Monetary Authority of Singapore

GUIDELINES TO MAS NOTICE PS-N02 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

16 MARCH 2020

TABLE OF CONTENTS

For ease of reference, the chapter numbers in these Guidelines mirror the corresponding paragraph numbers in the MAS Notice PS-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Holders of Payment Service Licence (Digital Payment Token Service) (e.g. Chapter 2 of the Guidelines provides guidance in relation to paragraph 2 of the Notice). Not every paragraph in the Notice has a corresponding paragraph in these Guidelines and this explains why not all chapter numbers are utilised in these Guidelines.

GUIDELINES TO MAS NOTICE PS-N02 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

1 Introduction

1-1 These Guidelines provide guidance to all holders of a payment service licence that carry on a business of providing digital payment token ("DPT") service (hereinafter "payment service providers") on the requirements in MAS Notice PS-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Service Licence (Digital Payment Token Service) ("the Notice"). These Guidelines should be read in conjunction with the Notice.

1-2 The expressions used in these Guidelines have the same meanings as those found in the Notice, except where expressly defined in these Guidelines or where the context otherwise requires. For the purpose of these Guidelines, a reference to "CDD measures" shall mean the measures as required by paragraphs 6, 7 and 8 of the Notice.

1-3 The degree of observance with these Guidelines by a payment service provider may have an impact on the Authority's overall risk assessment of the payment service provider, including the quality of its board and senior management oversight, governance, internal controls and risk management.

1-4 Key Concepts

Money Laundering

1-4-1 Money laundering ("ML") is a process intended to mask the benefits derived from criminal conduct so that they appear to have originated from a legitimate source. Singapore's primary legislation to combat ML is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A). A payment service provider should refer to the website of the Singapore Police Force's Commercial Affairs Department ("CAD") for more information.

1-4-2 Generally, the process of ML comprises three stages, namely —

(a) Placement – The physical or financial disposal of the benefits derived from criminal conduct. Such benefits (or assets) would include digital payment tokens, and other types of virtual assets.

(b) Layering – The separation of these benefits from their original source by creating layers of financial transactions designed to disguise the ultimate source and transfer of these benefits.

(c) Integration – The provision of apparent legitimacy to the benefits derived from criminal conduct. If the layering process succeeds, the integration schemes place the laundered funds or assets back into the economy so that they re-enter the financial system appearing to be legitimate funds or assets.

1-4-3 As transactions facilitated by payment service providers are unlikely to be predominantly cash based, they are more likely to be used in the layering stage. However, where the transactions involve cash, there is an increased risk of these

transactions being used at the placement stage (for funding) or integration (for withdrawals).

1-4-4 Transactions facilitated by payment service providers offer a vast array of opportunities for transforming money into a diverse range of assets. The ease with which these assets can be converted to other types of assets, especially if such assets are liquid, also aids the layering process. Hence, such transactions are particularly attractive to money-launderers for layering their illicit proceeds for eventual integration into the general economy.

Terrorism Financing

1-4-5 Acts of terrorism seek to influence or compel governments into a particular course of action or to intimidate the public or a section of the public. Payment service providers are reminded of the broad definitions of "terrorist" and "terrorist acts" set out in the Terrorism (Suppression of Financing) Act (Cap. 325) ("TSOFA").

1-4-6 Terrorists require funds to carry out acts of terrorism, and support their nefarious activities. Terrorism financing ("TF") is the act of providing these funds.

1-4-7 The funds or assets may be raised or obtained from criminal activities such as robbery, drug-trafficking, kidnapping, extortion, fraud, or hacking of online accounts. They can also be moved through various means, before being converted and put to use for illicit purposes. In cases where they are related to criminal activities, there may also be an element of ML involved to disguise the source of funds or to move them.

1-4-8 However, terrorist acts and organisations may also be raised from legitimate sources such as donations from charities, legitimate business operations, self-funding by individuals, etc. Coupled with the fact that TF need not always involve large sums of money, TF can be hard to detect and payment service providers should remain vigilant.

1-4-9 Singapore's primary legislation to combat TF is the TSOFA. Payment service providers may also refer to the MAS website and Inter-Ministry Committee on Terrorist Designation's website for more information.

The Three Lines of Defence

1-4-10 Each payment service provider is reminded that the ultimate responsibility and accountability for ensuring compliance with anti-money laundering and countering the financing of terrorism ("AML/CFT") laws, regulations and notices rests with its board of directors and senior management.

1-4-11 A payment service provider's board of directors and senior management are responsible for ensuring strong governance and sound ML/TF risk management and controls at the payment service provider. While certain responsibilities can be delegated to senior AML/CFT employees, final accountability rests with the payment service provider's board of directors and senior management. A payment

service provider should ensure a strong compliance culture throughout its organisation, where the board of directors and senior management set the right tone. The board of directors and senior management should also set a clear risk appetite and ensure a strong compliance culture.

1-4-12 Business units (e.g. front office customer-facing functions of the payment service provider's business) constitute the first line of defence in charge of identifying, assessing and controlling the ML/TF risks of their business. The second line of defence includes the AML/CFT compliance function, as well as other support functions such as operations, human resource or technology, which work together with the AML/CFT compliance function to identify ML/TF risks when they process transactions or applications or deploy systems or technology. The third line of defence is the payment service provider's internal audit function or external audit firm appointed by the payment service provider as set out in paragraph 1-4-15.

1-4-13 As part of the first line of defence, a payment service provider should ensure that its customer-facing functions have in place robust controls to detect illicit activities. This includes having sufficient resources, including IT, to perform this function effectively, clear communication of AML/CFT policies, procedures and controls, as well as adequate training of the relevant staff in customer-facing functions. The payment service provider's policies, procedures and controls on AML/CFT should be clearly specified in writing, and communicated to all relevant employees and officers in the customer-facing functions. The payment service provider should adequately train employees and officers to be aware of their obligations, and provide instructions as well as guidance on how to ensure the payment service provider's compliance with prevailing AML/CFT laws, regulations and notices.

1-4-14 As the core of the second line of defence, the AML/CFT compliance function is responsible for ongoing monitoring of the payment service provider's fulfilment of all AML/CFT duties by the payment service provider. This implies sample testing and the review of exception reports. The AML/CFT compliance function should alert the payment service provider's senior management or the board of directors if it believes that its employees or officers are failing or have failed to adequately address ML/TF risks and concerns. Other support functions such as operations, human resource or technology also play a role to help mitigate the ML/TF risks that the payment service provider faces. The AML/CFT compliance function is typically the contact point regarding all AML/CFT issues for domestic and foreign authorities, including supervisory authorities, law enforcement authorities and financial intelligence units.

1-4-15 As the third line of defence, the payment service provider's internal audit function plays an important role in independently evaluating the ML/TF risk management framework and controls for purposes of reporting to the audit committee of the payment service provider's board of directors, or a similar oversight body. This independent evaluation is achieved through the internal audit or equivalent function's periodic evaluations of the effectiveness of the payment service provider's compliance with prevailing AML/CFT policies, procedures and controls. Where there is no internal audit function, the payment service provider should engage an external audit firm to audit the AML/CFT risk management framework

and controls, in the course of auditing the digital payment token service business for the submission of statutory returns to the Authority, and in so doing, to act as the third line of defence. A payment service provider should establish policies for periodic AML/CFT internal audits covering areas such as —

(a) the adequacy of the payment service provider's AML/CFT policies, procedures and controls in identifying ML/TF risks, addressing the identified risks and complying with laws, regulations and notices;

(b) the effectiveness of the payment service provider's implementation of the payment service provider's policies, procedures and controls;

(c) the effectiveness of the compliance oversight and quality control including parameters and criteria for transaction alerts; and

(d) the effectiveness of the payment service provider's training of relevant employees and officers.

Governance

1-4-16 The payment service provider's board of directors and senior management should ensure that the payment service provider's processes are robust and there are adequate risk mitigating measures in place. The successful implementation and effective operation of a risk-based approach to AML/CFT depends on the payment service provider's employees and officers having a good understanding of the ML/TF risks inherent in the payment service provider's business.

1-4-17 A payment service provider's board of directors and senior management should understand the ML/TF risks the payment service provider is exposed to and how the payment service provider's AML/CFT control framework operates to mitigate those risks. This should involve the board of directors and senior management —

(a) receiving sufficient, timely and objective information to form an accurate picture of the ML/TF risks including emerging or new ML/TF risks, which the payment service provider is exposed to through its activities or business relations;

(b) receiving sufficient and objective information to assess whether the payment service provider's AML/CFT controls are adequate and effective;

(c) receiving information on legal and regulatory developments and the impact these have on the payment service provider's AML/CFT framework; and

(d) ensuring that processes are in place to escalate important decisions that directly impact the ability of the payment service provider to address and control ML/TF risks, especially where AML/CFT controls are assessed to be inadequate or ineffective.

2 Notice Paragraph 2 – Definitions, Clarifications and Examples

Connected Party

2-1 The term "partnership" as it appears in the definition of "connected party" includes foreign partnerships. The term "manager" as it appears in limb (b) of the definition of "connected party" takes reference from section 2(1) of the Limited Liability Partnership Act (Cap. 163A) and section 28 of the Limited Partnership Act (Cap. 163B).

2-2 Examples of natural persons with executive authority in a company include the Chairman and Chief Executive Officer. An example of a natural person with executive authority in a partnership is the Managing Partner.

Legal Arrangements

2-3 In relation to the definition of "legal arrangement" in the Notice, examples of legal arrangements are trust, fiducie, treuhand and fideicomiso.

Legal Persons

2-4 In relation to the definition of "legal person" in the Notice, examples of legal persons are companies, bodies corporate, foundations, anstalt, partnerships, joint ventures or associations.

Officer

2-5 A reference to "officer" refers to a payment service provider's board of directors, senior management or equivalent functions.

Custodian Wallet Service

2-6 In relation to a "custodian wallet service", a person is deemed to have control over a digital payment token if the person has control over the digital payment token whether jointly or severally with one of more persons.

2-7 In addition –

(a) A digital payment token instrument means any instrument that enables control over the digital payment token associated with the instrument, such as the private key that allows a user to access his or her digital payment token(s);

(b) The service of administration of a digital payment token or instrument means the service of carrying out an instruction relating to a digital payment token for a customer, or a digital payment token associated with the digital payment token instrument for a customer.

4 Notice Paragraph 4 – Assessing Risks and Applying a Risk-Based Approach

Countries or Jurisdictions of its Customers

4-1 In relation to a customer who is a natural person, this refers to the nationality and place of domicile, business or work. For a customer who is a legal person or arrangement, this refers to both the country or jurisdiction of establishment, incorporation, or registration, and, if different, the country or jurisdiction of operations as well.

Other Relevant Authorities in Singapore

4-2 Examples include law enforcement authorities (e.g. Singapore Police Force, CAD, Corrupt Practices Investigation Bureau) and other government authorities (e.g. Attorney General's Chambers, Ministry of Home Affairs, Ministry of Finance, Ministry of Law).

Risk Assessment

4-3 In addition to assessing the ML/TF risks presented by an individual customer, a payment service provider shall identify and assess ML/TF risks on an enterprise-wide level. This shall include a consolidated assessment of the payment service provider's ML/TF risks that exist across all its business units, product lines and delivery channels. The enterprise-wide ML/TF risk assessment relates to a payment service provider in the following ways:

(a) A payment service provider shall take into account the ML/TF risks of its branches and subsidiaries, including those outside Singapore, as part of its consolidated assessment of its enterprise-wide ML/TF risks.

(b) A payment service provider which is the Singapore branch of an entity incorporated outside Singapore may refer to an enterprise-wide ML/TF risk assessment performed by the head office, group or regional AML/CFT function, provided that the assessment adequately reflects the ML/TF risks faced in the context of its operations in Singapore.

4-4 The enterprise-wide ML/TF risk assessment is intended to enable the payment service provider to better understand its overall vulnerability to ML/TF risks and forms the basis for the payment service provider's overall risk-based approach.

4-5 A payment service provider's senior management shall approve its enterprise-wide ML/TF risk assessment and all employees and officers should give their full support and active co-operation to the enterprise-wide ML/TF risk assessment.

4-6 In conducting an enterprise-wide risk assessment, the broad ML/TF risk factors that the payment service provider should consider include —

(a) in relation to its customers —

(i) target customer markets and segments;

(ii) profile and number of customers identified as higher risk;

(iii) volumes and sizes of its customers' transactions and funds or value transfers, considering the usual activities and the risk profiles of its customers;

(iv) volumes and sizes of customers' transactions in DPT products that pose higher ML/TF risk (please refer to paragraph 5-3 for a list of factors that may be considered in assessing products' ML/TF risk);

(v) use of Internet Protocol anonymizers, or any other technological tool that obfuscates one's physical location, by customers;

(vi) use of mixers and tumblers, or any anonymity-enhancing technologies that obfuscate the identities of customers and/or their counterparties.

(b) in relation to the countries or jurisdictions its customers are from or in, or where the payment service provider has operations in —

(i) countries or jurisdictions the payment service provider is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its customers (including financial institutions ("FI"), with whom the payment service provider provides services to or engages to facilitate the provision of services), especially countries or jurisdictions with relatively higher levels of corruption, organised crime or inadequate AML/CFT measures, as identified by the Financial Action Task Force ("FATF");

(ii) when assessing ML/TF risks of countries and jurisdictions, the following criteria may be considered:

- reliable evidence of adverse news or relevant public criticism of a country or jurisdiction, including FATF public documents on High Risk and Other Monitored jurisdictions;

- independent and public assessment of the country's or jurisdiction's overall AML/CFT regime such as FATF or FATF-Styled Regional Bodies' ("FSRBs") Mutual Evaluation reports and the International Monetary Fund ("IMF")/World Bank Financial Sector Assessment Programme Reports or Reports on the Observance of Standards and Codes for guidance on the country's or jurisdiction's AML/CFT measures;

- the AML/CFT laws, regulations and standards of the country or jurisdiction, including those in relation to payment service providers (or virtual assets service providers[1] ("VASPs"));

- implementation standards (including quality and effectiveness of supervision) of the AML/CFT regime;

- whether the country or jurisdiction is a member of international groups that only admit countries or jurisdictions which meet certain AML/CFT benchmarks;

- contextual factors, such as political stability, maturity and sophistication of the regulatory and supervisory regime, level of corruption, financial inclusion, etc;

(c) in relation to the products, services, transactions and delivery channels of the payment service provider —

(i) the nature, scale, diversity and complexity of the payment service provider's business activities and whether any of these factors introduces additional risks or exacerbates specific risks;

(ii) the nature of products and services offered by the payment service provider, especially products and services that may present higher ML/TF risks. In this regard, the payment service provider should, at minimum, consider the product ML/TF risk indicators set out in paragraph 5-3; and

(iii) the delivery channels, including whether the payment service provider operates an open or closed-loop system, and the extent to which the payment service provider deals directly with the customer, relies on third parties to perform CDD measures or uses technology (e.g. an online exchange platform that establishes business relations through non-face-to-face measures).

