

CONSULTATION PAPER

P001 - 2005
January 2005

Draft Notice on Prevention of Money Laundering and Countering The Financing of Terrorism

MAS

Monetary Authority of Singapore

PREFACE

Money laundering is a concern of all of the world's financial centres, including Singapore. Since 1991, Singapore has been a member of the Financial Action Task Force (FATF), the inter-governmental body established in 1989 to develop and promote policies to combat money laundering. Towards this end, the FATF developed and first issued, in 1990, its Forty Recommendations on Money Laundering. Shortly after the terrorist attacks of 11 Sep 2001, the FATF expanded its mission to include the development and promotion of policies to counter the financing of terrorist acts. To this end, in October 2001, the FATF further issued its Eight Special Recommendations on Terrorist Financing.

These two sets of recommendations are now well known within the international financial community as the FATF 40+8 Recommendations, and constitute the international standard against money laundering and terrorist financing (AML/CFT).

As a leading financial centre and a member of the FATF, Singapore recognises that it is essential to have a rigorous legal regime to guard against the abuse of its financial system for the purposes of money laundering and terrorist financing, and has long had in place a regulatory regime requiring all banks and financial institutions to take measures to prevent this. In the context of the banking sector, the leading instrument for this purpose is MAS Notice to Banks No. 626, whose latest edition was issued on 11 November 2002.

In June 2003, the FATF revised its Forty Recommendations on Money Laundering. This was necessary in order that the Recommendations remain relevant and effective. The revised Forty Recommendations took into account the increasingly sophisticated combination of techniques that have evolved and are employed by criminal elements to disguise the ownership and control of illegal proceeds. Combined with the Eight Special Recommendations on Terrorist Financing, they now form a comprehensive framework of minimum standards designed to combat money laundering and terrorist financing. In February 2004, the FATF also adopted a new

Methodology for Assessing Compliance with the FATF Forty Recommendations and the FATF Eight Special Recommendations.

Within the international arena generally, there has also been strong support for AML/CFT initiatives by the International Monetary Fund and the World Bank (through their Financial Sector Assessment Programme) and also by the Basel Committee on Banking Supervision (which had issued several papers on the subject).

Taking into account all of the above developments, MAS began in 2004 a process of reviewing and revising Notice 626 to ensure that the AML/CFT regime for Singapore's financial sector incorporates the prevailing international standards. MAS is now pleased to release, for public consultation, a draft of the revised MAS Notice 626.

OVERVIEW OF REVISED MAS NOTICE 626

The key changes in the revised MAS Notice 626 are as follows:

- (a) The revised Notice has been expanded to cover both terrorist financing as well as money laundering.
- (b) The revised Notice stipulates a more exhaustive regime of customer due diligence (CDD) measures that banks are required to perform. It also sets out more comprehensively the timing for completion of CDD measures, and the consequential steps to be taken should CDD measures cannot be satisfactorily performed.
- (c) The new AML/CFT regime incorporates an element of risk sensitivity. Simplified CDD measures will be permitted but enhanced CDD measures will be required in other situations where the risk of AML/CFT may be higher. In particular, the Notice will now require banks to have in place measures to deal with politically exposed persons.

- (d) The revised Notice also includes a proposal for giving effect to the FATF's Special Recommendation VII on Wire Transfers.¹

INVITATION FOR COMMENTS

MAS invites comments on the revised MAS Notice 626. Please note that all submissions received may be made public unless confidentiality is expressly requested for all or part of the submission.

MAS will shortly be effecting revisions to the AML/CFT regime for the other financial institutions supervised by MAS. These will be based largely on what is now proposed in the revised MAS Notice 626. At this juncture, MAS also welcomes comments and suggestions on the revision of the AML/CFT regime for merchant banks, finance companies, life insurers, capital markets services licensees, financial advisers, approved trustees, money changers and remittance agents.

Comments are requested to be submitted via electronic mail to aml@mas.gov.sg by 18 Feb 05. Alternatively, written comments may be delivered by post to:

International & Regional Relations Division
External Department
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117

Submission via electronic mail is encouraged.

¹ The revised Notice does not presently stipulate a threshold figure, as this is still the subject of ongoing discussion within the FATF.

MAS 626

Date

NOTICE TO BANKS
BANKING ACT, CAP 19

(MAS 626 dated 11 Nov 2002 is cancelled with effect from date)

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

1 INTRODUCTION

- 1.1 This Notice is issued pursuant to Section 55 of the Banking Act (Cap. 19) and applies to all banks in Singapore.
- 1.2 This Notice sets out the measures to be taken by all banks in Singapore to help prevent the banking system of Singapore from being used for money laundering or terrorist financing. The measures in this Notice may be supplemented from time to time by other notices, circulars and directives issued by MAS.
- 1.3 All banks in Singapore are reminded of their obligations and responsibilities under the law, including in particular the following:
 - (a) The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A);
 - (b) The Terrorism (Suppression of Financing) Act (Cap. 325); and
 - (c) The Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002.
- 1.4 Where relevant, banks in Singapore shall also take into account international best practices when developing and maintaining their internal policies, procedures and controls against money laundering and terrorist financing.
- 1.5 For the purposes of this Notice –

“AML/CFT” means anti-money laundering and countering the financing of terrorism;

“beneficial owner” means a natural person who ultimately owns or controls a customer or on whose behalf a transaction is being conducted by the

customer; and includes the person(s) who exercises ultimate effective control over a legal person;

“CDD” means customer due diligence;

“customer” means the person in whose name an account is opened or to whom a bank provides any financial service whether or not an account is opened;

“government entity” means a government ministry, department or agency, but does not include a company that is wholly owned by a government and established under the ordinary company law of that country or jurisdiction.

“legal person” means any person that is not a natural person and includes for the avoidance of doubt any body corporate or unincorporate established to carry on business or to carry out specific functions;

“PEP” means politically exposed person, as defined in paragraph 7.1;

“STR” means suspicious transaction report; and

“STRO” means the Suspicious Transactions Reporting Office, Commercial Affairs Department of the Singapore Police Force.

2 DESCRIPTION OF MONEY LAUNDERING

2.1 Money laundering is a process intended to mask the benefits derived from drug trafficking or criminal conduct so that they appear to have originated from a legitimate source.

2.2 Generally, the process of money laundering comprises three stages, during which there may be numerous transactions that could alert a bank to the money laundering activity:

(a) Placement - The physical disposal of the benefits of drug trafficking or criminal conduct;

(b) Layering - The separation of the benefits of drug trafficking or criminal conduct from their source by creating layers of financial transactions designed to disguise the audit trail;

(c) Integration - The provision of apparent legitimacy to the benefits of drug trafficking or 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 business funds.

