using reliable, independent source data, documents or information.

6.11 A bank shall verify the due authority of each natural person appointed to act on behalf of the customer by:

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

(b) verifying that such 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.

6.11A Where the bank –

(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 the natural person who acts or is appointed to act on behalf of the customer after taking reasonable measures,

the bank may obtain the business address of this natural person, in lieu of the residential address.

6.11B Where the bank has obtained the business address of the natural person referred to in paragraph 6.11A, the bank shall take reasonable measures to verify the business address using reliable, independent source data, documents or information.

6.11C The bank shall document the results of the assessment in paragraph 6.11A(a) and all the measures taken under paragraph 6.11A(b).

6.12 Where the customer is a Singapore Government entity, the bank shall only be required to obtain such 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

6.13 Subject to paragraph 6.16, a bank shall inquire if there exists any beneficial owner in relation to a customer.

6.14 Where there is one or more beneficial owners in relation to a customer, the bank shall 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 bank shall -

(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) as to whether the natural persons who ultimately own the legal person are the beneficial owners or where 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) where 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 every beneficiary that falls within a designated characteristic or class)[3], and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership); and

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

6.15 Where the customer is not a natural person, the bank shall understand the nature of the customer's business and its ownership and control structure.

6.16 A bank shall not be required to inquire if there exists any 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[4] -

(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,

---

[3] In relation to a beneficiary of a trust designated by characteristics or by class, the bank 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.

[4] For the avoidance of doubt, the bank shall be required to inquire if there exists any beneficial owners in relation to a customer that is an investment vehicle to which it provides the regulated activity of fund management as the primary manager, except where the interests in the investment vehicle are distributed by a financial institution as described in paragraphs 6.16(c) or 6.16(d).

unless the bank 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.

6.17 For the purposes of paragraphs 6.16(d) and 6.16(e)(ii), a bank shall document the basis for its determination that the requirements in those paragraphs have been duly met.

(IVA) Identification of Beneficiary

6.17A Paragraphs 6.17B and 6.17C shall apply where a bank distributes life policies on behalf of a direct life insurer licensed under section 11 of the Insurance Act 1966.

6.17B A bank shall, as soon as a beneficiary of a life policy is identified to the bank as a specifically named natural person, legal person or legal arrangement, obtain the full name, including any aliases, of such beneficiary.

6.17C A bank shall, as soon as a beneficiary of a life policy is designated by characteristics, class or other means and is known to the bank, obtain sufficient information concerning the beneficiary to satisfy the direct life insurer that such direct life insurer will be able to establish the identity of the beneficiary at the time of payout.

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

6.18 A bank shall, 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.

(VI) Ongoing Monitoring

6.19 A bank shall monitor on an ongoing basis, its business relations with customers.

6.20 A bank shall, 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 bank's knowledge of the customer, its business and risk profile and where appropriate, the source of funds. If a bank is participating in COSMIC and receives, through COSMIC, information relating to a customer, its business, risk profile or source of funds, the bank's knowledge of the customer, its business and risk profile and, if appropriate, the source of funds, must include the information received through COSMIC.

6.20A A bank shall perform enhanced risk mitigation measures where the transaction involves a transfer of a digital token to or a receipt of a digital token 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.

6.21 A bank shall 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. If a bank is participating in COSMIC, the bank must take into account information that it has received through COSMIC, in determining whether transactions undertaken throughout the course of business relations are complex, unusually large or part of an unusual pattern of transactions that have no apparent or visible economic or lawful purpose.

6.22 For the purposes of ongoing monitoring, a bank shall put in place and implement adequate systems and processes, commensurate with the size and complexity of the bank, to –

(a) monitor its business relations with customers; and

(b) detect and report suspicious, complex, unusually large or unusual patterns of transactions.

6.23 A bank shall, to the extent possible, inquire into the background and purpose of the transactions in paragraph 6.21 and document its findings with a view to making this information available to the relevant authorities should the need arise.