4-7 The scale and scope of the enterprise-wide ML/TF risk assessment should be commensurate with the nature and complexity of the payment service provider's business.

4-8 As far as possible, a payment service provider's enterprise-wide ML/TF risk assessment should entail both qualitative and quantitative analyses to ensure that the payment service provider accurately understands its exposure to ML/TF risks. A quantitative analysis of the payment service provider's exposure to ML/TF risks

[1] Defined in this document to be entities that perform the 5 activities identified to pose ML/TF risks, both internationally and in Singapore's context. They are:

i. exchange between VA and fiat currencies;
ii. exchange between one or more forms of VAs;
iii. transfer of VAs;
iv. safekeeping of VAs; and
v. provision of financial services related to an issuer's offer.

should involve evaluating data on the payment service provider's activities using the applicable broad risk factors set out in paragraph 5-3.

4-9 As required by paragraph 4.1(d) of the Notice, a payment service provider shall take into account all its existing products, services, transactions and delivery channels offered as part of its enterprise-wide ML/TF risk assessment.

4-10 In assessing its overall ML/TF risks, a payment service provider should make its own determination as to the risk weights to be given to the individual factor or combination of factors.

Singapore's National ML/TF Risk Assessment ("NRA") Report

4-11 A payment service provider should incorporate the results of Singapore's NRA Report and relevant updates from the authorities into its enterprise-wide ML/TF risk assessment process. This includes the report on the ML/TF risks arising from the use of virtual assets in Singapore, in section II of these Guidelines. When performing the enterprise-wide risk assessment, a payment service provider should take into account any financial or non-financial sector that has been identified as presenting higher ML/TF risks. A payment service provider should consider the NRA and its enterprise-wide ML/TF risk assessment results when assessing the ML/TF risks presented by customers from specific sectors.

4-12 A payment service provider should consider the prevailing crime types that may impact them when assessing its enterprise-wide ML/TF risks of products, services, transactions and delivery channels and whether it is more susceptible to the higher risk prevailing crime types. Where appropriate, a payment service provider should also take these results into account as part of the payment service provider's ongoing monitoring of the conduct of customers' accounts, and the payment service provider's scrutiny of customers' transactions undertaken in the course of a business relation or transactions undertaken without an account being opened.

Risk Mitigation

4-13 The nature and extent of AML/CFT risk management systems and controls implemented should be commensurate with the ML/TF risks identified via the enterprise-wide ML/TF risk assessment. A payment service provider shall put in place adequate policies, procedures and controls to mitigate the ML/TF risks.

4-14 A payment service provider's enterprise-wide ML/TF risk assessment serves to guide the allocation of AML/CFT resources by the payment service provider.

4-15 A payment service provider should assess the effectiveness of its risk mitigation procedures and controls by monitoring the following:

(a) the ability to identify changes in a customer profile (e.g. Politically Exposed Persons status) and transactional behaviour observed in the course of its business;

(b) the potential for abuse of new business initiatives, products, practices and services for ML/TF purposes;

(c) the compliance arrangements (through its internal audit or quality assurance processes or external review);

(d) the balance between the use of technology-based or automated solutions with that of manual or people-based processes, for AML/CFT risk management purposes;

(e) the coordination between AML/CFT compliance and other functions (e.g. anti-fraud, general compliance etc.) of the payment service provider;

(f) the adequacy of training provided to employees and officers and awareness of the employees and officers on AML/CFT matters;

(g) the process of management reporting and escalation of pertinent AML/CFT issues to the payment service provider's board of directors and senior management;

(h) the cooperation and coordination between the payment service provider and regulatory or law enforcement agencies; and

(i) the performance of third parties relied upon by the payment service provider to carry out CDD measures.

Documentation

4-16 The documentation should include —

(a) the enterprise-wide ML/TF risk assessment by the payment service provider;

(b) details of the implementation of the AML/CFT risk management systems and controls as guided by the enterprise-wide ML/TF risk assessment;

(c) the reports to senior management on the results of the enterprise-wide ML/TF risk assessment and the implementation of the AML/CFT risk management systems and controls; and

(d) details of the frequency of review of the enterprise-wide ML/TF risk assessment.

4-17 A payment service provider should ensure that the enterprise-wide ML/TF risk assessment and the risk assessment information are made available to the Authority upon request.

Frequency of Review

4-18 To keep its enterprise-wide risk assessments up-to-date, a payment service provider should review its risk assessment at least once every two years or when material trigger events occur, whichever is earlier. Such material trigger events include, but are not limited to, the acquisition of new customer segments or delivery channels, or the launch of new products and services by the payment service provider. The results of these reviews should be documented and approved by senior management even if there are no significant changes to the payment service provider's enterprise-wide risk assessment.

5 Notice Paragraph 5 – New Products, Practices and Technologies

5-1 International developments of new technologies to provide financial services are fast-changing and growing at an accelerated pace. A payment service provider shall keep abreast of such new developments and the ML/TF risks associated with them.

5-2 A payment service provider's assessment of ML/TF risks in relation to new products, practices and technologies is separate from, and in addition to, the payment service provider's assessment of other risks such as credit risks, operational risks or market risks. For example, in the assessment of ML/TF risks, a payment service provider should pay attention to new products, practices and technologies that deal with customer funds, including those involving the use of digital payment tokens, or the movement of such funds. These assessments should be approved by senior management.

5-3 A payment service provider's ML/TF risk assessment for new products should consider the following indicators (which are non-exhaustive):

(a) whether the product has characteristics that promote anonymity, obfuscate transactions or undermine the payment service provider's ability to identify its customers and/or their counterparties, or implement effective CDD and other AML/CFT measures;

(b) whether the product is known to be used by criminals for illicit purposes;

(c) whether the volatility and liquidity of the product render it susceptible to market manipulation and fraud; and

(d) whether the product has been developed and/or issued by reputable entities for lawful and legitimate purposes.

6 Notice Paragraph 6 – Customer Due Diligence

Notice Paragraph 6.2

6-1 Where There are Reasonable Grounds for Suspicion prior to the Establishment of Business Relations or Undertaking any Transaction without Opening an Account

6-1-1 In arriving at its decision for each case, a payment service provider should take into account the relevant facts, including information that may be made available by the authorities, and conduct a proper risk assessment.

Notice Paragraphs 6.3 to 6.4

6-2 When CDD is to be Performed and Linked Transactions

6-2-1 Two or more transactions may be related or linked if they involve the same sender or recipient. A payment service provider should be aware that transactions may be entered into consecutively, with the intention of circumventing applicable thresholds set out in the Notice.

Notice Paragraphs 6.5 to 6.18

6-3 CDD Measures under Paragraphs 6.5 to 6.18

6-3-1 When relying on documents, a payment service provider should be aware that the best documents to use to verify the identity of the customer are those most difficult to obtain illicitly, counterfeit or falsify digitally. These may include government-issued identity cards or passports, reports from independent company registries, published or audited annual reports and other reliable sources of information. The rigour of the verification process should be commensurate with the customer's risk profile.

6-3-2 A payment service provider should exercise greater caution when dealing with an unfamiliar or a new customer. Apart from obtaining the identification information required by paragraph 6.6 of the Notice, a payment service provider should (if not already obtained as part of its account opening process) also obtain additional information on the customer's background such as occupation, employer's name, nature of business, range of annual income, and whether the customer holds or has held a prominent public function. Such additional identification information enables a payment service provider to obtain better knowledge of its customer's risk profile, as well as the purpose and intended nature of the business relation or transaction.

Notice Paragraph 6.6

6-4 Identification of Customer

6-4-1 With respect to paragraph 6.6(c) of the Notice, a P.O. box address should only be used for jurisdictions where the residential address (e.g. street name or house number) is not applicable or available in the local context.

6-4-2 A payment service provider should obtain a customer's contact details such as personal, office or work telephone numbers.

Notice Paragraph 6.8

6-5 Identification of Customer that is a Legal Person or Legal Arrangement

6-5-1 Under paragraph 6 and paragraph 8 of the Notice, a payment service provider is required to identify and screen all the connected parties of a customer. However, a payment service provider may verify their identities using a risk-based approach[2]. A payment service provider is reminded of its obligations under the Notice to identify connected parties and remain apprised of any changes to connected parties.

6-5-2 Identification of connected parties may be done using publicly available sources or databases such as company registries, annual reports or based on substantiated information provided by the customers.

6-5-3 In relation to legal arrangements, a payment service provider shall perform CDD measures on the customer by identifying the settlors, trustees, the protector (if any), the beneficiaries (including every beneficiary that falls within a designated characteristics or class) and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership), as required by paragraph 6.14 of the Notice.

Notice Paragraph 6.9

6-6 Verification of Identity of Customer

6-6-1 Where the customer is a natural person, a payment service provider should obtain identification documents that contain a clear photograph of that customer.

6-6-2 In verifying the identity of a customer, a payment service provider may obtain the following documents:

(a) Natural Persons —

[2] For guidance on SCDD measures in relation to the identification and verification of the identities of connected parties of a customer, payment service providers are to refer to paragraph 7-3 of these Guidelines.

(i) name, unique identification number, date of birth and nationality based on a valid passport or a national identity card that bears a photograph of the customer; and

(ii) residential address based on national identity card, recent utility or phone bill, bank statement or correspondence from a government agency.

(b) Legal Persons or Legal Arrangements —

(i) name, legal form, proof of existence and constitution based on certificate of incorporation, certificate of good standing, partnership agreement, trust deed, constitutional document, certificate of registration or any other documentation from a reliable independent source; and

(ii) powers that regulate and bind the legal person or arrangement based on memorandum and articles of association, and board resolution authorising the opening of an account and appointment of authorised signatories.

6-6-3 Further guidance on verification of different types of customers (including legal persons or legal arrangements) is set out in Appendix A.

6-6-4 In exceptional circumstances where the payment service provider is unable to retain a copy of documentation used to verify the customer's identity, the payment service provider should record the following:

(a) information that the original documentation had served to verify;

(b) title and description of the original documentation produced to the payment service provider's employee or officer for verification, including any particular or unique features or condition of that documentation (e.g. whether it is worn out or damaged);

(c) reasons why a copy of that documentation could not be made; and

(d) name of the payment service provider's employee or officer who carried out the verification, a statement by that employee or officer certifying verification of the information against the documentation and the date of the verification.

Reliability of Information and Documentation

6-6-5 Where a payment service provider obtains data, documents or information from the customer or a third party, it should ensure that such data, documents or information are current at the time they are provided to the payment service provider.

6-6-6 Where the customer is unable to produce an original document, a payment service provider may consider accepting a copy of the document —

(a) that is certified to be a true copy by a suitably qualified person (e.g. a notary public, a lawyer or certified public or professional accountant); or

(b) if a payment service provider's employee or officer independent of the payment service provider's dealing with the customer has confirmed that he has sighted the original document.

6-6-7 Where a document is in a foreign language, appropriate steps should be taken by a payment service provider to be reasonably satisfied that the document does in fact provide evidence of the customer's identity. The payment service provider should ensure that any document that is critical for performance of any measures required under the Notice is translated into English by a suitably qualified translator. Alternatively, the payment service provider may rely on a translation of such document by a payment service provider's employee or officer, independent of the payment service provider's dealing with the customer, who is conversant in that foreign language. This is to allow all employees and officers of the payment service provider involved in the performance of any measures required under the Notice to understand the contents of the documents, for effective determination and evaluation of ML/TF risks associated with the customer.

6-6-8 The payment service provider should ensure that documents obtained for performing any measures required under the Notice are clear and legible. This is important for the establishment of a customer's identity.

Notice Paragraphs 6.10 to 6.12

6-7 Identification and Verification of Identity of Natural Person Appointed to Act on a Customer's Behalf

6-7-1 Appropriate documentary evidence of a customer's appointment of a natural person to act on its behalf includes a board resolution or similar authorisation documents.

6-7-2 Where there is a long list of natural persons appointed to act on behalf of the customer (e.g. a list comprising more than 10 authorised signatories), the payment service provider should verify at a minimum those natural persons who deal directly with the payment service provider.

Notice Paragraphs 6.13 to 6.17

6-8 Identification and Verification of Identity of Beneficial Owner

6-8-1 A payment service provider should note that measures listed under paragraph 6.14(a)(i), (ii) and (iii) as well as paragraph 6.14(b)(i) and (ii) of the Notice are not alternative measures but are cascading measures with each to be used where the immediately preceding measure has been applied but has not resulted in the identification of a beneficial owner.

6-8-2 In relation to paragraph 6.14(a)(i) and (b)(i) of the Notice, when identifying the natural person who ultimately owns the legal person or legal arrangement, the shareholdings within the ownership structure of the legal person or legal arrangement should be considered. It may be based on a threshold (e.g. any person owning more than 25% of the legal person or legal arrangement, taking into account any aggregated ownership for companies with cross-shareholdings).

6-8-3 A natural person who does not meet the shareholding threshold referred to in paragraph 6-8-2 above but who controls the customer (e.g. through exercising significant influence), is a beneficial owner under the Notice.

6-8-4 A payment service provider may also consider obtaining an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner. Notwithstanding the obtaining of such an undertaking or declaration, the payment service provider remains responsible for complying with its obligations under the Notice to take reasonable measures to verify the identity of the beneficial owner by, for example, researching publicly available information on the beneficial owner or arranging a face-to-face meeting with the beneficial owner, to corroborate the undertaking or declaration provided by the customer.

6-8-5 Where the customer is not a natural person and has a complex ownership or control structure, a payment service provider should obtain enough information to sufficiently understand if there are legitimate reasons for such ownership or control structure.

