MAS Notice PSN02

5 December 2019

NOTICE TO HOLDERS OF PAYMENT SERVICE LICENCE (DIGITAL PAYMENT TOKEN SERVICE)
MONETARY AUTHORITY OF SINGAPORE ACT, CAP. 186

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

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 27B of the Monetary Authority of Singapore Act (Cap. 186) ("MAS Act") and applies to all holders of a payment service licence under the Payment Services Act 2019 (Act 2 of 2019) ("PS Act") that carry on a business of providing digital payment token service ("payment service provider").

1.2 This Notice shall take effect from 28 January 2020.

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" has the same meaning as section 2(1) of the Banking Act (Cap. 19);

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

"bearer negotiable instrument" means –

(a) a traveller's cheque; or

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

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

omitted;

"beneficial owner", in relation to a customer of a payment service provider, means the natural person who ultimately owns or controls the customer or the natural person on whose behalf a transaction is conducted or business relations are established, and includes any person who exercises ultimate effective control over a legal person or legal arrangement;

"beneficiary institution" means the financial institution that receives the value transfer from the ordering institution, directly or through an intermediary institution, and makes one or more digital payment tokens available to the value transfer beneficiary;

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

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

"cash" means physical currency;

"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 (Cap. 65A);

"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;

"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 payment service provider, means a person (whether a natural person, legal person or legal arrangement) –

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

(a) with whom the payment service provider establishes or intends to establish business relations; or

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

"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;

"FATF" means the Financial Action Task Force;

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

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

"government entity" means a government of a country or jurisdiction, a ministry within 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;

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

"merchant bank in Singapore" means –

(a) a merchant bank incorporated in Singapore; or

(b) in the case of a merchant bank incorporated outside Singapore, the branches and offices of the merchant bank located within Singapore;

"officer" —

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

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

(c) in relation to a payment service provider that is a legal arrangement, means any

member of the committee of management of the legal arrangement;

"partnership" means a partnership, a limited partnership within the meaning of the Limited Partnerships Act (Cap. 163B) or a limited liability partnership within the meaning of the Limited Liability Partnerships Act (Cap. 163A);

"ordering institution" means the financial institution that initiates the value transfer and transfers one or more digital payment tokens upon receiving the request for a value transfer on behalf of the value transfer originator;

"personal data" has the same meaning as defined in section 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012);

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

"recipient" —

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

(b) means an FX counterparty;

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

(a) a financial institution as defined in section 27A(6) of the MAS 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;

"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;

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

"TSOFA" means the Terrorism (Suppression of Financing) Act (Cap. 325); and

"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 payment tokens 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 payment service provider's compliance with the relevant threshold or value limit, either as published by the payment service provider in the course of its business or offered by the payment service provider to its customer in relation to the 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 PS Act.

3 UNDERLYING PRINCIPLES

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

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

(c) A payment service provider 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 payment service provider 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 payment service provider has operations in; and

(d) the products, services, transactions and delivery channels of the payment service provider.

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

(a) documenting the payment service provider'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 payment service provider's risk assessments up-to-date; and

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

Risk Mitigation

4.3 A payment service provider shall —

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

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

(c) perform enhanced measures 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 address the risk assessment and guidance from the Authority or other relevant authorities in Singapore.

5 NEW PRODUCTS, PRACTICES AND TECHNOLOGIES

5.1 A payment service provider 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 pre-existing products.

5.2 A payment service provider 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 payment service provider 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 Fictitious Account

6.1 No payment service provider 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 payment service provider establishing business relations or undertaking any transaction without opening an account, where the payment service provider 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 payment service provider 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 payment service provider shall perform the measures as required by paragraphs 6, 7 and 8 when —

(a) the payment service provider establishes business relations with any customer;

(b) the payment service provider undertakes any transaction for any customer who has not otherwise established business relations with the payment service provider;

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

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

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

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

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

6.5 A payment service provider shall identify each customer.

6.6 For the purposes of paragraph 6.5, a payment service provider 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 –

[2] Please note in particular section 48 of the CDSA on tipping-off.

(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 payment service provider 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 payment service provider 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).

(II) Verification of Identity of Customer

6.9 A payment service provider 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 payment service provider 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 his behalf in establishing business relations with a payment service provider or the customer is not a natural person, the payment service provider 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 payment service provider shall verify the due authority of each natural person appointed to act on behalf of the customer by obtaining at least the following:

(a) appropriate documentary evidence authorising the appointment of such natural person by the customer to act on his or its behalf; and

(b) the specimen signature of each natural person appointed.

6.12 Where the customer is a Singapore Government entity, the payment service provider 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 payment service provider shall inquire if there exists any beneficial owner in relation to a customer.

6.14 Where there is one or more beneficial owner in relation to a customer, the payment service provider 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 payment service provider 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 subparagraph (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 payment service provider shall understand the nature of the customer's business and its ownership and control structure.

6.16 A payment service provider shall not be required to inquire if there exists any beneficial owner, in relation to a customer that is —

(a) an entity listed on the Singapore Exchange;

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

(i) regulatory disclosure requirements; and

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

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

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

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

(i) set out in Appendix 1; or

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

(a) before making a distribution to that beneficiary; or
(b) when that beneficiary intends to exercise vested rights.

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

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

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

6.18 A payment service provider shall, when processing the application to establish business relations or undertake a transaction without an account being opened, understand and as appropriate, obtain from the customer information as to the purpose and intended nature of business relations or transaction.

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

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

6.20 Where a payment service provider establishes business relations with a customer, the payment service provider shall review any transaction undertaken before the business relations are established, to ensure that the business relations are consistent with the payment service provider's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

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

6.22 For the purposes of reviewing transactions undertaken without an account being opened as required by paragraph 6.19, a payment service provider shall put in place and implement adequate systems and processes, commensurate with the size and complexity of the payment service provider to —

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

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

6.23 A payment service provider 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 Where there are any reasonable grounds for suspicion that a transaction for a customer undertaken without an account being opened is connected with money laundering or terrorism financing, and where the payment service provider considers it appropriate to undertake the transaction, the payment service provider shall substantiate and document the reasons for undertaking the transaction.

(VI) Ongoing Monitoring

6.25 A payment service provider shall monitor on an ongoing basis, its business relations with customers.

6.26 A payment service provider 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 payment service provider's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

6.27 A payment service provider shall perform enhanced risk mitigation measures where the transaction involves a transfer of a digital payment token to or a receipt of a digital payment token from an entity other than:

(i) a financial institution as defined in section 27A(6) of the MAS Act; or

(ii) 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.

6.28 A payment service provider 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.

6.29 For the purposes of ongoing monitoring, a payment service provider shall put in place and implement adequate systems and processes, commensurate with the size and complexity of the payment service provider to —

(a) monitor its business relations with customers; and

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

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

6.31 A payment service provider 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.

6.32 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 payment service provider considers it appropriate to retain the customer —

(a) the payment service provider shall substantiate and document the reasons for retaining the customer; and

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

6.33 Where the payment service provider assesses the customer or the business relations with the customer referred to in paragraph 6.32 to be of higher risk, the payment service provider shall perform enhanced CDD measures, which shall include obtaining the approval of the payment service provider's senior management to retain the customer.

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

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

6.35 A payment service provider shall implement the policies and procedures referred to in paragraph 6.34 when establishing business relations with a customer and when conducting ongoing due diligence.

6.36 Where there is no face-to-face contact, the payment service provider shall perform CDD measures that are at least as stringent as those that would be required to be performed if there was face-to-face contact.

6.37 Where a payment service provider conducts its first non-face-to-face business contact, the payment service provider shall, at his or its own expense, appoint an external auditor or an independent qualified consultant to assess the effectiveness of the policies and

procedures referred to in paragraph 6.34, including the effectiveness of any technology solutions used to manage impersonation risks.

6.38 The payment service provider shall submit to the Authority a report of the assessment no later than one year after conduct of the payment service provider's non-face-to-face business contact.

6.39 Where there has been a substantial change in the policies and procedures referred to in paragraph 6.34, the payment service provider shall appoint an external auditor or an independent qualified consultant to carry out an assessment of the new policies and procedures, and shall submit the report of the assessment to the Authority no later than one year after the implementation of the change in policies and procedures.

Reliance by Acquiring Payment Service Provider on Measures Already Performed

6.40 When a payment service provider ("acquiring payment service provider") acquires, either in whole or in part, the business of another payment service provider (whether in Singapore or elsewhere), the acquiring payment service provider 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 payment service provider 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 payment service provider as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring payment service provider, and document such enquiries.

Measures for Non-Account Holder

6.41 A payment service provider that undertakes any transaction for any customer who does not otherwise have business relations with the payment service provider shall —

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

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

Timing for Verification

6.42 Subject to paragraphs 6.43 and 6.44, a payment service provider 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 before —

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

(b) the payment service provider undertakes any transaction for the customer, where the customer has not otherwise established business relations with the payment service provider; or

(c) the payment service provider effects or receives digital payment tokens by value transfer for the customer, where the customer has not otherwise established business relations with the payment service provider.

6.43 A payment service provider 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 payment service provider.

6.44 Where the payment service provider 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 payment service provider 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

6.45 Where the payment service provider 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.

6.46 Where the payment service provider is unable to complete the measures as required by paragraphs 6, 7 and 8, the payment service provider shall consider if the circumstances are suspicious so as to warrant the filing of an STR.

6.47 For the purposes of paragraphs 6.45 and 6.46, completion of the measures means the situation where the payment service provider has obtained, screened and verified (including by delayed verification as allowed under paragraphs 6.43 and 6.44) all necessary CDD information under paragraphs 6, 7 and 8, and where the payment service provider has received satisfactory responses to all inquiries in relation to such necessary CDD information.

Joint Account

6.48 In the case of a joint account, a payment service provider shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the payment service provider.

Screening

6.49 A payment service provider 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.

6.50 A payment service provider shall screen the persons referred to in paragraph 6.49 —

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

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

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

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

(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 payment service provider; or

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

6.51 A payment service provider shall screen all value transfer originators and value transfer beneficiaries as defined in paragraph 13, 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.

6.52 The results of screening and assessment by the payment service provider shall be documented.

7 SIMPLIFIED CUSTOMER DUE DILIGENCE

7.1 Subject to paragraph 7.4, a payment service provider 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 payment service provider 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 payment service provider.

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

7.4 A payment service provider shall not perform simplified CDD measures —

(a) where one or more transactions undertaken, whether in the course of business relations or otherwise, by the payment service provider for a customer in any one year period cumulatively exceeds S$20,000[4];

(b) 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;

(c) 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 payment service provider for itself or notified to payment service providers generally by the Authority, or other foreign regulatory authorities; or

(d) where the payment service provider suspects that money laundering or terrorism financing is involved.

7.5 Subject to paragraphs 7.2, 7.3 and 7.4, a payment service provider may perform

[4] Please note paragraph 6.4 of the Notice.

simplified CDD measures in relation to a customer that is a financial institution set out in Appendix 2.

7.6 Where the payment service provider 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;

"international organisation" means an entity established by formal political agreements between member countries that have the status of international treaties, whose existence is recognised by law in member countries and which is not treated as a resident institutional unit of the country 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 payment service provider 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.

8.3 A payment service provider 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 payment service provider to be a politically exposed person, or a family member or close associate of a politically exposed person under paragraph 8.2:

(a) obtain approval from the payment service provider's senior management to establish or continue business relations with 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 the 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 payment service provider may adopt a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for —

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

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

(c) politically exposed persons who have stepped down from their prominent public functions, taking into consideration the level of influence 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 with the payment service provider or transaction without an account being opened by the payment service provider present a higher risk for money laundering or terrorism financing.

Other Higher Risk Categories

8.5 A payment service provider shall implement appropriate internal risk management systems, policies, procedures and controls to determine if business relations with or transactions undertaken without an account being opened for any 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) 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 payment service provider shall treat any business relations with or transactions for any such customer as presenting a higher risk for money laundering or terrorism financing; and

(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 payment service provider for itself or notified to payment service providers generally by the Authority or other foreign regulatory authorities, the payment service provider shall assess whether any such customer presents a higher risk for money laundering or terrorism financing.

8.7 A payment service provider shall perform the appropriate enhanced CDD measures in paragraph 8.3 for business relations with, or transactions for any customer —

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

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

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

8.8 A payment service provider shall, in taking enhanced CDD measures to manage and mitigate any higher risks that have been identified by the payment service provider or notified to it by the Authority or other relevant authorities in Singapore, ensure that the enhanced CDD measures take into account the requirements of any laws, regulations or directions administered by the Authority, including but not limited to the regulations or directions issued by the Authority under section 27A of the MAS Act.

9 FOREIGN CURRENCY EXCHANGE TRANSACTIONS

9.1 Where the value of an FX transaction is equal or exceeds S$20,000 (or its equivalent in a foreign currency), a payment service provider shall comply with paragraphs 6, 7, and 8

in relation to an FX transaction as if the references to a customer and transaction in those paragraphs were references to a relevant FX counterparty and the FX transaction respectively.

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

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

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

10 ISSUANCE OF BEARER NEGOTIABLE INSTRUMENTS AND RESTRICTION OF CASH PAYOUT

Prohibition of Issuance of Bearer Negotiable Instruments

10.1 No payment service provider shall in the course of carrying on its business to provide a specified payment service or an FX transaction make any payment for any sum of money in the form of a bearer negotiable instrument to any recipient or to any person appointed to act on behalf of a recipient.

Restriction on Cash Payouts by Payment Service Providers

10.2 No payment service provider shall, in respect of a payment transaction processed, accepted, or executed in the course of carrying on its business to provide a specified payment service, or an FX transaction, pay any cash in an amount that is equal to or exceeds S$20,000 to any recipient or person appointed to act on behalf of a recipient.

10.3 Where a payment provider suspects that two or more payment transactions or FX transactions, as the case may be, are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for in paragraph 10.2, the payment service provider shall treat the payment transactions or FX transactions, as the case may be, as a single transaction and aggregate their value for the purposes of paragraph 10.2.

10.4 A payment service provider may make any payment of S$20,000 and above by cheque if all the following conditions are met:

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

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

10.5 Paragraph 10 shall not apply to any payment service provider that holds a casino licence under section 49 of the Casino Control Act (Cap. 33A).

11 RELIANCE ON THIRD PARTIES

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

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

(b) a financial institution which is subject to and supervised by a foreign authority for compliance with AML/CFT requirements consistent with standards set by the FATF (other than a holder of a payment services licence or equivalent licence); and

(c) the parent entity, the branches and subsidiaries of the parent entity, and other related corporations, of a payment service provider (except where such entity is a holder of a payment services licence or equivalent licence).

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

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

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

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

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

11.3 No payment service provider shall rely on a third party to conduct ongoing monitoring of business relations with customers.

11.4 Where a payment service provider 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 paragraph 11.2(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.

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

12 CORRESPONDENT ACCOUNTS

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

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

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

(i) a bank in Singapore; or

(ii) a merchant bank in Singapore.

12.2 For the purposes of paragraph 12 —

"correspondent account services" means:

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

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

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

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

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

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

"similar services" include:

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

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

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

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

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

(ii) determine from 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 the payment service provider and the respondent financial institution; and

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

12.4 Where the provision of correspondent account services or similar services by the payment service provider involve a payable-through account, the payment service provider 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 payment service provider upon request.

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

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

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

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

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

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

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

12.6 The payment service provider shall document the basis for its satisfaction that the requirements in paragraphs 12.3 to 12.5 are met.

12.7 No payment service provider shall enter into or continue correspondent account services or other similar services relationship with another financial institution that does not have adequate controls against money laundering or terrorism financing activities, is not effectively supervised by the relevant authorities or is a shell financial institution.

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

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

13 VALUE TRANSFERS

13.1 Paragraph 13 shall apply to a payment service provider when it effects the sending of one or more digital payment tokens by value transfer or when it receives one or more digital payment 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 payment service provider and another financial institution where the payment service provider and the other financial institution are acting on their own behalf as the value transfer originator and the value transfer beneficiary.

13.2 For the purposes of paragraph 13 —

"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 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 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 payment 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

13.3 Before effecting a value transfer, every payment service provider that is an ordering institution shall —

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

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

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

13.4 Subject to paragraph 13.5, in a value transfer where the amount to be transferred is below or equal to S$1,500, every payment service provider 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).

13.5 In a value transfer where the amount to be transferred is below or equal to S$1,500, every payment service provider which is an ordering institution may, in the message or payment instruction that accompanies or relates to the value transfer to an intermediary institution in Singapore, include only the unique transaction reference number and the value transfer beneficiary information set out in paragraph 13.4(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 paragraph 13.4(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 paragraph 13.4(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 paragraph 13.4(a) to (d) to the beneficiary institution.

(III) <u>Value Transfers Exceeding S$1,500</u>

13.6 Subject to paragraph 13.8, in a value transfer where the amount to be transferred exceeds S$1,500, every payment service provider which is an ordering institution shall identify the value transfer originator and verify his or its identity, and include in the message or payment instruction that accompanies or relates to the value transfer the information required by paragraph 13.4(a) to 13.4(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).

13.7 Where several individual value transfers from a single value transfer originator are bundled in a batch file for transmission to value transfer beneficiaries, a payment service provider shall ensure that the batch transfer file contains —

(a) the value transfer originator information required by paragraph 13.6[5] and which has been verified; and

(b) the value transfer beneficiary information required by paragraph 13.6[6],

which are fully traceable within the beneficiary country.

13.8 In a value transfer where the amount to be transferred exceeds S$1,500, every payment service provider which is an ordering institution may, in the message or payment instruction that accompanies or relates to the value transfer to an intermediary institution in Singapore, include only the unique transaction reference number and the value transfer beneficiary information required by paragraph 13.6[7], 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 13.6[8] 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 13.6[9] 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

[5] Please note the references to paragraph 13.4 (a) and (b) in paragraph 13.6.

[6] Please note the references to paragraph 13.4 (c) and (d) in paragraph 13.6.

[7] Please note the references to paragraph 13.4 (c) and (d) in paragraph 13.6.

[8] Please note the references to paragraph 13.4 (a) to (d) in paragraph 13.6.

[9] Please note the references to paragraph 13.4 (a) to (d) in paragraph 13.6.

value transfer beneficiary information set out in paragraph 13.6 to the beneficiary institution.

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

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

13.11 Where the ordering institution is unable to comply with the requirements in paragraphs 13.3 to 13.10, it shall not execute the value transfer.

Responsibility of the Beneficiary Institution

13.12 A payment service provider 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.

13.13 For value transfers where the beneficiary institution pays out the transferred digital payment 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.

13.14 A payment service provider 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.

13.15 For a payment service provider 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 affected by the value transfer, and make transaction information available to the relevant authorities.

Responsibility of the Intermediary Institution

13.16 A payment service provider that is an intermediary institution shall retain all the information accompanying the value transfer.

13.17 Where a payment service provider that is an intermediary institution effects a value transfer to another intermediary institution or a beneficiary institution, the payment service provider shall immediately and securely provide the information accompanying the value transfer, to that other intermediary institution or beneficiary institution.

13.18 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.

13.19 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.

13.20 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.

14 RECORD KEEPING

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

14.2 A payment service provider shall perform the measures as required by paragraph 14.1 such that —

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

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

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

(d) the payment service provider 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.

14.3 Subject to paragraph 14.5 and any other requirements imposed by law, a payment service provider shall, for the purposes of record retention under paragraphs 14.1 and 14.2 and when setting its record retention policies, comply with the following record retention periods:

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

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

14.5 A payment service provider 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.

15 PERSONAL DATA

15.1 For the purposes of paragraph 15, “individual” means a natural person, whether living or deceased.

15.2 Subject to paragraph 15.3 and for the purposes of complying with this Notice, a payment service provider shall not be 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) any access to personal data about the individual that is in the possession or under the control of the payment service provider;

(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 payment service provider; 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 payment service provider.

15.3 A payment service provider 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 payment service provider:

(i) his full name, including any alias;

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

(iii) his residential address;

(iv) his date of birth;

(v) his nationality;

(vi) subject to section 21(2) and (3) read with the Fifth Schedule to the Personal Data Protection Act 2012 (Act 26 of 2012), any other personal data of the respective individual provided by that individual to the payment service provider; and

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

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

16 SUSPICIOUS TRANSACTIONS REPORTING

16.1 A payment service provider shall keep in mind the provisions in the CDSA[10] 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.

16.2 A payment service provider 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.

16.3 A payment service provider 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 payment service provider 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 payment service provider, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

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

17 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

17.1 A payment service provider 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

[10] Please note in particular section 48 of the CDSA on tipping-off.

terrorism financing and communicate these to its employees.

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

Compliance

17.3 A payment service provider shall develop appropriate compliance management arrangements, including at least, the appointment of an AML/CFT compliance officer, at the management level.

17.4 A payment service provider shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, is suitably qualified and, has adequate resources and timely access to all customer records and other relevant information which he requires to discharge his functions.

Audit

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

Employee Hiring

17.6 A payment service provider shall have in place screening procedures to ensure high standards when hiring employees and appointing officers.

Training

17.7 A payment service provider 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, detecting and reporting of suspicious transactions;

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

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

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 (Cap. 336) read with regulation 4 of the Trust Companies (Exemption) Regulations (Rg. 1).

2. Persons exempted under section 23(1)(f) of the Financial Advisers Act (Cap. 110) read with regulation 27(1)(d) of the Financial Advisers Regulations (Rg. 2).

3. Persons exempted under section 99(1)(h) of the Securities and Futures Act (Cap. 289) 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 section 7 of the Banking Act (Cap.19).

2. Merchant banks approved under section 28 of the Monetary Authority of Singapore Act (Cap. 186).

3. Finance companies licensed under section 6 of the Finance Companies Act (Cap. 108).

4. Financial advisers licensed under section 6 of the Financial Advisers Act (Cap. 110) 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 Securities and Futures Act (Cap. 289).

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 23(1)(f) of the Financial Advisers Act 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 Securities and Futures Act 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 Securities and Futures Act.

10. Trust companies licensed under section 5 of the Trust Companies Act (Cap. 336).

11. Direct life insurers licensed under section 8 of the Insurance Act (Cap. 142).

12. Insurance brokers registered under the Insurance Act which, by virtue of such registration, are exempted under section 23(1)(c) of the Financial Advisers Act 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.