

# GUIDELINES TO MAS NOTICE 626 ON PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

---

## Introduction

1. These Guidelines are issued to provide guidance to the banks on some of the requirements in MAS Notice 626 (“the Notice”).
2. Banks are reminded that the ultimate responsibility and accountability for ensuring the bank’s compliance with anti-money laundering and countering the financing of terrorism (“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 customer due diligence (“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 the natural persons appointed to act on the customer’s behalf;
  - Determining if there exists any beneficial owner and applying the identification and verification procedures to those beneficial owners;
  - Where business relations are to be established, obtaining information as to the nature and purpose of the intended business relations;
  - After business relations are established, conducting ongoing monitoring of business relations; and

- Reviewing periodically the adequacy of customer information after business relations are established.
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 politically exposed persons (“PEP”) 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.<sup>1</sup>
  8. The Notice then deals with two specific situations – the 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**

### *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.

---

<sup>1</sup> 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.

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 (G.N. No. S 515/2002).
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 for 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 (or in the case of a branch network, another branch of the company) in accordance with paragraph 7 of the Notice.

### **Paragraphs 4.5, 4.6 and 4.7 of the Notice – Identification of Customers that are Not Natural Persons**

19. Where the customer is not a natural person, paragraphs 4.5, 4.6 and 4.7 of the Notice require the bank to further identify the directors, partners or persons having executive authority, of the customer.
20. A bank should assess the risk of money laundering or terrorist financing, having regard to the circumstances of each case, in determining whether to verify the identity of any of the persons referred to in paragraphs 4.5, 4.6 and 4.7.
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 4.8 and 4.9 of the Notice - Verification of Identity**

22. The requirements on verification of identity are intended to ensure that the 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 photograph of that person.
24. The bank should retain copies of all documentation used to verify the identity of the customer. 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 4.14 to 4.18 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 the measures which 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. 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.
28. 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.
29. Paragraph 4.17 of the Notice states that banks are not required to inquire if there exists any beneficial owner in relation to the entities specified in sub-paragraphs (a) to (g).
30. The Authority recognises that it would be unnecessary to attempt to determine if beneficial owners exist in relation to the entities specified in sub-paragraphs (a) to (g), since adequate information would already be available. For example, in the case of publicly listed companies, the shareholders 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 supervised by the Authority, there would have been adequate disclosure of the ownership and structure to the Authority.
31. 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, the bank should not treat these entities as automatically eligible for simplified CDD measures. The bank must comply with the requirements of paragraph 5 of the Notice before applying simplified CDD measures.<sup>2</sup>

---

<sup>2</sup> 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 4.2(c) of the Notice.

## **Reliability of Information and Documentation**

32. Where the bank obtains information or documents from the customer or a third party, it should take reasonable steps to assure itself that such information or documents are reliable and, where appropriate, reasonably up to date at the time they are provided to the bank.
33. Where the customer is unable to produce original documents, the bank may consider accepting documents that are certified to be true copies by qualified persons, such as lawyers and accountants.

## **Paragraphs 4.25, 4.26 and 4.27 of the Notice – Non-Face-to-Face Verification**

34. Paragraphs 4.25, 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. 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 have face-to-face contact when establishing business relations:
  - (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 - Timing for Verification**

36. Paragraph 4.32 of the Notice allows banks to establish business relations before completing the verification of the identity of the customer and beneficial owner, 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 completing the verification of the identity of the customer and beneficial owner. 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 verification of the identity of the customer and the beneficial owner be completed as soon as reasonably practicable, if a bank allows business relations to be established without first completing such verification. Examples of reasonable timeframe are:
  - (a) the bank completing such verification 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 such verification remains uncompleted 30 working days after the establishment of business relations; and
  - (c) the bank terminating business relations with the customer if such verification remains 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 4.36 of the Notice - Existing Customers**

41. Paragraph 4.36 of the Notice concerns the application of CDD measures to the customers and accounts which the bank has as at 1 March 2007 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, taking into account 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 on the areas found deficient.

#### **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.

48. Paragraph 5.2 of the Notice makes clear the circumstances when simplified CDD measures are not permitted, namely, where the customers are from or in countries and jurisdictions known to have inadequate AML/CFT measures, or where the bank suspects that money laundering or terrorist financing is involved.

