



Monetary Authority of Singapore

**GUIDELINES TO
MAS NOTICE 3001
ON PREVENTION OF
MONEY LAUNDERING
AND COUNTERING THE
FINANCING OF
TERRORISM**

24 APRIL 2015

Last revised on 9 January 2019

TABLE OF CONTENTS

1	Introduction	1
2	Notice Paragraph 2 – Definitions, Clarifications and Examples	5
4	Notice Paragraph 4 – Assessing Risks and Applying a Risk-Based Approach	6
5	Notice Paragraph 5 – New Products, Practices and Technologies.....	11
6	Notice Paragraph 6 – Customer Due Diligence	12
7	Notice Paragraph 7 – Simplified Customer Due Diligence.....	27 26
8	Notice Paragraph 8 – Enhanced Customer Due Diligence	29 28
9	Notice Paragraph 9 – Reliance on Third Parties.....	35 34
10	Notice Paragraph 10 – Provision of Remittance Services to Financial Institutions or Through Financial Institutions.....	37 36
11	Notice Paragraph 11 – Agency Arrangements	39 38
12	Notice Paragraph 12 – Sending or Receiving Funds by Wire Transfers...	40 39
15	Notice Paragraph 15 – Suspicious Transactions Reporting.....	42 41
16	Notice Paragraph 16 – Internal Policies, Compliance, Audit and Training	44 43
I	Other Key Topics – Guidance to Licensees on Proliferation Financing	47 46
II	Useful Links	50 49
	APPENDIX A – Examples of CDD Information for Customers (Including Legal Persons/Arrangements).....	51 50
	APPENDIX B – Examples of Suspicious Transactions	55 53

For ease of reference, the chapter numbers in these Guidelines mirror the corresponding paragraph numbers in the MAS Notice 3001 on Prevention of Money Laundering and Countering the Financing of Terrorism - Holders of Money-Changer's Licence and Remittance Licence (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 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

1 Introduction

- 1-1 These Guidelines provide guidance to all holders of a money-changer's licence and holders of a remittance licence (hereinafter "licensees") on the requirements in MAS Notice 3001 on Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Money-Changer's Licence and Remittance Licence ("the Notice"). These Guidelines should be read in conjunction with the Notice.
- 1-2 The expressions used in these Guidelines have the same meanings as those found in the Notice, except where expressly defined in these Guidelines or where the context otherwise requires. For the purpose of these Guidelines, a reference to "CDD measures" shall mean the measures as required by paragraphs 6, 7 and 8 of the Notice.
- 1-3 The degree of observance with these Guidelines by a licensee may have an impact on the Authority's overall risk assessment of the licensee, 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). A licensee should refer to the Commercial Affairs Department's ("CAD") website for more information.
- 1-4-2 Generally, the process of ML comprises three stages, namely —
- (a) Placement – The physical or financial disposal of the benefits derived from criminal conduct.
 - (b) Layering – The separation of these benefits from their original source by creating layers of financial transactions designed to disguise the ultimate source and transfer of these benefits.
 - (c) Integration – The provision of apparent legitimacy to the benefits derived from criminal conduct. If the layering process succeeds, the integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate funds.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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. Licensees are 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 licensees should remain vigilant.
- 1-4-6 Singapore’s primary legislation to combat TF is the TSOFA. Licensees may refer to the Inter-Ministry Committee on Terrorist Designation’s (“IMC-TD”) website for more information.

The Three Lines of Defence

- 1-4-7 Each licensee is reminded that the ultimate responsibility and accountability for ensuring compliance with anti-money laundering and countering the financing of terrorism (“AML/CFT”) laws, regulations and notices rests with its board of directors and senior management.
- 1-4-8 A licensee’s board of directors and senior management are responsible for ensuring strong governance and sound AML/CFT risk management and controls at the licensee. While certain responsibilities can be delegated to senior AML/CFT employees, final accountability rests with the licensee’s board of directors and senior management. A licensee should ensure a strong compliance culture throughout its organisation, where the board of directors and senior management set the right tone. The board of directors and senior management should also set a clear risk appetite and ensure a compliance culture where financial crime is not acceptable.
- 1-4-9 Business units (e.g. front office customer-facing functions of the licensee’s business premises) constitute the first line of defence in charge of identifying, assessing and controlling the ML/TF risks of their business. The second line of defence includes the AML/CFT compliance function, as well as other support functions such as operations, human resource or technology, which work together with the AML/CFT compliance function to identify ML/TF risks when they process transactions or applications or deploy systems or technology. The third line of defence is the licensee’s internal audit function or external audit firm appointed by the licensee as set out in paragraph 1-4-12.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- 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 licensee'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 licensee should adequately train employees and officers to be aware of their obligations, and provide instructions as well as guidance on how to ensure the licensee'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 licensee's fulfilment of all AML/CFT duties by the licensee. This implies sample testing and the review of exception reports. The AML/CFT compliance function should alert the licensee's senior management or the board of directors if it believes that the employees or officers of the business units 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 licensee 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 licensee's internal audit 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 licensee'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 licensee's compliance with prevailing AML/CFT policies, procedures and controls. Where there is no internal audit function, the licensee should engage an external audit firm to audit the AML/CFT risk management framework and controls, in the course of auditing the money-changing and/or remittance business for the submission of statutory returns to the Authority, and in so doing, to act as the third line of defence. A licensee should establish policies for periodic AML/CFT internal audits covering areas such as —
- (a) the adequacy of the licensee'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 licensee's employees and officers in implementing the licensee's policies, procedures and controls;
 - (c) the effectiveness of the compliance oversight and quality control including parameters and criteria for transaction alerts; and
 - (d) the effectiveness of the licensee's training of relevant employees and officers.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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 licensee. The board of directors and senior management should ensure that the licensee'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 licensee's employees and officers having a good understanding of the ML/TF risks inherent in the licensee's business.
- 1-4-14 A licensee's board of directors and senior management should understand the ML/TF risks the licensee is exposed to and how the licensee's AML/CFT control framework operates to mitigate those risks. This should involve the board of directors 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 licensee is exposed to through its activities, account relationships and relevant business transactions without an account being opened;
 - (b) receiving sufficient and objective information to assess whether the licensee's AML/CFT controls are adequate and effective;
 - (c) receiving information on legal and regulatory developments and the impact these have on the licensee's AML/CFT framework; and
 - (d) ensuring that processes are in place to escalate important decisions that directly impact the ability of the licensee to address and control ML/TF risks, especially where AML/CFT controls are assessed to be inadequate or ineffective.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

2 Notice Paragraph 2 – Definitions, Clarifications and Examples

Account Relationship

- 2-1 For the avoidance of doubt and, subject to paragraph 6.3 and the ongoing monitoring requirements set out in Part VII of the Notice, a licensee is not required to repeat the identification and verification measures set out in paragraph 6 of the Notice every time the licensee undertakes a transaction for a customer with whom the licensee has an account relationship.

Connected Party

- 2-2 The term “partnership” as it appears in the definition of “connected parties” includes foreign partnerships. The term “manager” as it appears in limb (b) of the definition of “connected parties” takes reference from section 2(1) of the Limited Liability Partnership Act (Cap. 163A) and section 28 of the Limited Partnership Act (Cap. 163B).
- 2-3 Examples of natural persons with executive authority in a company include the Chairman and Chief Executive Officer. An example of a natural person with executive authority in a partnership is the Managing Partner.

Legal Arrangements

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

Legal Persons

- 2-5 In relation to the definition of “legal person” in the Notice, examples of legal persons are companies, bodies corporate, foundations, anstalt, partnerships, joint ventures or associations.

Officer

- 2-6 A reference to “officer” refers to a licensee’s board of directors, senior management or equivalent functions.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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

Countries or Jurisdictions of its Customers

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

Other Relevant Authorities in Singapore

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

Risk Assessment

4-3 In addition to assessing the ML/TF risks presented by an individual customer, a licensee shall identify and assess ML/TF risks on an enterprise-wide level. This shall include a consolidated assessment of the licensee's ML/TF risks that exist across all its business units, product lines and delivery channels. The enterprise-wide ML/TF risk assessment relates to a licensee in the following ways:

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

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

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

4-5 A licensee's senior management shall approve its enterprise-wide ML/TF risk assessment and all employees and officers should give their full support and active co-operation to the enterprise-wide ML/TF risk assessment.