6-8-6 A payment service provider should take particular care when dealing with companies with bearer shares, since beneficial ownership is difficult to establish. For such companies, a payment service provider should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the payment service provider is notified whenever there is a change of beneficial owner of such shares. At a minimum, these procedures should require the payment service provider to obtain an undertaking in writing from the beneficial owner of such bearer shares stating that the payment service provider shall be immediately notified if the shares are transferred to another natural person, legal person or legal arrangement. Depending on its risk assessment of the customer, the payment service provider may require that the bearer shares be held by a named custodian, with an undertaking from the custodian that the payment service provider will be notified of any changes to ownership of these shares or the named custodian.

6-8-7 For the purposes of paragraph 6.16 of the Notice, where the customer is a legal person publicly listed on a stock exchange and subject to regulatory disclosure requirements relating to adequate transparency in respect of its beneficial owners (imposed through stock exchange rules, law or other enforceable means), it is not necessary to identify and verify the identities of the beneficial owners of the customer.

6-8-8 In determining if the foreign stock exchange imposes regulatory disclosure and adequate transparency requirements, the payment service provider should put in place an internal assessment process with clear criteria, taking into account,

amongst others, the country risk and the level of the country's compliance with the FATF standards.

6-8-9 Where the customer is a majority-owned subsidiary of a publicly listed legal person, it is not necessary to identify and verify the identities of beneficial owners of the customer. However, for such a customer, if there are other non-publicly listed legal persons who own more than 25% of the customer or who otherwise control the customer, the beneficial owners of such non-publicly listed legal persons should be identified and verified.

6-8-10 Where a customer is one which falls within paragraph 6.16 of the Notice, this does not in itself constitute an adequate analysis of low ML/TF risks for the purpose of performing SCDD measures under paragraph 7 of the Notice.

Notice Paragraph 6.18

6-9 Information on the Purpose and Intended Nature of Business Relations and Transaction Undertaken without an Account Being Opened

6-9-1 The measures taken by a payment service provider to understand the purpose and intended nature of business relations and transactions undertaken without an account being opened should be commensurate with the complexity of the customer's business and risk profile. For higher risk customers, a payment service provider should seek to understand upfront the expected account activity (e.g. frequency of transactions likely to pass through, expected amount for each transaction, names of persons to whom moneys are to be transferred) and consider, as part of ongoing monitoring, whether the activity corresponds with the stated purpose. This will enable a more effective ongoing monitoring of the customer's business relations, and transactions without an account being opened.

Notice Paragraphs 6.19 to 6.24

6-10 Review of Transactions Undertaken without an Account Being Opened

6-10-1 The payment service provider should make further enquiries when customers perform frequent and cumulatively large transactions without an account being opened, without any apparent or visible economic or lawful purpose. For example, any such transactions that are not consistent with the payment service provider's knowledge of the customer, including frequent transfers of funds or DPT to the same recipient, frequent transactions to buy or sell DPT over a short period of time, or multiple transfers of funds or DPT such that the amount of each fund or value transfer is not substantial, but the total of which is substantial.

6-10-2 Where there are indications that the risks may have increased over time, the payment service provider should request additional information and conduct a review of the customer's risk profile in order to determine if additional measures are necessary.

6-10-3 In determining what would constitute suspicious, complex, unusually large or unusual pattern of transactions undertaken without an account being opened, a payment service provider should consider, amongst others, international typologies and information obtained from law enforcement and other authorities that may point to jurisdiction-specific considerations. As part of the review of such transactions, a payment service provider should pay attention to transaction characteristics, such as —

(a) the nature of a transaction (e.g. abnormal size or frequency for that customer or peer group);

(b) whether a series of transactions is conducted with the intent to avoid reporting thresholds (e.g. by structuring an otherwise single transaction into a number of transactions);

(c) the geographic destination or origin of a payment (e.g. to or from an individual originating from or located in a higher risk country); and

(d) the parties concerned (e.g. a request to make a payment to or from a person on a sanctions list).

6-10-4 A payment service provider's transaction monitoring processes or systems for review of transactions undertaken without an account being opened may vary in scope or sophistication (e.g. using manual spreadsheets to automated and complex systems). The degree of automation or sophistication of processes and systems depends on the size and complexity of the payment service provider's operations. The payment service provider may adjust the extent and depth of monitoring of a customer according to the customer's ML/TF risk profile. The adequacy of monitoring and the factors leading the payment service provider to adjust the level of monitoring should be reviewed regularly for effectiveness in mitigating the payment service provider's ML/TF risks.

6-10-5 The transaction monitoring processes and systems used by the payment service provider should provide its business units and compliance officers (including employees and officers who are tasked with conducting investigations) with timely information needed to identify, analyse and effectively monitor customers for ML/TF.

6-10-6 The parameters and thresholds used by a payment service provider to identify suspicious transactions undertaken without an account being opened should be properly documented and independently validated to ensure that they are appropriate to its operations and context. A payment service provider should periodically review the appropriateness of the parameters and thresholds used in the review process.

Notice Paragraphs 6.25 to 6.33

6-11 Ongoing Monitoring

6-11-1 Ongoing monitoring of business relations is a fundamental feature of an effective AML/CFT risk management system. Ongoing monitoring should be conducted in relation to all business relations, but the payment service provider may adjust the extent and depth of monitoring of a customer according to the customer's ML/TF risk profile. Enhanced monitoring should be conducted for higher risk situations and extend beyond the immediate transaction between the payment service provider or its customer or counterparty. For example, the payment service provider may need to trace previous transactions of the digital payment token as far back as necessary to reasonably assess whether the circumstances are unusual or suspicious. The adequacy of monitoring systems and factors leading the payment service provider to adjust the level of monitoring should be reviewed regularly for effectiveness in mitigating the payment service provider's ML/TF risks.

6-11-2 A payment service provider should make further enquiries when a customer performs frequent and cumulatively large transactions in the course of business relations without any apparent or visible economic or lawful purpose. For example, transactions in the course of business relations that are not consistent with the payment service provider's knowledge of the customer, including frequent transfers of funds or DPT to the same recipient, frequent transactions to buy or sell DPT over a short period of time or multiple transfers of funds or DPT such that the amount of each fund or value transfer is not substantial, but the total of which is substantial.

6-11-3 Where there are indications that the risks associated with an existing business relationship may have increased, the payment service provider should request additional information and conduct a review of the customer's risk profile in order to determine if additional measures are necessary.

6-11-4 A key part of ongoing monitoring includes maintaining relevant and up-to-date CDD data, documents and information so that the payment service provider can identify changes to the customer's risk profile —

(a) for higher risk categories of customers, a payment service provider should obtain updated CDD information (including updated copies of the customer's passport or identity documents if these have expired), as part of its periodic CDD review, or upon the occurrence of a trigger event, whichever is earlier; and

(b) for all other risk categories of customers, a payment service provider should obtain updated CDD information upon the occurrence of a trigger event.

6-11-5 Examples of trigger events are when (i) a significant transaction takes place, (ii) a material change occurs in the way the customer's account is operated, (iii) the payment service provider's policies, procedures or standards relating to the documentation of CDD information change substantially, and (iv) the payment

service provider becomes aware that it lacks sufficient information about the customer concerned.

6-11-6 The frequency of CDD review may vary depending on each customer's risk profile. Higher risk customers should be subject to more frequent periodic review (e.g. on an annual basis) to ensure that CDD information such as nationality, passport details, certificate of incumbency, ownership and control information that the payment service provider has previously obtained remain relevant and up-to-date.

6-11-7 In determining what would constitute suspicious, complex, unusually large or unusual pattern of transactions, a payment service provider should consider, amongst others, international typologies and information obtained from law enforcement and other authorities that may point to jurisdiction-specific considerations. As part of ongoing monitoring, a payment service provider should pay attention to transaction characteristics, such as —

(a) the nature of a transaction (e.g. abnormal size or frequency for that customer or peer group);

(b) whether a series of transactions is conducted with the intent to avoid reporting thresholds (e.g. by structuring an otherwise single transaction into a number of transactions);

(c) the geographic destination or origin of a payment (e.g. to or from a higher risk country); and

(d) the parties concerned (e.g. a request to make a payment to or from a person on a sanctions list).

6-11-8 A payment service provider's transaction monitoring processes or systems may vary in scope or sophistication (e.g. using manual spreadsheets to automated and complex systems). The degree of automation or sophistication of processes and systems depends on the size and complexity of the payment service provider's operations.

6-11-9 Nevertheless, the processes and systems used by the payment service provider should provide its business units and compliance officers (including employees and officers who are tasked with conducting investigations) with timely information needed to identify, analyse and effectively monitor customer accounts for ML/TF.

6-11-10 The transaction monitoring processes and systems should enable the payment service provider to monitor the accounts of a customer holistically across business units to identify any suspicious transactions. In the event that a business unit discovers suspicious trends or transactions in a customer's account, such information should be shared across other business units to facilitate a holistic assessment of the ML/TF risks presented by the customer. Therefore, payment service providers should have processes in place to share such information across business units. In addition, payment service providers should perform trend analyses of transactions to identify unusual or suspicious transactions. Payment

service providers should also monitor transactions with parties in high risk countries or jurisdictions.

6-11-11 In addition, payment service providers should have processes in place to monitor related customer accounts holistically within and across business units, so as to better understand the risks associated with such customer groups, identify potential ML/TF risks and report suspicious transactions.

6-11-12 In the conduct of monitoring, a payment service provider could establish parameters, thresholds or specific scenarios that would enable them to better determine the activities that will be reviewed. The parameters, thresholds and scenarios used by a payment service provider to identify suspicious transactions should be properly documented and independently validated to ensure that they are appropriate to its operations and context. Payment service providers should utilise data and distributed ledger analytics tools that are commensurate with their risks, as well as size and sophistication of their business, to enhance the detection of suspicious transactions. A payment service provider should also periodically review the appropriateness of the parameters, thresholds and scenarios used in the monitoring process.

6-11-13 A payment service provider should clearly document the criteria applied to decide the frequency and intensity of the monitoring of different customer segments. A payment service provider should also properly document and retain the results of their monitoring, as well as any assessment performed.

Notice Paragraphs 6.34 to 6.39

6-12 CDD Measures for Non-Face-to-Face Business Relations or Non-Face-to-Face Transactions Undertaken without an Account Being Opened

6-12-1 A reference to “specific risks” in paragraph 6.34 of the Notice includes risks arising from establishing business relations, undertaking transactions in the course of a business relations or undertaking transactions without an account being opened, according to instructions conveyed by customers over the internet, post, fax or phone. A payment service provider should note that applications and transactions undertaken across the internet or phone may pose greater risks than other non-face-to-face business due to the following factors:

(a) the ease of unauthorised access to the facility, across time zones and location;

(b) the ease of making multiple fictitious applications without incurring extra cost or the risk of detection;

(c) the absence of physical documents; and

(d) the speed of electronic transactions,

that may, taken together, aggravate the ML/TF risks.

6-12-2 The measures taken by a payment service provider for verification of an identity in respect of non-face-to-face business relations with or transactions undertaken for the customer will depend on the nature and characteristics of the product or service provided and the customer's risk profile.

6-12-3 Where verification of identity is performed without face-to-face contact (e.g. electronically), a payment service provider should apply additional checks to manage the risk of impersonation. The additional checks may consist of robust anti-fraud checks that the payment service provider routinely undertakes as part of its existing procedures, which may include some or all of the following —

(a) phone contact with the customer at a personal, residential or business number that can be verified independently;

(b) confirmation of the customer's address through an exchange of correspondence or other appropriate method;

(c) subject to the customer's consent, phone confirmation of the customer's employment status with his employer's human resource department at a listed business number of the employer;

(d) confirmation of the customer's salary details by requiring the presentation of recent bank statements, where applicable;

(e) provision of certified identification documents by lawyers or notaries public;

(f) requirement for customer to make an initial deposit into the account with the payment service provider from funds held by the customer in an account with a bank in Singapore;

(g) measures for customer to demonstrate control over the DPT wallet address making the initial deposit of DPT into the customer's account with the payment service provider (e.g. by effecting a transfer of an amount specified by the payment service provider);

(h) collection of customer device identifiers, IP addresses with associated time stamps, geo-location data;

(i) real-time video conferencing that is comparable to face-to-face communication;

(j) verification of a customer's identity through a document that customer has signed with a secure digital signature using a set of PKI based credentials issued by a certified Certificate Authority under the Electronic Transaction Act; or

(k) use of technology solutions to manage the impersonation risks including, but not limited to, the use of biometric technologies (e.g. fingerprint or iris scans, facial recognition etc.) which should be linked incontrovertibly to the customer.

6-12-4 A payment service provider should regularly review the effectiveness of its checks to manage the risk of impersonation following the conduct of its non-face-to-face business contact.

6-12-5 A payment service provider may wish to conduct the independent assessment in paragraph 6.37 of the Notice as part of its annual audit. In appointing the external auditor or independent consultant for the independent assessment, the payment service provider should consider the competency of the external auditor or independent consultant, including their track record, and knowledge of technology solutions and regulatory requirements.

6-12-6 In considering whether there has been a substantial change in the policies and procedures in paragraph 6.39 of the Notice, a payment service provider should take into account the likely impact of the new policy or procedure on the specific risks associated with non-face-to-face business relations with a new customer or non-face-to-face transactions undertaken without an account being opened for a customer, for example, the adoption of a technology solution different from that used in the existing policies and procedures.

Notice Paragraph 6.40

6-13 Reliance by Acquiring Payment Service Provider on Measures Already Performed

6-13-1 When a payment service provider acquires the business of another FI, either in whole or in part, it is not necessary for the identity of all existing customers to be verified again, provided that the requirements of paragraph 6.40 of the Notice are met. A payment service provider shall maintain proper records of its due diligence review performed on the acquired business.

6-13-2 Notwithstanding the reliance on identification and verification that has already been performed, an acquiring payment service provider is responsible for its obligations under the Notice.

6-13-3 When a payment service provider acquires the business of another FI, either in whole or in part, the payment service provider is reminded that in addition to complying with paragraph 6.40 of the Notice, it is also required to comply with the requirements set out in paragraphs 6.19 to 6.33 of the Notice.

