Monetary Authority of Singapore

GUIDELINES TO MAS NOTICE FAA-N06 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

24 APRIL 2015

TABLE OF CONTENTS

1 Introduction 2
2 Notice Paragraph 2 – Definitions, Clarifications and Examples 7
4 Notice Paragraph 4 – Assessing Risks and Applying a Risk-Based Approach ... 9
5 Notice Paragraph 5 – New Products, Practices and Technologies 14
6 Notice Paragraph 6 – Customer Due Diligence 15
7 Notice Paragraph 7 – Simplified Customer Due Diligence 29
8 Notice Paragraph 8 – Enhanced Customer Due Diligence 31
9 Notice Paragraph 9 – Reliance on Third Parties 40
12 Notice Paragraph 12 – Suspicious Transactions Reporting 42
13 Notice Paragraph 13 – Internal Policies, Compliance, Audit and Training 44
I Other Key Topics - Guidance to Financial Advisers on Proliferation Financing 48
II Useful Links 50
APPENDIX A – Examples of CDD Information for Customers (including Legal Persons/Arrangements) 51
APPENDIX B – Examples of Suspicious Transactions 55

For ease of reference, the chapter numbers in these Guidelines mirror the corresponding paragraph numbers in MAS Notice FAA-N06 on Prevention of Money Laundering and Countering The Financing of Terrorism - Financial Advisers (e.g. Chapter 2 of the Guidelines provides guidance in relation to paragraph 2 of the Notice). Not every paragraph in the Notice has a corresponding paragraph in these Guidelines and this explains why not all chapter numbers are utilised in these Guidelines.

1 Introduction

1-1 These Guidelines provide guidance on the requirements in MAS Notice FAA-N06 on Prevention of Money Laundering and Countering the Financing of Terrorism - Financial Advisers ("the Notice") to the following, except those which only provide advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product (collectively "financial advisers"):

(a) licensed financial advisers;

(b) registered insurance brokers which are exempt under section 23(1)(c) of the Financial Advisers Act (Cap. 110), from holding a financial adviser's licence to act as a financial adviser in Singapore in respect of any financial advisory service; and

(c) persons exempt, under section 23(1)(f) of the Financial Advisers Act read with regulation 27(1)(d) of the Financial Advisers Regulations (Rg. 2), from holding a financial adviser's licence to act as a financial adviser in Singapore in respect of any financial advisory service.

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 financial adviser may have an impact on the Authority's overall risk assessment of the financial adviser, 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 (Cap. 65A). A financial

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

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

Terrorism Financing

1-4-3 Acts of terrorism seek to influence or compel governments into a particular course of action or to intimidate the public or a section of the public. Financial advisers are reminded of the definitions of "terrorist" and "terrorist act" set out in the Terrorism (Suppression of Financing) Act (Cap. 325) ("TSOFA").

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

1-4-5 However, terrorist acts and organisations may also be financed from legitimate sources such as donations from charities, legitimate business operations, self-funding by individuals etc. Coupled with the fact that TF need not always involve large sums of money, TF can be hard to detect and financial advisers should remain vigilant.

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

Proliferation Financing

1-4-6A 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

1-4-7 Each financial adviser is reminded that the ultimate responsibility and accountability for ensuring compliance with anti-money laundering and countering the financing of terrorism ("AML/CFT") laws, regulations and notices rests with its board of directors and senior management.

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

1-4-9 Business units (e.g. front office, customer-facing functions) constitute the first line of defence in charge of identifying, assessing and controlling the ML/TF risks of their business. The second line of defence includes the AML/CFT compliance function, as well as other support functions such as operations, human resource or technology, which work together with the AML/CFT compliance function to identify ML/TF risks when they process transactions or applications or deploy systems or technology. The third line of defence is the financial adviser's internal audit function.

1-4-10 As part of the first line of defence, business units require robust controls to detect illicit activities. They should be allocated sufficient resources to perform this function effectively. The financial adviser'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 financial adviser 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 financial adviser's compliance with prevailing AML/CFT laws, regulations and notices.

1-4-11 As the core of the second line of defence, the AML/CFT compliance function is responsible for ongoing monitoring of the fulfilment of all AML/CFT duties by the financial adviser. This implies sample testing and the review of exception reports.

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

The AML/CFT compliance function should alert the financial adviser's senior management or the board of directors if it believes that the employees or officers in the line departments are failing or have failed to adequately address ML/TF risks and concerns. Other support functions such as operations, human resource or technology also play a role to help mitigate the ML/TF risks that the financial adviser faces. The AML/CFT compliance function is typically the contact point regarding all AML/CFT issues for domestic and foreign authorities, including supervisory authorities, law enforcement authorities and financial intelligence units.