4-6 In conducting an enterprise-wide risk assessment, the broad ML/TF risk factors that the licensee 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;

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- (iii) volumes and sizes of its customers' transactions and funds transfers, considering the usual activities and the risk profiles of its customers.
- (b) in relation to the countries or jurisdictions its customers are from or in, or where the licensee has operations in —
 - (i) countries or jurisdictions the licensee is exposed to, either through its own activities (including where its branches, subsidiaries and agents operate in) or the activities of its customers (including the financial institutions, "FI", with whom the licensee provides remittance services to or engages to facilitate the provision of remittance services), especially countries or jurisdictions with relatively higher levels of corruption, organised crime or inadequate AML/CFT measures, as identified by the Financial Action Task Force ("FATF");
 - (ii) when assessing ML/TF risks of countries and jurisdictions, the following criteria may be considered:
 - 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 International Monetary Fund ("IMF")/World Bank Financial Sector Assessment Programme Reports or Reports on the Observance of Standards and Codes for guidance on the country's or jurisdiction's AML/CFT measures;
 - the AML/CFT laws, regulations and standards of the country or jurisdiction;
 - implementation standards (including quality and effectiveness of supervision) of the AML/CFT regime;
 - whether the country or jurisdiction is a member of international groups that only admit countries or jurisdictions which meet certain AML/CFT benchmarks;
 - contextual factors, such as political stability, maturity and sophistication of the regulatory and supervisory regime, level of corruption, financial inclusion, etc;
- (c) in relation to the products, services, transactions and delivery channels of the licensee —

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- (i) the nature, scale, diversity and complexity of the licensee's business activities;
- (ii) the nature of products and services offered by the licensee; and
- (iii) the delivery channels, including the extent to which the licensee 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 licensee's business.

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

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

4-10 In assessing its overall ML/TF risks, a licensee 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 A licensee should incorporate the results of Singapore's NRA Report into its enterprise-wide ML/TF risk assessment process. When performing the enterprise-wide risk assessment, a licensee should take into account any financial or non-financial sector that has been identified as presenting higher ML/TF risks. A licensee should consider the NRA and its enterprise-wide ML/TF risk assessment results when assessing the ML/TF risks presented by customers from specific sectors.

4-12 The NRA also identifies certain prevailing crime types as presenting higher ML/TF risks. A licensee should consider these results when assessing its enterprise-wide ML/TF risks of products, services, transactions and delivery channels and whether it is more susceptible to the higher risk prevailing crime types. Where appropriate, a licensee should also take these results into account as part of the licensee's ongoing monitoring of the conduct of customers' accounts, and the licensee's scrutiny of customers' transactions undertaken in the course of an account relationship or relevant business transactions undertaken without an account being opened.

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

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

enterprise-wide ML/TF risk assessment. A licensee shall put in place adequate policies, procedures and controls to mitigate the ML/TF risks.

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

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

- (a) the ability to identify changes in a customer profile (e.g. Politically Exposed Persons status) and transactional behaviour observed in the course of its business;
- (b) the potential for abuse of new business initiatives, products, practices and services for ML/TF purposes;
- (c) the compliance arrangements (through its internal audit or quality assurance processes or external review);
- (d) the balance between the use of technology-based or automated solutions with that of manual or people-based processes, for AML/CFT risk management purposes;
- (e) the coordination between AML/CFT compliance and other functions of the licensee;
- (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 licensee's senior management;
- (h) the coordination between the licensee and regulatory or law enforcement agencies; and
- (i) the performance of third parties relied upon by the licensee to carry out CDD measures.

Documentation

4-16 The documentation should include —

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

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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

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

Frequency of Review

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

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

5 Notice Paragraph 5 – New Products, Practices and Technologies

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

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

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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 Account Relationships or Undertaking any Transaction without Opening an Account

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

Notice Paragraphs 6.3 to 6.4

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

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

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

6-2-3 Two or more transactions may be related or linked if they involve the same sender or recipient. A licensee should be aware that transactions may be entered into consecutively to deliberately restructure an otherwise single transaction, with the intention of circumventing applicable thresholds set out in paragraph 6.3(b) of the Notice in relation to relevant business transactions undertaken without an account being opened.

Notice Paragraphs 6.5 to 6.18

6-3 CDD Measures under Paragraphs 6.5 to 6.18

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

6-3-2 A licensee should exercise greater caution when dealing with an unfamiliar or a new customer. Apart from obtaining the identification information required by paragraph 6.6 of the Notice, a licensee should (if not already obtained as part of its account opening process) also obtain additional information on the customer's background such as occupation, employer's name, nature of business, range of

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

annual income, and whether the customer holds or has held a prominent public function. Such additional identification information enables a licensee to obtain better knowledge of its customer's risk profile, as well as the purpose and intended nature of the account relationship or relevant business transaction.

Notice Paragraph 6.6

6-4 Identification of Customer

- 6-4-1 With respect to paragraph 6.6(c) of the Notice, a P.O. box address should only be used for jurisdictions where the residential address (e.g. street name or house number) is not applicable or available in the local context.
- 6-4-2 A licensee should obtain a customer's contact details such as personal, office or work telephone numbers.

Notice Paragraph 6.8

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

- 6-5-1 Under paragraph 6 and paragraph 8 of the Notice, a licensee is required to identify and screen all the connected parties of a customer. However, a licensee may verify their identities using a risk-based approach¹. A licensee is reminded of its obligations under the Notice to identify connected parties and remain apprised of any changes to connected parties.
- 6-5-2 Identification of connected parties may be done using publicly available sources or databases such as company registries, annual reports or based on substantiated information provided by the customers.
- 6-5-3 In relation to legal arrangements, a licensee 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 characteristics or class) and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership), as required by paragraph 6.14 of the Notice.

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

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

Notice Paragraph 6.9

6-6 Verification of Identity of Customer

- 6-6-1 Where the customer is a natural person, a licensee should obtain identification documents that contain a clear photograph of that customer.
- 6-6-2 In verifying the identity of a customer, a licensee may obtain the following documents:
- (a) Natural Persons —
 - (i) name, unique identification number, date of birth and nationality based on a valid passport or a national identity card that bears a photograph of the customer; and
 - (ii) residential address based on national identity card, recent utility or telephone bill, bank statement or correspondence from a government agency.
 - (b) Legal Persons or Legal Arrangements —
 - (i) name, legal form, proof of existence and constitution based on certificate of incorporation, certificate of good standing, partnership agreement, trust deed, constitutional document, certificate of registration or any other documentation from a reliable independent source; and
 - (ii) powers that regulate and bind the legal person or arrangement based on memorandum and articles of association, and board resolution authorising the opening of an account and appointment of authorised signatories.
- 6-6-3 Further guidance on verification of different types of customers (including legal persons or legal arrangements) is set out in Appendix A.
- 6-6-4 In exceptional circumstances where the licensee is unable to retain a copy of documentation used to verify the customer's identity, the licensee 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 licensee'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 licensee'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.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

Reliability of Information and Documentation

- 6-6-5 Where a licensee obtains data, documents or information from the customer or a third party, it should ensure that such data, documents or information are current at the time they are provided to the licensee.
- 6-6-6 Where the customer is unable to produce an original document, a licensee may consider accepting a copy of the document —
- (a) that is certified to be a true copy by a suitably qualified person (e.g. a notary public, a lawyer or certified public or professional accountant); or
 - (b) if a licensee's employee or officer independent of the licensee's dealing with the customer has confirmed that he has sighted the original document.
- 6-6-7 Where a document is in a foreign language, appropriate steps should be taken by a licensee to be reasonably satisfied that the document does in fact provide evidence of the customer's identity. The licensee 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 licensee may rely on a translation of such document by a licensee's employee or officer, independent of the licensee's dealing with the customer, who is conversant in that foreign language. This is to allow all employees and officers of the licensee involved in the performance of any measures required under the Notice to understand the contents of the documents, for effective determination and evaluation of ML/TF risks associated with the customer.
- 6-6-8 The licensee should ensure that documents obtained for performing any measures required under the Notice are clear and legible. This is important for the establishment of a customer's identity.

