Monetary Authority of Singapore

GUIDELINES TO MAS NOTICE 626 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

28 MARCH 2024

TABLE OF CONTENTS

1	Introduction	1
2	Notice Paragraph 2 – Definitions, Clarifications and Examples	5
4	Notice Paragraph 4 – Assessing Risks and Applying a Risk-Based Approach	8
5	Notice Paragraph 5 – New Products, Practices and Technologies	13
6	Notice Paragraph 6 – Customer Due Diligence	14
7	Notice Paragraph 7 – Simplified Customer Due Diligence	28
8	Notice Paragraph 8 – Enhanced Customer Due Diligence	30
9	Notice Paragraph 9 – Reliance on Third Parties	36
10	Notice Paragraph 10 – Correspondent Banking and Similar Services	38
11	Notice Paragraph 11 – Wire Transfers	40
14	Notice Paragraph 14 – Suspicious Transactions Reporting	42
15	Notice Paragraph 15 – Internal Policies, Compliance, Audit and Training	44
I	Other Key Topics - Guidance to Banks on Proliferation Financing	48
II	Useful Links	50
APPENDIX A – Examples of CDD Information for Customers (Including Legal Persons/Arrangements)		51

For ease of reference, the chapter numbers in these Guidelines mirror the corresponding paragraph numbers in the MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism - Banks (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.

1 Introduction

1-1 These Guidelines provide guidance to all banks on the requirements in MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism – Banks ("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 purposes of these Guidelines, a reference to "CDD measures" shall mean the measures as required by paragraphs 6, 7 and 8 of the Notice.

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

1-4 Key Concepts

Money Laundering

1-4-1 Money laundering ("ML") is a process intended to mask the benefits derived from criminal conduct so that they appear to have originated from a legitimate source. Singapore's primary legislation to combat ML is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992. A bank should refer to the Commercial Affairs Department's ("CAD") website for more information.

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

(a) <u>Placement</u> – The physical or financial disposal of the benefits derived from criminal conduct.

(b) <u>Layering</u> – 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) <u>Integration</u> – The provision of apparent legitimacy to the benefits derived from criminal conduct. If the layering process succeeds, the integration schemes 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. Banks are reminded of the definitions of terrorism set out in the Terrorism (Suppression of Financing) Act 2002 ("TSOFA") and the United Nations (Anti-terrorism Measures) Regulations (Rg. 1).

1-4-4 Terrorists require funds to carry out acts of terrorism, and terrorism financing ("TF") is the act of providing these funds. Such funds may be derived from criminal activities such as robbery, drug-trafficking, kidnapping, extortion, fraud or hacking of online accounts. In such cases, there may be an element of ML involved to disguise the source of funds.

1-4-5 However, terrorist acts and organisations may also be financed 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 banks should remain vigilant.

1-4-6 Singapore's primary legislation to combat TF is the TSOFA. Banks may refer to the Inter-Ministry Committee on Terrorist Designation's ("IMC-TD") website for more information.

The Three Lines of Defence

1-4-7 Each bank 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.

1-4-8 A bank's board of directors and senior management are responsible for ensuring strong governance and sound AML/CFT risk management and controls at the bank. While certain responsibilities can be delegated to senior AML/CFT employees, final accountability rests with the bank's board of directors and senior management. A bank 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 set a clear risk appetite and ensure a compliance culture where financial crime is not acceptable.

1-4-9 Business units (e.g. front office, customer-facing functions) 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 bank's internal audit function.

1-4-10 As part of the first line of defence, business units require robust controls to detect illicit activities. They should be allocated sufficient resources to perform this function effectively. The bank's policies, procedures and controls on AML/CFT should be clearly specified in writing, and communicated to all relevant employees and officers in the business units. The bank should adequately train employees and officers to be aware of their obligations, and provide instructions as well as guidance on how to ensure the bank's compliance with prevailing AML/CFT laws, regulations and notices.

1-4-11 As the core of the second line of defence, the AML/CFT compliance function is responsible for ongoing monitoring of the bank's fulfilment of all AML/CFT duties by the bank. This implies sample testing and the review of exception reports. The AML/CFT compliance function should alert the bank's senior management or the board of directors if it believes that the employees or officers in the line departments 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 bank 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.

1-4-12 As the third line of defence, the bank's internal audit function or an equivalent function plays an important role in independently evaluating the AML/CFT risk management framework and controls for purposes of reporting to the audit committee of the bank'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 bank's compliance with prevailing AML/CFT policies, procedures and controls. A bank should establish policies for periodic AML/CFT internal audits covering areas such as —

(a) the adequacy of the bank'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 bank's employees and officers in implementing the bank'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 bank's training of relevant employees and officers.

Governance

1-4-13 Strong board and senior management leadership is indispensable in the oversight of the development and implementation of a sound AML/CFT risk management framework across the bank. The board of directors and senior management should ensure that the bank'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 bank's employees and officers having a good understanding of the ML/TF risks inherent in the bank's business.

1-4-14 A bank's board of directors and senior management should understand the ML/TF risks the bank is exposed to and how the bank's AML/CFT control framework operates to mitigate those risks. This should involve the board and senior management —

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

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

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

(d) ensuring that processes are in place to escalate important decisions that directly impact the ability of the bank 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 parties" includes foreign partnerships. The term "manager" as it appears in limb (b) of the definition of "connected parties" 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.

Customer

2-3 When performing Customer Due Diligence ("CDD") measures in the scenarios below, the following approaches may be adopted:

(a) Portfolio Managers

A bank may encounter cases where, to its knowledge, the customer is a manager of a portfolio of assets and who is operating the account in that capacity. In such cases, the underlying investors of the portfolio shall be beneficial owners within the meaning of the Notice.

However, the Authority recognises that a bank may not be able to perform CDD measures on the underlying investors. For instance, the portfolio manager may be reluctant, for commercial reasons, to reveal information on the underlying investors to the bank. In such circumstances, the bank should evaluate the risks arising from each case and determine the appropriate CDD measures to take. The bank may consider whether simplified CDD ("SCDD") measures could be applied to underlying investors under paragraph 7 of the Notice. However, where the customer falls within paragraph 6.16 of the Notice, the bank is exempted from making inquiries about the existence of such underlying investors (i.e. beneficial owners). Therefore, the bank does not need to identify and verify such underlying investors.

(b) Credit or Charge Card Customers

Where a bank issues a credit card or a charge card as defined in section 56 of the Banking Act 1970, or a particular type of credit card or charge card defined in regulation 2 of the Banking (Credit Card and Charge Card) Regulations 2013 (such as a business card, business card with no personal liability, corporate card, guarantee card, corporate card with no personal liability, corporate purchasing card, guaranteed credit card or guaranteed charge card), the following are customers for the purposes of the Notice:

(i) the principal credit card or charge card holder;

(ii) any supplementary credit card or charge card holder;
(iii) any employee to whom the business card is issued;
(iv) the sole proprietor or partnership which bears liability for the business card issued;
(v) any employee or officer of a body corporate to whom the corporate card is issued, and the body corporate; and
(vi) the guarantor of any guaranteed credit card or guaranteed charge card.

A merchant for whom the bank opens or maintains an account (including a ledger account) for the purchase of goods by, or provision of services to, any person from the merchant, using any credit card or charge card, should be considered a customer for the purposes of the Notice.

(c) Location of Relationship Management
Given the globalised nature of modern banking, it may often be the case that a bank's relationship and transactions with a particular customer is managed by a bank employee or officer based in one country or jurisdiction but the account itself is held with an office in another country or jurisdiction for bookkeeping purposes. The Authority will generally look at the substance of the relationship management as a whole. A bank should perform the applicable CDD measures if in substance, the relationship or account is managed by an employee or officer of the bank in Singapore even though the account is booked in another country or jurisdiction. However, the bank may rely on the CDD measures carried out by its related entity (or in the case of a branch network, another branch of the bank) in accordance with paragraph 9 of the Notice.

Financial Advice

2-4 The bank need not perform the CDD measures where the bank solely prospects natural persons, legal persons or legal arrangements, without the provision of financial advice.

Legal Arrangements

2-5 In relation to the definition of "legal arrangement" in the Notice, examples of legal arrangements are trust, fiducie, treuhand and fideicomiso.

Legal Persons

2-6 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

2-7 A reference to "officer" refers to a bank's board of directors and senior management.

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

Countries or Jurisdictions of its Customers

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

Other Relevant Authorities in Singapore

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

Risk Assessment

4-3 In addition to assessing the ML/TF risks presented by an individual customer, a bank shall identify and assess ML/TF risks on an enterprise-wide level. This shall include a consolidated assessment of the bank'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 bank in Singapore in the following ways:

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

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

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

4-5 A bank's senior management shall approve its enterprise-wide ML/TF risk assessment and relevant business units should give their full support and active co-operation to the enterprise-wide ML/TF risk assessment.

4-6 In conducting an enterprise-wide risk assessment, the broad ML/TF risk factors that the bank 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 or in, or where the bank has operations in —

(i) countries or jurisdictions the bank is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its customers (including the bank's network of correspondent banking relationships), 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:

- evidence of adverse news or relevant public criticism of a country or jurisdiction, including FATF public documents on High Risk and Noncooperative 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 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 bank —

(i) the nature, scale, diversity and complexity of the bank's business activities;

(ii) the nature of products and services offered by the bank; and

(iii) the delivery channels, including the extent to which the bank deals directly with the customer, relies on third parties to perform CDD measures or uses technology.

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

4-8 As far as possible, a bank's enterprise-wide ML/TF risk assessment should entail both qualitative and quantitative analyses to ensure that the bank accurately understands its exposure to ML/TF risks. A quantitative analysis of the bank's exposure to ML/TF risks should involve evaluating data on the bank's activities using the applicable broad risk factors set out in paragraph 4-6.

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

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

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

4-11 A bank should incorporate the results of Singapore's NRA Report into its enterprise-wide ML/TF risk assessment process. When performing the enterprise-wide risk assessment, a bank should take into account any financial or non-financial sector that has been identified as presenting higher ML/TF risks. A bank should consider the NRA results and its enterprise-wide ML/TF risk assessment results when assessing the ML/TF risks presented by customers from specific sectors.

4-12 The NRA also identifies certain prevailing crime types as presenting higher ML/TF risks. A bank 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 bank should also take these results into account as part of the bank's ongoing monitoring of the conduct of customers' accounts and the bank's scrutiny of customers' transactions.

Risk Mitigation

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

4-14 A bank's enterprise-wide ML/TF risk assessment serves to guide the allocation of AML/CFT resources within the bank.

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

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

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

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

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

(e) the coordination between AML/CFT compliance and other functions of the bank;

(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 bank's senior management;

(h) the coordination between the bank and regulatory or law enforcement agencies; and

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

Documentation

4-16 The documentation should include —

(a) the enterprise-wide ML/TF risk assessment by the bank;

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

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

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

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

Frequency of Review

4-18 To keep its enterprise-wide risk assessments up-to-date, a bank 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 bank. The results of these reviews should be documented and approved by senior management even if there are no significant changes to the bank's enterprise-wide risk assessment.

5 Notice Paragraph 5 – New Products, Practices and Technologies

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

5-2 A bank's assessment of ML/TF risks in relation to new products, practices and technologies is separate from, and in addition to, the bank's assessment of other risks such as credit risks, operational risks or market risks. For example, in the assessment of ML/TF risks, a bank 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 and heads of business, risk and compliance.

5-3 An example of a "new delivery mechanism" as set out in paragraph 5 of the Notice is mobile banking.

6 Notice Paragraph 6 – Customer Due Diligence

Notice Paragraph 6.2

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

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

Notice Paragraphs 6.3 to 6.4

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

6-2-1 Paragraph 6.4 of the Notice is applicable to a bank when it undertakes transactions for customers who or which have not established business relations with the bank.

6-2-2 A bank should monitor whether the related or linked transactions exceed the thresholds set out in paragraph 6.3(b) or paragraph 6.3(c) of the Notice and should take these into consideration when formulating scenarios and parameters.

6-2-3 Two or more transactions may be related or linked if they involve the same sender or recipient. A bank 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 in relation to the circumstances set out in paragraphs 6.3(b) or (c).

Notice Paragraphs 6.5 to 6.18

6-3 CDD Measures under Paragraphs 6.5 to 6.18

6-3-1 When relying on documents, a bank 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.

