Monetary Authority of Singapore

GUIDELINES TO MAS NOTICE SFA03AA-N01 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

3 JANUARY 2016

TABLE OF CONTENTS

For ease of reference, the chapter numbers in these Guidelines mirror the corresponding paragraph numbers in the Notice [MAS Notice SFA03AA-N01 on Prevention of Money Laundering and Countering the Financing of Terrorism – the Depository] (e.g. Chapter 2 of the Guidelines provides guidance in relation to paragraph 2 of the Notice). Not every paragraph in the Notice has a corresponding paragraph in these Guidelines and this explains why not all chapter numbers are utilised in these Guidelines.

GUIDELINES TO MAS NOTICE SFA03AA-N01 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

1 Introduction

1-1 These Guidelines provide guidance to the Depository on the requirements in MAS Notice SFA03AA-N01 on Prevention of Money Laundering and Countering the Financing of Terrorism – the Depository ("the Notice"). These Guidelines should be read in conjunction with the Notice.

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

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

1-4 Key Concepts

Money Laundering

1-4-1 Money laundering ("ML") is a process intended to mask the benefits derived from criminal conduct so that they appear to have originated from a legitimate source. Singapore's primary legislation to combat ML is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A). The Depository 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 transfers 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. The Depository is reminded of the definitions of terrorism set out in the Terrorism (Suppression of Financing) Act (Cap. 325) ("TSOFA") and the United Nations (Anti-terrorism Measures) Regulations (Rg. 1).

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

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

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

The Three Lines of Defence

1-4-7 The Depository 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 The Depository's board of directors and senior management are responsible for ensuring strong governance and sound AML/CFT risk management and controls at the Depository. While certain responsibilities can be delegated to senior AML/CFT employees, final accountability rests with the Depository's board of directors and senior management. The Depository should ensure a strong compliance culture throughout its organisation, where the 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. 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 transfers or applications or deploy systems or technology. The third line of defence is the Depository'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 Depository's policies, procedures and controls on AML/CFT should be clearly specified in writing, and communicated to all relevant employees and officers in the business units. The Depository should adequately train employees and officers to be aware of their obligations, and provide instructions as well as guidance on how to ensure the Depository'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 Depository's fulfilment of all AML/CFT duties by the Depository. This implies sample testing and the review of exception reports. The AML/CFT compliance function should alert the Depository'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 Depository 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 Depository'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 Depository'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 Depository's compliance with prevailing AML/CFT policies, procedures and controls. The Depository should establish policies for periodic AML/CFT internal audits covering areas such as —

(a) the adequacy of the Depository'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 Depository's employees and officers in implementing the Depository's policies, procedures and controls;

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

(d) the effectiveness of the Depository's training of relevant employees and officers.

Governance

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

1-4-14 The Depository's board of directors and senior management should understand the ML/TF risks the Depository is exposed to and how the Depository's AML/CFT

control framework operates to mitigate those risks. This should involve the board and senior management —

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

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

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

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

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

Customer

2-3 For the avoidance of doubt, the definition of "customer" for the purposes of the Notice includes any natural person, legal person or legal arrangement that withdraws a share scrip, to effect a transfer or an intention to transfer, to another Depository account or other equivalent account in Singapore or elsewhere.

2-4 When performing Customer Due Diligence ("CDD") measures in the scenarios below, the following approaches may be adopted:

(a) Portfolio Managers

The Depository 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 the Depository 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 Depository. In such circumstances, the Depository should evaluate the risks arising from each case and determine the appropriate CDD measures to take. The Depository 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 Depository is exempted from making inquiries about the existence of such underlying investors (i.e. beneficial owners). Therefore, the Depository does not need to identify and verify such underlying investors.

Legal Arrangements

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

Legal Persons

2-6 In relation to the definition of "legal person" in the Notice, examples of legal persons are companies, bodies corporate, foundations, anstalt, partnerships, joint ventures or associations.

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, the Depository shall identify and assess ML/TF risks on an enterprise-wide level. This shall include a consolidated assessment of the Depository's ML/TF risks that exist across all its business units, product lines and delivery channels.