1-4-12 As the third line of defence, the financial adviser'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 financial adviser'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 financial adviser's compliance with prevailing AML/CFT policies, procedures and controls. A financial adviser should establish policies for periodic AML/CFT internal audits covering areas such as

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

Governance

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

1-4-14 A financial adviser's board of directors and senior management should understand the ML/TF risks the financial adviser is exposed to and how the financial adviser'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 financial adviser is exposed to through its activities and individual business relations;

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

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

(d) ensuring that processes are in place to escalate important decisions that directly impact the ability of the financial adviser 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 (Cap. 163A) and section 28 of the Limited Partnerships Act (Cap. 163B).

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

Customer

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

(a) Portfolio Managers

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

However, the Authority recognises that a financial adviser may not be able to perform CDD measures on the underlying investors. For instance, the portfolio manager may be reluctant, for commercial reasons, to reveal information on the underlying investors to the financial adviser. In such circumstances, the financial adviser should evaluate the risks arising from each case and determine the appropriate CDD measures to take. The financial adviser may consider whether simplified CDD ("SCDD") measures could be applied to underlying investors under paragraph 7 of the Notice. However, where the customer falls within paragraph 6.15 of the Notice the financial adviser is exempted from making inquiries about the existence of such underlying investors (i.e. beneficial owners). Therefore, the financial adviser does not need to identify and verify such underlying investors.

(b) Location of Relationship Management

Given the globalised nature of modern financial advisory business, it may be the case that a financial adviser's relationship and transactions with a particular customer is managed by a financial adviser 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 financial adviser should perform the applicable CDD measures if in substance, the relationship or account is managed by an employee, officer

or representative of the financial adviser in Singapore even though the account is booked in another country or jurisdiction. However, the financial adviser may rely on the CDD measures carried out by its related entity (or in the case of a branch network, another branch of the financial adviser) in accordance with paragraph 9 of the Notice.

Legal Arrangements

2-4 In relation to the definition of "legal arrangement" in the Notice, examples of legal arrangements are trust, fiducie, treuhand and fideicomiso.

Legal Persons

2-5 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

2-6 A reference to "officers" refers to a member of the board of directors or senior management of a financial adviser.

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

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

4-5 A financial adviser'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 financial adviser should consider include –

(a) in relation to its customers –

(i) the target customer markets and segments;

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

(iii) the 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 financial adviser has operations in –

(i) countries or jurisdictions the financial adviser is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its customers, 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, 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; and

- 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 financial adviser –

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

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

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

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

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

4-11 A financial adviser should incorporate the results of Singapore's ~~NRA Report~~ risk assessment reports[4] in~~to~~ its enterprise-wide ML/TF risk assessment process. When performing the enterprise-wide risk assessment, a financial adviser 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 financial adviser should consider the ~~NRA results~~ findings in the risk assessment reports and 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 ~~NRA~~ risk assessment reports also identify~~ies~~ certain prevailing crime types as presenting higher ML/TF risks. A financial adviser 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 financial adviser should also take these results into account as part of the financial adviser's ongoing monitoring of the conduct of customers' accounts and scrutiny of customers' transactions.

Risk Mitigation

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

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

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

(a) the financial adviser's 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 financial adviser;

(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 financial adviser's senior management;

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

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

Documentation

4-16 The documentation should include –

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

(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 financial adviser should ensure that the enterprise-wide ML/TF risk assessment and the risk assessment information are made available to the Authority upon request.

Frequency of Review

4-18 To keep its enterprise-wide risk assessments up-to-date, a financial adviser 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 financial adviser. The results of these reviews should be documented and approved by senior management even if there are no significant changes to the financial adviser'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 financial adviser shall keep abreast of such new developments and the ML/TF risks associated with them.

5-2 A financial adviser's assessment of ML/TF risks in relation to new products, practices and technologies is separate from, and in addition to, the financial adviser's assessment of other risks such as credit risks, operational risks or market risks. For example, in the assessment of ML/TF risks, a financial adviser should pay attention to new products, practices and technologies that deal with customer funds or the movement of such funds. These assessments should be approved by senior management and heads of business, risk and compliance.

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

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

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

Notice Paragraph 6.3

6-2 When CDD is to be Performed

6-2-1 A financial adviser need not perform CDD measures where the financial adviser solely prospects natural persons, legal persons or legal arrangements, without the provision of financial advice.

Notice Paragraphs 6.4 to 6.17

6-3 CDD Measures under Paragraphs 6.4 to 6.17

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

6-3-2 A financial adviser should exercise greater caution when dealing with an unfamiliar or a new customer. Apart from obtaining the identification information required by paragraph 6.5 of the Notice, a financial adviser 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 financial adviser and whether the customer holds or has held a prominent public function. Such additional identification information enables a financial adviser to obtain better knowledge of its customer's risk profile, as well as the purpose and intended nature of the account.