Notice Paragraphs 6.42 to 6.44

6-14 Timing for Verification

6-14-1 With reference to paragraph 6.43 of the Notice, an example of when the deferral of completion of the verification is essential in order not to interrupt the normal conduct of business operations is securities trades, where timely execution of trades is critical given changing market conditions. One way a payment service

provider could effectively manage the ML/TF risks arising from the deferral of completion of verification is to put in place appropriate limits on the financial services available to the customer (e.g. limits on the number, type and value of transactions that can be effected) and institute closer monitoring procedures, until the verification has been completed.

6-14-2 With reference to paragraph 6.44 of the Notice —

(a) the completion of verification should not exceed 30 business days after the establishment of business relations;

(b) the payment service provider should suspend business relations with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if such verification remains uncompleted 30 business days after the establishment of business relations;

(c) the payment service provider should terminate business relations with the customer if such verification remains uncompleted 120 business days after the establishment of business relations; and

(d) the payment service provider should factor these time limitations in its policies, procedures and controls.

6-14-3 For avoidance of doubt, delayed verification should not be applied for transactions undertaken without an account being opened[3].

Notice Paragraphs 6.49 to 6.52

6-15 Screening

6-15-1 Screening is intended to be a preventive measure. A payment service provider is reminded that all parties identified pursuant to the Notice are required to be screened, irrespective of the risk profile of the customer.

6-15-2 Where screening results in a positive hit against sanctions lists, a payment service provider is reminded of its obligations to freeze without delay and without prior notice, the funds or other assets of designated persons and entities that it has control over, so as to comply with applicable laws and regulations in Singapore, including the TSOFA and MAS Regulations issued under section 27A of the Monetary Authority of Singapore Act (Cap. 186) ("MAS Act") relating to sanctions and freezing of assets of persons. Any such assets should be reported promptly to the relevant authorities and a Suspicious Transaction Report ("STR") should be filed.

[3] As required by paragraphs 6.3(a), (b) and (c) of the Notice, a payment service provider shall perform the requisite CDD measures on every customer, regardless of whether an account has been opened for that customer.

6-15-3 A payment service provider should put in place policies, procedures and controls that clearly set out —

(a) the ML/TF information sources used by the payment service provider for screening (including commercial databases used to identify adverse information on individuals and entities, individuals and entities covered under MAS Regulations issued pursuant to section 27A of the MAS Act, individuals and entities identified by other sources such as the payment service provider's head office or parent supervisory authority, lists and information provided by the Authority and relevant authorities in Singapore);

(b) the roles and responsibilities of the payment service provider's employees and officers involved in the screening, reviewing and dismissing of alerts, maintaining and updating of the various screening databases and escalating hits;

(c) the frequency of review of such policies, procedures and controls;

(d) the frequency of periodic screening;

(e) how apparent matches from screening are to be resolved by the payment service provider's employees and officers, including the process for determining that an apparent match is a positive hit and for dismissing an apparent match as a false hit; and

(f) the steps to be taken by the payment service provider's employees and officers for reporting positive hits to the payment service provider's senior management and to the relevant authorities.

6-15-4 The level of automation used in the screening process should take into account the nature, size and risk profile of a payment service provider's business. A payment service provider should be aware of any shortcomings in its automated screening systems. In particular, it is important to consider "fuzzy matching" to identify non-exact matches. The payment service provider should ensure that the fuzzy matching process is calibrated to the risk profile of its business. As application of the fuzzy matching process is likely to result in the generation of an increased number of apparent matches which have to be checked, the payment service provider's employees and officers will need to have access to CDD information to enable them to exercise their judgment in identifying true hits.

6-15-5 A payment service provider should be aware that performing screening after business relations have been established or transactions without an account being opened have been undertaken could lead to a breach of relevant laws and regulations in Singapore relating to sanctioned parties. When the payment service provider becomes aware of such breaches, it should immediately take the necessary actions and inform the relevant authorities.

6-15-6 In screening periodically as required by paragraph 6.50(d) of the Notice, a payment service provider should pay particular attention to changes in customer status (e.g.

whether the customer has over time become subject to prohibitions and sanctions) or customer risks (e.g. a connected party of a customer, a beneficial owner of the customer or a natural person appointed to act on behalf of the customer subsequently becomes a Politically Exposed Person or presents higher ML/TF risks, or a customer subsequently becomes a Politically Exposed Person or presents higher ML/TF risks) and assess whether to subject the customer to the appropriate ML/TF risk mitigation measures (e.g. enhanced CDD measures).

6-15-7 A payment service provider should ensure that the identification information of a customer, a connected party of the customer, a natural person appointed to act on behalf of the customer and a beneficial owner of the customer is entered into the payment service provider's customer database for periodic name screening purposes. This will help the payment service provider to promptly identify any existing customers who have subsequently become higher risk parties.

6-15-8 In determining the frequency of periodic name screening, a payment service provider should consider its customer's risk profile.

6-15-9 The payment service provider should ensure that it has adequate arrangements to perform screening of the payment service provider's customer database when there are changes to the lists of sanctioned individuals and entities, covered by the TSOFA and MAS Regulations issued under section 27A of the MAS Act[4]. The payment service provider should implement "four-eye checks" on alerts from sanctions review before closing an alert, or conduct quality assurance checks on closure of such alerts on a sample basis.

6-15-10 With reference to paragraph 6.51 of the Notice, transaction screening should take place on a real-time basis (i.e. the screening or filtering of relevant payment instructions or value transfer requests should be carried out before the transaction is executed).

[4] Please refer to the following link for the relevant MAS ML/TF Regulations - https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions

7 Notice Paragraph 7 – Simplified Customer Due Diligence

7-1 Paragraph 7.1 of the Notice permits a payment service provider to adopt a risk-based approach in assessing the necessary measures to be performed, and to perform appropriate SCDD measures, in cases where the payment service provider is satisfied, upon analysis, that the ML/TF risks are low.

7-2 Where a payment service provider applies SCDD measures, it is still required to perform ongoing monitoring of business relations and reviews of transactions undertaken without an account being opened, under the Notice. In addition, to ensure compliance with applicable laws and regulations in Singapore, including the MAS Regulations issued under section 27A of the Monetary Authority of Singapore Act (Cap. 186) ("MAS Act) relating to sanctioned parties, a payment service provider is reminded that where it applies SCDD measures, it is still required to screen all parties under the Notice.

7-3 Under SCDD, a payment service provider may adopt a risk-based approach in assessing whether any measures should be performed for connected parties of the customers.

7-4 Subject to paragraph 7.4 of the Notice, where a payment service provider is satisfied that the risks of money laundering and terrorism financing are low, a payment service provider may perform SCDD measures,. Examples of possible SCDD measures include —

(a) reducing the frequency of updates of customer identification information;

(b) reducing the degree of ongoing monitoring and scrutiny of transactions, based on a reasonable monetary threshold; or

(c) choosing another method to understand the purpose and intended nature of business relations or a transaction undertaken without an account being opened by inferring this from the type of transactions, instead of collecting information as to the purpose and intended nature of such business relations or transaction.

7-5 Subject to the requirement that a payment service provider's assessment of low ML/TF risks is supported by an adequate analysis of risks, examples of potentially lower ML/TF risk situations include —

(a) Customer risk

(i) a Singapore Government entity;

(ii) entities listed on a stock exchange and subject to regulatory disclosure requirements relating to adequate transparency in respect of beneficial owners (imposed through stock exchange rules, law or other enforceable means); and

(iii) an FI incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

(b) Product, service, transaction or delivery channel risk

(i) financial products or services that provide appropriately defined and limited services to certain types of customers (e.g. to increase customer access for financial inclusion purposes); and

(ii) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.

8 Notice Paragraph 8 – Enhanced Customer Due Diligence

8-1 Where the ML/TF risks are identified to be higher, a payment service provider shall take enhanced CDD ("ECDD") measures to mitigate and manage those risks.

8-2 Examples of potentially higher risk categories under paragraph 8.7 of the Notice include —

(a) Customer risk

(i) customers from higher risk businesses/ activities/ sectors identified in Singapore's NRA, guidance from the Authority, as well as other higher risk businesses/ activities/ sectors identified by the payment service provider;

(ii) the ownership structure of the legal person or arrangement appears unusual or excessively complex given the nature of the legal person's or legal arrangement's business;

(iii) legal persons or legal arrangements that are personal asset holding vehicles;

(iv) the business relations with a customer or transactions undertaken without an account being opened that are conducted under unusual circumstances (e.g. significant unexplained geographic distance between the licensee and the customer);

(v) companies that have nominee shareholders or shares in bearer form; and

(vi) cash-intensive businesses.

(b) Country or geographic risk

(i) countries or jurisdictions the payment service provider is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its customers (including payment service provider's network of correspondent account relationships) which have relatively higher levels of corruption, organised crime or inadequate AML/CFT measures, as identified by the FATF; and

(ii) countries identified by credible bodies (e.g. reputable international bodies such as Transparency International) as having significant levels of corruption, terrorism financing or other criminal activity.

(c) Product, service, transaction or delivery channel risk

(i) anonymous transactions (which may involve cash); and

(ii) frequent payments received from unknown or unassociated third parties.

8-3 When considering the ML/TF risks presented by a country or jurisdiction, a payment service provider should take into account, where appropriate, variations in ML/TF risks across different regions or areas within a country.

Notice Paragraph 8.1

8-4 Politically Exposed Persons ("PEPs") Definitions

8-4-1 The definitions in paragraph 8.1 of the Notice are drawn from the FATF Recommendations. The definition of PEPs is not intended to cover middle-ranking or more junior individuals in the categories listed.

8-4-2 In the context of Singapore, domestic PEPs should include at least all Government Ministers, Members of Parliament, Nominated Members of Parliament and Non-Constituency Members of Parliament.

8-4-3 When determining whether a person is a "close associate" of a PEP, the payment service provider may consider factors such as the level of influence the PEP has on such a person or the extent of his exposure to the PEP. The payment service provider may rely on information available from public sources and information obtained through customer interaction.

8-4-4 With reference to paragraph 8.1 of the Notice, examples of an "international organisation" include the United Nations and affiliated agencies such as the International Maritime Organisation and the International Monetary Fund; regional international organisations such as the Asian Development Bank, Association of Southeast Asian Nations Secretariat, institutions of the European Union, the Organisation for Security and Cooperation in Europe; military international organisations such as the North Atlantic Treaty Organisation; and economic organisations such as the World Trade Organisation or the Asia-Pacific Economic Cooperation Secretariat.

8-4-5 Examples of persons who are or have been entrusted with prominent functions by an international organisation are members of senior management such as directors, deputy directors and members of the board or equivalent functions. Other than relying on information from a customer, the payment service provider may consider information from public sources in determining whether a person has been or is entrusted with prominent functions by an international organisation.

Notice Paragraphs 8.2 to 8.4

8-5 PEPs

8-5-1 If a payment service provider determines that any natural person appointed to act on behalf of a customer or any connected party of a customer is a PEP, the payment service provider should assess the ML/TF risks presented and consider factors such as the level of influence that the PEP has on the customer. Payment

service providers should consider factors such as whether the PEP is able to exercise substantial influence over the customer, to determine the overall ML/TF risks presented by the customer. Where the customer presents higher ML/TF risks, the payment service provider should apply ECDD measures on the customer accordingly.

8-5-2 It is generally acceptable for a payment service provider to refer to commercially available databases to identify PEPs. However, a payment service provider should also obtain from the customer details of his occupation and the name of his employer. In addition, a payment service provider should consider other non-public information that the payment service provider is aware of. A payment service provider shall exercise sound judgment in identifying any PEP, having regard to the risks and the circumstances.

8-5-3 In relation to paragraph 8.3(a) of the Notice, the approval shall be obtained from senior management. Inputs should also be obtained from the payment service provider's AML/CFT compliance function.

8-5-4 In relation to paragraph 8.3(b) of the Notice, a payment service provider may refer to information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. A payment service provider should note that not all declarations are publicly available. A payment service provider should also be aware that certain jurisdictions impose restrictions on their PEPs' ability to hold foreign bank accounts, to hold other office or paid employment.

8-5-5 Source of wealth generally refers to the origin of the customer's and beneficial owner's entire body of wealth (i.e. total assets). This relates to how the customer and beneficial owner have acquired the wealth which is distinct from identifying the assets that they own. Source of wealth information should give an indication about the size of wealth the customer and beneficial owner would be expected to have, and how the customer and beneficial owner acquired the wealth. Although the payment service provider may not have specific information about assets that are not processed by the payment service provider, it may be possible to obtain general information from the customer, commercial databases or other open sources. Examples of appropriate and reasonable means of establishing source of wealth are information and documents such as evidence of title, copies of trust deeds, audited accounts, salary details, tax returns and bank statements.

8-5-6 Source of funds refers to the origin of the particular funds or other assets which are the subject of the establishment of business relations with a customer or the undertaking of transactions without an account being opened (e.g. the amounts being deposited or transferred as part of the business relations or transaction). In order to ensure that the funds are not proceeds of crime, the payment service provider should not limit its source of funds inquiry to identifying the other FI from which the funds have been transferred, but more importantly, the activity that generated the funds. The information obtained should be substantive and facilitate the establishment of the provenance of the funds or reason for the funds having

been acquired. Examples of appropriate and reasonable means of establishing source of funds are information such as salary payments or sale proceeds. Where the incoming funds in question are DPTs, a payment service provider should consider if the use of insights from distributed ledger analytics and/or other surveillance tools is necessary to assess the legitimacy of these funds.

8-5-7 Based on its risk assessment of the PEP, a payment service provider should consider whether the information regarding source of wealth and source of funds should be corroborated. In relation to paragraph 8.3(b) of the Notice, examples of "appropriate and reasonable means" for establishing source of wealth or source of funds are financial statements of the legal person or legal arrangement owned or controlled by the PEP, site visits, a copy of the will (in cases where the source of wealth or funds is an inheritance), and conveyancing documents (in cases where the source of wealth or funds is a sale of property).

8-5-8 In relation to paragraph 8.3 of the Notice, other ECDD measures that may be performed include —

(a) requiring the first payment to be carried out through an account in the customer's name with another FI subject to similar or equivalent CDD standards;

(b) using public sources of information (e.g. websites) to gain a better understanding of the reputation of the customer or any beneficial owner of a customer. Where the payment service provider finds information containing allegations of wrongdoing by a customer or a beneficial owner of a customer, the payment service provider should assess how this affects the level of risk associated with the business relations or transaction undertaken without an account being opened;

(c) commissioning external intelligence reports where it is not possible for a payment service provider to easily obtain information through public sources or where there are doubts about the reliability of public information;

(d) obtaining the following additional information from the customer:

(i) DPT sending or receiving wallet addresses;

(ii) Receipts or other forms of documentation of original purchase of the DPT from an exchange or similar intermediary;

(iii) Transaction details in relation to original purchase of DPT, e.g. number (hash) of transaction, value of transaction (e.g. 2 Bitcoins), timestamp, fee (cost of transaction), size of transaction (in bytes), funds balance history in the address, message recorded in transaction;

(iv) Reasons for purchase of the DPT or current transaction, where applicable.

8-5-9 In relation to paragraph 8.4(a) and (b) of the Notice, where the payment service provider assesses that the business relations with, or the transaction undertaken without an account being opened for, a domestic PEP or an international organisation PEP do not present higher ML/TF risks and that therefore ECDD measures need not be applied, the payment service provider shall nevertheless apply measures under paragraph 6 of the Notice on the customer. However, where changes in events, circumstances or other factors lead to the payment service provider's assessment that the business relations with, or the transactions for, the customer present higher ML/TF risks, the payment service provider should review its risk assessment and apply ECDD measures.

8-5-10 While domestic PEPs and international organisation PEPs may be subject to a risk-based approach, it does not preclude such persons from presenting the same ML/TF risks as a foreign PEP.

8-5-11 With reference to paragraph 8.4(c) of the Notice, while the time elapsed since stepping down from a prominent public function is a relevant factor to consider when determining the level of influence a PEP continues to exercise, it should not be the sole determining factor. Other risk factors that the payment service provider should consider are —

(a) the seniority of the position that the individual previously held when he was a PEP; and

(b) whether the individual's previous PEP position and current function are linked in any way (e.g. whether the ex-PEP was appointed to his current position or function by his successor, or whether the ex-PEP continues to substantively exercise the same powers in his current position or function).

Notice Paragraphs 8.5 to 8.8

8-6 Other Higher Risk Categories

8-6-1 In relation to paragraph 8.7 of the Notice, a payment service provider may refer to preceding paragraph section 8-5-8 of these Guidelines for further guidance on the ECDD measures to be performed.

8-6-2 For customers highlighted in paragraph 8.6(a) of the Notice, a payment service provider shall assess them as presenting higher ML/TF risks. For such customers, the payment service provider shall ensure that the ECDD measures performed are commensurate with the risks. For customers highlighted in paragraph 8.6(b) of the Notice, a payment service provider shall assess whether any such customer presents a higher risk for ML/TF and ensure that the measures under paragraph 6 of the Notice, or ECDD measures where the payment service provider assesses the customer to present a higher risk for ML/TF, performed are commensurate with the risk.

8-6-3 With reference to paragraph 8.6(a) of the Notice, a payment service provider should refer to the FATF Public Statement on High Risk and Other Monitored Jurisdictions on which the FATF has called for counter-measures[5]. FATF updates this Public Statement on a periodic basis and payment service providers should regularly refer to the FATF website for the latest updates[6].

8-6-4 For the purposes of paragraph 8.8 of the Notice, regulations issued by the Authority include the Regulations relating to the freezing of assets of persons and sanctioning of persons.

8-6-5 With regard to tax and other serious crimes, as a preventive measure, payment service providers are expected to reject a prospective customer where there are reasonable grounds to suspect that the customer's assets are the proceeds of serious crimes, including wilful and fraudulent tax evasion. Where there are grounds for suspicion in an existing business relation or when undertaking a transaction without opening an account, payment service providers should conduct enhanced monitoring and where appropriate, discontinue the relationship or not undertake the transaction respectively. If the payment service provider is inclined to retain the customer, approval shall be obtained from senior management with the substantiating reasons properly documented, and the account or transaction subjected to close monitoring and commensurate risk mitigation measures, as applicable. This requirement applies to serious foreign tax offences, even if the foreign offence is in relation to the type of tax for which an equivalent obligation does not exist in Singapore. Examples of tax crime related suspicious transactions are set out in Appendix B of these Guidelines.

[5] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

[6] The link to the FATF website is as follows: http://www.fatf-gafi.org/

11 Notice Paragraph 11 – Reliance on Third Parties

11-1 Paragraph 11 does not apply to outsourcing. Third party reliance under paragraph 11 of the Notice is different from an outsourcing arrangement or agreement.

11-2 In a third party reliance scenario, the third party will typically have an existing relationship with the customer that is independent of the relationship to be formed by the customer with the relying payment service provider. The third party will therefore perform the CDD measures on the customer according to its own AML/CFT policies, procedures and controls.

11-3 In contrast to a third party reliance scenario, the outsourced service provider performs the CDD measures (e.g. performs centralised transaction monitoring functions) on behalf of the payment service provider, in accordance with the payment service provider's AML/CFT policies, procedures and standards, and is subject to the payment service provider's control measures to effectively implement the payment service provider's AML/CFT procedures.

11-4 For avoidance of doubt, holders of a payment services licence or any foreign payment service providers (or its equivalent) are not considered as eligible third parties on which the payment service provider would be able to rely.

11-5 The payment service provider may take a variety of measures, where applicable, to satisfy the requirements in paragraph 11.2(a) and 11.2(b) of the Notice, including—

(a) referring to any independent and public assessment of the overall AML/CFT regime to which the third party is subject, such as the FATF or FSRB's Mutual Evaluation reports and the IMF/World Bank Financial Sector Assessment Programme Reports/Reports on the Observance of Standards and Codes;

(b) referring to any publicly available reports or material on the quality of that third party's compliance with applicable AML/CFT rules;

(c) obtaining professional advice as to the extent of AML/CFT obligations to which the third party is subject to with respect to the laws of the jurisdiction in which the third party operates;

(d) examining the AML/CFT laws in the jurisdiction where the third party operates and determining its comparability with the AML/CFT laws of Singapore;

(e) reviewing the policies and procedures of the third party.

11-6 The reference to "documents" in paragraph 11.2(d) of the Notice includes a reference to the underlying CDD-related documents and records obtained by the third party to support the CDD measures performed (e.g. copies of identification information, CDD/Know Your Customer forms). Where these documents and records are kept by the third party, the payment service provider should obtain an undertaking from the third party to keep all underlying CDD-related documents and

records for at least five years following the termination of the payment service provider's business relations with the customer or the completion of transactions undertaken without an account being opened.

11-7 Paragraph 11.3 of the Notice prohibits the payment service provider from relying on the third party to carry out ongoing monitoring or review of transactions without an account being opened. Paragraph 11.3 of the Notice should be read with the requirements in Parts (VI) and (VII) of paragraph 6 of the Notice.

11-8 For the avoidance of doubt, paragraph 11 of the Notice does not apply to the outsourcing of the ongoing monitoring process by a payment service provider to its parent entity, branches and subsidiaries. A payment service provider may outsource the first-level review of alerts from the transaction monitoring systems, or sanctions reviews, to another party. However, the payment service provider remains responsible for complying with ongoing monitoring requirements under the Notice.

12 Notice Paragraph 12 – Correspondent Accounts

12-1 Payment service providers should note that the requirements under paragraph 12 of the Notice are in addition to performing measures set out under paragraphs 6, 7 and 8 of the Notice, as applicable.

12-2 A payment service provider could act as a correspondent for many payment service providers or FIs around the world. Respondent FIs may be provided with a wide range of services, including custodian wallet services, payable-through accounts and DPT exchange or transfer services.

12-3 Payment service providers should note that foreign exchange and money market transactions do not fall within the scope of "similar services" as referred to in paragraph 12.1 of the Notice.

12-4 After a payment service provider obtains adequate information as required by paragraph 12.3(a) and 12.5(a) of the Notice to establish a correspondent account relationship or the provision of similar services, such information should continue to be updated on a periodic basis thereafter.

12-5 The payment service provider should update the assessment of the suitability of the respondent FI or correspondent FI as required by paragraphs 12.3(a) and 12.5(a) of the Notice respectively, on a periodic basis. If there are material changes to the assessment, the payment service provider should obtain approval from its senior management to continue the provision of correspondent account services to the respondent FI or the use of correspondent account services from the correspondent FI.

12-6 Other factors that a payment service provider should consider in complying with paragraph 12.3(a) and 12.5(a) of the Notice include —

(a) the business group to which the respondent FI or correspondent FI belongs, country of incorporation, and the countries or jurisdictions in which subsidiaries and branches of the group are located;

(b) information about the respondent FI's or correspondent FI's management and ownership, reputation, major business activities, target markets, customer base and their locations;

(c) the purpose of the services provided to the respondent FI and expected business volume; and

(d) the potential use of the account by other respondent FIs in a "nested" correspondent account relationship[7]; the payment service provider should review the risks posed by such "nested" relationships.

[7] Nested correspondent accounts refers to the use of a payment service provider's correspondent relationship by a number of respondent FIs, through their relationships with the payment service provider's direct respondent FI, to conduct transactions and obtain access to other financial services.

12-7 To assess the ML/TF risk associated with a particular country or jurisdiction as required by paragraph 12.3(a)(iii) and 12.5(a)(iii) of the Notice, a correspondent payment service provider may rely on information from the FATF mutual evaluation reports and statements on countries or jurisdictions identified as either being subject to countermeasures or having strategic AML/CFT deficiencies, mutual evaluation reports by FSRBs, publicly available information from national authorities and any restrictive measures imposed on a country, particularly prohibitions on providing correspondent account or other similar services.

12-8 Where a payment service provider provides correspondent account services to, or receives correspondent account services from, FIs that are its related entities, the appropriate level of measures as required under paragraphs 6, 7 and 8 of the Notice (as applicable), and paragraph 12 of the Notice should be applied, bearing in mind that the risk profiles of individual entities within the same financial group could differ significantly. The payment service provider should take into consideration the parent company's level of oversight and control over these related entities, and other risk factors unique to the entities such as their customers and products, the legal and regulatory environment they operate in, and sanctions by authorities for AML/CFT lapses.

12-9 The CDD process should result in a thorough understanding of the ML/TF risks arising from a relationship with the respondent FI or correspondent FI. It should not be treated as a "form-filling" exercise. A payment service provider's assessment of the respondent FI or correspondent FI may be enhanced through meetings with the respondent FI's or correspondent FI's management and compliance head, banking and AML/CFT regulators.

12-10 A payment service provider may apply a risk-based approach in complying with the requirements set out in paragraph 12 of the Notice, but should be mindful that correspondent account relationships generally present higher ML/TF risks.

12-11 If a relevant payment service provider provides correspondent account or other similar services to its related respondent FIs, or receives correspondent account or other similar services from its related correspondent FIs, within the same financial group, the payment service provider should ensure that it still assesses the ML/TF risks presented by its related respondent FI or related correspondent FI.

12-12 Where the head office of the financial group is incorporated in Singapore, it should monitor the correspondent account relationships between payment service providers in its financial group, and ensure that adequate information sharing mechanisms within the financial group are in place.

12-13 For the purposes of paragraph 12 of the Notice, a payment service provider should take into account, for example, any sanctions imposed by relevant authorities on a respondent FI or correspondent FI for failing to have adequate controls against ML/TF activities.

12-14 In assessing whether a FI falls within the meaning of "shell FI" for the purposes of paragraph 12 of the Notice, a payment service provider should note that physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level employees does not constitute physical presence.

13 Notice Paragraph 13 – Value Transfers

13-1 In relation to paragraph 13.1 of the Notice, value transfers include all forms of electronic transmission including, but not limited to, email, facsimile, short message service or other means of secure electronic transmission for payment instructions.

13-2 A payment service provider may use any technology or software solution to transmit the necessary information in the message or payment instruction that accompanies or relates to the value transfer, as long as it enables the ordering institution and the beneficiary institution to comply with the requirements under paragraph 13 of the Notice.

13-3 A payment service provider should not omit, delete or alter information in payment messages, for the purpose of avoiding detection of that information by another FI in the payment process.

13-4 A payment service provider should monitor payment messages to and from higher risk countries or jurisdictions, as well as transactions with higher risk countries or jurisdictions and suspend or reject payment messages or transactions with sanctioned parties or countries or jurisdictions.

13-5 Where name screening checks confirm that the value transfer originator or value transfer beneficiary is a terrorist or terrorist entity, the requirement for the payment service provider to block, reject or freeze assets of these terrorists or terrorist entities cannot be risk-based.

13-6 Where there are positive hits arising from name screening checks, they should be escalated to the AML/CFT compliance function. The decision to approve or reject the receipt or release of the value transfer should be made at an appropriate level and documented.

13-7 For the avoidance of doubt, paragraph 13 of the Notice does not apply to transfers of DPT received from or made to persons who do not fall within the definition of an "ordering institution" or a "beneficiary institution" respectively. A payment service provider may therefore choose to engage in such transactions without applying the requirements set out in paragraph 13. However, as required under paragraph 6.27 of the Notice, the payment service provider should recognise that such transactions may present higher ML/TF risks, and apply appropriate enhanced risk mitigation measures, which could include but are not limited to –

(a) identifying and verifying the identities of the originator and beneficiary of the transfers:

(i) where the transfer of DPT has been received from or sent to the payment service provider's own customer's personal wallet address, requiring the customer to demonstrate control over the said wallet address, by effecting a transfer of DPT of an amount specified by the payment service provider;

(ii) where the originator or beneficiary is identified to be a third party, taking reasonable steps to verify the identity of the third party, which could include the additional checks listed under paragraph 6-12-3 above;

(b) establishing the identity of the beneficial owners of such beneficiaries; and

(c) performing screening and enhanced monitoring over such transactions.

Notice Paragraphs 13.3 to 13.11

13-8 Responsibility of the Ordering Institution

13-8-1 For joint accounts, the ordering institution shall provide all of the joint account holders' information to the beneficiary institution in accordance with paragraph 6.48 of the Notice.

13-8-2 The ordering institution shall include value transfers in its ongoing monitoring of the business relations with the customer or review of transactions undertaken without an account being opened, in accordance with paragraph 6 of the Notice.

13-8-3 In relation to paragraph 13.3 of the Notice, 'value date' refers to the date of receipt of funds by the value transfer beneficiary.

