Monetary Authority of Singapore

GUIDELINES TO MAS NOTICE PSN01 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

2 April 2024

Last revised on 1 July 2025

TABLE OF CONTENTS

For ease of reference, the chapter numbers in these Guidelines mirror the corresponding paragraph numbers in MAS Notice PSN01 on Prevention of Money Laundering and Countering the Financing of Terrorism - Holders of Payment Services Licence (Specified Payment Services) (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 PSN01 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 services licence that carry on a business of providing a specified payment service, and all persons exempt under section 13(1) of the Payment Services Act 2019 ("PS Act") where such person offers a specified product (collectively referred to as "payment service providers") on the requirements in MAS Notice PSN01 on Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Specified Payment Services) ("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 7, 8 and 9 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]

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 1992. 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.

(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

[1] Money laundering includes proliferation financing, and all references in these Guidelines to money laundering (including money laundering risks) are to be construed accordingly.

place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate funds.

Terrorism Financing

1-4-3 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 act" set out in the Terrorism (Suppression of Financing) Act 2002 ("TSOFA").

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

1-4-5 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.

1-4-6 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.

1-4-7 Singapore's primary legislation to combat TF is the TSOFA. Payment service providers may also refer to the MAS website and the Inter-Ministry Committee on Terrorist Designation's website for more information.

Proliferation Financing

1-4-7A Proliferation financing ("PF") refers to the raising, moving or making available of funds, other assets or other economic resources, or financing, in whole or in part, to individuals or entities for the purposes of the proliferation of weapons of mass destruction, including the proliferation of their means of delivery or related materials (including both dual-use technology and dual-use goods for non-legitimate purposes), under the relevant regulations issued under section 192 read with section 15(1)(b) of the Financial Services and Markets Act 2022 ("FSM Act") relating to sanctions and freezing of assets of persons ("FSM Sanctions Regulations")[2].

[2] The FSM Sanctions Regulations include the regulations issued under section 192 read with sections 15(1)(b) and 219(d) of the FSM Act. Please refer to the following link for the FSM Sanctions Regulations: https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/regulations-for-targeted-financial-sanctions. Currently, the relevant FSM Sanctions Regulations are those relating to the Democratic People's Republic of Korea and Iran.

The Three Lines of Defence

1-4-8 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.

1-4-9 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.

1-4-10 Business units (e.g. front office customer-facing functions of the payment service provider's business premises) 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 1-413.

1-4-11 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 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.

1-4-12 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.

1-4-13 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 payment 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

1-4-14 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.

1-4-15 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 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 Partnerships Act 2005 and section 28 of the Limited Partnerships Act 2008.

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 member of the board of directors, senior management or equivalent functions of a payment service provider.

Payment for Goods or Services

2-6 In relation to the definition of "payment for goods or services" in the Notice, a payment service provider should ascertain to a high degree of certainty that the transactions are made only for the intended purposes of payment for goods or services to merchants, and not for peer-to-peer transactions.

2-7 The payment service provider should adopt appropriate and reasonable means to ascertain that the merchant, to whom the payment is intended for, is legitimately in the business of providing goods or services. This may be achieved using technological, contractual and/or other means (e.g. site visits). It should be noted that "payment for goods or services" would not apply where payment is made to a shell company, since there would be no provision of goods or services to speak of normally.

2-8 For the avoidance of doubt, payment to individuals should not be considered as payment for goods or services as it would be difficult to reliably determine whether every payment is for actual payments for goods or services or peer-to-peer transfers.

2-9 A payment service provider should also put in place mitigating measures to detect and prohibit transactions that are not for payment of goods or services.

3 Notice Paragraph 3 – Application of Notice

3-1 MAS has assessed that a combination of certain characteristics of a payment service provider, or product, would pose sufficiently low ML/TF risks, and therefore exempted from certain AML/CFT requirements in the Notice. Nonetheless, given rapid developments in the payment services sector, with the emergence of new business models and payment methods, MAS and the relevant authorities will regularly monitor and review the risks arising from this sector. We may adjust the AML/CFT requirements and our supervisory expectations accordingly, after due consultation.

3-2 With respect to paragraph 3.1(a) of the Notice, MAS has identified the following activities (i.e. the specified payment services) as activities that carry ML/TF risks, and which will be subject to the AML/CFT requirements under the Notice:

(a) account issuance services;
(b) domestic money transfer services;
(c) cross-border money transfer services; and
(d) money-changing services.

3-3 With respect to paragraph 3.1(b) of the Notice, a person exempt under section 13(1) of the PS Act ("exempted person") is exempted from the requirements of the relevant MAS Notice on Prevention of Money Laundering and Countering the Financing of Terrorism that is applicable to the class of financial institutions the person belongs to ("respective Notices"), and which the person is already subject to. The exemption is pursuant to MAS Notice PSN10 on Prevention of Money Laundering and Countering the Financing of Terrorism – Exempt Payment Service Provider, and applies only to the extent that such requirements relate to the exempted person's provision of payment services for a specified product. The exempted person should continue to comply with the requirements under the respective Notices in relation to its other business activities. For example, a bank licensed under the Banking Act 1970 is exempted from MAS Notice 626 in relation to payment services for a specified product, but must continue to comply with MAS Notice 626 in relation to its banking and other services. In addition, the bank must comply with the Notice, i.e. MAS Notice PSN01, in relation to the provision of payment services for the specified product.

3-4 With respect to paragraph 3.3 of the Notice, a payment service provider that offers a product that is an exempted product should have in place processes and procedures to verify and ensure that such exempted product(s) meet the definition of "exempted product" as set out in paragraph 2 of the Notice, on an on-going basis. The payment service provider does not have to comply with the paragraphs of the Notice set out in paragraph 3.3, in relation to the exempted product(s).

3-5 For the avoidance of doubt, the requirements in the Notice would not apply to a payment service provider that only offers payment services for exempted products.

A payment service provider that provides payment services for exempted products, in addition to other specified payment services, must comply with the requirements in the Notice, but need not comply with the paragraphs set out in paragraph 3.3 of the Notice in relation to such exempted product(s). In other words, the payment service provider shall comply, in relation to all its businesses relating to payment services (which may include exempted product(s) and other specified payment services) with paragraphs 4 (Underlying Principles)[3], 5 (Assessing Risks and Applying a Risk-based Approach), 6 (New Products, Practices and Technologies), 16 (Record Keeping)[4], 17 (Personal Data), 18 (Suspicious Transactions Reporting), and 19 (Internal Policies, Compliance, Audit and Training) of the Notice.

[3] In relation to the application of paragraph 4 (Underlying Principles), MAS will not require payment service providers, where they offer exempted product(s), to comply with paragraph 4.1(a) of the Notice in relation to the exempted product(s).
[4] In relation to the application of Section 16 (Record Keeping), MAS will not require payment service providers, where they offer exempted product(s), to comply with record keeping requirements in relation to the retention of CDD information as set out in paragraph 16.2(c) of the Notice insofar that it relates to the exempted product(s).

5 Notice Paragraph 5 – Assessing Risks and Applying a Risk-Based Approach

Countries or Jurisdictions of its Customers

5-1 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

5-2 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

5-3 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.[5] 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, subsidiaries and agents, 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.

5-4 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.

5-5 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.

[5] To avoid doubt, ML/TF risks, whether presented by an individual customer or on an enterprise-wide level, include PF risks.

5-6 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 transfers, considering the usual activities and the risk profiles of its customers.

(b) in relation to the countries or jurisdictions its customers are from, in or transacting with, 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, subsidiaries and agents operate in) or the activities of its customers (including the financial institutions ("FI") with whom the payment service provider provides payment services to or engages to facilitate the provision of payment 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;

- 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; and

(iii) the delivery channels, including whether the payment service provider operates entirely online or in person, 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.

5-7 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.

5-8 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 should involve evaluating data on the payment service provider's activities using the applicable broad risk factors set out in paragraph 5-6.

5-9 As required by paragraph 5.1(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.

5-10 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 Risk Assessment Reports

5-11 A payment service provider should incorporate the results of Singapore's risk assessment reports[6] in its enterprise-wide ML/TF risk assessment process. 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 in the risk assessment reports 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.

5-12 The risk assessment reports also identify certain prevailing crime types as presenting higher ML/TF risks. A payment service provider should consider these results 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 business relations or transactions undertaken without an account being opened.

Risk Mitigation

5-13 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.

5-14 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.

5-15 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);

[6] These risk assessment reports include the Money Laundering National Risk Assessment Report, the Terrorism Financing National Risk Assessment Report, the Proliferation Financing National Risk Assessment Report and other risk assessment reports, which can be found at this link: https://www.mas.gov.sg/regulation/anti-money-laundering/ml-tf-pf-risk-assessments.

(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. antifraud, general compliance, trade operations 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 senior management and board;

(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

5-16 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.

5-17 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

5-18 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.

6 Notice Paragraph 6 – New Products, Practices and Technologies

6-1 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.

6-2 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 or the movement of such funds. These assessments should be approved by senior management.

6-3 An example of a "new delivery mechanism" as set out in paragraph 6 of the Notice is mobile applications for payment services.

7 Notice Paragraph 7 – Customer Due Diligence

Notice Paragraph 7.2

7-1 Where There are Reasonable Grounds for Suspicion prior to the Establishment of Business Relations or Undertaking any Transaction without Opening an Account

7-1-1 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 7.3 to 7.4

7-2 When CDD is to be Performed and Linked Transactions

7-2-1 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 to deliberately restructure an otherwise single transaction, with the intention of circumventing applicable thresholds set out in the Notice.

7-2-2 A payment service provider should make further enquiries when a customer performs frequent and cumulatively large transactions without any apparent of visible economic or lawful purpose. For example, frequent deposits and withdrawals from the same account over a short period of time, or multiple money transfers over a short period of time such that the amount of each money transfer is not substantial, but the total of which is substantial.

Notice Paragraphs 7.5 to 7.18

7-3 CDD Measures under Paragraphs 7.5 to 7.18

7-3-1 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 or to counterfeit. 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.

7-3-2 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 7.6 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 7.6

7-4 Identification of Customer

7-4-1 With respect to paragraph 7.6(a)(iii) 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.

7-4-2 A payment service provider should obtain a customer's contact details such as personal, office or work telephone numbers.

Notice Paragraph 7.8

7-5 Identification of Customer that is a Legal Person or Legal Arrangement

7-5-1 Under paragraph 7 and paragraph 9 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[7]. 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.

7-5-2 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.

7-5-3 In relation to legal arrangements, a payment service provider shall perform CDD measures on the customer by identifying the trust relevant parties, as required by paragraph 7.14 of the Notice.

Notice Paragraph 7.9

[7] 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 8-3 of these Guidelines.

7-6 Verification of Identity of Customer

7-6-1 Where the customer is a natural person, a payment service provider should obtain identification documents that contain a clear photograph of that customer.

7-6-2 In verifying the identity of a customer, a payment service provider may obtain the following documents:

(a) Natural Persons —

(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 or its equivalent, 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.

7-6-3 Further guidance on verification of different types of customers (including legal persons or legal arrangements) is set out in Appendix A.

7-6-4 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

7-6-5 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.

7-6-5A A payment service provider should ensure that staff are provided with adequate guidance on how to identify indicators of fraudulent or tampered data, documents or information. A payment service provider should also have processes in place to ensure that such indicators are escalated, and the appropriate ML/TF risk mitigation measures are applied, in a timely manner. Examples of indicators of fraudulent or tampered data, documents or information include:

(a) significant discrepancies in a customer's representations (e.g. relating to material sources of wealth or significant transactions) that are found when these representations are checked against independent sources of information, such as corporate data reports;

(b) anomalies in financial statements that are not in line with the payment service provider's understanding of the customer's profile; and

(c) lack of sign-off by relevant certifying parties such as an auditor or notary public.

