Monetary Authority of Singapore

GUIDELINES TO MAS NOTICE SFA04-N02 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

1July 2025

TABLE OF CONTENTS

For ease of reference, the chapter numbers in these Guidelines mirror the corresponding paragraph numbers in MAS Notice SFA04-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism – Capital Markets Intermediaries (e.g. Chapter 2 of the Guidelines provides guidance in relation to paragraph 2 of the Notice). Not every paragraph in the Notice has a corresponding paragraph in these Guidelines and this explains why not all chapter numbers are utilised in these Guidelines.

GUIDELINES TO MAS NOTICE SFA04-N02 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

1 Introduction

1-1 These Guidelines provide guidance to all holders of a capital markets services licence and all persons exempted under paragraph 7(1)(b) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations from having to hold a capital markets services licence (collectively "CMIs") on some of the requirements in MAS Notice SFA04-N02 on Prevention of Money Laundering and Countering the Financing Of Terrorism – Capital Markets Intermediaries ("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 CMI may have an impact on the Authority's overall risk assessment of the CMI, including the quality of its board and senior management oversight, governance, internal controls and risk management.

1-4 Key Concepts

Money Laundering[1]

1-4-1 Money laundering ("ML") is a process intended to mask the benefits derived from criminal conduct so that they appear to have originated from a legitimate source. Singapore's primary legislation to combat ML is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992. A CMI 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) Placement – The physical or financial disposal of the benefits derived from criminal conduct.

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

(c) Integration – The provision of apparent legitimacy to the benefits derived from criminal conduct. If the layering process succeeds, the integration schemes

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

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

1-4-3 As capital markets transactions are no longer predominantly cash-based, they are more likely to be used in the layering stage rather than placement stage of money laundering. However, where the transactions are in cash, there is still the risk of capital markets transactions being used at the placement stage.

1-4-4 Capital markets transactions offer a vast array of opportunities for transforming money into a diverse range of assets. The ease with which these assets can be converted to other types of assets, especially if they are liquid and marketable, also aids the layering process. Hence, capital markets transactions are particularly attractive to money-launderers for layering their illicit proceeds for eventual integration into the general economy.

Terrorism Financing

1-4-5 Acts of terrorism seek to influence or compel governments into a particular course of action or to intimidate the public or a section of the public. CMIs are reminded of the definitions of "terrorist" and "terrorist act" set out in the Terrorism (Suppression of Financing) Act 2002 ("TSOFA").

1-4-6 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.

1-4-7 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 CMIs should remain vigilant.

1-4-8 Singapore's primary legislation to combat TF is the TSOFA. CMIs may refer to the Inter-Ministry Committee on Terrorist Designation's ("IMC-TD") website for more information.

Proliferation Financing

1-4-8A Proliferation financing ("PF") refers to the raising, moving or making available of funds, other assets or other economic resources, or financing, in whole or in part, to individuals or entities for the purposes of the proliferation of weapons of mass destruction, including the proliferation of their means of delivery or related materials (including both dual-use technology and dual-use goods for non-legitimate purposes), under the relevant regulations issued under section 192 read with section 15(1)(b) of the Financial Services and Markets Act 2022 ("FSM Act")

relating to sanctions and freezing of assets of persons ("FSM Sanctions Regulations")[2].

The Three Lines of Defence

1-4-9 Each CMI 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.

1-4-10 A CMI's board of directors and senior management are responsible for ensuring strong governance and sound AML/CFT risk management and controls at the CMI. While certain responsibilities can be delegated to senior AML/CFT employees, final accountability rests with the CMI's board of directors and senior management. A CMI 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.

1-4-11 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 CMI's internal audit function.

1-4-12 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 CMI's policies, procedures and controls on AML/CFT should be clearly specified in writing, and communicated to all relevant employees, officers and representatives in the business units. The CMI should adequately train employees, officers and representatives to be aware of their obligations, and provide instructions as well as guidance on how to ensure the CMI's compliance with prevailing AML/CFT laws, regulations and notices.

1-4-13 As the core of the second line of defence, the AML/CFT compliance function is responsible for ongoing monitoring of the fulfilment of all AML/CFT duties by the CMI. This implies sample testing and the review of exception reports. The AML/CFT compliance function should alert the CMI'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

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

concerns. Other support functions such as operations, human resource or technology also play a role to help mitigate the ML/TF risks that the CMI 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.

1-4-14 As the third line of defence, the CMI'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 CMI'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 CMI's compliance with prevailing AML/CFT policies, procedures and controls. A CMI should establish policies for periodic AML/CFT internal audits covering areas such as —

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

Governance

1-4-15 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 CMI. The board of directors and senior management should ensure that the CMI'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 CMI's employees, officers and representatives having a good understanding of the ML/TF risks inherent in the CMI's business.

1-4-16 A CMI's board of directors and senior management should understand the ML/TF risks the CMI is exposed to and how the CMI's AML/CFT control framework operates to mitigate those risks. This should involve the board and senior management —

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

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

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

(d) ensuring that processes are in place to escalate important decisions that directly impact the ability of the CMI 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.

