CONSULTATION PAPER

P010 - 2006
August 2006

Draft Guidelines to Notices on Prevention of Money Laundering and Countering the Financing of Terrorism

Monetary Authority of Singapore

PUBLIC CONSULTATION ON GUIDELINES TO DRAFT NOTICES TO FINANCIAL INSTITUTIONS ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

PREFACE

The Monetary Authority of Singapore (MAS) issued a Consultation Paper on draft Notices on Prevention of Money Laundering and Countering the Financing of Terrorism on 4 August 2006. These Notices cover nine financial sectors – banks, finance companies, merchant banks, money changers and remitters, life insurers, capital markets intermediaries, financial advisers, approved trustees and trust companies.

Guidelines have been prepared to supplement the draft Notices and hence should be read in conjunction with the respective draft Notices. The objective of this set of Guidelines is to provide further guidance on the requirements set out in the draft Notices.

INVITATION FOR COMMENTS

MAS invites interested parties to provide views and comments on the draft Guidelines. All respondents should note that submissions received by MAS may be made public unless confidentiality is expressly requested in respect of all or any part of the submission.

Submissions in electronic form (Microsoft Word) are strongly preferred, and should be sent via e-mail to the following address: aml@mas.gov.sg

In the alternative, submissions in hard copy format may be delivered by post to:

AML/CFT Policy Unit
External Department
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117

All submissions should be made by 27 September 2006.

TABLE OF CONTENTS

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

[MAS Notice 626]

Introduction

1. These Guidelines are issued to provide guidance to the banks on some of the requirements in MAS Notice 626 (the "Notice") issued on [date].

2. Banks are reminded that the ultimate responsibility and accountability for ensuring the bank's compliance with AML/CFT laws, regulations and guidelines rests with the bank, its board of directors and senior management.

3. The expressions used in these Guidelines shall, except where expressly defined in these Guidelines or where the context otherwise requires, have the same respective meanings as in the Notice.

The structure of MAS Notice 626

4. The Notice sets out the obligations of a bank to take measures to help mitigate the risk of the banking system of Singapore being used for money-laundering or terrorist financing.

5. Paragraph 4 of the Notice deals with CDD measures. This paragraph sets out the standard CDD measures to be applied, of which there are seven principal components:

   - Identification of the customer by obtaining certain information pertaining to the customer and, where the customer is not a natural person, certain other persons associated with that customer;

   - Verifying the identification information obtained;

   - Where the customer is not a natural person, identifying and verifying the identity of its representatives;

   - Determining if there exists any beneficial owner (other than the customer) and applying the identification and verification procedures to those beneficial owners;

- Where business relations are to be established (as defined in the Notice), obtaining information as to the nature and purpose of the intended business relations;

- After business relations are established, conducting on-going monitoring of business relations; and

- After business relations are established, periodically reviewing the adequacy of customer information.

6. Paragraphs 5 and 6 of the Notice provide for the risk-based customisation of the CDD measures. Thus, paragraph 5 on simplified CDD allows a bank to take lesser measures than those specified in paragraph 4 of the Notice provided that the conditions for simplified CDD are met. This will largely be a matter for individual banks to assess, but the bank must be able to justify its decision. Conversely, in situations where PEPs may be involved or in other situations where there is a higher risk of money laundering or terrorist financing, a bank is required under paragraph 6 of the Notice to take enhanced CDD measures.

7. To cater to cross-referrals, paragraph 7 of the Notice allows a bank to rely on another party, an intermediary, to perform certain elements of the CDD process, provided that certain conditions are met. This paragraph may typically be applied where a new customer is introduced to the bank by an intermediary resulting in direct business relations between the bank and the new customer. Thus, if the intermediary has already performed its own CDD on the new customer, then paragraph 7 allows the bank to dispense with performing CDD on the new customer if the conditions are satisfied. Paragraph 7 is not intended to cover the situation where a bank outsources the function of performing CDD measures to a third party. [1]

8. The Notice then deals with two specific situations – the regulatory requirements when establishing correspondent banking relations (paragraph 8), and the requirement to include originator information in cross-border wire transfers (paragraph 9).

9. Finally, the Notice updates the previous requirements with respect to record keeping (paragraph 10), reporting of suspicious transactions (paragraph 11) and the institution of internal policies, procedures and controls for AML/CFT (paragraph 12).

Key Concepts of the Notice

[1] The Notice does not prohibit the outsourcing of the CDD function to a third party but where this occurs, the bank must remain fully responsible and accountable for the conduct of CDD measures as if the function had remained within the bank.

Money Laundering

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

11. 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 criminal conduct;

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

    (c) Integration - The provision of apparent legitimacy to the benefits of 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.

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

Terrorist Financing

12. 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. Banks should refer to the legal definitions of terrorism found in the law such as the Terrorism (Suppression of Financing) Act (Cap. 325), the United Nations (Anti-terrorism Measures) Regulations (Rg 1) and the Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002.

13. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. 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.

14. 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.

15. 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.

Paragraph 2.1 of the Notice – Definition of "Customer"

16. Paragraph 2.1 of the Notice defines "customer", in relation to a bank, as the person in whose name an account is opened or intended to be opened, or to whom a bank undertakes or intends to undertake any transaction without an account being opened.

17. The definition circumscribes the scope of the Notice. Banks should in general seek to perform CDD as widely as possible on persons that they deal with in the course of their banking operations.

18. In the cases below, the following approaches below may be adopted:

(a) Portfolio Managers

A bank may often encounter cases where, to the bank's knowledge, the customer is a manager of a portfolio of assets and is operating the account in that capacity. In such cases, the underlying investors of the portfolio will be beneficial owners within the meaning of the Notice.

However, the Authority recognises that a bank may not be able to perform CDD on the underlying investors. For instance, the portfolio manager may be reluctant, for legitimate commercial reasons, to reveal information on the underlying investors to the bank. In such circumstances, the bank should evaluate the risks arising for each case and determine the appropriate CDD measures to take. The bank may consider whether simplified CDD measures could be applied under paragraph 5 of the

Notice, so that identification and verification of the underlying investors as beneficial owners are dispensed with.

(b) Location of Relationship Management

Given the globalised nature of modern banking, it may often be the case that a bank's relationship and transactions with a particular customer would be managed by bank officers based in one country or jurisdiction but the account itself is held with an office in another country or jurisdiction for book-keeping purposes. For the purposes of the Notice, the Authority will generally look at the substance of the relationship as a whole. A bank should perform CDD if in substance, the person is a customer of the bank in Singapore even though the account is booked in another country or jurisdiction. However, the bank may rely on the CDD done by its related entity in accordance with paragraph 7 of the Notice.

Paragraphs 4.6, 4.8 and 4.9 of the Notice – Identification of Customers that are Not Natural Persons

19. Where the customer is not a natural person, paragraphs 4.6, 4.8 and 4.9 of the Notice require the bank to further establish the identity of the directors, partners or persons having executive authority, of the customer respectively.

20. The bank should assess and determine, with respect to each customer, the key persons whose details they consider necessary to verify.

21. For the purposes of paragraph 20 above, the bank should consider whether persons, either singly or jointly with another, are able to give instructions concerning the use or transfer of funds or assets belonging to the customer in question.

Paragraphs 4.10 and 4.11 of the Notice - Verification of Identity

22. The requirements on verification of identity are intended to ensure that identity information provided by the customer is authentic.

23. Where the person whose identity is to be verified is a natural person, the bank should ask for some form of identification that contains a recent photograph of that person.

24. The bank should retain copies of all documentation used for verification of identity. Only in exceptional circumstances where the bank is unable to

retain a copy of documentation used in verifying the customer's identity, the bank should record the following:

(a) the information that the original documentation had served to verify;

(b) the title and description of the original documentation produced to the bank officer for verification, including any particular or unique features or condition of that documentation (whether it is worn out, or damaged etc);

(c) the reasons why a copy of that documentation could not be made; and

(d) the name of the bank officer who carried out the verification, a statement by that officer certifying that he or she has duly verified the information against the documentation, and the date the verification took place.

Paragraphs 4.16 to 4.19 of the Notice - Identification of Beneficial Owners and Verification of their Identities

25. Banks are under a duty to take steps to determine if there exists, other than the person *ex facie* dealing with the bank as a customer, any other beneficial owner in relation to the customer.

26. Generally, the bank should assess and determine what measures would be appropriate to determine the beneficial owners, if any. The bank should be able to justify the reasonableness of the measures taken, having regard to the circumstances of each case.

27. Where the customer is not a natural person, the bank should take steps such as:

(a) finding out about the ownership and structure of the company; and

(b) identifying the natural persons who have a controlling interest in the customer or who comprise the mind and management of the customer.

28. The bank may also consider obtaining an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner.

29. Paragraph 18(a) of these Guidelines makes reference to the case where the customer is a portfolio manager. In that situation, as well as other

instances where the customer has a *bona fide* and legitimate interest or duty not to disclose to the bank the identity or particulars of beneficial owners who are known to exist, the bank may consider the application of simplified CDD set out in paragraph 5 of the Notice.

30. Paragraph 4.18 of the Notice states that banks are not required to inquire if there exists any beneficial owner beyond the entities specified in sub-paragraphs (a) to (f).

31. The Authority recognises that it would be unnecessary to attempt to determine if beneficial owners exist behind these entities, since adequate information would already be available. For example, in the case of publicly listed companies, the shareholders (who would be the beneficial owners) would be changing relatively frequently and there would already be disclosure obligations imposed on substantial shareholders of such companies. In the case of financial institutions, there would have been adequate disclosure of the ownership and structure to the financial regulator.

32. While the entities listed would also typically be entities for which a bank may consider applying simplified CDD in accordance with paragraph 5 of the Notice, it is not the intent that the bank should thereby deem these entities to be automatically eligible for simplified CDD measures. The bank must comply with the requirements of paragraph 5 of the Notice before applying simplified CDD measures.[2]

Reliability and Authenticity of Information and Documentation

33. Where the bank obtains information or documents through the customer or a third party, the bank should ensure that there is satisfactory evidence to show that the information or documents have been endorsed or otherwise authenticated by the relevant authority or official registry. Such information or documents should be as current as possible at the time they are provided to the bank.

Paragraphs 4.26 and 4.27 of the Notice – Non face-to-face Verification

34. Paragraphs 4.26 and 4.27 of the Notice address the situation where business relations are established or financial services are provided without face-to-face contact. Measures for managing the risks should include specific and effective procedures for CDD that apply to non face-

[2] Banks should further note that where there is actual cause for suspecting money laundering or terrorist financing, the appropriate measures will be required – see paragraph 4.3(c) of the Notice.

to-face customers. In particular, a bank should take appropriate measures to address risks arising from establishing business relations and undertaking transactions through instructions conveyed by customers over the internet, the post or the telephone.

35. As a guide, banks should take one or more of the following measures to mitigate the heightened risk associated with not being able to conduct an interview face-to-face:

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

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

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

(d) confirmation of the customer's salary details by requiring the presentation of recent bank statements from another bank;

(e) certification of identification documents by lawyers or notary publics presented by the customer;

(f) requiring the customer to make an initial deposit using a cheque drawn on the customer's personal account with another bank in Singapore; and

(g) any other reliable verification checks adopted by the bank for non-face- to-face banking business.

Paragraphs 4.32 and 4.33 of the Notice - Deferring the completion of CDD measures: Time limits for completion

36. Paragraph 4.32 of the Notice allows banks to establish business relations before completing the CDD measures if it is essential for the bank not to interrupt the normal conduct of business and if the risks can be effectively managed.

37. An example where it may be essential not to interrupt the normal course of business would be with respect to securities trades, where market conditions are such that the bank has to execute transactions for the customer very rapidly.

38. An example where the bank may have effectively managed the risks of money laundering and terrorist financing is if the bank has adopted internal policies, procedures and controls that set appropriate limits on the financial services available to the customer before completion of CDD measures. These may include, for example, limiting the number, type and value of transactions that might be effected in the interim period, and also the institution of a procedure that is more rigorous and intensive than usual for the monitoring of complex or unusually large transactions.

39. Paragraph 4.33 of the Notice requires that CDD measures be completed as soon as reasonably practicable, if a bank allows business relations to be established without first completing CDD measures. Examples of reasonable timeframe are:

    (a) the bank completing CDD measures no later than 30 working days after the establishment of business relations;

    (b) the bank suspending business relations with the customer and refraining from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if CDD measures remain uncompleted 30 working days after the establishment of business relations; and

    (c) the bank terminating business relations with the customer if CDD measures remain uncompleted 120 working days after the establishment of business relations.

40. The bank should factor these time limitations in their internal policies, procedures and controls.

Paragraph 4.35 of the Notice - Existing Customers

41. Paragraph 4.35 of the Notice concerns the application of CDD measures to the customers and accounts which the bank has as at (date) when the Notice comes into force. Banks are required to review the adequacy of identification information on the basis of materiality and risk, and to perform CDD measures on existing customers as may be appropriate.

42. In relation to accounts for which CDD measures had not previously been applied in accordance with the Notice, the bank should make an assessment with regard to materiality and risk and determine when would be an appropriate time for the performance of CDD measures, subject to the more specific requirements for PEPs specified in paragraph 6.2 of the Notice.

43. As a guide, a bank should perform CDD, in relation to paragraph 42 above, when:

(a) there is a transaction that is significant, having regard to the manner in which the account is ordinarily operated;

(b) there is a substantial change in the bank's own customer documentation standards;

(c) there is a material change in the way that business relations with the customer are conducted;

(d) the bank becomes aware that it may lack adequate identification information on a customer; and

(e) 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.

44. Where a bank becomes aware upon a review that it may lack sufficient identification information on a customer, it should proceed to perform CDD afresh.

Paragraph 5 of the Notice - Simplified Customer Due Diligence

45. Paragraph 5.1 of the Notice allows banks to apply simplified CDD measures in cases where the bank is satisfied that the risk of money laundering or terrorist financing is low.

46. The bank should assess the risks of money laundering or terrorist financing, having regard to the circumstances of each case, before applying the lesser or reduced CDD measures. Where the bank adopts such lesser or reduced CDD measures, such measures should be commensurate with the bank's assessment of the risks.

47. Examples of when the bank might adopt lesser or reduced CDD measures are:

(a) where reliable information on the customer is publicly available to the bank,

(b) the bank is dealing with another bank whose AML/CFT controls it is well familiar with by virtue of a previous course of dealings; or

(c) the customer is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, or a listed company that is subject to regulatory disclosure requirements.

Paragraph 6.2 of the Notice - Identifying and dealing with PEPs

48. The definition of PEPs used in the Notice is drawn from the work of the FATF. The Authority recognises that the process of determining whether an individual is a PEP may not always be straightforward and a more precise definition would carry with it a greater risk of circumvention of the requirements under the Notice.

49. In the circumstances, the Authority would generally consider it acceptable for a bank to refer to databases of PEPs either compiled commercially or by official authorities. However, in doing so, the Authority would expect the bank to exercise a measure of discretion and sound judgment in determining for itself whether an individual should indeed be treated as a PEP, having regard to the risks and the circumstances.

Paragraphs 6.3 and 6.4 of the Notice - Other High Risk Categories

50. Paragraph 6.3 of the Notice requires enhanced CDD measures to be applied to other categories of customers apart from PEPs, which a bank may consider to present a greater risk of money laundering or terrorist financing. Such high risk categories may include, for example, non-resident customers, private banking customers, body corporates set up as personal asset holding vehicles, or companies that have nominee shareholders or that issue shares in bearer form.

51. Banks are also required by paragraph 6.4 of the Notice to give particular attention to business relations and transactions with persons from or in countries that have inadequate AML/CFT measures. For this purpose, banks may take a range of steps, including the adoption of measures similar to those for PEPs and other high risk categories.

52. While the Authority may from time to time circulate names of countries and jurisdictions with inadequate AML/CFT regimes (which can then be used as a reference guide), banks are also encouraged to refer, where practicable, to other sources of information to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.

Paragraph 7 of the Notice - Reliance on Intermediaries

53. Where a bank wishes to rely on an intermediary to perform elements of the CDD measures, paragraph 7.1(a) of the Notice requires the bank to be satisfied that the 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 the Notice or the equivalent foreign measures.

54. The bank may take a variety of measures, including but not limited to the following in determining whether the intermediary satisfies the requirements in paragraph 7.1(a):

(a) referring to any publicly available reports or material on the quality of AML/CFT supervision in the jurisdiction where that intermediary operates (such as mutual evaluation reports of the FATF and its associated bodies, or assessment reports made under the Financial Sector Assessment Programme of the International Monetary Fund and the World Bank);

(b) referring to any publicly available reports or material on the quality of that intermediary's compliance with applicable AML/CFT rules;

(c) obtaining professional advice as to the extent of AML/CFT obligations to which the intermediary is subject by the laws of the jurisdiction in which the intermediary operates; or

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

55. To the extent that the performance of CDD is undertaken by the intermediary rather than by the bank, the bank should be able to justify that that the conditions of paragraph 7 of the Notice have been met. The bank should take considerable care when deciding if an intermediary is one on whom it can safely rely on to perform the CDD measures.

Paragraph 9.6 of the Notice - Responsibility of the beneficiary bank in identifying/handling in-coming wire transfers

56. Paragraph 9.6 of the Notice requires banks to adopt appropriate risk-based procedures for identifying and handling in-coming wire transfers that are not accompanied by complete originator information. Banks should consider not accepting in-coming wire transfers from or terminating business relations with, overseas ordering banks that, to their knowledge,

are required to provide originator information but fail to do so. In this respect, banks should therefore take into account any requirements that may be imposed on the overseas ordering bank, either by law or as a regulatory measure, in respect of cross-border wire transfers.

57. In complying with paragraph 9.6, banks should therefore take into account any requirements that may be imposed on the overseas ordering bank, either by law or as a regulatory measure, in respect of cross-border wire transfers.

Paragraph 11 of the Notice - Suspicious Transaction Reporting

58. Paragraphs 11 of the Notice provide for the establishment of internal procedures for reporting suspicious transactions.

59. Banks are required to have adequate processes and systems for identifying and detecting suspicious transactions. The Authority also expects the bank to put in place effective and efficient procedures for reporting suspicious transactions.

60. The bank should ensure that the internal process for evaluating whether a matter should be referred to the STRO via an STR be completed within 7 working days of the case being referred by the relevant bank staff, unless the circumstances are most extraordinary.

61. Examples of suspicious transactions are set out in Appendix II to these Guidelines. These examples are not intended to be exhaustive and are only examples of the most basic ways money may be laundered. If any transactions similar to those in Appendix II, or any other suspicious transactions, are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds.

62. Banks are required to keep watch for suspicious transactions in the course of conducting screening against lists of terrorist suspects as may be required by law or circulated by any relevant authority. The bank should consider filing an STR even though there is no positive match against any name if the surrounding circumstances raise sufficient suspicions.

63. Subject to any written law or any directions given by STRO or the Authority, banks should as far as possible follow the reporting formats specified in Appendices III to V to these Guidelines. 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 should give initial notification to STRO by telephone or email and follow up

with such other means of reporting as STRO may direct. A copy of the STR should also be sent to the Authority.

64. Every bank should maintain a complete file of all transactions that have been brought to the attention of its AML/CFT compliance officer or unit, including transactions that are not reported to STRO.

Paragraphs 12.8 and 12.9 of the Notice - Compliance

65. The responsibilities of the AML/CFT compliance officer should include the following:

(a) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;

(b) advising and training senior management and staff on development and implementing internal policies, procedures and controls on AML/CFT;

(c) carrying out, or overseeing the carrying out of, on-going monitoring of business relations and sample reviewing of accounts for compliance with the Notice and these Guidelines; and

(d) promoting compliance with the Notice and these Guidelines, including in particular observance of the underlying principles on AML/CFT in the Notice and taking overall charge of all AML/CFT matters within the organisation.

Paragraph 12.12 of the Notice - Conducting Training

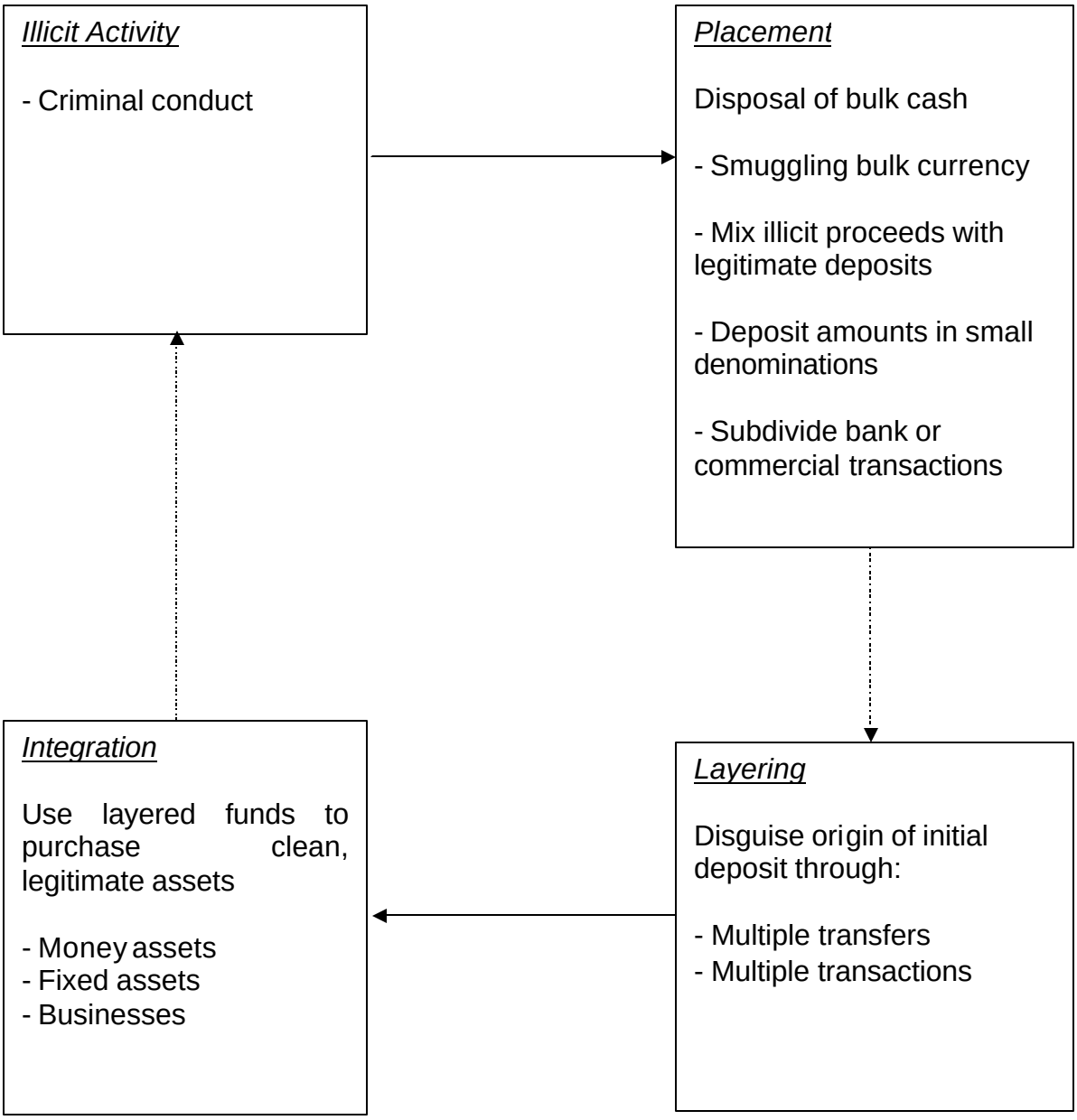
66. As stated in paragraph 12.12 of the Notice, it is the responsibility of banks to provide appropriate training on AML/CFT measures for its staff. To help ensure the effectiveness of training, banks should monitor attendance at such training and take the appropriate follow-up action in relation to staff who absent themselves without reasonable cause.

67. Apart from the initial training, banks should also provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training should be held at least once a year.

……

APPENDIX I

PROCESS OF MONEY LAUNDERING



APPENDIX II

EXAMPLES OF SUSPICIOUS TRANSACTIONS

1 General Comments

The list of situations given below is intended to highlight 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 a suspicious transaction. The list is not exhaustive 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 where a customer has a large number of accounts with the same bank, and has 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.

viii) Cash deposited at one location is withdrawn at another location almost immediately.

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.

xiii) A large amount of cash is withdrawn and immediately deposited into another account.

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.

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

ix) Transfers of funds from a company's account to an employee's account and vice-versa.

5 Transactions Involving Transfers Abroad

i) Transfer of a large amount of money abroad by a person whose does not maintain an account with the bank and who fails to provide a legitimate reason when asked.

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.

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) other 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.

viii) "U-turn" transactions. i.e. where funds received from a person or company in a foreign jurisdiction are immediately remitted to another person or company in the same foreign jurisdiction, or to the sender's account in another jurisdiction.

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.

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

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 Other Types of 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.

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

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

vi) Frequent changes to the address or authorised signatories.

vii) A large amount of funds is received and immediately used as collateral for banking facilities.

viii) When a young person (aged about 17-26) opens an account and either withdraws or transfers the funds within a short period.

ix) When a person receives funds from a religious or charitable organisation and utilises the funds for purchase of assets or transfers out the funds within a relatively short period.

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 is to 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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

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 is to 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 each of the following documents is attached:

- Account Opening Forms

- Customer Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

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 is to 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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

[MAS Notice 3001]

Introduction

1. These Guidelines are issued to provide guidance to the holders of money-changer's licence and remittance licence (the "Licensees") on some of the requirements in MAS Notice 3001 (the "Notice") issued on [date].

2. Licensees are reminded that the ultimate responsibility and accountability for ensuring the licensee's compliance with AML/CFT laws, regulations and guidelines rests with the licensee.

3. The expressions used in these Guidelines shall, except where expressly defined in these Guidelines or where the context otherwise requires, have the same respective meanings as in the Notice.

The structure of MAS Notice 3001

4. The Notice sets out the obligations of a licensee to take measures to help mitigate the risk of the money-changing and remittance industry of Singapore being used for money laundering or terrorist financing.