Notice Paragraph 6.5

6-4 Identification of Customer

6-4-1 With respect to paragraph 6.5~~(c)~~(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 financial adviser should obtain a customer's contact details such as personal, office or work telephone numbers.

Notice Paragraph 6.7

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 financial adviser is required to identify and screen all the connected parties of a customer. However, a financial adviser may verify their identities using a risk-based approach[5]. A financial adviser 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 financial adviser shall perform CDD measures on the customer by identifying the~~ settlors, trustees, the protector (if any), the beneficiaries (including every beneficiary that falls within a designated characteristic or class) and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership)~~ trust relevant parties, as required by paragraph 6.13 of the Notice.

Notice Paragraph 6.8

6-6 Verification of Identity of Customer

6-6-1 Where the customer is a natural person, a financial adviser 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, financial advisers are to refer to paragraph 7-3 of these Guidelines.

6-6-2 In verifying the identity of a customer, a financial adviser 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, or 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 financial adviser is unable to retain a copy of the documentation used to verify the customer's identity, the financial adviser 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 financial adviser'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 financial adviser'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 financial adviser obtains data, documents or information from the customer or a third party, it should ensure that such data, documents or information or document is current at the time they are provided to the financial adviser.

6-6-5A A financial adviser should ensure that staff are provided with adequate guidance on how to identify indicators of fraudulent or tampered data, documents or information. A financial adviser 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 that are found when these representations are checked against independent sources of information, such as corporate data reports;

(b) accounting errors, or anomalies in financial statements that are not in line with the financial adviser'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 financial adviser 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 a certified public or professional accountant); or

(b) if a staff of the financial adviser 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 financial adviser to be reasonably satisfied that the document does in fact provide evidence of the customer's identity. The financial adviser 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 financial adviser may rely on a translation of such document by a staff of the financial adviser independent of the customer relationship who is conversant in that foreign language. This is to allow all employees, officers and representatives of the financial adviser involved in the performance of any measures required under the Notice to understand the contents of the documents, for effective determination and evaluation of ML/TF risks associated with the customer.

6-6-8 The financial adviser 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 6.9 to 6.11

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 financial adviser should verify at a minimum those natural persons who deal directly with the financial adviser.

Notice Paragraphs 6.12 to 6.16

6-8 Identification and Verification of Identity of Beneficial Owner

6-8-1 A financial adviser should note that measures listed under paragraph 6.13(a)(i), (ii) and (iii) as well as paragraph 6.13(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 6.13(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 financial adviser 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 financial adviser 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 financial adviser should obtain enough information to sufficiently understand if there are legitimate reasons for such an ownership or control structure.

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

6-8-7 For the purposes of paragraph 6.15 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 financial adviser should put in place an internal assessment process with clear criteria, taking into account, amongst others, the country risk and the level of the country's compliance with the FATF standards.

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

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

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

6-8-12 Where a customer is one which falls within paragraph 6.15 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 6.17

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

6-9-1 The measures taken by a financial adviser 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 financial adviser 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 6.18 to 6.25

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 financial adviser 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 financial adviser to adjust the level of monitoring should be reviewed regularly for effectiveness in mitigating the financial adviser's ML/TF risks.

6-10-2 Where there are indications that the risks associated with ~~an~~ 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 financial adviser 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 financial adviser should also request additional information and conduct a review of the customer's risk profile in order to determine if further ~~additional~~ measures are necessary.

6-10-3 A key part of ongoing monitoring includes maintaining relevant and up-to-date CDD data, documents and information so that the financial adviser can identify changes to the customer's risk profile –

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

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

6-10-4 Examples of trigger events are when (i) a significant transaction takes place, (ii) a material change occurs in the way the customer's business relations are managed, (iii) the financial adviser's policies, procedures or standards relating to the documentation of CDD information change substantially, and (iv) the financial adviser becomes aware that it lacks sufficient information about the customer concerned.

6-10-5 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 financial adviser has previously obtained remains relevant and up-to-date.

6-10-6 In determining what would constitute suspicious, complex, unusually large or unusual pattern of transactions, a financial adviser 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 financial adviser 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;

(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).

6-10-7 A financial adviser'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 financial adviser's operations.

6-10-8 Nevertheless, the processes and systems used by the financial adviser 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.

6-10-9 The transaction monitoring processes and systems should enable the financial adviser 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 customers' account, such information should be shared across their business units (e.g. High Net-Worth Clients and Retail Business units) to facilitate a holistic assessment of the ML/TF risks presented by the customer. Therefore, financial advisers should have processes in place to share such information across business units. In addition, financial advisers should perform trend analyses of transactions to identify unusual or suspicious transactions. Financial advisers should also monitor transactions with parties in high risk countries or jurisdictions.