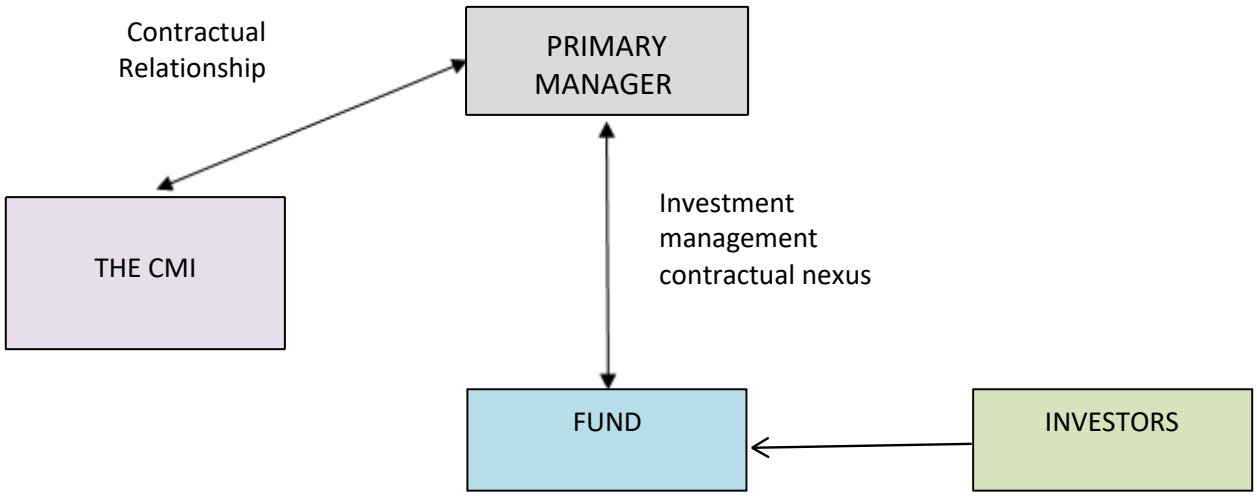
Customer

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

(a) Portfolio Managers

A CMI (for e.g. a securities broker or fund management company) may encounter cases where the customer is the primary manager of a fund (as set out in Scenario 1 below). In this case, the CMI may consider whether paragraph 6.16(c) and (d) of the Notice or simplified CDD ("SCDD") measures under paragraph 7 of the Notice may be applicable.

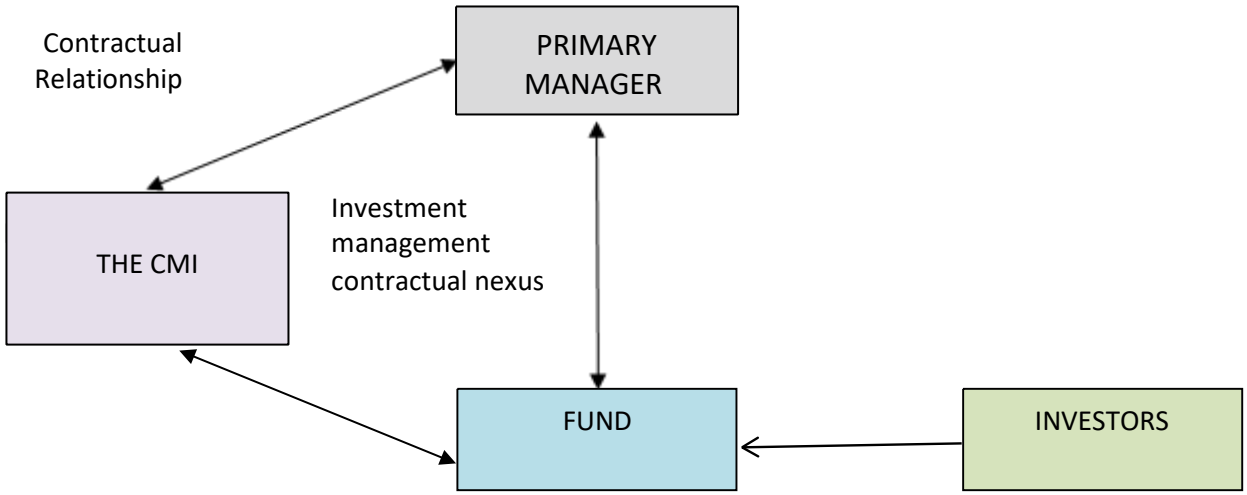
SCENARIO 1: CONTRACTUAL NEXUS WITH PRIMARY MANAGER



It could also encounter cases whereby the fund managed by the primary manager (who is not the CMI) may also be a customer of the CMI by virtue of a contractual nexus (as depicted in Scenario 2 below). In Scenario 2, the

underlying investors of the portfolio shall be the beneficial owners of the customer (i.e. the fund) within the meaning of the Notice.

SCENARIO 2: TRI-PARTITE CONTRACTUAL NEXUS



In Scenario 2, the Authority recognises that a CMI may not be able to perform CDD measures on the investors of the fund. For instance, the portfolio manager may be reluctant, for commercial reasons, to reveal information on the underlying investors to the CMI. In such circumstances, the CMI should evaluate the risks arising from each case and determine the appropriate CDD measures to take. If the fund meets one or more of the criteria in paragraph 6.16 of the Notice, the CMI may avail itself to the exemption from making inquiries about the existence of its investors. If these are not met, the CMI will have to apply appropriate CDD measures on the underlying investors. It may only apply SCDD measures on these investors if it is able to satisfy the requirements in section 7 of the Notice.

(b) Engagement of Distributors

Where the CMI has engaged distributors (for e.g. banks and financial advisors) to market their products such as funds, the end investors of the funds marketed by a distributor would be considered beneficial owners of the CMI's customers (i.e. the funds managed by the CMI). Under these arrangements, the CMI typically has no visibility of the underlying investors as the business relations are owned by the distributor and the distributor could be using omnibus accounts in its own name in order to engage in securities transactions on behalf of its clients. For legitimate business reasons, the distributor may also not be prepared to reveal the identity of the underlying investors.

Where the underlying investors of the funds are customers of a distributor that is a financial institution ("FI") supervised by the Authority or a foreign FI

incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with the standards set by the FATF, the CMI should obtain confirmation from the distributor that the latter would be responsible for carrying out AML/CFT checks on the underlying investors. The CMI may also consider whether SCDD measures under paragraph 7 of the Notice are applicable in relation to the distributors.

(c) Location of Relationship Management

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

Financial Advice

2-4 In practice, a CMI may conduct marketing activities or rely on referrals or other means to acquire new customers. The CMI need not perform the CDD measures where the CMI 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 member of the board of directors or senior management of a CMI.

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 CMI shall identify and assess ML/TF risks on an enterprise-wide level.[3] This shall include a consolidated assessment of the CMI'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 CMI in Singapore in the following ways:

(a) A CMI 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 CMI 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 CMI to better understand its overall vulnerability to ML/TF risks and forms the basis for the CMI's overall risk-based approach.

4-5 A CMI'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.

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

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

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

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

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

(iii) the delivery channels, including the extent to which the CMI 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 CMI's business.

4-8 As far as possible, a CMI's enterprise-wide ML/TF risk assessment should entail both qualitative and quantitative analyses to ensure that the CMI accurately understands its exposure to ML/TF risks. A quantitative analysis of the CMI's exposure to ML/TF risks should involve evaluating data on the CMI'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 CMI 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 CMI should make its own determination as to the risk weights to be given to the individual factor or combination of factors.

Singapore's Risk Assessment Reports

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

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

4-12 The risk assessment reports also identify certain prevailing crime types as presenting higher ML/TF risks. A CMI 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 CMI should also take these results into account as part of the CMI's ongoing monitoring of the conduct of customers' accounts and the CMI'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 a CMI's enterprise-wide ML/TF risk assessment. A CMI shall put in place adequate policies, procedures and controls to mitigate the ML/TF risks.

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

4-15 A CMI 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 CMI;

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

(g) the process of management reporting and escalation of pertinent AML/CFT issues to the CMI's senior management;

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

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

Documentation

4-16 The documentation should include —

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

(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 CMI 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 In keeping its enterprise-wide risk assessments up-to-date, a CMI 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 CMI. The results of these reviews should be documented and approved by senior management even if there are no significant changes to the CMI'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 CMI should keep abreast of such new developments and the ML/TF risks associated with them.

5-2 A CMI's assessment of ML/TF risks in relation to new products, practices and technologies is separate from, and in addition to, the CMI's assessment of other risks such as credit risks, operational risks or market risks. For example, in the assessment of ML/TF risks, a CMI 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 "delivery mechanism" as set out in paragraph 5 of the Notice is mobile trading.

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 CMI 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 CMI when it undertakes transactions for customers who or which have not established business relations with the CMI.

6-2-2 A CMI should monitor whether the related or linked transactions exceed the thresholds set out in paragraph 6.3(b) 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 CMI 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 paragraph 6.3(b).

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 CMI 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, checks against 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 CMI 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 CMI 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 CMI and whether the customer holds or has held a prominent public function. Such additional identification information enables a CMI to obtain better knowledge of its customers' 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(a)(iii) of the Notice, a P.O. box address should only be used for jurisdictions where the residential address (e.g. street name or house number) is not applicable or available in the local context.

6-4-2 A CMI 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 CMI is required to identify and screen all the connected parties of a customer. However, a CMI may verify their identities using a risk-based approach[5]. A CMI 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 CMI shall perform CDD measures on the customer by identifying the trust relevant parties, as required by paragraph 6.14 of the Notice.

Notice Paragraph 6.9

6-6 Verification of Identity of Customer

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

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

6-6-2 In verifying the identity of a customer, a CMI 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 or its equivalent, constitutional document, certificate of registration or any other documentation from a reliable independent source; and

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

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 CMI is unable to retain a copy of the documentation used to verify the customer's identity, the CMI 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 CMI'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 CMI'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 CMI 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 CMI.

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

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

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

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

6-6-6 Where the customer is unable to produce an original document, a CMI 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 CMI's 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 CMI to be reasonably satisfied that the document does in fact provide evidence of the customer's identity. The CMI 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 CMI may rely on a translation of such document by a CMI's staff independent of the customer relationship who is conversant in that foreign language. This is to allow all employees, officers and representatives of the CMI 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/FT risks associated with the customer.

6-6-8 The CMI 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 CMI should verify at a minimum those natural persons who will deal directly with the CMI.

Notice Paragraphs 6.13 to 6.17

6-8 Identification and Verification of Identity of Beneficial Owner

6-8-1 A CMI 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 CMI 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 CMI 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 CMI should obtain enough information to sufficiently understand if there are legitimate reasons for such ownership or control structure.