6-3-2 A bank should exercise greater caution when dealing with an unfamiliar or a new customer. Apart from obtaining the identification information required by paragraph 6.6 of the Notice, a bank 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, other related accounts with the same bank and whether the customer holds or has held a prominent public function. Such additional identification information enables a bank to obtain better knowledge of its customer's risk profile, as well as the purpose and intended nature of the account.

Notice Paragraph 6.6

6-4 Identification of Customer

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

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

Notice Paragraph 6.8

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

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

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

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

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

Notice Paragraph 6.9

6-6 Verification of Identity of Customer

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

6-6-2 In verifying the identity of a customer, a bank 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 telephone bill, bank statement or correspondence from a government agency;

(b) Legal Persons or Legal Arrangements —

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

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

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

6-6-4 In exceptional circumstances where the bank is unable to retain a copy of the documentation used to verify the customer's identity, the bank 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 bank'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 bank's employee or officer who carried out the verification, a statement by that employee or officer certifying verification of the information against the documentation and the date of the verification.

Reliability of Information and Documentation

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

6-6-6 Where the customer is unable to produce an original document, a bank 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 bank staff independent of the customer relationship has confirmed that he has sighted the original document.

6-6-7 Where a document is in a foreign language, appropriate steps should be taken by a bank to be reasonably satisfied that the document does in fact provide evidence of the customer's identity. The bank 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 bank may rely on a translation of such document by a bank staff independent of the customer relationship who is conversant in that foreign language. This is to allow all employees and officers of the bank involved in the performance of any measures required under the Notice to understand the contents of the documents, for effective determination and evaluation of ML/TF risks associated with the customer.

6-6-8 The bank 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, particularly in situations where business relations are established without face-to-face contact.

Notice Paragraphs 6.10 to 6.12

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

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

6-7-2 Where there is a long list of natural persons appointed to act on behalf of the customer (e.g. a list comprising more than 10 authorised signatories), the bank should verify at a minimum those natural persons to whom the customer has assigned the authority to operate the customer's account with the bank or move the funds in and out of that account.

Notice Paragraphs 6.13 to 6.17

6-8 Identification and Verification of Identity of Beneficial Owner

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

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

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

6-8-4 A bank 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 bank remains responsible for complying with its obligations under the Notice to take reasonable measures to verify the identity of the beneficial owner by, for example, researching publicly available information on the beneficial owner or arranging a face-to-face meeting with the beneficial owner, to corroborate the undertaking or declaration provided by the customer.

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

6-8-6 A bank should take particular care when dealing with companies with bearer shares, since the beneficial ownership is difficult to establish. For such companies, a bank should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the bank is notified whenever there is a change of beneficial owner of such shares. At a minimum, these procedures should require the bank to obtain an undertaking in writing from the beneficial owner of such bearer shares stating that the bank 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 bank may require that the bearer shares be held by a named custodian, with an undertaking from the custodian that the bank will be notified of any changes to ownership of these shares or the named custodian.

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

6-8-8 In determining if the foreign stock exchange imposes regulatory disclosure and adequate transparency requirements, the bank should put in place an internal assessment process with clear criteria, taking into account, amongst others, the country risk and the level of the country's compliance with the FATF standards.

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

6-8-10 *Deleted with effect from 30 November 2015.*

6-8-11 *Deleted with effect from 30 November 2015.*

6-8-12 Where a customer is one which falls within paragraph 6.16 of the Notice, this does not in itself constitute an adequate analysis of low ML/TF risks for the purpose of performing SCDD measures under paragraph 7 of the Notice.

Notice Paragraph 6.18

6-9 Information on Purpose and Intended Nature of Business Relations

6-9-1 The measures taken by a bank to understand the purpose and intended nature of business relations should be commensurate with the complexity of the customer's business and risk profile. For higher risk customers, a bank should seek to understand upfront the expected account activity (e.g. types of transactions likely to pass through, expected amount for each transaction, names of counterparties) and consider, as part of ongoing monitoring, whether the activity corresponds with the stated purpose of the accounts. This will enable a more effective ongoing monitoring of the customer's business relations and transactions.

Notice Paragraphs 6.19 to 6.26

6-10 Ongoing Monitoring

6-10-1 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 bank 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 bank to adjust the level of monitoring should be reviewed regularly for effectiveness in mitigating the bank's ML/TF risks.

6-10-2 A bank should make further enquiries when a customer performs frequent and cumulatively large transactions without any apparent or visible economic or lawful purpose. For example, frequent transfers of funds to the same recipient over a short period of time, multiple deposits of cash such that the amount of each deposit is not substantial, but the total of which is substantial.

6-10-3 Where there are indications that the risks associated with an existing business relations may have increased, the bank should request additional information and conduct a review of the customer's risk profile in order to determine if additional measures are necessary.

6-10-4 A key part of ongoing monitoring includes maintaining relevant and up-to-date CDD data, documents and information so that the bank can identify changes to the customer's risk profile —

(a) for higher risk categories of customers, a bank 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 as deemed necessary by the bank, whichever is earlier; and

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

6-10-5 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 bank's policies, procedures or standards relating to the documentation of CDD information change substantially, and (iv) the bank becomes aware that it lacks sufficient information about the customer concerned.

6-10-6 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 bank has previously obtained remain relevant and up-to-date.

6-10-7 In determining what would constitute suspicious, complex, unusually large or unusual pattern of transactions, a bank 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 bank 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).

6-10-8 A bank'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 bank's operations.

6-10-9 Nevertheless, the processes and systems used by the bank should provide its business units (e.g. front office and relationship managers) and compliance officers (including employees and officers who are tasked with conducting investigations) with timely information needed to identify, analyse and effectively monitor customer accounts for ML/TF.

6-10-10 The transaction monitoring processes and systems should enable the bank to monitor multiple accounts of a customer holistically within a business unit and across business units to identify any suspicious transactions. In the event that a business unit discovers suspicious transactions in a customer's account, such information should be shared across their business units (e.g. Private Banking and Retail Banking business units) to facilitate a holistic assessment of the ML/TF risks presented by the customer. Therefore, banks should have processes in place to share such information across business units. In addition, banks should perform trend analyses of transactions to identify unusual or suspicious transactions. Banks should also monitor transactions with parties in high risk countries or jurisdictions.