6-10-10 In addition, financial advisers should have processes in place to monitor related customer accounts holistically within or 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 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 financial adviser under Section 6 of the Notice as well as source of wealth information collected by the financial adviser under paragraph 8.3(b) of the Notice.

6-10-11 The parameters and thresholds used by a financial adviser to identify suspicious transactions should be properly documented and independently validated to ensure that they are appropriate to its operations and context. A financial adviser should periodically review the appropriateness of the parameters and thresholds used in the monitoring process.

Notice Paragraphs 6.26 to 6.28

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

6-11-1 A reference to "specific risks" in paragraph 6.26 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 financial adviser 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, amplify the ML/TF risks.

6-11-2 The measures taken by a financial adviser for verification of an identity in respect of non-face-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 financial adviser should apply additional checks to manage the risk of impersonation. The additional checks may consist of robust anti-fraud checks that the financial adviser routinely undertakes as part of its existing procedures, which may include –

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

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

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

(d) confirmation of the customer's salary details by requiring the presentation of recent bank statements, 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 financial adviser from funds held by the customer in an account with a bank in Singapore.

Notice Paragraph 6.29

6-12 Reliance by Acquiring Financial adviser on Measures Already Performed

6-12-1 When a financial adviser acquires the business of another financial institution ("FI"), either in whole or in part, it is not necessary for the identity of all existing customers to be verified again, provided that the requirements of paragraph 6.29 of the Notice are met. A financial adviser 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 financial adviser is responsible for its obligations under the Notice.

6-12-3 When a financial adviser acquires the business of another FI, either in whole or in part, the financial adviser is reminded that in addition to complying with paragraph 6.29 of the Notice, it is also required to comply with ongoing monitoring requirements set out in paragraphs 6.18 to 6.25 of the Notice.

Notice Paragraphs 6.30 to 6.32

6-13 Timing for Verification

6-13-1 With reference to paragraph 6.31 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 financial adviser 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 6.32 of the Notice –

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

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

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

Notice Paragraph 6.36

6-14 Existing Customers

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

6-14-2 In taking into account any previous measures as referred to in paragraph 6.36 of the Notice, a financial adviser 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 financial adviser.

Notice Paragraphs 6.37 to 6.39

6-15 Screening

6-15-1 Screening is intended to be a preventive measure. A financial adviser 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 financial adviser is reminded of its obligations to freeze without delay and without prior notice, the funds or other assets of designated persons and entities that it has control over, so as to comply with applicable laws and regulations in Singapore, including the TSOFA and MAS Regulations issued under section 27A of the MAS Act (Cap. 186) ("MAS Act") relating to sanctions and freezing of assets of persons. Any such assets should be reported promptly to the relevant authorities and a Suspicious Transaction Report ("STR") should be filed as soon as possible, no later than 1 business day after suspicion was first established.

6-15-3 A financial adviser should put in place policies, procedures and controls that clearly set out –

(a) the ML/TF information sources used by the financial adviser for screening (including (i) commercial databases and pertinent search engines[6] used to identify adverse information on individuals and entities, (ii) individuals and entities covered under the MAS Regulations issued pursuant to section 27A of the MAS Act and TSOFA, and (iii) individuals and entities identified by other

[6] Where necessary, the financial adviser should conduct screening in the native language(s) of the person screened and on pertinent search engines used in countries or jurisdictions closely associated with the person screened.

sources such as the financial adviser's head office or parent supervisory authority, lists and information provided by the Authority and relevant authorities in Singapore);

(b) the roles and responsibilities of the financial adviser'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 financial adviser'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 financial adviser's employees for reporting positive hits to the financial adviser'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 financial adviser's business. A financial adviser 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 financial adviser 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 financial adviser'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 financial adviser 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 financial adviser 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 6.38(c) of the Notice, a financial adviser 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 the 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 financial adviser 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 financial adviser's customer database for periodic name screening purposes. This will help the financial adviser to promptly identify any existing customers who have subsequently become higher risk parties.

6-15-8 The financial adviser should ensure that it has adequate arrangements to perform screening of the financial adviser's customer database when there are changes to the lists of sanctioned individuals and entities, covered by the TSOFA, MAS Regulations issued under section 27A of the MAS Act[7] and MAS Notice MA-N-EXT1/2012 ("Prohibition on Transactions with the Iranian Government and with Iranian Financial Institutions"). The financial adviser should implement "four-eye checks" on alerts from sanction reviews before closing an alert, or conduct quality assurance checks on the closure of such alerts on a sample basis.