13-8-4 In relation to paragraph 13.9 of the Notice, 'immediately' means that the information collected by the ordering institution should be submitted to the beneficiary institution simultaneously or concurrent with the value transfer. 'Securely' is meant to convey that a payment service provider should protect from unauthorised access, and the integrity of, the value transfer information collected or received, to facilitate record keeping and compliance with other requirements of this Notice.

Notice Paragraphs 13.12 to 13.15

13-9 Responsibility of the Beneficiary Institution

13-9-1 Where an incoming value transfer is not accompanied by complete value transfer originator information and value transfer beneficiary, a beneficiary institution shall request the information from the ordering institution. A payment service provider should consider rejecting incoming value transfers or terminating business relations with overseas ordering institutions that fail to provide originator information. An STR should be filed if appropriate. In this regard, a payment service provider should be mindful of any requirements that may be imposed on the overseas ordering institution, either by law or as a regulatory measure, in relation to value transfers.

13-9-2 As part of its internal risk-based policies, procedures and controls, a payment service provider should consider rejecting incoming value transfers or terminating

business relations with overseas ordering institutions if the payment service provider is not satisfied that it can justify to the Authority the reasons for executing value transfers that lack full originator information.

Notice Paragraphs 13.16 to 13.20

13-10 Responsibility of the Intermediary Institution

13-10-1 An intermediary institution is required under the Notice to retain, and to pass on to the beneficiary institution or another intermediary institution that it effects a value transfer to, all the information accompanying a value transfer effected from an ordering institution or another intermediary institution, to it. The information accompanying the value transfer will be either the unique transaction reference number, as permitted by the Notice, or the full originator and value transfer beneficiary information.

16 Notice Paragraph 16 – Suspicious Transactions Reporting

16-1 A payment service provider should ensure that the internal process for evaluating whether a matter should be referred to the Suspicious Transaction Reporting Office ("STRO") via an STR is completed without delay and should not exceed 15 business days of the case being referred by the relevant employee or officer, unless the circumstances are exceptional or extraordinary.

16-2 A payment service provider should note that an STR filed with STRO would also meet the reporting obligations under the TSOFA.

16-3 Examples of suspicious transactions are set out in Appendix B of these Guidelines. These examples are not intended to be exhaustive and are only examples of basic ways in which money may be laundered or used for TF purposes. Identification of suspicious transactions should prompt further enquiries and where necessary, investigations into the source of funds. A payment service provider should also consider filing an STR if there is any adverse news on its customers in relation to financial crimes. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

16-4 Once suspicion has been raised in relation to a customer or any transaction for that customer, in addition to reporting the suspicious activity, a payment service provider should ensure that appropriate action is taken to adequately mitigate the risk of the payment service provider being used for ML/TF activities. This may include strengthening its AML/CFT processes. This may also include a review of either the risk classification of the customer, or the business relations with the customer. Appropriate action should be taken, including escalating the issue to the appropriate decision making level, taking into account any other relevant factors, such as cooperation with law enforcement agencies.

16-5 STR reporting templates are available on CAD's website[8]. Payment service providers are strongly encouraged to use SONAR, the online system provided by STRO, to lodge STRs. In the event that the payment service provider is of the view that STRO should be informed on an urgent basis, particularly where a transaction is known to be part of an ongoing investigation by the relevant authorities, a payment service provider should give initial notification to STRO by phone or email and follow up with such other means of reporting as STRO may direct. A list of the STR information fields relevant to DPT transactions can be found in Appendix C of these Guidelines.

16-6 A payment service provider should document all transactions that have been brought to the attention of its AML/CFT compliance function, including transactions that are not reported to STRO. To ensure that there is proper accountability for decisions made, the basis for not submitting STRs for any suspicious transactions escalated by its employees and officers should be properly substantiated and documented.

[8] The website address as at 16 March 2020 : https://police.gov.sg/about-us/organisational-structure/specialist-staff-departments/commercial-affairs-department/aml-cft/suspicious-transaction-reporting

16-7 Payment service providers are reminded to read paragraph 16.4 of the Notice together with paragraphs 6.45, 6.46 and 6.47 of the Notice. Where a payment service provider stops performing CDD measures as permitted under paragraph 16.4 and is, as a result, unable to complete CDD measures (as specified under paragraph 6.46), the payment service provider is reminded that it shall not commence or continue the business relations with that customer or undertake any transaction for that customer.

17 Notice Paragraph 17 – Internal Policies, Compliance, Audit and Training

17-1 As internal policies and procedures serve to guide employees and officers in ensuring compliance with AML/CFT laws and regulations, it is important that a payment service provider updates its policies and procedures in a timely manner, to take into account new operational, legal and regulatory developments and emerging or new ML/TF risks.

Notice Paragraphs 17.3 to 17.4

17-2 Compliance

17-2-1 A payment service provider should ensure that the AML/CFT compliance officer has the necessary seniority and authority to effectively perform his responsibilities.

17-2-2 The responsibilities of the AML/CFT compliance officer should include —

(a) carrying out, or overseeing the carrying out of

(i) ongoing monitoring of business relations or review of transactions undertaken without an account being opened; and

(ii) sample review of accounts or transactions for compliance with the Notice and these Guidelines;

(b) promoting compliance with the Notice and these Guidelines, as well as MAS Regulations issued under section 27A of the MAS Act, and taking overall charge of all AML/CFT matters within the organisation;

(c) informing employees and officers promptly of regulatory changes;

(d) ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;

(e) reporting, or overseeing the reporting of, suspicious transactions;

(f) advising and training employees and officers on developing and implementing internal policies, procedures and controls on AML/CFT;

(g) reporting to senior management on the outcome of reviews of the payment service provider's compliance with the Notice and these Guidelines, as well as MAS Regulations issued under section 27A of the MAS Act and risk assessment procedures; and

(h) reporting regularly on key AML/CFT risk management and control issues (including information outlined in paragraph 1-4-17 of the Guidelines), and any necessary remedial actions, arising from audit, inspection, and compliance

reviews, to the payment service provider's senior management, at least annually and as and when needed.

17-2-3 The business interests of a payment service provider should not interfere with the effective discharge of the above-mentioned responsibilities of the AML/CFT compliance officer, and potential conflicts of interest should be avoided. To enable unbiased judgments and facilitate impartial advice to management, the AML/CFT compliance officer should, for example, be distinct from the internal audit and business line functions. Where any conflicts between business lines and the responsibilities of the AML/CFT compliance officer arise, procedures should be in place to ensure that AML/CFT concerns are objectively considered and addressed at the appropriate level of the payment service provider's management.

Notice Paragraph 17.5

17-3 Audit

17-3-1 A payment service provider's AML/CFT framework should be subject to periodic audits (including sample testing). Auditors should assess the effectiveness of measures taken to prevent ML/TF. This would include, among others —

(a) determining the adequacy of the payment service provider's AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;

(b) reviewing the content and frequency of AML/CFT training programmes, and the extent of employees' and officers' compliance with established AML/CFT policies and procedures; and

(c) assessing whether instances of non-compliance are reported to senior management on a timely basis.

17-3-2 The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the payment service provider's business.

Notice Paragraph 17.6

17-4 Employee Hiring

17-4-1 The screening procedures applied when a payment service provider hires employees and appoints officers should include —

(a) background checks with past employers;

(b) screening against ML/TF information sources; and

(c) bankruptcy searches.

17-4-2 In addition, a payment service provider should conduct credit history checks, on a risk-based approach, when hiring employees and appointing officers.

Notice Paragraph 17.7

17-5 Training

17-5-1 As stated in paragraph 17.7 of the Notice, it is a payment service provider's responsibility to provide adequate training for its employees and officers so that they are adequately trained to implement its AML/CFT policies and procedures. The scope and frequency of training should be tailored to the specific risks faced by the payment service provider and pitched according to the job functions, responsibilities and experience of the employees and officers. New employees and officers should be required to attend training as soon as possible after being hired or appointed.

17-5-2 Apart from the initial training, a payment service provider should also provide refresher training at least once every two years, or more regularly as appropriate, to ensure that employees and officers are reminded of their responsibilities and are kept informed of new developments related to ML/TF. A payment service provider should maintain the training records for audit purposes.

17-5-3 A payment service provider should monitor the effectiveness of the training provided to its employees and officers. This may be achieved by —

(a) testing their understanding of the payment service provider's policies and procedures to combat ML/TF, their obligations under relevant laws and regulations, and their ability to recognise suspicious transactions;

(b) monitoring their compliance with the payment service provider's AML/CFT policies, procedures and controls as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action taken; and

(c) monitoring attendance and following up with employees and officers who miss such training without reasonable cause.

I Other Key Topics - Guidance to Payment Service Providers on Proliferation Financing

I-1 Overview

I-1-1 MAS issues Regulations under section 27A of the MAS Act in order to discharge or facilitate the discharge of any obligation binding on Singapore by virtue of a United Nations Security Council Resolution ("UNSCR")[9]. These Regulations apply to all FIs (including payment service providers) regulated by MAS and generally impose financial sanctions on designated persons and prohibit specified activities.

I-1-2 Specifically, a UNSCR may designate certain individuals and entities involved in the proliferation of weapons of mass destruction and its financing. The relevant information and full listings of persons designated by UNSCRs can be found on the UN website[10].

I-1-3 MAS has given effect to relevant UNSCRs, including those as listed by the FATF Recommendations (2012) to be relevant to combating proliferation financing by issuing Regulations. Examples of such Regulations are the MAS (Sanctions and Freezing of Assets of Persons – Iran) Regulations 2016 and MAS (Sanctions and Freezing of Assets of Persons – Democratic People's Republic of Korea) Regulations 2016.

I-1-4 A payment service provider should rely on its CDD measures (including screening measures) under the Notice to detect and prevent proliferation financing activities and transactions.

I-1-5 A payment service provider should also ensure compliance with legal instruments issued by MAS relating to proliferation financing risks, as well as take into account any other guidance from MAS. An example would be the MAS' Sound Practices to Counter Proliferation Financing available on MAS' website.

I-2 CDD and Internal Controls

I-2-1 It is important to ensure that name screening by a payment service provider, as required under the Notice, is performed against the latest UN listings as they are updated from time to time. A payment service provider should have in place policies, procedures and controls to continuously monitor the listings and take necessary follow-up action within a reasonable period of time, as required under the applicable laws and regulations.

1-2-2 The payment service provider's CDD policies and procedures should have clear processes on the idenfication of the customer's beneficial owners, and the forming of a good understanding of the customer's business and transactions from the

[9] Please refer to the MAS website for a full listing of Regulations issued by MAS pursuant to the United Nations Security Council Resolutions.

[10] Please see: http://www.un.org/sc/committees/1718 and http://www.un.org/sc/committees/1737

proliferation financing perspective. Enhanced due diligence measures, including the conduct of periodic reviews and closer scrutiny (including on counterparties) should also be applied where the customer or transaction pose higher risks.

I-2-3 A payment service provider should also have policies and procedures to detect attempts by its employees or officers to circumvent the applicable laws and regulations (including MAS Regulations) such as —

(a) omitting, deleting or altering information in payment messages for the purpose of avoiding detection of that information by the payment service provider itself or other payment service providers involved in the payment process; and

(b) structuring transactions with the purpose of concealing the involvement of designated persons.

I-2-4 A payment service provider should have policies and procedures to prevent such attempts, and take appropriate measures against such employees and officers.

I-3 Obligation of Payment Service Provider to Freeze without Delay

I-3-1 A payment service provider is reminded of its obligations under the MAS Regulations issued under section 27A of the MAS Act[11] to immediately freeze any funds, financial assets or economic resources owned or controlled, directly or indirectly, by designated persons that the payment service provider has in its possession, custody or control. For the avoidance of doubt, the obligations to freeze without delay also applies to all DPTs. The payment service provider should also promptly file an STR in such cases.

I-4 Potential Indicators of Proliferation Financing

I-4-1 A payment service provider should develop indicators and monitoring capabilities that would alert it to customers and transactions (actual or proposed) that are possibly associated with proliferation financing-related activities, including indicators such as whether —

(a) the customer is vague and resistant to providing additional information when asked;

(b) the customer's activity does not match its business profile;

(c) the transaction involves designated persons;

[11] Please refer to the following link for the MAS AML/CFT Regulations - https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions

(d) the transaction involves higher risk countries or jurisdictions which are known to be involved in proliferation of weapons of mass destruction or proliferation financing activities;

(e) the transaction involves other FIs with known deficiencies in AML/CFT controls or controls for combating proliferation financing;

(f) the transaction involves possible shell companies (e.g. companies that do not have a high level of capitalisation or display other shell company indicators) or front companies and transactions involving accounts held in third countries;

(g) the transaction involves containers whose numbers have been changed or ships that have been renamed;

(h) the shipment of goods takes a circuitous route or the financial transaction is structured in a circuitous manner;

(i) the transaction involves the shipment of goods inconsistent with normal geographic trade patterns (e.g. the country involved would not normally export or import such goods);

(j) the transaction involves the shipment of goods incompatible with the technical level of the country to which goods are being shipped (e.g. semiconductor manufacturing equipment shipped to a country with no electronics industry);

(k) there are inconsistencies in the information provided in trade documents and financial flows (e.g. in the names, companies, addresses, ports of call and final destination); or

(l) there are indications of illicit ship to ship transactions that have taken place (e.g. (shipping documents on movement of goods may indicate atypical flows or movements, or involving ports that would normally not be suitable to handle specific products).

I-4-2 Please also refer to the MAS' Sound Practices to Counter Proliferation Financing available on MAS' website for more examples of indicators and risk mitigation.

I-5 Other Sources of Guidance on Proliferation Financing

I-5-1 The FATF has also provided guidance on measures to combat proliferation financing and a payment service provider may wish to refer to the FATF website for additional information.

II ML/TF Risks Arising from Use of Virtual Assets

II-1 Background

II-1-1 Recent rapid technology improvements has a far-reaching impact, including in the world of payments. Enhancements in financial technology in particular, has opened up new opportunities for faster and more efficient payment methods. However, these new payment methods also give rise to new money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks.

II-1-2 Singapore had highlighted the potential ML/TF risks from virtual assets[12] in our National Risk Assessment in 2014. We had identified it as an area of further study and to include it within our AML/CFT regulations – virtual assets were gaining acceptance as a means of payment globally, but at that point, there was no global standard on how virtual assets should be treated[13]. Taking into account the potential ML/TF/PF risks, we first consulted with industry in 2016, with the intention of developing a framework to regulate virtual assets (or digital payment tokens (DPTs) as used in the PS Act) activities. Singapore also recognises the potential ML/TF risks with regard to virtual assets (for investment purposes), that are capital market products. For such cases, the entities that deal in such products would already be required under the Securities and Futures Act to comply with AML/CFT requirements – please see section on *Securities and Futures Act* below.

Prevalence on Use of Virtual Assets in Singapore

II-1-3 MAS' surveillance suggests that virtual assets activity in Singapore has increased from a low base in recent years. Speculative trading of virtual assets on exchange platforms hit a peak in early 2018 with the rise in virtual assets market capitalisations, although the monthly trading volumes are less than 1% of those on the Singapore Exchange. Initial coin offerings (ICO) also gained popularity as a means for issuers to raise capital[14].

II-1-4 While these activities have become more prevalent in recent years, activities relating to virtual assets has slowed noticeably in 2019, particularly as virtual asset valuations fell to substantially below their peaks. It is also noted that despite Singapore's FinTech hub status, virtual assets activity in Singapore forms a small portion of global activity, and is not material compared to traditional financial activities in Singapore's financial system.[15]

II-1-5 Virtual asset service providers (VASPs) or DPT service providers operating in Singapore largely relate to: (i) exchange platforms (exchange between fiat and

[12] A virtual asset is defined by the Financial Action Task Force as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

[13] FATF, the global AML/CFT standards setter, adopted enhanced standards on virtual assets in June 2019.

[14] Please see section on "Securities and Futures Act" below for more details.

[15] For more details, please see MAS Financial Stability Review Box B (November 2018), "Monitoring Digital Token Markets: An Early Look at Frameworks and Techniques".

virtual assets or between 2 different types of virtual assets); and (ii) financial services surrounding ICOs.

II-1-6 It has been observed overseas that there is an emergence of standalone custodial wallet service providers and service providers facilitating the transfer of virtual assets – however, in Singapore, these activities are usually provided by platforms that also offer exchange services, rather than as standalone services. Another area of emerging risk focus would be the transfer of the same virtual assets between exchanges (e.g. an exchange is used to intermediate between the transfer of bitcoin from a wallet to another wallet).

II-2 Environment

Threats posed by Virtual Assets

II-2-1 Virtual assets could be abused for ML/TF purposes particularly because of: (i) the pseudonymity (or in some cases anonymity) they offer; (ii) the convenience they provide as a near-instantaneous value transfer medium; and (iii) cross-border nature of the transactions.

II-2-2 Virtual assets were first identified as an emerging risk in the National Risk Assessment in 2014. Since then, law enforcement has noted an upward trend of reported cases involving virtual assets with a total of 383 of such reports lodged from 2016 to 2018.

II-2-3 The majority of the cases reported relate to cheating (e.g. scams) and offences under the Computer Misuse and Cybersecurity Act. Law enforcement agencies have also noted an instance of attempted money laundering relating to virtual assets (see below for ML case study). These developments are consistent with international typologies where cases tend to relate more to fraud/cheating types and with some indication of virtual assets being used for money laundering, usually associated with organised crimes and/or drug trafficking.[16]

II-2-4 While we have noted foreign cases of virtual assets being used for TF purposes, we have to date not observed such cases in Singapore, although Singapore authorities continue to be vigilant and mindful of such vulnerabilities.

II-2-5 To mitigate potential risks, relevant authorities in Singapore are continuously enhancing capabilities to detect and investigate crimes and illicit activity involving virtual assets.

II-2-6 From the reports received by law enforcement, and our surveillance there are three broad ways that virtual assets can be exploited in Singapore; as a payment method, marketed product, and as a targeted item.

[16] FATF's Guidance for a risk-based approach to virtual assets also affirms that virtual assets have characteristics such as increased anonymity, which may make them more susceptible to abuse by criminals, money launderers and terrorist financiers. Significant cases involving virtual assets were related to hacking incidents, including Mt Gox, Coincheck, Bitfinex, and Binance. BTC-e was another example that involved computer hacking, identity theft, tax fraud schemes and drug trafficking.

(a) **Payment Method:** Ransomware malware where ransom payment (in virtual assets like Bitcoin) are demanded, impersonation scams where scammers impersonate foreign officials (e.g. government officials) to demand a settlement fee in virtual asset for offences victims allegedly committed. In some cases, tainted assets had flowed through virtual assets exchanges.

(b) **Marketed Product:** Schemes involving ICOs, e-commerce scams selling virtual assets.

(c) **Targeted Item:** Unauthorised transactions involving virtual assets (e.g. hacking).

Money Laundering Typologies

II-2-7 Many of the money laundering typologies found in the virtual asset space are similar to those existing in the traditional or fiat space, involving placement, layering and integration of funds/assets to conceal its illicit source. However, criminals using virtual assets could also seek to utilise the anonymising features (e.g. TORs, tumblers/mixers, privacy coins) inherent in the distributed ledger technology as a means to further obscure the transaction chain. The Darknet is also known to be used to further such ML schemes. The use of such anonymising features should, at minimum, be considered as indicators of higher risk transactions.

II-2-8 The **placement stage** could involve VASPs (especially those with weak AML/CFT controls), unlicensed VASPs, ICO-related schemes, or Bitcoin ATMs. These VASPs may only require very limited or basic information at the account opening stage, allowing customers to put false or vague information to conceal their true identity (e.g. just a pseudonym and email address required). VASPs may also have lax or inadequate due diligence checks on the source of wealth and source of funds (e.g. from mixers/tumblers, private wallets (in particular of unknown third parties), Darknet or originating from higher risk jurisdictions). Ongoing monitoring at the VASP may also be weak to non-existent, which further exposes the VASP to the risk of being abused for ML/TF if access to its accounts are compromised, either by complicit involvement of the account holders, or due to unusual movements arising from hacks or scams.

II-2-9 The **layering stage** could involve the distribution of illicit funds/assets via “mule” accounts, exchanging different forms of virtual assets (including privacy-enhanced virtual assets, i.e. privacy coins) through many hops, through the use of decentralised exchanges or mixers/tumblers. With the increase in use of non-face-to-face verification at the on-boarding stage, there is also an emergence of “mule” accounts using stolen online KYC information. Decentralised exchanges would also present higher risk as they are often unregulated (due to the lack of a central administrator), and may not apply adequate AML/CFT measures. Privacy coins are intentionally structured to conceal identities of counterparties and transactions, which would also serve to conceal illicit sources of funds/assets.

II-2-10 The **integration stage** could involve exchanging of virtual assets into fiat, and transferring it into the traditional financial system (e.g. bank account). As virtual assets become increasingly accepted as modes of payment, they could also be used to purchase goods, especially high value goods, as a further store of value.

Case Study 1

Proceeds from an email fraud perpetuated against a victim in Country A were transferred to a Singaporean bank account used by a Singaporean company. The Singaporean company offers an online trading platform and payment gateway for virtual assets.

Using forged documents, the perpetuator opened an online trading account with the Singaporean company. The perpetuator had credited his account with criminal proceeds from the Country A. The perpetuator then purchased Bitcoins, regardless of the price, through the online trading platform. Due to the unusual trading pattern, the online trading account was blocked by the Singaporean company. Upon receiving a recall letter from the bank, the Singaporean company liquidated the Bitcoins that the perpetuator purchased. The funds were seized by the Police and subsequently returned to the victim.

Terrorism Financing Typologies

II-2-11 Singapore, as a major financial centre with a tech-savvy populace, and a significant migrant and expatriate community, is vulnerable to abuse for terrorism financing using virtual assets. These risks are also increased due to the region that Singapore is located.

II-2-12 Our surveillance has noted evidence of foreign cases of virtual assets being exploited by terrorist groups, while there is no evidence of widespread usage, there is an increasing trend of terrorist groups soliciting funding (or raise funds) via virtual assets in the last three years.

II-2-13 Jihadist groups have encouraged supporters to donate “millions of dollars” in Bitcoin and other virtual assets to ISIS, Al-Qaeda and Hamas. These assets can be moved through charities, media offices, aid organisations, or directly through jihadi blogs.

II-2-14 Individuals and small terror cells may also fund activity using virtual assets – these transactions are much harder to detect from patterns of generic money laundering, although it is noted that they are more directed towards higher TF-risk jurisdictions (such as those identified by the FATF), or could be transferred (through multiple hops in a short duration) to an address associated to extremist sites.

II-2-15 Law enforcement agencies in Singapore continue to closely monitor the potential TF activity related to virtual assets. At this time, there are no indications that the abuse of virtual assets for TF is an avenue of significant concern in Singapore.

Suspicious Transaction Reports Involving Virtual Assets

II-2-16 Although we have observed an increasing level of threat posed by virtual assets, there is also increased vigilance within the financial sector and by VASPs in Singapore of the potential misuse of virtual assets.

II-2-17 The number of STRs filed involving virtual assets is on an increasing trend, indicating better risk understanding and awareness amongst the regulated sectors that deal with virtual assets, VASPs, or are VASPs themselves.

II-2-18 **VA-related STRs filed by Reporting Sector:** The majority of the virtual assets-related STRs were filed by Banks, Other Payment Method Providers (e.g. a payment operator) and Virtual Assets Intermediaries (or DPT service providers).

II-2-19 **Offences:** The majority of the STRs relating to virtual assets did not disclose any specific offence, and were mainly filed based on the filer's review of the transactions, including reasons such as:

(a) Unable to determine relationship between parties of transaction for CDD purposes;

(b) Transaction inconsistent with known profile of entities;

(c) Funds received are immediately transferred out/withdrawn;

(d) Transaction involving instruments where identity of source of funds cannot be immediately known.

II-2-20 For STRs with possible offence disclosed, Fraud/Cheating and Offences under the Computer Misuse Act[17] are the most common offences.

International Cooperation on Cases involving Virtual Assets

II-2-21 In line with the increasing prevalence and misuse of virtual assets globally, there is also an upward trend of requests for assistance (RFAs) involving virtual assets.

II-2-22 The VA-related RFAs pertain mostly to possible Fraud/Cheating, Drug Related and/or Money Laundering offences.

Case Study 2

The requesting state was investigating a domestic company ("Company A") for fraud and money laundering, in connection with another company overseas ("Company B"). Company B was running a pyramid scheme, which sold to customers "educational packages" that could be converted to OneCoin, purported to be a cryptocurrency. However, OneCoin failed to meet the digital currency

[17] These offences typically relate to cybersecurity issues such as unauthorised access.

criteria due to the lack of blockchain technology. As a result, OneCoin could not perform the functions of a normal cryptocurrency, like payments.

Between March 2017 and October 2017, payments for Company B's educational packages were made to a bank account traced to Company A. Money was transferred from Company A's account to a bank account with a company based in Singapore ("Company C").

Singapore authorities rendered assistance to the requesting state through the provision of a voluntary statement and company documents from Company C. Singapore will not hesitate to take enforcement action should there be domestic laws breached.

II-3 Virtual Assets Regulatory and Supervisory Framework in Singapore

Supervisory Approach

II-3-1 MAS applies a risk-based approach to supervision, including VASPs regulated in Singapore. Our supervision includes a combination of on-site inspections and off-site monitoring and surveillance. Our on-site inspections include regular and thematic inspections to test FIs' effectiveness in key areas such as ongoing monitoring, and combating proliferation financing and terrorism financing. Virtual asset service providers, including FIs which are involved in such activities, will be included in these thematic inspections, where they are identified as higher risk. In addition, MAS' off-site monitoring will also enable us to identify and target specific key risks and initiate supervisory follow-up actions including for-cause inspections as necessary.

Payment Services Act

II-3-2 ML/TF risks have been identified as the primary risk concerns posed by virtual assets, given the anonymity, speed and cross-border nature of transactions facilitated by virtual asset providers. Under the Payment Services Act (PS Act), MAS will impose AML/CFT requirements on the intermediaries that buy, sell or exchange virtual assets in Singapore – these are the VASP business models identified to be operating in Singapore.

II-3-3 Under the PS Act, aligned with the FATF standards, DPT service providers are required to conduct customer due diligence and transaction monitoring measures, as well as to report suspicious transactions to the authorities. They are also required to screen and submit information on their customers when transferring DPTs to one another on behalf of their customers, and make this information available on request to appropriate authorities in Singapore. In addition, transfer

requirements, in line with the FATF Standards (i.e. para 7(b) of the Interpretive Note to Recommendation 15) apply to DPT service providers[18].

II-3-4 MAS takes a risk sensitive approach to applying AML/CFT requirements, according to the ML/TF risks posed by the activities. Activities that pose higher ML/TF risks are subject to the full suite of requirements, while activities that present lower risks are subject to lesser requirements. Applying this risk sensitive approach, cross border peer-to-peer money transfers are subject to full AML/CFT requirements while payments for goods and services funded through an identifiable source[19] which present low ML/TF risks and will not be subject to AML/CFT requirements.

II-3-5 In addition, DPT service providers have to understand the ML/TF risks they face, and apply appropriate mitigating measures. For example, a Singapore-incorporated entity that only offers services outside of Singapore, may pose higher ML/TF risks due to the lack of operational presence in the foreign jurisdiction. Dealing with an entity that is not subject to AML/CFT regulation would also similarly pose higher ML/TF risks.

II-3-6 MAS will apply a risk-based approach to supervision of DPT providers. This will include robust licensing fit and proper checks, and inspections to be conducted to test FIs' effectiveness at combating ML/TF and PF. MAS' AML/CFT supervision will also be supplemented by findings from MAS' surveillance of higher risk areas in the virtual assets space. MAS' surveillance includes looking at virtual asset transactions and networks to detect unusual behaviours or suspicious transactions. We will also use it to proactively detect entities that may be operating illegally without a licence.

Securities and Futures Act

II-3-7 Offers or issues of virtual assets are also regulated by MAS if the virtual assets are capital markets products under the existing Securities and Futures Act (SFA). This includes the financial activities surrounding the issuance of a virtual asset. Capital markets products include any securities, units in a collective investment scheme, derivatives contracts and spot foreign exchange contracts for purposes of leveraged foreign exchange trading

II-3-8 MAS has clarified our regulatory position on virtual assets that are capital market products, in various media releases, replies to parliamentary questions and through the issuance of "A Guide to Digital Token Offerings" (https://mas.gov.sg/publications/monographs-or-information-paper/2019/a-guide-

[18] As required under paragraph 13 (Value Transfers) of the Notice, DPT service providers that facilitate the sending of DPTs are required to obtain and hold required and accurate originator information and required beneficiary information on DPT transfers, immediately and securely submit the above information to beneficiary DPT service providers and counterparts (if any), and make the information available on request to appropriate authorities.