6-10-11 In addition, banks should have processes in place to monitor related customer accounts holistically within and across business units, so as to better understand the risks associated with such customer groups, identify potential ML/TF risks and report suspicious transactions.

6-10-12 The parameters and thresholds used by a bank to identify suspicious transactions should be properly documented and independently validated to ensure that they are appropriate to its operations and context. A bank should periodically review the appropriateness of the parameters and thresholds used in the monitoring process.

Notice Paragraphs 6.27 to 6.29

6-11 CDD Measures for Non-Face-to-Face Business Relations

6-11-1 A reference to “specific risks” in paragraph 6.27 of the Notice includes risks arising from establishing business relations and undertaking transactions according to instructions conveyed by customers over the internet, post, fax or telephone. A bank should note that applications and transactions undertaken across the internet may pose greater risks than other non-face-to-face business due to the following factors:

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

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

(c) the absence of physical documents; and

(d) the speed of electronic transactions,

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

6-11-2 The measures taken by a bank for verification of an identity in respect of nonface-to-face business relations with or transactions for the customer will depend on the nature and characteristics of the product or service provided and the customer’s risk profile.

6-11-3 Where verification of identity is performed without face-to-face contact (e.g. electronically), a bank should apply additional checks to manage the risk of impersonation. The additional checks may consist of robust anti-fraud checks that the bank routinely undertakes as part of its existing procedures, which may include —

(a) telephone contact with the customer at a 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, telephone 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 from another bank, where applicable;

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

(f) requiring the customer to make an initial deposit into the account with the bank from funds held by the customer in an account with another bank in Singapore.

Notice Paragraph 6.30

6-12 Reliance by Acquiring Bank on Measures Already Performed

6-12-1 When a bank acquires the business of another financial institution ("FI"), either in whole or in part, it is not necessary for the identity of all existing customers to be verified again, provided that the requirements of paragraph 6.30 of the Notice are met. A bank shall maintain proper records of its due diligence review performed on the acquired business.

6-12-2 Notwithstanding the reliance on identification and verification that has already been performed, an acquiring bank is responsible for its obligations under the Notice.

6-12-3 When a bank acquires the business of another FI, either in whole or in part, the bank is reminded that in addition to complying with paragraph 6.30 of the Notice, it is also required to comply with ongoing monitoring requirements set out in paragraphs 6.19 to 6.26 of the Notice.

Notice Paragraphs 6.32 to 6.34

6-13 Timing for Verification

6-13-1 With reference to paragraph 6.33 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 bank could effectively manage the ML/TF risks arising from the deferral of completion of verification is to put in place appropriate limits on the financial services available to the customer (e.g. limits on the number, type and value of transactions that can be effected) and institute closer monitoring procedures, until the verification has been completed.

6-13-2 With reference to paragraph 6.34 of the Notice —

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

(b) the bank 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 bank should terminate business relations with the customer if such verification remains uncompleted 120 business days after the establishment of business relations; and

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

Notice Paragraph 6.38

6-14 Existing Customers

6-14-1 In relation to customer accounts which pre-date the coming into force of the current Notice, the bank should prioritise the remediation of higher risk customers.

6-14-2 In taking into account any previous measures as referred to in paragraph 6.38 of the Notice, a bank 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 are 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 bank.

<u>Notice Paragraphs 6.39 to 6.42</u>

6-15 <u>Screening</u>

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

6-15-2 Where screening results in a positive hit against sanctions lists, a bank 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 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[2] ("FSM Sanctions Regulations"). Any such assets should be reported promptly to the relevant authorities and a Suspicious Transaction Report ("STR") should be filed.

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

(a) the ML/TF information sources used by the bank for screening (including commercial databases used to identify adverse information on individuals and entities, individuals and entities covered under the FSM Sanctions Regulations, individuals and entities identified by other sources such as the bank'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 bank's employees 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;

[2] Including 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 relevant Financial Services and Markets Regulations: https://mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/regulations-for-targeted-financial-sanctions

(e) how apparent matches from screening are to be resolved by the bank's employees, 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 bank's employees for reporting positive hits to the bank's senior management and to the relevant authorities.

6-15-4 The level of automation used in the screening process should take into account the nature, size and risk profile of a bank's business. A bank 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 bank 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 bank's employees will need to have access to CDD information to enable them to exercise their judgment in identifying true hits.

6-15-5 A bank should be aware that performing screening after business relations have been established could lead to a breach of relevant laws and regulations in Singapore relating to sanctioned parties. When the bank becomes aware of such breaches, it should immediately take the necessary actions and inform the relevant authorities.

6-15-6 In screening periodically as required by paragraph 6.40(d) of the Notice, a bank should pay particular attention to changes in customer status (e.g. whether the customer has over time become subject to prohibitions and sanctions) or customer risks (e.g. a connected party of a customer, a beneficial owner of the customer or a natural person appointed to act on behalf of the customer subsequently becomes a Politically Exposed Person or presents higher ML/TF risks, or a customer subsequently becomes a Politically Exposed Person or presents higher ML/TF risks) and assess whether to subject the customer to the appropriate ML/TF risk mitigation measures (e.g. enhanced CDD measures).

6-15-7 A bank 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 bank's customer database for periodic name screening purposes. This will help the bank to promptly identify any existing customers who have subsequently become higher risk parties.

6-15-8 In determining the frequency of periodic name screening, a bank should consider its customers' risk profile.

6-15-9 The bank should ensure that it has adequate arrangements to perform screening of the bank'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 bank should implement "four-eye checks" on alerts from sanctions reviews before closing an alert, or conduct quality assurance checks on the closure of such alerts on a sample basis.

6-15-10 With reference to paragraph 6.41 of the Notice, transaction screening should take place on a real-time basis [i.e. the screening or filtering of relevant payment instructions (e.g. MT103, MT 202) should be carried out before the transaction is executed]. For intermediary institutions, identification information in the cover payments (e.g. MT202COV) should be screened.

7 Notice Paragraph 7 – Simplified Customer Due Diligence

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

7-2 Where a bank applies SCDD measures, it is still required to perform ongoing monitoring of business relations under the Notice.