### **Paragraph 6.2 of the Notice - Identifying and Dealing with PEPs**

49. The definition of PEPs used in the Notice was originally 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.

50. 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**

51. 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. In assessing the risk of money laundering or terrorist financing, the bank may take into account factors such as the type of customer, the type of product or service that the customer purchases, and the geographical area of operation of the customer's business.

52. 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.

53. 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 - Performance of CDD Measures by Intermediaries**

54. 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 of various matters, including that the intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with the standards set by the FATF, and that the intermediary has measures in place to comply with the requirements.
55. 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) of the Notice:
  - (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;
  - (d) examining the AML/CFT laws in the jurisdiction where the intermediary operates and determining its comparability with the AML/CFT laws of Singapore.
56. To the extent that the performance of CDD is undertaken by the intermediary rather than by the bank, the bank is required to immediately obtain from the intermediary the information relating to CDD obtained by the intermediary.
57. In addition, where the bank relies on the intermediary to undertake the performance of CDD, the bank should be able to justify 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.

#### **Para 9.4 of the Notice – Cross-Border Wire Transfers Exceeding S\$2,000**

58. Paragraph 9.4 of the Notice requires an ordering institution to include in the message or payment instruction accompanying the wire transfer certain information relating to the originator. A bank should ensure that the requirements are adequately communicated and explained to their customers,

and that they have the necessary customer consent to include such information in the wire transfer or payment instruction

### **Paragraph 9.6 of the Notice - Responsibility of the Beneficiary Bank in Identifying/Handling In-coming Wire Transfers**

59. 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. The risk-based procedures include, but are not limited to, requesting for the missing originator information from the ordering bank and filing the necessary suspicious transaction report (“STR”) if the ordering bank is unwilling to provide the missing information.
60. 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 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**

61. Paragraph 11 of the Notice provides for the establishment of internal procedures for reporting suspicious transactions.
62. Banks are required to have adequate processes and systems for detecting and identifying suspicious transactions. The Authority also expects the bank to put in place effective and efficient procedures for reporting suspicious transactions.
63. The bank should ensure that the internal process for evaluating whether a matter should be referred to the Suspicious Transactions Reporting Office (“STRO”) via an STR be completed without delay and not exceeding 15 working days of the case being referred by the relevant bank staff, unless the circumstances are exceptional or extraordinary.
64. 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.
65. 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.

66. Subject to any written law or any directions given by STRO, 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 ongoing 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.
67. 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**