2.3 The chart in Appendix I illustrates these three stages of money laundering in greater detail.

3 DESCRIPTION OF TERRORIST FINANCING

- 3.1 Terrorism seeks to influence or compel governments into a particular course of action or seeks to intimidate the public or a section of the public through the use or threat of violence, damage to property, danger to life, serious risks to health or safety of the population or disruption of key public services or infrastructure.
- 3.2 Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed.
- 3.3 Sources of terrorist financing may be legitimate or illegitimate. It may be derived from criminal activities such as kidnapping, extortion, fraud or drug trafficking. It may also be derived from legitimate income such as membership dues, sale of publications, donations from persons or entities sympathetic to their cause and sometimes income from legitimate business operations belonging to terrorist organisations.
- 3.4 Terrorist financing involves amounts that are not always large, and the associated transactions may not necessarily be complex given that some sources of terrorist funds may be legitimate.
- 3.5 However, the methods used by terrorist organisations to move, collect, hide or make available funds for their activities remain similar to those used by criminal organisations to launder their funds. This is especially so when the funds are derived from illegitimate sources, in which case, the terrorist organisation would have similar concerns to a typical criminal organisation in laundering the funds. Where the funds are derived from legitimate sources, terrorist organisations would usually still need to employ the same laundering techniques to obscure or disguise the links between the organisation and the funds.

4 BASIC PRINCIPLES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

- 4.1 Every bank shall observe the following basic principles on AML/CFT in the conduct of its activities:
 - (a) Customer Due Diligence - Every bank shall obtain satisfactory evidence of the identity of the customer and beneficial owner, understand the purpose and nature of business relations between the bank and the customer, monitor customers' transactions and have effective procedures for verifying the bona fides of new customers.
 - (b) Compliance with laws - Every bank shall conduct its business in conformity with high ethical standards, comply with all applicable laws and regulations, and not provide any service or undertake any

transaction if it has reasons to suspect that the service or transaction is or may be connected with money laundering or terrorist financing.

- (c) Co-operation with law enforcement agencies - Every bank shall cooperate fully with law enforcement agencies in accordance with the law, including taking the appropriate measures allowed by law if there are reasonable grounds for suspecting money laundering or terrorist financing. To facilitate the reporting of suspicious transactions to STRO, every bank shall identify a single reference point within their organisation to whom bank staff are instructed to promptly report transactions suspected of being connected with money-laundering or terrorist financing.
- (d) Policies, procedures, controls and training - Every bank shall implement specific policies, procedures and controls for CDD, retention of financial transaction documents, reporting of suspicious transactions and staff training. Every bank shall also ensure that its staff are adequately informed of and trained in matters covered by this Notice.

5 CUSTOMER DUE DILIGENCE

General

- 5.1 No bank shall open or maintain anonymous accounts or accounts in fictitious names.

When CDD is required

- 5.2 Every bank shall perform CDD measures in accordance with this Notice when:
 - (a) establishing business relations with any person, which expression includes opening an account for the use of the person or providing any financial service to the person with or without an account being opened;
 - (b) the bank suspects that a transaction is connected with money laundering or terrorist financing, regardless of any exemption or threshold otherwise provided for in this Notice; and
 - (c) the bank has doubt about the veracity or adequacy of previously obtained information relating to the customer, of beneficial owner(s), the purpose and intended nature of business relations (whether between the bank and the customer, or between the customer and the beneficial owner) or its understanding or expectation of the way business relations are to be conducted.

CDD Measures

Customer Identification

- 5.3 Every bank shall identify their customers. The information to be obtained by banks to identify their customers shall include, in respect of each customer:
- (a) Full name of the customer (including all aliases used);
 - (b) Unique identification number (such as Singapore NRIC number, birth certificate number, Singapore or foreign passport number, Singapore-issued foreign identification number, company incorporation number, business registration number, or tax reference number);
 - (c) Permanent residential address, registered or business address (as may be appropriate) and contact telephone number(s);
 - (d) Date of birth, incorporation or registration (as may be appropriate); and
 - (e) Nationality, place of incorporation or registration (as may be appropriate).

Verification of customer's identity

- 5.4 Every bank shall verify a customer's identity using reliable, independent sources.
- 5.5 Every bank shall retain copies of documents used in verifying the customer's identity. Where copies cannot be made, the bank shall procure that the bank officer who had sight of the original document record immediately:
- (a) all the information specified in paragraph 5.3;
 - (b) the title and description of the original document produced to the bank officer;
 - (c) the reasons why copies could not be made;
 - (d) the name of the bank officer attending to the customer and a statement certifying that the bank officer has verified each of the specified information against the specified original documents; and
 - (e) the date and time the record is made.

Beneficial Ownership

- 5.6 Every bank shall identify the beneficial owner and take all reasonable measures to verify the identity of the beneficial owner using reliable, independent sources.

- (a) For all customers, the bank shall determine whether the customer is acting on behalf or for the benefit of another person and take all reasonable steps to obtain sufficient information to verify the identity of that other person.
- (b) For customers that are legal persons, the bank shall:
 - (i) take all reasonable measures to understand the ownership and control structure of the customer; and
 - (ii) determine who are the natural persons that ultimately own or control the customer, including those persons who exercise ultimate effective control over the customer.
- (c) Where the ownership and control structure of the customer is such that there does not appear to be any person capable of exercising effective control over the customer, the bank shall only be required to identify and verify the identity of the person for whom the customer directly acts and understand the general ownership and control structure of that customer.

5.7 The procedure for identifying and verifying the identity of the beneficial owner shall be the same as that to be applied for identifying and verifying the identity of the customer.

5.8 Every bank shall also observe the conduct of the customer's account during the course of business relations. Where the observed conduct reasonably suggests that the customer or any person known to the bank as the beneficial owner is not the true beneficial owner, the bank shall take all reasonable measures to verify the accuracy of the information previously obtained, and if necessary re-perform CDD.

Obtaining information on the purpose and intended nature of business relations

5.9 Every bank shall record in reasonable detail in its file on each customer, the purpose and intended nature of business relations with the customer. For efficiency and to facilitate recording, a bank may predefine categories of common purposes or types of business relations. However, the bank shall ensure that categories are sufficiently specific to provide the bank with an accurate and clear understanding of the purpose and nature of each business relation.

On-going monitoring

5.10 Every bank shall perform ongoing monitoring of business relations with customers and scrutinise transactions undertaken, to ensure that the transactions are consistent with the bank's knowledge of the customer and the customer's business and risk profile (as determined by the bank) and where necessary, the source of funds.

Joint accounts

- 5.11 In respect of joint accounts, every bank shall perform the CDD measures on all of the joint account holders.

CDD measures specific to natural persons

- 5.12 Every bank shall verify the customer's identity against original documents of identity issued by an official authority (bearing a recent photograph of the customer).

CDD measures specific to legal persons

- 5.13 In addition to the information set out in paragraph 5.3 in respect of the customer, every bank shall also obtain the following from a customer who is an incorporated legal person:

- (a) The information set out at paragraph 5.3 in respect of all directors; and
- (b) The information set out at paragraph 5.3 in respect of any other person acting on behalf of the customer in its business relations with the bank.

- 5.14 In addition to the information set out in paragraph 5.3, every bank shall also obtain the following from a customer who is an unincorporated legal person:

- (a) For a sole proprietorship, the information set out at paragraph 5.3 in respect of the sole proprietor and of any other person acting on behalf of the customer in its business relations with the bank;
- (b) For a partnership, the information set out at paragraph 5.3 above in respect of all partners and of any other person acting on behalf of the customer in its business relations with the bank;
- (c) For other unincorporated legal persons, the information set out at paragraph 5.3 above in respect of all persons having executive authority and of any other person acting on behalf of the customer in respect of its business relations with the bank.

- 5.15 Every bank shall verify the information obtained against information or documents from the relevant authority or official registry. Where the bank obtains such information or documents through the customer or other third party, the bank shall ensure that there is satisfactory evidence to show that the information or documents have been provided or endorsed by the relevant authority or official registry. Such information or documents shall be current at the time of their provision to the bank.

- 5.16 Where the customer is a legal person, every bank shall verify that all persons purporting to act on behalf of the customer are in fact authorised to do so. In addition to obtaining account opening documents from the customer

appointing signatories and containing specimen signatures, banks shall obtain at least the following:

- (a) In respect of an incorporated legal person:
 - (i) a certified extract of directors' resolution authorising the named person(s) to act on behalf of the customer in establishing and conducting business relations with the bank; and
 - (ii) a certified copy of the memorandum and articles of association or other constitutional document, regulating the power to bind the customer.
- (b) In respect of an unincorporated legal person:
 - (i) a certified extract of the resolution of the customer's decision making body, authorising the named person(s) to act on behalf of the customer in establishing and conducting business relations with the bank;
 - (ii) certified copies of the customer's constitutional documents, regulating the power to bind the customer.
- (c) In respect of a partnership, appropriate documentary evidence that the named person(s) is authorised by all partners to act on their behalf in establishing and conducting business relations with the bank.

5.17 Where the customer is incorporated or established outside Singapore and the circumstances pertaining to the customer are such that no relevant authority or official registry exists, or the required documents or information are unavailable or inadequate, the bank shall obtain comparable documents. However, as different countries and jurisdictions have varying legal regimes and standards of control, attention shall be paid to the origin of such documents and their reliability. The bank shall require the customer to furnish the original copies or certified copies of all such documents.

5.18 Where the customer is a Singapore government entity, banks shall only be required to obtain such information as may be required to confirm that the customer is in fact a Singapore government entity as asserted.

5.19 Where the customer is a foreign government entity, the bank shall perform the CDD measures set out in this Notice as far as possible, obtaining where necessary comparable documents. If the bank is not familiar with the foreign country or jurisdiction with which the customer is connected, it shall as far as possible rely on reliable, independent sources not related to that foreign country or jurisdiction.

Transactions Undertaken for Non-Account Holders

- 5.20 Every bank that undertakes a transaction for a customer who does not have an account with the bank shall, unless the transaction is entirely an exempted transaction:
- (a) identify the customer and verify the identity of the customer in accordance with paragraphs 5.3 to 5.19; and
 - (b) record sufficient details of the transaction as to enable the transaction to be accurately described, including at least the type, currency, value and value date of the transaction, and the identity of the beneficiary (if any).
- 5.21 For the purposes of paragraph 5.20, “exempted transaction” means any of the following transactions of a value not exceeding the sum of S\$20,000 (or its equivalent in any currency):
- (a) Money changing;
 - (b) Cheque encashing;
 - (c) Cash withdrawal using a debit card or credit card;
 - (d) Sale, or top-up of, or withdrawal of value from, any other stored value card or stored value facility;
 - (e) Bill payment, where payment is made to a bank in Singapore or into a person’s account with a bank in Singapore and the paying bank has no grounds to believe that the CDD measures in this Notice have not been satisfactorily performed on the payee by the payee bank.

Provided always that a transaction shall not be an exempted transaction if the bank suspects that it is connected with money laundering or terrorist financing.

- 5.22 Where it appears to a bank that two or more transactions are related, linked or are the result of having been deliberately split up into separate transactions of smaller values in order to evade the measures that banks are required to take under this Notice, the bank shall treat such transactions as a single transaction and accordingly aggregate them when determining the actual value.

Non Face-to-Face Verification

- 5.23 Every bank shall assess the risk of money laundering or terrorist financing posed by the provision of financial service or transactions that do not involve face-to-face contact and implement specific and effective CDD measures to address this risk. In particular, every bank shall take particular care when establishing business relations and conducting ongoing monitoring of business relations operated via the internet, post or telephone, especially in relation to cheque and money transmission facilities.

- 5.24 Every bank's CDD measures for non face-to-face contact shall be at least as stringent as those performed where there is face-to-face contact. Banks shall also take appropriate steps to guard against fraud and fictitious applications.
- 5.25 Every bank shall consider conducting one or more of the following additional checks in respect of any customer who wishes to establish business relations with the bank without face-to-face contact:
- (a) Telephone contact with the customer at an independently verifiable residential or business number;
 - (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 the employer's personnel department at a listed business number;
 - (d) Confirmation of the customer's salary details by requiring the presentation of recent bank statements from another bank;
 - (e) Certification of documents presented by lawyers or notary publics;
 - (f) Requiring the customer to make an initial deposit using a cheque drawn on another bank in Singapore

Reliance on identification and verification already performed

- 5.26 When a bank acquires, either in whole or in part, the business of another bank (whether in Singapore or elsewhere), it shall not be necessary to re-perform CDD measures on those customers acquired with the business at the time of acquisition, provided that:
- (a) all customer records (including identification information) are acquired with the business;
 - (b) the acquiring bank has conducted due diligence enquiries and such enquiries do not raise any doubt that the AML/CFT measures previously adopted by the acquired business meet the requirements of this Notice or, where the acquired business is outside Singapore, requirements equivalent to those in this Notice; and
 - (c) the acquiring bank has no doubt about the veracity or adequacy of customer identification information acquired.

Timing for CDD measures

- 5.27 Unless otherwise provided in this Notice, every bank shall complete the CDD measures specified in this Notice before establishing business relations with any customer.
- 5.28 A bank may establish business relations with a customer without having completed CDD measures only if all of the following conditions are satisfied:
- (a) it is essential for the bank not to interrupt the normal conduct of business; and
 - (b) the risks of money laundering and terrorist financing have been effectively managed by the bank.
- 5.29 For the purposes of paragraph 5.28, MAS may regard the risks of money laundering and terrorist financing as having been effectively managed by a bank where the bank has adopted internal policies, procedures and controls circumscribing the financial services available to the customer, before completion of CDD measures. These shall include limitation of the number, type and value of transactions and the monitoring of large or complex transactions that are outside of expected norms.
- 5.30 Where business relations are permitted to be established before completion of CDD measures:
- (a) Until CDD measures are completed, no bank shall carry out any cross border payment or transfer of funds, except to return funds received to the source;
 - (b) CDD measures shall be completed as soon as practicable and in any event no later than 30 working days after the establishment of business relations;
 - (c) If CDD measures remain uncompleted 30 working days after the establishment of business relations, the bank shall suspend business relations with the customer and no further transactions shall be carried out except to return funds received to their source; and
 - (d) If CDD measures remain uncompleted 90 working days after the establishment of business relations, the bank shall terminate business relations with the customer.