5. Paragraph 4 of the Notice deals with CDD measures. This paragraph sets out the standard CDD measures to be applied, of which there are four principal components:

   - Identification of the customer by obtaining certain information pertaining to the customer and, where the customer is not a natural person, certain other persons associated with that customer;

   - Verifying the identification information obtained;

   - Where the customer is not a natural person, identifying and verifying the identity of its representatives; and

   - Determining if there exists any beneficial owner (other than the customer) and applying the identification and verification procedures to those beneficial owners;

6. Paragraphs 5 and 6 of the Notice provide for the risk-based customisation of the CDD measures. Thus, paragraph 5 on simplified CDD allows a licensee, with the prior approval of the Authority, to take lesser measures than those specified in paragraph 4 of the Notice but the licensee must be able to justify its decision in its application to the Authority. Conversely, in situations where PEPs may be involved or in other situations where there is a higher risk of

money laundering or terrorist financing, a licensee is required under paragraph 6 of the Notice to take enhanced CDD measures.

7. The Notice also contains the requirements for a licensee to include originator information in cross-border wire transfers (paragraph 7) and updated versions of the previous requirements with respect to the maintenance and retention of records on all transactions with customers (paragraph 8), the reporting of suspicious transactions (paragraph 9) and the implementation of internal policies, procedures and controls on AML/CFT (paragraph 10).

Key Concepts of the Notice

Money Laundering

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

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

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

(b) Layering - The separation of the benefits of 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 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.

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

Terrorist Financing

10. 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. Licensees should refer to the legal definitions of terrorism found in the law such as the Terrorism (Suppression of Financing) Act (Cap. 325), the United Nations (Anti-terrorism Measures) Regulations (Rg 1) and the Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002.

11. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. 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.

12. 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.

13. 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.

Paragraph 2.1 of the Notice – Definition of "Customer"

14. Paragraph 2.1 of the Notice defines "customer", in relation to a licensee, as the person for whom the licensee undertakes or intends to undertake a relevant business transaction.

15. The definition circumscribes the scope of the Notice. Licensees should in general seek to perform CDD as widely as possible on persons that they deal with in the course of their operations.

Paragraphs 4.5, 4.7 and 4.8 of the Notice – Identification of Customers that are Not Natural Persons

16. Where the customer is not a natural person, paragraphs 4.5, 4.7 and 4.8 of the Notice respectively require the licensee to further establish the identity of the customer's directors, partners or persons having executive authority, of the customer respectively.

17. The licensee should assess and determine, with respect to each customer, the key persons whose details they consider necessary to verify.

18. For the purposes of paragraphs 4.5, 4.7 and 4.8 above, the licensee should consider whether persons, either singly or jointly with another, are able to give instructions concerning the use or transfer of funds or assets belonging to the customer in question.

Paragraphs 4.9 and 4.10 of the Notice – Verification of Identity

19. The requirements on verification of identity are intended to ensure that identity information provided by the customer is authentic.

20. Where the person whose identity is to be verified is a natural person, the licensee should ask for some form of identification that contains a recent photograph of that person.

21. The licensee should retain copies of all documentation used for verification of identity. Only in exceptional circumstances where the licensee is unable to retain a copy of documentation used in verifying the customer's identity, the licensee should record the following:

    (a) the information, that the original documentation had served to verify;

    (b) the title and description of the original documentation produced to the licensee for verification, including any particular or unique features or condition of that documentation (whether it is worn out, or damaged etc);

    (c) the reasons why a copy of that documentation could not be made; and

    (d) the name of the licensee who carried out the verification, a statement certifying that the licensee has duly verified the information against the documentation, and the date the verification took place.

Paragraphs 4.15 to 4.20 of the Notice – Identification of Beneficial Owners and Verification of their Identities

22. Licensees are under a duty to take steps to determine if there exists, other than the person *ex facie* dealing with the licensee as a customer, any other beneficial owner in relation to the customer.

23. Generally, the licensee should assess and determine what measures would be appropriate to determine the beneficial owners, if any. The licensee should be able to justify the reasonableness of the measures taken, having regard to the circumstances of each case.

24. Where the customer is not a natural person, the licensee should take steps such as:

    (a) finding out about the ownership and structure of the company; and

    (b) identifying the natural persons who have a controlling interest in the customer or who comprise the mind and management of the customer.

25. The licensee may also consider obtaining an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner.

26. Paragraph 4.17 of the Notice states that licensees are not required to inquire if there exists any beneficial owner beyond the entities specified in sub-paragraphs (a) to (f).

27. The Authority recognises that it would be unnecessary to attempt to determine if beneficial owners exist behind these entities, since adequate information would already be available. For example, in the case of publicly listed companies, the shareholders (who would be the beneficial owners) would be changing relatively frequently and there would already be disclosure obligations imposed on substantial shareholders of such companies. In the case of financial institutions, there would have been adequate disclosure of the ownership and structure to the financial regulator.

28. While the entities listed would also typically be entities for which a licensee may consider applying simplified CDD in accordance with paragraph 5 of the Notice, it is not the intent that the licensee should thereby deem these entities to be automatically eligible for simplified CDD measures. The licensee must comply with the requirements of paragraph 5 of the Notice before applying simplified CDD measures.[3]

Reliability and Authenticity of Information and Documentation

29. Where the licensee obtains information or documents through the customer or a third party, the licensee should ensure that there is satisfactory evidence to show that the information or documents have been endorsed or otherwise authenticated by the relevant authority or official registry. Such information or documents should be as current as possible at the time they are provided to the licensee.

Paragraphs 4.21 to 4.22 of the Notice – Non Face-to-face Verification

30. Paragraph 4.21 of the Notice prohibits licensees from transacting with customers without face-to-face contact, except with the approval of the Authority. Licensees have to satisfy the Authority that they have the necessary internal policies, procedures and controls for addressing the risks of money laundering and terrorist financing and that CDD measures undertaken would be as stringent as those applied if there were face-to-face contact.

Paragraphs 4.23 to 4.24 of the Notice – Time for completion of CDD measures

[3] Licensees should further note that where there is actual cause for suspecting money laundering or terrorist financing, then the appropriate measures will be required- see paragraph 4.1(b) of the Notice.

31. Paragraph 4.23 of the Notice specifies that completion of CDD measures should not be deferred. Licensees are required to complete CDD measures before undertaking any relevant business transaction with a customer to address risks of money laundering and terrorist financing.

32. Where the CDD measures cannot be completed due to the customer not being able to furnish either his particulars or evidence of his identity, the licensee shall terminate the business transaction and consider if circumstances warrant the filing of an STR.

Paragraph 5 of the Notice – Simplified Customer Due Diligence

33. Paragraph 5.1 of the Notice allows licensees to apply to the Authority for approval to perform simplified CDD measures in cases where the licensee is satisfied that the risk of money laundering or terrorist financing is low.

34. Examples of when the licensee might adopt lesser or reduced CDD measures, subject to the Authority's prior approval, are:

(a) where reliable information on the customer is publicly available to the licensee; or

(b) the customer is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, or a listed company that is subject to regulatory disclosure requirements.

Paragraph 6.2 of the Notice – Identifying and dealing with PEPs

35. The definition of PEPs used in the Notice is drawn from the work of the FATF. The Authority recognises that the process of determining whether an individual is a PEP may not always be straightforward and a more precise definition would carry with it a greater risk of circumvention of the requirements under the Notice.

36. In the circumstances, the Authority would generally consider it acceptable for a licensee to refer to databases of PEPs either compiled commercially or by official authorities. However, in doing so, the Authority would expect the licensee to exercise a measure of discretion and sound judgment in determining for itself whether an individual should indeed be treated as a PEP, having regard to the risks and the circumstances.

Paragraphs 6.3 and 6.4 of the Notice – Other High Risk Categories

37. Paragraph 6.3 of the Notice requires enhanced CDD measures to be applied to other categories of customers apart from PEPs, which a licensee may consider to present a greater risk of money laundering or terrorist financing.

38. Licensees are also required by paragraph 6.4 of the Notice to give particular attention to business relations and transactions with persons from or in countries that have inadequate AML/CFT measures. For this purpose, licensees may take a range of steps, including the adoption of measures similar to those for PEPs and other high risk categories.

39. While the Authority may from time to time circulate names of countries and jurisdictions with inadequate AML/CFT regimes (which can then be used as a reference guide), licensees are also encouraged to refer, where practicable, to other sources of information to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.

Paragraph 7.6 of the Notice – Responsibility of the beneficiary institution in identifying/handling in-coming wire transfers

40. Paragraph 7.6 of the Notice requires licensees to adopt appropriate risk-based procedures for identifying and handling in-coming wire transfers that are not accompanied by complete originator information. Licensees should consider not accepting in-coming wire transfers from or, terminating business relations with, overseas ordering institutions, that to their knowledge, are required to provide originator information but fail to do so. In this respect, licensees should therefore take into account any requirements that may be imposed on the overseas ordering institution, either by law or as a regulatory measure, in respect of cross-border wire transfers.

Paragraph 9 of the Notice – Suspicious Transaction Reporting

41. Paragraph 9 of the Notice provides for the establishment of internal procedures for reporting suspicious transactions.

42. Licensees are required to have adequate processes and systems for identifying and detecting suspicious transactions. The Authority expects the licensee to put in place effective and efficient procedures for reporting suspicious transactions.

43. The licensee should ensure that the internal process for evaluating whether a matter should be referred to the STRO via an STR be completed within 7 working days of the case being referred by the relevant reporting staff, unless the circumstances are most extraordinary.

44. Examples of suspicious transactions are set out in Appendix II to these Guidelines. These examples are not intended to be exhaustive and are only examples of the most basic ways in which money may be laundered. If any transactions similar to those in Appendix II or any other suspicious transactions are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds.

45. Licensees are required to keep watch for suspicious transactions in the course of conducting screening against lists of terrorist suspects as may be required by law or circulated by any relevant authority. The licensee should consider filing an STR even though there is no positive match against any name if the surrounding circumstances raise sufficient suspicions.

46. Subject to any written law or any directions given by STRO or the Authority, licensees should as far as possible follow the reporting formats specified in Appendices III to V to these Guidelines. 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, licensees should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct. A copy of the STR should also be sent to the Authority.

47. Every licensee should maintain a complete file of all transactions that have been brought to the attention of its AML/CFT compliance officer or unit, including transactions that are not reported to STRO.

Paragraphs 10.8 to 10.10 of the Notice – Compliance

48. The responsibilities of the AML/CFT compliance officer should include the following:

(a) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;

(b) advising and training senior management and staff on development and implementing internal policies, procedures and controls on AML/CFT as well as training;

(c) carrying out, or overseeing the carrying out of, on-going monitoring of business relations and sample reviewing of accounts for compliance with the Notice and these Guidelines; and

(d) promoting compliance with the Notice and these Guidelines, including in particular observance of the underlying principles on AML/CFT in the Notice and taking overall charge of all AML/CFT matters within the organisation.

Paragraph 10.13 of the Notice – Conducting Training

49. As stated in paragraph 10.13 of the Notice, it is the responsibility of the licensees to provide appropriate training on AML/CFT measures for its staff. To help ensure the effectiveness of training, licensees should monitor attendance at such training and take the appropriate follow-up action in relation to staff who absent themselves without reasonable cause.

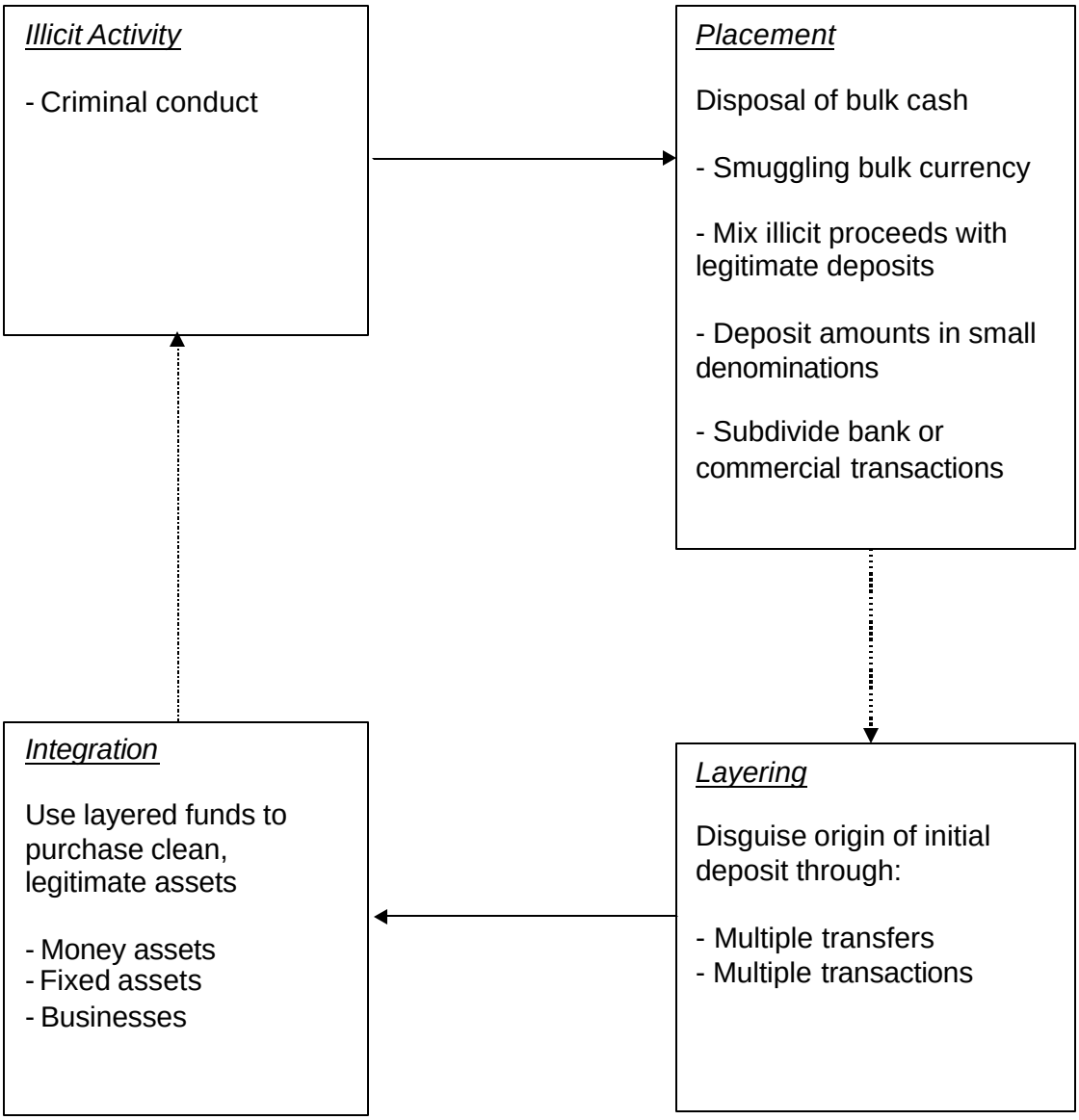
50. Apart from the initial training, licensees should also provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training should be held at least once a year.

51. Proper records on training provided to the staff should be maintained by the licensee.

……

APPENDIX I

PROCESS OF MONEY LAUNDERING



APPENDIX II

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 a suspicious 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 in the course of business transaction. Licensees should pay attention to customers who provide minimal, false or misleading information or, information that is difficult or expensive for the licensees to verify.

2 Transactions Which Do Not Make Economic Sense

i) Transactions which are incompatible with the licensee's knowledge and experience of the customer in question or with the purpose of the business relationship.

ii) Conceal or disguise significant transactions to avoid disclosure for record purpose by executing frequent or several transactions such that each transaction by itself is not required to be recorded.

iii) Transactions that cannot be reconciled with the usual activities of the customer.

3 Transactions Involving Large Amounts of Cash

i) Exchanging an unusually large amount of small-denominated notes for those of higher denomination in a different currency.

ii) Frequent transactions of large cash amounts that do not appear to be justified by the customer's business activity.

iii) Customers whose funds contain counterfeit notes.

iv) Customers remitting large amounts of money to persons outside Singapore with instructions for payment in cash.

v) Large and regular payments that cannot be identified as bona fide transactions, to countries associated with the production, processing or marketing of narcotics or other illegal drugs.

vi) Cash payments remitted to a single account by a large number of different persons without an adequate explanation.

4 Other Types of Transactions

i) 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 terrorist activities or with persons that have been designated as terrorists.

iii) Frequent changes to the local address of the customer.

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 Licensee	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
Licensee's 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):	

Employment Details	
Employer's Name:	
Address:	
Telephone:	

Suspicious Transaction(s)				
Amount in S$	**Amount in Foreign Currency**	**Date of Transaction**	**Source/Sender of Funds**	**Destination (for Funds Remitted)**

Reason(s) for Suspicion:

Other Relevant Information (including any actions taken by the reporting licensee in response to the transaction)**:**

A copy each of the following documents is attached:

- Customer Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

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 Licensee	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
Licensee's 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):	

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

[#] The licensee's reporting officer shall provide data on other authorised signatories, if any.

Suspicious Transaction(s)				
Amount in S$	**Amount in Foreign Currency**	**Date of Transaction**	**Source/Sender of Funds**	**Destination (for Funds Remitted)**

Reason(s) for Suspicion:

Other Relevant Information (including any actions taken by the reporting licensee in response to the transaction)**:**

A copy each of the following documents is attached:

- Customer Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

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**
(* delete where applicable)

Reporting Licensee	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
Licensee's 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):	

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

The licensee's reporting officer shall provide data on other authorised signatories, if any.

Suspicious Transaction(s)				
Amount in S$	**Amount in Foreign Currency**	**Date of Transaction**	**Source/Sender of Funds**	**Destination (for Funds Remitted)**

Reason(s) for Suspicion:

Other Relevant Information (Including any actions taken by the reporting licensee in response to the transaction)**:**

A copy each of the following documents is attached:

- Customer Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

_____

(Signature of Reporting Officer)

Date:

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

[MAS Notice 824]

Introduction

1. These Guidelines are issued to provide guidance to the finance companies on some of the requirements in MAS Notice 824 (the "Notice") issued on [date].

2. Finance companies are reminded that the ultimate responsibility and accountability for ensuring the finance company's compliance with AML/CFT laws, regulations and guidelines rests with the finance company, its board of directors and senior management.

3. The expressions used in these Guidelines shall, except where expressly defined in these Guidelines or where the context otherwise requires, have the same respective meanings as in the Notice.

The structure of MAS Notice 824

4. The Notice sets out the obligations of a finance company to take measures to mitigate the risks of the banking system of Singapore being used for money laundering or terrorist financing.

5. Paragraph 4 of the Notice deals with CDD measures. This paragraph sets out the standard CDD measures to be applied, of which there are seven principal components:

   - Identification of the customer by obtaining certain information pertaining to the customer and, where the customer is not a natural person, certain other persons associated with that customer;

   - Verifying the identification information obtained;

   - Where the customer is not a natural person, verifying that the persons purporting to act for the customer are in fact authorised to act;

   - Determining if there exists any beneficial owner (other than the customer) and applying the identification and verification procedures to those beneficial owners;

- Where business relations are to be established (as defined in the Notice), obtaining information as to the nature and purpose of the intended business relations;

- After business relations are established, conducting on-going monitoring of business relations; and

- After business relations are established, periodically reviewing the adequacy of customer information.

6. Paragraphs 5 and 6 of the Notice provide for the risk-based customisation of the CDD measures. Thus, paragraph 5 on simplified CDD allows a finance company to take lesser measures than those specified in paragraph 4 of the Notice provided that the conditions for simplified CDD are met. This will largely be a matter for individual finance companies to assess, but the finance company must be able to justify its decision. Conversely, in situations where PEPs may be involved or in other situations where there is a higher risk of money laundering or terrorist financing, a finance company is required under paragraph 6 of the Notice to take enhanced CDD measures.

7. To cater to cross-referrals, paragraph 7 of the Notice allows a finance company to rely on another party, an intermediary, to perform certain elements of the CDD process, provided that certain conditions are met. This paragraph may typically be applied where a new customer is introduced to the finance company by an intermediary resulting in direct business relations between the finance company and the new customer. Thus, if the intermediary has already performed its own CDD on the new customer, then paragraph 7 allows the finance company to dispense with performing CDD on the new customer if the conditions are satisfied. Paragraph 7 is not intended to cover the situation where a finance company outsources the function of performing CDD measures to a third party.[4]

8. The Notice then deals with the requirement to include originator information in cross-border wire transfers (paragraph 8).

9. Finally, the Notice updates the previous requirements with respect to record keeping (paragraph 9), reporting of suspicious transactions (paragraph 10) and the institution of internal policies, procedures and controls for AML/CFT (paragraph 11).

---

[4] The Notice does not prohibit the outsourcing of the CDD function to a third party but where this occurs, the finance company must remain fully responsible and accountable for the conduct of CDD measures as if the function had remained within the finance company.

Key Concepts of the Notice

Money Laundering

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

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

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

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

    (c) Integration - The provision of apparent legitimacy to the benefits of 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.

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

Terrorist Financing

12. 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. Finance companies should refer to the legal definitions of terrorism found in the law such as the Terrorism (Suppression of Financing) Act (Cap. 325), the United Nations (Anti-terrorism Measures) Regulations (Rg 1) and the Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002.

13. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. 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.

14. 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.

15. 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.

Paragraph 2.1 of the Notice – Definition of "Customer"

16. Paragraph 2.1 of the Notice defines "customer", in relation to a finance company, as the person in whose name an account is opened or intended to be opened, or to whom a finance company undertakes or intends to undertake any transaction without an account being opened.

17. The definition circumscribes the scope of the Notice. Finance companies should in general seek to perform CDD as widely as possible on persons that they deal with in the course of their financing operations.

18. In the case below, the following approach below may be adopted:

Portfolio Managers

A finance company may often encounter cases where, to the finance company's knowledge, the customer is a manager of a portfolio of assets and is operating the account in that capacity. In such cases, the underlying investors of the portfolio will be beneficial owners within the meaning of the Notice.

However, the Authority recognises that a finance company may not be able to perform CDD on the underlying investors. For instance, the portfolio manager may be reluctant, for legitimate commercial reasons, to reveal information on the underlying investors to the finance company. In such circumstances, the finance company should evaluate the risks arising for each case and determine the appropriate CDD measures to take. The finance company may consider if simplified CDD measures

could be applied under paragraph 5 of the Notice, so that identification and verification of the underlying investors as beneficial owners are dispensed with.

Paragraphs 4.6, 4.8 and 4.9 of the Notice – Identification of Customers that are Not Natural Persons

19. Where the customer is not a natural person, paragraphs 4.6, 4.8 and 4.9 of the Notice require the finance company to further establish the identity of the directors, partners or persons having executive authority, of the customer respectively.

20. The finance company should assess and determine, with respect to each of the customer, the key persons whose details they consider necessary to verify.

21. For the purposes of paragraph 20 above, the finance company should consider whether persons, either singly or jointly with another, are able to give instructions concerning the use or transfer of funds or assets belonging to the customer in question.

Paragraphs 4.10 and 4.11 of the Notice - Verification of Identity

22. The requirements on verification of identity are intended to ensure that identity information provided by the customer is authentic.

23. Where the person whose identity is to be verified is a natural person, the finance company should ask for some form of identification that contains a recent photograph of that person.

24. The finance company should retain copies of all documentation used for verification of identity. Only in exceptional circumstances where the finance company is unable to retain a copy of documentation used in verifying the customer's identity, the finance company should record the following:

    (a) the information that the original documentation had served to verify;

    (b) the title and description of the original documentation produced to the finance company officer for verification, including any particular or unique features or condition of that documentation (whether it is worn out, or damaged etc);

(c) the reasons why a copy of that documentation could not be made; and

(d) the name of the finance company officer who carried out the verification, a statement by that officer certifying that he or she has duly verified the information against the documentation, and the date the verification took place.

Paragraphs 4.16 to 4.19 of the Notice - Identification of Beneficial Owners and Verification of their Identities

25. Finance companies are under a duty to take steps to determine if there exists, other than the person *ex facie* dealing with the finance company as a customer, any other beneficial owner in relation to the customer.

26. Generally, the finance company should assess and determine what measures would be appropriate to determine the beneficial owners, if any. The finance company should be able to justify the reasonableness of the measures taken, having regard to the circumstances of each case.

27. Where the customer is not a natural person, the finance company should take steps such as:

(a) finding out about the ownership and structure of the company; and

(b) identifying the natural persons who have a controlling interest in the customer or who comprise the mind and management of the customer.

28. The finance company should also consider obtaining an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner.

29. Paragraph 18 of these Guidelines makes reference to the case where the customer is a portfolio manager. In that situation, as well as other instances where the customer has a *bona fide* and legitimate interest or duty not to disclose to the finance company the identity or particulars of beneficial owners who are known to exist, the finance company may apply simplified CDD set out in paragraph 5 of the Notice.

30. Paragraph 4.18 of the Notice states that finance companies are not required to inquire if there exists any beneficial owner beyond the entities specified in sub-paragraphs (a) to (f).

31. The Authority recognises that it would be unnecessary to attempt to determine if beneficial owners exist behind these entities, since adequate information would already be available. For example, in the case of publicly listed companies, the shareholders (who would be the beneficial owners) would be changing relatively frequently and there would already be disclosure obligations imposed on substantial shareholders of such companies. In the case of financial institutions, there would have been adequate disclosure of the ownership and structure to the financial regulator.

32. While the entities listed would also typically be entities for which a finance company may consider applying simplified CDD in accordance with paragraph 5 of the Notice, it is not the intent that the finance company should thereby deem these entities to be automatically eligible for simplified CDD measures. The finance company must comply with the requirements of paragraph 5 of the Notice before applying simplified CDD measures.[5]

Reliability and Authenticity of Information and Documentation

33. Where the finance company obtains information or documents through the customer or a third party, the finance company should ensure that there is satisfactory evidence to show that the information or documents have been endorsed or otherwise authenticated by the relevant authority or official registry. Such information or documents should be as current as possible at the time they are provided to the finance company.

Paragraphs 4.26 and 4.27 of the Notice - Non Face-to-Face Verification

34. Paragraphs 4.26 and 4.27 of the Notice address the situation where business relations are established or financial services are provided without face-to-face contact. Measures for managing the risks should include specific and effective procedures for CDD that apply to non face-to-face customers. In particular, a finance company should take appropriate measures to address risks arising from establishing business relations and undertaking transactions through instructions conveyed by customers over the internet, the post or the telephone.

35. As a guide, finance companies should take one or more of the following measures to mitigate the heightened risk associated with not being able to conduct an interview face-to-face:

[5] Finance companies should further note that where there is actual cause for suspecting money laundering or terrorist financing, the appropriate measures will be required – see paragraph 4.3(c) of the Notice.

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

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

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

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

(e) certification of identification documents by lawyers or notary publics presented by the customer;

(f) requiring the customer to make an initial deposit using a cheque drawn on the customer's personal account with a bank in Singapore; and

(g) any other reliable verification checks adopted by the finance company for non-face- to-face financing business.