6.24 A bank shall 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.

6.25 Where there are any reasonable grounds for suspicion that existing business relations with a customer are connected with money laundering or terrorism financing, and where the bank considers it appropriate to retain the customer -

(a) the bank shall substantiate and document the reasons for retaining the customer; and

(b) the customer's business relations with the bank shall be subject to commensurate risk mitigation measures, including enhanced ongoing monitoring.

6.26 Where the bank assesses the customer or the business relations with the customer referred to in paragraph 6.25 to be of higher risk, the bank shall perform enhanced CDD measures, which shall include obtaining the approval of the bank's senior management to retain the customer.

CDD Measures for Non-Face-to-Face Business Relations

6.27 A bank shall develop policies and procedures to address any specific risks associated with non-face-to-face business relations with a customer or transactions for a customer.

6.28 A bank shall implement the policies and procedures referred to in paragraph 6.27 when establishing business relations with a customer and when conducting ongoing due diligence.

6.29 Where there is no face-to-face contact, the bank shall 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.

Reliance by Acquiring Bank on Measures Already Performed

6.30 When a bank ("acquiring bank") acquires, either in whole or in part, the business of another financial institution (whether in Singapore or elsewhere), the acquiring bank shall perform the measures as required by paragraphs 6, 7 and 8, on the customers acquired with the business at the time of acquisition except where the acquiring bank has –

(a) acquired at the same time all 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 any doubt on the part of the acquiring bank as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring bank and document such enquiries.

CDD Measures for Non-Account Holder

6.31 A bank that undertakes any transaction of a value exceeding S$20,000, other than any digital token transaction referred to in paragraph 6.31A, or effects or receives any funds by domestic wire transfer, or by cross-border wire transfer that exceeds S$1,500, for any customer who does not otherwise have business relations with the bank shall –

(a) perform CDD measures as if the customer had applied to the bank to establish business relations; and

(b) record adequate details of the 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.

6.31A A bank that undertakes any digital token transaction, or effects or receives any digital token by value transfer, for any customer who does not otherwise have business relations with the bank shall –

(a) perform CDD measures as if the customer had applied to the bank to establish business relations; and

(b) record adequate details of the digital token transaction so as to permit the reconstruction of the transaction, including the nature and date of the transaction,

the type and amount of currency, the type and value of digital token(s) involved, the value date, and the details of the payee or beneficiary.

Timing for Verification

6.32 Subject to paragraphs 6.33 and 6.34, a bank shall complete verification of the identity of a customer as required by paragraph 6.9, natural persons appointed to act on behalf of the customer as required by paragraph 6.10(b) and beneficial owners of the customer as required by paragraph 6.14 -

(a) before the bank establishes business relations with the customer;

(b) before the bank undertakes any transaction of a value exceeding S$20,000 for the customer, other than any digital token transaction referred to in paragraph 6.32(d), where the customer has not otherwise established business relations with the bank;

(c) before the bank effects or receives any funds by domestic wire transfer, or by cross-border wire transfer that exceeds S$1,500, for any customer who has not otherwise established business relations with the bank;

(d) before the bank undertakes any digital token transaction, where the customer has not otherwise established business relations with the bank; or

(e) before the bank effects or receives any digital token by value transfer, for any customer who has not otherwise established business relations with the bank.

6.33 A bank may establish business relations with a customer before completing the verification of the identity of the customer as required by paragraph 6.9, natural persons appointed to act on behalf of the customer as required by paragraph 6.10(b) and beneficial owners of the customer as required by paragraph 6.14 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 bank.

6.34 Where the bank establishes business relations with a customer before verifying the identity of the customer as required by paragraph 6.9, natural persons appointed to act on behalf of the customer as required by paragraph 6.10(b), and beneficial owners of the customer as required by paragraph 6.14, the bank shall -

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

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

Where Measures are Not Completed

6.35 Where the bank is unable to complete the measures as required by paragraphs 6, 7 and 8, it shall not commence or continue business relations with any customer or undertake any transaction for any customer. The bank shall consider if the circumstances are suspicious so as to warrant the filing of an STR.