[19] Identifiable source means an account maintained with an MAS-regulated FI that is subject to AML/CFT requirements, or an account maintained with a foreign FI, that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF. Refer to Regulation 28(7) of the Payment Services Regulation 2019 for the full definition.

to-digital-token-offerings) to provide further guidance on the application of securities laws to offers of virtual assets in Singapore. MAS has also taken action to enforce its regulatory message for persons to comply with our securities laws, for virtual assets offered as securities.[20]

III Conclusions

III-1-1 MAS considers that transactions involving virtual assets carry higher inherent ML/TF/PF risks, due to the anonymity, speed and cross-border nature of the transactions. MAS has put in place risk targeted regulations to address and mitigate the ML/TF/PF risks posed by virtual assets in Singapore today. Effective implementation of MAS' AML/CFT requirements by DPT providers and other FIs will be supported by a robust combination of off-site supervision and on-site inspections.

III-1-2 It is also acknowledged that virtual assets activities are continually evolving, with new business models emerging. Singapore authorities, including MAS, are closely monitoring the risks posed by these new business models, and will take the necessary steps to mitigate the risks posed.

III-1-3 In light of the enhanced FATF standards for virtual assets (issued in June 2019), MAS has announced its intention to expand the scope of legislation, including the PS Act, to cover additional activities of virtual assets by service providers so as to fully align with international AML/CFT requirements. To this end, we will cover entities incorporated in Singapore which are involved in providing virtual assets services, i.e. those relating to payments and/or investments, outside of Singapore.

III-1-4 Concomitantly, MAS expects all FIs to assess and monitor the risks posed by virtual assets in their business operations, and take necessary steps to mitigate risks as appropriate. In addition, FIs should properly communicate their risk concerns so that legitimate customers are given opportunities to address them adequately. For example, banks should assess each VASP customer on its own merits, identifying the risks associated with the customer, communicate the risk concerns to the customer and assess if and how the risks can be adequately mitigated. Banks should not deny bank accounts without cause, for entire classes of customers including VASPs. It is important for banks to adopt this balanced approach to avoid unduly affecting the banking needs of customers conducting legitimate businesses.

[20] For instance, in 24 May 2018, MAS directed an ICO issuer to stop offering its digital tokens and to return all funds received from Singapore-based investors. MAS also warned eight digital token exchanges in Singapore not to facilitate trading in digital tokens that are securities or futures contracts without MAS' authorisation (http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-warns-Digital-Token-Exchanges-and-ICO-Issuer.aspx) In January 2019, MAS warned an ICO issuer not to proceed with its securities token offering in Singapore until it can comply with regulatory requirements (https://www.mas.gov.sg/news/media-releases/2019/mas-halts-securities-token-offering-for-regulatory-breach)

IV Useful Links

Financial Action Task Force ("FATF"): http://www.fatf-gafi.org/

FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

……

APPENDIX A – Examples of CDD Information for Customers (Including Legal Persons/Arrangements)

Customer Type	Examples of CDD Information
Sole proprietorships	• Full registered business name • Business address or principal place of business • Information about the purpose and intended nature of the business relations or transaction with the payment service provider • Names of all natural persons who act on behalf of the sole proprietor (where applicable) • Name of the sole proprietor • Information about the source of funds • A report of the payment service provider's visit to the customer's place of business, where the payment service provider assesses it as necessary • Structure of the sole proprietor's business (where applicable) • Records in an independent company registry or evidence of business registration
Partnerships and unincorporated bodies	• Full name of entity • Business address or principal place of business • Information about the purpose and intended nature of the business relations or transaction with the payment service provider • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the payment service provider's visit to the customer's place of business, where the payment service provider assesses it as necessary • Ownership and control structure • Records in an independent company registry • Partnership deed • The customer's membership with a relevant professional body • Any association the entity may have with other countries or jurisdictions (e.g. the location of the entity's headquarters, operating facilities, branches, subsidiaries)
Companies	• Full name of entity • Business address or principal place of business

Customer Type	Examples of CDD Information
	• Information about the purpose and intended nature of the business relations transaction with the payment service provider • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the payment service provider's visit to the customer's place of business, where the payment service provider assesses it as necessary • Ownership and control structure • Records in an independent company registry • Certificate of incumbency, certificate of good standing, share register, as appropriate • Memorandum and Articles of Association • Certificate of Incorporation • Board resolution authorising the opening of the customer's account with the payment service provider • Any association the entity may have with other countries or jurisdictions (e.g. the location of the entity's headquarters, operating facilities, branches, subsidiaries)
Public sector bodies, government, state-owned companies and supranationals (other than sovereign wealth funds)	• Full name of entity • Nature of entity (e.g. overseas government, treaty organisation) • Business address or principal place of business. • Information about the purpose and intended nature of business relations or transaction with the payment service provider • Name of the home state authority and nature of its relationship with its home state authority • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Information about the source of funds • Ownership and control structure • A report of the payment service provider's visit to the customer's place of business, where the payment service provider assesses it as necessary • Board resolution authorising the opening of the customer's account with a licensee
Clubs, Societies and Charities	• Full name of entity • Business address or principal place of business

Customer Type	Examples of CDD Information
	• Information about the purpose and intended nature of business relations or transaction with the payment service provider • Information about the nature of the entity's activities and objectives • Names of all trustees (or equivalent) • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the payment service provider's visit to the customer's place of business, where the payment service provider assesses it as necessary • Ownership and control structure • Constitutional document • Certificate of registration • Committee/Board resolution authorising the opening of the customer's account with the payment service provider • Records in a relevant and independent registry in the country of establishment

Customer Type	Examples of CDD Information
Trust and Other Similar Arrangements (e.g. Foundations, Fiducie, Treuhand and Fideicomiso)	• Full name of entity • Business address or principal place of business • Information about the nature, purpose and objectives of the entity (e.g. discretionary, testamentary) • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the payment service provider's visit to the customer's place of business, where the payment service provider assesses it is necessary • Information about the purpose and intended nature of business relations or transaction with the payment service provider • Records in a relevant and independent registry in the country or jurisdiction of constitution • Country or jurisdiction of constitution • Trust deed • Names of the settlors/trustees/beneficiaries or any person who has power over the disposition of any property that is subject to the trust • Declaration of trusts • Deed of retirement and appointment of trustees (where applicable)

APPENDIX B – Examples of Suspicious Transactions

B-1 General Comments

B-1-1 The list of situations given below is intended to highlight some basic ways in which money may be laundered or used for TF purposes. While each individual situation may not be sufficient to suggest that ML/TF is taking place, a combination of such situations may be indicative of a suspicious transaction. The list is intended solely as an aid, and must not be applied as a routine instrument in place of common sense.

B-1-2 The list is not exhaustive and may be updated due to changing circumstances and new methods of laundering money or financing terrorism. Payment service providers are to refer to STRO's website for the latest list of ML/TF red flags[21].

B-1-3 A customer's declarations regarding the background of such transactions should be checked for plausibility.

B-1-4 It is not unreasonable to proceed with caution any customer who is reluctant to provide normal information and documents required routinely by the payment service provider in the course of business relations or when undertaking any transaction without an account being opened. Payment service providers should pay attention to customers who provide minimal, false or misleading information or, when establishing business relations or undertaking a transaction without opening an account, provide information that is difficult or expensive for the payment service provider to verify.

B-2 Transactions Which Do Not Make Economic Sense

i) Transactions that cannot be reconciled with the usual activities of the customer.

ii) A customer relationship with the payment service provider where a customer has a large number of accounts with the same payment service provider, and/or makes frequent transfers between different accounts.

iii) Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal

iv) Transactions which are incompatible with the payment service provider's knowledge and experience of the customer in question.

[21] The website address as at 16 March 2020 : https://police.gov.sg/about-us/organisational-structure/specialist-staff-departments/commercial-affairs-department/aml-cft/suspicious-transaction-reporting

v) Unnecessary routing of funds through multiple intermediary payment service providers, FIs or persons.

vi) Substantial increase(s) in account activity by a customer without apparent cause, especially if value transfers are made to an account/ person not normally associated with the customer.

vii) Concentration of payments where multiple senders make value transfers to a single individual's account.

viii) Transactions which lack an apparent relationship between the sender and beneficiary, and/or personal transfers of value sent to countries or jurisdictions that have no apparent family or business link to customer, and/or the customer has no relation to the country where he/she sends/receives the value transfer and cannot sufficiently explain why value transfer is sent there/received from there.

ix) Large amounts of funds or DPT deposited into an account, which is inconsistent with the source of funds and/or wealth of the customer.

x) Transactions which, without plausible reason, result in the intensive use of what was previously a relatively inactive account, such as a customer's account which previously had virtually no personal or business related activities, but is now used to received or disburse unusually large sums which have no obvious purpose or relationship to the customer or his business.

B-3 Transactions Involving Large Amounts

i) Frequent transactions involving large cash amounts or a high value of DPT that do not appear to be justified by the customer's business activity or background.

ii) Customers making large and/or frequent value transfers, mostly to individuals and firms not normally associated with their business.

iii) Customers making large value transfers to persons outside Singapore with instructions for payment in cash.

iv) Numerous transactions by a customer, especially over a short period of time, such that the amount of each transaction is not substantial, but the cumulative total of which is substantial.

v) Customers who together, and simultaneously, use separate branches to conduct large (cash) transactions.

vi) Customers whose transactions involve counterfeit notes or forged instruments.

vii) Large and regular payments of funds or DPT that cannot be clearly identified as bona fide transactions, from and to countries associated with (a) the production, processing or marketing of narcotics or other illegal drugs or (b) other criminal conduct.

viii) Fund or value transfers made to a single person by a large number of different persons without an adequate explanation.

ix) Customers who receive frequent and/or large transactions from virtual asset kiosks.

B-4 Tax Crimes Related Transactions

i) Negative tax-related reports from the media or other credible information sources

ii) Unconvincing or unclear purpose or motivation for establishing business relations or conducting business transactions in Singapore.

iii) Originating sources of multiple or significant deposits/withdrawals are not consistent with declared purpose of the account.

iv) Inability to reasonably justify frequent and large fund or value transfers that originate from or are being made to a beneficiary in a country or jurisdiction that presents higher risk of tax evasion.

v) Customers send or receive (regular) payments from persons in countries which are regarded as “tax havens” or which are known to be exposed to risks such as drug trafficking, terrorism financing, smuggling. Amounts transacted are not necessarily large.

B-5 Other Types of Transactions

i) The customer fails to reasonably justify the purpose of a transaction when queried by the payment service provider.

ii) Transactions for which customers fail to provide a legitimate reason when asked.

iii) Account activity or transaction volume is not commensurate with the customer’s known profile (e.g. age, occupation, income).

iv) Account has undergone a long period of dormancy, followed by a large volume or velocity of transactions.

v) Transactions with persons in countries or entities that are reported to be associated with terrorism activities or with persons that have been designated as terrorists.

vi) Frequent changes to the customer's address or authorised signatories.

vii) When a young person opens an account and either withdraws or transfers the funds within a short period, which could be an indication of terrorism financing.

viii) When a person receives funds or DPT from a religious or charitable organisation and exchanges the funds or DPT, utilises the funds or DPT for purchase of assets or transfers the funds to another person within a relatively short period.

ix) Transactions where funds are deposited from or withdrawn to virtual asset addresses with direct or indirect links to known suspicious sources (e.g. darknet marketplaces, mixing/tumbling services, or addresses associated with illegal activities such as ransomware attacks).

x) Transfers from one or more senders often from different countries and/or in different currencies to a local person over a short period of time.

xi) Periodic transfers made by several people to the same person or related persons.

xii) False information during the identification process/ lack of co-operation. Use of third parties to effect funds or value transfers aimed at concealing the sender and/or receiver of moneys.

xiii) The customer uses intermediaries that are not subject to adequate AML/CFT laws.

xiv) No or limited information about the origin of funds or DPT.

xv) Funds or DPT used by a customer to settle his obligations are from a source(s) that appears to have no explicit or direct links to the customer.

xvi) Banknotes brought by customer are in small denominations and dirty; stains on the notes indicating that the funds have been carried or concealed, or the notes smell musty; notes are packaged carelessly and precipitately; when the funds are counted, there is a substantial difference between the actual amount and the amount indicated by the customer (over or under).

xvii) Transactions that are suspected to be in violation of another country's or jurisdiction's foreign exchange laws and regulations.

B-6 Customer Behaviour

i) Use of Virtual Private Network ("VPN") and/or The Onion Router ("TOR") to access his online account.

ii) Customer registers for an account using an encrypted, anonymous or temporary email service.

iii) Frequent changes in the customer's identification information, such as home address, IP address or linked bank accounts/wallet addresses.

iv) Customer shows uncommon curiosity about internal systems, controls and policies.

v) Customer is overly eager to provide information or details that are not requested for.

vi) Customer is willing to pay high commission fees for services in comparison to typical rates charged by other payment service providers.

APPENDIX C – STR Information Fields for DPT Transactions

C-1 General Comments

C-1-1 The table below is intended to highlight sections of STRO's STR reporting form, SONAR, which would be directly relevant for the reporting of suspicious transactions related to DPT services or transactions. The list is intended to provide a general guide to help facilitate the accurate and appropriate filing of STRs, and the examples featured are not meant to be exhaustive. Reporting entities are required to ensure that all relevant sections of the STR form, including those sections not featured below, are duly completed.

STR field	DPT information to provide
Part I: Reporting Institution	
Institution Type	• Select "Payment and Settlement System" if report relates to DPT and/or related intermediaries and services
Business Type	• Select "Virtual Currency Intermediaries" if report relates to DPT and/or related intermediaries and services
Part II: Account Information	
Are there account(s) involved in the suspicious activity you are reporting on	• Click "Yes" if DPT wallets/addresses are being reported on
Is the known account maintained with the reporting institution?	• Click "Yes" if DPT wallets/addresses are held with the reporting institution • Click "No" if DPT wallets/addresses are held elsewhere other than the reporting institution