7-6-6 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.

7-6-7 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.

7-6-8 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 7.10 to 7.12

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

7-7-1 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.

7-7-2 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 7.13 to 7.17

7-8 Identification and Verification of Identity of Beneficial Owner

7-8-1 A payment service provider should note that measures listed under paragraph 7.14(a)(i), (ii) and (iii) as well as paragraph 7.14(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.

7-8-2 In relation to paragraph 7.14(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).

7-8-3 A natural person who does not meet the shareholding threshold referred to in paragraph 7-8-2 above but who controls the customer (e.g. through exercising significant influence), is a beneficial owner under the Notice.

7-8-4 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.

7-8-5 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.

7-8-6 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.

7-8-7 For the purposes of paragraph 7.16 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.

7-8-8 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.

7-8-9 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.

7-8-10 Where a customer is one which falls within paragraph 7.16 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 8 of the Notice.

Notice Paragraph 7.18

7-9 Information on the Purpose and Intended Nature of Business Relations and Transaction Undertaken without an Account Being Opened

7-9-1 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 7.19 to 7.25

7-10 Review of Transactions Undertaken without an Account Being Opened

7-10-1 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 to the same recipient, frequent money-changing transactions over a short period of time or multiple transfers of funds such that the amount of each fund transfer is not substantial, but the total of which is substantial.

7-10-2 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.

7-10-3 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 cash 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).

7-10-4 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.

7-10-5 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.

7-10-6 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 7.26 to 7.33

7-11 Ongoing Monitoring

7-11-1 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. The adequacy of monitoring systems 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.

7-11-2 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 to the same recipient, frequent transactions over a short period of time or multiple transfers of funds such that the amount of each fund transfer is not substantial, but the total of which is substantial.

7-11-3 Where there are indications that the risks associated with existing business relationships may have increased (for example, where there are anomalies in the control or conduct of an account or discrepancies relating to a customer's source of wealth), the payment service provider should promptly implement commensurate risk mitigation measures, including enhanced ongoing monitoring. Examples of enhanced ongoing monitoring are enhanced monitoring of transactions (including pre-transaction checks) and the imposition of restrictions on the account. The payment service provider should also request additional information and conduct a review of the customer's risk profile in order to determine if further measures are necessary.

7-11-4 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.

7-11-5 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.

7-11-6 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.

7-11-7 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 cash 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).

7-11-8 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.

7-11-9 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.

7-11-10 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.

7-11-11 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. This includes having processes and appropriate confidentiality safeguards to share information on customers and their related accounts within and across business units, where information to be shared should minimally include CDD information collected by the payment service provider under Section 7 of the Notice as well as source of wealth information collected by the payment service provider under paragraph 9.3(b) of the Notice.

7-11-12 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 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.

7-11-13 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 7.34 to 7.40

7-12 CDD Measures for Non-Face-to-Face Business Relations or Non-Face-to Face Transactions Undertaken without an Account Being Opened

7-12-1 A reference to “specific risks” in paragraph 7.34 of the Notice includes risks arising from establishing business relations and undertaking transactions in the course of a business relations or undertaking transactions without an account being opened, according to instructions conveyed by customers through any means of communication (for example, 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 nonface-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.

7-12-2 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.

7-12-3 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 —

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

(h) verification of a customer's identity through a document that customer has signed with a secure digital signature using a set of PKIS based credentials issued by a certified Certificate Authority under the Electronic Transactions Act 2010; or

(i) 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.

7-12-4 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.

7-12-5 A payment service provider may wish to conduct the independent assessment in paragraph 7.37 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.

7-12-6 In considering whether there has been a substantial change in the policies and procedures in paragraph 7.39 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 7.41

7-13 Reliance by Acquiring Payment Service Provider on Measures Already Performed

7-13-1 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 7.41 of the Notice are met. A payment service provider shall maintain proper records of its due diligence review performed on the acquired business.

7-13-2 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.

7-13-3 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 7.41 of the Notice, it is also required to comply with the requirements set out in paragraphs 7.19 to 7.33 of the Notice.

Notice Paragraph 7.43 to 7.45

7-14 Timing for Verification

7-14-1 With reference to paragraph 7.44 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.

7-14-2 With reference to paragraph 7.45 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.

7-14-3 For avoidance of doubt, delayed verification should not be applied for transactions undertaken without an account being opened.

Notice Paragraph 7.50

7-15 Existing Customers

7-15-1 In relation to customer accounts which pre-date the coming into force of the current Notice, the payment service provider should prioritise the remediation of higher risk customers.

7-15-2 In taking into account any previous measures as referred to in paragraph 7.50 of the Notice, a payment service provider should consider whether —

(a) there has been any significant transaction undertaken, since the measures were last performed, having regard to the manner in which the account is ordinarily operated;

(b) there is a material change, since the measures were last performed, in the way that business relations with the customer is conducted;

(c) it lacks adequate identification information on a customer; and

(d) there is a change in the ownership or control of the customer, or the persons authorised to act on behalf of the customer in its business relations with the payment service provider.

Notice Paragraphs 7.51 to 7.54

7-16 Screening

7-16-1 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.

7-16-2 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 the FSM Sanctions Regulations. Any such assets should be reported promptly to the relevant authorities and a Suspicious Transaction Report ("STR") should be filed as soon as possible, no later than 1 business day after suspicion was first established[8].

7-16-3 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 (i) commercial databases and where appropriate,

[8] This refers to the point in time when the payment service provider concludes that the filing of an STR is warranted, based on available information, the circumstances and its investigations.

pertinent search engines[9] used to identify adverse information on individuals and entities, (ii) individuals and entities covered under the FSM Sanctions Regulations and TSOFA, and (iii) 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.

7-16-4 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.

7-16-5 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

[9] A risk-based approach may be adopted to determine when additional screening against pertinent search engines to address potential limitations or gaps in existing screening tools is appropriate. Take for example, the case where there is an apparent match in relation to material ML/TF concerns on the person screened, but further information is necessary to determine whether the apparent match is a positive match. In such a case, screening against pertinent search engines, such as internet-based search engines predominantly used in countries or jurisdictions closely associated with the nationality, residence or source of wealth of the person screened (as available), may be appropriate.

provider becomes aware of such breaches, it should immediately take the necessary actions and inform the relevant authorities.

7-16-6 In screening periodically as required by paragraph 7.52(e) 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).

7-16-7 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.

7-16-8 In determining the frequency of periodic name screening, a payment service provider should consider its customer's risk profile.

7-16-9 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 the FSM Sanctions Regulations. 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.

7-16-10 With reference to paragraph 7.53 of the Notice, transaction screening should take place on a real-time basis (i.e. the screening or filtering of relevant payment instructions should be carried out before the transaction is executed).

8 Notice Paragraph 8 – Simplified Customer Due Diligence

8-1 Paragraph 8.1 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 –

(a) the customer is one whom the payment service provider only effects or receives cross-border wire transfers that are solely for the payment of goods and services and funded from an identifiable source; or

(b) the payment service provider is satisfied, upon analysis, that the ML/TF risks are low.

8-2 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 FSM Sanctions Regulations 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.

8-3 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.

8-4 Subject to paragraph 8.4 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.

8-5 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) 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; and

(ii) 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).

9 Notice Paragraph 9 – Enhanced Customer Due Diligence

9-1 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.

9-2 Examples of potentially higher risk categories under paragraph 9.7 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 transaction undertaken without an account being opened is conducted under unusual circumstances (e.g. significant unexplained geographic distance between the payment service provider and the customer);

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

(vi) cash-intensive businesses; and

(vii) customers who exhibit characteristics of a higher risk shell company[10], including but not limited to:

(i) unclear economic purpose for requiring account relationship in Singapore:
    (i) E.g. foreign-incorporated companies with no business presence or activities in Singapore seek to open accounts in Singapore (including through a nominee arrangement);

(ii) unclear economic purpose for linking a common individual / address to multiple companies:

[10] FIs may refer to the following papers for further information
(i) MAS Guidance Paper on "Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons" (June 2019)
(ii) MAS "Guidance to Capital Markets Intermediaries on Enhancing AML/CFT Frameworks and Controls" (January 2019)
(iii) AML/CFT Industry Partnership ("ACIP") Best Practice Paper on "Legal Persons Misuse Typologies and Best Practices" (May 2018)

(i) E.g. multiple companies are linked to the same registered address, where the address is not in line with and/or fit for the companies' nature of business;
(ii) E.g. use of nominee individuals to obscure beneficial ownership and control of the account;

(iii) unrelated third parties (e.g. foreigners) added to operate account after account opening:
(i) E.g. directors are changed, post-account opening, to allow unrelated third parties to operate the account;

(iv) unusual change of corporate structure / beneficial owner after account opening;

(v) suspicious transactions which are not in line with the payment service provider's understanding of customer; or

(vi) superficial corporate websites inconsistent with scale of business:
(i) E.g. companies (including newly incorporated companies) that are stated to be involved in a wide range of activities without a dominant product/expertise;
(ii) E.g. corporate websites have vague descriptions and limited information, which are not in line with the turnover or business nature of the companies.

(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, subsidiaries and agents operate in) or the activities of its customers (including the 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.

9-3 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 9.1

9-4 Politically Exposed Persons ("PEPs") Definitions

9-4-1 The definitions in paragraph 9.1 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.

9-4-2 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.

9-4-3 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.

9-4-4 With reference to paragraph 9.1 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.

9-4-5 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 9.2 to 9.4

9-5 PEPs

9-5-1 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.

9-5-2 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.

9-5-3 In relation to paragraph 9.3(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.

9-5-4 In relation to paragraph 9.3(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.

9-5-5 Source of wealth generally refers to the origin of the customer's and beneficial owner's entire body of wealth (i.e. total assets), and includes seed money that generated subsequent wealth and gifts or other assets (if any) received by the customer and beneficial owner. Source of wealth 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 obtained by the payment service provider, should give an indication, to the extent practicable, about the entire body of wealth that the customer and beneficial owner would be expected to have, and how the customer and beneficial owner acquired the wealth. This information would enable the payment service provider to make a reasonable assessment of which sources of wealth of the customer and beneficial owner are material and/or present a higher risk for ML/TF. 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.

9-5-6 Source of funds refers to the origin of the particular funds or other assets which are the subject of the establishment of business relations 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.

9-5-7 Subject to paragraph 9.5 of the Notice, a payment service provider should corroborate the information regarding source of wealth and source of funds. In relation to paragraph 9.3(b) of the Notice, examples of "appropriate and reasonable means" for establishing source of wealth or source of funds are information and documents such as copies of trust deeds, salary details, tax returns, bank statements, audited 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), conveyancing documents (in cases where the source of wealth or funds is a sale of property) and credible public information sources. A payment service provider should take a risk-based approach and focus on corroboration of sources of wealth and sources of funds that are more material and/or present a higher risk for ML/TF. A payment service provider should ensure that such sources of wealth and sources of funds are established through appropriate and reasonable means, to the extent practicable, using reliable and independent sources of information. In cases where independent sources of information are not available, the payment service provider should exercise prudence in the use of non-independent sources of information, such as customer representations, assumptions and benchmarks, to ensure adequate rigour of assessment. This should include the performance of additional checks against alternative information sources to determine whether such information, representations, assumptions or benchmarks are reasonable and reliable. The payment service provider's basis for using such information should be documented and reviewed periodically. The payment service provider is also reminded that assumptions and benchmarks should facilitate its assessment of the plausibility of the customer or beneficial owner's source of wealth or source of funds, and should not be used to justify or support circumstances or explanations provided by the customer or beneficial owner if there are reasons that cast suspicion on their source of wealth or source of funds.

9-5-7A Where a payment service provider is unable to corroborate any source of wealth or source of funds that is more material and/or presents a higher risk for ML/TF, the payment service provider should assess whether the residual risks associated with not corroborating such source of wealth or source of funds is acceptable and whether additional risk mitigation measures should be applied in the absence of corroboration. Examples of risk mitigation measures include obtaining senior management's approval to establish or continue business relations with the customer and conducting enhanced ongoing monitoring of the business relationship.

9-5-7B Where a material source of wealth of the customer or beneficial owner is a gift or other asset received from third parties, a payment service provider should obtain information to establish the legitimacy and plausibility of such gift or other asset. This should include establishing the relationship between the third party and the customer or beneficial owner, and verifying the transaction(s) effecting such gift or

other asset against reliable and independent sources of information such as bank statements or public sources where practicable. A payment service provider should also assess the plausibility of the third party's source of wealth as part of the assessment. Where unable to do so, the payment service provider should assess the residual risks presented by the third party's source of wealth, and consider whether the additional risk mitigation measures as set out in paragraph 9-5-7A should be applied on the business relationship with the customer.

9-5-7C A payment service provider should assess if the customer and beneficial owner's source of wealth and source of funds are plausible and legitimate, considering all the information and documents that the payment service provider has obtained. Where the payment service provider is unable to ascertain the plausibility and legitimacy of the customer or beneficial owner's source of wealth or source of funds, the payment service provider should consider if there are grounds for terminating business relations with the customer and whether an STR should be filed.

9-5-8 In relation to paragraph 9.3 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.

9-5-9 In relation to paragraph 9.5(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 7 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.

9-5-10 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.

9-5-11 With reference to paragraph 9.5(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 9.6 to 9.9

9-6 Other Higher Risk Categories

9-6-1 In relation to paragraph 9.8 of the Notice, a payment service provider may refer to preceding paragraph section 9-5-8 of these Guidelines for further guidance on the ECDD measures to be performed. A payment service provider should assess whether the information regarding the source of wealth and source of funds of the customer and any beneficial owner should be corroborated against additional documentary evidence or public information sources and document its assessment [11]. The payment service provider may refer to the preceding paragraphs 9-5-5 to 9-5-7C of these Guidelines for further guidance on establishing the source of wealth and source of funds of customers and beneficial owners.

9-6-1A A payment service provider should pay attention to changes in the customer's risk profile, information and/or transactions that would warrant corroboration of the customer and any beneficial owner's source of wealth and source of funds, and do so in a timely manner.

9-6-2 For customers highlighted in paragraph 9.7(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

[11] For example, the payment service provider may assess whether source of wealth corroboration against additional documentary evidence is necessary, where the payment service provider's customer is (i) a listed company that has publicly available information on its wealth-generating commercial activities, or (ii) a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF and thus subject to corporate governance or other regulatory requirements.

commensurate with the risks. For customers highlighted in paragraph 9.7(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 7 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.

9-6-3 With reference to paragraph 9.7(a) of the Notice, a payment service provider should refer to the FATF Public Statement on High Risk Jurisdictions subject to a Call for Action[12]. FATF updates this Public Statement on a periodic basis and payment service providers should regularly refer to the FATF website for the latest updates[13].

9-6-4 For the purposes of paragraph 9.9 of the Notice, regulations issued by the Authority include the Regulations relating to the freezing of assets of persons and sanctioning of persons.

9-6-5 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 relations or when undertaking a transaction without opening an account, payment service providers should conduct enhanced monitoring and where appropriate, discontinue the relations 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.

[12] Please refer to the high-risk jurisdictions subject to a FATF call on its members and other jurisdictions to apply countermeasures (i.e. "black list" jurisdictions) in the FATF webpage - https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions.html

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

12 Notice Paragraph 12 – Reliance on Third Parties

12-1 Paragraph 12 does not apply to outsourcing. Third party reliance under paragraph 12 of the Notice is different from an outsourcing arrangement or agreement.

12-2 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.

12-3 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.

12-4 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.

12-5 The payment service provider may take a variety of measures, where applicable, to satisfy the requirements in paragraph 12.2(a) and 12.2(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.

12-6 The reference to "documents" in paragraph 12.2(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.

12-7 Paragraph 12.3 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 12.3 of the Notice should be read with the requirements in Parts (VI) and (VII) of paragraph 7 of the Notice.

12-8 For the avoidance of doubt, paragraph 12 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.

13 Notice Paragraph 13 – Correspondent Accounts

13-1 Payment service providers should note that the requirements under paragraph 13 of the Notice are in addition to performing measures set out under paragraphs 7, 8, 9 of the Notice, as applicable.

13-2 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 cash management (e.g. accounts in a variety of currencies), payable-through accounts and exchange services.

13-3 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 13.1 of the Notice.

13-4 After a payment service provider obtains adequate information as required by paragraphs 13.3(a) and 13.5(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.

13-5 The payment service provider should update the assessment of the suitability of the respondent FI or correspondent FI as required by paragraphs 13.3(a) and 13.5(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.

13-6 Other factors that a payment service provider should consider in complying with paragraphs 13.3(a) and 13.5(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[14]; the payment service provider should review the risks posed by such "nested" relationships.

13-7 To assess the ML/TF risks associated with a particular country or jurisdiction as required by paragraphs 13.3(a)(iii) and 13.5(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 or jurisdiction, particularly prohibitions on providing remittance services.

13-8 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 7, 8 and 9 of the Notice (as applicable), and paragraph 13 of the Notice should be applied, bearing in mind that the risk profiles of individual entities within the same 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.

13-9 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, compliance head and AML/CFT regulators.

13-10 A payment service provider may apply a risk-based approach in complying with the requirements set out in paragraph 13 of the Notice but should be mindful that correspondent account relationships generally present higher ML/TF risks.

13-11 If a 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.

13-12 Where the head office of the financial group is incorporated in Singapore, it should monitor the correspondent account relationships between payment service

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

providers in its financial group, and ensure that adequate information sharing mechanisms within the financial group are in place.

13-13 For the purposes of paragraph 13 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 criminal activities.

13-14 In assessing whether a FI falls within the meaning of “shell FI” for the purposes of paragraph 13 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.

13-15 In a country or jurisdiction where provision of cross border money transfer services is a regulated activity, a payment service provider should engage FIs which are regulated, to facilitate the cross border transfer of moneys to recipients in that country or jurisdiction, instead of entering into agreements or arrangements with other unregulated entities to do the same.

14 Notice Paragraph 14 – Agency Arrangements

14-1 For the avoidance of doubt, notwithstanding the appointment of an agent, the payment service provider shall remain responsible for its AML/CFT obligations in the Notice.

14-2 Paragraph 14.2(a) of the Notice requires that any agency arrangement be documented in writing because such written documentation is important to set out the respective roles and responsibilities of the payment service provider and the agent.

14-3 A payment service provider should develop stringent agent selection criteria to ensure that an agent is fit and proper and has the necessary resources to comply with the payment service provider's AML/CFT programme as required under paragraph 14.2(d) of the Notice. In monitoring agents' compliance with its AML/CFT programme as required under paragraph 14.2(d) of the Notice, a payment service provider should put in place and implement robust policies, procedures and controls. Such policies, procedures and controls should be approved by the payment service provider's senior management and reviewed periodically to ensure that they are kept up-to-date and relevant.

14-4 A payment service provider should conduct a periodic review of its agents to evaluate their compliance level with its policies and procedures. Where the payment service provider observes any non-compliance with its AML/CFT programme, it should document its findings and consider whether to take any remedial action, such as the termination of the agency agreement. The payment service provider should obtain approval from its senior management on the proposed action to be taken, including any proposal not to take any action.

14-5 In complying with paragraph 14.4 of the Notice, the payment service provider should obtain and retain with the current list of its agents, information such as the agents' full names (including any aliases), unique identification numbers (such as an identity card number, birth certificate number or passport number, or where the agent is not a natural person, the incorporation number or business registration number), residential addresses or registered or business addresses, and if different, principal place of businesses (as may be appropriate), dates of birth, establishment, incorporation or registration (as may be appropriate) and nationality or place of incorporation or registration (as may be appropriate). The payment service provider should obtain all necessary documentation that identifies and verifies the agent appointed, including its shareholding structure, the board of director, the management team, beneficial owner(s), where appropriate. The payment service provider should also record and retain information such as the date of commencement, date of termination and reasons for terminating the agency arrangement. The payment service provider should ensure that such information should continue to be relevant and updated on a regular basis thereafter.

14-6 A payment service provider should conduct regular AML/CFT training for all appointed agents similar to training of the payment service provider's employees and officers as required by paragraph 19.7 of the Notice.

15 Notice Paragraph 15 – Wire Transfers

15-1 In relation to paragraph 15.1 of the Notice, wire transfers include all forms of electronic transmission including, but not limited to, email, facsimile, short message service or other means of electronic transmission for payment instructions.

15-2 In relation to paragraph 15.9 of the Notice, examples of domestic wire transfers in Singapore include inter-bank transfers via the local MAS Electronic Payment System ("MEPS+").

15-3 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.

15-4 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.

15-5 Where name screening checks confirm that the wire transfer originator or wire 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.

15-6 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 wire transfer should be made at an appropriate level and documented.

Notice Paragraphs 15.3 to 15.11

15-7 Responsibility of the Ordering Institution

15-7-1 For joint accounts, the ordering institution shall provide all of the joint account holders' information to the beneficiary institution in accordance with paragraph 7.49 of the Notice.

15-7-2 The ordering institution shall include wire 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 7 of the Notice.

15-7-3 In relation to paragraph 15.3 of the Notice, 'value date' refers to the date of receipt of funds by the wire transfer beneficiary.

Notice Paragraphs 15.12 to 15.15

15-8 Responsibility of the Beneficiary Institution

15-8-1 Where an incoming wire transfer is not accompanied by complete wire transfer originator information and wire transfer beneficiary, a beneficiary institution shall request the information from the ordering institution. A payment service provider should consider rejecting incoming wire 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 cross-border wire transfers.

15-8-2 As part of its internal risk-based policies, procedures and controls, a payment service provider should consider rejecting incoming wire 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 wire transfers that lack full originator information.

Notice Paragraphs 15.16 to 15.20

15-9 Responsibility of the Intermediary Institution

15-9-1 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 wire transfer to, all the information accompanying a wire transfer effected from an ordering institution or another intermediary institution, to it. The information accompanying the wire transfer will be either the unique transaction reference number, as permitted by the Notice, or the full originator and wire transfer beneficiary information.

18 Notice Paragraph 18 – Suspicious Transactions Reporting

18-A The detection and investigation of concerns of higher ML/TF risks, even before suspicions of ML/TF are raised, can facilitate the early imposition of ML/TF risk mitigation measures. In this regard, a payment service provider should ensure that processes are in place to:

(a) identify and prioritise the review of concerns of higher ML/TF risks;

(b) ensure that such concerns of higher ML/TF risks are reviewed promptly; and

(c) require any such concerns of higher ML/TF risks that cannot be reviewed promptly to be escalated to senior management, or a similar oversight body, for the application of appropriate ML/TF risk mitigation measures.

18-1 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. The filing of an STR should not exceed 5 business days after suspicion was first established[15], unless the circumstances are exceptional or extraordinary. In cases involving sanctioned parties[16] and parties acting on behalf of or under the direction of sanctioned parties[17], a payment service provider should file the STRs as soon as possible, and no later than 1 business day after suspicion was first established[18].