Inability or Failure to complete CDD

- 5.31 Where business relations between the bank and the customer are or are to be terminated due to the inability or failure to complete the CDD measures or where the customer decides on its own accord to terminate business relations when requested to provide information to enable the bank to comply with this Notice, the bank shall consider making a STR in relation to the customer.

- 5.32 When a STR is to be made to STRO before the actual termination of business relations, the bank may, in accordance with any advice or directions from STRO, delay the termination of business relations.
- 5.33 Upon termination of business relations, the bank shall, unless otherwise directed by the relevant authorities, return all funds to their source(s).

Review of customers' identification information

- 5.34 Every bank shall review the adequacy of identification information on all of its customers on the basis of materiality and risk and perform CDD measures on its existing customers at appropriate times.
- 5.35 For purposes of paragraph 5.34, the expression "appropriate times" includes the following:
- (a) when there is a transaction which is significant, having regard to the manner in which the account is ordinarily operated;
 - (b) when there is a substantial change in the customer documentation standards of the bank;
 - (c) when there is a material change in the way that business relations with the customer are conducted;
 - (d) when the bank becomes aware that it may lack sufficient identification information on a customer; and
 - (e) when the bank becomes aware that there may be a change in the ownership or constitution of the customer, or the person(s) authorised to act on behalf of the customer in its business relations with the bank.
- 5.36 Where a bank becomes aware upon a review that it lacks sufficient identification information on a customer, the bank shall proceed as if business relations with that customer have been established without the prior completion of CDD measures, and paragraph 5.30 shall apply accordingly.

6 SIMPLIFIED CUSTOMER DUE DILIGENCE

- 6.1 A bank shall not be required to take all of the CDD measures set out in this Notice but may take simplified CDD measures sufficient to identify and verify the identity of the customer or beneficial owner in the following circumstances:
- (a) where information on the identity of the customer or beneficial owner (as the case may be) is publicly available;
 - (b) where the bank is satisfied that adequate AML/CFT measures in respect of the customer or beneficial owner (as the case may be) exist elsewhere in the legal system; or

- (c) in any other case where the bank is satisfied that the risk of money laundering or terrorist financing is low.
- 6.2 A bank shall not be required to identify or verify the identity of the beneficial owner, in relation to the following:
- (a) Singapore government entities and companies wholly owned by the Singapore government;
 - (b) Foreign government entities and legal persons wholly owned by a foreign government;
 - (c) Public companies listed on the Singapore Exchange;
 - (d) Public companies listed on stock exchanges outside of Singapore and subject to regulatory disclosure requirements;
 - (e) Financial institutions supervised by MAS (other than money changers and money remitters);
 - (f) Financial institutions incorporated or established outside Singapore and are subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the Financial Action Task Force.
- 6.3 In all cases where the bank relies on paragraphs 6.1(a), (b), (c) or 6.2(f), the bank shall document the basis for its determination that the requirements in paragraphs 6.1(a), (b), (c) or 6.2(f) (as the case may be) have been met.

7 ENHANCED CUSTOMER DUE DILIGENCE FOR POLITICALLY EXPOSED PERSONS

- 7.1 PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials. The term does not include middle ranking or more junior individuals in the foregoing categories. The term however does include family members (namely, spouses, parents, children and siblings) and close associates of the individuals in the foregoing categories.
- 7.2 Every bank shall, in addition to performing the CDD measures set out in paragraph 5, take all of the following enhanced measures:
- (a) Put in place internal policies, procedures and controls to determine whether a potential customer, a customer or beneficial owner is a PEP (which may include measures such as seeking information from the

customer, referring to publicly available information, querying affiliates and accessing reliable third party databases and information sources).

- (b) Obtain senior management approval before establishing business relations with a customer who is determined to be a PEP, and where a customer is initially accepted but the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, obtain senior management approval to continue business relations.
- (c) Take all reasonable measures to establish and document the source of wealth and source of funds of customers and beneficial owners determined to be PEPs.
- (d) Conduct enhanced ongoing monitoring of all business relations where the customer or beneficial owner is determined to be a PEP by reviewing the conduct of business relations with the customer for suspicious transaction and the adequacy of customer identification information at least once every two years. If there had been no previous review of business relations in respect of the customer, the first review shall cover a period of at least four years preceding the review.

8 OTHER HIGHER RISK CATEGORIES

- 8.1 The enhanced measures set out in paragraph 7.2 shall also be performed for such other categories of customers, business relations or transactions as the bank may consider to present a higher risk for money laundering and terrorist financing. Examples of higher risk categories would include, but are not limited to non-resident customers, private banking customers, legal persons used as personal asset holding vehicles, and companies that have nominee shareholders or issue shares in bearer form.

Countries or Jurisdictions with Inadequate AML/CFT Measures

- 8.2 Every bank shall give special attention to business relations and transactions with persons, whether natural or legal persons, from or in such countries and jurisdictions with inadequate AML/CFT measures as may be determined by the bank or as may be notified to all banks by MAS from time to time.

9 PERFORMANCE OF CUSTOMER DUE DILIGENCE BY INTERMEDIARIES

- 9.1 A bank may rely on an intermediary to perform elements of the applicable CDD measures on its behalf, provided that all of the following requirements are met:
- (a) The bank is satisfied that each intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements,

and that the intermediary has measures in place to comply with this Notice or measures equivalent thereto;

- (b) The bank ensures that the intermediary provides to it all the information required to be obtained, and within the time allowed to the bank, under this Notice.

9.2 Where the intermediary is a financial institution supervised by MAS (other than a money changer and remittance agent), the bank may regard the requirements of paragraph 9.1(a) as met, unless notified by MAS to the contrary. In all other cases, the bank shall document the basis of its determination that the requirements of paragraph 9.1(a) and (b) have been met.

9.3 Notwithstanding any permitted reliance on intermediaries, the bank shall remain ultimately responsible for the proper performance of CDD measures and compliance with this Notice.

9.4 For the avoidance of doubt, a person acting under a contractual outsourcing arrangement with a bank to discharge the bank's CDD responsibilities under this Notice shall not be regarded as an intermediary for the purposes of paragraph 9. In such an outsourcing arrangement, the performance of CDD measures by the outsourcee shall be deemed to be a performance by the bank itself, to which the full requirements of paragraph 5 shall apply.

10 CORRESPONDENT BANKING

10.1 For the purposes of paragraphs 10.1 to 10.4:

“correspondent banking” means the provision of banking services by one bank (“the correspondent bank”) to another bank (“the respondent bank”);

“cross-border corresponding banking” means corresponding banking where the correspondent bank and the respondent bank are in different countries or jurisdictions;

“payable-through account” means a correspondent account that is used directly by a third party to transact business on its own behalf; and

“shell bank” means a bank incorporated or established in a country or jurisdiction in which it has no physical presence.