Paragraphs 4.32 and 4.33 of the Notice - Deferring the completion of CDD measures: Time limits for completion

36. Paragraph 4.32 of the Notice allows finance companies to establish business relations before completing the CDD measures if it is essential for the finance company not to interrupt the normal conduct of business and if the risks can be effectively managed.

37. An example where it may be essential not to interrupt the normal course of business would be with respect to securities trades, where market conditions are such that the finance company has to execute transactions for the customer very rapidly.

38. An example where the finance company may have effectively managed the risks of money laundering and terrorist financing is if the finance company has adopted internal policies, procedures and controls that set appropriate limits on the financial services available to the customer before completion of CDD measures. These may include, for example, limiting the number, type and value of transactions that might be effected in the interim period, and also the institution of a procedure that is more

rigorous and intensive than usual for the monitoring of complex or unusually large transactions.

39. Paragraph 4.33 of the Notice requires that CDD measures be completed as soon as reasonably practicable, if a finance company allows business relations to be established without first completing CDD measures. Examples of reasonable timeframe are:

(a) the finance company completing CDD measures no later than 30 working days after the establishment of business relations;

(b) the finance company suspending business relations with the customer and refraining from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if CDD measures remain uncompleted 30 working days after the establishment of business relations; and

(c) the finance company terminating business relations with the customer if CDD measures remain uncompleted 120 working days after the establishment of business relations.

40. The finance company should factor these time limitations in their internal policies, procedures and controls.

Paragraph 4.35 of the Notice - Existing Customers

41. Paragraph 4.35 of the Notice concerns the application of CDD measures to the customers and accounts which the finance company has as at [date] when the Notice comes into force. Finance companies are required to review the adequacy of identification information on the basis of materiality and risk, and to perform CDD measures on existing customers as may be appropriate.

42. In relation to accounts for which CDD measures had not previously been applied in accordance with the Notice, the finance company should make an assessment with regard to materiality and risk and determine when would be an appropriate time for the performance of CDD measures, subject to the more specific requirements for PEPs specified in paragraph 6.2 of the Notice.

43. As a guide, a finance company should perform CDD, in relation to paragraph 42 above, when:

(a) there is a transaction that is significant, having regard to the manner in which the account is ordinarily operated;

(b) there is a substantial change in the finance company's own customer documentation standards;

(c) there is a material change in the way that business relations with the customer are conducted;

(d) the finance company becomes aware that it may lack adequate identification information on a customer; and

(e) the finance company 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 finance company.

44. Where a finance company becomes aware upon a review that it may lack sufficient identification information on a customer, it should proceed to perform CDD afresh.

Paragraph 5 of the Notice - Simplified Customer Due Diligence

45. Paragraph 5.1 of the Notice allows finance companies to apply simplified CDD measures in cases where the finance company is satisfied that the risk of money laundering or terrorist financing is low.

46. The finance company should assess the risks of money laundering or terrorist financing, having regard to the circumstances of each case, before applying the lesser or reduced CDD measures. Where the finance company adopts such lesser or reduced CDD measures, such measures should be commensurate with its assessment of the risks.

47. Examples of when the finance company may adopt lesser or reduced CDD measures are:

(a) where reliable information on the customer is publicly available to the finance company,

(b) the finance company is dealing with another financial institution whose AML/CFT controls it is well familiar with by virtue of a previous course of dealings; or

(c) the customer is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, or a listed company that is subject to regulatory disclosure requirements.

Paragraph 6.2 of the Notice - Identifying and dealing with PEPs

48. The definition of PEPs used in the Notice is drawn from the work of the FATF. The Authority recognises that the process of determining whether an individual is a PEP may not always be straightforward and a more precise definition would carry with it a greater risk of circumvention of the requirements under the Notice.

49. In the circumstances, the Authority would generally consider it acceptable for a finance company to refer to databases of PEPs either compiled commercially or by official authorities. However, in doing so, the Authority would expect the finance company to exercise a measure of discretion and sound judgment in determining for itself whether an individual should indeed be treated as a PEP, having regard to the risks and the circumstances

Paragraphs 6.3 and 6.4 of the Notice - Other High Risk Categories

50. Paragraph 6.3 of the Notice requires enhanced CDD measures to be applied to other categories of customers apart from PEPs, which a finance company may consider to present a greater risk of money laundering or terrorist financing. Such high risk categories may include, for example, non-resident customers, private banking customers, body corporates set up as personal asset holding vehicles, or companies that have nominee shareholders or that issue shares in bearer form.

51. Finance companies are also required by paragraph 6.4 of the Notice to give particular attention to business relations and transactions with persons from or in countries that have inadequate AML/CFT measures. For this purpose, finance companies may take a range of steps, including the adoption of measures similar to those for PEPs and other high risk categories.

52. While the Authority may from time to time circulate names of countries and jurisdictions with inadequate AML/CFT regimes (which can then be used as a reference guide), finance companies are also encouraged to refer to other sources of information to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.

Paragraph 7 of the Notice - Reliance on Intermediaries

53. Where a finance company wishes to rely on an intermediary to perform elements of the CDD measures, paragraph 7.1(a) of the Notice requires the finance company to be satisfied that the intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements, and that the intermediary have measures in place to comply with the Notice or the equivalent foreign measures.

54. The finance company may take a variety of measures, including but not limited to the following in determining whether the intermediary satisfies the requirements in paragraph 7.1(a):

(a) referring to any publicly available reports or material on the quality of AML/CFT supervision in the jurisdiction where that intermediary operates (such as mutual evaluation reports of the FATF and its associated bodies, or assessment reports made under the Financial Sector Assessment Programme of the International Monetary Fund and the World Bank);

(b) referring to any publicly available reports or material on the quality of that intermediary's compliance with applicable AML/CFT rules;

(c) obtaining professional advice as to the extent of AML/CFT obligations to which the intermediary is subject by the laws of the jurisdiction in which the intermediary operates; or

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

55. To the extent that the performance of CDD is undertaken by the intermediary rather than by the finance company, the finance company should be able to justify that that the conditions of paragraph 7 of the Notice have been met. The finance company should take considerable care when deciding if an intermediary is one on whom it can safely rely on to perform the CDD measures.

Paragraph 8.6 of the Notice - Responsibility of the beneficiary finance company in identifying/handling in-coming wire transfers

56. Paragraph 8.6 of the Notice requires finance companies to adopt appropriate risk-based procedures for identifying and handling in-coming wire transfers that are not accompanied by complete originator information. Finance companies should consider not accepting in-coming wire transfers from or, terminating business relations with, overseas ordering banks that, to their knowledge, are required to provide originator information but fail to do so. In this respect, finance companies should therefore take into account any requirements that may be imposed on the overseas ordering bank, either by law or as a regulatory measure, in respect of cross-border wire transfers.

Paragraph 10 of the Notice - Suspicious Transaction Reporting

57. Paragraphs 10 of the Notice provide for the establishment of internal procedures for reporting suspicious transactions.

58. Finance companies are required to have adequate processes and systems for identifying and detecting suspicious transactions. The Authority also expects that the finance company to put in place effective and efficient procedures for reporting suspicious transactions.

59. The finance company should ensure that the internal process for evaluating whether a matter should be referred to the STRO via an STR be completed within 7 working days of the case being referred by the relevant finance company staff, unless the circumstances are most extraordinary

60. Examples of suspicious transactions are set out in Appendix II to these Guidelines. These examples are not intended to be exhaustive and are only examples of the most basic ways money may be laundered. If any transactions similar to those in Appendix II, or any other suspicious transactions, are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds.

61. Finance companies are required to keep watch for suspicious transactions in the course of conducting screening against lists of terrorist suspects as may be required by law or circulated by any relevant authority. The finance company should consider filing an STR even though there is no positive match against any name if the surrounding circumstances raises sufficient suspicions.

62. Subject to any written law or any directions given by STRO or the Authority, finance companies should as far as possible follow the reporting formats specified in Appendices III to V to these Guidelines. 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, finance companies should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct. A copy of the STR should also be sent to the Authority.

63. Every finance company should maintain a complete file of all transactions that have been brought to the attention of its AML/CFT compliance officer or unit, including transactions that are not reported to STRO

Paragraphs 11.4 and 11.5 of the Notice - Compliance

64. The responsibilities of the AML/CFT compliance officer should include the following:

(a) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;

(b) advising and training senior management and staff on development and implementing internal policies, procedures and controls on AML/CFT;

(c) carrying out, or overseeing the carrying out of, on-going monitoring of business relations and sample reviewing of accounts for compliance with the Notice and these Guidelines; and

(d) promoting compliance with the Notice and these Guidelines, including in particular observance of the underlying principles on AML/CFT in the Notice and taking overall charge of all AML/CFT matters within the organisation.

Paragraph 11.8 of the Notice - Conducting Training

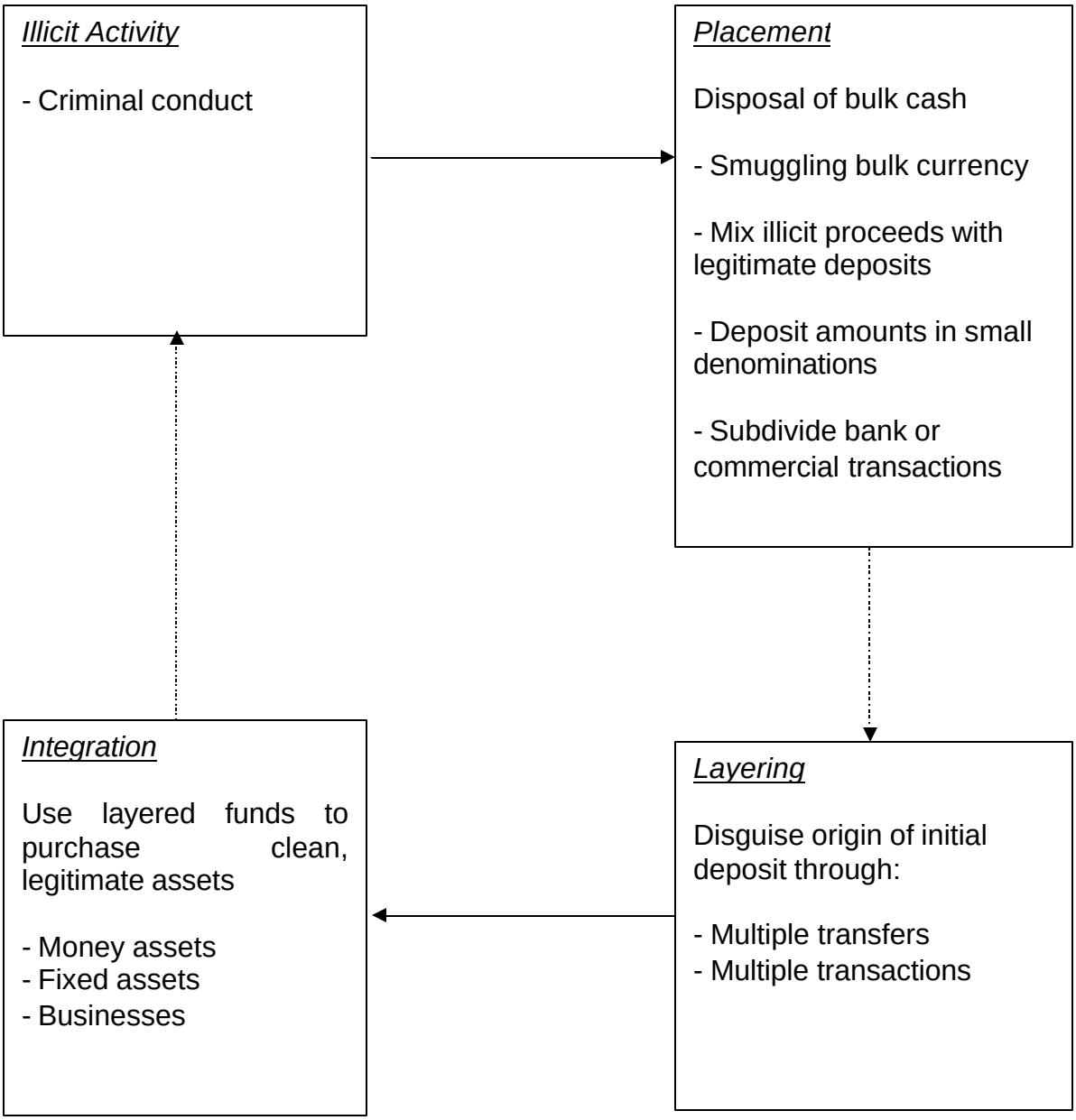
65. As stated in paragraph 11.8 of the Notice, it is the responsibility of finance companies to provide appropriate training on AML/CFT measures for its staff. To help ensure the effectiveness of training, finance companies should monitor attendance at such training and take the appropriate follow-up action in relation to staff who absent themselves without reasonable cause.

66. Apart from the initial training, finance companies should also provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training should be held at least once a year.

.....

APPENDIX I

PROCESS OF MONEY LAUNDERING



APPENDIX II

EXAMPLES OF SUSPICIOUS TRANSACTIONS

1 General Comments

The list of situations given below is intended to highlight 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 a suspicious transaction. The list is not exhaustive 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 finance company in the course of the business relationship. Finance companies 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 finance company to verify.

2 Transactions Which Do Not Make Economic Sense

i) A customer-relationship with the finance company where a customer has a large number of accounts with the same finance company, and has 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.

viii) Cash deposited at one location is withdrawn at another location almost immediately.

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 finance company.

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 finance company.

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.

xiii) A large amount of cash is withdrawn and immediately deposited into another account.

4 Transactions Involving Accounts with the Finance Company

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 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.

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

ix) Transfers of funds from a company's account to an employee's account and vice-versa.

5 Transactions Involving Transfers Abroad

i) Transfer of a large amount money of abroad by a person whose does not maintain an account with the finance company and who fails to provide a legitimate reason when asked.

ii) A customer who appears to have accounts with several financial institutions in the same locality, especially when the finance company 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.

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) other 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.

viii) "U-turn" transactions. i.e. where funds received from a person or company in a foreign jurisdiction are immediately remitted to another person or company in the same foreign jurisdiction, or to the sender's account in another jurisdiction.

6 Investment Related Transactions

i) Purchasing of securities to be held by the finance company 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.

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

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 finance company and who have no identifiable close relationship with the customer.

ii) Transfer of money to another financial institution 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 finance company.

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 Other Types of Transactions

i) Purchase or sale of large amounts of precious metals by an interim customer.

ii) Purchase of 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.

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

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

vi) Frequent changes to the address or authorised signatories.

vii) A large amount of funds is received and immediately used as collateral for financing facilities.

viii) When a young person (aged about 17-26) opens an account and either withdraws or transfers the funds within a short period.

ix) When a person receives funds from a religious or charitable organisation and utilises the funds for purchase of assets or transfers out the funds within a relatively short period.

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 Finance Company	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
Finance Company 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 finance company is to provide particulars on joint account holders, if any.

Employment Details	
Employer's Name:	
Address:	
Telephone:	
Business Relationship(s) with Customer	
Finance company 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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

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 Finance Company	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
Finance Company 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	

Finance company 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 finance company is to 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 each of the following documents is attached:

- Account Opening Forms

- Customer Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

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 Finance Company	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
Finance Company 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	
Finance company 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 finance company is to 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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

[MAS Notice 1014]

Introduction

1. These Guidelines are issued to provide guidance to the merchant banks on some of the requirements in MAS Notice 1014 (the "Notice") issued on [date].

2. Merchant banks are reminded that the ultimate responsibility and accountability for ensuring the merchant bank's compliance with AML/CFT laws, regulations and guidelines rests with the merchant bank, its board of directors and senior management.

3. The expressions used in these Guidelines shall, except where expressly defined in these Guidelines or where the context otherwise requires, have the same respective meanings as in the Notice.

The structure of MAS Notice 1014

4. The Notice sets out the obligations of a merchant bank to take measures to help mitigate the risk of the banking system of Singapore being used for money-laundering or terrorist financing.

5. Paragraph 4 of the Notice deals with CDD measures. This paragraph sets out the standard CDD measures to be applied, of which there are seven principal components:

   - Identification of the customer by obtaining certain information pertaining to the customer and, where the customer is not a natural person, certain other persons associated with that customer;

   - Verifying the identification information obtained;

   - Where the customer is not a natural person, identifying and verifying the identity of its representatives;

   - Determining if there exists any beneficial owner (other than the customer) and applying the identification and verification procedures to those beneficial owners;

- Where business relations are to be established (as defined in the Notice), obtaining information as to the nature and purpose of the intended business relations;

- After business relations are established, conducting on-going monitoring of business relations; and,

- After business relations are established, periodically reviewing the adequacy of customer information.

6. Paragraphs 5 and 6 of the Notice provide for the risk-based customisation of the CDD measures. Thus, paragraph 5 on simplified CDD allows a merchant bank to take lesser measures than those specified in paragraph 4 of the Notice provided that the conditions for simplified CDD are met. This will largely be a matter for individual merchant banks to assess, but the merchant bank must be able to justify its decision. Conversely, in situations where PEPs may be involved or in other situations where there is a higher risk of money laundering or terrorist financing, a bank is required under paragraph 6 of the Notice to take enhanced CDD measures.

7. To cater to cross-referrals, paragraph 7 of the Notice allows a merchant bank to rely on another party, an intermediary, to perform certain elements of the CDD process, provided that certain conditions are met. This paragraph may typically be applied where a new customer is introduced to the merchant bank by an intermediary resulting in direct business relations between the merchant bank and the new customer. Thus, if the intermediary has already performed its own CDD on the new customer, then paragraph 7 allows the merchant bank to dispense with performing CDD on the new customer if the conditions are satisfied. Paragraph 7 is not intended to cover the situation where a merchant bank outsources the function of performing CDD measures to a third party.[6]

8. The Notice then deals with two specific situations – the regulatory requirements when establishing correspondent merchant banking relations (paragraph 8), and the requirement to include originator information in cross-border wire transfers (paragraph 9).

9. Finally, the Notice updates the previous requirements with respect to record keeping (paragraph 10), reporting of suspicious transactions (paragraph 11) and the institution of internal policies, procedures and controls for AML/CFT (paragraph 12).

---

[6] The Notice does not prohibit the outsourcing of the CDD function to a third party but where this occurs, the merchant bank must remain fully responsible and accountable for the conduct of CDD measures as if the function had remained within the merchant bank.

Key Concepts of the Notice

Money Laundering

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

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

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

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

    (c) Integration - The provision of apparent legitimacy to the benefits of 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.

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

Terrorist Financing

12. 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. Merchant banks should refer to the legal definitions of terrorism found in the law such as the Terrorism (Suppression of Financing) Act (Cap. 325), the United Nations (Anti-terrorism Measures) Regulations (Rg 1) and the Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002.

13. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. 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.

14. 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.

15. 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.

Paragraph 2.1 of the Notice – Definition of "Customer"

16. Paragraph 2.1 of the Notice defines "customer", in relation to a merchant bank, as the person in whose name an account is opened or intended to be opened, or to whom a merchant bank undertakes or intends to undertake any transaction without an account being opened.

17. The definition circumscribes the scope of the Notice. Merchant banks should in general seek to perform CDD as widely as possible on persons that they deal with in the course of their banking operations.

18. In the cases below, the following approaches below may be adopted:

(a) Portfolio Managers

A merchant bank may often encounter cases where, to the merchant bank's knowledge, the customer is a manager of a portfolio of assets and is operating the account in that capacity. In such cases, the underlying investors of the portfolio will be beneficial owners within the meaning of the Notice.

However, the Authority recognises that a merchant bank may not be able to perform CDD on the underlying investors. For instance, the portfolio manager may be reluctant, for legitimate commercial reasons, to reveal information on the underlying investors to the merchant bank. In such circumstances, the merchant bank should evaluate the risks arising for each case and determine the appropriate CDD measures to take. The

merchant bank may consider whether simplified CDD measures could be applied under paragraph 5 of the Notice, so that identification and verification of the underlying investors as beneficial owners are dispensed with.

(b) Location of Relationship Management

Given the globalised nature of modern banking, it may often be the case that a merchant bank's relationship and transactions with a particular customer would be managed by bank officers based in one country or jurisdiction but the account itself is held with an office in another country or jurisdiction for book-keeping purposes. For the purposes of the Notice, the Authority will generally look at the substance of the relationship as a whole. A merchant bank should perform CDD if in substance, the person is a customer of the merchant bank in Singapore even though the account is booked in another country or jurisdiction. However, the merchant bank may rely on the CDD done by its related entity in accordance with paragraph 7 of the Notice,

Paragraphs 4.10 and 4.11 of the Notice - Verification of Identity

19. The requirements on verification of identity are intended to ensure that identity information provided by the customer is authentic.

20. Where the person whose identity is to be verified is a natural person, the merchant bank should ask for some form of identification that contains a recent photograph of that person.

21. The merchant bank should retain copies of all documentation used for verification of identity. Only in exceptional circumstances where the merchant bank is unable to retain a copy of documentation used in verifying the customer's identity, the merchant bank should record the following:

(a) the information that the original documentation had served to verify;

(b) the title and description of the original documentation produced to the bank officer for verification, including any particular or unique features or condition of that documentation (whether it is worn out, or damaged etc);

(c) the reasons why a copy of that documentation could not be made; and

(d) the name of the bank officer who carried out the verification, a statement by that officer certifying that he or she has duly verified the information against the documentation, and the date the verification took place.

Paragraphs 4.6, 4.8 and 4.9 of the Notice – Identification of Customers that are Not Natural Persons

22. Where the customer is not a natural person, paragraphs 4.6, 4.8 and 4.9 of the Notice require the merchant bank to further establish the identity of the directors, partners or persons having executive authority, of the customer respectively.

23. The merchant bank should assess and determine, with respect to each customer, the key persons whose details they consider necessary to verify.

24. For the purposes of paragraph 22 above, the merchant bank should consider whether persons, either singly or jointly with another, are able to give instructions concerning the use or transfer of funds or assets belonging to the customer in question.

Paragraphs 4.16 to 4.19 of the Notice - Identification of Beneficial Owners and Verification of their Identities

25. Merchant banks are under a duty to take steps to determine if there exists, other than the person *ex facie* dealing with the merchant bank as a customer, any other beneficial owner in relation to the customer.

26. Generally, the merchant bank should assess and determine what measures would be appropriate to determine the beneficial owners, if any. The merchant bank should be able to justify the reasonableness of the measures taken, having regard to the circumstances of each case.

27. Where the customer is not a natural person, the merchant bank should take steps such as:

(a) finding out about the ownership and structure of the company; and

(b) identifying the natural persons who have a controlling interest in the customer or who comprise the mind and management of the customer.

28. The merchant bank may also consider obtaining an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner.

29. Paragraph 18(a) of these Guidelines makes reference to the case where the customer is a portfolio manager. In that situation, as well as other instances where the customer has a *bona fide* and legitimate interest or duty not to disclose to the merchant bank the identity or particulars of beneficial owners who are known to exist, the merchant bank may consider the application of simplified CDD set out in paragraph 5 of the Notice.

30. Paragraph 4.18 of the Notice states that merchant banks are not required to inquire if there exists any beneficial owner beyond the entities specified in sub-paragraphs (a) to (f).

31. The Authority recognises that it would be unnecessary to attempt to determine if beneficial owners exist behind these entities, since adequate information would already be available. For example, in the case of publicly listed companies, the shareholders (who would be the beneficial owners) would be changing relatively frequently and there would already be disclosure obligations imposed on substantial shareholders of such companies. In the case of financial institutions, there would have been adequate disclosure of the ownership and structure to the financial regulator.

32. While the entities listed would also typically be entities for which a merchant bank may consider applying simplified CDD in accordance with paragraph 5 of the Notice, it is not the intent that the merchant bank should thereby deem these entities to be automatically eligible for simplified CDD measures. The merchant bank must comply with the requirements of paragraph 5 of the Notice before applying simplified CDD measures.[7]

Reliability and Authenticity of Information and Documentation

33. Where the merchant bank obtains information or documents through the customer or a third party, the merchant bank should ensure that there is satisfactory evidence to show that the information or documents have been endorsed or otherwise authenticated by the relevant authority or official registry. Such information or documents should be as current as possible at the time they are provided to the merchant bank.

[7] Merchant banks should further note that where there is actual cause for suspecting money laundering or terrorist financing, the appropriate measures will be required – see paragraph 4.3(c) of the Notice.

Paragraphs 4.26 and 4.27 of the Notice – Non face-to-face Verification

34. Paragraphs 4.26 and 4.27 of the Notice address the situation where business relations are established or financial services are provided without face-to-face contact. Measures for managing the risks should include specific and effective procedures for CDD that apply to non face-to-face customers. In particular, a merchant bank should take appropriate measures to address risks arising from establishing business relations and undertaking transactions through instructions conveyed by customers over the internet, the post or the telephone.

35. As a guide, merchant banks should take one or more of the following measures to mitigate the heightened risk associated with not being able to conduct an interview face-to-face:

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

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

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

(d) confirmation of the customer's salary details by requiring the presentation of recent bank statements from another bank;

(e) certification of identification documents by lawyers or notary publics presented by the customer;

(f) requiring the customer to make an initial deposit using a cheque drawn on the customer's personal account with a bank in Singapore; and

(g) any other reliable verification checks adopted by the merchant bank for non-face- to-face banking business.

Paragraphs 4.32 and 4.33 of the Notice - Deferring the completion of CDD measures: Time limits for completion

36. Paragraph 4.32 of the Notice allows merchant banks to establish business relations before completing the CDD measures if it is essential for the

merchant bank not to interrupt the normal conduct of business and if the risks can be effectively managed.

37. An example where it may be essential not to interrupt the normal course of business would be with respect to securities trades, where market conditions are such that the merchant bank has to execute transactions for the customer very rapidly.

38. An example where the merchant bank may have effectively managed the risks of money laundering and terrorist financing is if the merchant bank has adopted internal policies, procedures and controls that set appropriate limits on the financial services available to the customer before completion of CDD measures. These may include, for example, limiting the number, type and value of transactions that might be effected in the interim period, and also the institution of a procedure that is more rigorous and intensive than usual for the monitoring of complex or unusually large transactions.

39. Paragraph 4.33 of the Notice requires that CDD measures be completed as soon as reasonably practicable, if a merchant bank allows business relations to be established without first completing CDD measures. Examples of reasonable timeframe are:

(a) the merchant bank completing CDD measures no later than 30 working days after the establishment of business relations;

(b) the merchant bank suspending business relations with the customer and refraining from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if CDD measures remain uncompleted 30 working days after the establishment of business relations; and

(c) the merchant bank terminating business relations with the customer if CDD measures remain uncompleted 120 working days after the establishment of business relations.