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

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

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

(a) in relation to its customers —

(i) target customer markets and segments;

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

(iii) volume and size of its customers' transfers, considering the usual activity and the risk profile of its customers;

(b) in relation to the countries or jurisdictions its customers are from or in —

(i) countries or jurisdictions the Depository is exposed to, or the activities of its customers (including the Depository's network of correspondent accounts), 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 Non-cooperative jurisdictions;

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

- the AML/CFT laws, regulations and standards of the country or jurisdiction;

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

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

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

(c) in relation to the products, services, transfers and delivery channels of the Depository —

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

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

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

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

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

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

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

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

4-12 The NRA also identifies certain prevailing crime types as presenting higher ML/TF risks. The Depository should consider these results when assessing its enterprise-wide ML/TF risks of products, services, transfers and delivery channels and whether they are more susceptible to the higher risk prevailing crime types. Where appropriate, the Depository should also take these results into account as part of the Depository's ongoing monitoring of the conduct of customers' accounts and the Depository's scrutiny of transfers.

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 Depository's enterprise-wide ML/TF risk assessment. The Depository shall put in place adequate policies, procedures and controls to mitigate the ML/TF risks.

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

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

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

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

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

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

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

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

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

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

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

Documentation

4-16 The documentation should include —

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

(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 The Depository should also 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, the Depository 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 Depository. The results of these reviews should be documented and approved by senior management even if there are no significant changes to the Depository'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. The Depository shall keep abreast of such new developments and the ML/TF risks associated with them.

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

5-3 An example of "new delivery mechanism" as set out in paragraph 5 of the Notice is to allow customers to request for off-market transfers via the internet or mobile devices.

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

6-1-1 In arriving at its decision for each case, the Depository 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 The Depository should formulate scenarios and parameters for unusual transfers and monitor related or linked transfers.

6-2-2 Two or more transfers may be related or linked if they involve the same customer.

Notice Paragraphs 6.4 to 6.17

6-3 CDD Measures

6-3-1 When relying on documents, the Depository 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 The Depository should exercise greater caution when dealing with an unfamiliar or new customer. Apart from obtaining the identification information required by paragraph 6.5 of the Notice, the Depository should (if not already done 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 Depository and whether the customer holds or has held a prominent public function. Such additional identification information enables the Depository to obtain a 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) 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 The Depository 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, the Depository is required to identify and screen all the connected parties of a customer. However, the Depository may verify their identities using a risk-based approach [1]. The Depository 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, the Depository shall perform CDD measures on the customer by identifying the settlors, trustees, the protector (if any), the beneficiaries (including every beneficiary that falls within a designated characteristic or class) and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership), as required by paragraph 6.13 of the Notice.

Notice Paragraph 6.8

6-6 Verification of Identity of Customer

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

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

(a) Natural Persons —

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

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

(ii) residential address based on national identity card, recent utility or 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 teed, constitutional document, certificate of registration or any other documentation from a reliable independent source; and

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

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

6-6-4 In exceptional circumstances where the Depository is unable to retain a copy of the documentation used in verifying the customer's identity, the Depository 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 Depository'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 Depository'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 the Depository obtains data, documents or information from the customer or a third party, it should ensure that such data, documents or information is current at the time they are provided to the Depository.

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

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

(b) if a Depository staff independent of the customer relationship can confirm that he has sighted the original document.

6-6-7 Where a document is in a foreign language, appropriate steps should be taken by the Depository to be reasonably satisfied that the document does in fact provide evidence of the customer's identity. The Depository 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 Depository may rely on a translation of such document by a Depository staff independent of the customer relationship who is conversant in that foreign language. This is to allow all employees and officers of the Depository involved in the performance of any measures 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 Depository 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 Persons Appointed to Act on 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 Depository should verify at a minimum those natural persons to whom the customer has assigned the authority to operate the customer's account with the Depository or move securities in and out of that account.

Notice Paragraphs 6.12 to 6.16

6-8 Identification and Verification of Identity of Beneficial Owners

6-8-1 The Depository 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 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 The Depository 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 Depository 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, the Depository should obtain enough information to sufficiently understand if there are legitimate reasons for such ownership or control structure.

6-8-6 The Depository should take particular care when dealing with companies with bearer shares, since the beneficial ownership is difficult to establish. For such companies, the Depository should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the Depository is notified whenever there is a change of beneficial owner of such shares . At a minimum, these procedures should require the Depository to obtain an undertaking in writing from the beneficial owner of such bearer shares stating that the Depository 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 Depository may require that the bearer shares be held by a named custodian, with an undertaking from the custodian that the Depository 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 Depository should put in place an internal assessment process with clear criteria, taking into account, amongst

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

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

6-8-10 Where a customer is one which falls within paragraph 6.15 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 the Purpose and Intended Nature of Business Relations

6-9-1 The measures taken by the Depository 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, the Depository should seek to understand upfront the expected account activity (e.g. types of transfers 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 transfers.