Notice Paragraphs 6.10 to 6.12

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

- 6-7-1 Appropriate documentary evidence of a customer's appointment of a natural person to act on its behalf includes a board resolution or similar authorisation documents.
- 6-7-2 Where there is a long list of natural persons appointed to act on behalf of the customer (e.g. a list comprising more than 10 authorised signatories), the licensee should verify at a minimum those natural persons who deal directly with the licensee.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

Notice Paragraphs 6.13 to 6.17

6-8 Identification and Verification of Identity of Beneficial Owner

- 6-8-1 A licensee should note that measures listed under paragraph 6.14(a)(i), (ii) and (iii) as well as paragraph 6.14(b)(i) and (ii) of the Notice are not alternative measures but are cascading measures with each to be used where the immediately preceding measure has been applied but has not resulted in the identification of a beneficial owner.
- 6-8-2 In relation to paragraph 6.14(a)(i) and (b)(i) of the Notice, when identifying the natural person who ultimately owns the legal person or legal arrangement, the shareholdings within the ownership structure of the legal person or legal arrangement should be considered. It may be based on a threshold (e.g. any person owning more than 25% of the legal person or legal arrangement, taking into account any aggregated ownership for companies with cross-shareholdings).
- 6-8-3 A natural person who does not meet the shareholding threshold referred to in paragraph 6-8-2 above but who controls the customer (e.g. through exercising significant influence), is a beneficial owner under the Notice.
- 6-8-4 A licensee 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 licensee remains responsible for complying with its obligations under the Notice to take reasonable measures to verify the identity of the beneficial owner by, for example, researching publicly available information on the beneficial owner or arranging a face-to-face meeting with the beneficial owner, to corroborate the undertaking or declaration provided by the customer.
- 6-8-5 Where the customer is not a natural person and has a complex ownership or control structure, a licensee should obtain enough information to sufficiently understand if there are legitimate reasons for such ownership or control structure.
- 6-8-6 A licensee should take particular care when dealing with companies with bearer shares, since beneficial ownership is difficult to establish. For such companies, a licensee should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the licensee is notified whenever there is a change of beneficial owner of such shares. At a minimum, these procedures should require the licensee to obtain an undertaking in writing from the beneficial owner of such bearer shares stating that the licensee 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 licensee may require that the bearer shares be held by a named custodian, with an undertaking from the custodian that the licensee will be notified of any changes to ownership of these shares or the named custodian.
- 6-8-7 For the purposes of paragraph 6.16 of the Notice, where the customer is a legal person publicly listed on a stock exchange and subject to regulatory disclosure

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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 licensee should put in place an internal assessment process with clear criteria, taking into account, amongst others, the country risk and the level of the country's compliance with the FATF standards.
- 6-8-9 Where the customer is a majority-owned subsidiary of a publicly listed legal person, it is not necessary to identify and verify the identities of beneficial owners of the customer. However, for such a customer, if there are other non-publicly listed legal persons who own more than 25% of the customer or who otherwise control the customer, the beneficial owners of such non-publicly listed legal persons should be identified and verified.
- 6-8-10 *Deleted with effect from 30 November 2015.*
- 6-8-11 *Deleted with effect from 30 November 2015.*
- 6-8-12 Where a customer is one which falls within paragraph 6.16 of the Notice, this does not in itself constitute an adequate analysis of low ML/TF risks for the purpose of performing SCDD measures under paragraph 7 of the Notice.

Notice Paragraph 6.18

6-9 Information on the Purpose and Intended Nature of Account Relationship and Relevant Business Transaction Undertaken without an Account Being Opened

- 6-9-1 The measures taken by a licensee to understand the purpose and intended nature of account relationships and relevant business transactions undertaken without an account being opened should be commensurate with the complexity of the customer's business and risk profile. For higher risk customers, a licensee should seek to understand upfront the expected account activity (e.g. frequency of transactions likely to pass through, expected amount for each transaction, names of persons to whom moneys are to be remitted) and consider, as part of ongoing monitoring, whether the activity corresponds with the stated purpose. This will enable a more effective ongoing monitoring of the customer's account relationships and relevant business transactions without an account being opened.

Notice Paragraphs 6.19 to 6.24

6-10 Review of Relevant Business Transactions Undertaken without an Account Being Opened

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- 6-10-1 Where a licensee undertakes any relevant business transaction for a customer without opening an account for that customer (“current relevant business transaction”), the licensee shall review all such earlier relevant business transactions to ensure that the current relevant business transaction is consistent with the licensee’s knowledge of the customer, its business and risk profile and where appropriate, the source of funds.
- 6-10-2 Where a licensee establishes an account relationship with a customer, the licensee shall review all earlier relevant business transactions undertaken without an account being opened to ensure that the account relationship being established is consistent with the licensee’s knowledge of the customer, its business and risk profile and where appropriate, the source of funds.
- 6-10-3 The licensee should make further enquiries when customers perform frequent and cumulatively large relevant business transactions without an account being opened, without any apparent or visible economic or lawful purpose. For example, any such relevant business transactions that are not consistent with the licensee's knowledge of the customer, including frequent transfers of funds to the same recipient, frequent money-changing transactions over a short period of time or multiple transfers of funds such that the amount of each fund transfer is not substantial, but the total of which is substantial.
- 6-10-4 Where there are indications that the risks may have increased over time, the licensee should request additional information and conduct a review of the customer’s risk profile in order to determine if additional measures are necessary.
- 6-10-5 In determining what would constitute suspicious, complex, unusually large or unusual pattern of relevant business transactions undertaken without an account being opened, a licensee should consider, amongst others, international typologies and information obtained from law enforcement and other authorities that may point to jurisdiction-specific considerations. As part of the review of such relevant business transactions, a licensee should pay attention to transaction characteristics, such as —
- (a) the nature of a relevant business transaction (e.g. abnormal size or frequency for that customer or peer group);
 - (b) whether a series of relevant business transactions is conducted with the intent to avoid reporting thresholds (e.g. by structuring an otherwise single transaction into a number of cash transactions);
 - (c) the geographic destination or origin of a payment (e.g. to or from a higher risk country); and
 - (d) the parties concerned (e.g. a request to make a payment to or from a person on a sanctions list).
- 6-10-6 A licensee’s transaction monitoring processes or systems for review of relevant business transactions undertaken without an account being opened may vary in

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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 licensee's operations. The licensee may adjust the extent and depth of monitoring of a customer according to the customer's ML/TF risk profile. The adequacy of monitoring and the factors leading the licensee to adjust the level of monitoring should be reviewed regularly for effectiveness in mitigating the licensee's ML/TF risks.

- 6-10-7 The transaction monitoring processes and systems used by the licensee should provide its business units and compliance officers (including employees and officers who are tasked with conducting investigations) with timely information needed to identify, analyse and effectively monitor customers for ML/TF.
- 6-10-8 The parameters and thresholds used by a licensee to identify suspicious relevant business transactions undertaken without an account being opened should be properly documented and independently validated to ensure that they are appropriate to its operations and context. A licensee should periodically review the appropriateness of the parameters and thresholds used in the review process.

Notice Paragraphs 6.25 to 6.32

6-11 Ongoing Monitoring

- 6-11-1 Ongoing monitoring of account relationships is a fundamental feature of an effective AML/CFT risk management system. Ongoing monitoring should be conducted in relation to all account relationships, but the licensee 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 licensee to adjust the level of monitoring should be reviewed regularly for effectiveness in mitigating the licensee's ML/TF risks.
- 6-11-2 A licensee should make further enquiries when a customer performs frequent and cumulatively large transactions in the course of an account relationship without any apparent or visible economic or lawful purpose. For example, transactions in the course of an account relationship that are not consistent with the licensee's knowledge of the customer, including frequent transfers of funds to the same recipient, frequent money-changing transactions over a short period of time or multiple transfers of funds such that the amount of each fund transfer is not substantial, but the total of which is substantial.
- 6-11-3 Where there are indications that the risks associated with an existing account relationship may have increased, the licensee should request additional information and conduct a review of the customer's risk profile in order to determine if additional measures are necessary.
- 6-11-4 A key part of ongoing monitoring includes maintaining relevant and up-to-date CDD data, documents and information so that the licensee can identify changes to the customer's risk profile —

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- (a) for higher risk categories of customers, a licensee 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 licensee, whichever is earlier; and
 - (b) for all other risk categories of customers, a licensee should obtain updated CDD information upon the occurrence of a trigger event.
- 6-11-5 Examples of trigger events are when (i) a significant transaction takes place, (ii) a material change occurs in the way the customer's account is operated, (iii) the licensee's policies, procedures or standards relating to the documentation of CDD information change substantially, and (iv) the licensee becomes aware that it lacks sufficient information about the customer concerned.
- 6-11-6 The frequency of CDD review may vary depending on each customer's risk profile. Higher risk customers should be subject to more frequent periodic review (e.g. on an annual basis) to ensure that CDD information such as nationality, passport details, certificate of incumbency, ownership and control information that the licensee has previously obtained remain relevant and up-to-date.
- 6-11-7 In determining what would constitute suspicious, complex, unusually large or unusual pattern of transactions undertaken in the course of an account relationship, a licensee should consider, amongst others, international typologies and information obtained from law enforcement and other authorities that may point to jurisdiction-specific considerations. As part of ongoing monitoring, a licensee should pay attention to transaction characteristics, such as —
 - (a) the nature of a transaction (e.g. abnormal size or frequency for that customer or peer group);
 - (b) whether a series of transactions is conducted with the intent to avoid reporting thresholds (e.g. by structuring an otherwise single transaction into a number of cash transactions);
 - (c) the geographic destination or origin of a payment (e.g. to or from a higher risk country); and
 - (d) the parties concerned (e.g. a request to make a payment to or from a person on a sanctions list).
- 6-11-8 A licensee's transaction monitoring processes or systems may vary in scope or sophistication (e.g. using manual spreadsheets to automated and complex systems). The degree of automation or sophistication of processes and systems depends on the size and complexity of the licensee's operations.
- 6-11-9 Nevertheless, the processes and systems used by the licensee should provide its business units and compliance officers (including employees and officers who are

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

tasked with conducting investigations) with timely information needed to identify, analyse and effectively monitor customer accounts for ML/TF.

- 6-11-10 The transaction monitoring processes and systems should enable the licensee to monitor the accounts of a customer holistically across business units to identify any suspicious transactions undertaken in the course of an account relationship. In the event that a business unit discovers suspicious trends or transactions in a customer's account, such information should be shared across other business units to facilitate a holistic assessment of the ML/TF risks presented by the customer. Therefore, licensees should have processes in place to share such information across business units. In addition, licensees should perform trend analyses of transactions to identify unusual or suspicious transactions undertaken in the course of an account relationship. Licensees should also monitor transactions undertaken in the course of an account relationship with parties in high risk countries or jurisdictions.
- 6-11-11 In addition, licensees 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 undertaken in the course of an account relationship.
- 6-11-12 The parameters and thresholds used by a licensee to identify suspicious transactions undertaken in the course of an account relationship should be properly documented and independently validated to ensure that they are appropriate to its operations and context. A licensee should periodically review the appropriateness of the parameters and thresholds used in the monitoring process.

Notice Paragraphs 6.33 to 6.3637

6-12 CDD Measures for Non-Face-to-Face Account Relationships or Non-Face-to-Face Relevant Business Transactions Undertaken without an Account Being Opened

- 6-12-1 A reference to "specific risks" in paragraph 6.34-33 of the Notice includes risks arising from establishing account relationships, undertaking transactions in the course of an account relationship or undertaking relevant business transactions without an account being opened, according to instructions conveyed by customers over the internet, post, fax or telephone. A licensee should note that applications, transactions and relevant business transactions undertaken across the internet may pose greater risks than other non-face-to-face business contact 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

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

(d) the speed of electronic transactions,

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

6-12-2 The measures taken by a licensee for verification of an identity in respect of non-face-to-face account relationships with or relevant business transactions undertaken in the course of an account relationship or relevant business transactions undertaken without an account being opened for the customer will depend on the nature and characteristics of the product or service provided and the customer's risk profile.

6-12-3 Where verification of identity is performed without face-to-face contact (e.g. electronically), a licensee should apply additional checks to manage the risk of impersonation. The additional checks may consist of robust anti-fraud checks that the licensee routinely undertakes as part of its existing procedures, which may include —

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

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

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

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

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

~~(f) requirement for the customer to make an initial deposit into the account with the licensee from funds held by the customer in an account with a bank in Singapore;~~

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

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

~~(e)(i) use of technology solutions to manage impersonation risks including, but not limited to, the use of biometric technologies (e.g. fingerprint or iris scans, facial recognition etc.) which should be linked incontrovertibly to the customer.~~

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

6-12-4 A licensee should regularly review the effectiveness of its checks to manage the risk of impersonation following the conduct of its non-face-to-face business contact.

6-12-5 A licensee may wish to conduct the independent assessment in paragraph 6.36 of the Notice as part of its annual audit. In appointing the external auditor or independent consultant for the independent assessment, the licensee should consider the competency of the external auditor or independent consultant, including their track record, and knowledge of technology solutions and regulatory requirements.

6-12-6 In considering whether there has been a substantial change in the policies and procedures in paragraph 6.37 of the Notice, a licensee should take into account the likely impact of the new policy or procedure on the specific risks associated with non-face-to-face account relationships with a new customer or non-face-to-face relevant business transactions undertaken without an account being opened for a customer, for example, the adoption of a technology solution different from that used in the existing policies and procedures.

Notice Paragraph 6.3738

6-13 Reliance by Acquiring Licensee on Measures Already Performed

6-13-1 When a licensee acquires the business of another FI, either in whole or in part, it is not necessary for the identity of all existing customers to be verified again, provided that the requirements of paragraph 6.37-38 of the Notice are met. A licensee shall maintain proper records of its due diligence review performed on the acquired business.

6-13-2 Notwithstanding the reliance on identification and verification that has already been performed, an acquiring licensee is responsible for its obligations under the Notice.

6-13-3 When a licensee acquires the business of another FI, either in whole or in part, the licensee is reminded that in addition to complying with paragraph 6.37-38 of the Notice, it is also required to comply with the requirements set out in paragraphs 6.19 to 6.32 of the Notice.

Notice Paragraph 6.4142

6-14 Existing Customers

6-14-1 In taking into account any previous measures as referred to in paragraph 6.41-42 of the Notice, a licensee should consider whether —

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

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- (b) there is a material change, since the measures were last performed, in the way that account relationship with the customer is conducted;
- (c) it lacks adequate identification information on a customer; and
- (d) there is a change in the ownership or control of the customer, or the persons authorised to act on behalf of the customer in its account relationship with the licensee.

Notice Paragraphs 6.42-43 to 6.4546

6-15 Screening

- 6-15-1 Screening is intended to be a preventive measure. A licensee is reminded that all parties identified pursuant to the Notice are required to be screened, irrespective of the risk profile of the customer.
- 6-15-2 Where screening results in a positive hit against sanctions lists, a licensee 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 a Suspicious Transaction Report ("STR") should be filed.
- 6-15-3 A licensee should put in place policies, procedures and controls that clearly set out —
 - (a) the ML/TF information sources used by the licensee 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 licensee'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 licensee'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;

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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

- 6-15-4 The level of automation used in the screening process should take into account the nature, size and risk profile of a licensee's business. A licensee 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 licensee 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 licensee's employees and officers will need to have access to CDD information to enable them to exercise their judgment in identifying true hits.
- 6-15-5 A licensee should be aware that performing screening after account relationships have been established or relevant business transactions without an account being opened have been undertaken could lead to a breach of relevant laws and regulations in Singapore relating to sanctioned parties. When the licensee becomes aware of such breaches, it should immediately take the necessary actions and inform the relevant authorities.
- 6-15-6 In screening periodically as required by paragraph 6.4344(d) of the Notice, a licensee should pay particular attention to changes in customer status (e.g. whether the customer has over time become subject to prohibitions and sanctions) or customer risks (e.g. a connected party of a customer, a beneficial owner of the customer or a natural person appointed to act on behalf of the customer subsequently becomes a Politically Exposed Person or presents higher ML/TF risks, or a customer subsequently becomes a Politically Exposed Person or presents higher ML/TF risks) and assess whether to subject the customer to the appropriate ML/TF risk mitigation measures (e.g. enhanced CDD measures).
- 6-15-7 A licensee 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 licensee's customer database for periodic name screening purposes. This will help the licensee to promptly identify any existing customers who have subsequently become higher risk parties.
- 6-15-8 In determining the frequency of periodic name screening, a licensee should consider its customer's risk profile.
- 6-15-9 The licensee should ensure that it has adequate arrangements to perform screening of the licensee's customer database when there are changes to the lists of sanctioned individuals and entities, covered by the TSOFA, MAS Regulations

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

issued under section 27A of the MAS Act² and MAS Notice MA-N-EXT 1/2012 (“Prohibition on Transactions with the Iranian Government and with Iranian Financial Institutions”). The licensee should implement “four-eye checks” on alerts from sanctions review before closing an alert, or conduct quality assurance checks on closure of such alerts on a sample basis.

6-15-10 With reference to paragraph 6.~~44-45~~ of the Notice, transaction screening should take place on a real-time basis (i.e. the screening or filtering of relevant payment instructions should be carried out before the transaction is executed).

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/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism.aspx>~~http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism/Regulations.aspx~~

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

7 Notice Paragraph 7 – Simplified Customer Due Diligence

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

7-2 Where a licensee applies SCDD measures, it is still required to perform ongoing monitoring of account relationship and reviews of relevant business transactions undertaken without an account being opened, under the Notice.

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

7-4 Where a licensee is satisfied that the risks of money laundering and terrorism financing are low, a licensee may perform SCDD measures, subject to paragraphs 7.1 and 7.5 of the Notice. Examples of possible SCDD measures include —

- (a) reducing the frequency of updates of customer identification information;
- (b) reducing the degree of ongoing monitoring and scrutiny of transactions, based on a reasonable monetary threshold; or
- (c) choosing another method to understand the purpose and intended nature of an account relationship or a relevant business transaction undertaken without an account being opened by inferring this from the type of transactions, instead of collecting information as to the purpose and intended nature of such account relationship or relevant business transaction.

7-5 Subject to the requirement that a licensee's assessment of low ML/TF risks is supported by an adequate analysis of risks, examples of potentially lower ML/TF risk situations include —

(a) Customer risk

- (i) a Singapore Government entity;
- (ii) entities listed on a stock exchange and subject to regulatory disclosure requirements relating to adequate transparency in respect of beneficial owners (imposed through stock exchange rules, law or other enforceable means); and
- (iii) an FI incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

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

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- (i) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme; and
- (ii) financial products or services that provide appropriately defined and limited services to certain types of customers (e.g. to increase customer access for financial inclusion purposes).

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

8 Notice Paragraph 8 – Enhanced Customer Due Diligence

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

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

(a) Customer risk

- (i) customers from higher risk businesses/ activities/ sectors identified in Singapore’s NRA, as well as other higher risk businesses/ activities/ sectors identified by the licensee;
- (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 account relationship or relevant business transaction undertaken without an account being opened is conducted under unusual circumstances (e.g. significant unexplained geographic distance between the licensee 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 licensee is exposed to, either through its own activities (including where its branches, subsidiaries and agents operate in) or the activities of its customers (including the FIs with whom the licensee provides remittance services to or engages to facilitate the provision of remittance services) which have relatively higher levels of corruption, organised crime or inadequate AML/CFT measures, as identified by the FATF; and
- (ii) countries identified by credible bodies (e.g. reputable international bodies such as Transparency International) as having significant levels of corruption, terrorism financing or other criminal activity.

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

- (i) anonymous transactions (which may involve cash); and
- (ii) frequent payments received from unknown or unassociated third parties.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- 8-3 When considering the ML/TF risks presented by a country or jurisdiction, a licensee 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 licensee 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 licensee 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 licensee may consider information from public sources in determining whether a person has been or is entrusted with prominent functions by an international organisation.

Notice Paragraphs 8.2 to 8.4

8-5 PEPs

- 8-5-1 If a licensee determines that any natural person appointed to act on behalf of a customer or any connected party of a customer is a PEP, the licensee should assess the ML/TF risks presented and consider factors such as the level of

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

influence that the PEP has on the customer. Licensees 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 licensee should apply ECDD measures on the customer accordingly.

- 8-5-2 It is generally acceptable for a licensee to refer to commercially available databases to identify PEPs. However, a licensee should also obtain from the customer details of his occupation and the name of his employer. In addition, a licensee should consider other non-public information that the licensee is aware of. A licensee 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 licensee's AML/CFT compliance function.
- 8-5-4 In relation to paragraph 8.3(b) of the Notice, a licensee may refer to information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. A licensee should note that not all declarations are publicly available. A licensee 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 licensee may not have specific information about assets that are not processed by the licensee, 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 account relationship or the undertaking of relevant business transactions without an account being opened (e.g. the amounts being remitted). In order to ensure that the funds are not proceeds of crime, the licensee should not limit its source of funds inquiry to identifying the other FI from which the funds have been transferred, but more importantly, the activity that generated the funds. The information obtained should be substantive and facilitate the establishment of the provenance of the funds or reason for the funds having been acquired. Examples of appropriate and reasonable means of establishing source of funds are information such as salary payments or sale proceeds.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- 8-5-7 Based on its risk assessment of the PEP, a licensee should consider whether the information regarding source of wealth and source of funds should be corroborated. In relation to paragraph 8.3(b) of the Notice, examples of “appropriate and reasonable means” for establishing source of wealth or source of funds are financial statements of the legal person or legal arrangement owned or controlled by the PEP, site visits, a copy of the will (in cases where the source of wealth or funds is an inheritance), and conveyancing documents (in cases where the source of wealth or funds is a sale of property).
- 8-5-8 In relation to paragraph 8.3 of the Notice, other ECDD measures that may be performed include —
- (a) requiring the first payment to be carried out through an account in the customer’s name with another FI subject to similar or equivalent CDD standards;
 - (b) using public sources of information (e.g. websites) to gain a better understanding of the reputation of the customer or any beneficial owner of a customer. Where the licensee finds information containing allegations of wrongdoing by a customer or a beneficial owner of a customer, the licensee should assess how this affects the level of risk associated with the account relationship or relevant business transaction undertaken without an account being opened;
 - (c) commissioning external intelligence reports where it is not possible for a licensee to easily obtain information through public sources or where there are doubts about the reliability of public information.
- 8-5-9 In relation to paragraph 8.4(a) and (b) of the Notice, where the licensee assesses that the account relationship with, or the relevant business transaction undertaken without an account being opened for, a domestic PEP or an international organisation PEP do not present higher ML/TF risks and that therefore ECDD measures need not be applied, the licensee 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 licensee’s assessment that the account relationship with, or the relevant business transactions for, the customer present higher ML/TF risks, the licensee 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 licensee should consider are —

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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

Notice Paragraphs 8.5 to 8.8

8-6 Other Higher Risk Categories

- 8-6-1 In relation to paragraph 8.7 of the Notice, a licensee may refer to preceding paragraph section 8-5-8 of these Guidelines for further guidance on the ECDD measures to be performed.
- 8-6-2 For customers highlighted in paragraph 8.6(a) of the Notice, a licensee shall assess them as presenting higher ML/TF risks. For such customers, the licensee shall ensure that the ECDD measures performed are commensurate with the risks. For customers highlighted in paragraph 8.6(b) of the Notice, a licensee shall assess whether any such customer presents a higher risk for ML/TF and ensure that the measures under paragraph 6 of the Notice, or ECDD measures where the licensee assesses the customer to present a higher risk for ML/TF, performed are commensurate with the risk.
- 8-6-3 With reference to paragraph 8.6(a) of the Notice, a licensee should refer to the FATF Public Statement on High Risk and Non-Cooperative Jurisdictions on which the FATF has called for counter-measures³. FATF updates this Public Statement on a periodic basis and licensees should regularly refer to the FATF website for the latest updates⁴.
- 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, licensees are expected to reject a prospective customer where there are reasonable grounds to suspect that the customer's assets are the proceeds of serious crimes, including wilful and fraudulent tax evasion. Where there are grounds for suspicion in an existing account relationship or when undertaking a relevant business transaction without opening an account, licensees should conduct enhanced monitoring and where appropriate, discontinue the relationship or not undertake the relevant business transaction respectively. If the licensee is inclined to retain the customer, approval shall be obtained from senior management with the substantiating reasons properly documented, and the account or relevant business transaction

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/>

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

subjected to close monitoring and commensurate risk mitigation measures, as applicable. This requirement applies to serious foreign tax offences, even if the foreign offence is in relation to the type of tax for which an equivalent obligation does not exist in Singapore. Examples of tax crime related suspicious transactions are set out in Appendix B of these Guidelines.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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 licensee. The third party will therefore perform the CDD measures on the customer according to its own AML/CFT policies, procedures and controls.
- 9-3 In contrast to a third party reliance scenario, the outsourced service provider performs the CDD measures (e.g. performs centralised transaction monitoring functions) on behalf of the licensee, in accordance with the licensee's AML/CFT policies, procedures and standards, and is subject to the licensee's control measures to effectively implement the licensee's AML/CFT procedures.
- 9-4 The licensee may take a variety of measures, where applicable, to satisfy the requirements in paragraph 9.2(b) and 9.2(c) of the Notice, including —
- (a) referring to any independent and public assessment of the overall AML/CFT regime to which the third party is subject, such as the FATF or FSRB's Mutual Evaluation reports and the IMF/World Bank Financial Sector Assessment Programme Reports/Reports on the Observance of Standards and Codes;
 - (b) referring to any publicly available reports or material on the quality of that third party's compliance with applicable AML/CFT rules;
 - (c) obtaining professional advice as to the extent of AML/CFT obligations to which the third party is subject to with respect to the laws of the jurisdiction in which the third party operates;
 - (d) examining the AML/CFT laws in the jurisdiction where the third party operates and determining its comparability with the AML/CFT laws of Singapore;
 - (e) reviewing the policies and procedures of the third party.
- 9-5 The reference to "documents" in paragraph 9.2(e) 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 licensee 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 licensee's account relationship with the customer or the completion of relevant business transactions undertaken without an account being opened.
- 9-6 Paragraph 9.3 of the Notice prohibits the licensee from relying on the third party to carry out ongoing monitoring or review of relevant business transactions without

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

an account being opened. Paragraph 9.3 of the Notice should be read with the requirements in Parts (VI) and (VII) of paragraph 6 of the Notice.