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

7-4 Where a bank is satisfied that the risks of money laundering and terrorism financing are low, a bank 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 by inferring this from the type of transactions or business relations to be established, instead of collecting information as to the purpose and intended nature of business relations.

7-5 Subject to the requirement that a bank'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).

8 Notice Paragraph 8 – Enhanced Customer Due Diligence

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

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

(a) Customer risk

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

(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 is conducted under unusual circumstances (e.g. significant unexplained geographic distance between the bank and the customer);

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

(vi) cash-intensive businesses.

(b) Country or geographic risk

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

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

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

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

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

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

Notice Paragraph 8.1

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

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

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

8-4-3 When determining whether a person is a "close associate" of a PEP, the bank 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 bank may rely on information available from public sources and information obtained through customer interaction.

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

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

Notice Paragraphs 8.2 to 8.4

8-5 PEPs

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

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

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

8-5-4 In relation to paragraph 8.3(b) of the Notice, a bank 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 bank should note that not all declarations are publicly available. A bank should also be aware that certain jurisdictions impose restrictions on their PEPs' ability to hold foreign bank accounts, to hold other office or paid employment.

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

8-5-6 Source of funds refers to the origin of the particular funds or other assets which are the subject of the establishment of business relations (e.g. the amounts being invested, deposited, or wired as part of the business relations). In order to ensure that the funds are not proceeds of crime, the bank 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.

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

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

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

(b) using public sources of information (e.g. websites) to gain a better understanding of the reputation of the customer or any beneficial owner of a customer. Where the bank finds information containing allegations of wrongdoing by a customer or a beneficial owner of a customer, the bank should assess how this affects the level of risk associated with the business relations;

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

8-5-9 In relation to paragraphs 8.4(a) and (b) of the Notice, where the bank assesses that the business relations or transactions with 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 bank shall nevertheless apply measures under paragraph 6 of the Notice on the customer. However, where changes in events, circumstances or other factors lead to the bank’s assessment that the business relations or transactions with the customer present higher ML/TF risks, the bank should review its risk assessment and apply ECDD measures.

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

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

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

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

Notice Paragraphs 8.5 to 8.8

8-6 Other Higher Risk Categories

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

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

8-6-3 With reference to paragraph 8.6(a) of the Notice, a bank should refer to the FATF Public Statement on High Risk Jurisdictions subject to a Call for Action[3]. FATF updates this Public Statement on a periodic basis and banks should regularly refer to the FATF website for the latest updates[4].

8-6-4 For private banking business which inherently presents higher ML/TF risks, a bank should, regardless of the bank's internal risk classification of the customer, refer to the sound practices highlighted in the MAS Information Paper, "Guidance on Private Banking Controls"[5]. Such practices include ensuring that —

[3] 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

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

[5] https://www.mas.gov.sg/publications/monographs-or-information-paper/2014/guidance-on-private-banking-controls

(a) information obtained on the source of wealth of the customers and beneficial owners should be independently corroborated against documentary evidence or public information sources;

(b) parties screened should include operating companies and individual benefactors contributing to the customer's and beneficial owner's wealth or funds;

(c) the bank conducts periodic reviews of such customers; and

(d) where the bank is aware of customers having a common beneficial owner or a customer having multiple accounts with the bank, the bank should scrutinise transactions of these customer accounts holistically to better identify suspicious, complex, unusually large or unusual patterns of transactions, and perform periodic reviews on a consolidated basis.

8-6-5 For the purposes of paragraph 8.8 of the Notice, regulations issued by the Authority include the Regulations relating to the freezing of assets of persons and sanctioning of persons.

8-6-6 With regard to tax and other serious crimes, as a preventive measure, banks 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 customer relationship, banks should conduct enhanced monitoring and where appropriate, discontinue the relationship. If the bank is inclined to retain the customer, approval shall be obtained from senior management with the substantiating reasons properly documented, and the account subjected to close monitoring and commensurate risk mitigation measures. 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.

9 Notice Paragraph 9 – Reliance on Third Parties

9-1 Paragraph 9 does not apply to outsourcing. Third party reliance under paragraph 9 of the Notice is different from an outsourcing arrangement or agreement.

9-2 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 bank. The third party will therefore perform the CDD measures on the customer according to its own AML/CFT policies, procedures and controls.

9-3 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 bank, in accordance with the bank's AML/CFT policies, procedures and standards, and is subject to the bank's control measures to effectively implement the bank's AML/CFT procedures.

9-4 The bank may take a variety of measures, where applicable, to satisfy the requirements in paragraphs 9.2(a) and 9.2(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's 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.

9-5 The reference to "documents" in paragraph 9.2(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 bank 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 bank's business relations with the customer or the completion of transactions undertaken.

9-6 In a syndicated facility transaction, a participating bank may rely on the lead arranger's confirmation that the necessary CDD measures have been performed on the customer (i.e. borrower of the syndicated facility) to meet the Notice requirements, provided that the participating bank is satisfied that the requirements in paragraph 9.2 of the Notice are met. However, a participating bank should perform its own CDD measures on the customer in situations where its assessment of the customer's ML/TF risk leads to a higher risk classification than the lead arranger's assessment of the customer's ML/TF risks. Notwithstanding the reliance on CDD measures performed by the lead arranger, the participating bank remains responsible for its obligations under the Notice.

9-7 Paragraph 9.3 of the Notice prohibits the bank from relying on the third party to carry out ongoing monitoring. Paragraph 9.3 of the Notice should be read with the ongoing monitoring requirements in Part (VI) of paragraph 6 of the Notice.

9-8 For the avoidance of doubt, paragraph 9 of the Notice does not apply to the outsourcing of the ongoing monitoring process by a bank, including to its parent entity, branches and subsidiaries. A bank may outsource the first-level review of alerts from the transaction monitoring systems, or sanctions reviews, to another party. However, the bank remains responsible for complying with ongoing monitoring requirements under the Notice.

10 Notice Paragraph 10 – Correspondent Banking and Similar Services

10-1 Correspondent banks should note that the requirements under paragraph 10 of the Notice are in addition to performing measures set out under paragraphs 6, 7 and 8 of the Notice, as applicable.

10-2 A correspondent bank typically acts as a correspondent for many banks or FIs around the world. Respondent FIs may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

10-3 Correspondent banks should note that foreign exchange and money market transactions do not fall within the scope of "similar services" as referred to in paragraph 10.2 of the Notice.

10-4 After a correspondent bank obtains adequate information as required by paragraph 10.3(a) of the Notice to establish a correspondent banking relationship or the provision of similar services, such information should continue to be updated on a periodic basis thereafter.

10-5 Other factors that a correspondent bank should consider in complying with paragraph 10.3(a) of the Notice include —

(a) the business group to which the respondent 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 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 banking relationship[6]; the bank should review the risks posed by such "nested" relationships.

10-6 To assess the ML/TF risk associated with a particular country or jurisdiction as required by paragraph 10.3(a)(iii) of the Notice, a correspondent bank 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

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

strategic AML/CFT deficiencies, mutual evaluation reports by FSRBs, publicly available information from national authorities and any restrictive measures imposed on a country, particularly prohibitions on providing correspondent banking or other similar services.

10-7 For correspondent banking relationships established with a bank's related entities, the appropriate level of measures as required under paragraphs 6, 7 and 8 of the Notice (as applicable), and paragraph 10 of the Notice should be applied, bearing in mind that the risk profiles of individual entities within the same financial group could differ significantly. The bank should take into consideration the parent bank'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.

10-8 The CDD process should result in a thorough understanding of the ML/TF risks arising from a relationship with the respondent FI. It should not be treated as a "form-filling" exercise. A correspondent bank's assessment of the respondent FI may be enhanced through meetings with the respondent FI's management and compliance head, banking and AML/CFT regulators.

10-9 A correspondent bank may apply a risk-based approach in complying with the requirements set out in paragraph 10 of the Notice, but should be mindful that correspondent banking relationships generally present higher ML/TF risks.

10-10 If a correspondent bank provides correspondent banking or other similar services to its related respondent FIs within the same financial group, the correspondent bank should ensure that it still assesses the ML/TF risks presented by its related respondent FI.

10-11 Where the head office of the financial group is incorporated in Singapore, it should monitor the correspondent banking relationships between banks in its financial group, and ensure that adequate information sharing mechanisms within the financial group are in place.

10-12 For the purposes of paragraph 10 of the Notice, a correspondent bank should take into account, for example, any sanctions imposed by relevant authorities on a respondent FI for failing to have adequate controls against ML/TF activities.

10-13 In assessing whether a bank or FI falls within the meaning of "shell FI" for the purposes of paragraph 10 of the Notice, a correspondent bank 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.

11 Notice Paragraph 11 – Wire Transfers

11-1 Paragraph 11 of the Notice is not intended to cover any transfer that flows from a transaction carried out using a credit, charge, debit or prepaid card for the purchase of goods or services, so long as the credit, charge, debit or prepaid card number accompanies all transfers flowing from the transaction. However, paragraph 11 of the Notice applies when a credit, charge, debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, hence the necessary information should be included in the message for such transactions.

11-2 In relation to paragraph 11.7 of the Notice, examples of domestic wire transfers in Singapore include inter-bank transfers via the local MAS Electronic Payment System (“MEPS+”) system.

11-3 A bank 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.

11-4 A bank 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.

11-5 Where name screening checks confirm that the wire transfer originator or wire transfer beneficiary is a terrorist or terrorist entity, the requirement for the bank to block, reject or freeze assets of these terrorists or terrorist entities cannot be risk-based.

11-6 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.

11-7 Where a cross-border wire transfer, regardless of amount, is a cover payment (e.g. MT202COV payments), ordering institutions shall in accordance with the requirements of paragraph 11 of the Notice, ensure that the payment message of the cover payment sent to the intermediary institution contain information of the wire transfer originator and wire transfer beneficiary. The information included in the payment message of the cover payment shall be identical to that contained in the cross-border wire transfer message sent directly to the beneficiary institution.

11-8 An intermediary institution that receives and transmits a cover payment should ensure that the relevant fields for storing originator and beneficiary information in the payment message of the cover payment are duly completed. In addition, such intermediary institutions shall ensure that the wire transfer originator and wire transfer beneficiary information in the payment message of the cover payment is complete, in accordance with paragraph 11.15 of the Notice. The intermediary institution shall also screen the names of the wire transfer originator and wire transfer beneficiary in accordance with paragraph 6.41 of the Notice.

Notice Paragraphs 11.3 to 11.9

11-9 Responsibility of the Ordering Institution

11-9-1 For joint accounts, the ordering institution shall provide all of the joint account holders' information to the beneficiary institution in accordance with paragraph 6.37 of the Notice. If there are space constraints in the SWIFT message, the ordering institution may indicate in the wire transfer message that the originator information provided pertains to a joint account holder.

11-9-2 The ordering institution shall include wire transfers in its ongoing monitoring of the business relations with the customer, in accordance with paragraph 6 of the Notice.

Notice Paragraphs 11.10 to 11.12

11-10 Responsibility of the Beneficiary Institution

11-10-1 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 bank 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 bank 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.

14 Notice Paragraph 14 – Suspicious Transactions Reporting

14-1 A bank should ensure that the internal process for evaluating whether a matter should be referred to the Suspicious Transaction Reporting Office ("STRO") via an STR is completed without delay and should not exceed 15 business days of the case being referred by the relevant bank employee or officer, unless the circumstances are exceptional or extraordinary.

14-2 A bank should note that an STR filed with STRO would also meet the reporting obligations under the TSOFA.

14-3 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 the most 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 bank 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.

14-4 Once suspicion has been raised in relation to a customer or any transaction for that customer, in addition to reporting the suspicious activity, a bank should ensure that appropriate action is taken to adequately mitigate the risk of the bank being used for ML/TF activities. This may include strengthening its AML/CFT processes. This may also include a review of either the risk classification of the customer, or the business relations with the customer. Appropriate action should be taken, including escalating the issue to the appropriate decision making level, taking into account any other relevant factors, such as cooperation with law enforcement agencies.

14-5 STR reporting templates are available on CAD's website[7]. However, banks are strongly encouraged to use the online system provided by STRO to lodge STRs. In the event that the bank 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, the bank should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct.

14-6 A bank 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.

[7] The website address as at 28 March 2024: https://www.police.gov.sg/Advisories/Crime/Commercial-Crimes/Suspicious-Transaction-Reporting-Office

14-7 Banks are reminded to read paragraph 14.4 of the Notice together with paragraphs 6.35 and 6.36 of the Notice. Where a bank stops performing CDD measures as permitted under paragraph 14.4 and is, as a result, unable to complete CDD measures (as specified under paragraph 6.36), the bank is reminded that it shall not commence or continue business relations with that customer or undertake any transaction for that customer.

15 Notice Paragraph 15 – Internal Policies, Compliance, Audit and Training

15-1 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 bank 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 15.3 to 15.9

15-2 Group Policy

15-2-1 For the avoidance of doubt, Singapore branches of banks incorporated outside Singapore need not comply with paragraphs 15.3 to 15.9 of the Notice. Paragraphs 15.3 to 15.9 of the Notice are intended to be applied by a bank incorporated in Singapore to its branches and subsidiaries, but not to its parent entity and the bank’s other related corporations.

15-2-2 In relation to paragraph 15.6 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 bank, 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 bank incorporated in Singapore with the bank’s group level compliance, audit, and AML/CFT functions (whether in or outside Singapore), for risk management purposes.

Notice Paragraphs 15.10 to 15.11

15-3 Compliance

15-3-1 A bank should ensure that the AML/CFT compliance officer has the necessary seniority and authority within the bank to effectively perform his responsibilities.

15-3-2 The responsibilities of the AML/CFT compliance officer should include —

(a) carrying out, or overseeing the carrying out of, ongoing monitoring of business relations and sample review of accounts 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 bank'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 1-4-14 of the Guidelines), and any necessary remedial actions, arising from audit, inspection, and compliance reviews, to the bank's senior management, and in the case of locally incorporated banks, to the board of directors, at least annually and as and when needed.

15-3-3 The business interests of a bank 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 bank's management.

<u>Notice Paragraph 15.12</u>

15-4 <u>Audit</u>

15-4-1 A bank's AML/CFT framework should be subject to periodic audits (including sample testing). Such audits should be performed not just on individual business functions but also on a bank-wide basis. Auditors should assess the effectiveness of measures taken to prevent ML/TF. This would include, among others —

(a) determining the adequacy of the bank'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.

15-4-2 The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the bank's business.

Notice Paragraph 15.13

15-5 Employee Hiring

15-5-1 The screening procedures applied when a bank in Singapore hires employees and appoints officers should include —

(a) background checks with past employers;

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

(c) bankruptcy searches.

15-5-2 In addition, a bank should conduct credit history checks, on a risk-based approach, when hiring employees and appointing officers.

Notice Paragraph 15.14

15-6 Training

15-6-1 As stated in paragraph 15.14 of the Notice, it is a bank'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 bank 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.

15-6-2 Apart from the initial training, a bank 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 bank should maintain the training records for audit purposes.

15-6-3 A bank should monitor the effectiveness of the training provided to its employees. This may be achieved by —

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

(b) monitoring employees' compliance with the bank'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 who miss such training without reasonable cause.

I Other Key Topics - Guidance to Banks 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")[8]. These Regulations apply to all FIs (including banks) regulated by MAS and generally impose financial sanctions on designated persons.

I-1-2 Specifically, a UNSCR may designate certain individuals and entities involved in the proliferation of weapons of mass destruction and its financing. The relevant information and full listings of persons designated by UNSCRs can be found on the UN website[9].

I-1-3 MAS has given effect to UNSCRs as listed by 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 bank 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 bank should also ensure compliance with legal instruments issued by MAS relating to proliferation financing risks.

I-2 CDD and Internal Controls

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

I-2-2 A bank 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 —

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

[9] Please see: https://www.un.org/securitycouncil/content/un-sc-consolidated-list

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

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

I-2-3 A bank should have policies and procedures to prevent such attempts, and take appropriate measures against such employees and officers.

I-3 <u>Obligation of Bank to Freeze without Delay</u>

I-3-1 A bank 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 bank has in its possession, custody or control. The bank should also file an STR in such cases.

I-4 <u>Potential Indicators of Proliferation Financing</u>

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

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

(b) the customer's activity does not match its business profile or the end-user information does not match the end-user's business profile;

(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 indicators);

(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); or

(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).

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 bank may wish to refer to the FATF website for additional information.

II Useful Links

Financial Action Task Force ("FATF"): http://www.fatf-gafi.org/
Basel Committee on Banking Supervision - BIS: http://www.bis.org/bcbs/

…………………………

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 with the bank • 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 bank's visit to the customer's place of business, where the bank 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 with the bank • 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 bank's visit to the customer's place of business, where the bank 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)

Customer Type	Examples of CDD Information
Companies	• Full name of entity • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the bank • 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 bank's visit to the customer's place of business, where the bank 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 bank • 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, stateowned 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 the business relations with the bank • 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 bank's visit to the customer's place of business, where the bank assesses it as necessary • Board resolution authorising the opening of the customer's account with the bank

Customer Type	Examples of CDD Information
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 with the bank • 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 bank's visit to the customer's place of business, where the bank 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 bank • 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 bank's visit to the customer's place of business, where the bank assesses it as necessary • Information about the purpose and intended nature of business relations with the bank • Records in a relevant and independent registry in the country or jurisdiction of constitution • Country or jurisdiction of constitution • Trust deed • Names of the settlors/trustees/beneficiaries or any person who has power over the disposition of any property that is subject to the trust • Declaration of trusts • Deed of retirement and appointment of trustees (where applicable)

APPENDIX B – Examples of Suspicious Transactions

B-1 General Comments

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

B-1-2 The list is not exhaustive and may be updated due to changing circumstances and new methods of laundering money or financing terrorism. Banks are to refer to STRO's website for the latest list of red flags[10].

B-1-3 A customer's declarations regarding the background of such transactions should be checked for plausibility. Not every explanation offered by the customer can be accepted without scrutiny.

B-1-4 It is reasonable to suspect any customer who is reluctant to provide normal information and documents required routinely by the bank in the course of the business relations. Banks should pay attention to customers who provide minimal, false or misleading information, or when applying to open an account, provide information that is difficult or expensive for the bank to verify.

B-2 Transactions Which Do Not Make Economic Sense

i) Transactions that cannot be reconciled with the usual activities of the customer, for example —

(a) the use of Letters of Credit and other methods of trade finance to move money between countries or jurisdictions where such trade is not consistent with the customer's usual business;

(b) payment by unrelated third parties into a customer's credit card or charge card accounts via cash, cheques or debit cards;

(c) payment into a customer's credit card or charge card accounts received from different locations or accounts.

[10] The website address as at 28 March 2024: https://www.police.gov.sg/Advisories/Crime/Commercial-Crimes/Suspicious-Transaction-Reporting-Office

ii) A customer relationship with the bank where a customer has a large number of accounts with the same bank, and has frequent transfers between different accounts.

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

iv) Transactions which, 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 receive or disburse unusually large sums which have no obvious purpose or relationship to the customer or his business.

v) Large amounts of funds deposited into an account, which is inconsistent with the salary of the customer.

vi) Provision of bank guarantees or indemnities as collateral for loans between third parties that are not in conformity with market conditions.

vii) Unexpected repayment of an overdue credit without any plausible explanation.

viii) Unexpected repayment of credit facilities by a third party on behalf of the customer.

ix) Back-to-back loans without any identifiable and legally admissible purpose.

x) Cash deposited at one location is withdrawn at another location almost immediately.

xi) Customers running large positive credit card or charge card balances.

B-3 Transactions Involving Large Amounts of Cash

i) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity.

ii) Frequent withdrawal of large amounts by means of cheques, including traveller's cheques.

iii) Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their business.

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

v) A large amount of cash is withdrawn and immediately deposited into another account.

vi) Exchanging an unusually large amount of small-denominated notes for those of higher denomination.

vii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank.

viii) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company (e.g. cheques, letters of credit, bills of exchange).

ix) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the cumulative total of which is substantial.

x) The deposit of unusually large amounts of cash by a customer to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments.

xi) Large cash deposits using night safe facilities and cash deposit machines, thereby avoiding direct contact with the bank.

xii) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

xiii) Customers whose deposits contain counterfeit notes or forged instruments.

xiv) Customers who use cash advances from a credit card or charge card account to purchase money orders or bank drafts to transfer funds to foreign destinations.

xv) Customers who take cash advances from a credit card or charge card account to deposit into another account.

xvi) Large cash payments for outstanding credit card or charge card balances.

xvii) Customers who maintain positive balances on their credit card or charge card and then request cash advances or other type of refunds.

B-4 Transactions Involving Accounts of the Customer with the Bank

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) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using customer accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other customer company and trust accounts.

iii) Matching of payments out with credits paid in by cash on the same or previous day.

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

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

vi) Multiple depositors using a single account.

vii) Paying in large third party cheques endorsed in favour of the customer.

viii) Frequent deposits of a company’s cheques into an employee’s account.

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

B-5 Transactions Involving Transfers Abroad

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

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

iii) Transfer of a large amount of money abroad by a person who does not maintain an account with the bank and who fails to provide a legitimate reason when asked.

iv) Substantial increase in cash deposits by a customer without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account or to a destination not normally associated with the customer.

v) Repeated transfers of large amounts of money abroad accompanied by the instruction to pay the beneficiary in cash.

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

vii) Cash payments remitted to a single account by a large number of different persons without an adequate explanation.

viii) “U-turn” transactions, i.e. where funds received from a person or company in a foreign country or jurisdiction are immediately remitted to another person or company in the same country or foreign jurisdiction, or to the sender’s account in another country or jurisdiction.

B-6 Investment-Related Transactions

i) Purchasing of securities to be held by the bank in safe custody, where this does not appear appropriate given the customer’s apparent standing.

ii) Requests by a customer for investment management services where the source of funds is unclear or not consistent with the customer’s apparent standing.

iii) Larger or unusual settlements of securities transactions in cash form.

iv) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

v) Large transfers of securities to non-related accounts.

B-7 Merchants Acquired by a Bank for Credit Card or Charge Card Transactions

i) Principals of the merchant appear to be unfamiliar with, or lack a clear understanding of, the merchant’s business.

ii) Proposed transaction volume, refunds or charge-backs are inconsistent with information obtained from on-site visit or merchant/industry peer group.

iii) Unusual or excessive cash advances or credit refunds.

iv) Indications that a merchant's credit card or charge card terminal is being used by any third party.

B-8 Transactions Involving Unidentified Parties

i) Transfer of money to another bank without indication of the beneficiary.

ii) Payment orders with inaccurate information concerning the person placing the orders.

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

iv) Holding in trust of shares in an unlisted company whose activities cannot be ascertained by the bank.

v) Provision of collateral by way of pledge or guarantee without any discernible plausible reason by third parties unknown to the bank and who have no identifiable close relationship with the customer.

vi) 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-9 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 having accounts opened in Singapore.

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

iv) Inability to reasonably justify frequent and large wire transfers from or to a country or jurisdiction that presents higher risk of tax evasion.

v) Re-deposit or reinvestment of funds back into the original country or jurisdiction after being transferred to another country or jurisdiction, often a tax haven with poor track record on CDD or record keeping requirements.

vi) Accounts managed by external asset managers who may not be adequately regulated and supervised.

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

viii) Purchase of bank cheques on a large scale by a customer.

ix) Extensive or increased use of safe deposit facilities that do not appear to be justified by the background of the customer and for no apparent reason.

B-10 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[11].

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[12].

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.

---

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

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

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[13].

B-11 Other Types of Transactions

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

ii) The customer fails to reasonably justify the purpose of a transaction when queried by the bank.

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

iv) Frequent changes to the address or authorised signatories.

v) A large amount of funds is received and immediately used as collateral for banking facilities.

vi) When a young person (aged about 17-26) opens an account and either withdraws or transfers the funds within a short period, which could be an indication of terrorism financing.

vii) When a person receives funds from a religious or charitable organisation and utilises the funds for purchase of assets or transfers out the funds within a relatively short period.

viii) Customers requesting for a credit card or charge card to be sent to an international or domestic destination other than the customer's address or place of business.

ix) Indications of a credit card or charge card merchant refunding payments to any person without an underlying purchase of goods or services.

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

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

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