18-2 A payment service provider should note that an STR filed with STRO would also meet the reporting obligations under the TSOFA.

18-3 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.

18-4 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

[15] This refers to the point in time when the payment service provider concludes that the filing of an STR is warranted, based on available information, the circumstances and its investigations.
[16] "Sanctioned parties" include persons designated or covered under the Terrorism (Suppression of Financing) Act 2002 and the regulations issued under section 192 read with section 15(1)(b) of the Financial Services and Markets Act 2022 relating to sanctions and freezing of assets of persons.
[17] Such cases include cases involving any funds, other financial assets or economic resources owned or controlled, directly or indirectly, by sanctioned parties.
[18] This refers to the point in time when the payment service provider concludes that the filing of an STR is warranted, based on available information, the circumstances and its investigations.

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. Other appropriate action that should be taken include escalating the issue to the appropriate decision making level, taking into account any other relevant factors, such as cooperation with law enforcement agencies. After reporting the suspicious activity, where further suspicion is raised in relation to the customer or any transaction for the customer, the payment service provider should assess if the filing of a further or supplementary STR to report the further suspicion is warranted.

18-5 STR reporting templates are available on CAD's website[19]. 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.

18-6 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.

18-7 Payment service providers are reminded to read paragraph 18.4 of the Notice together with paragraphs 7.46, 7.47 and 7.48 of the Notice. Where a payment service provider stops performing CDD measures as permitted under paragraph 18.4 and is, as a result, unable to complete CDD measures (as specified under paragraph 7.47), 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.

[19] The website address as at 30 June 2025: https://www.police.gov.sg/Advisories/Crime/Commercial-Crimes/Suspicious-Transaction-Reporting-Office

19 Notice Paragraph 19 – Internal Policies, Compliance, Audit and Training

19-1 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 19.2A to 19.2H

19-2A Group Policy

19-2A-1 For the avoidance of doubt, Singapore branches of payment service providers incorporated outside Singapore need not comply with paragraphs 19.2A to 19.2H of the Notice. Paragraphs 19.2A to 19.2H of the Notice are intended to be applied by a payment service provider incorporated in Singapore to its branches and subsidiaries, but not to its parent entity and the payment service provider's other related corporations.

19-2A-2 In relation to paragraph 19.2D of the Notice, examples of the types of information that should be shared within the financial group for risk management purposes are positive name matches arising from screening performed against ML/TF information sources, a list of customers who have been exited by the payment service provider, its branches and subsidiaries based on suspicion of ML/TF and names of parties on whom STRs have been filed. Such information should be shared by a branch or subsidiary of a payment service provider incorporated in Singapore with the payment service provider's group level compliance, audit, and AML/CFT functions (whether in or outside Singapore), for risk management purposes.

Notice Paragraphs 19.3 to 19.4

19-2 Compliance

19-2-1 A payment service provider should ensure that the AML/CFT compliance officer has the necessary seniority and authority to effectively perform his responsibilities.

19-2-2 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 the FSM Sanctions Regulations, 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 the FSM Sanctions Regulations and risk assessment procedures; and

(h) reporting regularly on key AML/CFT risk management and control issues (including information outlined in paragraph 1-4-15 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.

19-2-3 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 19.5

19-3 Audit

19-3-1 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.

19-3-2 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 19.6

19-4 Employee Hiring

19-4-1 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.

19-4-2 In addition, a payment service provider should conduct credit history checks, on a risk-based approach, when hiring employees and appointing officers.

Notice Paragraph 19.7

19-5 Training

19-5-1 As stated in paragraph 19.7 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.

19-5-2 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.

19-5-3 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 the FSM Sanctions Regulations in order to discharge or facilitate the discharge of any obligation binding on Singapore by virtue of a United Nations Security Council Resolution ("UNSCR") adopted by the United Nations Security Council ("UNSC"). 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, the UNSC may designate certain individuals and entities involved in the proliferation of weapons of mass destruction and its financing. The relevant information and full lists of persons designated by the UNSC can be found at the UNSC's website[20].

I-1-3 MAS has given effect to relevant UNSCRs, including those as listed in the FATF Recommendations (2012) to be relevant to combating proliferation financing by issuing the FSM Sanctions Regulations. Examples of such Regulations are the Financial Services and Markets (Sanctions and Freezing of Assets of Persons – Iran) Regulations 2023 and the Financial Services and Markets (Sanctions and Freezing of Assets of Persons – Democratic People's Republic of Korea) Regulations 2023.

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.

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 UNSC sanctions lists as they are updated from time to time. A payment service provider should have in place policies, procedures and controls to continuously monitor the lists and take necessary follow-up action within a reasonable period of time, as required under the applicable laws and regulations.

I-2-2 The payment service provider's CDD policies and procedures should have clear processes on the identification of the customer's beneficial owners, and the

[20] Please see: https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list

forming of a good understanding of the customer's business and transactions from the 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 the FSM Sanctions 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 FSM Sanctions Regulations 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 apply to all digital payment tokens. The payment service provider should also report the freeze to MAS and file an STR as soon as possible, no later than 1 business day after suspicion was first established[21].

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, attempted 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;

[21] This refers to the point in time when the payment service provider concludes that the filing of an STR is warranted, based on available information, the circumstances and its investigations.

(c) the transaction involves designated persons;

(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 characteristics) 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-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 Useful Links

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

……

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

	• 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 • 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 payment service provider
Clubs, Societies and Charities	• Full name of entity • Business address or principal place of business

	• 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
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 or its equivalent • Names of the trust relevant parties • Declaration of trusts or its equivalent • 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[22].

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 the 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 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.

[22] The website address as at 30 June 2025: https://www.police.gov.sg/Advisories/Crime/Commercial-Crimes/Suspicious-Transaction-Reporting-Office

iv) 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 shows virtually no normal personal or business related activities but is used to received or disburse unusually large sums which have no obvious purpose or relationship to the customer or his business.

v) A customer who appears to have accounts with several payment service providers in the same locality, especially when the payment service provider is aware of a regular consolidated process from such accounts prior to a request for onward transmission of the funds elsewhere.

vi) Large amount of e-money being topped up into an account, which is inconsistent with the salary of the customer.