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

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

10 Notice Paragraph 10 – Provision of Remittance Services to Financial Institutions or Through Financial Institutions

- 10-1 Licensees should note that the requirements under paragraph 10 of the Notice are in addition to performing measures set out under paragraph 6 of the Notice.
- 10-2 The licensee should update the assessment of the suitability of the FI as required by paragraph 10.3(a) of the Notice on a periodic basis. If there are material changes to the assessment, the licensee should obtain approval from its senior management to continue the provision of remittance services to or the use of remittance services from the FI.
- 10-3 Other factors that a licensee should consider in complying with paragraph 10.3(a) of the Notice include —
- (a) the business group to which the FI belongs, country of incorporation, and the countries or jurisdictions in which subsidiaries and branches of the group are located;
 - (b) information about the FI’s management and ownership, reputation, major business activities, target markets, customer base and their locations; and
 - (c) the purpose of the services provided to the FI and expected business volume.
- 10-4 To assess the ML/TF risks associated with a particular country or jurisdiction as required by paragraph 10.3(a)(iii) of the Notice, a licensee may rely on information from the FATF mutual evaluation reports and statements on countries or jurisdictions identified as either being subject to countermeasures or having strategic AML/CFT deficiencies, mutual evaluation reports by FSRBs, publicly available information from national authorities and any restrictive measures imposed on a country or jurisdiction, particularly prohibitions on providing remittance services.
- 10-5 Where a licensee provides remittance services to FIs that are its related entities or engages such related entities to facilitate the provision of remittance services, the appropriate level of measures as required under paragraphs 6 and 10 of the Notice should be applied, bearing in mind that the risk profiles of individual entities within the same group could differ significantly. The licensee should take into consideration the parent company’s level of oversight and control over these related entities, and other risk factors unique to the entities such as their customers and products, the legal and regulatory environment they operate in, and sanctions by authorities for AML/CFT lapses.
- 10-6 The CDD process should result in a thorough understanding of the ML/TF risks arising from a relationship with the FI. It should not be treated as a “form-filling” exercise. A licensee’s assessment of the FI may be enhanced through meetings with the FI’s management, compliance head and AML/CFT regulators.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- 10-7 A licensee may apply a risk-based approach in complying with the requirements set out in paragraph 10 of the Notice but should be mindful that the provision of remittance services to a FI generally presents higher ML/TF risks.
- 10-8 For the purposes of paragraph 10 of the Notice, a licensee should take into account, for example, any sanctions imposed by relevant authorities on a FI for failing to have adequate controls against criminal activities.
- 10-9 In assessing whether a FI falls within the meaning of “shell FI” for the purposes of paragraph 10 of the Notice, a licensee 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.
- 10-10 In a country or jurisdiction where provision of remittance services is a regulated activity, a licensee should engage FIs which are regulated, to facilitate the remittance of moneys to recipients in that country or jurisdiction, instead of entering into agreements or arrangements with other unregulated entities to do the same.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

11 Notice Paragraph 11 – Agency Arrangements

- 11-1 For the avoidance of doubt, notwithstanding the appointment of an agent, the licensee shall remain responsible for its AML/CFT obligations in the Notice.
- 11-2 Paragraph 11.2(a) of the Notice requires that any agency arrangement be documented in writing because such written documentation is important to set out the respective roles and responsibilities of the licensee and the agent.
- 11-3 A licensee should develop stringent agent selection criteria to ensure that an agent is fit and proper and has the necessary resources to comply with the licensee's AML/CFT programme as required under paragraph 11.2(d) of the Notice. In monitoring agents' compliance with its AML/CFT programme as required under paragraph 11.2(d) of the Notice, a licensee should put in place and implement robust policies, procedures and controls. Such policies, procedures and controls should be approved by the licensee's senior management and reviewed periodically to ensure that they are kept up-to-date and relevant.
- 11-4 A licensee should conduct a periodic review of its agents to evaluate their compliance level with its policies and procedures. Where the licensee observes any non-compliance with its AML/CFT programme, it should document its findings and consider whether to take any remedial action, such as the termination of the agency agreement. The licensee should obtain approval from its senior management on the proposed action to be taken, including any proposal not to take any action.
- 11-5 In complying with paragraph 11.4 of the Notice, the licensee should obtain and retain with the current list of its agents, information such as the agents' full names (including any aliases), unique identification numbers (such as an identity card number, birth certificate number or passport number, or where the agent is not a natural person, the incorporation number or business registration number), residential addresses or registered or business addresses, and if different, principal place of businesses (as may be appropriate), dates of birth, establishment, incorporation or registration (as may be appropriate) and nationality or place of incorporation or registration (as may be appropriate). The licensee should obtain all necessary documentation that identifies and verifies the agent appointed, including its shareholding structure, the board of director, the management team, beneficial owner(s), where appropriate. The licensee should also record and retain information such as the date of commencement, date of termination and reasons for terminating the agency arrangement. The licensee should ensure that such information should continue to be relevant and updated on a regular basis thereafter.
- 11-6 A licensee should conduct regular AML/CFT training for all appointed agents similar to training of the licensee's employees and officers as required by paragraph 16.7 of the Notice.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

12 Notice Paragraph 12 – Sending or Receiving Funds by Wire Transfers

- 12-1 In relation to paragraph 12.1 of the Notice, wire transfers include all forms of electronic transmission including, but not limited to, email, facsimile, short message service or other means of electronic transmission for payment instructions.
- 12-2 In relation to paragraph 12.9 of the Notice, examples of domestic wire transfers in Singapore include inter-bank transfers via the local MAS Electronic Payment System (“MEPS+”).
- 12-3 A licensee should not omit, delete or alter information in payment messages, for the purpose of avoiding detection of that information by another FI in the payment process.
- 12-4 A licensee should monitor payment messages to and from higher risk countries or jurisdictions, as well as transactions with higher risk countries or jurisdictions and suspend or reject payment messages or transactions with sanctioned parties or countries or jurisdictions.
- 12-5 Where name screening checks confirm that the wire transfer originator or wire transfer beneficiary is a terrorist or terrorist entity, the requirement for the licensee to block, reject or freeze assets of these terrorists or terrorist entities cannot be risk-based.
- 12-6 Where there are positive hits arising from name screening checks, they should be escalated to the AML/CFT compliance function. The decision to approve or reject the receipt or release of the wire transfer should be made at an appropriate level and documented.

Notice Paragraphs 12.3 to 12.11

12-7 Responsibility of the Ordering Institution

- 12-7-1 For joint accounts, the ordering institution shall provide all of the joint account holders’ information to the beneficiary institution in accordance with paragraph 6.40 of the Notice.
- 12-7-2 The ordering institution shall include wire transfers in its ongoing monitoring of the account relationship with the customer or review of relevant business transactions undertaken without an account being opened, in accordance with paragraph 6 of the Notice.
- 12-7-3 In relation to paragraph 12.3 of the Notice, ‘value date’ refers to the date of receipt of funds by the wire transfer beneficiary.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

Notice Paragraphs 12.12 to 12.15

12-8 Responsibility of the Beneficiary Institution

- 12-8-1 Where an incoming wire transfer is not accompanied by complete wire transfer originator information and wire transfer beneficiary, a beneficiary institution shall request the information from the ordering institution. A licensee should consider rejecting incoming wire transfers or terminating business relations with overseas ordering institutions that fail to provide originator information. An STR should be filed if appropriate. In this regard, a licensee should be mindful of any requirements that may be imposed on the overseas ordering institution, either by law or as a regulatory measure, in relation to cross-border wire transfers.
- 12-8-2 As part of its internal risk-based policies, procedures and controls, a licensee should consider rejecting incoming wire transfers or terminating business relations with overseas ordering institutions if the licensee is not satisfied that it can justify to the Authority the reasons for executing wire transfers that lack full originator information.

Notice Paragraphs 12.16 to 12.20

12-9 Responsibility of the Intermediary Institution

- 12-9-1 An intermediary institution is required under the Notice to retain, and to pass on to the beneficiary institution or another intermediary institution that it effects a wire transfer to, all the information accompanying a wire transfer effected from an ordering institution or another intermediary institution, to it. The information accompanying the wire transfer will be either the unique transaction reference number, as permitted by the Notice, or the full originator and wire transfer beneficiary information.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

15 Notice Paragraph 15 – Suspicious Transactions Reporting

- 15-1 A licensee 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.
- 15-2 A licensee should note that an STR filed with STRO would also meet the reporting obligations under the TSOFA.
- 15-3 Examples of suspicious transactions are set out in Appendix B of these Guidelines. These examples are not intended to be exhaustive and are only examples of basic ways in which money may be laundered or used for TF purposes. Identification of suspicious transactions should prompt further enquiries and where necessary, investigations into the source of funds. A licensee should also consider filing an STR if there is any adverse news on its customers in relation to financial crimes. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.
- 15-4 Once suspicion has been raised in relation to a customer or any transaction for that customer, in addition to reporting the suspicious activity, a licensee should ensure that appropriate action is taken to adequately mitigate the risk of the licensee being used for ML/TF activities. This may include strengthening its AML/CFT processes. This may also include a review of either the risk classification of the customer, or the account relationship 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.
- 15-5 STR reporting templates are available on CAD’s website⁵. However, licensees are strongly encouraged to use the online system provided by STRO to lodge STRs. In the event that the licensee is of the view that STRO should be informed on an urgent basis, particularly where a transaction is known to be part of an ongoing investigation by the relevant authorities, a licensee should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct.
- 15-6 A licensee should document all transactions that have been brought to the attention of its AML/CFT compliance function, including transactions that are not reported to STRO. To ensure that there is proper accountability for decisions made, the basis for not submitting STRs for any suspicious transactions escalated by its employees and officers should be properly substantiated and documented.
- 15-7 Licensees are reminded to read paragraph 15.4 of the Notice together with paragraphs 6.38 and 6.39 of the Notice. Where a licensee stops performing CDD measures as permitted under paragraph 15.4 and is, as a result, unable to