6.36 For the purposes of paragraph 6.35, completion of the measures means the situation where the bank has obtained, screened and verified (including by delayed verification as allowed under paragraphs 6.33 and 6.34) all necessary CDD information required under paragraphs 6, 7 and 8, and where the bank has received satisfactory responses to all inquiries in relation to such necessary CDD information.

Joint Account

6.37 In the case of a joint account, a bank shall perform CDD measures on all of the joint account holders as if each of them were individual customers of the bank.

Existing Customers

6.38 A bank shall 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

6.39 A bank shall 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 or 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.

6.40 A bank shall screen the persons referred to in paragraph 6.39 -

(a) when, or as soon as reasonably practicable after, the bank establishes business relations with a customer;

(b) when the bank undertakes any transaction of a value exceeding S$20,000, other than any digital token transaction referred to in paragraph 6.40(f), for a customer who has not otherwise established business relations with the bank;

(c) when the bank effects or receives any funds by domestic wire transfer, or by cross-border wire transfer that exceeds S$1,500, for a customer who has not otherwise established business relations with the bank;

(d) on a periodic basis after the bank establishes business relations with the customer;

(e) when there are any changes or updates to -

(i) the lists and information provided by the Authority or other relevant authorities in Singapore to the bank; or

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

(f) when the bank undertakes any digital token transaction for a customer who has not otherwise established business relations with the bank; and

(g) when the bank effects or receives any digital token by value transfer, for a customer who has not otherwise established business relations with the bank.

6.41 A bank shall screen all wire transfer originators and wire transfer beneficiaries as defined in paragraph 11, against lists and information provided by the Authority or any other relevant authorities in Singapore for the purposes of determining if there are any money laundering or terrorism financing risks in relation to any such persons.

6.41A A bank shall screen all value transfer originators and value transfer beneficiaries as defined in paragraph 11A, against lists and information provided by the Authority and any other relevant authorities in Singapore for the purposes of determining if there are any money laundering or terrorism financing risks in relation to any such persons.

6.42 The results of screening and assessment by the bank shall be documented.

6.43 For the purposes of paragraph 6:

(a) a reference to “transaction” shall include a digital token transaction; and

(b) a reference to “lists and information provided by the Authority and other relevant authorities in Singapore” does not include the platform screening list, as defined in MAS Notice FSM-N02 on Prevention of Money Laundering and Countering of Financing of Terrorism – Financial Institutions’ Information Sharing Platform.

7 SIMPLIFIED CUSTOMER DUE DILIGENCE

7.1 Subject to paragraph 7.4, a bank may perform simplified CDD measures in relation to a customer, any natural person appointed to act on behalf of the customer and any beneficial owner of the customer (other than any beneficial owner that the bank is exempted from making inquiries about under paragraph 6.16) if it is satisfied that the risks of money laundering and terrorism financing are low.

7.2 The assessment of low risks shall be supported by an adequate analysis of risks by the bank.

7.3 The simplified CDD measures shall be commensurate with the level of risk, based on the risk factors identified by the bank.

7.4 A bank shall not perform simplified CDD measures -

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

(b) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the bank for itself, or notified to banks generally by the Authority, or other foreign regulatory authorities; or

(c) where the bank suspects that money laundering or terrorism financing is involved.

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

7.6 Where the bank performs simplified CDD measures in relation to a customer, any natural person appointed to act on behalf of the customer and any beneficial owner of the customer, it shall document -

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

7.7 For avoidance of doubt, the term "CDD measures" in paragraph 7 means the measures required by paragraph 6.

8 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

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 bank shall implement appropriate internal risk management systems, policies, procedures and controls to determine if a customer, any natural person appointed to act on behalf of the customer, any connected party of the customer or any beneficial owner of the customer is a politically exposed person, or a family member or close associate of a politically exposed person. If a bank is participating in COSMIC, the bank must ensure that under its internal risk management systems, policies, procedures and controls in this paragraph 8.2, the bank takes into account information relating to the aforementioned persons that it has received through COSMIC.