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

viii) Conceal or disguise significant transactions to avoid disclosure for record purpose by executing frequent or several transactions such that each transaction by itself is below CDD thresholds. For example, carrying out several transactions, either in a single day or over a period of days, by breaking them into smaller amounts in order to avoid the mandatory threshold customer identification requirements.

ix) "U-turn" transactions, i.e. where moneys received from a person or company in a foreign jurisdiction are transferred to another person or company in the same foreign jurisdiction, or to the sender's account in another jurisdiction.

x) Unnecessary routing of funds through multiple intermediary payment service providers, financial institutions or persons.

xi) Substantial increase(s) in the number of transactions/ frequency/ amounts by a customer without apparent cause, especially if fund transfers are made to a destination/ person not normally associated with the customer.

xii) Substantial increase in e-money top-ups by a customer without apparent cause, especially if such top-ups are subsequently transferred within a short period out of the account or to a destination not normally associated with the customer

xiii) Concentration of payments where multiple senders transfer moneys to a single individual's account.

xiv) Transactions which lack an apparent relationship between the sender and beneficiary, and/or personal money transfers sent to countries or jurisdictions that have no apparent family or business link to customer,

and/or the customer has no relation to country where he/she sends/receives the money and cannot sufficiently explain why money is sent there/received from there.

xv) Building up large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

B-3 Transactions Involving Large Amounts of Cash

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

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

iii) Customers transferring large amounts of money to persons outside Singapore with instructions for payment in cash.

iv) Exchanging an unusually large amount of small-denominated notes for those of higher denomination in a different currency.

v) 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.

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

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

viii) Large and regular payments 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.

ix) Cash payments transferred to a single person by a large number of different persons without an adequate explanation.

x) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received and unexpected large credit from aboard.

xi) A large amount of funds is withdrawn and immediately deposited into another account.

B-4 Transactions Involving Accounts of the Customer with the Payment Service Provider

i) High velocity of funds through an account, i.e. low beginning and ending daily balances, which do not reflect the large volume of funds flowing through an account.

ii) Transfers of funds from a company's account to an individual account of an employee or persons related to the employee and vice-versa.

iii) Transfers of funds from various third parties into an account, which is inconsistent with the nature of the customer's business.

iv) Multiple users using a single account.

v) An account operated in the name of an offshore company with structured movement of funds.

B-5 Transactions Involving Unidentified Parties

i) Transfer of money to another payment service provider without indication of the beneficiary.

ii) Use of pseudonyms or numbered accounts for effecting commercial transactions by enterprises active in trade and industry.

iii) Holding in trust of shares in an unlisted company whose activities cannot be ascertained by the payment service provider.

iv) Customers who wish to maintain a number of trustee or customers' accounts that do not appear consistent with their type of business, including transactions that involve nominee names.

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 transfers that originate from or are being made to a beneficiary in a country or jurisdiction that presents higher risk of tax evasion.

v) Purchase or sale of large amounts of precious metals by a customer which is not in line with his business or background.

vi) Participation in a Tax Amnesty Programme ("TAP")[23]

B-5 Trade-based Related Transactions

i) The commodity is shipped to (or from) a country or jurisdiction designated as "higher risk" for ML/TF activities.

ii) The type of commodity shipped is designated as "higher risk" for ML/TF activities[24].

iii) Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice.

iv) Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped.

v) Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.

vi) The size of the shipment appears inconsistent with the scale of the exporter or importer's regular business activities.

vii) The type of commodity shipped appears inconsistent with the exporter or importer's regular business activities.

viii) The method of payment appears inconsistent with the risk characteristics of the transaction[25].

---

[23] If a customer participates in a TAP, a payment service provider should:
(i) file an STR, indicating that the customer has participated in a TAP and which account(s) has been declared under the TAP;
(ii) adopt a risk-based approach to determine whether to conduct a review of the customer's account(s) and if so, how to prioritise this review;
(iii) where a review raises grounds for suspicion, file a further STR with the findings of the account(s) review.
The payment service provider should encourage customers to use the opportunity accorded by a TAP to ensure that their tax affairs are in order or regularised.

[24] For example, high-value, low-volume goods (e.g. consumer electronics), which have high turnover rates and present valuation difficulties.

[25] For example, the use of an advance payment for a shipment from a new supplier in a high-risk country.

[14] For example, the use of a forty-foot container to transport a small amount of relatively low-value goods.

ix) The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction.

x) The transaction involves the use of repeatedly amended or frequently extended letters of credit.

xi) The transaction involves the use of front (or shell) companies.

xii) The commodity is transhipped through one or more countries or jurisdictions for no apparent economic reason.

xiii) The shipment does not make economic sense[14].

B-6 Other Types of Transactions

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

ii) 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.

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

iv) 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.

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

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

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

viii) 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.

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

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

xi) The customer uses intermediaries which are not subject to adequate AML/CFT laws.

xii) 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.

xiii) No or limited information about the origin of funds.

xiv) Funds 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.

xv) 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).

xvi) Fund transfers made to high-risk countries or jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings.

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

B-7 Customer Behaviour

i) Customer is accompanied by others who keep a low profile or stay just outside the premise. Customer appears to be in doubt when asked for further details.

ii) Customer is in a hurry to complete the transaction, with promises to provide the supporting information later.

iii) Customer shows no interest in costs and/or is happy with a poor rate.

iv) Two or more customers appear to be trying to avoid reporting requirements and seem to be working together to break one transaction into two or more transactions.

v) The customer only seems to know the amount to be transferred after the payment service provider has counted the customer's moneys.

vi) The customer buys currency that does not fit with what is known about the customer's destination or the customer buys currency from an unusual location in comparison to his/her own location.