40. The merchant bank should factor these time limitations in their internal policies, procedures and controls.

Paragraph 4.35 of the Notice - Existing Customers

41. Paragraph 4.35 of the Notice concerns the application of CDD measures to the customers and accounts which the merchant bank has as at (date) when the Notice comes into force. Merchant banks are required to review the adequacy of identification information on the basis of materiality and risk, and to perform CDD measures on existing customers as may be appropriate.

42. In relation to accounts for which CDD measures had not previously been applied in accordance with the Notice, the merchant bank should make an assessment with regard to materiality and risk and determine when would be an appropriate time for the performance of CDD measures, subject to the more specific requirements for PEPs specified in paragraph 6.2 of the Notice.

43. As a guide, a merchant bank should perform CDD, in relation to paragraph 42 above, when:

(a) there is a transaction that is significant, having regard to the manner in which the account is ordinarily operated;

(b) there is a substantial change in the merchant bank's own customer documentation standards;

(c) there is a material change in the way that business relations with the customer are conducted;

(d) the merchant bank becomes aware that it may lack adequate identification information on a customer; and

(e) the merchant 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 merchant bank.

44. Where a merchant bank becomes aware upon a review that it may lack sufficient identification information on a customer, it should proceed to perform CDD afresh.

Paragraph 5 of the Notice - Simplified Customer Due Diligence

45. Paragraph 5.1 of the Notice allows merchant banks to apply simplified CDD measures in cases where the merchant bank is satisfied that the risk of money laundering or terrorist financing is low.

46. The merchant bank should assess the risks of money laundering or terrorist financing, having regard to the circumstances of each case, before applying the lesser or reduced CDD measures. Where the merchant bank adopts such lesser or reduced CDD measures, such measures should be commensurate with the merchant bank's assessment of the risks.

47. Examples of when the merchant bank might adopt lesser or reduced CDD measures are:

(a) where reliable information on the customer is publicly available to the merchant bank,

(b) the merchant bank is dealing with another bank whose AML/CFT controls it is well familiar with by virtue of a previous course of dealings; or

(c) the customer is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, or a listed company that is subject to regulatory disclosure requirements.

Paragraph 6.2 of the Notice - Identifying and dealing with PEPs

48. The definition of PEPs used in the Notice is drawn from the work of the FATF. The Authority recognises that the process of determining whether an individual is a PEP may not always be straightforward and a more precise definition would carry with it a greater risk of circumvention of the requirements under the Notice.

49. In the circumstances, the Authority would generally consider it acceptable for a merchant bank to refer to databases of PEPs either compiled commercially or by official authorities. However, in doing so, the Authority would expect the merchant bank to exercise a measure of discretion and sound judgment in determining for itself whether an individual should indeed be treated as a PEP, having regard to the risks and the circumstances.

Paragraphs 6.3 and 6.4 of the Notice - Other High Risk Categories

50. Paragraph 6.3 of the Notice requires enhanced CDD measures to be applied to other categories of customers apart from PEPs, which a merchant bank may consider to present a greater risk of money laundering or terrorist financing. Such high risk categories may include, for example, non-resident customers, private banking customers, body corporates set up as personal asset holding vehicles, or companies that have nominee shareholders or that issue shares in bearer form.

51. Merchant banks are also required by paragraph 6.4 of the Notice to give particular attention to business relations and transactions with persons from or in countries that have inadequate AML/CFT measures. For this purpose, merchant banks may take a range of steps, including the

adoption of measures similar to those for PEPs and other high risk categories.

52. While the Authority may from time to time circulate names of countries and jurisdictions with inadequate AML/CFT regimes (which can then be used as a reference guide), merchant banks are also encouraged to refer, where practicable, to other sources of information to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.

Paragraph 7 of the Notice - Reliance on Intermediaries

53. Where a merchant bank wishes to rely on an intermediary to perform elements of the CDD measures, paragraph 7.1(a) of the Notice requires the merchant bank to be satisfied that the 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 the Notice or the equivalent foreign measures.

54. The merchant bank may take a variety of measures, including but not limited to the following in determining whether the intermediary satisfies the requirements in paragraph 7.1(a):

(a) referring to any publicly available reports or material on the quality of AML/CFT supervision in the jurisdiction where that intermediary operates (such as mutual evaluation reports of the FATF and its associated bodies, or assessment reports made under the Financial Sector Assessment Programme of the International Monetary Fund and the World Bank);

(b) referring to any publicly available reports or material on the quality of that intermediary's compliance with applicable AML/CFT rules;

(c) obtaining professional advice as to the extent of AML/CFT obligations to which the intermediary is subject by the laws of the jurisdiction in which the intermediary operates; or

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

55. To the extent that the performance of CDD is undertaken by the intermediary rather than by the merchant bank, the merchant bank should be able to justify that that the conditions of paragraph 7 of the Notice have been met. The merchant bank should take considerable care when deciding if an intermediary is one on whom it can safely rely on to perform the CDD measures.

Paragraph 9.6 of the Notice - Responsibility of the beneficiary bank in identifying/handling in-coming wire transfers

56. Paragraph 9.6 of the Notice requires merchant banks to adopt appropriate risk-based procedures for identifying and handling in-coming wire transfers that are not accompanied by complete originator information. Merchant banks should consider not accepting in-coming wire transfers from or, terminating business relations with, overseas ordering banks that, to their knowledge, are required to provide originator information but fail to do so. In this respect, merchant banks should therefore take into account any requirements that may be imposed on the overseas ordering bank, either by law or as a regulatory measure, in respect of cross-border wire transfers.

57. In complying with paragraph 9.6, banks should therefore take into account any requirements that may be imposed on the overseas ordering bank, either by law or as a regulatory measure, in respect of cross-border wire transfers.

Paragraph 11 of the Notice - Suspicious Transaction Reporting

58. Paragraphs 11 of the Notice provide for the establishment of internal procedures for reporting suspicious transactions.

59. Banks are required to have adequate processes and systems for identifying and detecting suspicious transactions. The Authority expects the merchant bank to put in place effective and efficient procedures for reporting suspicious transactions.

60. The merchant bank should ensure that the internal process for evaluating whether a matter should be referred to the STRO via a STR be completed within 7 working days of the case being referred by the relevant bank staff, unless the circumstances are most extraordinary.

61. Examples of suspicious transactions are set out in Appendix II to these Guidelines. These examples are not intended to be exhaustive and are only examples of the most basic ways money may be laundered. If any transactions similar to those in Appendix II, or any other suspicious transactions, are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds.

62. Merchant banks are required to keep watch for suspicious transactions in the course of conducting screening against lists of terrorist suspects as may be required by law. The merchant bank should consider filing an STR

even though there is no positive match against any name if the surrounding circumstances raise sufficient suspicions.

63. Subject to any written law or any directions given by STRO or the Authority, merchant banks should as far as possible follow the reporting formats specified in Appendices III to V to these Guidelines. 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, merchant banks should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct. A copy of the STR should also be sent to the Authority.

64. Every merchant bank should maintain a complete file of all transactions that have been brought to the attention of its AML/CFT compliance officer or unit, including transactions that are not reported to STRO.

Paragraphs 12.8 and 12.9 of the Notice - Compliance

65. The responsibilities of the AML/CFT compliance officer should include the following:

(a) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;

(b) advising and training senior management and staff on development and implementing internal policies, procedures and controls on AML/CFT;

(c) carrying out, or overseeing the carrying out of, on-going monitoring of business relations and sample reviewing of accounts for compliance with the Notice and these Guidelines; and

(d) promoting compliance with the Notice and these Guidelines, including in particular observance of the underlying principles on AML/CFT in the Notice and taking overall charge of all AML/CFT matters within the organisation.

Paragraph 12.12 of the Notice - Conducting Training

66. As stated in paragraph 12.12 of the Notice, it is the responsibility of merchant banks to provide appropriate training on AML/CFT measures for their staff. To help ensure the effectiveness of training, merchant banks should monitor attendance at such training and take the appropriate

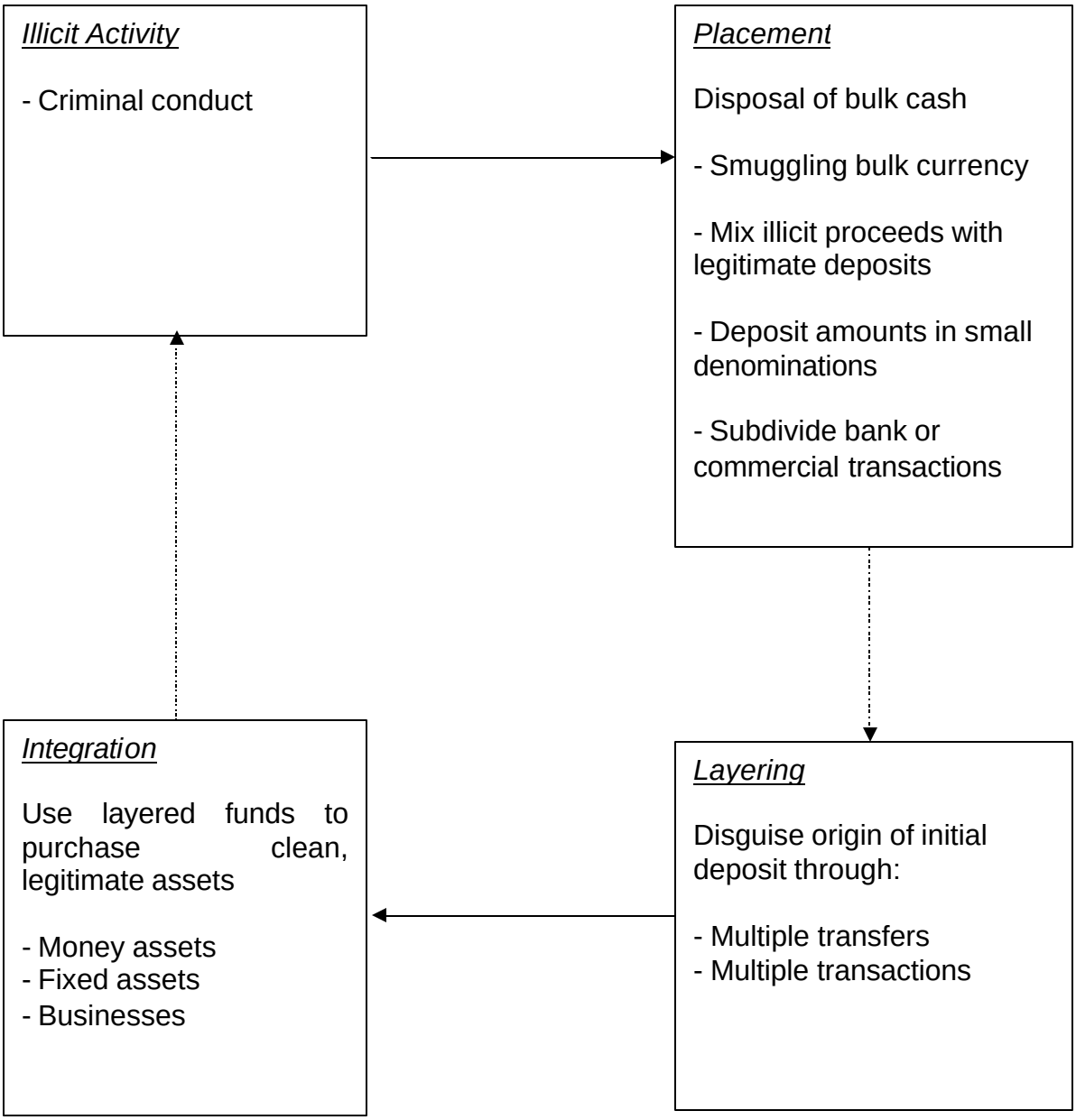
follow-up action in relation to staff who absent themselves without reasonable cause.

67. Apart from the initial training, merchant banks should also provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training should be held at least once a year.

……

APPENDIX I

PROCESS OF MONEY LAUNDERING



APPENDIX II

EXAMPLES OF SUSPICIOUS TRANSACTIONS

1 General Comments

The list of situations given below is intended to highlight 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 a suspicious transaction. The list is not exhaustive 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 merchant bank in the course of the business relationship. Merchant 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 merchant bank to verify.

2 Transactions Which Do Not Make Economic Sense

i) A customer-relationship with the merchant bank where a customer has a large number of accounts with the same bank, and has 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.

viii) Cash deposited at one location is withdrawn at another location almost immediately.

3 Transactions Involving Large Amounts of Cash

i) Frequent withdrawal of large amounts by means of cheques.

ii) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity.

iii) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

iv) 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.

vi) 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.

vii) 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.

viii) Customers whose deposits contain counterfeit notes or forged instruments.

ix) 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.

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.

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

ix) Transfers of funds from a company's account to an employee's account and vice-versa.

5 Transactions Involving Transfers Abroad

i) Transfer of a large amount of money abroad by a person who does not maintain an account with the merchant bank and who fails to provide a legitimate reason when asked.

ii) A customer who appears to have accounts with several banks in the same locality, especially when the merchant 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.

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) other 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.

viii) "U-turn" transactions. i.e. where funds received from a person or company in a foreign jurisdiction are immediately remitted to another person or company in the same foreign jurisdiction, or to the sender's account in another jurisdiction.

6 Investment Related Transactions

i) Purchasing of securities to be held by the merchant 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.

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

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

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

v) Frequent changes to the address or authorised signatories.

vi) A large amount of funds is received and immediately used as collateral for banking facilities.

vii) When a young person (aged about 17-26) opens an account and either withdraws or transfers the funds within a short period.

viii) When a person receives funds from a religious or charitable organisation and utilises the funds for purchase of assets or transfers out the funds within a relatively short period.

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 is to 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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

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 is to 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 each of the following documents is attached:

- Account Opening Forms
- Customer Identification Documents

- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)
Date:

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 is to 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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

[MAS Notice 314]

Introduction

1. These Guidelines are issued to provide guidance to the life insurers on some of the requirements in MAS Notice 314 (the "Notice") issued on [date].

2. Life insurers are reminded that the ultimate responsibility and accountability for ensuring the life insurer's compliance with AML/CFT laws, regulations and guidelines rests with the life insurer, its board of directors and senior management.

3. The expressions used in these Guidelines shall, except where expressly defined in these Guidelines or where the context otherwise requires, have the same respective meaning as in the Notice.

The structure of MAS Notice 314

4. The Notice sets out the obligations of a life insurer to take measures to help mitigate the risk of the Singapore life insurance industry from being used for money laundering or terrorist financing.

5. Paragraph 4 of the Notice deals with CDD measures. This paragraph sets out the standard CDD measures to be applied, of which there are six principal components:

   - Identification of the customer by obtaining certain information pertaining to the customer and, where the customer is not a natural person, certain other persons associated with that customer. Life insurers are also required to establish the identity of payees before making certain payments stipulated under paragraph 4.19 of the Notice;

   - Verifying the identification information obtained;

   - Where the customer is not a natural person, identifying and verifying the identity of its representatives;

   - Determining if there exists any beneficial owner (other than the customer) and applying the identification and verification procedures to those beneficial owners;

- After business relations are established, conducting on-going monitoring of business relations; and

- After business relations are established, periodically reviewing the adequacy of customer information.

6. Paragraphs 5 and 6 of the Notice provide for the risk-based customisation of the CDD measures. Thus, paragraph 5 on simplified CDD allows a life insurer to take lesser measures than those specified in paragraph 4 of the Notice provided that the conditions for simplified CDD are met. This will largely be a matter for individual life insurers to assess, but the life insurer must be able to justify its decision. Conversely, in situations where PEPs may be involved or in other situations where there is a higher risk of money laundering or terrorism financing, a life insurer is required under paragraph 6 of the Notice to take enhanced CDD measures.

7. To cater to cross-referrals, paragraph 7 of the Notice allows a life insurer to rely on another party, an intermediary, to perform certain elements of the CDD process, provided that certain conditions are met. This paragraph may typically be applied where a new customer is introduced to the life insurer by an intermediary resulting in direct business relations between the life insurer and the new customer. Thus, if the intermediary has already performed its own CDD on the new customer, then paragraph 7 allows the life insurer to dispense with performing CDD on the new customer if the conditions are satisfied. Paragraph 7 is not intended to cover the situation where a life insurer outsources the function of performing CDD measures to a third party.[8]

8. Finally, the Notice updates the previous requirements with respect to record keeping (paragraph 8), reporting of suspicious transactions (paragraph 9) and the institution of internal policies, procedures and control for AML/CFT (paragraph 10).

Key Concepts of the Notice

Money Laundering

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

[8] The Notice does not prohibit the outsourcing of the CDD function to a third party but where this occurs, the life insurer must remain fully responsible and accountable for the conduct of CDD measures as if the function had remained within the life insurer.

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

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

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

    (c) Integration - The provision of apparent legitimacy to the benefits of 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.

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

Terrorist Financing

11. 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. Life insurers should refer to the legal definitions of terrorism found in the law such as the Terrorism (Suppression of Financing) Act (Cap. 325), the United Nations (Anti-terrorism Measures) Regulations (Rg 1) and the Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002.

12. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. 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.

13. 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.

14. 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.

Paragraph 2.1 of the Notice – Definition of "Customer"

15. Paragraph 2.1 of the Notice defines "customer", in relation to a life insurer, as the person to whom a life insurance policy is issued or intended to be issued by the life insurer including, in the case of a group life insurance policy, the owner of the master policy issued or intended to be issued. In addition, the person for whom the life insurer undertakes or intends to undertake any transaction without a policy being issued would also be considered a customer of the life insurer.

16. The definition circumscribes the scope of the Notice. Life insurers should in general seek to perform CDD as widely as possible on persons that they deal with in the course of their operations.

Paragraphs 4.5, 4.7 and 4.8 of the Notice – Identification of Customers that are Not Natural Persons

17. Where the customer is not a natural person, paragraphs 4.5, 4.7 and 4.8 of the Notice require the life insurer to further establish the identity of the directors, partners or persons having executive authority of the customer respectively.

18. The life insurer should assess and determine, with respect to each customer, the key persons whose details they consider necessary to verify.

19. For the purposes of paragraph 18 above, the life insurer should consider whether persons, either singly or jointly with another, are able to give instructions concerning the use or transfer of funds or assets belonging to the customer in question.

Paragraphs 4.9 and 4.10 of the Notice - Verification of Identity

20. The requirements on verification of identity are intended to ensure that identity information provided by the customer is authentic.

21. Where the person whose identity is to be verified is a natural person, the life insurer should ask for some form of identification that contains a recent photograph of that person.

22. The life insurer should retain copies of all documentation used for verification of identity. Only in exceptional circumstances where the life insurer is unable to retain a copy of documentation used in verifying the customer's identity, the life insurer should record the following:

    (a) the information that the original documentation had served to verify;

    (b) the title and description of the original documentation produced to the life insurer's representative for verification, including any particular or unique features or condition of that documentation (whether it is worn out, or damaged etc);

    (c) the reasons why a copy of that documentation could not be made; and

    (d) the name of the life insurer's representative who carried out the verification, a statement by that representative certifying that he or she has duly verified the information against the documentation, and the date the verification took place.

Paragraphs 4.15 to 4.18 of the Notice -Identification of Beneficial Owners and Verification of their Identities

23. Life insurers are under a duty to take steps to determine if there exists, other than the person *ex facie* dealing with the life insurer as a customer, any other beneficial owner in relation to the customer.

24. Generally, the life insurer should assess and determine what measures would be appropriate to determine the beneficial owners, if any. The life insurer should be able to justify the reasonableness of the measures taken, having regard to the circumstances of each case.

25. Where the customer is not a natural person, the life insurer should take steps such as:

    (a) finding out about the ownership and structure of the company; and

(b) identifying the natural persons who have a controlling interest in the customer or who comprise the mind and management of the customer.

26. The life insurer may consider obtaining an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner.

27. Paragraph 4.17 of the Notice states that life insurers are not required to inquire if there exists any beneficial owner beyond the entities specified in sub-paragraphs (a) to (f).

28. The Authority recognises that it would be unnecessary to attempt to determine if beneficial owners exist behind these entities, since adequate information would already be available. For example, in the case of publicly listed companies, the shareholders (who would be the beneficial owners) would be changing relatively frequently and there would already be disclosure obligations imposed on substantial shareholders of such companies. In the case of financial institutions, there would have been adequate disclosure of the ownership and structure to the financial regulator.

29. While the entities listed would also typically be entities for which a life insurer may consider applying simplified CDD in accordance with paragraph 5 of the Notice, it is not the intent that the life insurer should thereby deem these entities to be automatically eligible for simplified CDD measures. The life insurer must comply with the requirements of paragraph 5 of the Notice before applying simplified CDD measures.[9]

Reliability and Authenticity of Information and Documentation

30. Where the life insurer obtains information or documents through the customer or a third party, the life insurer should ensure that there is satisfactory evidence to show that the information or documents have been endorsed or otherwise authenticated by the relevant authority or official registry. Such information or documents should be as current as possible at the time they are provided to the life insurer.

[9] Life insurers should further note that where there is actual cause for suspecting money laundering or terrorist financing, the appropriate measures will be required – see paragraph 4.2(c) of the Notice.

Paragraphs 4.24 and 4.25 of the Notice - Non Face-to-face verification

31. Paragraphs 4.24 and 4.25 of the Notice address the situation where business relations are established or financial services are provided without face-to-face contact. Measures for managing the risks should include specific and effective procedures for CDD that apply to non face-to-face customers. In particular, a life insurer should take appropriate measures to address risks arising from establishing business relations and undertaking transactions through instructions conveyed by customers over the internet, the post or the telephone.

32. As a guide, life insurers should take one or more of the following measures to mitigate the heightened risk associated with not being able to conduct an interview face-to-face:

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

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

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

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

(e) certification of identification documents by lawyers or notary publics presented by the customer;

(f) requiring the customer to make an initial premium payment using a cheque drawn on the customer's personal account with a bank in Singapore; or

(g) any other reliable verification checks adopted by the life insurer for non-face-to-face business.

Paragraphs 4.30 and 4.31 of the Notice - Deferring the completion of CDD measures: Time limits for completion

33. Paragraph 4.30 of the Notice allows life insurers to establish business relations before completing the CDD measures if it is essential for the life insurer not to interrupt the normal conduct of business and if the risks can be effectively managed.

34. An example where the life insurer may have effectively managed the risks of money laundering and terrorist financing if the life insurer has adopted internal policies, procedures and controls that set appropriate limits on the financial services available to the customer before completion of CDD measures. These may include, for example, limiting the number, type and value of transactions that might be effected in the interim period, and also the institution of a procedure that is more rigorous and intensive than usual for the monitoring of complex or unusually large transactions.

35. Paragraph 4.31 requires that CDD measures be completed as soon as reasonably practicable, if a life insurer allows business relations to be established without first completing CDD measures. Examples of reasonable timeframe are:

(a) the life insurer completing CDD measures no later than 30 working days after the establishment of business relations;

(b) the life insurer suspending business relations with the customer and refraining from carrying out further transactions (except to return premiums received) if CDD measures remain uncompleted 30 working days after the establishment of business relations; and

(c) the life insurer terminating business relations with the customer if CDD measures remain uncompleted 120 working days after the establishment of business relations.

36. The life insurer should factor these time limitations in their internal policies, procedures and controls.

Paragraph 4.33 of the Notice - Existing Customers

37. Paragraph 4.33 of the Notice concerns the application of CDD measures to the customers and policies which the life insurer has as at (date) when the Notice comes into force. Life insurers are required to review the adequacy of identification information on the basis of materiality and risk, and to perform CDD measures on existing customers as may be appropriate.

38. In relation to policies for which CDD measures had not previously been applied in accordance with the Notice, the life insurer should make an assessment with regard to materiality and risk and determine when would be an appropriate time for the performance of CDD measures, subject to the more specific requirements for PEPs specified in paragraph 6.2 of the Notice.

39. As a guide, a life insurer should perform CDD, in relation to paragraph 38 above, when:

(a) there is a transaction that is significant, having regard to the manner in which the policy is ordinarily operated;

(b) there is a substantial change in the life insurer's own customer documentation standards;

(c) there is a material change in the way that business relations with the customer are conducted;

(d) the life insurer becomes aware that it may lack adequate identification information on a customer; and

(e) the life insurer 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 life insurer.

40. Where a life insurer becomes aware upon a review that it may lack sufficient identification information on a customer, it should proceed to perform CDD afresh.

Paragraph 5 of the Notice - Simplified Customer Due Diligence

41. Paragraph 5.1 of the Notice allows life insurers to apply simplified CDD measures in cases where the life insurer is satisfied that the risk of money laundering or terrorist financing is low.

42. The life insurer should assess the risks of money laundering or terrorist financing, having regard to the circumstances of each case, before applying the lesser or reduced CDD measures. Where the life insurer adopts such lesser or reduced CDD measures, such measures should be commensurate with the life insurer's assessment of the risks.

43. Examples of when the life insurer might adopt lesser or reduced CDD measures are:

(a) where reliable information on the customer is publicly available to the life insurer,

(b) the life insurer is dealing with another financial institution whose AML/CFT controls it is well familiar with by virtue of a previous course of dealings; or

(c) the customer is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by FATF, or a listed company that is subject to regulatory disclosure requirements.

Paragraph 6.2 of the Notice - Identifying and dealing with PEPs

44. The definition of PEPs used in the Notice is drawn from the work of the FATF. The Authority recognises that the process of determining whether an individual is a PEP may not always be straightforward and a more precise definition would carry with it a greater risk of circumvention of the requirements under the Notice.

45. In the circumstances, the Authority would generally consider it acceptable for a life insurer to refer to databases of PEPs either compiled commercially or by official authorities. However, in doing so, the Authority would expect the life insurer to exercise a measure of discretion and sound judgment in determining for itself whether an individual should indeed be treated as a PEP, having regard to the risks and the circumstances.

Paragraph 6.3 and 6.4 of the Notice - Other High Risk Categories

46. Paragraph 6.3 of the Notice requires enhanced CDD measures to be applied to other categories of customers apart from PEPs, which a life insurer may consider to present a greater risk of money laundering or terrorist financing. Such high risk categories may include, for example, non-resident customers, body corporates set up as personal asset holding vehicles, or companies that have nominee shareholders or that issue shares in bearer form.

47. Life insurers are also required by paragraph 6.4 to give particular attention to business relations and transactions with persons from or in countries that have inadequate AML/CFT measures. For this purpose, life insurers may take a range of steps, including the adoption of measures similar to those for PEPs and other high risk categories.

48. While the Authority may from time to time circulate names of countries and jurisdictions with inadequate AML/CFT regimes (which can then be used as a reference guide), life insurers are also encouraged to refer, where

practicable, to other sources of information to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.

Paragraph 7 of the Notice - Reliance on Intermediaries

49. Where a life insurer wishes to rely on an intermediary to perform elements of the CDD measures, paragraph 7.1(a) of the Notice requires the life insurer to be satisfied that the 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 the Notice or the equivalent foreign measures.

50. The life insurers may take a variety of measures, including but not limited to the following in determining whether the intermediary satisfies the requirements in paragraph 7.1(a):

(a) referring to any publicly available reports or material on the quality of AML/CFT supervision in the jurisdiction where that intermediary operates (such as mutual evaluation reports of the FATF and its associated bodies, or assessment reports made under the Financial Sector Assessment Programme of the International Monetary Fund and the World Bank);

(b) referring to any publicly available reports or material on the quality of that intermediary's compliance with applicable AML/CFT rules;

(c) obtaining professional advice as to the extent of AML/CFT obligations to which the intermediary is subject by the laws of the jurisdiction in which the intermediary operates; or

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

51. To the extent that the performance of CDD is undertaken by the intermediary rather than by the life insurer, the life insurer should be able to justify that that the conditions of paragraph 7 of the Notice have been met. The life insurer should take considerable care when deciding if an intermediary is one on whom it can safely rely on to perform the CDD measures.

Paragraph 9 of the Notice - Suspicious Transaction Reporting

Paragraph 9 of the Notice provide for the establishment of internal procedures for reporting suspicious transactions.

52. Life insurers are required to have adequate processes and systems for identifying and detecting suspicious transactions. The Authority also expects the life insurer to put in place effective and efficient procedures for reporting suspicious transactions.

53. The life insurer should also ensure that the internal process for evaluating whether a matter should be referred to the STRO via an STR be completed within 7 working days of the case being referred by the relevant life insurer staff to the AML/CFT compliance officer, unless the circumstances are most extraordinary.

54. Examples of suspicious transactions are set out in Appendix II to these Guidelines. These examples are not intended to be exhaustive and are only examples of the most basic ways money may be laundered. If any transactions similar to those in Appendix II or any other suspicious transactions are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds.

55. Life insurers are required to keep watch for suspicious transactions in the course of conducting screening against lists of terrorist suspects as may be required by law or circulated by any relevant authority. The life insurer should consider filing an STR even though there is no positive match against any name if the surrounding circumstances raises sufficient suspicions.

56. Subject to any written law or any directions given by STRO or other relevant authorities, life insurers should as far as possible follow the reporting formats specified in Appendices III to V to these Guidelines. 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, life insurers should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct. A copy of the STR should also be sent to the Authority.

57. Every life insurer shall maintain a complete file of all transactions that have been brought to the attention of its AML/CFT compliance officer or unit, including transactions that are not reported to STRO.

Paragraph 10.8 and 10.9 of the Notice - Compliance

58. The responsibilities of the AML/CFT compliance officer should include the following:

(a) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;

(b) advising and training senior management and staff on development and implementing internal policies, procedures and controls on AML/CFT;

(c) carrying out, or overseeing the carrying out of on-going monitoring of business relations and sample reviewing of policies for compliance with the Notice and these Guidelines; and

(d) promoting compliance with the Notice and these Guidelines, including in particular observance of the underlying principles on AML/CFT in the Notice and taking overall charge of all AML/CFT matters within the organisation.

Paragraph 10.12 of the Notice - Conducting Training

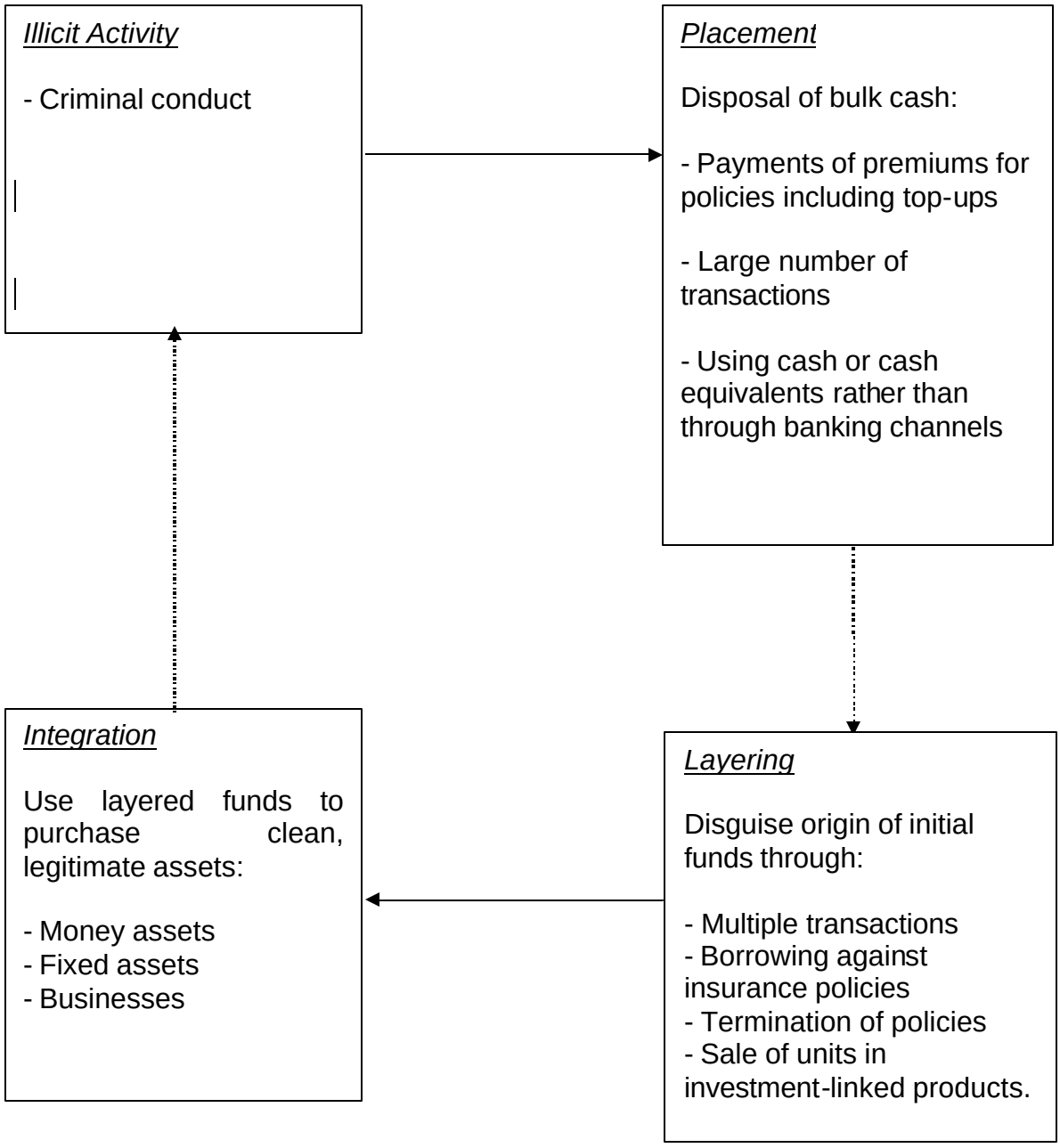
59. As stated in paragraph 10.12 of the Notice, it is the responsibility of life insurers to provide appropriate training on AML/CFT measures for its staff. To help ensure the effectiveness of training, life insurers should monitor attendance at such training and take the appropriate follow-up action in relation to staff who absent themselves without reasonable cause.

60. Apart from the initial training, life insurers should also provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training should be held at least once a year.

……..

APPENDIX I

PROCESS OF MONEY LAUNDERING



APPENDIX II

EXAMPLES OF SUSPICIOUS TRANSACTIONS

1 General Comments

The list of situations given below is intended to highlight 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 a suspicious transaction. The list is not exhaustive 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 life insurer in the course of the business relationship. Life insurers should pay attention to customers who provide minimal, false or misleading information or, when applying for a policy, provide information that is difficult or expensive for the life insurer to verify.

2 Transactions Which Do Not Make Economic Sense

i) A customer-relationship with the life insurer that does not appear to make economic sense, for example, the early redemption of a policy when the surrender value is less than the value of premiums paid.

ii) Transactions in which policies are cancelled shortly after premiums have been paid, resulting in the return of premiums, unless the life insurer is furnished with a plausible reason for the cancellation, especially where policy premiums have been paid in cash.

iii) Transactions that are incompatible with the normal activities of the customer, for example, taking out a policy loan soon after the inception of the policy. In addition, if an existing customer whose current contracts are small and/or involve only small, regular premium payments makes a sudden request for a purchase of a significantly large single premium policy, this may also prompt further investigations by the life insurer.

iv) Transactions that are not commensurate with the customer's apparent financial means, for example, where customers without reasonable financial standing purchase large single premium policies for a large assured sum.

v) Transactions where the nature, size or frequency appears unusual, for example, a customer requests for transactions involving multiple policies of similar nature, which aggregate to large amounts. In addition, a customer request for the early termination of a single premium policy especially when cash had been tendered may also prompt further investigations by the life insurer.

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

vii) Abnormal settlement instructions, including payment to apparently unconnected parties.

3 Transactions Involving Large Sums

i) Payment of premiums via large or unusual amounts of cash. In particular, an insurer should be vigilant in verifying information and the nature of transactions of any customer if any single payment exceeds $20,000 in cash.

ii) Frequent taking out of policy loans that are repaid with large amounts of cash.

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

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

4 Transactions Involving Transfers Abroad

i) Large and regular premium payments that cannot be clearly identified as bona fide transactions, from countries associated with (i) the production, processing or marketing of narcotics or other illegal drugs or (ii) other criminal conduct.

ii) Substantial increase in cash premium payments from foreign countries by a customer without apparent cause, especially when such transactions are not consistent with the customer's transaction history.

5 Transactions Involving Unidentified Parties

i) Paying premiums in large third party cheques on behalf of the customer.

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

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

6 Free-Look Provisions and Other Matters

i) Frequent changes to the address or where the customer is a non-natural person, frequent changes to authorised signatories.

ii) A policyholder may exercise cancellation rights or cooling off rights on life insurance products where the sum invested must be repaid (subject to any shortfall deduction where applicable). This could offer a readily available route for laundering money, and insurers should therefore be alert to any abnormal exercise of cancellation/cooling off rights by any policyholder. In the event that abnormal exercise of these rights becomes apparent, the matter should be treated as suspicious and reported through the usual channels.

iii) Employees or agents who have consistently high activity levels of single premium business far in excess of any average company expectation.

iv) The use of an address that is not the customer's permanent address, for example, utilisation of the agent’s office or home address for the dispatch of customer documentation.

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 Life Insurer	
Name:	
Address:	
Telephone:	
Fax:	
E-mail:	
Life Insurer 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 life insurer shall provide particulars on joint policyholders, if any.

Employment Details	
Employer's Name:	
Address:	
Telephone:	
Business Relationship(s) with Customer	
Life insurer policy No.:	
Type of policy:	
Date of Commencement:	
Name of Agent: *(if applicable)*	
Agent's NRIC/Passport No.: *(if applicable)*	
Sum Assured:	
Payment Mode:	
Premiums Payable:	
(in Original Currency)	
(in Singapore Currency)	
Other Business Relationships:	

Suspicious Transaction(s)		
Amount	**Date**	**Description of Transaction (E.g. Nature/type of transaction, source of funds, destination, etc)**

Reason(s) for Suspicion:

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

A copy each of the following documents is attached:

- Policy Application Forms
- Agent's Report
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

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 Life Insurer	
Name:	
Address:	
Telephone:	
Fax:	
E-mail:	
Life Insurer 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	
Life insurer policy No.:	
Type of policy:	
Date of Commencement:	
Name of Agent: *(if applicable)*	
Agent's NRIC/Passport No.: *(if applicable)*	
Sum Assured:	
Payment Mode:	
Premiums Payable:	
(in Original Currency)	
(in Singapore Currency)	
Other Business Relationships:	

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

[#] The reporting officer of the life insurer shall provide data on other authorised signatories, if any.

Suspicious Transaction(s)		
Amount	**Date**	**Description of Transaction (E.g. Nature/type of transaction, source of funds, destination, etc)**

Reason(s) for Suspicion:

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

A copy each of the following documents is attached:

- Policy Application Forms
- Agent's Report
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

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 Life Insurer	
Name:	
Address:	
Telephone:	
Fax:	
E-mail:	
Life Insurer 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	
Life insurer policy No.:	
Type of policy:	
Date of Commencement:	
Name of Agent: *(if applicable)*	
Agent's NRIC/Passport No.: *(if applicable)*	
Sum Assured:	
Payment Mode:	
Premiums Payable:	
(in Original Currency)	
(in Singapore Currency)	
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 life insurer shall provide data on other authorised signatories, if any.

Suspicious Transaction(s)		
Amount	**Date**	**Description of Transaction (E.g. Nature/type of transaction, 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 each of the following documents is attached:

- Policy Application Forms
- Agent's Report
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

[MAS Notice SFA04-N02]

Introduction

1. These Guidelines are issued to provide guidance to holders of a Capital Markets Services licence and persons exempt under paragraph 4(1)(c), 5(1)(d) or 7(1)(b) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations from having to hold a Capital Markets Services licence (hereinafter the "Capital Markets intermediaries" or "CMIs") on some of the requirements of SFA 04-N02 ("the Notice") issued on [date].

2. CMIs are reminded that the ultimate responsibility and accountability for ensuring the CMI's compliance with AML/CFT laws, regulations and guidelines rests with the CMI, its board of directors and senior management.

3. The expressions used in these Guidelines shall, except where expressly defined in these Guidelines or where the context otherwise requires, have the same respective meanings as in the Notice.

The structure of SFA 04-N02

4. The Notice sets out the obligations of a CMI to take measures to help mitigate the risk of Singapore's capital markets being used for money laundering or terrorist financing.

5. While the Authority has drawn up our requirements for the financial industry to implement the FATF's recommendations, sector specific needs are also taken into consideration. For CMIs, we have also incorporated guidance and principles developed by the International Organisation of Securities Commissions ("IOSCO")[10].

6. Paragraph 4 of the Notice deals with CDD measures. This paragraph sets out the standard CDD measures to be applied, of which there are seven principal components:

---

[10] Specifically, the sector specific guidance is drawn from the two IOSCO papers, "Principles on Identification and Beneficial Ownership for the Securities Industry" and "Anti-Money Laundering Guidance for Collective Investment Schemes" issued in May 2004 and October 2005 respectively.

- Identification of the customer by obtaining certain information pertaining to the customer and, where the customer is not a natural person, certain other persons associated with that customer;

- Verifying the identification information obtained;

- Where the customer is not a natural person, identifying and verifying the identity of its representatives;

- Determining if there exists any beneficial owner (other than the customer) and applying the identification procedures to those beneficial owners;

- Where business relations are to be established (as defined in the Notice), obtaining information as to the nature and purpose of the intended business relations;

- After business relations are established, conducting on-going monitoring of business relations; and

- After business relations are established, periodically review the adequacy of customer information.

7. Paragraphs 5 and 6 of the Notice provide for the risk-based customisation of CDD measures. Thus, paragraph 5 on simplified CDD allows a CMI to take lesser measures than those specified in paragraph 4 of the Notice provided that the conditions for simplified CDD are met. This will largely be a matter for individual CMIs to assess, but the CMI must be able to justify its decision. Conversely, in situations where PEPs may be involved or in other situations where there is a higher risk of money laundering or terrorist financing, a CMI is required under paragraph 6 of the Notice to take enhanced CDD measures.

8. To cater to cross-referrals, paragraph 7 of the Notice allows a CMI to rely on another party, an intermediary, to perform certain elements of the CDD process, provided that certain conditions are met. This paragraph may typically be applied where a new customer is introduced to the CMI by an intermediary resulting in direct business relations between the CMI and the new customer. Thus, if the intermediary has already performed its own CDD on the new customer, then paragraph 7 allows the CMI to dispense with performing CDD on the new customer if the conditions are satisfied. Paragraph 7 is not intended to cover the situation where a CMI outsources the function of performing CDD measures to a third party.[11]

[11] The Notice does not prohibit the outsourcing of the CDD function to a third party but where this occurs, the CMI must remain fully responsible and accountable for the conduct of CDD measures as if the function had remained within the CMI.

9. Finally, the Notice updates the previous requirements with respect to record keeping (paragraph 10), reporting of suspicious transactions (paragraph 11) and the institution of internal policies, procedures and controls for AML/CFT (paragraph 12).

Key Concepts of the Notice

Money Laundering

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

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

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

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

(c) Integration - The provision of apparent legitimacy to the benefits of 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.

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

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

13. Capital markets offer a vast array of opportunities for transforming money into a diverse range of assets. For liquid assets, they allow a high frequency of transactions which aids the layering process. Hence, capital markets are particularly attractive to money-launderers for layering their illicit proceeds for eventual integration into the general economy.

Terrorist Financing

14. 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. CMIs should refer to the legal definitions of terrorism found in the law such as the Terrorism (Suppression of Financing) Act (Cap. 325), the United Nations (Anti-terrorism Measures) Regulations (Rg 1) and the Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002.

15. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. 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.

16. 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.

17. 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.

Paragraph 2.1 of the Notice – Definition of "Customer"

18. Paragraph 2.1 of the Notice defines "customer", in relation to a CMI, as the person in whose name an account is opened or intended to be opened, or to whom a CMI undertakes or intends to undertake any transaction without an account being opened.

19. The definition circumscribes the scope of the Notice. CMIs should in general seek to perform CDD as widely as possible on persons that they deal with in the course of their business operations.

20. In the cases below, the following approaches below may be adopted:

(a) Portfolio Managers

A CMI may often encounter cases where, to the CMI's knowledge, the customer is a manager of a portfolio of assets and is operating the account in that capacity. In such cases, the underlying investors of the portfolio will be beneficial owners within the meaning of the Notice.

However, the Authority recognises that a CMI may not be able to perform CDD on the underlying investors. For instance, the portfolio manager may be reluctant, for legitimate commercial reasons, to reveal information on the underlying investors to the CMI. In such circumstances, the CMI should evaluate the risks arising for each case and determine the appropriate CDD measures to take. The CMI may consider whether simplified CDD measures could be applied under paragraph 5 of the Notice, so that identification and verification of the underlying investors as beneficial owners are dispensed with.

In addition, where a collective investment scheme ("CIS") is the customer for a CMI, the CMI should take steps to identify whether it is an "exchange-listed" CIS or an "open-ended" CIS. A CMI is not expected to identify the beneficial owners of an exchange-listed CIS that is subject to regulatory disclosure requirements, unless there is a suspicion that a transaction is connected with money laundering or terrorist financing. For an open-ended CIS, a CMI can consider if there is a case for simplified CDD if the CIS and/or its manager, as the case may be, are subject to and supervised for compliance with AML/CFT requirements that are consistent with standards set by FATF and ISOCO.

(b) Omnibus Accounts

Omnibus accounts may be established by and in the name of financial institutions in order to engage in securities transactions on behalf of their clients. When the CMI opens an omnibus account for a customer who is a financial institution supervised by the Authority, the risk of the omnibus account being used for money laundering or terrorist financing is generally lower. The CMI can consider if there is a case under paragraph 5 of the Notice for the application of simplified CDD measures, so that there is no need to identify and verify the underlying clients of the financial institution.

However, when the CMI opens an omnibus account for a customer who is a foreign financial institution, the risks associated with the account in some circumstances may be considered to be potentially higher, and enhanced CDD measures may be appropriate.

(c) Location of Relationship Management

Given the globalised nature of modern capital markets, it may often be the case that a CMI's relationship and transactions with a particular customer would be managed by officers based in one country or jurisdiction but the account itself is held with an office in another country or jurisdiction for book-keeping purposes. For the purposes of the Notice, the Authority will generally look at the substance of the relationship as a whole. A CMI should maintain basic customer identification information if in substance, the person is a customer of the CMI in Singapore even though the account is booked in another country or jurisdiction. However, the CMI may rely on the CDD done by its related entity in accordance with paragraph 7 of the Notice.

Paragraphs 4.6, 4.8 and 4.9 of the Notice – Identification of Customers that are not Natural Persons

21. Where the customer is not a natural person, paragraphs 4.6, 4.8 and 4.9 of the Notice respectively require the CMI to further establish the identity of the directors, partners or persons having executive authority, of the customer respectively.

22. The CMI should assess and determine, with respect to each customer, the key persons whose details they consider necessary to verify.

23. For purposes of paragraph 22 above, the CMI should consider whether persons, either singly or jointly with another, are able to give instructions concerning the use or transfer of funds or assets belonging to the customer in question.

Paragraphs 4.10 and 4.11 of the Notice - Verification of Identity

24. The requirements on verification of identity are intended to ensure that identity information provided by the customer is authentic.

25. Where the person whose identity is to be verified is a natural person, the CMI should ask for some form of identification that contains a recent photograph of that person.

26. The CMI should retain copies of all documentation used for verification of identity. Only in exceptional circumstances where the CMI is unable to retain a copy of documentation used in verifying the customer's identity, the CMI should record the following:

(a) the information that the original documentation had served to verify;

(b) the title and description of the original documentation produced to the CMI's officer for verification, including any particular or unique features or condition of that documentation (whether it is worn out, or damaged etc);

(c) the reasons why a copy of that documentation could not be made; and

(d) the name of the CMI's officer who carried out the verification, a statement by that officer certifying that he or she has duly verified the information against the documentation, and the date the verification took place.

Paragraphs 4.16 to 4.19 of the Notice - Identification of Beneficial Owners and Verification of their Identities

27. CMIs are under a duty to take steps to determine if there exists, other than the person *ex facie* dealing with the CMI as a customer, any other beneficial owner in relation to the customer.

28. Generally, the CMI should assess and determine what measures would be appropriate to determine the beneficial owners. The CMI should be able to justify the reasonableness of the measures taken, having regard of the circumstances of each case. In general, CMIs should adopt a risk based approach when taking steps to identify the beneficial owners of legal vehicles such as companies that issue shares in bearer form, unregistered or unregulated investment vehicles, highly leveraged institutions, mandates and trusts on a risk-based approach.

29. Where the customer is not a natural person, such as a company, the CMI should take steps such as:

(a) finding out about the ownership and control structure of the company; and

(b) identifying the natural persons who have a controlling interest in the customer or who comprise the mind and management of the customer.

30. The CMI may also consider obtaining an undertaking or declaration from the customer on the identity of and the information relating to the beneficial owner.

31. Paragraph 20(a) of these Guidelines makes reference to the case where the customer is a portfolio manager. In that situation, as well as other instances where the customer has a *bona fide* and legitimate interest or duty not to disclose to the CMI the identity or particulars of beneficial owners who are known to exist, the CMI may consider the application of simplified CDD set out in paragraph 5 of the Notice.

32. Paragraph 4.18 of the Notice states that CMIs are not required to inquire if there exists any beneficial owner beyond the entities specified in sub-paragraphs (a) to (f).

33. The Authority recognises that it would be unnecessary to attempt to determine if beneficial owners exist behind these entities, since adequate information would already be available. For example, in the case of publicly listed companies, the shareholders (who would be the beneficial owners) would be changing relatively frequently and there would already be disclosure obligations imposed on substantial shareholders of such companies. In the case of financial institutions, there would ordinarily have been adequate disclosure of the ownership and structure to the financial regulator.

34. While the entities listed would also typically be entities for which a CMI may consider applying simplified CDD in accordance with paragraph 5 of the Notice, it is not the intent that the CMI should thereby deem these entities to be automatically eligible for simplified CDD measures. The CMI must still comply with the requirements of paragraph 5 of the Notice before applying simplified CDD measures.[12]

Reliability and Authenticity of Information and Documentation

35. Where the CMI obtains information or documents through the customer or a third party, the CMI should ensure that there is satisfactory evidence to show that the information or documents have been endorsed or otherwise authenticated by the relevant authority or official registry. Such information or documents should be as current as possible at the time they are provided to the CMI.

Paragraphs 4.26 and 4.27 of the Notice - Non Face-to-Face Verification

36. Paragraphs 4.26 and 4.27 of the Notice address the situation where business relations are established or financial services are provided without face-to-face contact. Measures for managing the risks should include specific and effective procedures for CDD that apply to non face-

[12] CMIs should further note that where there is actual cause for suspecting money laundering or terrorist financing, the appropriate measures will be required – see paragraph 4.3(c) of the Notice.

to-face customers. In particular, a CMI should take appropriate measures to address risks arising from establishing business relations and undertaking transactions through instructions conveyed by customers over the internet, the post or the telephone.

37. As a guide, CMIs should take one or more of the following measures to mitigate the heightened risk associated with not being able to conduct an interview face-to-face:

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

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

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

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

(e) certification of identification documents by lawyers or notary publics presented by the customer;

(f) requiring the customer to make an initial deposit drawn on a personal cheque of the customer drawn on a bank in Singapore; and

(g) any other reliable verification checks adopted by the CMI for non-face- to-face business.

Paragraphs 4.29 and 4.30 of the Notice – CDD Measures for Non-Account Holders

38. A CMI would typically not be expected to have customers who are non-account holders. In particular, while a CMI may not directly open and maintain accounts for customers, it may provide other complementary services such as monitoring asset holdings, sending statements of holdings or other related services which in substance relates to the maintaining of accounts for the customers. A CMI should not consider such customers as non-account holders.

Direct subscription and redemption of CIS

While most CIS managers prefer to focus on the fund management business and are not involved directly in the distribution business, it is recognised that some CIS managers do allow retail customers to subscribe and redeem CIS directly. A CMI should not consider such subscription and redemption of CIS as occasional transactions of non-account holders.

Paragraphs 4.32 and 4.33 of the Notice - Deferring the completion of CDD measures : Time limits for completion

39. Paragraph 4.32 of the Notice allows CMIs to establish business relations before completing the CDD measures if it is essential for the CMI not to interrupt the normal conduct of business and if the risks can be effectively managed.

40. An example where it may be essential not to interrupt the normal course of business would be with respect to securities trades, where market conditions are such that the CMI has to execute transactions for the customer very rapidly.

41. An example where the CMI may have effectively managed the risks of money laundering and terrorist financing is if the CMI has adopted internal policies, procedures and controls that set appropriate limits on the financial services available to the customer before completion of CDD measures. These may include, for example, limiting the number, type and value of transactions that might be effected in the interim period, and also the institution of a procedure that is more rigorous and intensive than usual for the monitoring of complex or unusually large transactions.

42. Paragraph 4.33 requires that CDD measures be completed as soon as reasonably practicable, if a CMI allows business relations to be established without first completing CDD measures. Examples of reasonable timeframe are:

(a) the CMI completing CDD measures no later than 30 working days after the establishment of business relations;

(b) the CMI suspending business relations with the customer and refraining from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if CDD measures remain uncompleted 30 working days after the establishment of business relations; and

(c) the CMI terminating business relations with the customer if CDD measures remain uncompleted 120 working days after the establishment of business relations.

43. The CMI should factor these time limitations in their internal policies, procedures and controls.

Paragraph 4.35 of the Notice - Existing Customers

44. Paragraph 4.35 of the Notice concerns the application of CDD measures to the customers and accounts which the CMI has as at (date) when the Notice comes into force. CMIs are required to review the adequacy of identification information on the basis of materiality and risk, and to perform CDD measures on existing customers as may be appropriate.

45. In relation to accounts for which CDD measures had not previously been applied in accordance with the Notice, the CMI should make an assessment with regard to materiality and risk and determine when would be an appropriate time for the performance of CDD measures, subject to the more specific requirements for PEPs specified in paragraph 6.2 of the Notice.

46. As a guide, a CMI should perform CDD, in relation to paragraph 45 above when:

(a) there is a transaction that is significant, having regard to the manner in which the account is ordinarily operated;

(b) there is a substantial change in the CMI's own customer documentation standards;

(c) there is a material change in the way that business relations with the customer are conducted;

(d) the CMI becomes aware that it may lack adequate identification information on a customer; and

(e) the CMI 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 CMI.

47. Where a CMI becomes aware upon a review that it may lack sufficient identification information on a customer, it should proceed to perform CDD afresh.

Paragraph 5 of the Notice - Simplified Customer Due Diligence

48. Paragraph 5.1 of the Notice allows CMIs to apply simplified CDD measures in cases where the CMI is satisfied that the risk of money laundering or terrorist financing is low.

49. The CMI should assess the risks of money laundering or terrorist financing, having regard to the circumstances of each case, before applying the lesser or reduced CDD measures. Where the CMI adopts such lesser or reduced CDD measures, such measures should be commensurate with the CMI's assessment of the risk.

50. Examples of when the CMI might adopt lesser or reduced CDD measures are:

    (a) where reliable information on the customer is publicly available to the CMI;

    (b) the CMI is dealing with another financial institution whose AML/CFT controls it is well familiar with by virtue of a previous course of dealings; or

    (c) the customer is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, or a listed company that is subject to regulatory disclosure requirements.

Paragraph 6.2 of the Notice - Identifying and dealing with PEPs

51. The definition of PEPs used in the Notice is drawn from the work of the FATF. The Authority recognises that the process of determining whether an individual is a PEP may not always be straightforward and a more precise definition would carry with it a greater risk of circumvention of the requirements of the Notice.

52. In the circumstances, the Authority would generally consider it acceptable for a CMI to refer to databases of PEPs either compiled commercially or by official authorities. However, in doing so, the Authority would expect the CMI to exercise a measure of discretion and sound judgment in determining for itself whether an individual should indeed be treated as a PEP, having regard to the risks and the circumstances.

Paragraph 6.3 and 6.4 of the Notice - Other High Risk Categories

53. Paragraph 6.3 of the Notice requires enhanced CDD measures to be applied to other categories of customers apart from PEPs, which a CMI may consider to present a greater risk of money laundering or terrorist financing. Such high risk categories may include, for example, non-resident customers, private banking customers, body corporates set up as personal asset holding vehicles, or companies that have nominee shareholders or that issue shares in bearer form.

54. CMIs are also required by paragraph 6.4 of the Notice to give particular attention to business relations and transactions with persons from or in countries that have inadequate AML/CFT measures. For this purpose, CMIs may take a range of steps, including the adoption of measures similar to those for PEPs and other high risk categories.

55. While the Authority may from time to time circulate names of countries and jurisdictions with inadequate AML/CFT regimes (which can then be used as a reference guide), CMIs are also encouraged to refer, where practicable, to other sources of information to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.

Paragraph 7 of the Notice - Reliance on Intermediaries

56. Where a CMI wishes to rely on an intermediary to perform elements of the CDD measures, paragraph 7.1(a) of the Notice requires the CMI to be satisfied that the 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 the Notice or the equivalent foreign measures.

57. The CMI may take a variety of measures, including but not limited to the following in determining whether the intermediary satisfies the requirements in paragraph 7.1(a):

    (a) referring to any publicly available reports or material on the quality of AML/CFT supervision in the jurisdiction where that intermediary operates (such as mutual evaluation reports of the FATF and its associated bodies, or assessment reports made under the Financial Sector Assessment Programme of the International Monetary Fund and the World Bank);

    (b) referring to any publicly available reports or material on the quality of that intermediary's compliance with applicable AML/CFT rules;

(c) obtaining professional advice as to the extent of AML/CFT obligations to which the intermediary is subject by the laws of the jurisdiction in which the intermediary operates; or

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

58. To the extent that the performance of CDD is undertaken by the intermediary rather than by the CMI, the CMI should be able to justify that the conditions of paragraph 7 of the Notice have been met. The CMI should take considerable care when deciding if an intermediary is one on whom it can safely rely on to perform the CDD measures.

Paragraph 11 of the Notice - Suspicious Transaction Reporting

59. Paragraph 11 of the Notice provides for the establishment of internal procedures for reporting suspicious transactions.

60. CMIs are required to have adequate processes and systems for identifying and detecting suspicious transactions. The Authority also expects the CMI to put in place effective and efficient procedures for reporting suspicious transactions.

61. The CMI should ensure that the internal process for evaluating whether a matter should be referred to the STRO via a STR be completed within 7 working days of the case being referred by the relevant CMI's staff.

62. Examples of suspicious transactions are set out in Appendix II to these Guidelines. These examples are not intended to be exhaustive and are only examples of the most basic ways money may be laundered. If any transactions similar to those in Appendix II, or any other suspicious transactions, are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds.

63. CMIs are required to keep watch for suspicious transactions in the course of conducting screening against lists of terrorist suspects as may be required by law or circulated by any relevant authority. The CMI should consider filing an STR even though there is no positive match against any name if the surrounding circumstances raise sufficient suspicions.

64. Subject to any written law or any directions given by STRO or the Authority, CMIs should as far as possible follow the reporting formats specified in Appendices III to V to these Guidelines. 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, CMIs should give initial notification to STRO by telephone or e-mail and follow up with such other means of reporting as STRO may direct. A copy of the STR should also be sent to the Authority.

65. Every CMI should maintain a complete file of all transactions that have been brought to the attention of its AML/CFT compliance officer or unit, including transactions that are not reported to STRO.

Paragraphs 12.8 and 12.9 of the Notice - Compliance

66. The responsibilities of the AML/CFT compliance officer should include the following:

(a) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;

(b) advising and training senior management and staff on development and implementing internal policies, procedures and controls on AML/CFT;

(c) carrying out, or overseeing the carrying out of, on-going monitoring of business relations and sample reviewing of accounts for compliance with the Notice and these Guidelines; and

(d) promoting compliance with the Notice and these Guidelines, including in particular observance of the underlying principles on AML/CFT in the Notice and taking overall charge of all AML/CFT matters within the organisation.

Paragraph 12.12 of the Notice - Conducting Training

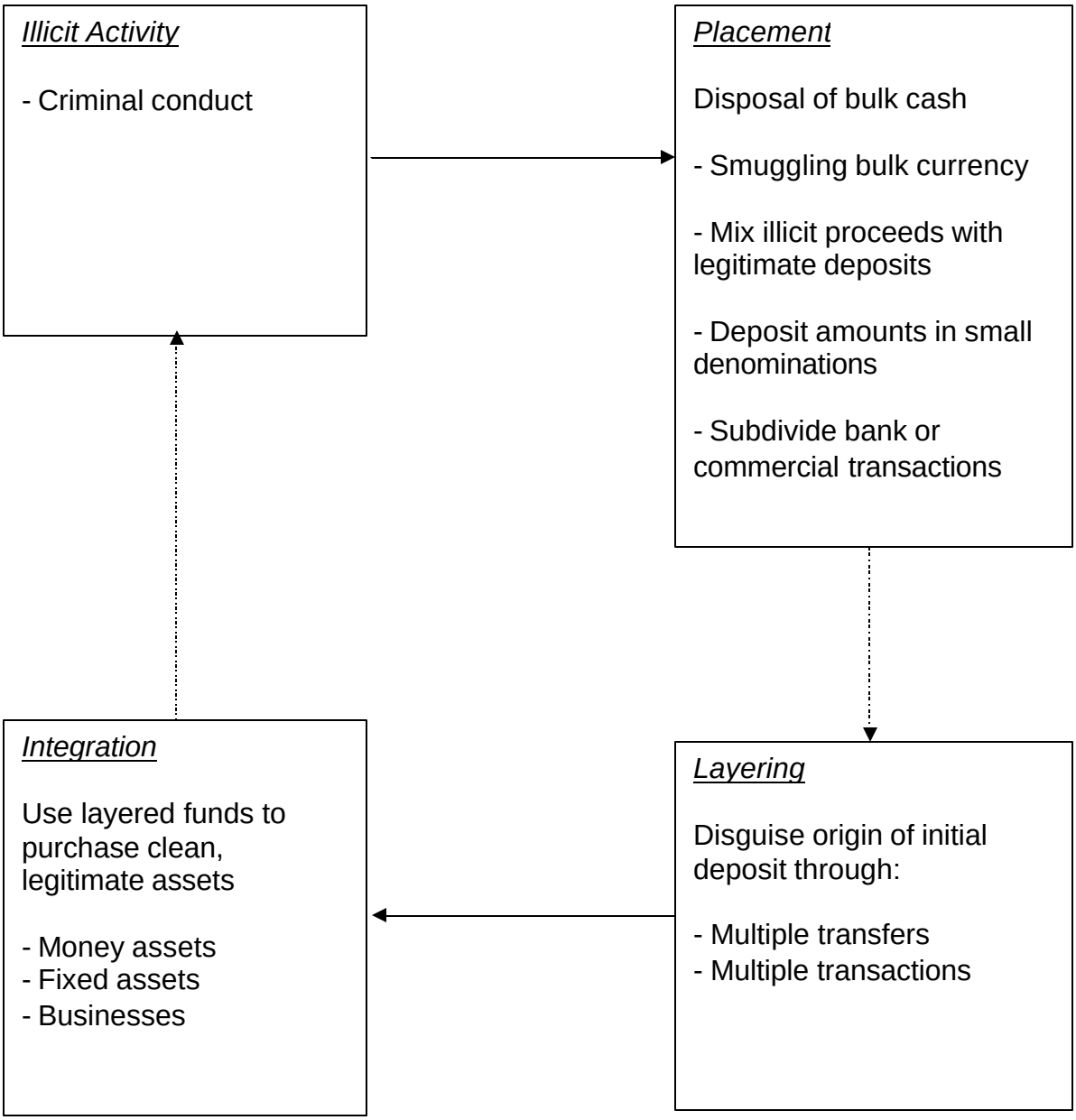
67. As stated in paragraph 12.12 of the Notice, it is the responsibility of CMIs to provide appropriate training on AML/CFT measures for its staff. To help ensure the effectiveness of training, CMIs should monitor attendance at such training and take the appropriate follow-up action in relation to staff who absent themselves without reasonable cause.

68. Apart from the initial training, CMIs should also provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training should be held at least once a year.

……

APPENDIX I

PROCESS OF MONEY LAUNDERING



APPENDIX II

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 a suspicious 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 CMI in the course of the business relationship. CMIs should pay attention to customers who provide minimal, false or misleading information or, when applying to open an account, provide information that is difficult or expensive for the CMI to verify.

2 Transactions Which Do Not Make Economic Sense

i) A customer-relationship with the CMI that does not appear to make economic sense, for example, a customer who carries out frequent large transactions which do not fit his economic background.

ii) Transactions in which funds are withdrawn immediately after being deposited[13], 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, switching from trading only penny stocks to predominantly blue chips.

iv) Sudden increase in intensity of transactions, without plausible reason, of what was previously a relatively inactive customer trading account.

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

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

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

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

3 Transactions Involving Cash

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

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

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

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

vii) Payments and/or deposits containing counterfeit notes or forged instruments.

viii) Customers making large and frequent cash deposits but payments made from the account are mostly to individuals and firms not normally associated with their business.

ix) A large amount of cash is withdrawn and immediately credited into another account.

x) Unusual settlements of securities transactions in cash form.

4 Transactions Involving CMIs' Accounts

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

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

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) Accounts operated in the name of an offshore company with structured movement of funds and assets.

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

5 Transactions Involving Transfers Abroad

i) Large and regular injection of funds 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) other criminal conduct.

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

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

6 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 CMI and who have no identifiable close relationship with the customer.

ii) Transfer of money and assets to a third party without indication of the beneficiary.

iii) Payment instructions with inaccurate and/or incomplete information concerning the payee.

iv) Use of pseudonyms or numbered accounts for effecting trading and/or investment transactions.

v) Holding in trust of shares in an unlisted company whose activities cannot be ascertained by the CMI.

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.

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

7 Other Types of Transactions

i) Purchase or sale of large amounts of futures contracts on precious metals by an interim customer.

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

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

iv) Frequent changes to the address or authorised signatories.

v) A large amount of funds is received and immediately used as collateral for margining and/or financing facilities.

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 CMI	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
CMI 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 CMI shall provide particulars on joint account holders, if any.

Employment Details	
Employer's Name:	
Address:	
Telephone:	
Business Relationship(s) with Customer	
CMI 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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

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 CMI	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
CMI 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	

CMI 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 CMI 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 each of the following documents is attached:

- Account Opening Forms
- Customer Identification Documents

- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

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 CMI	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
CMI 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	
CMI 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 CMI 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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

[MAS Notice FAA-N06]

Introduction

1. These Guidelines are issued to provide guidance to the licensed financial advisers and exempt persons under Regulation 27(1) (d) of the Financial Advisers Regulations, other than those which only provide advice by means of issuing research analyses and reports concerning any investment product (hereinafter referred to as "financial advisers") on some of the requirements in FAA-N06 (the "Notice") issued on [date].

2. Financial advisers are reminded that the ultimate responsibility and accountability for ensuring the financial adviser's compliance with AML/CFT laws, regulations and guidelines rests with the financial adviser, its board of directors and senior management.

3. The expressions used in these Guidelines shall, except where expressly defined in these Guidelines or where the context otherwise requires, have the same respective meanings as in the Notice.

The structure of FAA-N06

4. The Notice sets out the obligations of a financial adviser to take measures to help mitigate the risk of the financial advisory market in Singapore being used for money laundering or terrorist financing.

5. Paragraph 4 of the Notice deals with CDD measures. This paragraph sets out the standard CDD measures to be applied, of which there are seven principal components:

   - Identification of the customer by obtaining certain information pertaining to the customer and, where the customer is not a natural person, certain other persons associated with that customer;

   - Verifying the identification information obtained;

   - Where the customer is not a natural person, identifying and verifying the identity of its representatives;

- Determining if there exists any beneficial owner (other than the customer) and applying the identification and verification procedures to those beneficial owners;

- Where business relations are to be established (as defined in the Notice), obtaining information as to the nature and purpose of the intended business relations;

- After business relations are established, conducting on-going monitoring of business relations; and

- After business relations are established, periodically reviewing the adequacy of customer information.

6. Paragraphs 5 and 6 of the Notice provide for the risk-based customisation of the CDD measures. Thus, paragraph 5 on simplified CDD allows a financial adviser to take lesser measures than those specified in paragraph 4 of the Notice provided that the conditions for simplified CDD are met. This will largely be a matter for individual financial advisers to assess, but the financial adviser must be able to justify its decision. Conversely, in situations where PEPs may be involved or in other situations where there is a higher risk of money laundering or terrorist financing, a financial adviser is required under paragraph 6 of the Notice to take enhanced CDD measures.

7. To cater to cross-referrals, paragraph 7 of the Notice allows a financial adviser to rely on another party, an intermediary, to perform certain elements of the CDD process, provided that certain conditions are met. This paragraph may typically be applied where a new customer is introduced to the financial adviser by an intermediary resulting in direct business relations between the financial adviser and the new customer. Thus, if the intermediary has already performed its own CDD on the new customer, then paragraph 7 allows the financial adviser to dispense with performing CDD on the new customer if the conditions are satisfied. Paragraph 7 is not intended to cover the situation where a financial adviser outsources the function of performing CDD measures to a third party.[14]

8. Finally, the Notice updates the previous requirements with respect to record keeping (paragraph 8), reporting of suspicious transactions (paragraph 9) and the institution of internal policies, procedures and controls for AML/CFT (paragraph 10).

[14] The Notice does not prohibit the outsourcing of the CDD function to a third party but where this occurs, the financial adviser must remain fully responsible and accountable for the conduct of CDD measures as if the function had remained within the financial adviser.

Key Concepts of the Notice

Money Laundering

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

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

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

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

    (c) Integration - The provision of apparent legitimacy to the benefits of 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.

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

Terrorist Financing

11. 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. Financial advisers should refer to the legal definitions of terrorism found in the law such as the Terrorism (Suppression of Financing) Act (Cap. 325), the United Nations (Anti-terrorism Measures) Regulations (Rg 1) and the Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002.

12. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. 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.

13. 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.

14. 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.

Paragraph 2.1 of the Notice – Definition of "Customer"

15. Paragraph 2.1 of the Notice defines "customer", in relation to a financial adviser, as the person in whose name an account is opened or intended to be opened, and includes, in the case where the financial adviser arranges a group life insurance policy, the owner of the master policy.

16. The definition circumscribes the scope of the Notice. Financial advisers should in general seek to perform CDD as widely as possible on persons that they deal with in the course of their provision of financial advisory services.

17. In the case below, the following approach below may be adopted:

Portfolio Managers

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

However, the Authority recognises that a financial adviser may not be able to perform CDD on the underlying investors. For instance, the portfolio manager may be reluctant, for legitimate commercial reasons, to reveal information on the underlying investors to the financial adviser. In such circumstances, the financial adviser should evaluate the risks arising for

each case and determine the appropriate CDD measures to take. The financial adviser may consider whether simplified CDD measures could be applied under paragraph 5 of the Notice, so that identification and verification of the underlying investors as beneficial owners are dispensed with.

Paragraphs 4.6, 4.8 and 4.9 of the Notice – Identification of Customers that are Not Natural Persons

18. Where the customer is not a natural person, paragraphs 4.6, 4.8 and 4.9 of the Notice require the financial adviser to further establish the identity of the directors, partners or persons having executive authority, of the customer respectively.

19. The financial adviser should assess and determine, with respect to each customer, the key persons whose details they consider necessary to verify.

20. For the purposes of paragraph 18 to 19 above, the financial adviser should consider whether persons, either singly or jointly with another, are able to give instructions concerning the use or transfer of funds or assets belonging to the customer in question.

Paragraphs 4.10 and 4.11 of the Notice - Verification of Identity

21. The requirements on verification of identity are intended to ensure that identity information provided by the customer is authentic.

22. Where the person whose identity is to be verified is a natural person, the financial adviser should ask for some form of identification that contains a recent photograph of that person.

23. The financial adviser should retain copies of all documentation used for verification of identity. Only in exceptional circumstances where the financial adviser is unable to retain a copy of documentation used in verifying the customer's identity, the financial adviser should record the following:

    (a) the information that the original documentation had served to verify;

    (b) the title and description of the original documentation produced to the financial adviser's officer for verification, including any particular or unique features or condition of that documentation (whether it is worn out, or damaged etc);

(c) the reasons why a copy of that documentation could not be made; and

(d) the name of the officer who carried out the verification, a statement by that officer certifying that he or she has duly verified the information against the documentation, and the date the verification took place.

Paragraphs 4.16 to 4.19 of the Notice - Identification and Verification of Identity of Beneficial Owners

24. Financial advisers are under a duty to take steps to determine if there exists, other than the person *ex facie* dealing with the financial adviser as a customer, any other beneficial owner in relation to the customer.

25. Generally, the financial adviser should assess and determine what measures would be appropriate to determine the beneficial owners, if any. The financial adviser should be able to justify the reasonableness of the measures taken, having regard to the circumstances of each case.

26. Where the customer is not a natural person, the financial adviser should take steps such as:

(a) Finding out about the ownership and structure of the company; and

(b) Identifying the natural persons who have a controlling interest in the customer or who comprise the mind and management of the customer.

27. The financial adviser may also consider obtaining an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner.

28. Paragraph 17 of these Guidelines makes reference to the case where the customer is a portfolio manager. In that situation, as well as other instances where the customer has a *bona fide* and legitimate interest or duty not to disclose to the financial adviser the identity or particulars of beneficial owners who are known to exist, the financial adviser may consider the application of simplified CDD set out in paragraph 5 of the Notice.

29. Paragraph 4.18 of the Notice states that financial advisers are not required to inquire if there exists any beneficial owner beyond the entities specified in sub-paragraphs (a) to (f).

30. The Authority recognises that it would be unnecessary to attempt to determine if beneficial owners exist behind these entities, since adequate information would already be available. For example, in the case of publicly listed companies, the shareholders (who would be the beneficial owners) would be changing relatively frequently and there would already be disclosure obligations imposed on substantial shareholders of such companies. In the case of financial institutions, there would have been adequate disclosure of the ownership and structure to the financial regulator.

31. While the entities listed would also typically be entities for which a financial adviser may consider applying simplified CDD in accordance with paragraph 5 of the Notice, it is not the intent that the financial adviser should thereby deem these entities to be automatically eligible for simplified CDD measures. The financial advisers must comply with the requirements of paragraph 5 of the Notice before applying simplified CDD measures.[15]

Reliability and Authenticity of Information and Documentation

32. Where the financial adviser obtains information or documents through the customer or a third party, the financial adviser should ensure that there is satisfactory evidence to show that the information or documents have been endorsed or otherwise authenticated by the relevant authority or official registry. Such information or documents should be as current as possible at the time they are provided to the financial adviser.

Paragraphs 4.26 and 4.27 of the Notice - Non Face-to-Face Verification

33. Paragraphs 4.26 to 4.27 of the Notice address the situation where business relations are established or financial services are provided without face-to-face contact. Measures for managing the risks should include specific and effective procedures for CDD that apply to non face-to-face customers. In particular, a financial adviser should take appropriate measures to address risks arising from establishing business relations and undertaking transactions through instructions conveyed by customers over the internet, the post or the telephone.

[15] Financial advisers should further note that where there is actual cause for suspecting money laundering or terrorist financing, the appropriate measures will be required – see paragraph 4.3(c) of the Notice.

34. As a guide, financial advisers should take one or more of the following measures to mitigate the heightened risk associated with not being able to conduct an interview face-to-face:

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

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

(c) subject to the customer's consent, telephone confirmation of the customer's employment status with the customer's employer's personnel 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;

(e) certification of identification documents by lawyers or notary publics presented by the customer;

(f) requiring the customer to make an initial deposit using a cheque drawn on the customer's personal account with a bank in Singapore; and

(g) any other reliable verification checks adopted by the financial adviser for non-face- to-face provision of financial advisory services.

Paragraphs 4.30 and 4.31 of the Notice - Deferring the completion of CDD measures: Time limits for completion

35. Paragraph 4.30 of the Notice allows financial advisers to establish business relations before completing the CDD measures if it is essential for the financial adviser not to interrupt the normal conduct of business and if the risks can be effectively managed.

36. An example where it may be essential not to interrupt the normal course of business would be with respect to investment transactions, where market conditions are such that the financial adviser has to execute transactions for the customer very rapidly.

37. An example where the financial adviser may have effectively managed the risks of money laundering and terrorist financing is if the financial adviser has adopted internal policies, procedures and controls that set appropriate limits on the financial services available to the customer before completion of CDD measures. These may include, for example, limiting the number,

type and value of transactions that might be effected in the interim period, and also the institution of a procedure that is more rigorous and intensive than usual for the monitoring of complex or unusually large transactions.

38. Paragraph 4.31 of the Notice requires that CDD measures be completed as soon as reasonably practicable, if a financial adviser allows business relations to be established without first completing CDD measures. Examples of reasonable timeframe are:

(a) the financial adviser completing CDD measures no later than 30 working days after the establishment of business relations;

(b) the financial adviser suspending business relations with the customer and refraining from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if CDD measures remain uncompleted 30 working days after the establishment of business relations; and

(c) the financial adviser terminating business relations with the customer if CDD measures remain uncompleted 120 working days after the establishment of business relations.

39. The financial adviser should factor these time limitations in their internal policies, procedures and controls.

Paragraph 4.33 of the Notice - Existing Customers

40. Paragraph 4.33 of the Notice concerns the application of CDD measures to the customers and accounts which the financial adviser already has as at (date) when the Notice comes into force. Financial advisers are required to review the adequacy of identification information on the basis of materiality and risk, and to perform CDD measures on existing customers as may be appropriate.

41. In relation to accounts for which CDD measures had not previously been applied in accordance with the Notice, the financial adviser should make an assessment with regards to materiality and risk and determine when would be an appropriate time for the performance of CDD measures, subject to the more specific requirements for PEPs specified in paragraph 6.2 of the Notice.

42. As a guide, a financial adviser should perform CDD, in relation to paragraph 41 above, when:

(a) there is a transaction that is significant, having regard to the manner in which the account is ordinarily operated;

(b) there is a substantial change in the financial adviser's own customer documentation standards;

(c) there is a material change in the way that business relations with the customer are conducted;

(d) the financial adviser becomes aware that it may lack adequate identification information on a customer; and

(e) the financial adviser 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 financial adviser.

43. Where a financial adviser becomes aware upon a review that it may lack sufficient identification information on a customer, it should proceed to perform CDD afresh.

Paragraph 5 of the Notice - Simplified Customer Due Diligence

44. Paragraph 5.1 of the Notice allows financial advisers to apply simplified CDD measures in cases where the financial adviser is satisfied that the risk of money laundering or terrorist financing is low.

45. The financial adviser should assess the risks of money laundering or terrorist financing, having regard to the circumstances of each case, before applying the lesser or reduced CDD measures. Where the financial adviser adopts such lesser or reduced CDD measures, such measures should be commensurate with the financial adviser's assessment of the risks.