6-8-6 A CMI should take particular care when dealing with companies with bearer shares, since the beneficial ownership is difficult to establish. For such companies, a CMI should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the CMI is notified whenever there is a change of beneficial owner of such shares. At a minimum, these procedures should require the CMI to obtain an undertaking in writing from the beneficial owner of such bearer shares stating that the CMI 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 CMI may require that the bearer shares be held by a named custodian, with an undertaking from the custodian that the CMI 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 CMI 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 the beneficial owners of the customer. However, for such a customer, if there are other non-publicly listed legal persons who own more than 25% of the customer or who otherwise control the customer, the beneficial owners of such non-publicly listed legal persons should be identified and verified.

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

Notice Paragraph 6.18

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

6-9-1 The measures taken by a CMI 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 CMI 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 CMI 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 CMI to adjust the level of monitoring should be reviewed regularly for effectiveness in mitigating the CMI's ML/TF risks.

6-10-2 A CMI 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 existing business relations may have increased (for example, where there are anomalies in the control or conduct of an account or discrepancies relating to a customer's source of wealth), the CMI should promptly implement commensurate risk mitigation measures, including enhanced ongoing monitoring. Examples of enhanced ongoing monitoring are enhanced monitoring of transactions (including pre-transaction checks) and the imposition of restrictions on the account. The CMI should also request additional information and conduct a review of the customer's risk profile in order to determine if further 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 CMI can identify changes to the customer's risk profile —

(a) for higher risk categories of customers, a CMI should obtain updated CDD information (including updated copies of the customers' 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 CMI, whichever is earlier; and

(b) for all other risk categories of customers, a CMI 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 CMI's policies, procedures or standards relating to the documentation of CDD information change substantially, and (iv) the CMI 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 CMI 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 CMI 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 CMI 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 CMI'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 CMI's operations.

6-10-9 Nevertheless, the processes and systems used by the CMI should provide its business units (e.g. front office) 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 CMI 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. Retail Business and Corporate Business units) to facilitate a holistic assessment of the ML/TF risks presented by the customer. Therefore, CMIs should have processes in place to share such information across business units. In addition, CMIs should perform trend analyses of transactions to identify unusual or suspicious transactions. CMIs should also monitor transactions with parties in high risk countries or jurisdictions.

6-10-11 In addition, CMIs should have processes in place to monitor related customer accounts holistically within and across business units, so as to better understand the risks associated with such customer groups, identify potential ML/TF risks and report suspicious transactions. This includes having processes and appropriate confidentiality safeguards to share information on customers and their related accounts within and across business units, where information to be shared should minimally include CDD information collected by the CMI under Section 6 of the Notice as well as source of wealth information collected by the CMI under paragraph 8.3(b) of the Notice.

6-10-12 The parameters and thresholds used by a CMI to identify suspicious transactions should be properly documented and independently validated to ensure that they are appropriate to its operations and context. A CMI 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 through any means of communication (for example, the internet, post, fax or telephone). A CMI 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 CMI 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 CMI should apply additional checks to manage the risk of impersonation. The additional checks may consist of robust anti-fraud checks that the CMI 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 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 a 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 CMI from funds held by the customer in an account with a bank in Singapore.

Notice Paragraph 6.30

6-12 Reliance by Acquiring CMI on Measures Already Performed

6-12-1 When a CMI acquires the business of another FI, either in whole or in part, it is not necessary for the identity of all existing customers to be verified again, provided that the requirements of paragraph 6.30 of the Notice are met. A CMI 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 CMI is responsible for its obligations under the Notice.

6-12-3 When a CMI acquires the business of another FI, either in whole or in part, the CMI 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 CMI 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 CMI 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 CMI should terminate business relations with the customer if such verification remains uncompleted 120 business days after the establishment of business relations; and

(d) the CMI 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 CMI 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 CMI 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 CMI.

Notice Paragraphs 6.39 to 6.41

6-15 Screening

6-15-1 Screening is intended to be a preventive measure. A CMI 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 CMI 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 FSM Sanctions Regulations. Any such assets should be reported promptly to the relevant authorities and a Suspicious Transaction Report ("STR") should be filed as soon as possible, no later than 1 business day after suspicion was first established[6].

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

(a) the ML/TF information sources used by the CMI for screening (including (i) commercial databases and where appropriate, pertinent search engines[7] used to identify adverse information on individuals and entities, (ii) individuals and entities covered under the FSM Sanctions Regulations and TSOFA, and (iii) individuals and entities identified by other sources such as the CMI's head office or parent supervisory authority, lists and information provided by the Authority and relevant authorities in Singapore);

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

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

(b) the roles and responsibilities of the CMI'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;

(e) how apparent matches from screening are to be resolved by the CMI'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 CMI's employees for reporting positive hits to the CMI'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 CMI's business. A CMI 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 CMI 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 CMI'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 CMI 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 CMI 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(c) of the Notice, a CMI 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 CMI 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 CMI's customer database for periodic name screening purposes. This will help the CMI 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 CMI should consider its customers' risk profile.

6-15-9 The CMI should ensure that it has adequate arrangements to perform screening of the CMI'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 CMI 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.

7 Notice Paragraph 7 – Simplified Customer Due Diligence

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

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

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

7-4 Where a CMI is satisfied that the risks of money laundering and terrorism financing are low, a CMI 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 CMI'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 CMI 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 CMI;

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

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

(vi) cash-intensive businesses; and

(vii) customers who exhibit characteristics of a higher risk shell company[8], including but not limited to:

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

(i) unclear economic purpose for requiring account relationship in Singapore:
    (i) E.g. foreign-incorporated companies with no business presence or activities in Singapore seek to open accounts in Singapore (including through a nominee arrangement);
(ii) unclear economic purpose for linking a common individual / address to multiple companies:
    (i) E.g. multiple companies are linked to the same registered address, where the address is not in line with and/or fit for the companies' nature of business;
    (ii) E.g. use of nominee individuals to obscure beneficial ownership and control of the account;
(iii) unrelated third parties (e.g. foreigners) added to operate account after account opening:
    (i) E.g. authorised signatories or directors are changed, post-account opening, to allow unrelated third parties to operate the account;
(iv) unusual change of corporate structure / beneficial owner after account opening;
(v) suspicious transactions which are not in line with the CMI's understanding of customer; or
(vi) superficial corporate websites inconsistent with scale of business:
    (i) E.g. companies (including newly incorporated companies) that are stated to be involved in a wide range of activities without a dominant product/expertise;
    (ii) E.g. corporate websites have vague descriptions and limited information, which are not in line with the turnover or business nature of the companies.

(b) Country or geographic risk

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

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

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

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

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

8-3 When considering the ML/TF risks presented by a country or jurisdiction, a CMI 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 CMI 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 CMI 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 the information from a customer, the CMI 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 CMI determines that any natural person appointed to act on behalf of a customer or any connected party of a customer is a PEP, the CMI should assess the ML/TF risks presented and consider factors such as the level of influence that the PEP has on the customer. CMI 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 CMI should apply ECDD measures on the customer accordingly.

8-5-2 It is generally acceptable for a CMI to refer to commercially available databases to identify PEPs. However, a CMI should also obtain from the customer details of his occupation and the name of his employer. In addition, a CMI should consider other non-public information that the CMI is aware of. A CMI 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 CMI's AML/CFT compliance function.

8-5-4 In relation to paragraph 8.3(b) of the Notice, a CMI 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 CMI should note that not all declarations are publicly available. A CMI should also be aware that certain jurisdictions impose restrictions on their PEPs' ability to hold foreign investment 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), and includes seed money that generated subsequent wealth and gifts or other assets (if any) received by the customer and beneficial owner. Source of wealth relates to how the customer and beneficial owner of the customer have acquired the wealth, which is distinct from identifying the assets that they own. Source of wealth information obtained by the CMI should give an indication, to the extent practicable, about the entire body of wealth that the customer and beneficial owner would be expected to have, and how the customer and beneficial owner acquired the wealth. This information would enable the CMI to make a reasonable assessment of which sources of wealth of the customer and beneficial owner that are material and/or present a higher risk for ML/TF. Although the CMI may not have specific information about assets that are not deposited with or processed by the CMI, it may be possible to obtain general information from the customer, commercial databases or other open sources.

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 CMI 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 Subject to paragraph 8.4 of the Notice, a CMI should corroborate the information regarding source of wealth and source of funds. 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 information and documents such as copies of trust deeds, salary details, tax returns, bank statements, audited financial statements of the legal person or legal arrangement owned or controlled by the PEP, site visits, a copy of the will (in cases where the source of wealth or funds is an inheritance), conveyancing documents (in cases where the source of wealth or funds is a sale of property) and credible public information sources. A CMI should take a risk-based approach and focus on corroboration of sources of wealth and sources of funds that are more material and/or present a higher risk for ML/TF. A CMI should ensure that such sources of wealth and sources of funds are established through appropriate and reasonable means, to the extent practicable, using reliable and independent sources of information. In cases where independent sources of information are not available, the CMI should exercise prudence in the use of non-independent sources of information, such as customer representations, assumptions and benchmarks, to ensure adequate rigour of assessment. This should include the performance of additional checks against alternative information sources to determine whether such information, representations, assumptions or benchmarks are reasonable and reliable. The CMI's basis for using such information should be documented and reviewed periodically. The CMI is also reminded that assumptions and benchmarks should facilitate its assessment of the plausibility of the customer or beneficial owner's source of wealth or source of funds, and should not be used to justify or support circumstances or explanations provided by the customer or beneficial owner if there are reasons that cast suspicion on their source of wealth or source of funds.

8-5-7A Where a CMI is unable to corroborate any source of wealth or source of funds that is more material and/or presents a higher risk for ML/TF, the CMI should assess whether the residual risks associated with not corroborating such source of wealth or source of funds is acceptable and whether additional risk mitigation measures should be applied in the absence of corroboration. Examples of risk mitigation measures include obtaining senior management's approval to establish or continue business relations with the customer and conducting enhanced ongoing monitoring of the business relationship.

8-5-7B Where a material source of wealth of the customer or beneficial owner is a gift or other asset received from third parties, a CMI should obtain information to establish the legitimacy and plausibility of such gift or other asset. This should include establishing the relationship between the third party and the customer or beneficial owner, and verifying the transaction(s) effecting such gift or other asset against reliable and independent sources of information such as bank statements or public sources where practicable. A CMI should also assess the plausibility of the third party's source of wealth as part of the assessment. Where unable to do so, the CMI should assess the residual risks presented by the third party's source of wealth, and consider whether the additional risk mitigation measures as set out in paragraph 8-5-7A should be applied on the business relationship with the customer.

8-5-7C A CMI should assess if the customer and beneficial owner's source of wealth and source of funds are plausible and legitimate, considering all the information and documents that the CMI has obtained. Where the CMI is unable to ascertain the plausibility and legitimacy of the customer or beneficial owner's source of wealth or source of funds, the CMI should consider if there are grounds for terminating business relations with the customer and whether an STR should be filed.

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 CMI finds information containing allegations of wrongdoing by a customer or a beneficial owner of a customer, the CMI 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 CMI 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 CMI 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 CMI 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 CMI's assessment that that the business relations or transactions with the customer present higher ML/TF risks, the CMI 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 CMI 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 CMI may refer to the preceding paragraph 8-5-8 of these Guidelines for further guidance on the ECDD measures to be performed. A CMI should assess whether the information regarding the source of wealth and source of funds of the customer and any beneficial owner should be corroborated against additional documentary evidence or public information sources and document its assessment[9]. The CMI may refer to the preceding paragraphs 8-5-5 to 8-5-7C of these Guidelines for further guidance on establishing the source of wealth and source of funds of customers and beneficial owners.

8-6-1A A CMI should pay attention to changes in the customer's risk profile, information and/or transactions that would warrant corroboration of the customer and any beneficial owner's source of wealth and source of funds, and do so in a timely manner.

8-6-2 For customers highlighted in paragraph 8.6(a) of the Notice, a CMI shall assess them as presenting higher ML/TF risks. For such customers, the CMI shall ensure that the ECDD measures performed are commensurate with the risks. For customers highlighted in paragraph 8.6(b) of the Notice, a CMI shall assess

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

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 CMI 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 CMI should refer to the FATF's Public Statements on High-Risk Jurisdictions subject to a Call for Action [10]. FATF updates this Public Statement on a periodic basis and CMIs should regularly refer to the FATF website for the latest updates[11].

8-6-4 For higher risk business (e.g. private banking business and wealth management for high-net-worth individuals) which inherently presents higher ML/TF risks, a CMI should, regardless of the CMI's internal risk classification of the customer, refer to the sound practices highlighted in the MAS Information Paper, "Guidance on Private Banking Controls"[12]. Such practices include ensuring that –

(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/ funds;

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

(d) where the CMI is aware of customers having a common beneficial owner or a customer having multiple accounts with the CMI, the CMI 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, CMIs 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, CMIs should conduct enhanced monitoring and

[10] 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

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

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

where appropriate, discontinue the relationship. If the CMI 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 CMI. 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 CMI, in accordance with the CMI's AML/CFT policies, procedures and standards, and is subject to the CMI's control measures to effectively implement the CMI's AML/CFT procedures.

9-4 The CMI 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 or FSRBs' 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 CMI 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 CMI's business relations with the customer or the completion of transactions undertaken.

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

9-7 For the avoidance of doubt, paragraph 9 of the Notice does not prevent the CMI from outsourcing a part of the ongoing monitoring processes. A CMI may outsource the first-level review of alerts from the transaction monitoring systems, or sanctions reviews, to another party. However, the CMI remains responsible for complying with ongoing monitoring requirements under the Notice.

10 Notice Paragraph 10 – Correspondent Accounts

10-1 CMIs 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 CMI may provide correspondent account services for financial institutions around the world. An example of a correspondent account service is where a securities firm outside Singapore opens a securities trading account with a CMI in Singapore, to trade on its own behalf or for its customers.

10-3 After a CMI obtains adequate information as required by paragraph 10.3(a) of the Notice to establish a correspondent account relationship, such information should continue to be updated on a periodic basis thereafter.

10-4 Other factors that a CMI 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 account relationship[13]; the CMI should review the risks posed by such "nested" relationships.

10-5 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 CMI may rely on information from the FATF mutual evaluation reports and statements on countries or jurisdictions identified as either being subject to countermeasures or having strategic AML/CFT deficiencies, mutual evaluation reports by FSRBs, publicly available information from national authorities and any restrictive measures imposed on a country, particularly prohibitions on providing correspondent account services.

10-6 For correspondent account relationships established with a CMI's related entities, the appropriate level of measures as required under paragraphs 6, 7 and 8 of the

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

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 CMI should take into consideration the parent financial institution'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.

10-7 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 CMI's assessment of the respondent FI may be enhanced through meetings with the respondent FI's management and compliance head, capital markets and AML/CFT regulators.

10-8 A CMI 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 account relationships generally present higher ML/TF risks.

10-9 If a CMI provides correspondent account services to its related respondent FIs within the same financial group, the CMI should ensure that it still assesses the ML/TF risks presented by its related respondent FI.

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

10-11 For the purposes of paragraph 10 of the Notice, a CMI 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.

10-12 In assessing whether a CMI or FI falls within the meaning of "shell FI" for the purposes of paragraph 10 of the Notice, a CMI should note that physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level employees does not constitute physical presence.

13 Notice Paragraph 13 – Suspicious Transactions Reporting

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

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

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

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

13-1 A CMI should ensure that the internal process for evaluating whether a matter should be referred to the Suspicious Transaction Reporting Office ("STRO") via an STR is completed without delay. The filing of an STR should not exceed 5 business days after suspicion was first established[14], officer or representative, unless the circumstances are exceptional or extraordinary. In cases involving sanctioned parties[15] and parties acting on behalf of or under the direction of sanctioned parties[16], a CMI should file the STRs as soon as possible, and no later than 1 business day after suspicion was first established[17].

13-2 A CMI should note that an STR filed with STRO would also meet the reporting obligations under the TSOFA.

13-3 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 CMI 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.

13-4 Once suspicion has been raised in relation to a customer or any transaction for that customer, in addition to reporting the suspicious activity, a CMI should ensure that appropriate action is taken to adequately mitigate the risk of the CMI being

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

[15] Sanctioned parties" include persons designated or covered under the Terrorism (Suppression of Financing) Act 2002 and the regulations issued under section 192 read with section 15(1)(b) of the Financial Services and Markets Act 2022 relating to sanctions and freezing of assets of persons.

[16] Such cases include cases involving any funds, other financial assets or economic resources owned or controlled, directly or indirectly, by sanctioned parties.

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

used for ML/TF activities. This may include strengthening its AML/CFT processes. This may also include a review of either the risk classification of the customer, or the business relations with the customer. Other appropriate action that should be taken include escalating the issue to the appropriate decision making level, taking into account any other relevant factors, such as cooperation with law enforcement agencies. After reporting the suspicious activity, where further suspicion is raised in relation to the customer or any transaction for the customer, the CMI should assess if the filing of a further or supplementary STR to report the further suspicion is warranted.

13-5 STR reporting templates are available on CAD's website[18]. However, CMIs are strongly encouraged to use the online system provided by STRO to lodge STRs. In the event that the CMI 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 CMI should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct.

13-6 A CMI 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, officers and representatives should be properly substantiated and documented.

13-7 CMIs are reminded to read paragraph 13.4 of the Notice together with paragraphs 6.35 and 6.36 of the Notice. Where a CMI stops performing CDD measures as permitted under paragraph 13.4 and is, as a result, unable to complete CDD measures (as specified under paragraph 6.36), the CMI is reminded that it shall not commence or continue business relations with that customer or undertake any transaction for that customer.

14 Notice Paragraph 14 – Internal Policies, Compliance, Audit and Training

14-1 As internal policies and procedures serve to guide employees, officers and representatives in ensuring compliance with AML/CFT laws and regulations, it is important that a CMI 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.

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

Notice Paragraphs 14.3 to 14.9

14-2 Group Policy

14-2-1 For the avoidance of doubt, Singapore branches of CMIs incorporated outside Singapore need not comply with paragraphs 14.3 to 14.9 of the Notice. Paragraphs 14.3 to 14.9 of the Notice are intended to be applied by a CMI incorporated in Singapore to its branches and subsidiaries, but not to its parent entity and the CMI's other related corporations.

14-2-2 In relation to paragraph 14.6 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 CMI, 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 CMI incorporated in Singapore with the CMI's group level compliance, audit, and AML/CFT functions (whether in or outside Singapore), for risk management purposes.

Notice Paragraphs 14.10 to 14.11

14-3 Compliance

14-3-1 A CMI should ensure that the AML/CFT compliance officer has the necessary seniority and authority within the CMI to effectively perform his responsibilities.

14-3-2 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, officers and representatives 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, officers and representatives on developing and implementing internal policies, procedures and controls on AML/CFT;

(g) reporting to senior management on the outcome of reviews of the CMI'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 1-4-16 of the Guidelines), and any necessary remedial actions, arising from audit, inspection, and compliance reviews, to the CMI's senior management, and in the case of locally incorporated CMIs, to the board of directors, at least annually and as and when needed.

14-3-3 The business interests of a CMI 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 CMI's management.

Notice Paragraph 14.12

14-4 Audit

14-4-1 A CMI'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 CMI-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 CMI'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', officers' and representatives' 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.

14-4-2 The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the CMI's business.

Notice Paragraph 14.13

14-5 Employee and Representative Hiring

14-5-1 The screening procedures applied when a CMI in Singapore hires employees, and appoints officers and representatives should include —

(a) background checks with past employers;

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

(c) bankruptcy searches.

14-5-2 In addition, a CMI should conduct credit history checks, on a risk-based approach, when hiring employees, and appointing officers and representatives.

Notice Paragraph 14.14

14-6 Training

14-6-1 As stated in paragraph 14.14 of the Notice, it is a CMI's responsibility to provide adequate training for its employees, officers and representatives 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 CMI and pitched according to the job functions, responsibilities and experience of the employees, officers and representatives. New employees, officers and representatives should be required to attend training as soon as possible after being hired or appointed.

14-6-2 Apart from the initial training, a CMI should also provide refresher training at least once every two years, or more regularly as appropriate, to ensure that employees, officers and representatives are reminded of their responsibilities and are kept informed of new developments related to ML/TF. A CMI should maintain the training records for audit purposes.

14-6-3 A CMI should monitor the effectiveness of the training provided to its employees, officers and representatives. This may be achieved by —

(a) testing employees', officers' and representatives' understanding of the CMI'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', officers' and representatives' compliance with the CMI'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, officers and representatives who miss such training without reasonable cause.

I Other Key Topics - Guidance to CMIs on Proliferation Financing

I-1 Overview

I-1-1 MAS issues FSM Sanctions Regulations in order to discharge or facilitate the discharge of any obligation binding on Singapore by virtue of a United Nations Security Council Resolution ("UNSCR") adopted by the United Nations Security Council ("UNSC"). These Regulations apply to all FIs (including CMIs) regulated by MAS and generally impose financial sanctions on designated persons.

I-1-2 Specifically, the UNSC may designate certain individuals and entities involved in the proliferation of weapons of mass destruction and its financing. The relevant information and full lists of persons designated by the UNSC can be found at the UNSC's website[19].

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

I-1-4 A CMI 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 CMI 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 CMI, as required under the Notice, is performed against the latest UNSC sanctions lists as they are updated from time to time. A CMI should have in place policies, procedures and controls to continuously monitor the lists and take necessary follow-up action within a reasonable period of time, as required under the applicable laws and regulations.

I-2-2 A CMI should also have policies and procedures to detect attempts by its employees, officers or representatives to circumvent the applicable laws and regulations (including the FSM Sanctions Regulations), such as—

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

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

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

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

I-3 Obligation of CMI to Freeze without Delay

I-3-1 A CMI 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 CMI has in its possession, custody or control. The CMI should also report the freeze to MAS and file an STR as soon as possible, no later than 1 business day after suspicion was first established[20].

I-4 Potential Indicators of Proliferation Financing

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

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

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

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

(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 CMI may wish to refer to the FATF website for additional information.

II Useful Links

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

The International Organization of Securities Commissions: http://www.iosco.org/

……

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

Customer Type	Examples of CDD Information
Sole proprietorships	• Full registered business name • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the CMI • 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 CMI's visit to the customer's place of business, where the CMI 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 CMI • 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 CMI's visit to customer's place of business, where the CMI 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 CMI • 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 CMI's visit to the customer's place of business, where the CMI 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 CMI • Any association the entity may have with other countries or jurisdictions (e.g. the location of the entity's headquarters, operating facilities, branches, subsidiaries)
Public sector bodies, government, state-owned companies and supranationals (other than sovereign wealth funds)	• Full name of entity • Nature of entity (e.g. overseas government, treaty organisation) • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the CMI • 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 CMI's visit to the customer's place of business, where the CMI assesses it as necessary • Board resolution authorising the opening of the customer's account with the CMI

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 CMI • 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 CMI's visit to the customer's place of business, where the CMI 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 CMI • Records in a relevant and independent registry in the country of establishment

Customer Type	Examples of CDD Information
Trusts 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 CMI's visit to the customer's place of business, where the CMI assesses it as necessary • Information about the purpose and intended nature of business relations with the CMI • Records in a relevant and independent registry in the country or jurisdiction of constitution • Country or jurisdiction of constitution • Trust deed or its equivalent • Names of the trust relevant parties • Declaration of trusts or its equivalent • Deed of retirement and appointment of trustees (where applicable)

APPENDIX B – Examples of Suspicious Transactions

B-1 General Comments

B-1-1 The list of situations given below is intended to highlight some basic ways in which money may be laundered or used for TF purposes. While each individual situation may not be sufficient to suggest that ML/TF is taking place, a combination of such situations may be indicative of a suspicious transaction. The list is not exhaustive and will require constant updating and adaptation to changing circumstances and new methods of laundering money or financing terrorism. 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. CMIs are to refer to STRO's website for the latest list of red flags[21].

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 CMI in the course of the business relations. CMIs 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 CMI 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 switching from trading only penny stocks to predominantly blue chips.

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

iii) Transactions in which assets are withdrawn immediately after being deposited[22], unless the customer's business activities furnish a plausible reason for immediate withdrawal.

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

[22] For CMIs, this could mean depositing of funds into trust accounts, margin accounts, as collaterals or for fund management purposes.

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) Unexpected repayment of a delinquent account without any plausible explanation.

vi) Corporate finance transactions under consideration that do not make economic sense in respect of the business operations of the customer, particularly if the customer is not a listed company.

vii) Request by a customer for investment management services where the source of funds is unclear or not consistent with the customer's apparent standing.

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

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

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) Provision of funds for investment and fund management purposes in the form of large cash amounts.

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) Provision of margin collaterals in the form of large cash amounts.

vii) Payments made via large amounts of cash. A guideline to what constitutes a large or substantial cash amount would be a cash amount exceeding S$20,000 (or its equivalent in any currency).

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) Crediting of customer trust or margin accounts using cash and by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

x) Payments or deposits containing counterfeit notes or forged instruments.

xi) Unusual settlements of securities transactions in cash form.

B-4 Transactions Involving CMIs' Accounts

i) 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.

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

iii) Multiple depositors using a single account.

iv) Paying in large third party cheques endorsed in favour of the customer in settlement for securities purchased, or for other financial services provided.

v) Frequent deposits of a company's cheques into an employee's account.

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

vii) Purchase of securities to be held by the CMI in safe custody, where this does not appear appropriate given the customer's apparent standing.

viii) Requests for refunds of unaccountable "erroneous" payments to CMIs' or customers' trust accounts by unknown persons.

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

B-5 Transactions Involving Transfers Abroad

i) 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.

ii) Cross border transactions involving acquisition or disposal of high value assets that cannot be clearly identified as bona fide transactions.

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

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

B-6 Transactions Involving Unidentified Parties

i) Transfer of money to another CMI 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 CMI.

v) Provision of collateral by way of pledge or guarantee without any discernible plausible reason by third parties unknown to the CMI 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.

vii) Requests by a customer for investment management services where the source of funds is unclear.

B-7 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 fund transfers from or to a country or jurisdiction that presents higher risk of tax evasion.

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

B-8 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 CMI.

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 margining or financing facilities.

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

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

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