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

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

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

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

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

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

6-10-5 Examples of trigger events are when (i) a significant transfer takes place, (ii) a material change occurs in the way the customer's account is operated, (iii) the Depository's procedures, policies or standards relating to the documentation of CDD information change substantially, and (iv) the Depository becomes aware that it lacks sufficient information about the customer concerned.

6-10-6 The frequency of CDD review may vary depending on each customer's risk profile. Higher risk customers should be subject to more frequent periodic review (e.g. on an annual basis) to ensure that CDD information such as nationality, passport details, certificate of incumbency, ownership and control information that the Depository has previously obtained remain relevant and up-to-date.

6-10-7 In determining what would constitute suspicious, complex, unusually large or unusual pattern of transfers, the Depository 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, the Depository should pay attention to transfer characteristics, such as —

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

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

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

6-10-8 The Depository's transfer 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 Depository's operations.

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

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

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

6-10-12 The parameters and thresholds used by the Depository to identify suspicious transfers should be properly documented and independently validated to ensure that they are appropriate to its operations and context. The Depository 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 Measures 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 transfers according to instructions conveyed by customers over the internet, post, fax or telephone. The Depository should note that applications and transfers 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 transfers,

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

6-11-2 The measures taken by the Depository for verification of an identity in respect of non-face-to-face business relations with or transfers 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), the Depository should apply additional checks to manage the risk of impersonation. The additional checks may consist of robust anti-fraud checks that the Depository routinely undertakes as part of its existing procedures, which may include —

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

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

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

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

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

Notice Paragraph 6.29

6-12 Reliance by the Depository on Measures Already Performed

6-12-1 When the Depository 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. The Depository 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, the Depository is responsible for its obligations under the Notice.

6-12-3 When the Depository acquires the business of another FI, either in whole or in part, the Depository 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 Paragraph 6.33

6-13 Existing Customers

6-13-1 In relation to customer accounts which pre-date the coming into force of the current Notice, the Depository should prioritise the remediation of higher risk customers.

6-13-2 In taking into account any previous measures as referred to in paragraph 6.33 of the Notice, the Depository should consider whether —

(a) there has been any significant transfer 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 CDD 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 may be 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 Depository.

Notice Paragraphs 6.34 to 6.36

6-14 Screening

6-14-1 Screening is intended to be a preventive measure. The Depository is reminded that all parties identified pursuant to the Notice are required to be screened, irrespective of the risk profile of the customer.

6-14-2 Where screening results in a positive hit against sanctions lists, the Depository is reminded of its obligations to freeze without delay and without prior notice, the funds or other assets of designated persons and entities that it has control over, so as to comply with applicable laws and regulations in Singapore, including the TSOFA and MAS Regulations issued under section 27A of the Monetary Authority of Singapore Act (Cap. 186) ("MAS Act") relating to sanctions and freezing of assets of persons. Any such assets should be reported promptly to the relevant authorities and an Suspicious Transaction Report ("STR") should be filed.

6-14-3 The Depository should put in place policies, procedures and controls that clearly set out —

(a) the ML/TF information sources used by the Depository for screening (including commercial databases used to identify adverse information on individuals and entities, individuals and entities covered under MAS Regulations issued pursuant to section 27A of the MAS Act, individuals and entities identified by other sources such as the Depository'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 Depository's employees and officers involved in the screening, reviewing and dismissing of alerts, maintaining and updating of the various screening databases and escalating hits;

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

(d) the frequency of periodic screening;

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

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

6-14-4 The level of automation used in the screening process should take into account the nature, size and risk profile of the Depository's business. The Depository 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 Depository 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 Depository's employees and officers may need to exercise their judgment in identifying true hits.

6-14-5 The Depository 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 Depository becomes aware of such breaches, it should immediately take the necessary actions and inform the relevant authorities.

6-14-6 In screening periodically as required by paragraph 6.35(b) of the Notice, the Depository should pay particular attention to changes in customer status (e.g. whether the customer has over time become subject to prohibitions and sanctions) or customer risks (e.g. a connected party of a customer, a beneficial owner of the customer or a natural person appointed to act on behalf of the customer subsequently becomes a Politically Exposed Person or presents higher ML/TF risks, or a customer subsequently becomes a Politically Exposed Person

or presents higher ML/TF risks) and assess whether to subject the customer to the appropriate ML/TF risk mitigation measures (e.g. enhanced CDD measures).

6-14-7 The Depository 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 Depository's customer database for periodic name screening purposes. This will enable the Depository to promptly identify any existing customers who have subsequently become higher risk parties.

6-14-8 In determining the frequency of periodic name screening, the Depository should consider its customers' risk profile.

6-14-9 The Depository should ensure that it has adequate arrangements to perform screening of the Depository'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[2] and MAS Notice MA-N-EXT 1/2012 ("Prohibition on Transactions with the Iranian Government and with Iranian Financial Institutions. The Depository should implement "four-eye checks" on alerts from sanctions reviews before closing an alert, or conduct quality assurance checks on the closure of such alerts on a sample basis.

[2] 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-Financial-Sanctions/Targeted-Financial-Sanctions/MAS-Regulations.aspx

7 Notice Paragraph 7 – Simplified Customer Due Diligence

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

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

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

7-4 Where the Depository is satisfied that the risks of money laundering and terrorism financing are low, the Depository 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 scrutinising of transfers, based on a reasonable monetary threshold; or

(c) choosing another method to understand the purpose and intended nature of business relations by inferring this from the type of transfers 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 the Depository'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.

8 Notice Paragraph 8 – Enhanced Customer Due Diligence

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

8-2 Examples of potentially higher risk categories under paragraph 8.5 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 Depository;

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

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

(vi) cash-intensive businesses.

(b) Country or geographic risk

(i) countries or jurisdictions the Depository is exposed to, either through its own activities or the activities of its customers (including the Depository's network of correspondent account relationships) which have relatively higher levels of corruption, organised crime or inadequate AML/CFT measures, as identified by 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.

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

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

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

8-5-5 Source of wealth generally refers to the origin of the customer's and beneficial owner's entire body of wealth (i.e. total assets). This relates to how the customer and beneficial owner have acquired the wealth which is distinct from identifying the assets that they own. Source of wealth information should give an indication about the size of wealth the customer and beneficial owner would be expected to have, and how the customer and beneficial owner acquired the wealth. Although the Depository may not have specific information about assets not custodised at the Depository, 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 securities deposited, or transferred as part of the business relations). The information obtained should be substantive and facilitate the establishment of the provenance of the funds or reason for the funds having been acquired. Examples of appropriate and reasonable means of establishing source of funds are information such as salary payments or sale proceeds.

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

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

(a) 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 Depository finds information containing allegations of wrongdoing by a customer or a beneficial owner of a customer, the Depository should assess how this affects the level of risk associated with the business relations;

(b) commissioning external intelligence reports where it is not possible for the Depository 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 Depository assesses that the business relationship or transfers with a domestic PEP or an international organisation PEP does not present higher ML/TF risks and that therefore ECDD measures need not be applied, the Depository 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 Depository's assessment that the business relationship or transfers with the customer presents higher ML/TF risks, the Depository 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 Depository 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 (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, the Depository may refer to the preceding paragraph 8-5-8 of these Guidelines for further guidance on the ECDD measures to be performed.

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

8-6-3 With reference to paragraph 8.6(a) of the Notice, the Depository should refer to the FATF Public Statement on High Risk and Non-Cooperative Jurisdictions on which FATF has called for counter-measures[3]. FATF updates this Public Statement on a periodic basis and the Depository should regularly refer to the FATF website for the latest updates[4].

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

8-6-5 With regard to tax and other serious crimes, as a preventive measure, the Depository is expected to reject a prospective customer where there are reasonable grounds to suspect that the customer's assets are the proceeds of a serious crimes, including wilful and fraudulent tax evasion. Where there are grounds for suspicion in an existing customer relationship, the Depository should conduct enhanced monitoring and where appropriate, discontinue the relationship. If the Depository is inclined to retain the customer, approval shall be obtained from senior management with the substantiating reasons properly documented, and the account subjected to close monitoring and commensurate risk mitigation measures. This requirement applies to serious foreign tax offences, even if the foreign offence is in relation to the type of tax for which an equivalent obligation does not exist in Singapore. Examples of tax crime related suspicious transactions are set out in Appendix B of these Guidelines.

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

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

9 Notice Paragraph 9 – Reliance on Third Parties

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

9-2 In a third-party reliance scenario, the third party will typically have an existing relationship with the customer that is independent of the relationship to be formed by the customer with the relying bank. The third party will therefore perform the CDD measures on the customer according to its own AML/CFT policies, procedures and controls.

9-3 In contrast to a third party reliance scenario, the outsourced service provider performs the CDD measures (e.g. performs centralised transfer monitoring functions) on behalf of the Depository, in accordance with the Depository's AML/CFT policies, procedures and standards, and is subject to the Depository's control measures to effectively implement the Depository's AML/CFT procedures.

9-4 The Depository 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 with respect to the laws of the jurisdiction in which the third party operates;

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

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

9-5 The reference to "documents" in paragraph 9.2(d) of the Notice includes a reference to the underlying CDD-related documents and records obtained by the third party to support the CDD measures performed (e.g. copies of identification information, CDD/Know Your Customer forms). Where these documents and records are kept by the third party, the Depository 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 Depository's business relations with the customer or the completion of transfers undertaken.

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

9-7 For avoidance of doubt, paragraph 9 of the Notice does not apply to the outsourcing of the ongoing monitoring process by the Depository to its parent entity. The Depository may outsource the first-level review of alerts from the transfer monitoring systems, or sanctions reviews, to another party. However, the Depository remains responsible for complying with ongoing monitoring requirements under the Notice.

10 Notice Paragraph 10 – Correspondent Accounts

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

10-2 After the Depository obtains adequate information as required by paragraph 10.3(a) of the Notice to establish a correspondent account relationship, such information should continue to be updated on a periodic basis thereafter.

10-3 Other factors that the Depository should consider in complying with paragraph 10.3(a) of the Notice include —

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

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

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

(d) the potential use of the account by other respondent FIs in a "nested" correspondent account relationship[5]; the Depository should review the risks posed by such "nested" relationships.

10-4 To assess the ML/TF risk associated with a particular country or jurisdiction as required by paragraph 10.3(a)(iii) of the Notice, the Depository may rely on information from FATF mutual evaluation reports and statements on countries or jurisdictions identified as either being subject to countermeasures or having strategic AML/CFT deficiencies, mutual evaluation reports by FSRBs, publicly available information from national authorities and any restrictive measures imposed on a country, particularly prohibitions on providing correspondent account services.

10-5 For correspondent account relationships established with the Depository's related entities, the appropriate level of measures as required under paragraphs 6, 7 and 8 of the Notice (as applicable), and paragraph 10 of the Notice should be applied, bearing in mind that the risk profiles of individual entities within the same financial group could differ significantly. the Depository should take into consideration the parent institution's level of oversight and control over these related entities, and other risk factors unique to the entities such as its customers and products, the

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

legal and regulatory environment they operate in, and sanctions by authorities for AML/CFT lapses.

10-6 The CDD process should result in a thorough understanding of the ML/TF risks arising from a relationship with the respondent FI. It should not be treated as a "form-filling" exercise. The Depository's assessment of the respondent FI may be enhanced through meetings with the respondent FI's management and compliance head, respondent FI's regulators and AML/CFT regulators.

10-7 The Depository may apply a risk-based approach in complying with the requirements set out in paragraph 10 of the Notice, but should be mindful that correspondent account relationships generally present higher ML/TF risks.

10-8 If the Depository provides correspondent account services to its related respondent FIs within the same financial group, the Depository should ensure that it still assesses the ML/TF risks presented by its related respondent FI.

10-9 Where the head office of the financial group is incorporated in Singapore, it should monitor the correspondent account relationships between FIs in its financial group, and ensure that adequate information sharing mechanisms within the financial group are in place.

10-10 For the purposes of paragraph 10.6 of the Notice, the Depository should take into account, for example, any sanctions imposed by relevant authorities on a respondent FI for failing to have adequate controls against criminal activities.

10-11 In assessing whether an FI falls within the meaning of "shell FI" for the purposes of paragraph 10 of the Notice, the Depository should note that physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level employees does not constitute physical presence.

13 Notice Paragraph 13 – Suspicious Transactions Reporting

13-1 The Depository should ensure that the internal process for evaluating whether a matter should be referred to the Suspicious Transaction Reporting Office ("STRO") via an STR is completed without delay and should not exceed 15 business days of the case being referred by the relevant employee or officer, unless the circumstances are exceptional or extraordinary.

13-2 The Depository should note that an STR filed with STRO would also meet the reporting obligations under the Terrorist (Suppression of Financing) Act.

13-3 Examples of suspicious transfers 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 transfers should prompt further enquiries and, where necessary investigations, into the source of funds. The Depository should also consider filing an STR if there is any adverse news on its customers in relation to financial crimes. A transfer may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

13-4 Once suspicion has been raised in relation to a customer or any transaction for that customer, in addition to reporting the suspicious activity, the Depository should ensure that appropriate action is taken to adequately mitigate the risk of the Depository being used for ML/TF activities. This may include strengthening its AML/CFT processes. This may include a review of either the risk classification of the customer, or the business relations with the customer. Appropriate action should be taken, including escalating the issue to the appropriate decision making level, taking into account any other relevant factors, such as cooperation with law enforcement agencies.

13-5 STR reporting templates are available on CAD's website [6]. However, the Depository is strongly encouraged to use the online system provided by STRO to lodge STRs. In the event that the Depository 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 Depository should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct.

13-6 The Depository should document all transfers that have been brought to the attention of its AML/CFT compliance function, including transfers 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 transfers escalated by its employees and officers should be properly substantiated and documented.

13-7 The Depository is reminded to read paragraph 13.4 of the Notice together with paragraphs 6.30 and 6.31 of the Notice. Where the Depository stops performing

[6] The website address as at 3 January 2016: http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting.

CDD measures as permitted under paragraph 13.4 and is, as a result, unable to complete CDD measures (as specified under paragraph 6.31), the Depository is reminded that it shall not commence or continue business relations with that customer.

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

14-1 As internal policies and procedures serve to guide employees and officers in ensuring compliance with AML/CFT laws and regulations, it is important that the Depository updates its policies and procedures in a timely manner, to take into account new operational, legal and regulatory developments and emerging or new ML/TF risks.

Notice Paragraphs 14.3 to 14.4

14-2 Compliance

14-2-1 The Depository should ensure that the AML/CFT compliance officer has the necessary seniority and authority within the Depository to effectively perform his responsibilities.

14-2-2 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 MAS Regulations issued under section 27A of the MAS Act, and taking overall charge of all AML/CFT matters within the organisation;

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

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

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

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

(g) reporting to senior management on the outcome of reviews of the Depository's compliance with the Notice and these Guidelines and risk assessment procedures; and

(h) reporting regularly on key AML/CFT risk management and control issues, (including information outlined in paragraph 1-4-14 of the Guidelines), and any necessary remedial actions, arising from audit, inspection, and compliance reviews, to the Depository's senior management at least annually and as and when needed.

14-2-3 The business interests of the Depository 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 Depository's management.

Notice Paragraph 14.5

14-3 Audit

14-3-1 The Depository's AML/CFT framework should be subject to periodic audits, (including sample testing). Such audits should be performed not just on individual business functions but also on a Depository-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 Depository's AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;

(b) reviewing the content and frequency of AML/CFT training programmes, and the extent of employees' and officers' (including senior management's) 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.

The frequency and extent of the audit should be commensurate with the risks of ML/TF and the size and complexity of the Depository's business.

Notice Paragraph 14.6

14-4 Employee Hiring

14-4-1 The screening procedures applied when the Depository in Singapore hires employees and appoints officers should include —

(a) background checks with past employers;

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

(c) bankruptcy searches.

14-4-2 In addition, the Depository should conduct credit history checks, on a risk-based approach, when hiring employees and appointing officers.

Notice Paragraph 14.7

14-5 Training

14-5-1 As stated in paragraph 14.7 of the Notice, it is the Depository's responsibility to provide adequate training for its employees and officers so that they are adequately trained to implement its AML/CFT policies and procedures. The scope and frequency of training should be tailored to the specific risks faced by the Depository and pitched according to the job functions, responsibilities and experience of the employees and officers. New employees and officers should be required to attend training as soon as possible after being hired or appointed.

14-5-2 Apart from the initial training, the Depository should also provide refresher training at least once every two years, or more regularly as appropriate, to ensure that employees and officers are reminded of their responsibilities and are kept informed of new developments related to ML/TF. The Depository should maintain the training records for audit purposes.

14-5-3 The Depository should monitor the effectiveness of the training provided to its employees and officers. This may be achieved by —

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

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

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

I Other Key Topics – Guidance to the Depository 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")[7]. These Regulations apply to all FIs (including the Depository) regulated by MAS and generally impose financial sanctions on designated persons.

I-1-2 Specifically, a UNSCR may designate certain individuals and entities involved in the proliferation of weapons of mass destruction and its financing. The relevant information and full listings of persons designated by UNSCRs can be found on the UN website[8].

I-1-3 MAS has given effect to UNSCRs as listed by the FATF Recommendations (2012) to be relevant to combating proliferation financing, by issuing 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 The Depository should rely on its CDD measures (including screening measures) under the Notice to detect and prevent proliferation financing activities and transactions.

I-1-5 The Depository 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 the Depository, as required under the Notice, is performed against the latest UN listings, as they are updated from time to time. The Depository should have in place policies, procedures and controls to continuously monitor the listings and take necessary follow-up action within a reasonable period of time, as required under the applicable laws and regulations.

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

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

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

(a) omitting, deleting or altering information in payment messages for the purpose of avoiding detection of that information by the Depository itself; and

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

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

I-3 Obligation of the Depository to Freeze without Delay

I-3-1 The Depository is reminded of its obligations under the MAS Regulations issued under section 27A of the MAS Act[9] to immediately freeze any securities owned or controlled, directly or indirectly, by designated persons that the Depository has in its possession, custody or control. The Depository should also file an STR in such cases.

I-4 Potential Indicators of Proliferation Financing

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

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

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

(c) the transaction involves designated persons;

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

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

(f) the transaction involves possible shell companies (e.g. companies that do not have a high level of capitalisation or display other shell company indicators);

[9] Please refer to the following link for the relevant MAS ML/TF Regulations - http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism/Regulations.aspx

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

II Useful Links

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

……

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

Customer Type	Examples of CDD Information
Sole proprietorships	• Full registered business name • Business address or principal place of business • Information about the purpose and intended nature of the business relationship with the Depository • 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 Depository's visit to the customer's place of business, where the Depository 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 relationship with the Depository • 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 Depository's visit to customer's place of business, where the Depository assesses it as necessary • Ownership and control structure • Records in an independent company registry • Partnership deed • Any association the entity may have with other 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 relationship with the Depository • Names of all natural persons who act on behalf of the entity • Names of all connected parties

Customer Type	Examples of CDD Information
	• Names of all beneficial owners • Information about the source of funds • A report of the Depository's visit to the customer's place of business, where the Depository assesses it as necessary • Ownership and control structure • Records in an independent company registry • Certificate of incumbency, certificate of good standing, share register, as appropriate • Memorandum and Articles of Association • Certificate of Incorporation • Board resolution authorising the opening of the customer's account with the bank • Any association the entity may have with other 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 organization) • Business address or principal place of business • Information about the purpose and intended nature of the business relationship with the Depository • 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 Depository's visit to the customer's place of business, where the Depository assesses it as necessary • Board resolution authorising the opening of the customer's account with the Depository
Clubs, Societies and Charities	• Full name of entity • Business address or principal place of business • Information about the purpose and intended nature of business relationship with the Depository • 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

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

APPENDIX B – Examples of Suspicious Transfers

B-1 General Comments

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

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

B-1-3 A customer's declarations regarding the background of such transfers 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 Depository in the course of the business relationship. The Depository 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 Depository to verify.

B-2 Transfers Which Do Not Make Economic Sense

i) Transfers in which securities are withdrawn immediately after being transferred, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

ii) Large amounts of securities transferred into an account, which is inconsistent with the financial standing of the customer.

B-3 Transactions Involving Transfers Abroad

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

[10] The website address as at 3 January 2016: http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting.

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

B-4 Investment-Related Transfers

i) Purchasing of securities to be held by the Depository, where this does not appear appropriate given the customer's apparent standing.

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

B-5 Tax Crimes Related Transfers

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

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

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

iv) Inability to reasonably justify frequent and large transfers from / to a high tax-risk country or jurisdiction.

v) Re-deposit of securities 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.

B-6 Other Types of Transfers

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

ii) Transfers 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) When a young person (aged about 18-26) opens an account and transfers the securities within a short period, which could be an indication of terrorism financing.

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