10.2 Every bank shall, in addition to performing the CDD measures set out in paragraph 5, take the following measures in relation to cross-border correspondent banking relations:

- (a) Assess the suitability of entering into a correspondent banking relationship by:

- (i) Gathering sufficient information about the respondent bank to understand fully the nature of the respondent bank's business, including but not limited to making queries on its management, major business activities and the country or jurisdiction from which it operates;
 - (ii) Determining from publicly available sources the reputation of the respondent bank and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action; and
 - (iii) Considering the respondent bank's AML/CFT controls and ascertaining that they are adequate and effective, keeping in mind the adequacy of AML/CFT measures of the country or jurisdiction in which the respondent bank (or the relevant branch) operates.
- (b) Obtain approval from senior management before establishing new correspondent banking relations; and
 - (c) Document the respective AML/CFT responsibilities of each bank.

10.3 Where a correspondent banking relation involves a payable-through account, the correspondent bank shall further satisfy itself that:

- (a) the respondent bank has performed CDD measures on the customer having direct access to the account of the correspondent bank; and
- (b) the respondent bank is able to perform ongoing monitoring of its business relations with the customer having such direct access and to provide customer identification information upon request to the correspondent bank.

10.4 Banks shall not enter into, or continue, correspondent banking relations with shell banks. Banks shall also guard against establishing correspondent banking relations with any respondent bank that permit their accounts to be used by shell banks.

11 WIRE TRANSFERS

11.1 For the purposes of paragraphs 11.1 to 11.5:

“cross-border wire transfer” means a wire transfer where the ordering bank and the beneficiary bank are in different countries or jurisdictions;

“domestic wire transfer” means a wire transfer where both the ordering and the beneficiary bank are in the same country or jurisdiction;

“originator” means the person requesting a bank to effect a wire transfer of funds;

“ordering bank” means the bank which acts on behalf of the originator in ordering or initiating the wire transfer;

“beneficiary” means the person to whom or for whose benefit the funds are to be sent by wire transfer; and

“beneficiary bank” means the bank which acts for the beneficiary in receiving the funds from a wire transfer.

Responsibility of the ordering bank

Identification and recording of information

- 11.2 Before effecting any wire transfer, every ordering bank shall identify and record the identification information of the originator and the particulars of the wire transfer.
- (a) The ordering bank shall record the identification information of the originator as set out in paragraph 5.3. Where the originator is a customer of the ordering bank and the required identification information is already available with the ordering bank, the ordering bank may, in lieu of recording the identification information, assign to the wire transfer a reference number that would enable the ordering bank to relate the customer and his relevant identification information to the wire transfer.
 - (b) The particulars of the wire transfer to be recorded shall be of sufficient detail so as to enable the wire transfer to be accurately described. The particulars to be recorded shall include but are not limited to the amount, currency, value date, the identity of the beneficiary and of the beneficiary bank.

Cross-border Wire Transfers

- 11.3 In relation to a cross-border wire transfer where the amount to be transferred exceeds the sum of (a threshold to be determined later), the ordering bank shall include and obtain customer consent to include in the message accompanying the wire transfer:
- (a) the name of the originator;
 - (b) the originator’s account number (or a unique reference number where no account exists); and
 - (c) the originator’s address.

Domestic Wire Transfers

- 11.4 In relation to a domestic wire transfer, the ordering bank shall include and obtain customer consent to include in the message accompanying the wire transfer all originator information required to be included in the case of a cross-border wire transfer. Alternatively, the ordering bank may include only the originator's account number (or unique reference number where the originator does not have an account with the ordering bank) but in such a case, the ordering bank shall have to be in the position to provide full originator information to the beneficiary bank or to STRO within 3 working days of its receiving a request.

Responsibility of the beneficiary bank

- 11.5 Every beneficiary bank shall adopt such risk-based procedures as may be appropriate for identifying and handling wire transfers that are not accompanied by complete originator information. Such procedures could include but are not limited to requesting for the missing originator information from the ordering bank, and if the missing information is not forthcoming considering whether in all the circumstances the absence of complete originator information creates or contributes to suspicion, and whether there is a case for making an STR. In appropriate circumstances, the beneficiary bank shall consider not accepting wire transfers from or terminating business relations with ordering banks that are required to but do not provide complete originator information.

12 RECORD KEEPING

- 12.1 Every bank shall prepare, maintain and retain documentation on all their business relations and transactions with their customers, such that:
- (a) all requirements imposed by law (including this Notice) are met;
 - (b) any transaction effected through the bank can be reconstructed;
 - (c) the relevant authorities in Singapore and the internal and external auditors of the bank are able to assess the bank's transactions and level of compliance with this Notice; and
 - (d) it can satisfy, within a reasonable time, any enquiry or order from the relevant authorities in Singapore for information regarding its customers and their financial activities.
- 12.2 Every bank shall maintain a complete file on all transactions that have been referred to the compliance officer responsible for suspicious transaction reporting, including transactions referred but not reported to STRO. Records of all these transactions shall be kept together with the findings of the compliance officer evaluating them.

- 12.3 Every bank, in setting their record retention policies, shall comply with the following document retention periods:
- (a) Customer identification information, and other documents related to the establishment of business relations, as well as account files and business correspondence, shall be kept for at least 6 years following termination of business relations.
 - (b) Records on transactions, including any information needed to explain and reconstruct a transaction, shall be kept for at least 6 years following completion of the transaction takes place.
- 12.4 Documents may be retained as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible in evidence in a Singapore court of law.
- 12.5 Notwithstanding paragraph 12.3, records pertaining to a matter which is under investigation or which has been the subject of an STR shall be retained for such longer period as may be necessary in accordance with any request or direction from the relevant authorities.

13 REPORTING OF SUSPICIOUS TRANSACTIONS

- 13.1 Under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act and the Terrorism (Suppression of Financing) Act, a bank (as is any other person) is obliged to report a transaction to the authorities if it has reasonable grounds to suspect money laundering or terrorist financing. All suspicious transactions, including attempted transactions, should be reported to STRO. A copy of the STR shall also be extended to MAS for information, addressed to the relevant MAS officer authorised to receive STRs.
- 13.2 Each bank shall institute an internal procedure for handling and reporting suspicious transactions. This includes appointing one or more senior officers to be responsible for submitting STRs. Subject to any regulations made or directions given by the relevant authorities, banks shall follow the reporting formats set out in Appendices III to V. In the event that urgent disclosure is required, particularly where a transaction is known to be part of an on-going investigation by the relevant authorities, banks shall give initial notification to STRO by telephone and follow up with such other means of reporting as STRO may direct.
- 13.3 Bank staff who suspect that a transaction is connected with money laundering or terrorist financing shall refer the case to the relevant compliance officer within the bank, in accordance with the bank's internal procedures. The compliance officer shall promptly evaluate whether there is a case for making an STR. If there is, the compliance officer shall immediately file an STR with STRO. Except in extraordinary circumstances, banks shall procure that the

internal evaluation process for suspicious transactions be completed within 10 working days of the case being referred to the compliance officer.

