

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

Introduction

1. These Guidelines are issued to provide guidance to the holders of a money-changer's licence and holders of remittance licence (the "licensee") on some of the requirements in MAS Notice 3001 ("the Notice").
2. Licensees are reminded that the ultimate responsibility and accountability for ensuring the licensee's compliance with anti-money laundering and countering the financing of terrorism ("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 customer due diligence ("CDD") measures. This paragraph sets out the standard CDD measures to be applied, of which there are five 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; and
 - Reviewing the earlier relevant business transactions undertaken by a customer where a licensee has one or more relevant business transactions with the customer.
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 politically exposed persons (“PEP”) 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 record keeping (paragraph 8), reporting of suspicious transactions (paragraph 9) and the institution 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; 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

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 (G.N. No. S 515/2002).

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 business.

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

16. Where the customer is not a natural person, paragraphs 4.5, 4.6 and 4.7 of the Notice respectively require the licensee to further identify the directors, partners or persons having executive authority, of the customer.
17. The licensee 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 persons referred to in paragraphs 4.5, 4.6 and 4.7.
18. For the purposes of paragraph 17 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 belonging to the customer in question.

Paragraphs 4.8 and 4.9 of the Notice – Verification of Identity

19. The requirements on verification of identity are intended to ensure that the 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 photograph of that person.
21. The licensee should retain copies of all documentation used to verify the identity of the customer. 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 4.14 to 4.18 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 the measures which 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. 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.
25. Paragraph 4.17 of the Notice states that licensees are not required to inquire if there exists any beneficial owner in relation to the entities specified in sub-paragraphs (a) to (g).
26. 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.

27. 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, the licensee should not treat these entities as automatically eligible for simplified CDD measures. The licensee must comply with the requirements of paragraph 5 of the Notice before applying simplified CDD measures.¹

Reliability of Information and Documentation

28. Where the licensee 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 licensee.
29. Where the customer is unable to produce original documents, the licensee may consider accepting documents that are certified to be true copies by qualified persons, such as lawyers and accountants.

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

30. Paragraph 4.22 of the Notice prohibits licensees from transacting with customers without face-to-face contact, except with the approval of the Authority. Licensees should 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

31. Under paragraph 4.23 of the Notice, a licensee is required to complete CDD measures before undertaking any relevant business transaction with a customer. This is to address risks of money laundering and terrorist financing.
32. Where the customer is not able to furnish either his particulars or evidence of his identity, the licensee shall 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 a licensee to apply to the Authority for approval to perform simplified CDD measures. The licensee should be satisfied that the risk of money laundering or terrorist financing is low.

¹ 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.

34. A licensee should also consider the following factors in determining whether to apply for approval to perform simplified CDD measures:
- (a) whether reliable information on the customer is publicly available; or
 - (b) whether 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 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.
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. In assessing the risk of money laundering or terrorist financing, the licensee 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.
38. Licensees are also required by paragraph 6.4 of the Notice to give particular attention to relevant business 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. The risk-based procedures include, but are not limited to, requesting for the missing originator information from the ordering financial institution and filing the necessary suspicious transaction report (“STR”) if the ordering financial institution is unwilling to provide the missing information.
41. Licensees should consider not accepting in-coming wire transfers from or terminating their business relationships with overseas ordering institutions that, to their knowledge, are required to provide originator information but fail to do so. In this respect, licensees should 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

42. Paragraph 9 of the Notice provides for the establishment of internal procedures for reporting suspicious transactions.
43. Licensees are required to have adequate processes and systems for detecting and identifying suspicious transactions. The Authority also expects the licensee to put in place effective and efficient procedures for reporting suspicious transactions.
44. The licensee 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 reporting staff, unless the circumstances are exceptional or extraordinary.
45. 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.
46. 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.
47. Subject to any written law or any directions given by STRO, 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 ongoing 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.

48. 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.