[7] Please refer to the following link for the relevant MAS ML/TF Regulations - http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-FinancialSanctions/Targeted-Financial-Sanctions/MAS-Regulations.aspx

7 Notice Paragraph 7 – Simplified Customer Due Diligence

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

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

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

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

(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 financial adviser'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 financial adviser 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 financial adviser;

(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 financial adviser and the customer);

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

(vi) cash-intensive businesses; and

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

(i) unclear economic purpose for requiring account relationship in Singapore:

(i) E.g. foreign-incorporated companies with no business presence or activities in Singapore seek to open accounts in Singapore (including through a nominee arrangement);

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

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

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

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

(v) suspicious transactions which are not in line with the financial adviser'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 financial adviser is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its customers 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 un-associated third parties.

8-3 When considering the ML/TF risks presented by a country or jurisdiction, a financial adviser 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 financial adviser 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 financial adviser may rely on information available from public sources and information obtained through customer interaction.

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

8-4-5 Examples of persons who are or have been entrusted with prominent functions by an international organisation are members of senior management such as directors, deputy directors and members of the board or equivalent functions. Other than relying on information from a customer, the financial adviser 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 financial adviser determines that any natural person appointed to act on behalf of a customer or any connected party of a customer is a PEP, the financial adviser should assess the ML/TF risks presented and consider factors such as the level of influence that the PEP has on the customer. Financial advisers 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 financial adviser should apply ECDD measures on the customer accordingly.

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

8-5-4 In relation to paragraph 8.3(b) of the Notice, a financial adviser 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 financial adviser should note that not all declarations are publicly available. A financial adviser 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 ~~This~~ relates to how the customer and beneficial owner have acquired the wealth, which is distinct from identifying the assets that they own. Source of wealth information obtained by the financial adviser should give an indication, to the extent practicable, about the entire body ~~size~~ of wealth that the customer and beneficial owner would be expected to have, and how the customer and beneficial owner acquired the wealth. This would enable the financial adviser to determine the sources of wealth of the customer and beneficial owner that are material and/or present a higher risk for ML/TF. Although the financial adviser may not have specific information about assets that are not processed by the financial adviser, it may be possible to obtain general information from the customer, commercial databases or other open sources. ~~Examples of appropriate and reasonable means of establishing source of wealth are information and documents such as evidence of title, copies of trust deeds, audited accounts, salary details, tax returns and bank statements.~~

8-5-6 Source of funds refers to the origin of the particular funds or other assets which are the subject of the establishment of business relations (e.g. the amounts being invested, deposited, or wired as part of the business relations). In order to ensure that the funds are not proceeds of crime, the financial adviser 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 financial adviser should corroborate the information ~~Based on its risk assessment of the PEP, a financial adviser should consider whether the information~~ regarding source of wealth and source of funds ~~should be corroborated~~. In relation to paragraph 8.3(b) of the Notice, examples of "appropriate and reasonable means" for establishing source of wealth or source of funds are financial statements of the legal person or legal arrangement owned or controlled by the PEP, site visits, a copy of the will (in cases where the source of wealth or funds is an inheritance), ~~and~~ conveyancing documents (in cases where the source of wealth or funds is a sale of property) and credible public information sources. A financial adviser 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 financial adviser 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 financial adviser 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 financial adviser's basis for using such information should be documented and reviewed periodically. The financial adviser 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 financial adviser 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 financial adviser 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 financial adviser 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 financial adviser should also assess the plausibility of the third party's source of wealth as part of the assessment. Where unable to do so, the financial adviser 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 financial adviser 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 financial adviser has obtained. Where the financial adviser is unable to ascertain the plausibility and legitimacy of the customer or beneficial owner's source of wealth or source of funds, the financial adviser 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 financial adviser finds information containing allegations of wrongdoing by a customer or a beneficial owner of a customer, the financial adviser should assess how this affects the level of risk associated with the business relations; and

(c) commissioning external intelligence reports where it is not possible for a financial adviser 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 financial adviser 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 financial adviser 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 financial adviser's assessment that the business relations or transactions with the customer present higher ML/TF risks, the financial adviser 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 financial adviser 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 financial adviser may refer to the preceding paragraphs 8-5-8 of these Guidelines for further guidance on the ECDD measures to be performed. A financial adviser 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 financial adviser 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 financial adviser 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, the financial adviser shall assess them as presenting higher ML/TF risks. For such customers, the financial adviser shall ensure that the ECDD measures performed are commensurate with the risks. For customers highlighted in paragraph 8.6(b) of the Notice, a financial adviser shall assess whether any such customer presents a higher risk for ML/TF and ensure that the measures under paragraph 6 of the Notice, or ECDD measures where the financial adviser assesses the customer to present a higher risk for ML/TF, performed are commensurate with the risk.

[9] For example, the financial adviser may assess whether source of wealth corroboration against additional documentary evidence is necessary, where the financial adviser'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.

8-6-3 With reference to paragraph 8.6(a) of the Notice, a financial adviser should refer to the FATF Public Statement on High Risk and Non-Cooperative Jurisdictions on which FATF has called for counter-measures [10] . FATF updates this Public Statement on a periodic basis and financial advisers should regularly refer to the FATF website for the latest updates[11].

8-6-4 For higher risk business[12] which inherently presents higher ML/TF risks, a financial adviser should, regardless of the financial adviser's internal risk classification of the customer, refer to the sound practices highlighted in the MAS Information Paper, "Guidance on Private Banking Controls"[13]. 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 financial adviser conducts periodic reviews of such customers; and

(d) where the financial adviser is aware of customers having a common beneficial owner or a customer having multiple accounts with the financial adviser, the financial adviser 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, financial advisers 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, financial advisers should conduct enhanced monitoring and where appropriate, discontinue the relationship. If the financial adviser is inclined to retain the customer, approval shall be obtained from senior management with the substantiating reasons properly documented, and the

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

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

[12] This includes, but is not limited to, the offering of personalised wealth management services, financial advisory services and financial products to high-net-worth individuals.

[13] http://www.mas.gov.sg/news-and-publications/monographs-and-information-papers/2014/guidance-on-private-bankingcontrols.aspx

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 financial adviser. 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 financial adviser, in accordance with the financial adviser's AML/CFT policies, procedures and standards, and is subject to the financial adviser's control measures to effectively implement the financial adviser's AML/CFT procedures.

9-4 The financial adviser may take a variety of measures, where applicable, to satisfy the requirements in paragraphs 9.2(a) and 9.2(b) of the Notice, including –

(a) referring to any independent and public assessment of the overall AML/CFT regime to which the third party is subject, such as the FATF's or 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 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; and

(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 financial adviser 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 financial adviser's business relations with the customer or the completion of transactions undertaken.

9-6 Paragraph 9.3 of the Notice prohibits the financial adviser 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 apply to the outsourcing of the ongoing monitoring process by a financial adviser, including to its parent entity, branches and subsidiaries. A financial adviser may outsource the first-level review of the alerts from the transaction monitoring systems, or sanctions reviews, to another party. However, the financial adviser remains responsible for complying with ongoing monitoring requirements under the Notice.

12 Notice Paragraph 12 – Suspicious Transactions Reporting

12-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 financial adviser 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.

12-1 A financial adviser 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, ~~and should not exceed 15 business days of the case being referred by the relevant employee, representative or officer,~~ unless the circumstances are exceptional or extraordinary. In cases involving sanctioned parties[14] and parties acting on behalf of or under the direction of sanctioned parties[15], a financial adviser should file the STRs as soon as possible, no later than 1 business day after suspicion was first established.

12-2 A financial adviser should note that an STR filed with STRO would also meet the reporting obligations under the TSOFA.

12-3 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 financial adviser 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.

12-4 Once suspicion has been raised in relation to a customer, business relations with a customer or any transaction undertaken in the course of business relations for that customer, in addition to reporting the suspicious activity, a financial adviser should ensure that appropriate action is taken to adequately mitigate the risk of the

[14] "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.

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

financial adviser being used for ML/TF activities. This may include strengthening its AML/CFT processes. This may also include a review of either the risk classification of the customer, or the business relations with the customer. Other aAppropriate action that should be taken~~,~~ include ~~including~~ 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 financial adviser should assess if the filing of a further or supplementary STR to report the further suspicion is warranted.

12-5 STR reporting templates are available on CAD's website[16]. However, financial advisers are strongly encouraged to use the online system provided by STRO to lodge STRs. In the event that the financial adviser 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 financial adviser should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct.

12-6 A financial adviser 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.

12-7 Financial advisers are reminded to read paragraph 12.4 of the Notice together with paragraphs 6.33 and 6.34 of the Notice. Where a financial adviser stops performing CDD measures as permitted under paragraph 12.4 and is as a result unable to complete CDD measures (as specified under paragraph 6.34), the financial adviser is reminded that it shall not commence or continue business relations with that customer or undertake any transaction for that customer.

[16] The website address as at 24 April 2015:
http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting

13 Notice Paragraph 13 – Internal Policies, Compliance, Audit and Training

13-1 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 financial adviser update its policies and procedures in a timely manner, to take into account new operational, legal and regulatory developments and emerging or new ML/TF risks.

Notice Paragraphs 13.3 to 13.9

13-2 Group Policy

13-2-1 For the avoidance of doubt, Singapore branches of financial advisers incorporated outside Singapore need not comply with paragraphs 13.4 to 13.9 of the Notice. Paragraphs 13.3 to 13.9 of the Notice are intended to be applied by a financial adviser incorporated in Singapore to its branches and subsidiaries, but not to its parent entity and the financial adviser's other related corporations.

13-2-2 In relation to paragraph 13.6 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 financial adviser, 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 financial adviser incorporated in Singapore with the financial adviser's group level compliance, audit, and AML/CFT functions (whether in or outside Singapore), for risk management purposes.

Notice Paragraphs 13.10 to 13.11

13-3 Compliance

13-3-1 A financial adviser should ensure that the AML/CFT compliance officer has the necessary seniority and authority within the organisation to effectively perform his responsibilities.

13-3-2 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 MAS Regulations issued under section 27A of the MAS Act, and taking overall charge of all AML/CFT matters within the organisation;

(c) informing employees, 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 financial adviser's compliance with the Notice and these Guidelines, as well as the MAS Regulations issued under section 27A of the MAS Act and risk assessment procedures; and

(h) reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection, and compliance reviews, to the financial adviser's senior management, and in the case of locally incorporated financial advisers, to the board of directors, at least annually and as and when needed.

13-3-3 The business interests of a financial adviser 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 financial adviser's management.

Notice Paragraph 13.12

13-4 Audit

13-4-1 A financial adviser'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 an organisation-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 financial adviser'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.

13-4-2 The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the financial adviser's business.

Notice Paragraph 13.13

13-5 Employee and Representative Hiring

13-5-1 The screening procedures applied when a financial adviser in Singapore hires employees and appoints representatives and officers should include –

(a) background checks with past employers;

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

(c) bankruptcy searches.

13-5-2 In addition, a financial adviser should conduct credit history checks, on a risk-based approach, when hiring employees and appointing officers and representatives.

Notice Paragraph 13.14

13-6 Training

13-6-1 As stated in paragraph 13.14 of the Notice, it is a financial adviser'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 financial adviser 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.

13-6-2 Apart from the initial training, a financial adviser 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 financial adviser should maintain the training records for audit purposes.

13-6-3 A financial adviser should monitor the effectiveness of the training provided to its employees and representatives. This may be achieved by –

(a) testing employees' and representatives' understanding of the financial adviser'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' and representatives' compliance with the financial adviser's AML/CFT policies, procedures and controls as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action taken; and

(c) monitoring attendance and following-up with employees and representatives who miss such trainings without reasonable cause.

Endnotes on History of Amendments

1. Guidelines to MAS Notice FAA-N06 dated 2 July 2007.
2. Guidelines to MAS Notice FAA-N06 dated 2 July 2007 cancelled with effect from 24 May 2015.
3. Guidelines to MAS Notice FAA-N06 dated 24 April 2015 with effect from 24 May 2015.
   (a) Amended on 30 November 2015.
   (b) Amended on DD MM 2025.

I Other Key Topics - Guidance to Financial Advisers on Proliferation Financing

I-1 Overview

I-1-1 MAS issues Regulations under section 27A of the MAS Act in order to discharge or facilitate the discharge of any obligation binding on Singapore by virtue of a United Nations Security Council Resolution ("UNSCR")~~[17]~~ adopted by the United Nations Security Council ("UNSC"). These Regulations apply to all FIs (including financial advisers) regulated by MAS and generally impose financial sanctions on designated persons.

I-1-2 Specifically, the UNSC ~~a UNSCR~~ may designate certain individuals and entities involved in the proliferation of weapons of mass destruction and its financing. The relevant information and full list~~ing~~s of persons designated by the UNSC ~~UNSCRs~~ can be found at ~~on~~ the UNSC's website[18].

I-1-3 MAS has given effect to UNSCRs as listed in ~~by~~ the FATF Recommendations (2012) to be relevant to combating proliferation financing by issuing Regulations. Examples of such Regulations are the MAS (Sanctions and Freezing of Assets of Persons – Iran) Regulations 2007, MAS (Freezing of Assets of Persons – Democratic People's Republic of Korea) Regulations 2009 and MAS (Sanctions – Democratic People's Republic of Korea) Regulations 2009.

I-1-4 A financial adviser 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 financial adviser should also ensure compliance with legal instruments issued by MAS relating to proliferation financing risks. An example is the MAS' Notice on Prohibition on Transactions with the Iranian Government and with Iranian Financial Institutions.

I-2 CDD and Internal Controls

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

~~[17] Please refer to the MAS website for a full listing of Regulations issued by MAS pursuant to the United Nations Security Council Resolutions.~~

[18] Please see: https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list ~~http://www.un.org/sc/committees/1718 and http://www.un.org/sc/committees/1737.~~

I-2-2 A financial adviser should also have policies and procedures to detect attempts by its employees, officers or representatives to circumvent the applicable laws and regulations (including the MAS Regulations), such as –

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

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

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

I-3 Obligation of Financial Adviser to Freeze without Delay

I-3-1 A financial adviser is reminded of its obligations under the MAS Regulations issued under section 27A of the MAS Act[19] to immediately freeze any funds, financial assets or economic resources owned or controlled, directly or indirectly, by designated persons that the financial adviser has in its possession, custody or control. The financial adviser 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 ~~in such cases~~.

I-4 Potential Indicators of Proliferation Financing

I-4-1 A financial adviser 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;

[19] Please refer to the following link for the relevant MAS ML/TF Regulations - http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-FinancialSanctions/Targeted-Financial-Sanctions/MAS-Regulations.aspx

(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 ~~indicators~~).

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 financial adviser may wish to refer to the FATF website for additional information.

II Useful Links

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

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 financial adviser • 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 customer's visit to the customer's place of business, where the financial adviser 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 financial adviser • 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 financial adviser's visit to customer's place of business, where the financial adviser assesses it as necessary • Ownership and control structure • Records in an independent company registry • Partnership deed • The customer's membership with a relevant professional body • Any association the entity may have with other countries or jurisdictions (e.g. the location of the entity's headquarters, operating facilities, branches, subsidiaries)
Companies	• Full name of entity • Business address or principal place of business • Information about the purpose and intended nature of the business relations with the financial adviser • Names of all natural persons who act on behalf of the

Customer Type	Examples of CDD Information
	entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the financial adviser's visit to customer's place of business, where the financial adviser 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 financial adviser • 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 financial adviser • 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 customer's place of business, where the financial adviser assesses it as necessary • Board resolution authorising the opening of the customer's account with the financial adviser

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 financial adviser • 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 financial adviser's visit to the customer's place of business, where the financial adviser 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 financial adviser • 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 financial adviser's visit to the customer's place of business, where the financial adviser assesses it as necessary • Information about the purpose and intended nature of business relations with the financial adviser • 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 ~~settlors/trustees/beneficiaries or any person who has power over the disposition of any property that is subject to the trust~~ 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 or TF is taking place, a combination of such situations may be indicative of a suspicious transaction. The list is intended solely as an aid, and must not be applied as a routine instrument in place of common sense.

B-1-2 The list is not exhaustive and may be updated due to changing circumstances and new methods of laundering money or financing terrorism. Financial advisers are to refer to STRO's website for the latest list of red flags[20].

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 financial adviser in the course of the business relations. Financial advisers 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 financial adviser 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 investing predominantly in blue chip stocks to penny stocks.

ii) A customer relationship with the financial adviser where the customer carries out frequent large transactions which are beyond the customer's apparent financial means (for example, customer requests for a single premium contract with large sum assured).

iii) Transactions where the nature, size or frequency appears unusual, for example, a sudden request for a significant purchase of a lump sum contract from an existing customer whose current contracts are small and of regular payment only.

[20] The website address as at 24 April 2015:
http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting

iv) Transactions in which funds are received by way of a third party cheque, especially where there is no apparent connection between the third party and the customer.

v) Transactions which, without plausible reason, result in the intensive use of what was previously a relatively inactive account.

vi) Request by a customer for financial advisory services where the source of funds is unclear or not consistent with the customer's apparent standing.

B-3 Transactions Involving Large Amounts of Cash

i) 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).

ii) Customers whose funds contain counterfeit notes or forged instruments.

iii) Transactions in which funds are received from or paid to a customer's bank account in a financial haven, or in foreign currency, especially when such transactions are not consistent with the customer's transaction history.

iv) Overpayment of premiums with a request to refund the excess to a third party or to a bank account held in a different country.

B-4 Transactions Involving Accounts of the Customer with the Financial Advisers

i) Paying in large third party cheques endorsed in favour of the customer in settlement for investment services rendered, or for other financial services provided.

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

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

iv) 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) A customer introduced by an overseas FI, affiliate or other customer, where both the customer and introducer are based in countries or jurisdictions associated with (a) the production, processing or marketing of narcotics or other illegal drugs; or (b) other criminal conduct.

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

B-6 Transactions Involving Unidentified Parties

i) A customer, who is a natural person, for whom verification of identity proves unusually difficult and who is reluctant to provide details.

ii) A customer, which is a corporation, where there are difficulties and delays in obtaining copies of the financial accounts or other documents of incorporation.

iii) Assignment of a policy to unidentified third parties and for which no plausible reasons could be ascertained.

iv) A number of policies taken out by the same customer for low premiums, each purchased with cash and then cancelled with return of premiums to a third party.

B-7 Tax Crimes Related Transactions

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

ii) Unconvincing or unclear purpose or motivation for having accounts opened in Singapore

iii) 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.

iv) Life insurance solutions used for illegal purposes.

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

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

vii) Purchase of bank cheques on a large scale by an interim customer.

viii) Participation in a Tax Amnesty Programme ("TAP")[21]

B-8 Other Types of Transactions

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

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

iii) Frequent changes to the address or authorised signatories.

iv) A large amount of funds is received and immediately used as collateral for investment.

v) 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.

vi) 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.

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

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

[21] If a customer participates in a TAP, a bank 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 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.