⁵ The website address as at 24 April 2015: <http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting>

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

complete CDD measures (as specified under paragraph 6.39), the licensee is reminded that it shall not commence or continue the account relationship with that customer or undertake any transaction for that customer.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

16 Notice Paragraph 16 – Internal Policies, Compliance, Audit and Training

16-1 As internal policies and procedures serve to guide employees and officers in ensuring compliance with AML/CFT laws and regulations, it is important that a licensee 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 16.3 to 16.4

16-2 Compliance

16-2-1 A licensee should ensure that the AML/CFT compliance officer has the necessary seniority and authority to effectively perform his responsibilities.

16-2-2 The responsibilities of the AML/CFT compliance officer should include —

- (a) carrying out, or overseeing the carrying out of
 - (i) ongoing monitoring of account relationships or review of relevant business transactions undertaken without an account being opened; and
 - (ii) sample review of accounts or transactions for compliance with the Notice and these Guidelines;
- (b) promoting compliance with the Notice and these Guidelines, as well as 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 transactions;
- (f) advising and training employees and officers on developing and implementing internal policies, procedures and controls on AML/CFT;
- (g) reporting to senior management on the outcome of reviews of the licensee's compliance with the Notice and these Guidelines, as well as MAS Regulations issued under section 27A of the MAS Act and risk assessment procedures; and
- (h) reporting regularly on key AML/CFT risk management and control issues (including information outlined in paragraph 1-4-14 of the Guidelines), and any necessary remedial actions, arising from audit, inspection, and compliance

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

reviews, to the licensee's senior management, at least annually and as and when needed.

- 16-2-3 The business interests of a licensee 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 licensee's management.

Notice Paragraph 16.5

16-3 Audit

- 16-3-1 A licensee's AML/CFT framework should be subject to periodic audits (including sample testing). Auditors should assess the effectiveness of measures taken to prevent ML/TF. This would include, among others —

- (a) determining the adequacy of the licensee's AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;
- (b) reviewing the content and frequency of AML/CFT training programmes, and the extent of employees' and officers' compliance with established AML/CFT policies and procedures; and
- (c) assessing whether instances of non-compliance are reported to senior management on a timely basis.

- 16-3-2 The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the licensee's business.

Notice Paragraph 16.6

16-4 Employee Hiring

- 16-4-1 The screening procedures applied when a licensee hires employees and appoints officers should include —

- (a) background checks with past employers;
- (b) screening against ML/TF information sources; and
- (c) bankruptcy searches.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

16-4-2 In addition, a licensee should conduct credit history checks, on a risk-based approach, when hiring employees and appointing officers.

Notice Paragraph 16.7

16-5 Training

16-5-1 As stated in paragraph 16.8 of the Notice, it is a licensee'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 licensee 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.

16-5-2 Apart from the initial training, a licensee should also provide refresher training at least once every two years, or more regularly as appropriate, to ensure that employees and officers are reminded of their responsibilities and are kept informed of new developments related to ML/TF. A licensee should maintain the training records for audit purposes.

16-5-3 A licensee should monitor the effectiveness of the training provided to its employees and officers. This may be achieved by —

- (a) testing their understanding of the licensee's policies and procedures to combat ML/TF, their obligations under relevant laws and regulations, and their ability to recognise suspicious transactions;
- (b) monitoring their compliance with the licensee'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.

Endnotes on History of Amendments

1. Guidelines to MAS Notice 3001 dated 2 July 2007.
2. Guidelines to MAS Notice 3001 dated 2 July 2007 cancelled with effect from 24 May 2015.
3. Guidelines to MAS Notice 3001 dated 24 April 2015 with effect from 24 May 2015.
(a) Amended on 30 November 2015.
(a)(b) Amended on 9 January 2019.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

I Other Key Topics - Guidance to Licensees 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”)⁶. These Regulations apply to all FIs (including licensees) 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 website⁷.
- 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 A licensee should rely on its CDD measures (including screening measures) under the Notice to detect and prevent proliferation financing activities and transactions.
- I-1-5 A licensee should also ensure compliance with legal instruments issued by MAS relating to proliferation financing risks. An example is MAS Notice on Prohibition on Transactions with the Iranian Government and with Iranian Financial Institutions.

I-2 CDD and Internal Controls

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

⁶ Please refer to the MAS website for a full listing of Regulations issued by MAS pursuant to the United Nations Security Council Resolutions.

⁷ Please see: <http://www.un.org/sc/committees/1718> and <http://www.un.org/sc/committees/1737>

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- (a) omitting, deleting or altering information in payment messages for the purpose of avoiding detection of that information by the licensee itself or other licensees involved in the payment process; and
- (b) structuring transactions with the purpose of concealing the involvement of designated persons.

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

I-3 Obligation of Licensee to Freeze without Delay

I-3-1 A licensee is reminded of its obligations under the MAS Regulations issued under section 27A of the MAS Act⁸ to immediately freeze any funds, financial assets or economic resources owned or controlled, directly or indirectly, by designated persons that the licensee has in its possession, custody or control. The licensee should also file an STR in such cases.

I-4 Potential Indicators of Proliferation Financing

I-4-1 A licensee 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;
- (c) the transaction involves designated persons;
- (d) the transaction involves higher risk countries or jurisdictions which are known to be involved in proliferation of weapons of mass destruction or proliferation financing activities;
- (e) the transaction involves other FIs with known deficiencies in AML/CFT controls or controls for combating proliferation financing;
- (f) the transaction involves possible shell companies (e.g. companies that do not have a high level of capitalisation or display other shell company indicators);
- (g) the transaction involves containers whose numbers have been changed or ships that have been renamed;

⁸ 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>

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- (h) the shipment of goods takes a circuitous route or the financial transaction is structured in a circuitous manner;
- (i) the transaction involves the shipment of goods inconsistent with normal geographic trade patterns (e.g. the country involved would not normally export or import such goods);
- (j) the transaction involves the shipment of goods incompatible with the technical level of the country to which goods are being shipped (e.g. semiconductor manufacturing equipment shipped to a country with no electronics industry);
or
- (k) there are inconsistencies in the information provided in trade documents and financial flows (e.g. in the names, companies, addresses, ports of call and final destination).

I-5 Other Sources of Guidance on Proliferation Financing

- I-5-1 The FATF has also provided guidance on measures to combat proliferation financing and a licensee may wish to refer to the [FATF website](#) for additional information.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

II Useful Links

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

.....

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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

Customer Type	Examples of CDD Information
Sole proprietorships	<ul style="list-style-type: none"> • Full registered business name • Business address or principal place of business • Information about the purpose and intended nature of the account relationship or relevant business transaction with the licensee • 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 licensee’s visit to the customer’s place of business, where the licensee 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	<ul style="list-style-type: none"> • Full name of entity • Business address or principal place of business • Information about the purpose and intended nature of the account relationship or relevant business transaction with the licensee • 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 licensee’s visit to the customer’s place of business, where the licensee assesses it as necessary • Ownership and control structure • Records in an independent company registry • Partnership deed • The customer’s membership with a relevant professional body • Any association the entity may have with other countries or jurisdictions (e.g. the location of the entity’s headquarters, operating facilities, branches, subsidiaries)
Companies	<ul style="list-style-type: none"> • Full name of entity • Business address or principal place of business

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

Customer Type	Examples of CDD Information
	<ul style="list-style-type: none"> • Information about the purpose and intended nature of the account relationship or relevant business transaction with the licensee • 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 licensee’s visit to the customer’s place of business, where the licensee 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 licensee • Any association the entity may have with other countries or jurisdictions (e.g. the location of the entity’s headquarters, operating facilities, branches, subsidiaries)
<p>Public sector bodies, government, state-owned companies and supranationals (other than sovereign wealth funds)</p>	<ul style="list-style-type: none"> • Full name of entity • Nature of entity (e.g. overseas government, treaty organisation) • Business address or principal place of business. • Information about the purpose and intended nature of account relationship or relevant business transaction with the licensee • 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 licensee’s visit to the customer’s place of business, where the licensee assesses it as necessary • Board resolution authorising the opening of the customer’s account with a licensee
<p>Clubs, Societies and Charities</p>	<ul style="list-style-type: none"> • Full name of entity • Business address or principal place of business

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

Customer Type	Examples of CDD Information
	<ul style="list-style-type: none"> • Information about the purpose and intended nature of account relationship or relevant business transaction with the licensee • Information about the nature of the entity’s activities and objectives • Names of all trustees (or equivalent) • Names of all natural persons who act on behalf of the entity • Names of all connected parties • Names of all beneficial owners • Information about the source of funds • A report of the licensee’s visit to the customer’s place of business, where the licensee 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 licensee • Records in a relevant and independent registry in the country of establishment
<p>Trust and Other Similar Arrangements (e.g. Foundations, Fiducie, Treuhand and Fideicomiso)</p>	<ul style="list-style-type: none"> • 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 licensee’s visit to the customer’s place of business, where the licensee assesses it is necessary • Information about the purpose and intended nature of account relationship or relevant business transaction with the licensee • Records in a relevant and independent registry in the country or jurisdiction of constitution • Country or jurisdiction of constitution • Trust deed • Names of the settlors/trustees/beneficiaries or any person who has power over the disposition of any property that is subject to the trust • Declaration of trusts

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

Customer Type	Examples of CDD Information
	<ul style="list-style-type: none">• Deed of retirement and appointment of trustees (where applicable)

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

APPENDIX B – Examples of Suspicious Transactions

B-1 General Comments

- B-1-1 The list of situations given below is intended to highlight some basic ways in which money may be laundered or used for TF purposes. While each individual situation may not be sufficient to suggest that ML/TF is taking place, a combination of such situations may be indicative of a suspicious transaction. The list is intended solely as an aid, and must not be applied as a routine instrument in place of common sense.
- B-1-2 The list is not exhaustive and may be updated due to changing circumstances and new methods of laundering money or financing terrorism. Licensees are to refer to STRO's website for the latest list of red flags⁹.
- B-1-3 A customer's declarations regarding the background of such transactions should be checked for plausibility. Not every explanation offered by the customer can be accepted without scrutiny.
- B-1-4 It is reasonable to suspect any customer who is reluctant to provide normal information and documents required routinely by the licensee in the course of the account relationship or when undertaking any relevant business transaction without an account being opened. Licensees should pay attention to customers who provide minimal, false or misleading information or, when establishing an account relationship or undertaking a relevant business transaction without opening an account, provide information that is difficult or expensive for the licensee to verify.

B-2 Transactions Which Do Not Make Economic Sense

- i) Transactions that cannot be reconciled with the usual activities of the customer.
- ii) Transactions which are incompatible with the licensee's knowledge and experience of the customer in question or with the purpose of the relevant business transaction, for example, a mismatch between the economic activity, country of origin, or person and the remittances received.
- iii) Conceal or disguise significant transactions to avoid disclosure for record purpose by executing frequent or several transactions such that each transaction by itself is below CDD thresholds. For example, carrying out several transactions, either in a single day or over a period of days, by breaking them into smaller amounts in order to avoid the mandatory threshold customer identification requirements.

⁹ The website address as at 242 April 2015: <http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting>

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- iv) “U-turn” transactions, i.e. where funds received from a person or company in a foreign jurisdiction are remitted to another person or company in the same foreign jurisdiction, or to the sender’s account in another jurisdiction.
- v) Unnecessary routing of funds through various financial institutions or persons.
- vi) Substantial increase(s) in the number of transactions/ frequency/ amounts by a customer without apparent cause, especially if remittances are made to a destination/ person not normally associated with the customer.
- vii) Concentration of payments where multiple senders transfer funds to a single individual’s account.
- viii) There is lack of apparent relationship between the sender and beneficiary, and/or personal remittances sent to countries or jurisdictions that have no apparent family or business link to customer, and/or the customer has no relation to country where he/she sends/receives the money and cannot sufficiently explain why money is sent there/received from there.

B-3 Transactions Involving Large Amounts of Cash

- i) Frequent transactions of large cash amounts that do not appear to be justified by the customer’s business activity or background.
- ii) Customers making large and/or frequent remittances, mostly to individuals and firms not normally associated with their business.
- iii) Customers remitting large amounts of money to persons outside Singapore with instructions for payment in cash.
- iv) Exchanging an unusually large amount of small-denominated notes for those of higher denomination in a different currency.
- v) Numerous transactions by a customer, especially over a short period of time, such that the amount of each transaction is not substantial, but the cumulative total of which is substantial.
- vi) Customers who together, and simultaneously, use separate branches to conduct large (cash) transactions.
- vii) Customers whose transactions involve counterfeit notes or forged instruments.
- viii) Large and regular payments that cannot be clearly identified as bona fide transactions, from and to countries associated with (a) the production, processing or marketing of narcotics or other illegal drugs or (b) other criminal conduct.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

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

B-4 Tax Crimes Related Transactions

- i) Negative tax-related reports from the media or other credible information sources
- ii) Unconvincing or unclear purpose or motivation for establishing account relationships or conducting business transactions in Singapore.
- iii) Inability to reasonably justify frequent and large wire transfers from or to a country or jurisdiction that presents higher risk of tax evasion.
- iv) Purchase or sale of large amounts of precious metals by a customer which is not in line with his business or background.

B-5 Trade-based Related Transactions

- i) The commodity is shipped to (or from) a country or jurisdiction designated as “higher risk” for ML/TF activities.
- ii) The type of commodity shipped is designated as “higher risk” for ML/TF activities¹⁰.
- iii) Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice.
- iv) Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped.
- v) Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity’s fair market value.
- vi) The size of the shipment appears inconsistent with the scale of the exporter or importer’s regular business activities.
- vii) The type of commodity shipped appears inconsistent with the exporter or importer’s regular business activities.
- viii) The method of payment appears inconsistent with the risk characteristics of the transaction¹¹.

¹⁰ For example, high-value, low-volume goods (e.g. consumer electronics), which have high turnover rates and present valuation difficulties.

¹¹ For example, the use of an advance payment for a shipment from a new supplier in a high-risk country.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- ix) The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction.
- x) The transaction involves the use of repeatedly amended or frequently extended letters of credit.
- xi) The transaction involves the use of front (or shell) companies.
- xii) The commodity is transhipped through one or more countries or jurisdictions for no apparent economic reason.
- xiii) The shipment does not make economic sense¹².

B-6 Other Types of Transactions

- i) Account activity or transaction volume is not commensurate with the customer's known profile (e.g. age, occupation, income).
- ii) Transactions with 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 person receives funds from a religious or charitable organisation and exchanges the funds for a different currency or remits the funds to another person within a relatively short period.
- v) The customer fails to reasonably justify the purpose of a transaction when queried by the licensee.
- vi) Transactions for which customers fail to provide a legitimate reason when asked.
- vii) Transfers from one or more senders often from different countries and/or in different currencies to a local person over a short period of time.
- viii) Periodic transfers made by several people to the same person or related persons.
- ix) False information during the identification process/ lack of co-operation. Use of third parties to transfer funds aimed at concealing the sender and/or receiver of moneys.
- x) The customer uses intermediaries which are not subject to adequate AML/CFT laws.

¹² For example, the use of a forty-foot container to transport a small amount of relatively low-value goods.

GUIDELINES TO MAS NOTICE 3001 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

- x i) Customers send or receive (regular) payments from countries which are regarded as “tax havens” or which are known to be exposed to risks such as drug trafficking, terrorism financing, smuggling. Amounts transacted are not necessarily large.
- x ii) No or limited information about the origin of funds.
- x iii) Funds used by a customer to settle his obligations are from a source(s) that appears to have no explicit or direct links to the customer.
- x iv) Banknotes brought by customer are in small denominations and dirty; stains on the notes indicating that the funds have been carried or concealed, or the notes smell musty; notes are packaged carelessly and precipitately; when the funds are counted, there is a substantial difference between the actual amount and the amount indicated by the customer (over or under).
- x v) Remittances made to high-risk countries or jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings.
- x vi) Transactions that are suspected to be in violation of another country's or jurisdiction's foreign exchange laws and regulations.

B-7 Customer Behaviour

- i) Customer is accompanied by others who keep a low profile or stay just outside the premise. Customer appears to be in doubt when asked for further details.
- ii) Customer is in a hurry to complete the transaction, with promises to provide the supporting information later.
- iii) Customer shows no interest in costs and/or is happy with a poor rate.
- iv) Two or more customers appear to be trying to avoid reporting requirements and seem to be working together to break one transaction into two or more transactions.
- v) The customer only seems to know the amount to be remitted after the remittance licensee has counted the customer's moneys.
- vi) The customer buys currency that does not fit with what is known about the customer's destination or the customer buys currency from an unusual location in comparison to his/her own location.