46. Examples of when the financial adviser might adopt lesser or reduced CDD measures are:

(a) where reliable information on the customer is publicly available to the financial adviser;

(b) the financial adviser is dealing with another financial institution whose AML/CFT controls it is well familiar with by virtue of a previous course of dealings; or

(c) the customer is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent

with standards set by the FATF, or a listed company that is subject to regulatory disclosure requirements.

Paragraph 6.2 of the Notice - Identifying and dealing with PEPs

47. The definition of PEPs used in the Notice is drawn from the work of the FATF. The Authority recognises that the process of determining whether an individual is a PEP may not always be straightforward and a more precise definition would carry with it a greater risk of circumvention of the requirements under the Notice.

48. In the circumstances, the Authority would generally consider it acceptable for a financial adviser to refer to databases of PEPs either compiled commercially or by official authorities. However, in doing so, the Authority would expect the financial adviser to exercise a measure of discretion and sound judgment in determining for itself whether an individual should indeed be treated as a PEP, having regard to the risks and the circumstances.

Paragraphs 6.3 and 6.4 of the Notice - Other High Risk Categories

49. Paragraph 6.3 of the Notice requires enhanced CDD measures to be applied to other categories of customers apart from PEPs, which a financial adviser may consider to present a greater risk of money laundering or terrorist financing. Such high risk categories may include, for example, non-resident customers, private banking customers, body corporates set up as personal asset holding vehicles, or companies that have nominee shareholders or that issue shares in bearer form.

50. Financial advisers are also required by paragraph 6.4 of the Notice to give particular attention to business relations and transactions with persons from or in countries that have inadequate AML/CFT measures. For this purpose, financial advisers may take a range of steps, including the adoption of measures similar to those for PEPs and other high risk categories.

51. While the Authority may from time to time circulate names of countries and jurisdictions with inadequate AML/CFT regimes (which can then be used as a reference guide), financial advisers are also encouraged to refer, where practicable, to other sources of information to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.

Paragraph 7 of the Notice - Reliance on Intermediaries

52. Where a financial adviser wishes to rely on an intermediary to perform elements of the CDD measures, paragraph 7.1(a) of the Notice requires the financial adviser to be satisfied that the 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 the Notice or the equivalent measures.

53. The financial adviser may take a variety of measures, including but not limited to the following in determining whether the intermediary satisfies the requirements in paragraph 7.1(a) :

(a) referring to any publicly available reports or material on the quality of AML/CFT supervision in the jurisdiction where that intermediary operates (such as mutual evaluation reports of the FATF and its associated bodies, or assessment reports made under the Financial Sector Assessment Programme of the International Monetary Fund and the World Bank);

(b) referring to any publicly available reports or material on the quality of that intermediary's compliance with applicable AML/CFT rules;

(c) obtaining professional advice as to the extent of AML/CFT obligations to which the intermediary is subject by the laws of the jurisdiction in which the intermediary operates; or

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

54. To the extent that the performance of CDD is undertaken by the intermediary rather than by the financial adviser, the financial adviser should be able to justify that the conditions of paragraph 7 of the Notice have been met. The financial adviser should take considerable care when deciding if an intermediary is one on whom it can safely rely on to perform the CDD measures.

Paragraph 9 of the Notice - Suspicious Transaction Reporting

55. Paragraph 9 of the Notice provides for the establishment of internal procedures for reporting suspicious transactions.

56. Financial advisers are required to have adequate processes and systems for identifying and detecting suspicious transactions. The Authority also

expects the financial adviser to put in place effective and efficient procedures for reporting suspicious transactions.

57. The financial adviser should ensure that the internal process for evaluating whether a matter should be referred to STRO via an STR be completed within 7 working days of the case being referred by the relevant staff, unless the circumstances are most extraordinary.

58. Examples of suspicious transactions are set out in Appendix II to these Guidelines. These examples are not intended to be exhaustive and are only examples of the most basic ways money may be laundered. If any transactions similar to those in Appendix II, or any other suspicious transactions, are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds.

59. Financial advisers are required to keep watch for suspicious transactions in the course of conducting screening against lists of terrorist suspects as may be required by law or circulated by any relevant authority. The financial adviser should consider filing an STR even though there is no positive match against any name if the surrounding circumstances raise sufficient suspicions.

60. Subject to any written law or any directions given by STRO or the Authority, financial advisers should as far as possible follow the reporting formats specified in Appendices III to V to these Guidelines. 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, financial advisers should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct. A copy of the STR should also be sent to the Authority.

61. Every financial adviser should maintain a complete file of all transactions that have been brought to the attention of its AML/CFT compliance officer or unit, including transactions that are not reported to STRO.

Paragraphs 10.8 and 10.9 of the Notice - Compliance

62. The responsibilities of the AML/CFT compliance officer should include the following:

(a) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;

(b) advising and training senior management and staff on development and implementing internal policies, procedures and controls on AML/CFT;

(c) carrying out, or overseeing the carrying out of, on-going monitoring of business relations and sample reviewing of accounts for compliance with the Notice and these Guidelines; and

(d) promoting compliance with the Notice and these Guidelines, including in particular observance of the underlying principles on AML/CFT in the Notice and taking overall charge of all AML/CFT matters within the organisation.

Paragraph 10.12 of the Notice - Conducting Training

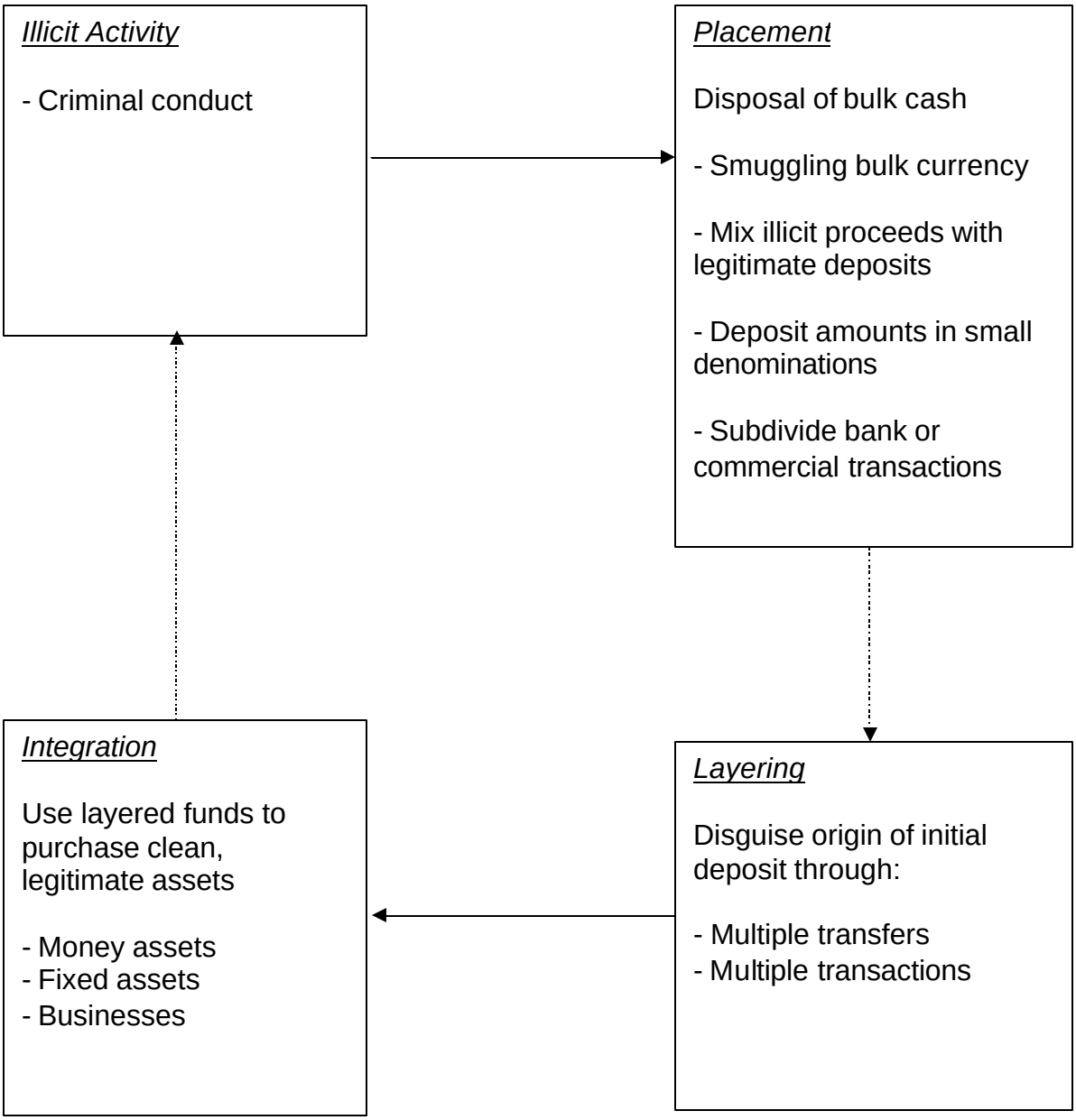
63. As stated in paragraph 10.12 of the Notice, it is the responsibility of financial advisers to provide appropriate training on AML/CFT measures for its staff. To help ensure the effectiveness of training, financial advisers should monitor attendance at such training and take the appropriate follow-up action in relation to staff who absent themselves without reasonable cause.

64. Apart from the initial training, financial advisers should also provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training should be held at least once a year.

……

APPENDIX I

PROCESS OF MONEY LAUNDERING



APPENDIX II

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 a suspicious 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 financial adviser in the course of the business relationship. Financial advisers should pay attention to customers who provide minimal, false or misleading information or, when applying to open an account, provide information that is difficult or expensive for the financial adviser to verify.

2 Transactions Which Do Not Make Economic Sense

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

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

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

3 Transactions Involving Large Amounts of Cash

i) Transactions where the customer makes a single payment exceeding $20,000 in cash.

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

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

4 Transactions Involving Transfers Abroad

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

5 Transactions Involving Unidentified Parties

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

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

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

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

6 Other Types of Transactions

i) Frequent changes to the address or authorised signatories.

ii) The use of an address that is not the customer's permanent address.

iii) A customer may exercise cancellation rights or cooling off rights on life policies or unit trusts where the sum invested must be repaid (subject to

any shortfall deduction where applicable). As this could offer a route for laundering money, financial advisers should therefore be alert to any unusual exercise of cancellation/cooling off rights by any customer. In the event that any unusual exercise of these rights become apparent, the transaction should be treated as suspicious and reported through the usual channels.

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 Financial Adviser	
Name:	
Address:	
Telephone:	
Fax:	
E-mail:	
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 financial adviser shall provide particulars on joint account holders, if any.

Employment Details	
Employer's Name:	
Address:	
Telephone:	
Business Relationship(s) with Customer	
Customer A/c No.:	
Type of A/c:	
Date A/c Opened:	
Market Value of Investments	
As At Date:	
Other Business Relationships:	

Suspicious Transaction(s)		
Amount	**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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

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 Financial Adviser	
Name:	
Address:	
Telephone:	
Fax:	
E-mail:	
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	
Customer A/c No.:	
Type of A/c.:	
Date A/c Opened:	
Market Value of Investments	
As At Date:	
Other Business Relationships:	

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

[#] The reporting officer of the financial adviser shall provide data on other authorised signatories, if any.

Suspicious Transaction(s)		
Amount	**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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

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 Financial Adviser	
Name:	
Address:	
Telephone:	
Fax:	
E-mail:	
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	
Customer A/c No.:	
Type of A/c.:	
Date A/c Opened:	
Market Value of Investments	
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 financial adviser shall provide data on other authorised signatories, if any.

Suspicious Transaction(s)		
Amount	**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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

[MAS Notice SFA13-N01]

Introduction

1. These Guidelines are issued to provide guidance to the trustees for collective investment schemes approved under the Securities and Futures Act (Cap 289) (hereinafter "approved trustees") on some of the requirements in SFA13-N01 (the "Notice") issued on [date].

2. Trustees are reminded that the ultimate responsibility and accountability for ensuring the bank's compliance with AML/CFT laws, regulations and guidelines rests with the bank, its board of directors and senior management.

3. The expressions used in these Guidelines shall, except where expressly defined in these Guidelines or where the context otherwise requires, have the same respective meanings as in the Notice.

The structure of MAS Notice SFA13-N01

4. The Notice sets out the legally binding obligations of an approved trustee to take measures to help mitigate the risk of Singapore's collective investment scheme regime from being used for money laundering or terrorist financing.

5. Paragraph 4 of the Notice deals with CDD measures. This paragraph sets out the standard CDD measures to be applied, of which there are four principal components:

   - Identification of the customer by obtaining certain information pertaining to the customer and, where the customer is not a natural person, certain other persons associated with that customer;

   - Verifying the identification information obtained;

   - Where the customer is not a natural person, identifying and verifying the identity of its representatives;

   - Where money laundering and/or the financing of terrorism are suspected, ascertaining the nature and clientele of the collective

investment scheme the customer is offering and for which the approved trustee is acting as trustee.

6. Paragraphs 5 and 6 of the Notice provide for the risk-based customisation of the CDD measures. Thus, paragraph 5 on simplified CDD allows an approved trustee to take lesser measures than those specified in paragraph 4 provided that the conditions for simplified CDD are met. This will largely be a matter for individual approved trustees to assess, but the approved trustee must be able to justify its decision. Conversely, in situations where PEPs may be involved or in other situations where there is a higher risk of money laundering or the financing of terrorism, an approved trustee is required under paragraph 6 to take enhanced CDD measures.

7. To cater for cross-referrals, paragraph 7 of the Notice allows an approved trustee to rely on another party, an intermediary, to perform certain elements of the CDD process, provided that certain conditions are met. This paragraph may typically be applied where a new customer is introduced to the approved trustee by an intermediary resulting in direct business relations between the approved trustee and the new customer. Thus, if the intermediary has already performed its own CDD on the new customer, then paragraph 7 allows the approved trustee to dispense with performing CDD on the new customer if the conditions are satisfied. Paragraph 7 is not intended to cover the situation where an approved trustee outsources the function of performing CDD measures to a third party.[16]

8. Finally, the Notice contains updated versions of the previous requirements with respect to record keeping (paragraph 8), reporting of suspicious transactions (paragraph 9) and the institution of internal policies, procedures and controls for AML/CFT (paragraph 10).

Key Concepts of the Notice

Money Laundering

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

[16] The Notice does not prohibit the outsourcing of the CDD function to a third party but where this occurs, the approved trustee must remain fully responsible and accountable for the conduct of CDD measures as if the function had remained within the approved trustee.

10. Generally, the process of money laundering comprises three stages, during which there may be numerous transactions that could alert an approved trustee to the money laundering activity:

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

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

    (c) Integration - The provision of apparent legitimacy to the benefits of 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.

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

Terrorist Financing

11. 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. Approved trustees should refer to the legal definitions of terrorism found in the law such as the Terrorism (Suppression of Financing) Act (Cap 325), the United Nations (Anti-terrorism Measures) Regulations (Rg 1) and the Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002.

12. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. 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.

13. 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.

14. 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.

Paragarph 2.1 of the Notice – Definition of "Customer"

15. Paragraph 2.1 of the Notice defines "customer", in relation to an approved trustee, as the fund manager or other person with whom the approved trustee deals with in the course of its operations as an approved trustee.

16. The definition circumscribes the scope of the Notice. Approved trustees should in general seek to perform CDD as widely as possible on persons whom they deal with in the course of their operations as approved trustees.

Paragraphs 4.5, 4.7 and 4.8 of the Notice – Identification of Customers that are not Natural Persons

17. Where the customer is not a natural person, paragraphs 4.5, 4.7 and 4.8 of the Notice require the approved trustee to further establish the identity of the customer's directors, partners or persons having executive authority, of the customer respectively.

18. The approved trustee should assess and determine, with respect to each customer, the key persons whose details they consider necessary to verify.

19. For the purposes of para 18 above, the approved trustee should consider whether persons, either singly or jointly with another, are able to give instructions concerning the use or transfer of funds or assets belonging to the customer in question.

Paragraphs 4.10 and 4.11 of the Notice – Verification of Identity

20. The requirements on verification of identity are intended to ensure that identity information provided by the customer is authentic.

21. Where the person whose identity is to be verified is a natural person, approved trustees should ask for some form of identification that contains a recent photograph of that person,

22. The approved trustee should retain copies of all documentation used for verification of identity. Only in exceptional circumstances where the approved trustee is unable to retain a copy of documentation used in verifying the customer's identity, the approved trustee should record the following:

(a) the information, that the original documentation had served to verify;

(b) the title and description of the original documentation produced to the approved trustee's officer for verification, including any particular or unique features or condition of that documentation (whether it is worn out, or damaged etc);

(c) the reasons why a copy of that documentation could not be made;

(d) the name of the approved trustee's officer who carried out the verification, a statement by that officer certifying that he or she has duly verified the information against the documentation, and the date the verification took place.

Reliability and Authenticity of Information and Documentation

23. Where the approved trustee obtains information or documents through the customer or a third party, the approved trustee should ensure that there is satisfactory evidence to show that the information or documents have been provided, endorsed or otherwise authenticated by the relevant authority or official registry. Such information or documents should be as current as possible at the time they are provided to the approved trustee.

Paragraphs 4.23 and 4.24 of the Notice – Non Face-to-Face Contact

24. Face-to-face contact between an approved trustee and its customer should be a norm in establishing the relationship.

Paragraph 4.286 of the Notice – Existing Customers

25. Paragraph 4.28 of the Notice concerns the application of CDD measures to the customers and accounts which the approved trustee already has as at (date) when the Notice comes into force. Approved trustees are

required to review the adequacy of identification information on the basis of materiality and risk, and to perform CDD measures on existing customers as may be appropriate.

26. In relation to business relationships for which CDD measures had not previously been applied in accordance with the Notice, the approved trustee should make an assessment with regard to materiality and risk and to determine when would be an appropriate time for the performance of CDD measures, subject only to the more specific requirements for PEPs specified in paragraph 6.2 of the Notice.

27. As a guide, an approved trustee should perform CDD in relation to paragraph 26 above when:

(a) there is a transaction that is significant, having regard to the manner in which the business relationship is ordinarily conducted;

(b) there is a substantial change in the approved trustee's own customer documentation standards;

(c) there is a material change in the way that business relations with the customer are conducted;

(d) the approved trustee becomes aware that it may lack adequate identification information on a customer; and

(e) the approved trustee 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 approved trustee.

28. Where an approved trustee becomes aware upon a review that it may lack sufficient identification information on a customer, it should proceed to perform CDD afresh.

Paragraph 5 of the Notice – Simplified Customer Due Diligence

29. Paragraph 5.1 of the Notice allows approved trustees to apply simplified CDD measures in cases where the approved trustee is satisfied that the risk of money laundering or terrorist financing is low.

30. Approved trustees should assess the risks of money laundering or terrorist financing, having regard to the circumstances of each case, before applying the lesser or reduced CDD measures. Where the approved trustee adopts such lesser of reduced CDD measures, such measures

should be commensurate with the approved trustee's assessment of the risks.

31. An example of a customer for which simplified CDD could apply would be a financial institution subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

.

Paragraph 6.2 of the Notice – Identifying and dealing with PEPs

32. The definition of PEPs used in the Notice is drawn from the work of the FATF. The Authority recognised that the process of determining whether an individual is a PEP may not always be straightforward and a more precise definition would carry with it a greater risk of circumvention of the requirements under the Notice.

33. In the circumstances, the Authority would generally consider it acceptable for an approved trustee to refer to databases of PEPs either compiled commercially or by official authorities. However, in doing so, the Authority would expect the approved trustee to exercise a measure of discretion and sound judgment in determining for itself whether an individual should indeed be treated as a PEP, having regard to the risks and the circumstances. .

Paragraphs 6.3 and 6.4 of the Notice -- Other High Risk Categories

34. Paragraph 6.3 of the Notice requires enhanced CDD measures to be applied to other categories of customers apart from PEPs, which an approved trustee may consider to present a greater risk of money laundering or terrorist financing. Such high risk categories may include, for example, fund managers who are not subject to and supervised for compliance with AML/CFT requirements.

35. Approved trustees are also required by paragraph 6.4 of the Notice to give particular attention to business relations and transactions with persons from or in countries that have inadequate AML/CFT measures. For this purpose, approved trustees may take a range of steps, including the adoption of measures similar to those for PEPs and other high risk categories.

36. While the Authority may from time to time circulate names of countries and jurisdictions with inadequate AML/CFT regimes (which can then be used as a reference guide), approved trustees are also encouraged to refer, where practicable, to other sources of information to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.

Paragraph 7 of the Notice – Reliance on Intermediaries

37. Where an approved trustee wishes to rely on an intermediary to perform elements of the CDD measures on its behalf, paragraph 7.1(a) of the Notice requires the approved trustee to be satisfied that the 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 the Notice or the equivalent foreign measures.

38. The approved trustee may take a variety of measures, including but not limited to the following, in determining whether the intermediary satisfies the requirements in paragraph 7.1(a):

(a) referring to any publicly available reports or material on the quality of AML/CFT supervision in the jurisdiction where that intermediary operates (such as mutual evaluation reports of the FATF and its associated bodies, or assessment reports made under the Financial Sector Assessment Programme of the International Monetary Fund and the World Bank);

(b) referring to any publicly available reports or material on the quality of that intermediary's compliance with applicable AML/CFT rules;

(c) obtaining professional advice as to the extent of AML/CFT obligations to which the intermediary is subject by the laws of the jurisdiction in which the regulated entity operates; or

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

39. To the extent that the performance of CDD is undertaken by the intermediary rather than by the approved trustee, the approved trustee should be able to justify that the conditions of paragraph 7 of the Notice have been met. The approved trustee should take considerable care when deciding if the intermediary is one on whom it can safely rely on to perform the CDD measures.

Paragraph 9 of the Notice – Suspicious Transaction Reporting

40. Paragraph 9 of the Notice provide for the establishment of internal procedures for reporting suspicious transactions.

41. Approved trustees are required to have adequate processes and systems for identifying and detecting suspicious transactions. The Authority also

expects the approved trustee to put in place effective and efficient procedures for reporting suspicious transactions.

42. The approved trustee should ensure that the internal process for evaluating whether a matter should be referred to the STRO via an "STR" should be completed within 7 working days of the case being referred by the relevant approved trustee's officer, unless the circumstances are most extraordinary.

43. Examples of suspicious transactions are asset out in Appendix II to these Guidelines. These examples are not intended to be exhaustive and are only examples of the most basic ways in which money may be laundered. If any transactions similar to those in Appendix II are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds.

44. Approved trustees are required to keep watch for suspicious transactions in the course of conducting screening against such lists of terrorist suspects as may be required by law or circulated by any relevant authority. The approved trustee should consider filing an STR even though there is no positive match against any name if the surrounding circumstances raise sufficient suspicions.

45. Subject to any written law or any directions given by STRO or the Authority, approved trustees should as far as possible follow the reporting formats specified in Appendices III to V to these Guidelines. 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, approved trustees should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct. A copy of the STR should also be sent to the Authority.

46. Every approved trustee should maintain a complete file of all transactions that have been brought to the attention of its AML/CFT compliance officer or unit, including transactions that are not reported to STRO.

Paragraph 10.8 and 10.9 of the Notice – Compliance

47. The responsibilities of the AML/CFT compliance officer should include the following:

(a) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;

(b) advising and training senior management and staff on development and implementing internal policies, procedures and controls on AML/CFT as well as training;

(c) carrying out or overseeing the carrying out of on-going monitoring of business relations and sample reviewing of accounts for compliance with the Notice and these Guidelines; and

(d) promoting compliance with the Notice and these Guidelines, including in particular observance of the underlying principles on AML/CFT in the Notice and taking overall charge of all AML/CFT matters within the organisation.

Paragarph 10.12 of the Notice – Training

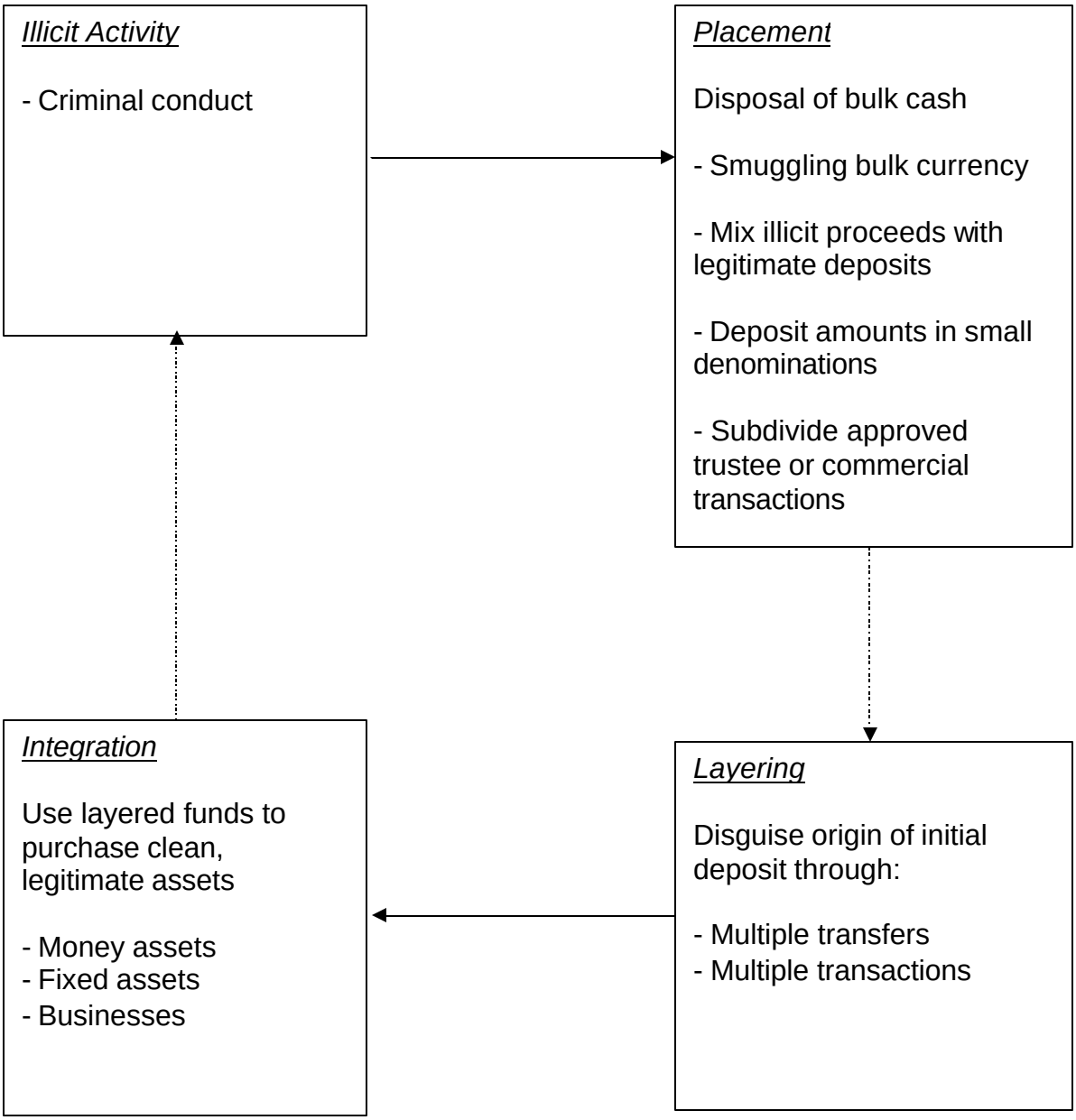
48. As stated in paragraph 10.12 of the Notice, it is the responsibility of approved trustees to provide appropriate training on AML/CFT measures for its staff. To help ensure the effectiveness of training, approved trustees should monitor attendance at such training and take the appropriate follow-up action in relation to staff who absent themselves without reasonable cause.