8.3 A bank shall, in addition to performing CDD measures (specified in paragraph 6), perform at least the following enhanced CDD measures where a customer or any beneficial owner of the customer is determined by the bank 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 bank's senior management to establish or continue business relations with, or undertake any transaction 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 any beneficial owner of the customer; and

(c) conduct, during the course of business relations with the customer, enhanced monitoring of business relations with the customer. In particular, the bank shall 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 bank 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 such 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 or transactions with the bank present a higher risk for money laundering or terrorism financing.

Other Higher Risk Categories

8.5 A bank shall implement appropriate internal risk management systems, policies, procedures and controls to determine if business relations with or transactions for any customer present a higher risk for money laundering or terrorism financing. If a bank is participating in COSMIC, the bank must ensure that under its internal risk management systems, policies, procedures and controls in this paragraph 8.5, the bank takes into account information relating to 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, where relevant, that it has received through COSMIC.

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) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures, the bank shall treat any business relations with or transactions for any such customer as presenting a higher risk for money laundering or terrorism financing;

(b) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the bank for itself, or notified to banks generally by the Authority or other foreign regulatory authorities, the bank shall assess whether any such customer presents a higher risk for money laundering or terrorism financing; and

(c) where a customer is a legal person for which the bank 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 bank,

the bank shall assess whether any such customer presents a higher risk for money laundering or terrorism financing.

8.7 A bank shall perform the appropriate enhanced CDD measures in paragraph 8.3 for business relations with or transactions for any customer -

(a) who the bank determines under paragraph 8.5; or

(b) the Authority or other relevant authorities in Singapore notify to the bank,

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

8.8 A bank shall, in taking enhanced CDD measures to manage and mitigate any higher risks that have been identified by the bank, 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 any 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.

8.9 For the purposes of paragraph 8, a reference to “transaction” shall include a digital token transaction.

9 RELIANCE ON THIRD PARTIES

9.1 For the purposes of paragraph 9, “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 holder of a payment services licence under the PS Act, or equivalent licences);

(c) in relation to a bank incorporated in Singapore, its branches, subsidiaries, parent entity, the branches and subsidiaries of the parent entity, and other related corporations; or

(d) in relation to a bank incorporated outside Singapore, its head office, its parent entity, the branches and subsidiaries of the head office, the branches and subsidiaries of the parent entity, and other related corporations.

9.2 Subject to paragraph 9.3, a bank may rely on a third party to perform the measures as required by paragraphs 6, 7 and 8 if the following requirements are met:

(a) the bank 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 bank 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 banks 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 bank's request, any data, documents or information obtained by the third party with respect to the measures applied on the bank's customer, which the bank would be required or would want to obtain.

9.3 No bank shall rely on a third party to conduct ongoing monitoring of business relations with customers.

9.4 Where a bank relies on a third party to perform the measures as required by paragraphs 6, 7 and 8, it shall -

(a) document the basis for its satisfaction that the requirements in paragraphs 9.2(a) and (b) have been met, except where 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.

9.5 For the avoidance of doubt, notwithstanding the reliance upon a third party, the bank shall remain responsible for its AML/CFT obligations in this Notice.

10 CORRESPONDENT BANKING

10.1 Paragraph 10 applies to a bank when it provides correspondent banking or other similar services in Singapore to a bank or financial institution that is operating outside Singapore.

10.2 For the purposes of paragraph 10 -

"correspondent bank" means a bank in Singapore that provides or intends to provide correspondent banking or other similar services;

"correspondent banking" means the provision of banking services by a correspondent bank to a respondent bank;

"payable-through account" means an account maintained at the correspondent bank by the respondent bank but which is accessible directly by a third party to effect transactions on its own behalf;

"respondent financial institution" means a bank or financial institution, outside Singapore to which correspondent banking or other similar services are provided;

"shell financial institution" means a bank or financial institution incorporated, formed or established in a country or jurisdiction where the bank or 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 services undertaken for securities transactions, funds transfers or digital token transactions, for the financial institution that is operating outside Singapore, whether as principal or for its customers.