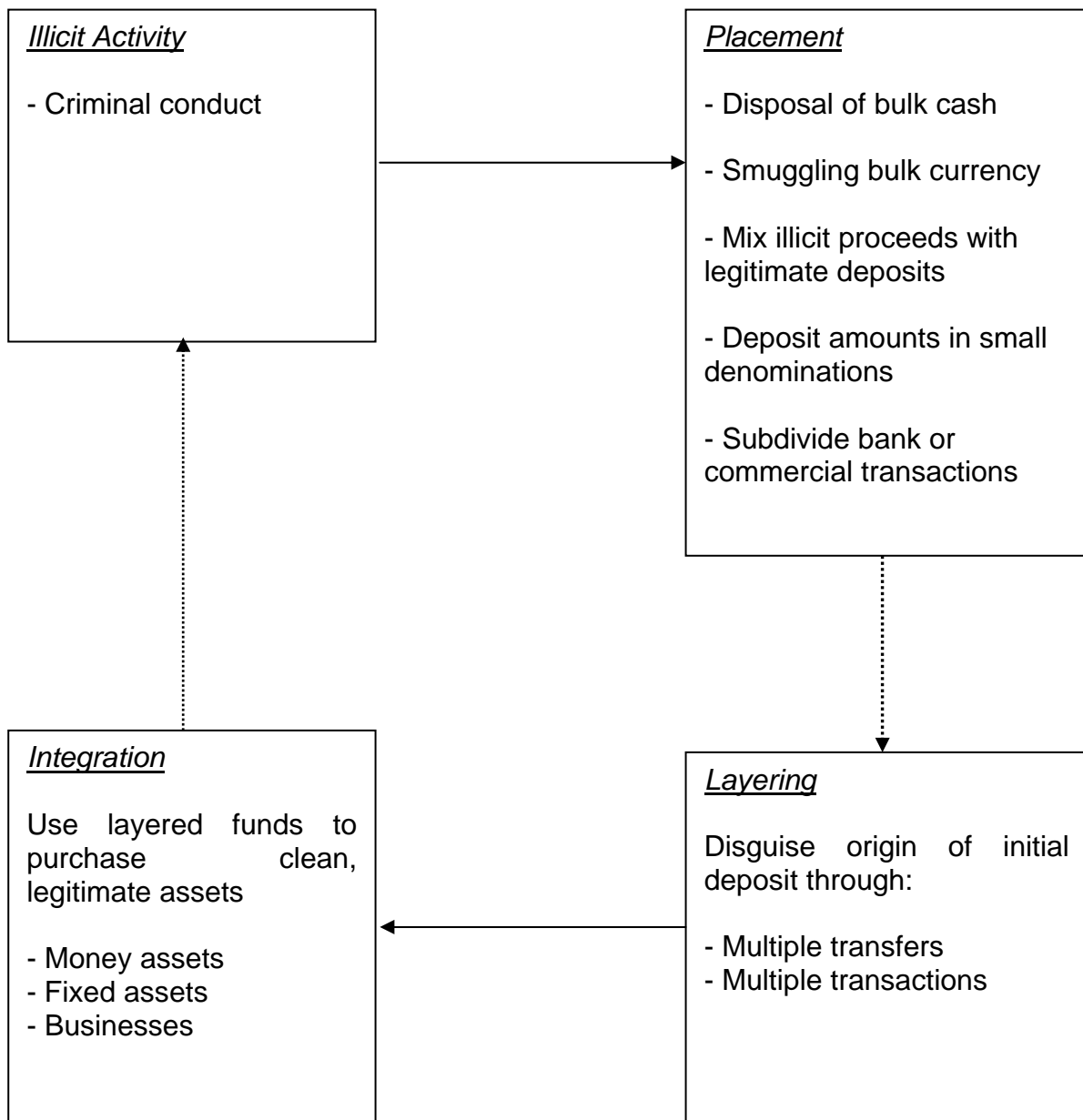
68. The responsibilities of the AML/CFT compliance officer should include the following:
  - (a) ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;
  - (b) advising and training senior management and staff on development and implementing internal policies, procedures and controls on AML/CFT;
  - (c) carrying out, or overseeing the carrying out of, ongoing 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 - Training**

69. 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.
70. 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 every two years.

.....

PROCESS OF MONEY LAUNDERING



## 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 reasonable 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 who 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.
- (i) Purchase of bank cheques on a large scale by an interim customer.
- (ii) Extensive or increased use of safe deposit facilities that do not appear to be justified by the customer's personal or business activities.
- (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, which could be indication of terrorist financing.

- (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.

**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**

<b>Reporting Bank</b>	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
<b>Bank Reporting Officer</b>	
Name:	
Designation:	
Report Reference:	
Contact Officer (if different from Reporting Officer):	
Designation:	
<b>Customer's Particulars #</b>	
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.

<b>Employment Details</b>	
Employer's Name:	
Address:	
Telephone:	
<b>Business Relationship(s) with Customer</b>	
Bank A/c No.:	
Type of A/c:	
Date A/c Opened:	
A/c Balance (Dr/Cr*)	
As At Date:	
Other Business Relationships:	

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

<b>Reason(s) for Suspicion:</b>

<b>Other Relevant Information</b> (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:

**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**

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



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

<b>Authorised Signatories' Particulars #</b>	
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.

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

<b>Reason(s) for Suspicion:</b>

<b>Other Relevant Information</b> (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:

**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**

<b>Reporting Bank</b>	
Name:	
Branch:	
Address:	
Telephone:	
Fax:	
E-mail:	
<b>Bank Reporting Officer</b>	
Name:	
Designation:	
Report Reference:	
Contact Officer: (if different from Reporting Officer)	
Designation:	
<b>Customer's Particulars</b>	
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):	

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

<b>Authorised Signatories' Particulars #</b>	
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.

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

<b>Reason(s) for Suspicion:</b>

**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: