MAS Notice XXX

[DD MMM 2024]

NOTICE TO APPROVED EXCHANGES AND RECOGNISED MARKET OPERATORS
FINANCIAL SERVICES AND MARKETS ACT 2022

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM – APPROVED EXCHANGES AND RECOGNISED MARKET OPERATORS

---

1 INTRODUCTION

1.1 This Notice is issued under section 16 of the Financial Services and Markets Act 2022 ("FSM Act") and applies to an approved exchange ("AE") as defined in section 2 of the Securities and Futures Act 2001 ("SFA") and a recognised market operator as defined in section 2 of the SFA that is formed or incorporated in Singapore ("RMO").

1.2 This Notice takes effect from [•*date* 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;

"beneficial owner", in relation to a customer of an AE or RMO, 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 a person who exercises ultimate effective control over a legal person or legal arrangement;

"business relations" means -

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

(b) the allowing of a trade-related activity to be performed on an organised market operated by the AE or RMO by or through; or

(c) the provision of services by the AE or RMO as may be required to facilitate the completion of a trade-related activity on an organised market operated by the AE or RMO, to,

a person (whether a natural person, legal person or legal arrangement) other than –

(i) a financial institution as set out in Appendix 2; and

(ii) the equivalent of a financial institution set out in Appendix 2 that is incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

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

"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;

"CMI" means a person holding a capital markets services licence under the SFA, 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 ("SF(LCB)R") or a person exempted from the requirement to hold such a licence under paragraphs 3(1)(d), 3A(1)(d) or 7(1)(b) of the Second Schedule to the SF(LCB)R

"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[1]; and

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

"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;

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

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

(b) for whom the AE or RMO undertakes or intends to undertake a transaction without an account being opened;

but does not include a person who is –

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

(i) a financial institution as set out in Appendix 2; and
(ii) the equivalent of a financial institution set out in Appendix 2, that is incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

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

"digital CMP token transaction" means a transaction which is –

(a) in connection with a trade-related activity; and

(b) in respect of a digital representation of derivatives contracts, securities, or units in collective investment schemes, that can be transferred, stored or traded electronically;

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

"entity" (other than in the definition of legal person) has the same meaning as defined in section 2(1) of the SFA, except that it includes a trust;

"FATF" means the Financial Action Task Force;

"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 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;

"officer" means a director or a member of the committee of management of the AE or RMO;

"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;

"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;

"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; and

"trade-related activity" means any of the following -

(a) the making or acceptance of an offer or invitation to exchange, sell or purchase derivatives contracts, securities, or units in collective investment schemes on an organised market operated by the AE or RMO;

(b) an act on an organised market operated by the AE or RMO that results in fiat currency, digital CMP token or digital payment token being transferred by any person across accounts (whether in consideration for derivatives contracts, securities, or units in collective investment schemes, or otherwise),

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 payment token. The equivalent amount in digital payment tokens is determined based on the conversion rates prevailing at the time of the AE's or RMO's compliance with the relevant threshold or value limit.

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

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which serves as a guide for an AE or RMO in the conduct of its operations and business activities:

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

(c) An AE or RMO 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 An AE or RMO must 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 AE or RMO has operations in; and

(d) the products, services, transactions, including digital CMP token transactions, and delivery channels of the AE or RMO.

4.2 The appropriate steps mentioned in paragraph 4.1 include –

(a) documenting the AE or RMO'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 AE or RMO's risk assessments up-to-date; and

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

Risk Mitigation

4.3 An AE or RMO must –

(a) develop and implement policies, procedures and controls, which are approved by senior management, to enable the AE or RMO to effectively manage and mitigate the risks that have been identified by the AE or RMO 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 An AE or RMO 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 An AE or RMO 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 An AE or RMO 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 An AE or RMO 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 an AE or RMO establishes business relations or undertakes a transaction without opening an account, if the AE or RMO 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 AE or RMO must –

(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 An AE or RMO must perform the measures as required by paragraphs 6, 7 and 8 when –

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

(a) the AE or RMO establishes business relations with a customer;

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

(c) the AE or RMO undertakes a digital CMP token transaction for a customer who has not otherwise established business relations with the AE or RMO;

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

(e) the AE or RMO has doubts about the veracity or adequacy of information previously obtained.

6.4 If an AE or RMO 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 paragraph 6.3(b), the AE or RMO must treat the transactions as a single transaction and aggregate their values for the purposes of this Notice.

(I) Identification of Customer

6.5 An AE or RMO must identify each customer.

6.6 For the purposes of paragraph 6.5, an AE or RMO must 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 if 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 If the customer is a legal person or legal arrangement, the AE or RMO must, 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 If the customer is a legal person or legal arrangement, the AE or RMO 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 AE or RMO –

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

6.10 The AE or RMO 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

6.11 An AE or RMO 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, an AE or RMO 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 an AE or RMO or the customer is not a natural person, the AE or RMO 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.

6.13 An AE or RMO must verify the due authority of the natural persons appointed to act on behalf of the customer by:

(a) obtaining the 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 AE or RMO –

(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 AE or RMO may obtain the business address of this natural person, in lieu of the residential address.

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

6.16 The AE or RMO 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 AE or RMO is only required to obtain the information as may be required to confirm that the customer is a Singapore Government entity as asserted.

(IV) <u>Identification and Verification of Identity of Beneficial Owner</u>

6.18 Subject to paragraph 6.21, an AE or RMO 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 AE or RMO 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 AE or RMO must –

(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 settlor, the trustee, the protector (if any), the beneficiaries (including beneficiaries that fall within a designated characteristic or class)[3], and natural persons 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).

6.20 If the customer is not a natural person, the AE or RMO must understand the nature of the customer's business and its ownership and control structure.

6.21 An AE or RMO 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) an investment vehicle where the managers are financial institutions –

(i) set out in Appendix 1; or

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

(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 AE or RMO 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.

(V) Information on the Purpose and Intended Nature of Business Relations

6.22 An AE or RMO 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.

(VI) Ongoing Monitoring

6.23 An AE or RMO must monitor on an ongoing basis, its business relations with customers.

6.24 An AE or RMO must, during the course of business relations with a customer, observe the conduct of the customer's account and scrutinise trade-related activities performed on the organised markets that it operates and any other activities that are incidental to such activities throughout the course of business relations, to ensure that the activities are consistent with the AE or RMO's knowledge of the customer, its business and risk profile and if appropriate, the source of funds.

6.25 An AE or RMO must perform enhanced risk mitigation measures if the transaction involves a transfer of one or more digital CMP tokens to or a receipt of one or more digital CMP 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.

6.26 An AE or RMO must pay special attention to all complex, unusually large or unusual patterns of trade-related activities performed on the organised markets that it operates throughout the course of business relations, that have no apparent or visible economic or lawful purpose.

6.27 For the purposes of ongoing monitoring, an AE or RMO must put in place and implement adequate systems and processes, commensurate with the size and complexity of the AE or RMO, to –

(a) monitor its business relations with customers; and

(b) detect and report suspicious, complex, unusually large or unusual patterns of trade-related activities on the organised markets that it operates, including trade-related activities performed by customers (whether as principal or agent).

6.28 An AE or RMO must, to the extent possible, inquire into the background and purpose of the trade-related activities 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 An AE or RMO 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.

6.30 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 AE or RMO considers it appropriate to retain the customer –

(a) the AE or RMO must substantiate and document the reasons for retaining the customer; and

(b) the customer's business relations with the AE or RMO must be subject to commensurate risk mitigation measures, including enhanced ongoing monitoring.

6.31 If the AE or RMO assesses the customer or the business relations with the customer mentioned in paragraph 6.30 to be of higher risk, the AE or RMO must perform enhanced CDD measures, which include obtaining the approval of the AE or RMO's senior management to retain the customer.

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

6.32 An AE or RMO must develop policies and procedures to address specific risks associated with non-face-to-face business relations with a customer or transactions for a customer.

6.33 An AE or RMO must implement the policies and procedures mentioned in paragraph 6.32 when establishing business relations with a customer and when conducting ongoing due diligence.

6.34 If there is no face-to-face contact, the AE or RMO 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.

Reliance by Acquiring AE or RMO on Measures Already Performed

6.35 When an AE or RMO ("acquiring AE or RMO") acquires, either in whole or in part, the business of another financial institution (whether in Singapore or elsewhere), the acquiring AE or RMO 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 AE or RMO 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 AE or RMO as to the adequacy of AML/CFT measures previously adopted in relation to

the business or part thereof now acquired by the acquiring AE or RMO and document the enquiries.

Measures for Non-Account Holder

6.36 An AE or RMO that undertakes a transaction (other than a digital CMP token transaction referred to in paragraph 6.37) of a value exceeding S$20,000 for a customer who does not otherwise have business relations with the AE or RMO must –

(a) perform CDD measures as if the customer had applied to the AE or RMO 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.

6.37 An AE or RMO that undertakes a digital CMP token transaction for a customer who does not otherwise have business relations with the AE or RMO must –

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

(b) record adequate details of the digital CMP 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 CMP token(s) involved, the value date, and the details of the payee or beneficiary.

Timing for Verification

6.38 Subject to paragraphs 6.39 and 6.40, an AE or RMO 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 6.19 –

(a) before the AE or RMO establishes business relations with the customer;

(b) before the AE or RMO undertakes a transaction (other than a digital CMP token transaction referred to in paragraph 6.38(c)) of a value exceeding S$20,000 for the customer, if the customer has not otherwise established business relations with the AE or RMO; or

(c) before the AE or RMO undertakes a digital CMP token transaction, if the customer has not otherwise established business relations with the AE or RMO.

6.39 An AE or RMO 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 6.19 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 AE or RMO.

6.40 If the AE or RMO 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 6.19, the AE or RMO 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.

If Measures are Not Completed

6.41 If the AE or RMO is unable to complete the measures as required under paragraphs 6, 7 and 8, it must not commence or continue business relations with a customer, or undertake a transaction, for a customer. The AE or RMO must consider if the circumstances are suspicious so as to warrant the filing of an STR.

6.42 For the purposes of paragraph 6.41, completion of the measures means the situation where the AE or RMO has obtained, screened and verified (including by delayed verification as allowed under paragraphs 6.39 and 6.40) all necessary CDD information required under paragraphs 6, 7 and 8, and the AE or RMO has received satisfactory responses to all the inquiries in relation to the necessary CDD information.

Joint Account

6.43 In the case of a joint account, an AE or RMO must perform CDD measures on all of the joint account holders as if each of them is an individual customer of the AE or RMO.

Existing Customers

6.44 An AE or RMO 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 previous measures applied, the time when the measures were last applied to the existing customers and the adequacy of data, documents or information obtained.

Screening

6.45 An AE or RMO 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.

6.46 An AE or RMO must screen the persons mentioned in paragraph 6.45 –

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

(b) when the AE or RMO undertakes a transaction (other than a digital CMP token transaction referred to in paragraph 6.46(e)) of a value exceeding S$20,000 for a customer who has not otherwise established business relations with the AE or RMO;

(c) on a periodic basis after the AE or RMO establishes business relations with the customer;

(d) when there is a change or update to –

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

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

(e) when the AE or RMO undertakes a digital CMP token transaction for a customer who has not otherwise established business relations with the AE or RMO.

6.47 The results of screening and assessment by the AE or RMO must be documented.

6.48 For the purposes of paragraph 6, a reference to "transaction" includes a digital CMP token transaction.

7 SIMPLIFIED CUSTOMER DUE DILIGENCE

7.1 Subject to paragraph 7.4, an AE or RMO 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 AE or RMO 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 AE or RMO.

7.3 The simplified CDD measures must be commensurate with the level of risk, based on the risk factors identified by the AE or RMO.

7.4 An AE or RMO must not perform simplified CDD measures –

(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;

(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 AE or RMO for itself or notified to AEs or RMOs generally by the Authority, or other foreign regulatory authorities; or

(c) if the AE or RMO suspects that money laundering or terrorism financing is involved.

7.5 If the AE or RMO 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.

7.6 To avoid 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 An AE or RMO 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 An AE or RMO 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 AE or RMO to be a politically exposed person, or a family member or close associate of a political exposed person under paragraph 8.2:

(a) obtain approval from the AE or RMO's senior management to establish or continue business relations with or undertake a 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 the beneficial owners 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 AE or RMO 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 An AE or RMO 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 or transactions with the AE or RMO present a higher risk for money laundering or terrorism financing.

Other Higher Risk Categories

8.5 An AE or RMO must implement appropriate internal risk management systems, policies, procedures and controls to determine if business relations with or transactions 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 AE or RMO must treat any business relations with or transactions for any such 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 AE or RMO, or notified to AEs and RMOs generally by the Authority or other foreign regulatory authorities, the AE or RMO must assess whether any such customer presents a higher risk for money laundering or terrorism financing; and

(c) if a customer is a legal person for which the AE or RMO is not able to establish if it has an –

(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 AE or RMO;

the AE or RMO must assess whether any such customer presents a higher risk for money laundering or terrorism financing.

8.7 An AE or RMO must perform the appropriate enhanced CDD measures in paragraph 8.3 for business relations with or transactions for a customer –

(a) whom the AE or RMO determines under paragraph 8.5; or

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

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

8.8 An AE or RMO must, in taking enhanced CDD measures to manage and mitigate any higher risks that have been identified by the AE or RMO, 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.

8.9 For the purposes of paragraph 8, a reference to "transaction" includes a digital CMP 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 an AE or RMO 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 an AE or RMO 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, an AE or RMO 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 AE or RMO 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 AE or RMO 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 AEs and RMOs 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 AE or RMO's request, data, documents or information obtained by the third party with respect to the measures applied on the AE or RMO's customer, which the AE or RMO would be required or would want to obtain.

9.3 An AE or RMO must not rely on a third party to conduct ongoing monitoring of business relations with customers.

9.4 If an AE or RMO 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 9.2(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.

9.5 To avoid doubt, despite the reliance upon a third party, the AE or RMO remains responsible for its AML/CFT obligations in this Notice.

10 RECORD KEEPING

10.1 An AE or RMO must, in relation to all data, documents and information that the AE or RMO is required to obtain or produce to comply with this Notice, prepare, maintain and retain records of the data, documents and information.

10.2 An AE or RMO must perform the measures as required by paragraph 10.1 such that -

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

(b) an individual transaction undertaken by the AE or RMO or individual trade-related activity performed on the organised markets operated by the AE or RMO 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 AE or RMO are able to review the AE or RMO's business relations, transactions, records and CDD information and assess the level of compliance with this Notice; and

(d) the AE or RMO 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.

10.3 Subject to paragraph 10.5 and other requirements imposed by law, an AE or RMO must, for the purposes of record retention under paragraphs 10.1 and 10.2, and when setting its record retention policies, comply with the following record retention periods:

(a) for CDD information relating to the business relations and 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 transactions; and

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

10.4 An AE or RMO 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.

10.5 An AE or RMO 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.

10.6 For the purposes of paragraph 10, a reference to "transaction" includes a digital CMP token transaction.

11 PERSONAL DATA

11.1 For the purposes of paragraph 11, "individual" means a natural person, whether living or deceased.

11.2 Subject to paragraph 11.3 and for the purposes of complying with this Notice, an AE or RMO 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 AE or RMO;

(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 AE or RMO; and

(c) a 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 AE or RMO.

11.3 An AE or RMO 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 AE or RMO:

(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 AE or RMO; 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 AE or RMO is satisfied that there are reasonable grounds for the request.

11.4 For the purposes of complying with this Notice, an AE or RMO 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.

12 SUSPICIOUS TRANSACTIONS REPORTING

12.1 An AE or RMO must keep in mind the provisions in the CDSA[4] 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, officers and representatives 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.

12.2 An AE or RMO 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.

12.3 An AE or RMO 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 AE or RMO is for any reason unable to complete the measures as required by paragraphs 6, 7 and 8; or

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

12.4 If an AE or RMO 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 AE or RMO may stop performing those measures. The AE or RMO must document the basis for its assessment and file an STR.

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

12.5 For the purposes of paragraph 12, a reference to "transaction" includes a digital CMP token transaction.

13 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

13.1 An AE or RMO 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.

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

Group Policy

13.3 For the purposes of paragraphs 13.4 to 13.9, a reference to "AE" and "RMO" means an AE or RMO incorporated in Singapore.

13.4 An AE or RMO 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.

13.5 If an AE or RMO 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 AE or RMO for itself, notified to AEs and RMOs generally by the Authority or other foreign regulatory authorities,

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

13.6 Subject to the AE or RMO putting in place adequate safeguards to protect the confidentiality and use of information that is shared, the AE or RMO 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.

13.7 The policies and procedures mentioned in paragraph 13.6 must include the provision, to the AE or RMO'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.

13.8 For the purposes of paragraph 13.7, the information to be shared with the AE or RMO's financial group must include information and analysis of transactions or activities that appear unusual.[5]

[5] 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.

13.9 If the AML/CFT requirements in the host country or jurisdiction differ from those in Singapore, the AE or RMO 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.

13.10 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 AE or RMO 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.

13.11 In the case of a Singapore branch of an AE or RMO incorporated outside Singapore, subject to the Singapore branch putting in place adequate safeguards to protect the confidentiality and use of information that is shared, the Singapore branch must share customer, account and transaction information within the AE or RMO's financial group when necessary for money laundering and terrorism financing risk management purposes. The information to be shared within the AE or RMO's financial group must include information and analysis of transactions or activities that appear unusual.[6]

Compliance

13.12 An AE or RMO must develop appropriate compliance management arrangements, including at least, the appointment of an AML/CFT compliance officer at the management level.

13.13 An AE or RMO 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

13.14 An AE or RMO must maintain an audit function that is adequately resourced and independent, and that is able to regularly assess the effectiveness of the AE or RMO's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

13.15 An AE or RMO must have in place screening procedures to ensure high standards when hiring employees and appointing officers.

Training

13.16 An AE or RMO 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

[6] 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.

(c) the AE or RMO's internal AML/CFT policies, procedures and controls, and the roles and responsibilities of employees and officers in combating money laundering and terrorism financing.

13.17 For the purposes of paragraph 13, a reference to "transaction" includes a digital CMP 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 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 paragraphs 3(1)(d), 3A(1)(d) or 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 an investment product.

8. Persons exempted under section 99(1)(h) of the SFA read with paragraphs 3(1)(d), 3A(1)(d) or 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.