- 13.4 Examples of suspicious transactions are found in Appendix II. These are not intended to be exhaustive and are only examples of the most basic ways in which money may be laundered. If transactions such as those in Appendix II are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds. Banks shall also keep watch for suspicious transactions in the course of conducting screening against such lists of terrorist suspects as may exist.
- 13.5 In the course of performing CDD measures, if there arises at any time a suspicion of money laundering or terrorist financing, a bank shall consider:
- (a) whether the continuation of CDD measures poses a material risk that the customer would be unintentionally tipped off; or
 - (b) whether to make a STR while proceeding, at the same time, with the CDD process so as not to compromise subsequent investigations.
- 13.6 Where a STR has been made to STRO and it becomes necessary to make further enquiries with the customer, the bank shall take care to ensure that the customer is not unintentionally tipped off that an STR has been made.

14 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

- 14.1 Each bank shall develop and maintain internal policies, procedures and controls against money laundering and terrorist financing. In formulating such policies, procedures and controls, banks shall take into consideration money laundering and terrorist financing threats that may arise from new or developing technologies that may favour anonymity and take steps to adequately address such threats.

Group Policy

- 14.2 A bank incorporated in Singapore shall communicate the bank's group policy on money laundering and terrorist financing to the management of all branches and subsidiaries located overseas.
- 14.3 Measures to prevent money laundering and terrorist financing at such overseas branches and subsidiaries shall be undertaken at least to the standard required under Singapore law, to the extent that the laws of the host country permit. Where the laws of the host country conflict with Singapore law and the branches or subsidiaries are thereby not able to fully observe the relevant AML/CFT requirements under Singapore law, the head office of the bank shall be notified of this, and it shall be the responsibility of the head office to notify MAS of the extent of any departure from the group policy.

Compliance

- 14.4 Each bank shall appoint a senior officer as the compliance officer. The compliance officer, reporting to the bank's management, shall be given the following responsibilities:
- (a) To ensure a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;
 - (b) To advise the bank's management and staff on developing and implementing internal policies, procedures and controls on AML/CFT;
 - (c) To carry out or oversee the carrying out of on-going monitoring of business relations and sample reviewing of accounts for compliance with CDD requirements; and
 - (d) To promote compliance with this Notice, including in particular observance of the basic principles in paragraph 4, and to take charge of all other matters connected with AML/CFT generally.
- 14.5 Every bank shall ensure that the compliance officer and any other persons appointed to assist the compliance officer have timely access to all customer records and other relevant information which they require to discharge their functions. This shall include, where necessary, accounts of customers to which access would normally have been restricted.

Audit

- 14.6 Every bank shall arrange that its internal auditors assess on a regular basis the effectiveness of all measures taken by the bank to prevent money laundering and terrorist financing.

Training

- 14.7 Every bank shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are adequately acquainted with:
- (a) their individual responsibilities and roles in combating money laundering and terrorist financing;
 - (b) prevailing techniques, methods and trends in money laundering and terrorist financing; and
 - (c) the bank's internal policies, procedures and controls on AML/CFT and for reporting suspicious transactions.
- 14.8 Every bank shall educate all relevant staff on the importance of CDD measures in helping to prevent money laundering and terrorist financing.

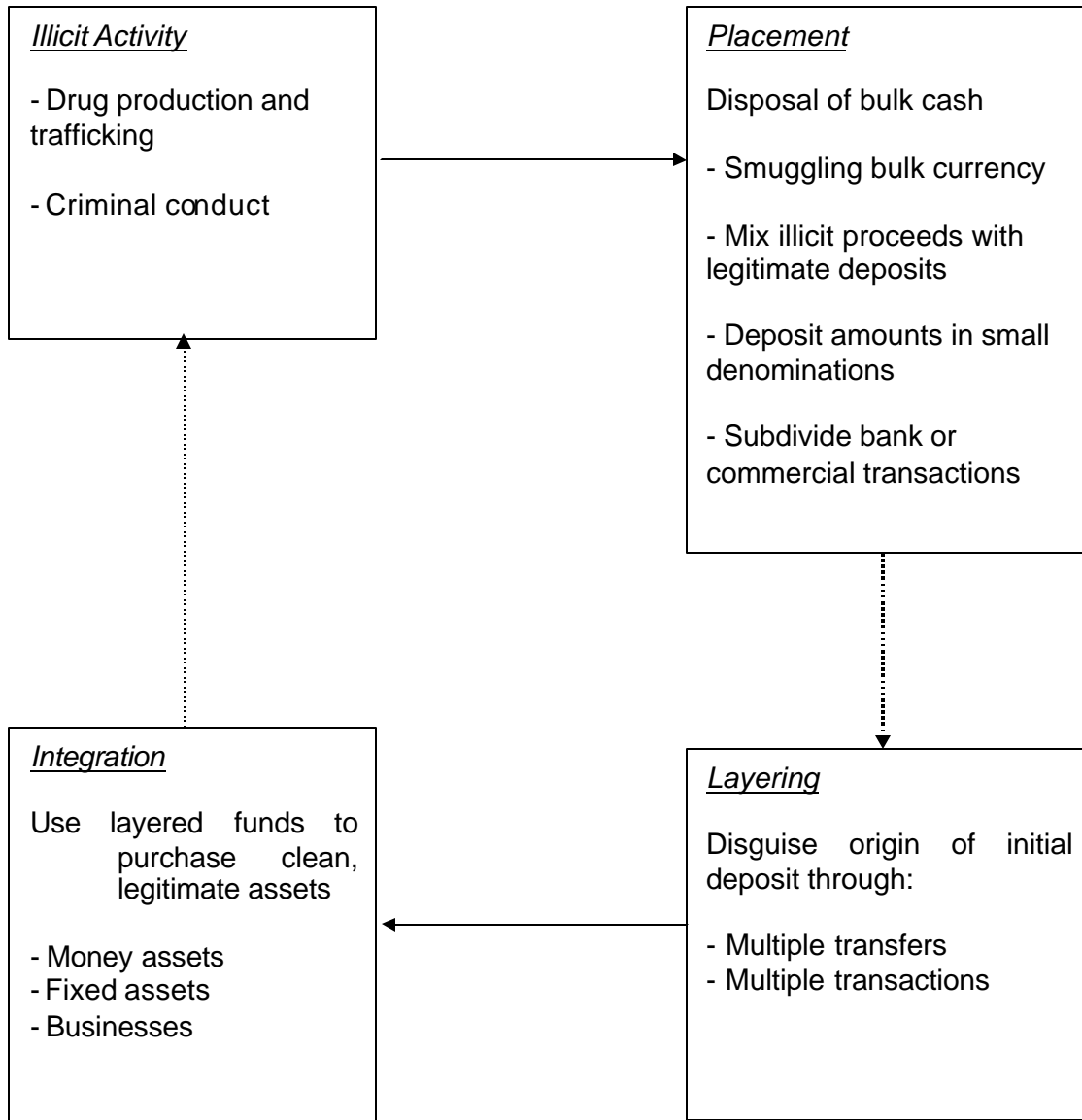
- (a) Training in this respect shall cover not only the importance of knowing the true identities of the persons the bank is dealing with, but also, where business relations have already been established, the importance of knowing at the outset enough about the transactions expected in relation to the customer, in order to know at a later date what might constitute suspicious transactions with respect to that customer.
- (b) Training shall also include educating staff to detect and be alert to any changes in the pattern of customers' transactions or to changes in circumstances that might suggest money laundering or terrorist financing.