10.3 A bank in Singapore shall perform the following measures, in addition to the measures as required by paragraphs 6, 7 and 8, when providing correspondent banking 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 any 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 each financial institution; and

(c) obtain approval from the bank's senior management before providing correspondent banking or similar services to a new financial institution.

10.4 Where the correspondent banking or other similar services involve a payable-through account, the correspondent bank shall 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 correspondent bank upon request.

10.5 The correspondent bank shall document the basis for its satisfaction that the requirements in paragraphs 10.3 and 10.4 are met.

10.6 No bank shall enter into or continue correspondent banking or other similar services relationship with another bank or 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.

10.7 A bank shall also take appropriate measures when establishing correspondent banking or other similar services relationship, to satisfy itself that its respondent financial institutions do not permit their accounts to be used by shell financial institutions.

11 WIRE TRANSFERS

11.1 Paragraph 11 shall apply to a bank when it effects the sending of funds by wire transfer or when it receives funds (including serial payments and cover payments) by wire transfer on the account of the wire transfer originator or the wire transfer beneficiary but shall not apply to a transfer and settlement between the bank and another financial institution where the bank and the other financial institution are acting on their own behalf as the wire transfer originator and the wire transfer beneficiary.

11.2 For the purposes of paragraph 11 -

"batch transfer" means a transfer comprising a number of individual wire transfers that are sent by a wire transfer originator to the same financial institutions, irrespective of whether the individual wire transfers are intended ultimately for one or more wire transfer beneficiaries;

"cover payment" means a wire transfer that combines a payment message sent directly by the ordering institution to the beneficiary institution with the routing of the funding instruction from the ordering institution to the beneficiary institution through one or more intermediary institutions;

"intermediary institution" means the financial institution in a serial payment or cover payment chain that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution;

"serial payment" means a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering institution to the beneficiary institution, directly or through one or more intermediary institutions;

"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 payment service provider in accordance with the protocols

of the payment and settlement system or messaging system used for the wire transfer, and which permits the traceability of the wire transfer;

"wire transfer beneficiary" means the natural person, legal person or legal arrangement who is identified by the wire transfer originator as the receiver of the wire transfer funds; and

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

Responsibility of the Ordering Institution

(I) Identification and Recording of Information

11.3 Before effecting a wire transfer, every bank that is an ordering institution shall -

(a) identify the wire transfer originator and verify the wire transfer originator's identity, as the case may be (if the bank has not already done so by virtue of paragraph 6); and

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

(II) Cross-Border Wire Transfers Below or Equal To S$1,500

11.4 In a cross-border wire transfer where the amount to be transferred is below or equal to S$1,500, every bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer the following:

(a) the name of the wire transfer originator;

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

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

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

(III) Cross-border Wire Transfers Exceeding S$1,500

11.5 In a cross-border wire transfer where the amount to be transferred exceeds S$1,500, every bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer the information required by paragraphs 11.4(a) to 11.4(d) and any of the following:

(a) the wire 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 wire transfer originator's unique identification number (such as an identity card number, birth certificate number or passport number, or where the wire 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 wire transfer originator (as may be appropriate).

11.6 Where several individual cross-border wire transfers from a single wire transfer originator are bundled in a batch file for transmission to wire transfer beneficiaries, a bank shall ensure that the batch transfer file contains -

(a) the wire transfer originator information required by paragraph 11.5[5] and which has been verified; and

(b) the wire transfer beneficiary information required by paragraph 11.5[6],

which are fully traceable within the beneficiary country or jurisdiction.

(IV) Domestic Wire Transfers

11.7 In a domestic wire transfer, every bank that is an ordering institution shall either –

(a) include in the message or payment instruction that accompanies or relates to the wire transfer the following:

(i) the name of the wire transfer originator;

(ii) the wire transfer originator's account number (or unique transaction reference number where no account number exists); and

(iii) any of the following:

(A) the wire transfer originator's:

(1) residential address; or

---

[5] Please note the references to paragraphs 11.4(a) and (b) in paragraph 11.5.

[6] Please note the references to paragraphs 11.4(c) and (d) in paragraph 11.5.

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

as may be appropriate;

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

(C) the date and place of birth, incorporation or registration of the wire transfer originator (as may be appropriate); or

(b) include only the wire transfer originator's account number (or unique transaction reference number where no account number exists), provided -

(i) that these details will permit the transaction to be traced back to the wire transfer originator and wire transfer beneficiary;

(ii) the ordering institution shall provide the wire transfer originator information set out in paragraph 11.7(a) within 3 business days of a request for such information by the beneficiary institution, by the Authority or other relevant authorities in Singapore; and

(iii) the ordering institution shall provide the wire transfer originator information set out in paragraph 11.7(a) immediately upon request for such information by law enforcement authorities in Singapore.

11.8 All wire transfer originator and beneficiary information collected by the ordering institution shall be documented.

11.9 Where the ordering institution is unable to comply with the requirements in paragraphs 11.3 to 11.8, it shall not execute the wire transfer.

Responsibility of the Beneficiary Institution

11.10 A bank that is a beneficiary institution shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack the required wire transfer originator or required wire transfer beneficiary information.

11.11 For cross-border wire transfers, a beneficiary institution shall identify and verify the identity of the wire transfer beneficiary if the identity has not been previously verified.

11.12 A bank that is a beneficiary institution shall implement appropriate internal risk-based policies, procedures and controls for determining -

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

(b) the appropriate follow-up action.

Responsibility of the Intermediary Institution

11.13 A bank that is an intermediary institution shall retain all the required wire transfer originator and wire transfer beneficiary information accompanying the wire transfer.

11.14 Where technical limitations prevent the required wire transfer originator or wire transfer beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record shall be kept, for at least five years, by the receiving intermediary institution of all the information received from the ordering institution or another intermediary institution.

11.15 An intermediary institution shall take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack the required wire transfer originator or wire transfer beneficiary information.

11.16 An intermediary institution shall implement appropriate internal risk-based policies, procedures and controls for determining -

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

(b) the appropriate follow-up action.

11A VALUE TRANSFERS

11A.1 Paragraph 11A shall apply to a bank when:

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

(b) when it receives one or more digital tokens by value transfer on the account of the value transfer originator or the value transfer beneficiary,

but shall not apply to a transfer and settlement between the bank and another financial institution where the bank and the other financial institution are acting on their own behalf as the value transfer originator and the value transfer beneficiary.

11A.2 For the purposes of paragraph 11A –

"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, irrespective of whether 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 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 bank 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 where there is no account, the natural person, legal person or legal arrangement that places the value transfer order with the ordering institution to perform the value transfer.

Responsibility of the Ordering Institution

(I) Identification and Recording of Information

11A.3 Before effecting a value transfer, every bank that is an ordering institution shall –

(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 bank 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

11A.4 Subject to paragraph 11A.5, in a value transfer where the amount to be transferred is below or equal to S$1,500, every bank which is an ordering institution shall 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 where 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 where no account number exists).

11A.5 In a value transfer where the amount to be transferred is below or equal to S$1,500, every bank 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 11A.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 shall provide the value transfer originator information and value transfer beneficiary information set out in paragraphs11.4(a) to (d) within 3 business days of a request for such information by the intermediary institution in Singapore, the Authority or other relevant authorities in Singapore;

(c) the ordering institution shall provide the value transfer originator information and value transfer beneficiary information set out in paragraphs 11.4(a) to (d) immediately upon request for such information by law enforcement authorities in Singapore; and

(d) the ordering institution shall provide the value transfer originator information and value transfer beneficiary information set out in paragraphs 11.4(a) to (d) to the beneficiary institution.

(III) Value Transfers Exceeding S$1,500

11A.6 Subject to paragraph 11A.8, in a value transfer where the amount to be transferred exceeds S$1,500, every bank which is an ordering institution shall 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 11A.4(a) to 11A.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 where 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).

11A.7 Where several individual value transfers from a single value transfer originator are bundled in a batch file for transmission to value transfer beneficiaries, a bank shall ensure that the batch transfer file contains –

(a) the value transfer originator information required by paragraph 11A.6[7] and which has been verified; and

(b) the value transfer beneficiary information required by paragraph 11A.6[8],

which are fully traceable within the beneficiary country or jurisdiction.

11A.8 In a value transfer where the amount to be transferred exceeds S$1,500, every bank 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 11A.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 shall provide the value transfer originator information and value transfer beneficiary information set out in paragraph 11A.6[10] within 3 business days of a request for such information by the intermediary institution in Singapore, the Authority or other relevant authorities in Singapore;

(c) the ordering institution shall provide the value transfer originator information and value transfer beneficiary information set out in paragraph 11A.6[11] immediately upon request for such information by law enforcement authorities in Singapore; and

(d) the ordering institution shall provide the value transfer originator information and value transfer beneficiary information set out in paragraph 11A.6 to the beneficiary institution.

11A.9 All value transfer originator and value transfer beneficiary information collected by the ordering institution shall be immediately and securely submitted to the beneficiary institution.

11A.10 All value transfer originator and value transfer beneficiary information collected by the ordering institution shall be documented.

11A.11 Where the ordering institution is unable to comply with the requirements in paragraphs 11A.3 to 11A.10, it shall not execute the value transfer.

[7] Please note the references to paragraphs 11A.4 (a) and (b) in paragraph 11A.6.
[8] Please note the references to paragraphs 11A.4 (c) and (d) in paragraph 11A.6.
[9] Please note the references to paragraphs 11A.4 (c) and (d) in paragraph 11A.6.
[10] Please note the references to paragraphs 11A.4 (a) to (d) in paragraph 11A.6.
[11] Please note the references to paragraphs 11A.4 (a) to (d) in paragraph 11A.6.

Responsibility of the Beneficiary Institution

11A.12 A bank that is a beneficiary institution shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify value transfers that lack the required value transfer originator or required value transfer beneficiary information.

11A.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 in Singapore, a beneficiary institution shall identify and verify the identity of the value transfer beneficiary if the identity has not been previously verified.

11A.14 A bank that is a beneficiary institution shall 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.

11A.15 For a bank that controls both the ordering institution and the beneficiary institution, it shall –

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

Responsibility of the Intermediary Institution

11A.16 A bank that is an intermediary institution shall retain all the information accompanying the value transfer.

11A.17 Where a bank that is an intermediary institution effects a value transfer to another intermediary institution or a beneficiary institution, the bank shall immediately and securely provide the information accompanying the value transfer, to that other intermediary institution or beneficiary institution.

11A.18 Where 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 shall be kept, for at least five years, by the receiving intermediary institution of all the information received from the ordering institution or another intermediary institution.

11A.19 An intermediary institution shall 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.

11A.20 An intermediary institution shall 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..

11A.21 For the purposes of paragraph 11A, a reference to "transaction" shall include a digital token transaction.

12 RECORD KEEPING

12.1 A bank shall, in relation to all data, documents and information that the bank is required to obtain or produce to meet the requirements under this Notice, prepare, maintain and retain records of such data, documents and information.

12.2 A bank shall perform the measures as required by paragraph 12.1 such that -

(a) all requirements imposed by law (including this Notice) are met;

(b) any individual transaction undertaken by the bank 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 bank are able to review the bank's business relations, transactions, records and CDD information and assess the level of compliance with this Notice; and

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

12.3 Subject to paragraph 12.5 and any other requirements imposed by law, a bank shall, for the purposes of record retention under paragraphs 12.1 and 12.2, and when setting its record retention policies, comply with the following record retention periods:

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

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

12.4 A bank 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.

12.5 A bank shall 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 any request or order from STRO or other relevant authorities in Singapore.

12.6 For the purposes of paragraph 12, a reference to "transaction" shall include a digital token transaction.

13 PERSONAL DATA

13.1 For the purposes of paragraph 13, "individual" means a natural person, whether living or deceased.

13.2 Subject to paragraph 13.3 and for the purposes of complying with this Notice, a bank shall not be required to provide an individual customer, an individual beneficiary of a life insurance policy, 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) any access to personal data about the individual that is in the possession or under the control of the bank;

(b) any 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 bank; and

(c) any right to correct an error or omission of the personal data about the individual that is in the possession or under the control of the bank.

13.3 A bank shall, 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 bank:

(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, any other personal data of the respective individual provided by that individual to the bank; 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 bank is satisfied that there are reasonable grounds for such request.

13.4 For the purposes of complying with this Notice, a bank may, whether directly or through a third party, collect, use and disclose personal data of an individual customer, an individual beneficiary of a life insurance policy, 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.

14 SUSPICIOUS TRANSACTIONS REPORTING

14.1 A bank shall 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.

14.2 A bank shall 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.

14.3 A bank shall consider if the circumstances are suspicious so as to warrant the filing of an STR and document the basis for its determination, including where -

(a) the bank 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 bank, or decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

14.4 Where a bank 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 bank may stop performing those measures. The bank shall document the basis for its assessment and file an STR.

14.5 For the purposes of paragraph 14, a reference to "transaction" shall include a digital token transaction.

15 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

15.1 A bank shall 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.

15.2 The policies, procedures and controls shall meet all the requirements of this Notice.

Group Policy

15.3 For the purposes of paragraphs 15.4 to 15.9, a reference to "bank" means a bank incorporated in Singapore.

15.4 A bank shall develop a group policy on AML/CFT to meet all the requirements of this Notice and extend this to all of its branches and subsidiaries in its financial group.

15.5 Where a bank 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 bank for itself, or notified to banks generally by the Authority or other foreign regulatory authorities,

the bank shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

15.6 Subject to the bank putting in place adequate safeguards to protect the confidentiality and use of any information that is shared, the bank shall develop and implement group policies and procedures for its branches and subsidiaries within the 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.

15.7 Such policies and procedures shall include the provision, to the bank'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.

15.7A For the purposes of paragraph 15.7, the information to be shared within the bank's financial group shall include any information and analysis of transactions or activities that appear unusual.[13]

15.8 Where the AML/CFT requirements in the host country or jurisdiction differ from those in Singapore, the bank shall 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.

15.9 Where 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 bank shall apply additional appropriate measures to manage the money laundering and terrorism financing risks, report this to the Authority and comply with such further directions as may be given by the Authority.

15.9A In the case of a Singapore branch of a bank incorporated outside Singapore, subject to the Singapore branch putting in place adequate safeguards to protect the confidentiality and use of any information that is shared, the Singapore branch shall share customer, account and transaction information within the bank's financial group when necessary for money laundering and terrorism financing risk management purposes. Such information to be shared within the bank's financial group shall include any information and analysis of transactions or activities that appear unusual.[14]

Compliance

15.10 A bank shall develop appropriate compliance management arrangements, including at least, the appointment of an AML/CFT compliance officer at the management level.

15.11 A bank shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist the AML/CFT compliance officer, is suitably qualified, and has adequate resources and timely access to all customer records and other relevant information which the AML/CFT compliance officer requires to discharge the AML/CFT compliance officer's functions.

[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.

[14] 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.

Audit

15.12 A bank shall maintain an audit function that is adequately resourced and independent, and that is able to regularly assess the effectiveness of the bank's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

15.13 A bank shall have in place screening procedures to ensure high standards when hiring employees and appointing officers.

Training

15.14 A bank shall 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 bank's internal AML/CFT policies, procedures and controls, and the roles and responsibilities of employees and officers in combating money laundering and terrorism financing.

15.15 For the purposes of paragraph 15, a reference to "transaction" shall include a digital token transaction.

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 referred to in paragraphs 2 and 3) who is exempted from licensing, approval or regulation by the Authority under any 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: For the avoidance of doubt, the financial institutions set out in Appendix 2 fall within Appendix 1.

Appendix 2

1. Banks in Singapore licensed under the BA.
2. Merchant banks in Singapore licensed under the BA.
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 any 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 such 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 any investment product.