49. Apart from the initial training, approved trustees should also provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training should be held at least once a year.

……

APPENDIX I

PROCESS OF MONEY LAUNDERING



APPENDIX II

EXAMPLES OF SUSPICIOUS TRANSACTIONS

1 General Comments

The situations given below are intended mainly as a means of highlighting some basic ways in which money may be laundered. They are by no means definitive, and require constant updating and adaptation to changing circumstances and new methods of laundering money. They are intended solely as an aid, and must not be applied as a routine instrument in place of common sense.

i) Transactions undertaken by fund manager which do not make economic sense, for example, buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

ii) Subscriptions and/or redemptions by fund managers for a large amount of units in collective investment schemes.

iii) Subscriptions and/or redemptions of an unusually large volume by an end investor.

iv) 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.

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

CORPORATIONS

Reporting Approved Trustee	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
Approved Trustee 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	

Approved Trustee Ref 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 approved trustee 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 each of the following documents is attached:

- Account Opening Forms

* Delete whichever is inappropriate

- 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

NATURAL PERSONS

Reporting Approved Trustee	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
Approved Trustee 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 approved trustee shall provide particulars on joint account holders, if any.

Employment Details	
Employe r's Name:	
Address:	
Telephone:	
Business Relationship(s) with Customer	
Approved Trustee Ref 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 each of the following documents is attached:

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

* Delete whichever is inappropriate

(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 Approved Trustee	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
Approved Trustee 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	
Approved Trustee Ref 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 approved trustee 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 each of the following documents is attached:

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

(Signature of Reporting Officer)

Date:

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

[MAS Notice TCA-N03]

Introduction

1. These Guidelines are issued to provide guidance to the trust companies on some of the requirements in MAS Notice TCA-N03 (the "Notice") issued on [date].

2. Trust companies are reminded that the ultimate responsibility and accountability for ensuring the trust company's compliance with AML/CFT laws, regulations and guidelines rests with the trust company, its board of directors and senior management.

3. The expressions used in these Guidelines shall, except where expressly defined in these Guidelines or where the context otherwise requires, have the same respective meanings as in the Notice.

The structure of MAS Notice TCA-N03

4. The Notice sets out the obligations of a trust company to take measures to help mitigate the risk of the trust services industry of Singapore being used for money laundering or terrorist financing.

5. Paragraph 4 of the Notice deals with CDD measures. This paragraph sets out the standard CDD measures to be applied, of which there are seven principal components:

   - Identification of the trust relevant party by obtaining certain information pertaining to the trust relevant party and, where the trust relevant party is not a natural person, certain other persons associated with that trust relevant party;

   - Verifying the identification information obtained;

   - Where the trust relevant party is not a natural person, identifying and verifying the identity of its representatives;

   - Determining if there exists any effective controller and applying the identification and verification procedures to those effective controllers;

- Where business contacts are to be established (as defined in the Notice), obtaining information as to the nature and purpose of the intended business contacts;

- After business contacts are established, conducting on-going monitoring of business contacts; and

- After business contacts are established, periodically reviewing the adequacy of trust relevant party information.

6. Paragraphs 5 and 6 of the Notice provide for the risk-based customisation of the CDD measures. Thus, paragraph 5 on simplified CDD allows a trust company to take lesser measures than those specified in paragraph 4 of the Notice provided that the conditions for simplified CDD are met. This will largely be a matter for individual trust companies to assess, but the trust company must be able to justify its decision. Conversely, in situations where PEPs may be involved or in other situations where there is a higher risk of money laundering or terrorist financing, a trust company is required under paragraph 6 of the Notice to take enhanced CDD measures.

7. To cater to cross-referrals, paragraph 7 of the Notice allows a trust company to rely on another party, an intermediary, to perform certain elements of the CDD process, provided that certain conditions are met. This paragraph may typically be applied where a new trust relevant party is introduced to the trust company by an intermediary resulting in direct business contacts between the trust company and the new trust relevant party. Thus, if the intermediary has already performed its own CDD on the new trust relevant party, then paragraph 7 allows the trust company to dispense with performing CDD on the new trust relevant party if the conditions are satisfied. Paragraph 7 is not intended to cover the situation where a trust company outsources the function of performing CDD measures to a third party.[17]

8. The Notice also contains the requirements with respect to record keeping (paragraph 8), reporting of suspicious transactions (paragraph 9) and the institution of internal policies, procedures and controls for AML/CFT (paragraph 10).

Key Concepts of the Notice

Money Laundering

[17] The Notice does not prohibit the outsourcing of the CDD function to a third party but where this occurs, the trust company must remain fully responsible and accountable for the conduct of CDD measures as if the function had remained within the trust company.

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

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

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

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

(c) Integration - The provision of apparent legitimacy to the benefits of 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.

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

Terrorist Financing

11. 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. Trust companies should refer to the legal definitions of terrorism found in the law such as the Terrorism (Suppression of Financing) Act (Cap. 325), the United Nations (Anti-terrorism Measures) Regulations (Rg 1) and the Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002.

12. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. 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.

13. 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.

14. 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.

Paragraphs 4.6, 4.8 and 4.9 of the Notice – Identification of Trust Relevant Parties that are Not Natural Persons

15. Where the trust relevant party is not a natural person, paragraphs 4.6, 4.8 and 4.9 of the Notice require the trust company to further establish the identity of the directors, partners or persons having executive authority, of the trust relevant party respectively.

16. The trust company should assess and determine, with respect to each trust relevant party, the key persons whose details they consider necessary to verify.

17. For the purposes of paragraph 16 above, the trust company should consider whether persons, either singly or jointly with another, are able to give instructions concerning the use of funds or assets of the trust.

Paragraphs 4.10 and 4.11 of the Notice - Verification of Identity

18. The requirements on verification of identity are intended to ensure that identity information provided by the trust relevant party is authentic.

19. Where the person whose identity is to be verified is a natural person, the trust company should ask for some form of identification that contains a recent photograph to that person.

20. The trust company should retain copies of all documentation used for verification of identity. Only in exceptional circumstances where the trust company is unable to retain a copy of documentation used in verifying the trust relevant party's identity, the trust company should record the following:

(a) the information that the original documentation had served to verify;

(b) the title and description of the original documentation produced to the trust company officer for verification, including any particular or unique features or condition of that documentation (whether it is worn out, or damaged etc);

(c) the reasons why a copy of that documentation could not be made; and

(d) the name of the trust company officer who carried out the verification, a statement by that officer certifying that he or she has duly verified the information against the documentation, and the date the verification took place.

Paragraphs 4.16 to 4.19 of the Notice - Identification and Verification of Identity of Effective Controllers

21. Trust companies are under a duty to take steps to determine if there exists, other than the person *ex facie* dealing with the trust company as a trust relevant party, any other effective controller in relation to the trust relevant party.

22. Generally, the trust company should assess and determine what measures would be appropriate to determine the effective controllers, if any. The trust company should be able to justify the reasonableness of the measures taken, having regard to the circumstances of each case.

23. Where the trust relevant party is not a natural person, the trust company should take steps such as:

(a) finding out about the ownership and structure of the company; and

(b) identifying the natural persons who have a controlling interest in the trust relevant party or who comprise the mind and management of the trust relevant party.

24. The trust company may also consider obtaining an undertaking or declaration from the trust relevant party on the identity of, and the information relating to, the effective controller.

25. In instances where the trust relevant party has a *bona fide* and legitimate interest or duty not to disclose to the trust company the identity or particulars of effective controllers who are known to exist, the trust company may consider the application of simplified CDD set out in paragraph 5 of the Notice.

26. Paragraph 4.18 of the Notice states that trust companies are not required to inquire if there exists any effective controller beyond the entities specified in sub-paragraphs (a) to (f).

27. The Authority recognises that it would be unnecessary to attempt to determine if effective controllers exist behind these entities, since adequate information would already be available. For example, in the case of publicly listed companies, the shareholders (who would be the effective controllers) would ordinarily be changing relatively frequently and there would already be disclosure obligations imposed on substantial shareholders of such companies. In the case of financial institutions, there would have been adequate disclosure of the ownership and control structure to the financial regulator.

28. While the entities listed would also typically be entities for which a trust company may consider applying simplified CDD measures in accordance with paragraph 5 of the Notice, it is not the intent that the trust company should thereby deem these entities to be automatically eligible for simplified CDD measures. The trust company must comply with the requirements of paragraph 5 of the Notice before applying simplified CDD measures.[18]

Reliability and Authenticity of Information and Documentation

29. Where the trust company obtains information or documents through the trust relevant party or a third party, the trust company should ensure that there is satisfactory evidence to show that the information or documents have been endorsed or otherwise authenticated by the relevant authority or official registry. Such information or documents should be as current as possible at the time they are provided to the trust company.

Paragraphs 4.27 and 4.28 of the Notice - Non Face-to-Face Verification

30. Paragraphs 4.27 and 4.28 of the Notice address the situation where business contacts are established without face-to-face contact. Measures for managing the risks should include specific and effective procedures for CDD that apply to non face-to-face trust relevant parties. In particular, a trust company should take appropriate measures to address risks arising from establishing business contacts and undertaking transactions through instructions conveyed by trust relevant parties over the internet, the post or the telephone.

[18] Trust companies should further note that where there is actual cause for suspecting money laundering or terrorist financing, the appropriate measures will be required – see paragraph 4.3(b) of the Notice.

31. As a guide, trust companies should take one or more of the following measures to mitigate the heightened risk associated with not being able to conduct an interview face-to-face:

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

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

(c) subject to the trust relevant party's consent, telephone confirmation of the trust relevant party's employment status with the trust relevant party's employer's personnel department at a listed business number of the employer;

(d) confirmation of the trust relevant party's salary details by requiring the presentation of recent bank statements;

(e) certification of identification documents by lawyers or notary publics presented by the trust relevant party; and

(f) any other reliable verification checks adopted by the trust company for non-face-to-face business contacts.

Paragraph 4.30 of the Notice - Existing Trust Relevant Parties

32. Paragraph 4.30 of the Notice concerns the application of CDD measures to the trust relevant parties and business contacts which the trust company already has as at [date] when the Notice comes into force. Trust companies are required to review the adequacy of identification information on the basis of materiality and risk, and to perform CDD measures on existing trust relevant parties as may be appropriate.

33. In relation to business contacts for which CDD measures had not previously been applied in accordance with the Notice, the trust company should make an assessment with regard to materiality and risk and to determine when would be an appropriate time for the performance of CDD measures, subject to the more specific requirements for PEPs specified in paragraph 6.2 of the Notice.

34. As a guide, a trust company should perform CDD, in relation to paragraph 33 above, when:

(a) there is a transaction that is significant, having regard to the manner in which the account is ordinarily operated;

(b) there is a substantial change in the trust company's own documentation standards in relation to trust relevant parties;

(c) there is a material change in the way that business contacts with the trust relevant party are established and maintained;

(d) the trust company becomes aware that it may lack adequate identification information on a trust relevant party; and

(e) the trust company becomes aware that there may be a change in the ownership or constitution of the trust relevant party, or the person(s) authorised to act on behalf of the trust relevant party in its business contacts with the trust company.

35. Where a trust company becomes aware upon a review that it may lack sufficient identification information on a trust relevant party, it should proceed to perform CDD afresh.

Paragraph 5 of the Notice - Simplified Customer Due Diligence

36. Paragraph 5.1 of the Notice allows trust companies to apply simplified CDD measures in cases where the trust company is satisfied that the risk of money laundering or terrorist financing is low.

37. The trust company should assess the risks of money laundering or terrorist financing, having regard to the circumstances of each case, before applying the lesser or reduced CDD measures. Where the trust company adopts such lesser or reduced CDD measures, such measures should be commensurate with the trust company's assessment of the risks.

38. Examples of when the trust company might adopt lesser or reduced CDD measures are:

(a) where reliable information on the trust relevant party is publicly available to the trust company;

(b) the trust company is dealing with another trust company whose AML/CFT controls it is well familiar with by virtue of a previous course of dealings; or

(c) the trust relevant party is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by FATF, or a listed company that is subject to regulatory disclosure requirements.

Paragraph 6.2 - Identifying and Dealing with PEPs

39. The definition of PEPs used in the Notice is drawn from the work of the FATF. The Authority recognises that the process of determining whether an individual is a PEP may not always be straightforward and a more precise definition would carry with it a greater risk of circumvention of the requirements under the Notice.

40. In the circumstances, the Authority would generally consider it acceptable for a trust company to refer to databases of PEPs either compiled commercially or by official authorities. However, in doing so, the Authority would expect the trust company to exercise a measure of discretion and sound judgment in determining for itself whether an individual should indeed be treated as a PEP, having regard to the risks and the circumstances.

Paragraphs 6.3 and 6.4 of the Notice - Other High Risk Categories

41. Paragraph 6.3 of the Notice requires enhanced CDD measures to be applied to other categories of trust relevant parties apart from PEPs, which a trust company may consider to present a greater risk of money laundering or terrorist financing.

42. Trust companies are also required by paragraph 6.4 of the Notice to give particular attention to business contacts and transactions with persons from or in countries that have inadequate AML/CFT measures. For this purpose, trust companies may take a range of steps, including the adoption of measures similar to those for PEPs and other high risk categories.

43. While the Authority may from time to time circulate names of countries and jurisdictions with inadequate AML/CFT regimes (which can then be used as a reference guide), trust companies are also encouraged to refer, where practicable, to other sources of information to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.

Paragraph 7 of the Notice - Performance of Customer Due Diligence by Intermediaries

44. Where a trust company wishes to rely on an intermediary to perform elements of the CDD measures, paragraph 7.1(a) of the Notice requires the trust company to be satisfied that the 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 the Notice or the equivalent foreign measures.

45. The trust company may take a variety of measures, including but not limited to the following in determining whether the intermediary satisfies the requirements in paragraph 7.1(a):

(a) referring to any publicly available reports or material on the quality of AML/CFT supervision in the jurisdiction where that intermediary operates (such as mutual evaluation reports of the FATF and its associated bodies, or assessment reports made under the Financial Sector Assessment Programme of the International Monetary Fund and the World Bank);

(b) referring to any publicly available reports or material on the quality of that intermediary's compliance with applicable AML/CFT rules;

(c) obtaining professional advice as to the extent of AML/CFT obligations to which the intermediary is subject by the laws of the jurisdiction in which the intermediary operates; or

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

46. To the extent that the performance of CDD is undertaken by the intermediary rather than by the trust company, the trust company should be able to justify that the conditions of paragraph 7 of the Notice have been met. The trust company should take considerable care when deciding if an intermediary is one on whom it can safely rely on to perform the CDD measures.

Paragraph 9 of the Notice - Suspicious Transactions Reporting

47. Paragraph 9 of the Notice provide for the establishment of internal procedures for reporting suspicious transactions.

48. Trust companies are required to have adequate processes and systems for identifying and detecting suspicious transactions. The Authority also expects the trust company to put in place effective and efficient procedures for reporting suspicious transactions.

49. The trust company should ensure that the internal process for evaluating whether a matter should be referred to STRO via an STR be completed within 7 working days of the case being referred by the relevant trust company staff, unless the circumstances are most extraordinary.

50. Indicators of money laundering and suspicious transactions are set out in Appendix II to these Guidelines. These examples are not intended to be exhaustive and are only examples of the most basic indicators of money laundering and suspicious transactions. If any indicators or transactions similar to those in Appendix II are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds.

51. Trust companies are required to keep watch for suspicious transactions in the course of conducting screening against lists of terrorist suspects as may be required by law or circulated by any relevant authority. The trust company should consider filing an STR even though there is no positive match against any name if the surrounding circumstances raise sufficient suspicions.

52. Subject to any written law or any directions given by STRO or the Authority, trust companies should as far as possible follow the reporting formats specified in Appendices III to V to these Guidelines. 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, trust companies should give initial notification to STRO by telephone or email and follow up with such other means of reporting as STRO may direct. A copy of the STR should also be sent to the Authority.

53. Every trust company should maintain a complete file of all transactions that have been brought to the attention of its AML/CFT compliance officer or unit, including transactions that are not reported to STRO.

Paragraphs 10.8 to 10.9 of the Notice - Compliance

54. The responsibilities of the AML/CFT compliance officer should include the following:

(a) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;

(b) advising and training senior management and staff on development and implementing internal policies, procedures and controls on AML/CFT;

(c) carrying out, or overseeing the carrying out of, on-going monitoring of business contacts and sample reviewing of accounts for compliance with the Notice and these Guidelines; and

(d) promoting compliance with the Notice and these Guidelines, including in particular observance of the underlying principles on

AML/CFT in the Notice and taking overall charge of all AML/CFT matters within the organisation.

Paragraph 10.12 of the Notice - Training

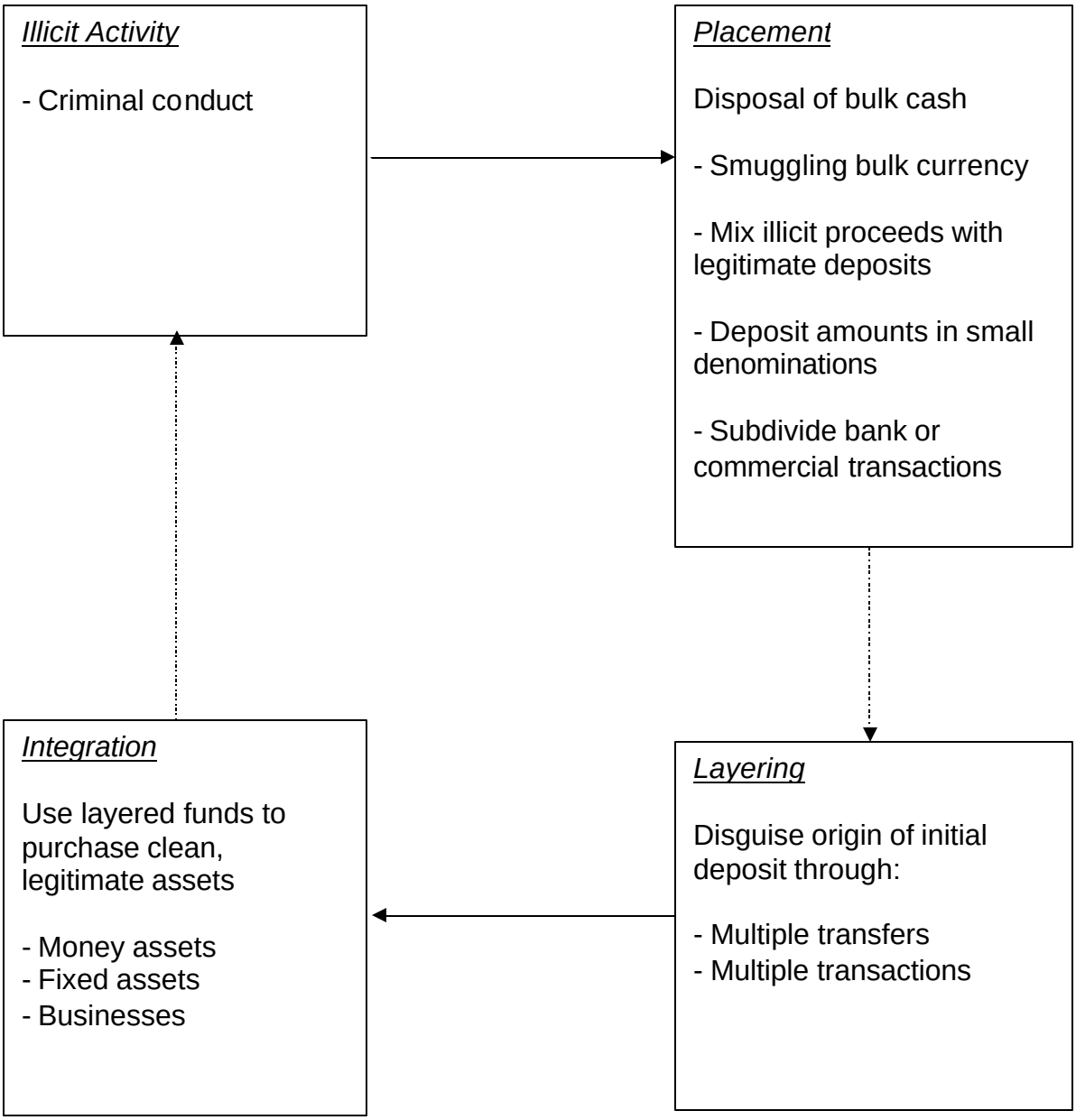
55. As stated in paragraph 10.12 of the Notice, it is the responsibility of trust companies to provide appropriate training on AML/CFT measures for its staff. To help ensure the effectiveness of training, trust companies should monitor attendance at such training and take the appropriate follow-up action in relation to staff who absent themselves without reasonable cause.

56. Apart from the initial training, trust companies should also provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training should be held at least once a year.

……

APPENDIX I

PROCESS OF MONEY LAUNDERING



APPENDIX II

INDICATORS OF MONEY LAUNDERING AND SUSPICIOUS TRANSACTIONS

1 General Comments

The list of situations given below is intended mainly as a means of highlighting the basic indicators of money laundering. 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 a suspicious 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 trust relevant party's declarations regarding the background of transactions relating to the trust account should be checked for plausibility. Not every explanation offered by the trust relevant party can be accepted without scrutiny.

It is justifiable to suspect any trust relevant party who is reluctant to provide normal information and documents required routinely by the trust company in the course of the business contact. Trust companies should pay attention to trust relevant parties who provide minimal, false or misleading information or information that is difficult or expensive for the trust company to verify.

2 Indicators

i) Trust relevant party evades attempts by the trust company to establish personal contact.

ii) Trust structure or related transactions indicate some illicit purpose or is inconsistent with the trust company's knowledge of the trust relevant party, its business and risk profile and where appropriate, the source of funds.

iii) Trust assets are withdrawn immediately after being settled into the trust account, unless there is a plausible reason for such immediate withdrawal.

iv) Previously inactive trust account is now used intensively, unless there is a plausible reason for such use.

v) Transactions relating to the trust account are conducted with countries or entities that are reported to be associated with terrorist activities or with persons that have been designated as terrorists.

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 Trust Company	
Name:	
Branch (where applicable):	
Address:	
Telephone:	
Fax:	
E-mail:	
Trust Company Reporting Officer	
Name:	
Designation:	
Report Reference:	
Contact Officer (if different from Reporting Officer):	
Designation:	
Trust Relevant Party's Particulars #	
Name:	
NRIC/Passport No.:	
Birth Date:	
Nationality:	
Address:	
Telephone:	
Occupation:	

Date when particulars were last updated (where available):	

In the case of a trust relevant party that comprises two or more persons acting jointly, the reporting officer of the trust company shall provide particulars on all of the persons as if each of them were individually trust relevant parties.

Employment Details	
Employer's Name:	
Address:	
Telephone:	
Business Contact(s) with Trust Relevant Party	

Suspicious Transaction(s)		
Amount	**Date**	**Description of Transaction**

Reason(s) for Suspicion:

Other Relevant Information (including information on any actions taken by the reporting entity in response to the transaction)**:**

A copy each of the following documents is attached:

- Trust Account Opening Forms
- Trust Relevant Party Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

APPENDIX IV

Reporting Format

(a) Reporting of Suspicious Money Laundering Transactions pursuant to Section 39, Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act

(b) Reporting of Suspicious Terrorist Financing Activities pursuant to Section 8, Terrorism (Suppression of Financing) Act

CORPORATIONS

Reporting Trust Company	
Name:	
Branch (where applicable):	
Address:	
Telephone:	
Fax:	
E-mail:	
Trust Company Reporting Officer	
Name:	
Designation:	
Report Reference:	
Contact Officer (if different from Reporting Officer):	
Designation:	
Trust Relevant Party's Particulars	
Name: Country of Registration:	
Registration Date:	
Registration No.:	
Address:	
Telephone:	
Name of CEO:	
Date when particulars were last updated (where available):	

Business Contact(s) with Trust Relevant Party

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

[#] The reporting officer of the trust company shall provide data on other authorised signatories, if any.

Suspicious Transaction(s)		
Amount	**Date**	**Description of Transaction**

Reason(s) for Suspicion:

Other Relevant Information (including information on any actions taken by the reporting entity in response to the transaction)**:**

A copy each of the following documents is attached:

- Trust Account Opening Forms
- Trust Relevant Party Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)
Date:

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 Trust Company	
Name:	
Branch (where applicable):	
Address:	
Telephone:	
Fax:	
E-mail:	
Trust Company Reporting Officer	
Name:	
Designation:	
Report Reference:	
Contact Officer: (if different from Reporting Officer)	
Designation:	
Trust Relevant Party'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 Contact(s) with Trust Relevant Party	

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 trust company shall provide data on other authorised signatories, if any.

Suspicious Transaction(s)		
Amount	**Date**	**Description of Transaction**

Reason(s) for Suspicion:

Other Relevant Information (Including information on any actions taken by the reporting entity in response to the transaction)**:**

A copy each of the following documents is attached:

- Trust Account Opening Forms
- Trust Relevant Party Identification Documents
- Relevant Documents Supporting the Suspicious Transactions

(Signature of Reporting Officer)

Date:

Monetary Authority of Singapore