14.9 Every bank may adapt the timing and content of training for various categories of bank staff in accordance with its operational needs. However, any such adaptation shall take into account the bank's assessment of the relative risks of money laundering and terrorist financing.

14.10 Every bank shall provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training for staff shall ordinarily be held at least once a year.

14.11 To ensure the effectiveness of all training conducted, staff attendance shall be monitored and appropriate follow-up action shall be taken in relation to staff who absent themselves without reasonable cause.

PROCESS OF MONEY LAUNDERING



EXAMPLES OF SUSPICIOUS TRANSACTIONS

1 General Comments

The list of situations given below is intended mainly as a means of highlighting the basic ways in which money may be laundered. While each individual situation may not be sufficient to suggest that money laundering is taking place, a combination of such situations may be indicative of such a transaction. Further, the list is by no means complete, and will require constant updating and adaptation to changing circumstances and new methods of laundering money. The list is intended solely as an aid, and must not be applied as a routine instrument in place of common sense.

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.

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

2 Transactions Which Do Not Make Economic Sense

- i) A customer-relationship with the bank that does not appear to make economic sense, for example, a customer having a large number of accounts with the same bank, frequent transfers between different accounts or exaggeratedly high liquidity.
- ii) Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.
- iii) Transactions that cannot be reconciled with the usual activities of the customer, for example, the use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
- iv) Transactions which, without plausible reason, result in the intensive use of what was previously a relatively inactive account, such as a customer's account which shows virtually no normal personal or business related activities but is used to receive or disburse unusually large sums which have no obvious purpose or relationship to the customer and/or his business.

- v) Provision of bank guarantees or indemnities as collateral for loans between third parties that are not in conformity with market conditions.
- vi) Unexpected repayment of an overdue credit without any plausible explanation.
- vii) Back-to-back loans without any identifiable and legally admissible purpose.

3 Transactions Involving Large Amounts of Cash

- i) Exchanging an unusually large amount of small-denominated notes for those of higher denomination.
- ii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank.
- iii) Frequent withdrawal of large amounts by means of cheques, including traveller's cheques.
- iv) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity.
- v) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- vi) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange, etc.
- vii) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.
- viii) The deposit of unusually large amounts of cash by a customer to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments.
- ix) Customers whose deposits contain counterfeit notes or forged instruments.
- x) Large cash deposits using night safe facilities, thereby avoiding direct contact with the bank.

- xi) Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their business.
- xii) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

4 Transactions Involving Bank Accounts

- i) Matching of payments out with credits paid in by cash on the same or previous day.
- ii) Paying in large third party cheques endorsed in favour of the customer.
- iii) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.
- iv) High velocity of funds through an account, i.e., low beginning and ending daily balances, which do not reflect the large volume of funds flowing through an account.
- v) Multiple depositors using a single bank account.
- vi) An account opened in the name of a moneychanger that receives structured deposits.
- vii) An account operated in the name of an offshore company with structured movement of funds.

5 Transactions Involving Transfers Abroad

- i) Transfer of money abroad by an interim customer¹ in the absence of any legitimate reason.
- ii) A customer who appears to have accounts with several banks in the same locality, especially when the bank is aware of a regular consolidated process from such accounts prior to a request for onward transmission of the funds elsewhere.
- iii) Repeated transfers of large amounts of money abroad accompanied by the instruction to pay the beneficiary in cash.

¹ An interim customer is one who is not a regular customer of the bank in question, or does not maintain an account, deposit account, safe deposit box, etc. with the bank.

- iv) Large and regular payments that cannot be clearly identified as bona fide transactions, from and to countries associated with (i) the production, processing or marketing of narcotics or other illegal drugs or (ii) criminal conduct.
- v) Substantial increase in cash deposits by a customer without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.
- vi) Building up large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.
- vii) Cash payments remitted to a single account by a large number of different persons without an adequate explanation.

6 Investment Related Transactions

- i) Purchasing of securities to be held by the bank in safe custody, where this does not appear appropriate given the customer's apparent standing.
- ii) Requests by a customer for investment management services where the source of funds is unclear or not consistent with the customer's apparent standing.
- iii) Larger or unusual settlements of securities transactions in cash form.
- iv) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

7 Transactions Involving Unidentified Parties

- i) Provision of collateral by way of pledge or guarantee without any discernible plausible reason by third parties unknown to the bank and who have no identifiable close relationship with the customer.
- ii) Transfer of money to another bank without indication of the beneficiary.
- iii) Payment orders with inaccurate information concerning the person placing the orders.
- iv) Use of pseudonyms or numbered accounts for effecting commercial transactions by enterprises active in trade and industry.

- v) Holding in trust of shares in an unlisted company whose activities cannot be ascertained by the bank.
- vi) Customers who wish to maintain a number of trustee or clients' accounts that do not appear consistent with their type of business, including transactions that involve nominee names.

8 Miscellaneous Transactions

- i) Purchase or sale of large amounts of precious metals by an interim customer.
- ii) Purchase of bank cheques on a large scale by an interim customer.
- iii) Extensive or increased use of safe deposit facilities that do not appear to be justified by the customer's personal or business activities.

APPENDIX III

Reporting Format

- (1) Reporting of Suspicious Money Laundering Transactions pursuant to Section 39, Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act
- (2) Reporting of Suspicious Terrorist Financing Activities pursuant to Section 8, Terrorism (Suppression of Financing) Act

NATURAL PERSONS

Reporting Bank	
Name:	
Branch:	
Address:	
Telephone:	
Fax :	
E-mail :	
Bank Reporting Officer	
Name:	
Designation:	
Report Reference:	
Contact Officer (if different from Reporting Officer):	
Designation:	
Customer's Particulars #	
Name:	
NRIC/Passport No.:	
Birth Date:	
Nationality:	
Address:	
Telephone:	
Occupation:	
Date when particulars were last updated (where available):	
# The reporting officer of the bank shall provide particulars on joint account holders, if any.	
Employment Details	
Employer's Name:	
Address:	

Telephone:	
Business Relationship(s) with Customer	
Bank A/c No.:	
Type of A/c:	
Date A/c Opened:	
A/c Balance (Dr/Cr*)	
As At Date:	
Other Business Relationships:	

Suspicious Transaction(s)		
Amount (Dr/Cr*)	Date	Description of Transaction (E.g. Funds transfer, source of funds, destination, etc)

Reason(s) for Suspicion:

Other Relevant Information (including information on other accounts that may be linked to the transaction(s) and any actions taken by the reporting entity in response to the transaction):

A copy of the following documents are attached:

- Account Opening Forms
- Customer Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

* Delete whichever is inappropriate

APPENDIX IV

Reporting Format

- (1) Reporting of Suspicious Money Laundering Transactions pursuant to Section 39, Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act
- (2) Reporting of Suspicious Terrorist Financing Activities pursuant to Section 8, Terrorism (Suppression of Financing) Act

CORPORATIONS

Reporting Bank	
Name:	
Branch:	
Address:	
Telephone:	
Fax :	
E-mail :	
Bank Reporting Officer	
Name:	
Designation:	
Report Reference:	
Contact Officer (if different from Reporting Officer):	
Designation:	
Customer's Particulars	
Name:	
Country of Registration:	
Registration Date:	
Registration No.:	
Address:	
Telephone:	
Name of CEO:	
Date when particulars were last updated (where available):	
Business Relationship(s) with Customer	
Bank A/c No.:	
Type of A/c.:	
Date A/c Opened:	

A/c Balance (Dr/Cr*)	
As At Date:	
Other Business Relationships:	

Authorised Signatories' Particulars #	
1. Name:	
Birth Date:	
Nationality:	
NRIC/Passport No.:	
Home Address:	

The reporting officer of the bank shall provide data on other authorised signatories, if any.

Suspicious Transaction(s)		
Amount (Dr/Cr*)	Date	Description of Transaction (E.g. Funds transfer, source of funds, destination, etc)

Reason(s) for Suspicion:

Other Relevant Information (including information on other accounts that may be linked to the transaction(s) and any actions taken by the reporting entity in response to the transaction):

A copy of the following documents are attached:

- Account Opening Forms
- Customer Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

* Delete whichever is inappropriate

APPENDIX V

Reporting Format

- (1) Reporting of Suspicious Money Laundering Transactions pursuant to Section 39, Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act
- (2) Reporting of Suspicious Terrorist Financing Activities pursuant to Section 8, Terrorism (Suppression of Financing) Act

* PARTNERSHIPS/ SOLE PROPRIETORS/ CLUBS & SOCIETIES

Reporting Bank	
Name:	
Branch :	
Address:	
Telephone:	
Fax :	
E-mail :	
Bank Reporting Officer	
Name:	
Designation:	
Report Reference:	
Contact Officer: (if different from Reporting Officer)	
Designation:	
Customer's Particulars	
Name:	
Country of Registration:	
Registration Date:	
Registration No.:	
Address:	
Telephone:	
Name of Partners/ Sole-Proprietors/ Trustees or equivalent:	
Date when particulars were last updated (where available):	
Business Relationship(s) with Customer	
Bank A/c No.:	
Type of A/c.:	

Date A/c Opened:	
A/c Balance (Dr/Cr*)	
As At Date:	
Other Business Relationships:	

Authorised Signatories' Particulars #	
1. Name:	
Birth Date:	
Nationality:	
NRIC/Passport No.:	
Home Address:	
Occupation:	
Employer's Name: (If applicable)	
Address:	

The reporting officer of the bank shall provide data on other authorised signatories, if any.

Suspicious Transaction(s)		
Amount (Dr/Cr*)	Date	Description of Transaction (E.g. Funds transfer, source of funds, destination, etc)

Reason(s) for Suspicion:

Other Relevant Information (Including information on other accounts that may be linked to the transaction(s) and any actions taken by the reporting entity in response to the transaction):

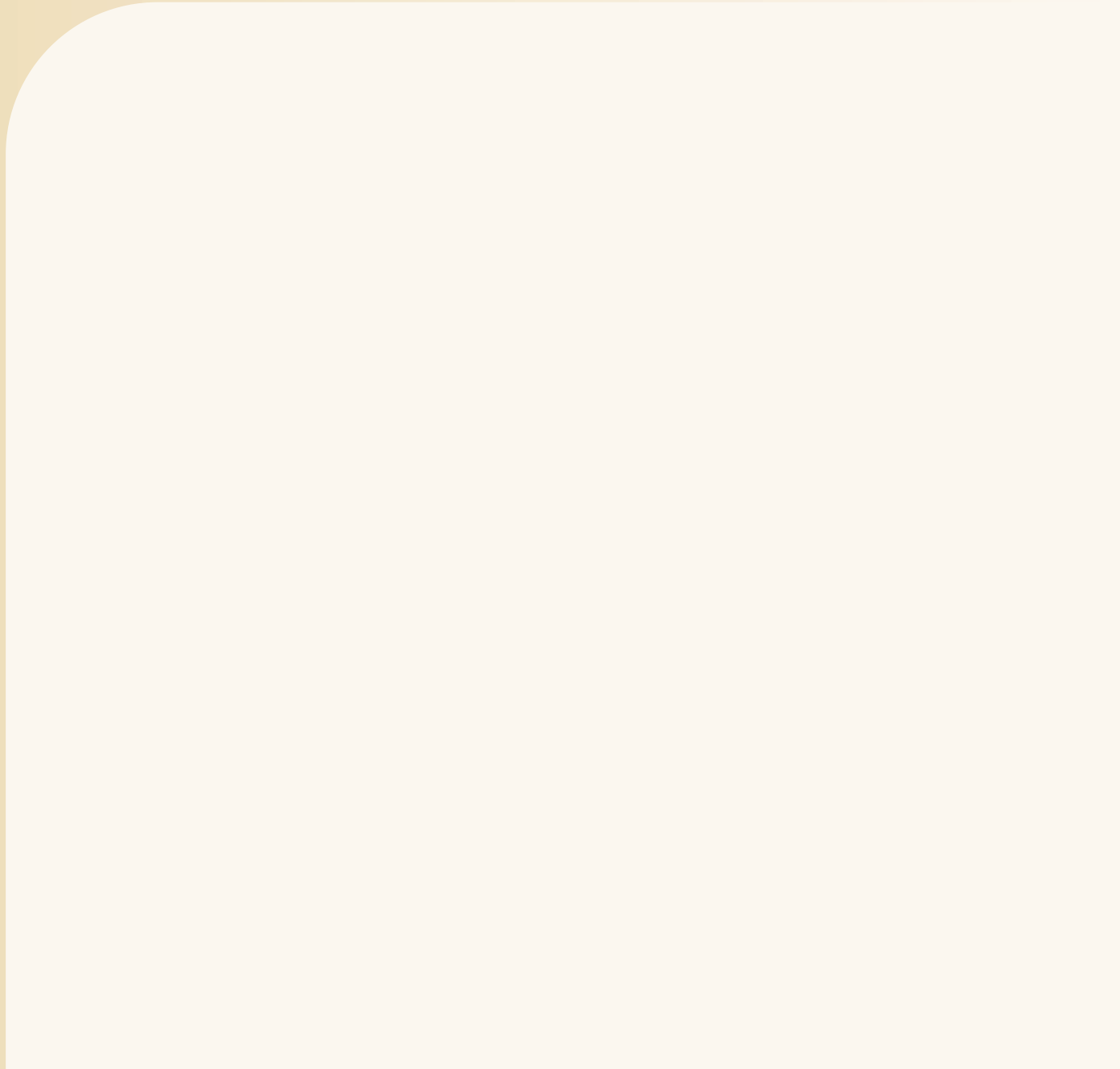
A copy of the following documents are attached:

- Account Opening Forms
- Customer Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

* Delete whichever is inappropriate

(Signature of Reporting Officer)

Date:



Monetary Authority of Singapore