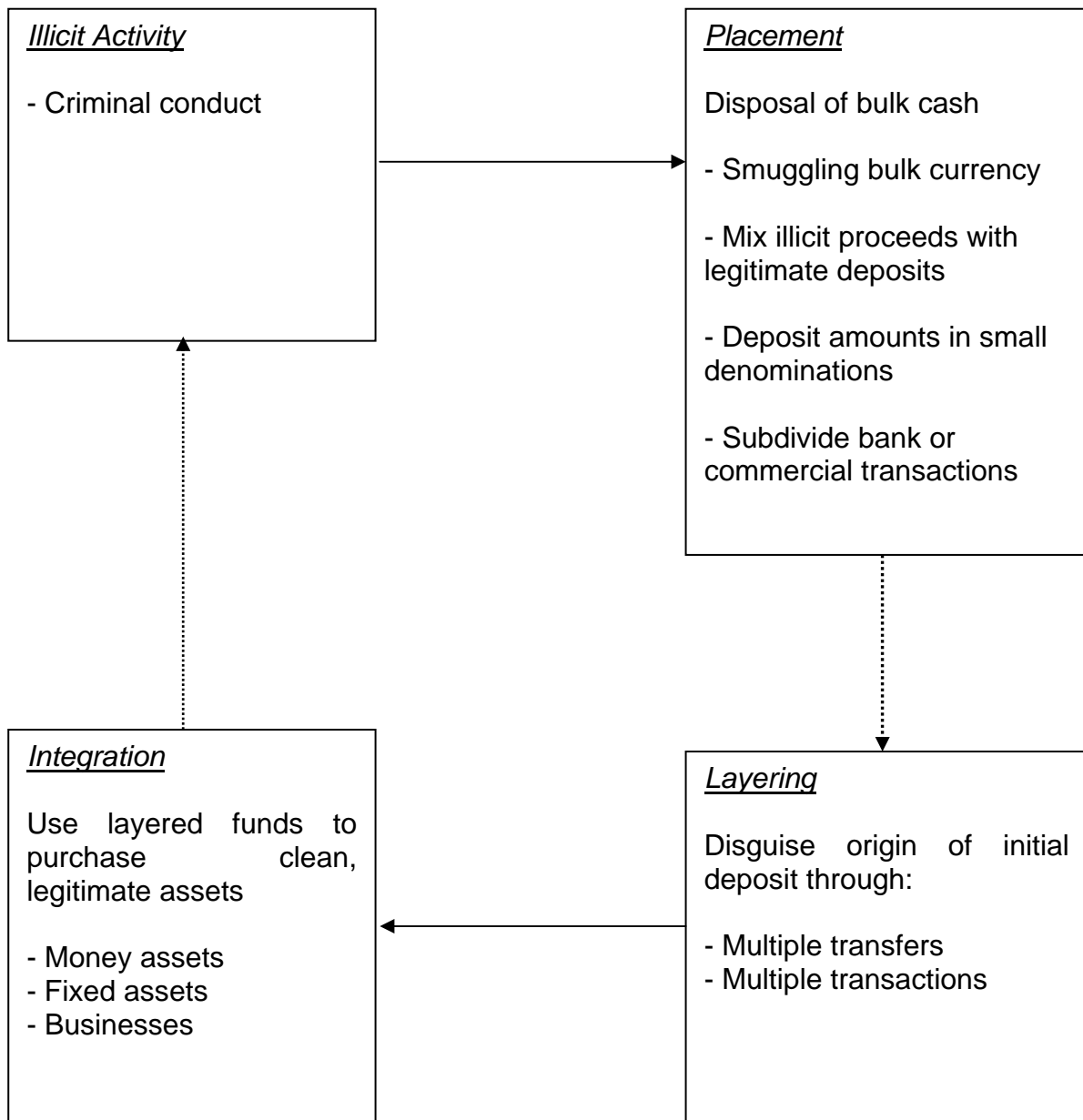
Paragraphs 10.8 to 10.10 of the Notice – Compliance

49. 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) reviewing the earlier relevant business transactions where the licensee has one or more relevant business transactions with the customer 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 – Training

50. 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.
51. 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 every two years.
52. Proper records on training provided to the staff should be maintained by the licensee.

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 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 relevant business transaction.
- 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.

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:

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:

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: