CONSULTATION PAPER

P008 - 2006
August 2006

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

MAS
Monetary Authority of Singapore

TABLE OF CONTENTS

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

PREFACE

On 3 Jan 2005, MAS released for public consultation, a first draft of a revised MAS Notice to Banks No. 626 on Prevention of Money Laundering and Countering the Financing of Terrorism (AML/CFT). A lot of useful comments and drafting suggestions have been received as a result, and MAS acknowledges and thanks the contributions of all respondents.

Since then, there have been substantial developments on the international front in the area of AML/CFT. The Financial Action Task Force (FATF) has begun its third round of mutual evaluation of FATF member countries. Taking into account the comments received during the Jan 2005 consultation and developments in the implementation of the FATF standards, MAS has been working on further refinements to the AML/CFT regime for the Singapore financial sector.

Draft notices on AML/CFT have now been prepared for each of the following financial sectors – banks, finance companies, merchant banks, money changers and remitters, life insurers, capital markets intermediaries, financial advisers, approved trustees, and trust companies.

The revised notices incorporate a number of key changes:

- A more rigorous set of Customer Due Diligence (CDD) measures, including measures to identify and verify the identity of customers and beneficial owners, timing of verification, measures for existing customers and legal entities, and the consequential steps to be taken if CDD measures cannot be satisfactorily performed;

- An element of risk sensitivity in CDD. Enhanced measures are now required of higher risk customers, including correspondent banks and politically exposed persons (PEP), while simplified CDD can be adopted in instances where the risks of money laundering and terrorism financing are assessed to be low; and

- Requirements to give effect to FATF's Special Recommendation on cross-border wire transfers.

Each of these notices will impose legally binding obligations on the respective financial sectors, and will be further supplemented by companion guidelines (to be issued by MAS around 2nd half of August).

INVITATION FOR COMMENTS

MAS invites comments on the draft notices set out in Annexures 1 to 9. 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 4 September 2006.

The consultation period has been extended to 15 Sep 2006.

Annex 1

MAS 626

Date;

NOTICE TO BANKS
BANKING ACT, CAP. 19

(MAS 626 dated 11 November 2002 is cancelled)

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 55 of the Banking Act (Cap. 19) and applies to all banks in Singapore.

2 DEFINITIONS

2.1 For the purposes of this Notice:

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

"beneficial owner", in relation to a customer of a bank, means any individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, however, without corresponding authority to control, manage or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner;

"company" includes a body corporate formed or established outside Singapore under the corporations law of a country or jurisdiction;

"CDD" or "customer due diligence" means the process of identifying the

customer and obtaining information required by paragraph 4;

"customer", in relation to a bank, means the person in whose name an account is opened or intended to be opened, or for whom the bank undertakes or intends to undertake any transaction without an account being opened;

"FATF" means the Financial Action Task Force;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law, but does not include a company that is wholly owned or controlled by a government;

"STR" means suspicious transaction report; and

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

2.2 A reference to business relations, in relation to a bank and a person, is a reference to the opening or maintenance of an account by the bank in the name of that person and the undertaking of transactions by the bank for that person on that account.

2.3 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

2.4 A reference to the completion of CDD measures is a reference to the situation when the bank has received satisfactory responses to all inquiries.

2.5 A reference to a transaction includes a reference to the provision of advice.

2.6 Unless the context otherwise requires, a reference to a financial institution supervised by the Authority does not include a reference to any person exempted from licensing by or registration with the Authority.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all banks in the conduct of their operations and business activities:

(a) A bank must exercise due diligence when dealing with customers and other persons in the course of business.

(b) A bank must conduct its business in conformity with high ethical standards, and guard against undertaking any transaction that is or may be connected with or may facilitate money laundering or terrorist financing.

(c) A bank should, whenever possible and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore in preventing money laundering and terrorist financing.

4 CUSTOMER DUE DILIGENCE

General

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

4.2 In the case of a joint account, a bank shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the bank.

When CDD measures are to be performed

4.3 Every bank shall perform CDD measures in accordance with this Notice when:

(a) the bank establishes business relations with any customer;

(b) the bank undertakes any transaction of a value exceeding S$20,000 for any customer who has not otherwise established business relations with the bank;

(c) there is a suspicion of money laundering or terrorist financing, notwithstanding that the bank would otherwise not be required by this Notice to perform CDD measures; or

(d) the bank has any doubt about the veracity or adequacy of any information previously obtained.

CDD Measures where Business Relations are Established

(I) Identification of Customers

4.4 Every bank shall establish the identity of each customer who applies to the bank to establish business relations.

4.5 For the purpose of the preceding paragraph, a bank shall obtain and record information of the customer, including but not limited to the following :

(a) Full name, including any aliases;

(b) Unique identification number (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

(d) Date of birth, incorporation or registration (as may be appropriate); and

(e) Nationality or place of incorporation or registration (as may be appropriate).

4.6 Where the customer is a company, the bank shall, apart from identifying the customer, also establish the identity of all the directors of the company in the like manner as if such persons were themselves customers.

4.7 Where the customer is a sole proprietorship, the bank shall, apart from identifying the customer, also establish the identity of the sole proprietor in the like manner as if the sole proprietor were a customer in his own name.

4.8 Where the customer is a partnership or a limited liability partnership, the bank shall, apart from identifying the customer, also establish the identity of all the partners in the like manner as if such persons were themselves customers.

4.9 Where the customer is any other body corporate or unincorporate, the bank shall, apart from identifying the customer, also establish the identity of the persons having executive authority in that body corporate or unincorporate in the like manner as if such persons were themselves customers.

(II) Verification of Identity

4.10 The bank shall verify the identity of the customer using reliable, independent sources.

4.11 The bank shall retain copies of all reference documents used in identity verification and the identification information.

(III) Identification and verification of identity of representatives

4.12 Where the customer appoints one or more natural persons to act on his behalf or the customer is not a natural person, a bank shall:

(a) establish the identity of the natural persons that act or are appointed to act on behalf of the customer, in the like manner as if such persons were themselves customers; and

(b) verify the identity of these persons using reliable, independent sources.

4.13 The bank shall verify the due authority of such persons to act on behalf of the customer.

4.14 Without limiting the generality of the preceding paragraph, the bank shall verify the due authority of such persons to act by obtaining:

(a) appropriate documentary evidence that the customer has appointed the persons to act on its behalf, and

(b) the specimen signatures of the persons appointed

4.15 Where the customer is a Singapore government entity, the bank shall only be required to obtain such information as may be required to confirm that the customer is a Singapore government entity as asserted.

(IV) Identification and Verification of Identity of Beneficial Owners

4.16 Every bank shall inquire if there exists any beneficial owner in relation to a customer.

4.17 Where there is one or more beneficial owners in relation to a customer, the bank

shall take reasonable measures to obtain information sufficient to establish and verify the identities of the beneficial owners.

4.18 A bank shall not be required to inquire if there exists any beneficial owner in relation to a customer that is:

(a) a Singapore government entity;

(b) a foreign government entity;

(c) a public company listed on the Singapore Exchange;

(d) a public company listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements;

(e) a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority); or

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF,

unless the bank suspects that the transaction is connected with money laundering or terrorist financing.

4.19 For the purposes of paragraph 4.18(f), the bank shall document the basis for its determination that the requirements in that paragraph have been duly met.

(V) Information on the purpose and intended nature of business relations

4.20 When processing the application to establish business relations, every bank shall obtain, from the customer, information as to the purpose and intended nature of business relations.

(VI) On-going monitoring

4.21 Every bank shall monitor on an ongoing basis, its business relations with customers.

4.22 A bank shall, during the course of business relations, observe the conduct of the customer's account and scrutinise transactions undertaken to ensure that the transactions are consistent with the bank's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

4.23 Every bank shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

4.24 A bank shall, to the extent possible, inquire into the background and purpose of the transactions in paragraph 4.23 and document its findings with a view to making this information available to the relevant competent authorities should the need arise.

(VII) Periodic Review of Identification Information

4.25 Every bank shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up-to-date, particularly for higher risk categories of customers.

Non Face-to-Face Verification

4.26 Every bank shall assess the risks of money laundering or terrorist financing posed by any activity that does not involve face-to-face contact with its customer, and implement appropriate policies and procedures to address these risks.

4.27 Where there is no face-to-face contact, the bank shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

Reliance on identification and verification already performed

4.28 When a bank ("acquiring bank") acquires, either in whole or in part, the business of another financial institution (whether in Singapore or elsewhere), the acquiring bank shall perform CDD measures on the customers acquired with the business at the time of acquisition except where the acquiring bank has:

(a) acquired at the same time all corresponding customer records (including

customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and

(b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring bank as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring bank.

CDD Measures for Non-Account Holders

4.29 Every bank that undertakes any transaction of a value exceeding S$20,000 for any customer who does not otherwise have business relations with the bank shall:

(a) establish and verify the identity of the customer in the like manner as if the customer had applied to the bank to establish business relations; and

(b) record adequate details of the transaction so as to permit the reconstruction of the transaction, including at least the nature and date of the transaction, the type and amount of currency involved, the value date, and the details of the payee or beneficiary.

4.30 Where a bank suspects that two or more transactions are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for in this Notice, the bank shall treat the transactions as a single transaction and aggregate their values for the purpose of this Notice.

Deferring the completion of CDD measures

4.31 Subject to paragraph 4.32 of this Notice, a bank shall complete CDD measures

(a) before the bank establishes business relations; or,

(b) before the bank undertakes any transaction for a customer, where the customer does not have business relations with the bank.

4.32 A bank may establish business relations with a customer before completing CDD measures if:

(a) the deferral of completion of CDD measures is essential in order not to interrupt the normal conduct of business operations; and

(b) the risks of money laundering and terrorist financing can be effectively managed by the bank.

4.33 Where the bank establishes business relations before completion of CDD measures, the bank shall complete CDD measures as soon as reasonably practicable.

4.34 Where the bank is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.

Existing customers

4.35 A bank shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.

5 SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1 Subject to paragraph 5.2, a bank may perform such simplified CDD measures as it considers adequate to effectively identify and verify the identity of the customer and any beneficial owner if it is satisfied that the risks of money laundering and terrorist financing are low.

5.2 The bank shall not perform simplified CDD measures in relation to customers that are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the bank for itself or notified to banks generally by the Authority or by other foreign regulatory authorities.

5.3 A bank may perform simplified CDD measures in relation to a customer that is a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority).

5.4 Where the bank performs simplified CDD measures in relation to a customer, it shall document:

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

6 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

6.1 For the purposes of paragraph 6:

"politically exposed person" means:

(a) a natural person who is or has been entrusted with prominent public functions in a foreign country;

(b) immediate family members of such a person; or

(c) close associates of such a person.

"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil servants, senior judicial or military officials, senior executives of state owned corporations, and senior political party officials.

6.2 Every bank shall, in addition to performing the CDD measures specified in paragraph 4, perform enhanced CDD measures in relation to politically exposed persons, including but not limited to the following:

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person;

(b) obtain approval from the bank's senior management to establish or continue business relations where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person;

(c) establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer or beneficial owner; and

(d) conduct, during the course of business relations, enhanced monitoring of

business relations with the customer.

Other Higher Risk Categories

6.3 The bank shall perform the enhanced CDD measures in paragraph 6.2 for such other categories of customers, business relations or transactions as the bank may assess to present a higher risk for money laundering and terrorist financing.

6.4 Every bank shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the bank for itself or notified to banks generally by the Authority or other foreign regulatory authorities.

7 PERFORMANCE OF CUSTOMER DUE DILIGENCE BY INTERMEDIARIES

7.1 Subject to paragraph 7.2 a bank may rely on an intermediary to perform the CDD measures in paragraph 4 of this Notice if the following requirements are met:

(a) the bank is satisfied that the intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;

(b) the intermediary is not one on which banks have been specifically precluded by the Authority from relying;

(c) the information that the bank would be required or would want to obtain which is being obtained by the intermediary may be relayed to the bank by the intermediary without any delay; and

(d) the intermediary is able and willing to provide, without delay, upon the bank's request, any document obtained by the intermediary which the bank would be required or would want to obtain.

7.2 The bank shall not rely on an intermediary to conduct ongoing monitoring of customers.

7.3 Where a bank does rely on an intermediary, it shall document the basis for its satisfaction that the requirements in paragraph 7.1(a) have been met except

where the intermediary is a financial institution supervised by the Authority (other than a money changer or remittance business).

7.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the bank shall remain responsible for its AML/CFT obligations in this Notice.

8 CORRESPONDENT BANKING

8.1 Paragraph 8 applies when a bank in Singapore provides correspondent banking services in Singapore to another bank or financial institution that is operating outside Singapore.

8.2 For the purposes of paragraph 8:

(a) "correspondent bank" means the bank in Singapore that provides or intends to provide correspondent banking services in Singapore;

(b) "cross-border correspondent banking" means correspondent banking services provided to a bank or financial institution that is operating outside Singapore;

(c) "payable-through account" means an account maintained at the correspondent bank by the respondent bank but which is accessible directly by a third party to effect transactions on its own behalf;

(d) "respondent bank" means the bank or financial institution outside Singapore to whom correspondent banking services in Singapore are provided; and

(e) "shell bank" means a bank incorporated, formed or established in a country or jurisdiction where the bank has no physical presence and which is unaffiliated to a regulated financial group.

8.3 Every bank in Singapore shall perform the following measures when providing cross-border correspondent banking services:

(a) assess the suitability of the respondent bank by taking at least the following steps:

(i) gather adequate information about the respondent bank to

understand fully the nature of the respondent bank's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;

(ii) determine from any available sources the reputation of the respondent bank and, as far as practicable, the quality of supervision over the respondent bank, including where possible whether it has been the subject of money laundering or terrorist financing investigation or regulatory action; and

(iii) assess the respondent bank's AML/CFT controls and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent bank operates;

(b) document the respective AML/CFT responsibilities of each bank; and

(c) obtain approval from the bank's senior management to provide new correspondent banking services.

8.4 Where the cross-border banking services involve a payable-through account, the correspondent bank shall be satisfied that:

(a) the respondent bank has performed appropriate CDD measures at least equivalent to those specified in paragraph 4 on the third party having direct access to the payable-through account; and

(b) the respondent bank is able to perform ongoing monitoring of its business relations with that third party and is willing and able to provide customer identification information to the correspondent bank upon request.

8.5 The correspondent bank shall document the basis for its satisfaction.

8.6 No bank in Singapore shall enter into, or continue correspondent banking relations with a shell bank.

8.7 Every bank shall also take appropriate measures when establishing correspondent banking relations, to satisfy itself that its respondent banks do not

permit their accounts to be used by shell banks.

9 WIRE TRANSFERS

9.1 Paragraph 9 shall apply when a bank in Singapore effects the sending of funds by wire transfer or when it receives funds by wire transfer on the account of a person.

9.2 For the purposes of paragraph 9:

"beneficiary institution" means the financial institution that receives the funds on the account of the wire transfer beneficiary;

"cross-border wire transfer" means a wire transfer where the ordering institution and the beneficiary institution are in different countries or jurisdictions;

"intermediary institution" means the financial institution that is an intermediary in the wire transfer payment chain;

"ordering institution" means the financial institution that acts on the instructions of the wire transfer originator in sending the funds;

"wire transfer beneficiary" means the person to whom or for whose benefit the funds are sent; and

"wire transfer originator" means the person who initiates the sending of funds.

Responsibility of the ordering institution

(I) Identification and recording of information

9.3 Before effecting a wire transfer, every bank that is an ordering institution shall:

(a) establish the identity of the wire transfer originator and verify his identity (if the bank has not already done so by virtue of paragraph 4); and

(b) record adequate details of the wire transfer so as to permit its reconstruction, including at least the date of the wire transfer, the type and amount of currency involved, the value date and the details of the wire transfer beneficiary and the beneficiary institution.

(II) Cross-border Wire Transfers exceeding S$2,000

9.4 In a cross-border wire transfer where the amount to be transferred exceeds S$2,000, every bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer:

(a) the name of the wire transfer originator;

(b) the wire transfer originator's account number (or unique reference number assigned by the ordering institution where no account number exists); and

(c) the wire transfer originator's address, unique identification number, or date and place of birth.

(III) Other Wire Transfers

9.5 In any other types of wire transfers, every bank that is an ordering institution shall either:

(a) include in the message or payment instruction that accompanies or relates to the wire transfer all of the originator information required to be included as if the transaction had been a cross-border wire transfer exceeding S$2,000; or

(b) include only the originator's account number (or unique reference number where no account number exists) but be in a position to make the remaining originator information available within 3 working days of a request being made by the beneficiary institution.

Responsibility of the beneficiary institution

9.6 Every bank that is a beneficiary institution shall implement appropriate internal risk-based policies, procedures and controls for identifying and handling in-coming wire transfers that are not accompanied by complete originator information.

Responsibility of Intermediary Institution

9.7 Every bank that is an intermediary institution shall, in passing onward the message or payment instruction, maintain all the required originator information with the wire transfer.

10 RECORD KEEPING

10.1 Every bank shall prepare, maintain and retain documentation on all its business relations and transactions with its customers such that:

(a) all requirements imposed by law (including this Notice) are met;

(b) any transaction undertaken by the bank can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) the relevant competent authorities in Singapore and the internal and external auditors of the bank are able to review the bank's transactions and assess the level of compliance with this Notice; and

(d) the bank can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities in Singapore for information.

10.2 Subject to paragraph 10.4 and any other requirements imposed by law, every bank shall, when setting its record retention policies, comply with the following document retention periods:

(a) a period of at least 6 years following the termination of business relations for customer identification information, and other documents relating to the establishment of business relations, as well as account files and business correspondence; and

(b) a period of at least 6 years following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

10.3 Every bank may retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

10.4 The bank shall retain records pertaining to a matter which is under investigation

or which has been the subject of an STR for such longer period as may be necessary in accordance with any request or order from STRO or from other relevant competent authorities.

11 SUSPICIOUS TRANSACTIONS REPORTING

11.1 Every bank shall keep in mind the provisions in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act[1] and in the Terrorism (Suppression of Financing) Act that provide for the reporting to the competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to STRO via STRs; and

(b) keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them.

11.2 The bank shall submit reports on suspicious transactions, including attempted transactions to STRO, and extend a copy to the Authority for information.

11.3 The bank shall consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, and document the basis for its determination where:

(a) the bank is for any reason unable to complete CDD measures; or

(b) the customer is reluctant, unable or unwilling to provide any information requested by the bank, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

[1] Please note in particular section 48 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act on tipping-off.

12 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

12.1 Every bank shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees.

12.2 The policies, procedures and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and/or suspicious transactions and the obligation to make suspicious transaction reports.

12.3 The bank shall take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favour anonymity, in formulating its policies, procedures and controls.

Group Policy

12.4 Every bank that is incorporated in Singapore shall develop a group policy on AML/CFT and extend this to all of its branches and subsidiaries outside Singapore.

12.5 Where a bank has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the bank for itself or notified to banks generally by the Authority or by other foreign regulatory authorities), the bank shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

12.6 Where the AML/CFT requirements in the host country or jurisdiction differ from those in Singapore, the bank shall require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

12.7 Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the bank's head office shall report this to the Authority and comply with such further directions as may be given by the Authority.

Compliance

12.8 Every bank shall develop appropriate compliance management arrangements,

including at least, the appointment of a management level officer as the AML/CFT compliance officer.

12.9 Every bank shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information which they require to discharge their functions.

Audit

12.10 Every bank shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the bank's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

12.11 Every bank shall have in place screening procedures to ensure high standards when hiring employees.

Training

12.12 Every bank shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are regularly trained on:

(a) AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and terrorist financing; and

(c) the bank's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

Annex 2

MAS 3001

Date;

NOTICE TO HOLDERS OF MONEY-CHANGER'S LICENCE AND REMITTANCE LICENCE
MONEY-CHANGING AND REMITTANCE BUSINESSES ACT, (CAP. 187)

(MAS 3001 dated 2 December 2005 is cancelled)

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 30 of the Money-changing and Remittance Businesses Act (Cap. 187) and applies to all money-changers and all remittance businesses in Singapore (hereinafter "licensee").

2 DEFINITIONS

2.1 For the purposes of this Notice:

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

"beneficial owner", in relation to a customer of a licensee, means any individual who has a level of control over, or entitlement to, the monies of a relevant business transaction that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the relevant business transaction. The ability to fund the relevant business transaction or the entitlement to the monies alone, however, without corresponding authority to control, manage or direct the relevant business transaction (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner.

"company" includes a body corporate formed or established outside Singapore under the corporations law of a country or jurisdiction;

"CDD" or "customer due diligence" means the process of identifying the customer and obtaining information required by paragraph 4 of this Notice;

"customer", in relation to a licensee, means the person for whom the licensee undertakes or intends to undertake a relevant business transaction;

"FATF" means the Financial Action Task Force;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law, but does not include a company that is wholly owned or controlled by a government;

"relevant business transaction" means:

(a) in relation to a licensed money-changer:

(i) a money-changing transaction of an aggregate value not less than S$5,000; or

(ii) a remittance transaction from another country or jurisdiction to Singapore; or

(b) in relation to a licensed remittance business, a remittance transaction, whether from Singapore to another country or jurisdiction or from another country or jurisdiction to Singapore;

"STR" means suspicious transaction report; and

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

2.2 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

2.3 A reference to the completion of CDD measures is a reference to the situation when the licensee has received satisfactory responses to all inquiries.

2.4 A reference to a transaction includes a reference to the provision of advice.

2.5 Unless the context otherwise requires, a reference to a financial institution supervised by the Authority does not include a reference to any person exempted from licensing by or registration with the Authority.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all licensees in the conduct of their operations and business activities:

(a) a licensee must exercise due diligence when dealing with customers and other persons in the course of business.

(b) a licensee must conduct its business in conformity with high ethical standards, and guard against undertaking any transaction that is or may be connected with or may facilitate money laundering or terrorist financing.

(c) a licensee should, whenever possible and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore in preventing money laundering and terrorist financing.

4 CUSTOMER DUE DILIGENCE

When CDD measures are to be performed

4.1 Every licensee shall perform CDD measures in accordance with this Notice when:

(a) the licensee undertakes a relevant business transaction for any customer;

(b) there is a suspicion of money laundering or terrorist financing, notwithstanding that the licensee would otherwise not be required by this Notice to perform CDD measures; or

(c) the licensee has any doubt about the veracity or adequacy of any information previously obtained.

CDD Measures where Business Relations are Established

(I) Identification of Customers

4.2 Every licensee shall establish the identity of the customer for whom the licensee undertakes a relevant business transaction;

4.3 Where a licensee suspects that two or more transactions are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the thresholds provided for in this Notice, the licensee shall aggregate them and treat them as a single transaction for the purposes of this Notice.

4.4 For the purpose of the preceding paragraph, a licensee shall obtain and record information of the customer, including but not limited to the following:

(a) Full name, including any aliases;

(b) Unique identification number (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

(d) Date of birth, incorporation or registration (as may be appropriate); and

(e) Nationality or place of incorporation or registration (as may be appropriate).

4.5 Where the customer is a company, the licensee shall, apart from identifying the customer, also establish the identity of all the directors of the company in the like manner as if such persons were themselves customers.

4.6 Where the customer is a sole proprietorship, the licensee shall, apart from identifying the customer, also establish the identity of the sole proprietor in the like manner as if the sole proprietor were a customer in his own name.

4.7 Where the customer is a partnership or a limited liability partnership, the licensee shall, apart from identifying the customer, also establish the identity of all partners in the like manner as if such persons were themselves customers.

4.8 Where the customer is any other body corporate or unincorporate, the licensee shall, apart from identifying the customer, also establish the identity of the persons having executive authority in that body corporate or unincorporate in the like manner as if such persons were themselves customers.

(II) Verification of Identity

4.9 The licensee shall verify the identity of the customer using reliable, independent sources.

4.10 The licensee shall retain copies of all reference documents used in identity verification and the identification information.

(III) Identification and verification of identity of representatives

4.11 Where the customer appoints one or more natural persons to act on his behalf, or the customer is not a natural person, a licensee shall:

(a) establish the identity of the natural persons that act or are appointed to act on behalf of the customer, in the like manner as if such persons were themselves customers; and

(b) verify the identity of these persons using reliable, independent sources.

4.12 The licensee shall verify the due authority of such persons to act on behalf of the customer.

4.13 Without limiting the generality of the preceding paragraph, the licensee shall verify the due authority of such persons to act by obtaining:

(a) appropriate documentary evidence that the customer has appointed the persons to act on its behalf, and

(b) the specimen signatures of the persons appointed.

4.14 Where the customer is a Singapore government entity, the licensee shall only be required to obtain such information as may be required to confirm that the customer is a Singapore government entity as asserted.

(IV) Identification and Verification of Identity of Beneficial Owners

4.15 Every licensee shall inquire if there exists any beneficial owner in relation to a customer.

4.16 Where there is one or more beneficial owners in relation to a customer, the licensee shall take reasonable measures to obtain information sufficient to establish and verify the identities of the beneficial owners.

4.17 A licensee shall not be required to inquire if there exists any beneficial owner in relation to a customer that is:

(a) a Singapore government entity;

(b) a foreign government entity;

(c) a public company listed on the Singapore Exchange;

(d) a public company listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements;

(e) a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority); or

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

unless the licensee suspects that the transaction is connected with money laundering or terrorist financing.

4.18 For the purposes of paragraph 4.17(f), the licensee shall document the basis for its determination that the requirements in that paragraph have been duly met.

4.19 Every licensee shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

4.12 A licensee shall, to the extent possible, inquire into the background and purpose of such transactions in paragraph 4.19 and document their findings with a view to making this information available to the relevant competent authorities should the need arise.

Non Face-to-Face Verification

4.13 Transactions without face-to-face contact shall not be undertaken by a licensee, except with the prior approval of MAS.

4.14 When applying to the Authority for such approval, the licensee shall have to satisfy the MAS that it has internal policies, procedures and controls in place to mitigate the risk of money laundering or terrorist financing, and that the CDD measures it will undertake will be no less stringent than those that would be required to be performed if there were face-to-face contact.

Time for completion of CDD measures

4.15 Unless and until a licensee is able to complete CDD measures in relation to a customer, it shall not undertake any relevant business transaction with that customer.

4.16 If the licensee is, for any reason, unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.

5 SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1. With the prior approval of the Authority, a licensee may, instead of taking all of the CDD measures specified in paragraph 4 of this Notice, take such simplified CDD measures in relation to all of its customers or certain categories of its customers as the Authority may determine.

5.2. When applying to the Authority for such approval, the licensee shall have to satisfy the Authority that the risks of money laundering and terrorist financing are low and that the simplified CDD measures that it proposes will effectively identify and verify the identity of the customer and any beneficial owner.

5.3. The licensee shall not perform simplified CDD measures in relation to customers that are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the licensee for itself or notified to all licensees generally by MAS or by other foreign regulatory authorities.

6 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

6.1. For the purposes of paragraph 6:

"politically exposed person" means:

(a) a natural person who is or has been entrusted with prominent public functions in a foreign country;

(b) immediate family members of such a person; or

(c) close associates of such a person.

"prominent public functions" include the roles held by a head of state, a head of government, government ministers, senior civil servants, senior judicial or military officials, senior executives of state owned corporations, and senior political party officials.

6.2. Every licensee shall, in addition to performing the CDD measures specified in paragraph 4, perform enhanced CDD measures in relation to politically exposed persons, including but not limited to the following:

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person;

(b) obtain approval from the licensee's senior management to establish or continue business transactions, where the customer or a beneficial

owner is a politically exposed person or subsequently becomes a politically exposed person.

(c) establish, by appropriate and reasonable means, the source of wealth and source of funds of any customer or beneficial owner.

Other Higher Risk Categories

6.3. The licensee shall perform the enhanced CDD measures in paragraph 6.2 for such other categories of customers, business relations or transactions as the licensee may consider to present a higher risk for money laundering and terrorist financing.

6.4. Every licensee shall give particular attention to relevant business transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the licensee for itself or notified to licensees generally by the Authority or other foreign regulatory authorities.

7 WIRE TRANSFERS

7.1 Paragraph 7 shall apply to a licensee who is a licensed remittance business when it effects the sending of funds by wire transfer or when it receives funds by wire transfer on the account of a person.

7.2 For the purposes of paragraph 7:

"beneficiary institution" means the financial institution that receives the funds on the account of the wire transfer beneficiary;

"cross-border wire transfer" means a wire transfer where the ordering institution and the beneficiary institution are in different countries or jurisdictions;

"intermediary institution" means the financial institution that is an intermediary in the wire transfer payment chain;

"ordering institution" means the financial institution that acts on the instructions of the wire transfer originator in sending the funds;

"wire transfer beneficiary" means the person to whom or for whose benefit the funds are sent; and

"wire transfer originator" means the person who initiates the sending of funds.

Responsibility of the ordering institution

(I) Identification and recording of information

7.3 Before effecting a wire transfer, every licensee that is an ordering institution shall:

(a) establish the identity of the wire transfer originator and verify his identity (if the licensee has not already done so by virtue of paragraph 4; and

(b) record adequate details of the wire transfer so as to permit its reconstruction, including at least the date of the wire transfer, the type and amount of currency involved, the value date, and the details of the wire transfer beneficiary and the beneficiary institution.

(II) Cross-border Wire Transfers exceeding S$2,000

7.4 In the case of a cross-border wire transfer where the amount to be transferred exceeds S$2,000, every licensee which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer:

(a) the name of the wire transfer originator;

(b) the wire transfer originator's account number (or unique reference number assigned by the ordering institution where no account number exists); and

(c) the wire transfer originator's address, unique identification number, or date and place of birth.

(III) Other Wire Transfers

7.5 In any other types of wire transfers, every licensee that is an ordering institution shall either:

(a) include in the message or payment instruction that accompanies or relates to the wire transfer all of the originator information required to be included as if the transaction had been a cross-border wire transfer exceeding S$2,000; or

(b) include only the originator's account number (or unique reference number where no account number exists) but be in a position to make the remaining originator information available within 3 working days of a request being made by the beneficiary institution.

Responsibility of the beneficiary institution

7.6 Every licensee that is a beneficiary institution shall implement appropriate internal risk-based policies, procedures and controls for identifying and handling in-coming wire transfers that are not accompanied by complete originator information.

Responsibility of Intermediary Institution

7.7 Every licensee that is an intermediary institution shall, in passing onward the message or payment instruction, maintain all the required originator information with the wire transfer.

8 RECORD KEEPING

8.1 Every licensee shall prepare, maintain and retain documentation on all their transactions with its customers such that:

(a) all requirements imposed by law (including this Notice) are met;

(b) any transaction undertaken by the licensee can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) the relevant competent authorities in Singapore and the internal and external auditors of the licensee are able to assess the licensee's transactions and level of compliance with this Notice; and

(d) the licensee can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities in Singapore for information.

8.2 Subject to paragraph 8.4 and any other requirements imposed by law, every licensee shall, when setting its record retention policies, comply with the following document retention periods:

(a) a period of at least 6 years following the completion of the transaction for customer identification information, transaction registers, receipts and instructions to banks or agents, as well as account files and business correspondence;

(b) a period of at least 6 years following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

8.3 Every licensee may retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

8.4 The licensee shall retain records pertaining to a matter which is under investigation or which has been the subject of an STR for such longer period as may be necessary in accordance with any request or order from STRO or from other relevant competent authorities.

9 SUSPICIOUS TRANSACTIONS REPORTING

9.1 Every licensee shall keep in mind the provisions in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act[2] and in the Terrorism (Suppression of Financing) Act that provide for the reporting to the competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to STRO via STRs;

[2] Please note in particular section 48 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act on tipping-off.

(b) keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them.

9.2 The licensee shall submit reports on suspicious transactions, including attempted transactions to STRO, and extend a copy to the Authority for information.

9.3 The licensee shall consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, and document the basis for its determination where:

(a) the licensee is for any reason unable to complete CDD measures; or

(b) the customer is reluctant, unable or unwilling to provide any information requested by the licensee, decides to withdraw a relevant business transaction that is pending.

10 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

10.1 Every licensee shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees.

10.2 The procedures, policies and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and suspicious transactions and the obligation to make suspicious transaction reports.

10.3 The licensee shall take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favour anonymity, in formulating its policies, procedures and controls.

Group Policy

10.4 Every licensee that is incorporated in Singapore shall develop a group policy on AML/CFT and extend this to its branches and subsidiaries outside Singapore.

10.5 Where a licensee has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the licensee

for itself or notified to licensees generally by the Authority or by other foreign regulatory authorities), the licensee shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

10.6 Where the AML/CFT requirements in the host country or jurisdiction differ from that in Singapore, the licensee shall require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

10.7 Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is thereby unable to fully observe the higher standard, the licensee's head office shall report this to the Authority and comply with such further directions as may be given by the Authority.

Compliance

10.8 Every licensee shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT compliance officer.

10.9 Every licensee shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information which they require to discharge their functions.

10.10 If the licensee's resources do not make it practicable to appoint an AML/CFT compliance officer, the responsibilities of the AML/CFT compliance officer outlined in this Notice shall be directly assumed by the licensee's senior management.

Audit

10.11 Every licensee shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the licensee's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

10.12 Every licensee shall have in place screening procedures to ensure high standards when hiring employees.

Training

10.13 Every licensee shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are regularly trained on:

(a) AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and terrorist financing; and

(c) the licensee's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

Annex 3

MAS 824

Date;

NOTICE TO FINANCE COMPANIES
FINANCE COMPANIES ACT, CAP. 108

(MAS 824 dated 22 February 2000 is cancelled)

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 30 of the Finance Companies Act (Cap. 108) and applies to all finance companies in Singapore.

2 DEFINITIONS

2.1 For the purposes of this Notice:

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

"beneficial owner", in relation to a customer of a finance company, means any any individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, however, without corresponding authority to control, manage or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner;

"company" includes a body corporate formed or established outside Singapore under the corporations law of a country or jurisdiction;

"CDD" or "customer due diligence" means the process of identifying the customer and obtaining information required by paragraph 4;

"customer", in relation to a finance company, means the person in whose name an account is opened or intended to be opened, or for whom the finance company undertakes or intends to undertake any transaction without an account being opened;

"FATF" means the Financial Action Task Force;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law, but does not include a company that is wholly owned or controlled by a government;

"STR" means suspicious transaction report; and

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

2.2 A reference to business relations, in relation to a finance company and a person, is a reference to the opening or maintenance of an account by the finance company in the name of that person and the undertaking of transactions by the finance company for that person on that account.

2.3 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

2.4 A reference to the completion of CDD measures is a reference to the situation when the finance company has received satisfactory responses to all inquiries.

2.5 A reference to a transaction includes a reference to the provision of advice.

2.6 Unless the context otherwise requires, a reference to a financial institution supervised by the Authority does not include a reference to any person exempted from licensing by or registration with the Authority.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all finance companies in the conduct of their operations and business activities:

(a) A finance company must exercise due diligence when dealing with customers and other persons in the course of business.

(b) A finance company must conduct its business in conformity with high ethical standards, and guard against undertaking any transaction that is or may be connected with or may facilitate money laundering or terrorist financing.

(c) A finance company should, whenever possible and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore in preventing money laundering and terrorist financing.

4 CUSTOMER DUE DILIGENCE

General

4.1 No finance company shall open or maintain anonymous accounts or accounts in fictitious names.

4.2 In the case of a joint account, a finance company shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the finance company.

When CDD measures are to be performed

4.3 Every finance company shall perform CDD measures in accordance with this Notice when:

(a) the finance company establishes business relations with any customer;

(b) the finance company undertakes any transaction of a value exceeding S$20,000 for any customer who has not otherwise established business relations with the finance company;

(c) there is a suspicion of money laundering or terrorist financing, notwithstanding that the finance company would otherwise not be required by this Notice to do so; or

(d) the finance company has any doubt about the veracity or adequacy of any information previously obtained.

CDD Measures where Business Relations are Established

(I) Identification of Customers

4.4 Every finance company shall establish the identity of each customer who applies to the finance company to establish business relations.

4.5 For the purpose of the preceding paragraph, the finance company shall obtain and record at least the following information of the customer, including but not limited to the following:

(a) Full name, including any aliases;

(b) Unique identification number (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

(d) Date of birth, incorporation or registration (as may be appropriate); and

(e) Nationality or place of incorporation or registration (as may be appropriate).

4.6 Where the customer is a company, the finance company shall, apart from identifying the customer, also establish the identity of all the directors of the company in the like manner as if such person were themselves customers.

4.7 Where the customer is a sole proprietorship, the finance company shall, apart from identifying the customer, also establish the identity of the sole proprietor in the like manner as if the sole proprietor were a customer in his own name.

4.8 Where the customer is a partnership or a limited liability partnership, the finance company shall, apart from identifying the customer, also establish the identity of all partners in the like manner as if such persons were themselves customers.

4.9 Where the customer is any other body corporate or unincorporate, the finance company shall, apart from identifying the customer, also establish the identity of the persons having executive authority in that body corporate or unincorporate in the like manner as if such persons were themselves customers.

(II) Verification of Identity

4.10 The finance company shall verify the identity of the customer using reliable, independent sources.

4.11 The finance company shall retain copies of all reference documents used in identity verification and the identification information.

(III) Identification and verification of identity of representatives

4.12 Where the customer appoints one or more natural persons to act on his behalf or the customer is not a natural person, a finance company shall:

(a) establish the identity of the natural persons that act or are appointed to act on behalf of the customer, in the like manner as if such persons were themselves customers; and

(b) verify the identity of these persons using reliable, independent sources.

4.13 The finance company shall verify the due authority of such persons to act on behalf of the customer.

4.14 Without limiting the generality of the preceding paragraph, the finance company shall verify the due authority of such persons to act by obtaining:

(a) appropriate documentary evidence that the customer has appointed the persons to act on its behalf, and

(b) the specimen signatures of the persons appointed.

4.15 Where the customer is a Singapore government entity, the finance company shall only be required to obtain such information as may be required to confirm that the customer is a Singapore government entity as asserted.

(IV) Identification and Verification of Identity of Beneficial Owners

4.16 Every finance company shall inquire if there exists any beneficial owner in relation to a customer.

4.17 Where there is one or more beneficial owners in relation to a customer, the finance company shall take reasonable measures to obtain information sufficient to establish and verify the identities of the beneficial owners.

4.18 A finance company shall not be required to inquire if there exists any beneficial owner in relation to a customer that is:

(a) a Singapore government entity;

(b) a foreign government entity;

(c) a public company listed on the Singapore Exchange;

(d) a public company listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements;

(e) a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority);or

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF

unless the finance company suspects that the transaction is connected with money laundering or terrorist financing.

4.19 For the purposes of paragraph 4.18(f), the finance company shall document the basis for its determination that the requirements in that paragraph have been duly met.

(V) Information on the purpose and intended nature of business relations

4.20 When processing the application to establish business relations, every finance company shall obtain, from the customer, information as to the purpose and intended nature of business relations.

(VI) On-going monitoring

4.21 Every finance company shall monitor on an ongoing basis, its business relations with customers.

4.22 A finance company shall, during the course of business relations, observe the conduct of the customer's account and scrutinise transactions undertaken to ensure that the transactions are consistent with the finance company's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

4.23 Every finance company shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

4.24 A finance company shall, to the extent possible, inquire into the background and purpose of the transactions in paragraph 4.23 and document their findings with a view to making this information available to the relevant competent authorities should the need arise.

(VII) Periodic Review of Identification Information

4.25 Every finance company shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up-to-date, particularly for higher risk categories of customers.

Non Face-to-Face Verification

4.26 Every finance company shall assess the risks of money laundering or terrorist financing posed by any activity that does not involve face-to-face contact, and implement appropriate policies and procedures to address these risks.

4.27 Where there is no face-to-face contact, the finance companies shall carry out CDD measures that are at least as stringent as those that would be required to be performed if there were face-to-face contact.

Reliance on identification and verification already performed

4.28 When a finance company ("acquiring finance company") acquires, either in whole or in part, the business of another financial institution (whether in Singapore or elsewhere), the acquiring finance company shall perform CDD measures on customers acquired with the business at the time of acquisition, except where the acquiring finance company has:

(a) acquired at the same time all corresponding customer records (including customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and

(b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring finance company as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring finance company.

CDD Measures for Non-Account Holders

4.29 Every finance company that undertakes any transaction of a value exceeding S$20,000 for any customer who does not otherwise have business relations with the finance company shall:

(a) establish and verify the identity of the customer in the like manner as if the customer had applied to the finance company to establish business relations; and

(b) record adequate details of the transaction so as to permit the reconstruction of the transaction, including at least the nature and date of the transaction, the type and amount of currency involved, the value date, and the details of the payee or beneficiary.

4.30 Where a finance company suspects that two or more transactions are or may be related or linked, or the result of the deliberate structuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for

in this Notice, the finance company shall treat them as a single transaction and aggregate their values for the purpose of this Notice.

Deferring the completion of CDD measures

4.31 Subject to paragraph 4.32 of this Notice, a finance company shall complete CDD measures

(a) before the finance company establishes business relations with a customer; or

(b) before the finance company undertakes any transaction for a customer, where the customer does not have business relations with the finance company.

4.32 A finance company may establish business relations with a customer before completing CDD measures if:

(a) the deferral of completion of CDD measures is essential in order not to interrupt the normal conduct of business operations; and

(b) the risks of money laundering and terrorist financing can be effectively managed by the finance company.

4.33 Where the finance company establishes business relations before completion of CDD measures, the finance company shall nevertheless complete CDD measures as soon as reasonably practicable.

4.34 Where the finance company is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.

Existing customers

4.35 A finance company shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.

5 SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1 Subject to paragraph 5.2, a finance company may perform such simplified CDD measures as it considers adequate to effectively identify and verify the identity of the customer and any beneficial owner if it is satisfied that the risks of money laundering and terrorist financing are low.

5.2 The finance company shall not perform simplified CDD measures in relation to customers that are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the finance company for itself or notified to finance companies generally by the Authority or by other foreign regulatory authorities.

5.3 A finance company may perform simplified CDD measures in relation to a customer that is a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority).

5.4 Where the finance company performs simplified CDD measures in relation to a customer, it shall document -

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

6 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

6.1 For the purposes of paragraph 6,

"politically exposed person" means:

(a) a natural person who is or has been entrusted with prominent public functions in a foreign country;

(b) immediate family members of such a person; or

(c) close associates of such a person.

'"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil servants, senior judicial or military officials, senior executives of state owned corporations, and senior political party officials.

6.2 Every finance company shall, in addition to performing the CDD measures specified in paragraph 4, perform enhanced CDD measures in relation to politically exposed persons, including but not limited to the following:

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person;

(b) obtain approval from the finance company's senior to establish or continue business relations, where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person.

(c) establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer or beneficial owner; and

(d) conduct during the course of business relations, enhanced monitoring of business relations with the customer.

Other Higher Risk Categories

6.3 The finance company shall perform the enhanced CDD measures in paragraph 6.2 for such other categories of customers, business relations or transactions as the finance company may consider to present a higher risk for money laundering and terrorist financing.

6.4 Every finance company shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the finance company for itself or notified to finance companies generally by the Authority or other foreign regulatory authorities.

7 PERFORMANCE OF CUSTOMER DUE DILIGENCE BY INTERMEDIARIES

7.1 Subject to paragraph 7.2, a finance company may rely on an intermediary to perform the CDD measures in paragraph 4 of this Notice if the following requirements are met:

(a) the finance company is satisfied that the intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;

(b) the intermediary is not one on which finance companies have been specifically precluded by the Authority from relying;

(c) the information that the finance company would be required or would want to obtain is being obtained by the intermediary, may be relayed to the finance company by the intermediary without any delay; and

(d) the intermediary is able and willing to provide, without delay, upon the finance company's request, any document obtained by the intermediary which the finance company would be required or would want to obtain.

7.2 The finance company shall not rely on an intermediary to conduct ongoing monitoring of customers.

7.3 Where a finance company does rely on an intermediary, it shall document the basis for its satisfaction that the requirements in paragraph 7.1(a) have been met except where the intermediary is a financial institution supervised by the Authority (other than a money changer or remittance agent).

7.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the finance company shall remain responsible for its AML/CFT obligations in this Notice.

8 WIRE TRANSFERS

8.1 Paragraph 8 shall apply (to the extent that a finance company is permitted to do so) when a finance company effects the sending of funds by wire transfer or when it receives funds by wire transfer on the account of a person.

8.2 For the purposes of paragraph 8:

"beneficiary institution" means the financial institution that receives the funds on the account of the wire transfer beneficiary;

"cross-border wire transfer" means a wire transfer where the ordering institution and the beneficiary institution are in different countries or jurisdictions;

"intermediary institution" means the financial institution that is an intermediary in the wire transfer payment chain;

"ordering institution" means the financial institution that acts on the instructions of the wire transfer originator in sending the funds;

"wire transfer beneficiary" means the person to whom or for whose benefit the funds are sent; and

"wire transfer originator" means the person who initiates the sending of funds.

Responsibility of the ordering institution

(I) Identification and recording of information

8.3 Before effecting a wire transfer, every finance company that is an ordering institution shall:

(a) establish the identity of the wire transfer originator and verify his identity (if the finance company has not already done by virtue of paragraph 4);

(b) record adequate details of the wire transfer so as to permit its reconstruction, including the date of the wire transfer, the type and amount of currency involved, the value date, and the details of the wire transfer beneficiary and the beneficiary institution.

(II) Cross-border Wire Transfers exceeding S$2,000

8.4 In a cross-border wire transfer where the amount to be transferred exceeds S$2,000, every finance company which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer:

(a) the name of the wire transfer originator;

(b) the wire transfer originator's account number (or unique reference number assigned by the ordering institution where no account number exists); and

(c) the wire transfer originator's address, unique identification number, or date and place of birth.

(III) Other Wire Transfers

8.5 In any other types of wire transfers, every finance company that is an ordering institution shall either:

(a) include in the message or payment instruction that accompanies or relates to the wire transfer all of the originator information required to be included as if the transaction had been a cross-border wire transfer exceeding S$2,000; or

(b) include only the originator's account number (or unique reference number where no account number exists) but be in a position to make the remaining originator information available within 3 working days of a request being made by the beneficiary institution.

Responsibility of the beneficiary institution

8.6 Every finance company that is a beneficiary institution shall implement appropriate internal risk-based policies, procedures and controls for identifying and handling in-coming wire transfers that are not accompanied by complete originator information.

Responsibility of Intermediary Institution

8.7 Every finance company that is an intermediary institution shall, in passing onward the message or payment instruction, maintain all the required originator information with the wire transfer.

9 RECORD KEEPING

9.1 Every finance company shall prepare, maintain and retain documentation on all its business relations and transactions with its customers such that:

(a) all requirements imposed by law (including this Notice) are met;

(b) any transaction undertaken by the finance company can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity the relevant competent authorities in Singapore and the internal and external auditors of the finance company are able to assess the finance company's transactions and level of compliance with this Notice; and

(c) the finance company can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities in Singapore for information.

9.2 Subject to paragraph 9.4 and any other requirements imposed by law, every finance company shall, when setting its record retention policies, comply with the following document retention periods:

(a) a period of at least 6 years following termination of business relations for customer identification information, and other documents relating to the establishment of business relations, as well as account files and business correspondence; and

(b) a period of at least 6 years following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

9.3 Every finance company may retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

9.4 The finance company shall retain records pertaining to a matter which is under investigation or which has been the subject of an STR for such longer period as may be necessary in accordance with any request or order from STRO or from other relevant competent authorities.

10 SUSPICIOUS TRANSACTIONS REPORTING

10.1 Every finance company shall keep in mind the provisions in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act[3] and in the Terrorism (Suppression of Financing) Act that provide for the reporting to the competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to STRO via STRs; and

(b) keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them.

10.2 The finance company shall submit reports on suspicious transactions, including attempted transactions to STRO, and extend a copy to the Authority for information.

10.3 The finance company shall consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, and document the basis for its determination where:

(a) a finance company is for any reason unable to complete CDD measures; or

(b) the customer is reluctant, unable or unwilling to provide any information requested by the finance company, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

11 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

[3] Please note in particular section 48 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act on tipping-off.

11.1 Every finance company shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees.

11.2 The procedures, policies and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and suspicious transactions and the obligation to make suspicious transaction reports.

11.3 The finance company shall take into consideration money laundering and terrorist financing threats that may arise from new or developing technologies, especially those that favour anonymity, in formulating its policies, procedures and controls.

Compliance

11.4 Every finance company shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT compliance officer.

11.5 Every finance company shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information which they require to discharge their functions.

Audit

11.6 Every finance company shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the finance company's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

11.7 Every finance company shall have in place screening procedures to ensure high standards when hiring employees.

Training

11.8 Every finance company shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are regularly trained on:

(a) AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and terrorist financing; and

(c) the finance company's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

Annex 4

MAS 1014

Date;

NOTICE TO MERCHANT BANKS
MAS ACT, CAP. 186

(MAS 1014 dated 22 February 2000 is cancelled)

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 28(3) of the Monetary Authority of Singapore Act (Cap. 186) and applies to all merchant banks in Singapore.

2 DEFINITIONS

2.1 For the purposes of this Notice:

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

"beneficial owner", in relation to a customer of a merchant bank, means any individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, however, without corresponding authority to control, manage or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner;

"company" includes a body corporate or unincorporated, formed or established outside Singapore under the corporations law of a country or jurisdiction;

"CDD" or "customer due diligence" means the process of identifying the customer and obtaining information required by paragraph 4 of this Notice;

"customer", in relation to a merchant bank, means the person in whose name an account is opened or intended to be opened, or for whom the merchant bank undertakes or intends to undertake any transaction without an account being opened;

"FATF" means the Financial Action Task Force;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law, but does not include a company that is wholly owned or controlled by a government;

"STR" means suspicious transaction report; and

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

2.2 A reference to business relations, in relation to a merchant bank and a person, is a reference to the opening or maintenance of an account by the merchant bank in the name of that person and the undertaking of transactions by the merchant bank for that person on that account.

2.3 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

2.4 A reference to the completion of CDD measures is a reference to the situation when the merchant bank has received satisfactory responses to all inquiries.

2.5 A reference to a transaction includes a reference to the provision of advice.

2.6 Unless the context otherwise requires, a reference to a financial institution supervised by the Authority does not include a reference to any person exempted from licensing by or registration with the Authority.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all merchant banks in the conduct of their operations and business activities:

(a) A merchant bank must exercise due diligence when dealing with customers and other persons in the course of business.

(b) A merchant bank must conduct its business in conformity with high ethical standards, and guard against undertaking any transaction that is or may be connected with or may facilitate money laundering or terrorist financing.

(c) A merchant bank should, whenever possible and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore in preventing money laundering and terrorist financing.

4 CUSTOMER DUE DILIGENCE

General

4.1 No merchant bank shall open or maintain anonymous accounts or accounts in fictitious names.

4.2 In the case of a joint account, a merchant bank shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the merchant bank.

When CDD measures are to be performed

4.3 Every merchant bank shall perform CDD measures in accordance with this Notice when:

(a) the merchant bank establishes business relations with any customer;

(b) the merchant bank undertakes any transaction of a value exceeding S$20,000 for any customer who has not otherwise established business relations with the merchant bank;

(c) there is a suspicion of money laundering or terrorist financing, notwithstanding that the merchant bank would otherwise not be required by this Notice to perform CDD measures; or

(d) the merchant bank has any doubt about the veracity or adequacy of any information previously obtained.

CDD Measures where Business Relations are Established

(I) Identification of Customers

4.4 Every merchant bank shall establish the identity of each customer who applies to the merchant bank to establish business relations.

4.5 For the purpose of the preceding paragraph, a merchant bank shall obtain and record information of the customer, including but not limited to the following:

(a) Full name, including any aliases;

(b) Unique identification number (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

(d) Date of birth, incorporation or registration (as may be appropriate); and

(e) Nationality or place of incorporation or registration (as may be appropriate).

4.6 Where the customer is a company, the merchant bank shall, apart from identifying the customer, also establish the identity of all the directors of the company in the like manner as if such persons were themselves customers.

4.7 Where the customer is a sole proprietorship, the merchant bank shall, apart from identifying the customer, also establish the identity of the sole proprietor in the like manner as if the sole proprietor were a customer in his own name.

4.8 Where the customer is a partnership or a limited liability partnership, the merchant bank shall, apart from identifying the customer, also establish the identity of all partners in the like manner as if such persons were themselves customers.

4.9 Where the customer is any other body corporate or unincorporate, the merchant bank shall, apart from identifying the customer, also establish the identity of the persons having executive authority in that body corporate or unincorporate in the like manner as if such persons were themselves customers.

(II) Verification of Identity

4.10 The merchant bank shall verify the identity of the customer using reliable, independent sources.

4.11 The merchant bank shall retain copies of all reference documents used in identity verification and the identification information.

(III) Identification and verification of identity of representatives

4.12 Where the customer appoints one or more natural persons to act on his behalf or the customer is not a natural person, a merchant bank shall:

(a) establish the identity of the natural persons that act or are appointed to act on behalf of the customer, in the like manner as if such persons were themselves customers; and

(b) verify the identity of these persons using reliable, independent sources.

4.13 The merchant bank shall verify the due authority of such persons to act on behalf of the customer.

4.14 Without limiting the generality of the preceding paragraph, the merchant bank shall verify the due authority of such persons to act by obtaining:

(a) appropriate documentary evidence that the customer has appointed the persons to act on its behalf, and

(b) the specimen signatures of the persons appointed.

4.15 Where the customer is a Singapore government entity, the merchant bank shall only be required to obtain such information as may be required to confirm that the customer is a Singapore government entity as asserted.

(IV) Identification and Verification of Identity of Beneficial Owners

4.16 Every merchant bank shall inquire if there exists any beneficial owner in relation to a customer.

4.17 Where there is one or more beneficial owners in relation to a customer, the merchant bank shall take reasonable measures to obtain information sufficient to establish and verify the identities of the beneficial owners.

4.18 A merchant bank shall not be required to inquire if there exists any beneficial owner in relation to a customer that is:

(a) a Singapore government entity;

(b) a foreign government entity;

(c) a public company listed on the Singapore Exchange;

(d) a public company listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements;

(e) a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority); or

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF

unless the merchant bank suspects that the transaction is connected with money laundering or terrorist financing.

4.19 For the purposes of paragraph 4.18(f), the merchant bank shall document the basis for its determination that the requirements in that paragraph have been duly met.

(V) Information on the purpose and intended nature of business relations

4.20 When processing the application to establish business relations, every merchant bank shall, obtain from the customer, information as to the purpose and intended nature of business relations.

(VI) On-going monitoring

4.21 Every merchant bank shall monitor on an ongoing basis, its business relations with customers.

4.22 A merchant bank shall, during the course of business relations, observe the conduct of the customer's account and scrutinise transactions undertaken to ensure that the transactions are consistent with the merchant bank's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

4.23 Every merchant bank shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

4.24 A merchant bank shall, to the extent possible, inquire into the background and purpose of the transactions in paragraph 4.23 and document its findings with a view to making this information available to the relevant competent authorities should the need arise.

(VII) Periodic Review of Identification Information

4.25 Every merchant bank shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up-to-date, particularly for higher risk categories of customers.

Non Face-to-Face Verification

4.26 Every merchant bank shall assess the risks of money laundering or terrorist financing posed by any activity that does not involve face-to-face contact with its customer, and implement appropriate policies and procedures to address these risks.

4.27 Where there is no face-to-face contact, the merchant bank shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

Reliance on identification and verification already performed

4.28 When a merchant bank ("acquiring merchant bank") acquires, either in whole or in part, the business of another financial institution (whether in Singapore or elsewhere), the acquiring merchant bank shall perform CDD measures on the customers acquired with the business at the time of acquisition, except where the acquiring merchant bank has:

(a) acquired at the same time all corresponding customer records (including customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and

(b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring merchant bank as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring merchant bank.

CDD Measures for Non-Account Holders

4.29 Every merchant bank that undertakes any transaction of a value exceeding S$20,000 for any customer who does not otherwise have business relations with the merchant bank shall:

(a) establish and verify the identity of the customer in the like manner as if the customer had applied to the merchant bank to establish business relations; and

(b) record adequate details of the transaction so as to permit the reconstruction of the transaction, including at least the nature and date of the transaction, the type and amount of currency involved, the value date, and the details of the payee or beneficiary.

4.30 Where a merchant bank suspects that two or more transactions are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for

in this Notice, the merchant bank shall treat the transactions as a single transaction and aggregate their values for the purpose of this Notice.

Deferring the completion of CDD measures

4.31 Subject to paragraph 4.32 of this Notice, a merchant bank shall complete CDD measures:

(a) before the merchant bank establishes business relations; or

(b) before the merchant bank undertakes any transaction for a customer where the customer does not have business relations with the merchant bank.

4.32 A merchant bank may establish business relations with a customer before completing CDD measures if:

(a) the deferral of completion of CDD measures is essential in order not to interrupt the normal conduct of business operations; and

(b) the risks of money laundering and terrorist financing can be effectively managed by the merchant bank.

4.33 Where the merchant bank establishes business relations before completion of CDD measures, the merchant bank shall complete CDD measures as soon as reasonably practicable.

4.34 Where the merchant bank is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.

Existing customers

4.35 A merchant bank shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.

5 SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1 Subject to paragraph 5.2, a merchant bank may perform such simplified CDD measures as it considers adequate to effectively identify and verify the identity of the customer and any beneficial owner if it is satisfied that the risks of money laundering and terrorist financing are low.

5.2 The merchant bank shall not perform simplified CDD measures in relation to customers that are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the merchant bank for itself or notified to merchant banks generally by the Authority or by other foreign regulatory authorities.

5.3 A merchant bank may perform simplified CDD measures in relation to a customer that is a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority);

5.4 Where the merchant bank performs simplified CDD measures in relation to a customer, it shall document:

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

6 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

6.1 For the purposes of paragraph 6:

"politically exposed person" means:

(a) a natural person who is or has been entrusted with prominent public functions in a foreign country;

(b) immediate family members of such a person; or

(c) close associates of such a person.

"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil servants, senior judicial or military officials, senior executives of state owned corporations, and senior political party officials.

6.2 Every merchant bank shall, in addition to performing the CDD measures specified in paragraph 4, perform enhanced CDD measures in relation to politically exposed persons, including but not limited to the following:

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person;

(b) obtain approval from the merchant bank's senior management on whether to establish or continue business relations, where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person;

(c) establish by appropriate and reasonable means, the source of wealth and source of funds of the customer or beneficial owner; and

(d) conduct, during the course of business relations, enhanced monitoring of business relations with the customer.

Other Higher Risk Categories

6.3 The merchant bank shall perform the enhanced CDD measures in paragraph 6.2 for such other categories of customers, business relations or transactions as the merchant bank may assess to present a higher risk for money laundering and terrorist financing.

6.4 Every merchant bank shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the merchant bank for itself or notified to merchant banks generally by the Authority or other foreign regulatory authorities.

7 PERFORMANCE OF CUSTOMER DUE DILIGENCE BY INTERMEDIARIES

7.1 Subject to paragraph 7.2, a merchant bank may rely on an intermediary to perform CDD measures in paragraph 4 of this Notice on its behalf if the following requirements are met:

(a) the merchant bank is satisfied that the intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;

(b) the intermediary is not one on which merchant banks have been specifically precluded by the Authority from relying;

(c) the information that the merchant bank would be required or would want to obtain which is being obtained by the intermediary may be relayed to the merchant bank by the intermediary without any delay; and

(d) the intermediary is able and willing to provide, without delay, upon the merchant bank's request, any document obtained by the intermediary which the merchant bank would be required or would want to obtain.

7.2 The merchant bank shall not rely on an intermediary to conduct ongoing monitoring of customers.

7.3 Where a merchant bank does rely on an intermediary, it shall document the basis for its satisfaction that the requirements in paragraph 7.1 (a) have been met except where the intermediary is a financial institution supervised by the Authority (other than a money changer or remittance business).

7.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the merchant bank shall remain responsible for its AML/CFT obligations in this Notice.

8 CORRESPONDENT BANKING

8.1 Paragraph 8 applies when a merchant bank in Singapore provides correspondent banking services in Singapore to another bank or financial institution that is operating outside Singapore.

8.2 For the purposes of this Notice:

(a) "correspondent bank" means the merchant bank in Singapore that provides or intends to provide correspondent banking services in Singapore;

(b) "cross-border correspondent banking" means correspondent banking services provided to a bank or financial institution that is operating outside Singapore;

(c) "payable-through account" means an account maintained at the correspondent bank by the respondent bank but which is accessible directly by a third party to effect transactions on its own behalf;

(d) "respondent bank" means the bank or financial institution outside Singapore to whom correspondent banking services in Singapore are provided; and

(e) "shell bank" means a bank incorporated, formed or established in a country or jurisdiction where the bank has no physical presence and which is unaffiliated to a regulated financial group.

8.3 Every merchant bank shall perform the following measures when providing cross-border correspondent banking services:

(a) assess the suitability of the respondent bank by taking at least the following steps:

(i) gather adequate information about the respondent bank to understand fully the nature of the respondent bank's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;

(ii) determine from any available sources the reputation of the respondent bank and, as far as practicable, the quality of supervision over the respondent bank, including where possible whether it has been the subject of money laundering or terrorist financing investigation or regulatory action; and

(iii) assess the respondent bank's AML/CFT controls and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent bank operates.

(b) document the respective AML/CFT responsibilities of each bank; and

(c) obtain approval from the merchant bank's senior management to provide new correspondent banking services.

8.4 Where the cross-border banking services involve a payable-through account, the correspondent bank shall be satisfied that:

(a) the respondent bank has performed appropriate CDD measures at least equivalent to those specified in paragraph 4 on the third party having direct access to the payable-through-account; and

(b) the respondent bank is able to perform ongoing monitoring of its business relations with that third party and is willing and able to provide customer identification information to the correspondent bank upon request.

8.5 The correspondent bank shall document the basis for its satisfaction.

8.6 No merchant bank in Singapore shall enter into, or continue, correspondent banking relations with a shell bank.

8.7 Every merchant bank shall also take appropriate measures when establishing correspondent banking relations, to satisfy itself that its respondent banks do not permit their accounts to be used by shell banks.

9 WIRE TRANSFERS

9.1 Paragraph 9 shall apply when a merchant bank effects the sending of funds by wire transfer or when it receives funds by wire transfer on the account of a person.

9.2 For the purposes of paragraph 9:

"beneficiary institution" means the financial institution that receives the funds on the account of the wire transfer beneficiary;

"cross-border wire transfer" means a wire transfer where the ordering institution and the beneficiary institution are in different countries or jurisdictions;

"intermediary institution" means the financial institution that is an intermediary in the wire transfer payment chain;

"ordering institution" means the financial institution that acts on the instructions of the wire transfer originator in sending the funds;

"wire transfer beneficiary" means the person to whom or for whose benefit the funds are sent; and

"wire transfer originator" means the person who initiates the sending of funds.

Responsibility of the ordering institution

(I) Identification and recording of information

9.3 Before effecting a wire transfer, every merchant bank that is an ordering institution shall:

(a) establish the identity of the wire transfer originator and verify his identity (if the merchant bank has not already done by virtue of paragraph 4); and

(b) record adequate details of the wire transfer so as to permit its reconstruction, including at least the date of the wire transfer, the type and amount of currency involved, the value date and the details of the wire transfer beneficiary and the beneficiary institution.

(II) Cross-border Wire Transfers exceeding S$2,000

9.4 In a cross-border wire transfer where the amount to be transferred exceeds S$2,000, every merchant bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer:

(a) the name of the wire transfer originator;

(b) the wire transfer originator's account number (or unique reference number assigned by the ordering institution where no account number exists); and

(c) the wire transfer originator's address, unique identification number, or date and place of birth.

(III) Other Wire Transfers

9.5 In any other types of wire transfers, every merchant bank that is an ordering institution shall either:

(a) include in the message or payment instruction that accompanies or relates to the wire transfer all of the originator information required to be included as if the transaction had been a cross-border wire transfer exceeding S$2,000; or

(b) include only the originator's account number (or unique reference number where no account number exists) but be in a position to make the remaining originator information available within 3 working days of a request being made by the beneficiary institution.

Responsibility of the beneficiary institution

9.6 Every merchant bank that is a beneficiary institution shall implement appropriate risk-based policies, procedures and controls for identifying and handling in-coming wire transfers that are not accompanied by complete originator information.

Responsibility of Intermediary Institution

9.7 Every merchant bank that is an intermediary institution shall, in passing onward the message or payment instruction, maintain all the required originator information with the wire transfer.

10 RECORD KEEPING

10.1 Every merchant bank shall prepare, maintain and retain documentation on all its business relations and transactions with its customers such that:

(a) all requirements imposed by law (including this Notice) are met;

(b) any transaction undertaken by the merchant bank can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) the relevant competent authorities in Singapore and the internal and external auditors of the merchant bank are able to review the merchant bank's transactions and assess the level of compliance with this Notice; and

(d) the merchant bank can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities in Singapore for information.

10.2 Subject to paragraph 10.4 and any other requirements imposed by law, every merchant bank shall, when setting its record retention policies, comply with the following document retention periods:

(a) a period of at least 6 years following the termination of business relations for customer identification information, and other documents relating to the establishment of business relations, as well as account files and business correspondence; and

(b) a period of at least 6 years following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

10.3 Every merchant bank may retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

10.4 The merchant bank shall retain records pertaining to a matter which is under investigation or which has been the subject of an STR for such longer period as may be necessary in accordance with any request or order from STRO or other relevant competent authorities.

11 SUSPICIOUS TRANSACTIONS REPORTING

11.1 Every merchant bank shall keep in mind the provisions in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act[4] and in the Terrorism (Suppression of Financing) Act that provide for the reporting to the competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to STRO via STRs; and

(b) keep records of all transactions so referred to STRO, together with all internal findings and analysis done in relation to them.

11.2 The merchant bank shall submit reports on suspicious transactions, including attempted transactions to STRO, and extend a copy to the Authority for information.

11.3 The merchant bank shall consider if the circumstances are suspicious so as to warrant the filing of a STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, and document the basis for its determination where:

(a) the merchant bank is for any reason unable to complete CDD measures; or

(b) the customer is reluctant, unable or unwilling to provide any information requested by the merchant bank, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

12 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

[4] Please note in particular section 48 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act on tipping-off.

12.1 Every merchant bank shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees.

12.2 The policies, procedures and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and suspicious transactions and the obligation to make suspicious transaction reports.

12.3 The merchant bank shall take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favour anonymity, in formulating its policies, procedures and controls.

Group Policy

12.4 Every merchant bank that is incorporated in Singapore shall develop a group policy on AML/CFT and extend this to all of its branches and subsidiaries outside Singapore.

12.5 Where a merchant bank has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the merchant bank for itself or notified to merchant banks generally by the Authority or by other foreign regulatory authorities), the merchant bank shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

12.6 Where the AML/CFT requirements in the host country or jurisdiction differ from that in Singapore, the merchant bank shall require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

12.7 Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is thereby unable to fully observe the higher standard, the merchant bank's head office shall report this to the Authority and comply with such further directions as may be given by the Authority.

Compliance

12.8 Every merchant bank shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT compliance officer.

12.9 Every merchant bank shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information which they require to discharge their functions.

Audit

12.10 Every merchant bank shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the merchant bank's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

12.11 Every merchant bank shall have in place screening procedures to ensure high standards when hiring employees.

Training

12.12 Every merchant bank shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are regularly trained on:

(a) AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and terrorist financing; and

(c) the merchant bank's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

Annex 5

MAS 314

Date;

NOTICE TO INSURERS
INSURANCE ACT, CAP. 142

(MAS 314 dated 11 Nov 2002 is cancelled)

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 64 of the Insurance Act (Cap 142) and applies to all life insurers in Singapore.

2 DEFINITIONS

2.1 For the purposes of this Notice:

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

"beneficial owner", in relation to a customer of a life insurer, means any individual who has a level of control over the policy, or entitlement to, the proceeds of the policy that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the policy. The ability to fund the policy or the entitlement to the proceeds of the policy alone, however, without corresponding authority to control, manage or direct the policy (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner;

"company" includes a body corporate formed or established outside Singapore under the corporations law of a country or jurisdiction;

"CDD" or "customer due diligence" means the process of identifying the customer and obtaining information required by paragraph 4;

"customer" in relation to a life insurer, means

(a) 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; or

(b) the person for whom the life insurer undertakes or intends to undertake any transaction without a policy being issued;

"FATF" means the Financial Action Task Force;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law, but does not include a company that is wholly owned or controlled by a government;

"STR" means suspicious transaction report; and

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

2.2 A reference to business relations, in relation to a life insurer and a person, is a reference to the issuance by the life insurer of a life insurance policy to that person.

2.3 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

2.4 A reference to the completion of CDD measures is a reference to the situation when the life insurer has received satisfactory responses to all inquiries.

2.5 A reference to a transaction includes a reference to the provision of advice.

2.6 Unless the context otherwise requires, a reference to a financial institution supervised by the Authority does not include a reference to any person exempted from licensing by or registration with the Authority.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all life insurers in the conduct of their operations and business activities:

(a) A life insurer must exercise due diligence when dealing with customers and other persons in the course of business.

(b) A life insurer must conduct its business in conformity with high ethical standards, and guard against undertaking any transaction that is or may be connected with or may facilitate money laundering or terrorist financing.

(c) A life insurer should, whenever possible and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore in preventing money laundering and terrorist financing.

4 CUSTOMER DUE DILIGENCE

General

4.1 No life insurer shall deal with any person on an anonymous basis or any person using a fictitious name.

When CDD measures are to be performed

4.2 Every life insurer shall perform CDD measures in accordance with this Notice when:

(a) the life insurer establishes business relations with any customer;

(b) the life insurer undertakes any transaction of a value exceeding S$20,000 for any customer who has not otherwise established business relations with the life insurer;

(c) there is a suspicion of money laundering or terrorist financing, notwithstanding that the life insurer would otherwise not be required by this Notice to do so; or

(d) the life insurer has any doubt about the veracity or adequacy of any information previously obtained.

CDD Measures where Business Relations are Established

(I) Identification of Customers

4.3 Every life insurer shall establish the identity of each customer who applies to the life insurer to establish business relations.

4.4 For the purpose of the preceding paragraph, a life insurer shall obtain and record information of the customer, including but not limited to the following:

(a) Full name, including any aliases;

(b) Unique identification number (such as an identity card number, birth certificate number, or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

(d) Date of birth, incorporation or registration (as may be appropriate); and

(e) Nationality or place of incorporation or registration (as may be appropriate).

4.5 Where the customer is a company, the life insurer shall, apart from identifying the customer, also establish the identity of all the directors of the company in the like manner as if such persons were themselves customers.

4.6 Where the customer is a sole proprietorship, the life insurer shall, apart from identifying the customer, also establish the identity of the sole proprietor in the like manner as if the sole proprietor were a customer in his own name.

4.7 Where the customer is a partnership or limited liability partnership, the life insurer shall, apart from identifying the customer, also establish the identity of all partners in the like manner as if such persons were themselves customers.

4.8 Where the customer is any other body corporate or unincorporated, the life insurer shall, apart from identifying the customer, also establish the identity of the persons having executive authority in that body corporate or unincorporated in the like manner as if such persons were themselves customers.

(II) Verification of Identity

4.9 The life insurer shall verify the identity of the customer using reliable, independent sources.

4.10 The life insurer shall retain copies of all reference documents used in identity verification and the identification information.

(III) Identification and verification of identity of representatives

4.11 Where the customer appoints one or more natural persons to act on his behalf or the customer is not a natural person, a life insurer shall:

(a) establish the identity of the natural persons that act or are appointed to act on behalf of the customer, in the like manner as if such persons were themselves customers; and

(b) verify the identity of these persons using reliable, independent sources.

4.12 The life insurer shall verify the due authority of such persons to act on behalf of the customer.

4.13 Without limiting the generality of the preceding paragraph, the life insurer shall verify the due authority of such persons to act by obtaining:

(a) appropriate documentary evidence that the customer has appointed the persons to act on its behalf, and

(b) the specimen signatures of the persons appointed.

4.14 Where the customer is a Singapore government entity, the life insurer shall only

be required to obtain such information as may be required to confirm that the customer is a Singapore government entity as asserted.

(IV) Identification and Verification of Identity of Beneficial Owners

4.15 Every life insurer shall inquire if there exists any beneficial owner in relation to a customer.

4.16 Where there is one or more beneficial owners in relation to a customer, the life insurer shall take reasonable measures to obtain information sufficient to establish and verify the identities of the beneficial owners.

4.17 A life insurer shall not be required to inquire if there exists any beneficial owner in relation to a customer that is:

(a) a Singapore government entity;

(b) a foreign government entity;

(c) a public company listed on the Singapore Exchange;

(d) a public company listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements;

(e) a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority); or

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

unless the life insurer suspects that the transaction is connected with money laundering or terrorist financing.

4.18 For the purposes of paragraph 4.17(f), the life insurer shall document the basis for its determination that the requirements in that paragraph have been duly met.

(V) Identification and verification of payee

4.19 Every life insurer intending to make any of the following types of payment to a person other than the customer of the life insurer shall, before doing so, establish the identity of the payee and verify his identity in the like manner as if the payee were a customer:

(a) payment of the sum assured (or part thereof) upon the occurrence of the risk insured against in accordance with the life insurance policy;

(b) payment of the surrender value of a life insurance policy;

(c) refund of premium upon the avoidance, cancellation and/or termination of any life insurance policy;

(d) refund of any other payment made in relation to any life insurance policy.

(VI) <u>On-going monitoring</u>

4.20 Every life insurer shall monitor on an ongoing basis, its business relations with customers.

4.21 A life insurer shall, during the course of business relations, observe the conduct of the customer's life insurance policy, scrutinise transactions undertaken to ensure that the transactions are consistent with the life insurer's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

4.22 Every life insurer shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. As far as possible, a life insurer shall inquire into the background and purpose of such transactions and document their findings with a view to making this information available to the relevant competent authorities should the need arise.

(VII) <u>Periodic Review of Identification Information</u>

4.23 Every life insurer shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up-to-date, particularly for higher risk categories of customers.

Non Face-to-Face Verification

4.24 Every life insurer shall assess the risk of money laundering or terrorist financing posed by any activity that does not involve face-to-face contact with its customer, and implement appropriate policies and procedures to address these risks.

4.25 Where there is no face-to-face contact, the life insurer shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

Reliance on identification and verification already performed

4.26 When a life insurer ("acquiring life insurer") acquires, either in whole or in part, the business of another financial institution (whether in Singapore or elsewhere), the acquiring life insurer shall perform CDD measures on customers acquired with the business at the time of acquisition, except where the acquiring life insurer has:

(a) acquired at the same time all corresponding customer records (including customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and

(b) conducted due diligence enquiries and such enquiries have not raised any doubt on the part of the acquiring life insurer as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring life insurer.

CDD Measures for Non-Policy Holders

4.27 Every life insurer that undertakes any transaction of a value exceeding S$20,000 for any customer who does not otherwise have business relations with the life insurer shall:

(a) establish and verify the identity of the customer in the like manner as if the customer had applied to the life insurer to establish business relations; and

(b) record adequate details of the transaction so as to permit the reconstruction of the transaction, including at least the nature and date of the transaction, the type and amount of currency involved, the value date, and the details of the payee or beneficiary.

4.28 Where a life insurer suspects that two or more transactions are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for in this Notice, the life insurer shall treat the transactions as a single transaction and aggregate their values for the purpose of this Notice.

Deferring the completion of CDD measures

4.29 Subject to paragraph 4.30 of this Notice, a life insurer shall complete CDD measures:

(a) (other than the CDD measures to be performed on a payee) before it establishes business relations; or

(b) before the life insurer undertakes any transaction for a customer, where the customer does not have business relations with the life insurer.

4.30 A life insurer may establish business relations with a customer before completing the CDD measures if:

(a) the deferral of completion of CDD measures is essential in order not to interrupt the normal conduct of business operations; and

(b) the risks of money laundering and terrorist financing can be effectively managed by the life insurer.

4.31 Where the life insurer establishes business relations before completion of CDD measures, the life insurer shall complete the CDD measures as soon as reasonably practicable.

4.32 Where the life insurer is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.

Existing customers

4.33 A life insurer shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.

5 SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1 Subject to paragraph 5.2, a life insurer may perform such simplified CDD measures as it considers adequate to effectively identify and verify the identity of the customer and any beneficial owner if it is satisfied that the risks of money laundering and terrorist financing are low.

5.2 The life insurer shall not perform simplified CDD measures in relation to customers that are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the life insurer for itself or notified to life insurers generally by the Authority or by other foreign regulatory authorities.

5.3 A life insurer may perform simplified CDD measures in relation to a customer that is a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority).

5.4 Where the life insurer performs simplified CDD measures in relation to a customer, it shall document:

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

6 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

6.1 For the purposes of paragraph 6:

"politically exposed person" means:

(a) a natural person who is or has been entrusted with prominent public functions in a foreign country;

(b) immediate family members of such a person; or

(c) close associates of such a person.

"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil servants, senior judicial or military officials, senior executives of state owned corporations, and senior political party officials.

6.2 Every life insurer shall, in addition to performing the CDD measures specified in paragraph 4, perform enhanced CDD measures in relation to politically exposed persons, including but not limited to the following:

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person;

(b) obtain approval from the life insurer's senior management to establish or continue business relations, where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person;

(c) establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer or beneficial owner; and

(d) conduct, during the course of business relations, enhanced monitoring of business relations with the customer.

Other Higher Risk Categories

6.3 The life insurer shall perform the enhanced CDD measures in paragraph 6.2 for such other categories of customers, business relations or transactions as the life insurer may assess to present a higher risk for money laundering and terrorist financing.

6.4 Every life insurer shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the life insurer for itself or

notified to life insurers generally by the Authority or other foreign regulatory authorities.

7 PERFORMANCE OF CUSTOMER DUE DILIGENCE BY INTERMEDIARIES

7.1 Subject to paragraph 7.2, a life insurer may rely on an intermediary to perform the CDD measures in paragraph 4 of this Notice if the following requirements are met:

(a) the life insurer is satisfied that each intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;

(b) the intermediary is not one on which life insurers have been specifically precluded by the Authority from relying;

(c) the information that the life insurer would be required or would want to obtain which is being obtained by the intermediary may be relayed to the life insurer by the intermediary without any delay; and

(d) the intermediary is able and willing to provide, without delay, upon the life insurer's request, any document obtained by the intermediary which the life insurer would be required or would want to obtain.

7.2 The life insurer shall not rely on an intermediary to conduct ongoing monitoring of customers.

7.3 Where the life insurer does rely on an intermediary, it shall document the basis for its satisfaction that the requirements in paragraph 7.1(a) have been met except where the intermediary is a financial institution supervised by the Authority (other than a moneychanger or remittance business).

7.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the life insurer shall remain responsible for its AML/CFT obligations in this Notice.

8 RECORD KEEPING

8.1 Every life insurer shall prepare, maintain and retain documentation on all its business relations and transactions with its customers, such that:

(a) all requirements imposed by law (including this Notice) are met;

(b) any transaction undertaken by the life insurer can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) the relevant competent authorities in Singapore and the internal and external auditors of the life insurer are able to assess the life insurer's transactions and level of compliance with this Notice; and

(d) the life insurer can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities in Singapore for information.

8.2 Subject to paragraph 8.4 and any other requirements imposed by law, every life insurer shall, when setting its record retention policies, comply with the following document retention periods:

(a) a period of at least 6 years following the termination of business relation for customer identification information, and other documents relating to the establishment of business relations, as well as policy files and business correspondence; and

(b) a period of at least 6 years following the completion of the transaction for records relating to other transactions, including any information needed to explain and reconstruct the transaction.

8.3 Every life insurer may retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

8.4 The life insurer shall retain records pertaining to a matter which is under investigation or which has been the subject of an STR for such longer period as may be necessary in accordance with any request or order from STRO or from other the relevant competent authorities.

9 SUSPICIOUS TRANSACTIONS REPORTING

9.1 Every life insurer shall keep in mind the provisions in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act[5] and in the Terrorism (Suppression of Financing) Act that provide for the reporting to the competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to STRO via STRs.

(b) keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them.

9.2 The life insurer shall submit reports on suspicious transactions, including attempted transactions to STRO, and extend a copy to the Authority for information.

9.3 The life insurer shall consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, and document the basis for its determination where:

(a) the life insurer is for any reason unable to complete CDD measures; or

(b) the customer is, reluctant, unable or unwilling to provide any information requested by the life insurer, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

[5] Please note in particular section 48 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act on tipping-off.

10 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

10.1 Every life insurer shall develop and maintain internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees.

10.2 The procedures, policies and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and suspicious transactions and the obligation to make suspicious transaction reports.

10.3 The life insurers shall take into consideration money laundering and terrorist financing threats that may arise from new or developing technologies, especially those that favour anonymity, in formulating its policies, procedures and controls.

Group Policy

10.4 Every life insurer that is incorporated in Singapore shall develop a group policy on AML/CFT and extend this to all of its branches and subsidiaries, outside Singapore.

10.5 Where a life insurer has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the life insurer for itself or notified to life insurer generally by the Authority or by other foreign regulatory authorities), the life insurer shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

10.6 Where the AML/CFT requirements in the host country or jurisdiction differ from those in Singapore, the life insurer shall require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

10.7 Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the life insurer's head office shall report this to the Authority and comply with such further directions as may be given by the Authority.

Compliance

10.8 Every life insurer shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT compliance officer.

10.9 Every life insurer shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist the compliance officer, has timely access to all customer records and other relevant information which they require to discharge their functions.

Audit

10.10 Every life insurer shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the life insurer's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

10.11 Every life insurer shall have in place screening to ensure high standards when hiring employees.

Training

10.12 Every life insurer shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are regularly trained on:

(a) AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and terrorist financing; and

(c) the life insurer's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

Annex 6

SFA 04-N02

Date;

NOTICE TO CAPITAL MARKETS SERVICES LICENCEES AND PERSONS EXEMPTED 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 LICENSE

SECURITIES AND FUTURES ACT (CAP. 289)

(SFA 04–N02 dated 11 November 2002 is cancelled)

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 101 of the Securities and Futures Act (Cap. 289) and applies to all holders of a Capital Markets Services license, and all persons exempted 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 license.

2 DEFINITIONS

2.1 For the purposes of this Notice:

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

"beneficial owner", in relation to a customer of a capital market intermediary, means any individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, however,

without corresponding authority to control, manage or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner;

"company" includes a body corporate formed or established outside Singapore under the corporations law of a country or jurisdiction;

"CDD" or "customer due diligence" means the process of identifying the customer and obtaining information required by paragraph 4;

"CMI" or "capital markets intermediary" means a person holding a Capital Markets Services license or a person exempted from having to hold such a license 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;

"customer", in relation to a CMI, means the person in whose name an account is opened or intended to be opened, or for whom a CMI undertakes or intends to undertake any transaction without an account being opened;

"FATF" means the Financial Action Task Force;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law, but does not include a company that is wholly owned or controlled by a government;

"STR" means suspicious transaction report; and

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

2.2 A reference to business relations, in relation to a CMI and a person, is a reference to the opening or maintenance of an account by the CMI in the name of that person and the undertaking of transactions by the CMI for that person on that account.

2.3 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

2.4 A reference to the completion of CDD measures is a reference to the situation when the CMI has received satisfactory responses to all inquiries.

2.5 A reference to a transaction includes a reference to the provision of advice.

2.6 Unless the context otherwise requires, a reference to a financial institution supervised by the Authority does not include a reference to any person exempted from licensing by or registration with the Authority.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all CMIs in the conduct of their operations and business activities:

(a) A CMI must exercise due diligence when dealing with customers and other persons in the course of business.

(b) A CMI must conduct its business in conformity with high ethical standards, and guard against undertaking any transaction that is or may be connected with or may facilitate money laundering or terrorist financing.

(c) A CMI should, whenever possible and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore in preventing money laundering and terrorist financing.

4 CUSTOMER DUE DILIGENCE

General

4.1 No CMI shall open or maintain anonymous accounts or accounts in fictitious names.

4.2 In the case of a joint account, a CMI shall perform CDD measures on all joint account holders as if each of them were individually customers of the CMI.

When CDD measures are to be performed

4.3 Every CMI shall perform CDD measures in accordance with this Notice when:

(a) the CMI establishes business relations with any person;

(b) the CMI undertakes any transaction of a value exceeding S$20,000 for any customer who has not otherwise established business relations with the CMI;

(c) there is a suspicion of money laundering or terrorist financing, notwithstanding that the CMI would otherwise not be required by this Notice to perform CDD measures; or

(d) the CMI has any doubt about the veracity or adequacy of any information previously obtained.

CDD Measures where Business Relations are Established

(I) Identification of Customers

4.4 Every CMI shall establish the identity of each customer who applies to the CMI to establish business relations.

4.5 For the purpose of the preceding paragraph, a CMI shall obtain and record information of the customer, including but not limited to the following:

(a) Full name, including any aliases;

(b) Unique identification number (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

(d) Date of birth, incorporation or registration (as may be appropriate); and

(e) Nationality or place of incorporation or registration (as may be appropriate).

4.6 Where the customer is a company, the CMI shall, apart from identifying the customer, also establish the identity of all the directors of the company in the like manner as if such persons were themselves customers.

4.7 Where the customer is a sole proprietorship, the CMI shall, apart from identifying the customer, also establish the identity of the sole proprietor in the like manner as if the sole proprietor were a customer in his own name.

4.8 Where the customer is a partnership or a limited liability partnership, the CMI shall, apart from identifying the customer, also establish the identity of all the partners in the like manner as if such persons were themselves customers.

4.9 Where the customer is any other body corporate or unincorporate, the CMI shall, apart from identifying the customer, also establish the identity of the persons having executive authority in that body corporate or unincorporate in the like manner as if such persons were themselves customers.

(II) Verification of Identity

4.10 The CMI shall verify the identity of the customer using reliable, independent sources.

4.11 The CMI shall retain copies of all reference documents used in identity verification and the identification information.

(III) Identification and verification of identity of representatives

4.12 Where the customer appoints one or more natural persons to act on his behalf or the customer is not a natural person, a CMI shall:

(a) establish the identity of the natural persons that act or are appointed to act on behalf of the customer, in the like manner as if such persons were themselves customers; and

(b) verify the identity of these persons using reliable, independent sources.

4.13 The CMI shall verify the due authority of such persons to act on behalf of the customer.

4.14 Without limiting the generality of the preceding paragraph, the CMI shall verify the due authority of such persons to act by obtaining:

(a) appropriate documentary evidence that the customer has appointed the persons to act on its behalf; and

(b) the specimen signatures of the persons appointed.

4.15 Where the customer is a Singapore government entity, the CMI shall only be required to obtain such information as may be required to confirm that the customer is a Singapore government entity as asserted.

(IV) Identification and Verification of Identity of Beneficial Owners

4.16 Every CMI shall inquire if there exists any beneficial owner in relation to a customer.

4.17 Where there is one or more beneficial owners in relation to a customer, the CMI shall take reasonable measures to obtain information sufficient to establish and verify the identities of the beneficial owners.

4.18 A CMI shall not be required to inquire if there exists any beneficial owner in relation to a customer that is:

(a) a Singapore government entity;

(b) a foreign government entity;

(c) a public company listed on the Singapore Exchange;

(d) a public company listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements;

(e) a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority); or

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF

unless the CMI suspects that the transaction is connected with money laundering or terrorist financing.

4.19 For the purposes of paragraph 4.18(f), the CMI shall document the basis for its determination that the requirements in that paragraph have been duly met.

(V) Information on the purpose and intended nature of business relations

4.20 When processing the application to establish business relations, every CMI shall obtain, from the customer, information as to the purpose and intended nature of business relations.

(VI) On-going monitoring

4.21 Every CMI shall monitor on an ongoing basis, its business relations with customers.

4.22 A CMI shall, during the course of business relations, observe the conduct of the customer's account and scrutinise transactions undertaken to ensure that the transactions are consistent with the CMI's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

4.23 Every CMI shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

4.24 A CMI shall, to the extent possible, inquire into the background and purpose of the transactions in paragraph 4.23 and document their findings with a view to making this information available to the relevant competent authorities should the need arise.

(VII) Periodic Review of Identification Information

4.25 Every CMI shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up-to-date, particularly for higher risk categories of customers.

Non Face-to-Face Verification

4.26 Every CMI shall assess the risks of money laundering or terrorist financing posed by any activity that does not involve face-to-face contact with its customer, and implement appropriate policies and procedures to address these risks.

4.27 Where there is no face-to-face contact, the CMI shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

Reliance on identification and verification already performed

4.28 When a CMI ("acquiring CMI") acquires, either in whole or in part, the business of another financial institution (whether in Singapore or elsewhere), the acquiring CMI shall perform CDD measures on customers acquired with the business at the time of acquisition except where the acquiring CMI has:

(a) acquired at the same time all corresponding customer records (including customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and

(b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring CMI as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring CMI.

CDD Measures for Non-Account Holders

4.29 Every CMI that undertakes any transaction of a value exceeding S$20,000 for any customer who does not otherwise have business relations with the CMI shall:

(a) establish and verify the identity of the customer in the like manner as if the customer had applied to the CMI to establish business relations; and

(b) record adequate details of the transaction so as to permit the reconstruction of the transaction, including at least the nature and date of the transaction, the type and amount of currency involved, the value date.

4.30 Where a CMI suspects that two or more transactions are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for in this Notice, the CMI shall treat the transactions as a single transaction and aggregate their values for the purpose of this Notice.

Deferring the completion of CDD measures

4.31 Subject to paragraph 4.32, a CMI shall complete CDD measures

(a) before the CMI establishes business relations; or

(b) before the CMI undertakes any transaction for a customer, where the customer does not have business relations with the CMI.

4.32 A CMI may establish business relations with a customer before completing the CDD measures if:

(a) the deferral of completion of CDD measures is essential in order not to interrupt the normal conduct of business operations; and

(b) the risks of money laundering and terrorist financing can be effectively managed by the CMI.

4.33 Where the CMI establishes business relations before completion of CDD measures, the CMI shall complete the CDD measures as soon as reasonably practicable.

4.34 Where the CMI is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.

Existing customers

4.35 A CMI shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.

5 SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1 Subject to paragraph 5.2, a CMI may perform such simplified CDD measures as it considers adequate to effectively identify and verify the identity of the customer and any beneficial owner if it is satisfied that the risks of money laundering or terrorist financing are low.

5.2 The CMI shall not perform simplified CDD measures in relation to customers that are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the CMI for itself or notified to CMIs generally by the Authority or by other foreign regulatory authorities.

5.3 A CMI may perform simplified CDD measures in relation to a customer that is a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority).

5.4 Where the CMI performs simplified CDD measures in relation to a customer, it shall document -

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

6 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

6.1 For the purposes of paragraph 6:

"politically exposed person" means:

(a) a natural person who is or has been entrusted with prominent public functions in a foreign country;

(b) immediate family members of such a person; or

(c) close associates of such a person.

"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil servants, senior judicial or

military officials, senior executives of state owned corporations, and senior political party officials.

6.2 Every CMI shall, in addition to performing the CDD measures specified in paragraph 4, perform enhanced CDD measures in relation to politically exposed persons, including but not limited to the following:

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person;

(b) obtain approval from the CMI's senior management to establish or continue business relations, where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person;

(c) establish, by appropriate and reasonable means, the source of wealth and source of funds of any customer or beneficial owner; and

(d) conduct, during the course of business relations, enhanced monitoring of business relations with the customer.

Other Higher Risk Categories

6.3 The CMI shall perform the enhanced CDD measures in paragraph 6.2 for such other categories of customers, business relations or transactions as the CMI may assess to present a higher risk for money laundering and terrorist financing.

6.4 Every CMI shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the CMI for itself or notified to CMIs generally by the Authority or other foreign regulatory authorities.

7 PERFORMANCE OF CUSTOMER DUE DILIGENCE BY INTERMEDIARIES

7.1 Subject to paragraph 7.2, a CMI may rely on an intermediary to perform the CDD measures in paragraph 4 of this Notice if the following requirements are met:

(a) the CMI is satisfied that each intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements

consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;

(b) the intermediary is not one on which CMIs have been specifically precluded by the Authority from relying;

(c) the information that the CMI would be required or would want to obtain which is being obtained by the intermediary, may be relayed to the CMI by the intermediary without any delay; and

(d) the intermediary is able and willing to provide, without delay, upon the CMI's request, any document obtained by the intermediary, which the CMI would be required or would want to obtain.

7.2 The CMI shall not rely on an intermediary to conduct ongoing monitoring of customers.

7.3 Where a CMI does rely on an intermediary, it shall document the basis for its satisfaction that the requirements in paragraph 7.1(a) have been met except where the intermediary is a financial institution supervised by the Authority (other than a money changer or remittance business).

7.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the CMI shall remain responsible for its AML/CFT obligations in this Notice.

8 RECORD KEEPING

8.1 Every CMI shall prepare, maintain and retain documentation on all its business relations and transactions with its customers such that:

(a) all requirements imposed by law (including this Notice) are met;

(b) any transaction undertaken by the CMI can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) the relevant competent authorities in Singapore and the internal and external auditors of the CMI are able to assess the CMI's transactions and level of compliance with this Notice; and

(d) the CMI can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities in Singapore for information.

8.2 Subject to paragraph 8.4 and any other requirements imposed by law, every CMI shall, when setting its record retention policies, comply with the following document retention periods:

(a) a period of at least 6 years following termination of business relation for customer identification information, and other documents relating to the establishment of business relations, as well as account files and business correspondence; and

(b) at least 6 years following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

8.3 Every CMI may retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

8.4 The CMI may retain records pertaining to a matter which is under investigation or which has been the subject of an STR for such longer period as may be necessary in accordance with any request or order from STRO or from other relevant competent authorities.

9 SUSPICIOUS TRANSACTIONS REPORTING

9.1 Every CMI shall keep in mind the provisions in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act[6] and in the Terrorism (Suppression of Financing) Act that provide for the reporting to the competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being

[6] Please note in particular section 48 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act on tipping-off.

connected with money-laundering or terrorist financing, for possible referral to STRO via STRs; and

(b) keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them.

9.2 The CMI shall submit reports on suspicious transactions, including attempted transactions to STRO, and extend a copy to the Authority for information.

9.3 The CMI shall consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, and document the basis for its determination where:

(a) the CMI is for any reason unable to complete CDD measures; or

(b) the customer is reluctant, unable or unwilling to provide any information requested by the CMI, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

10 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

10.1 Every CMI shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees.

10.2 The procedures, policies and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and suspicious transactions and the obligation to make suspicious transaction reports.

10.3 The CMI shall take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favour anonymity, in formulating its policies, procedures and controls.

Group Policy

10.4 Every CMI that is incorporated in Singapore shall develop a group policy on AML/CFT and extend this to all of its branches and subsidiaries outside Singapore.

10.5 Where a CMI has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the CMI for itself or notified to CMIs generally by the Authority or by other foreign regulatory authorities), the CMI shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

10.6 Where the AML/CFT requirements in the host country or jurisdiction differ from that in Singapore, the CMI shall require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

10.7 Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the CMI's head office shall report this to the Authority and comply with such further directions as may be given by the Authority.

Compliance

10.8 Every CMI shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT compliance officer.

10.9 Every CMI shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information which they require to discharge their functions.

Audit

10.10 Every CMI shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the CMI's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

10.11 Every CMI shall have in place screening procedures to ensure high standards when hiring employees.

Training

10.12 Every CMI shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are regularly trained on:

(a) AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and terrorist financing; and

(c) the CMI's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

Annex 7

FAA-N06

Date;

NOTICE TO FINANCIAL ADVISERS
FINANCIAL ADVISERS ACT, CAP. 110

(MAS Notice No. FAA-N06 dated 11 November 2002 is cancelled)

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 58 of the Financial Advisers Act (Cap 110) and applies to all licensed financial advisers and exempt persons under Regulation 27(1)(d) of the Financial Advisers Regulations, other than when they only provide advice by means of issuing research analyses and reports concerning any investment product.

2 DEFINITIONS

2.1 For the purposes of this Notice:

"AML/CFT" means anti-money laundering and countering financing of terrorism;

"beneficial owner", in relation to a customer of a financial adviser, means any individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, however, without corresponding authority to control, manage or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner;

"company" includes a body corporate formed or established outside Singapore

under the corporations law of a country or jurisdiction;

"CDD" or "customer due diligence" means the process of identifying the customer and obtaining information required by paragraph 4;

"customer", in relation to a financial adviser, means 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;

"FATF" means the Financial Action Task Force;

"financial adviser" means a licensed financial adviser or exempt person under Regulation 27(1)(d) of the FAR, other than those which only provide advice by means of issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law, but does not include a company that is wholly owned or controlled by a government;

"STR" means suspicious transaction report; and

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

2.2 A reference to business relations, in relation to a financial adviser and a person, is a reference to the opening or maintenance of an account by the financial adviser in the name of that person and the undertaking of transactions by the financial adviser for that person on that account.

2.3 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

2.4 A reference to the completion of CDD measures is a reference to the situation when the financial adviser has received satisfactory responses to all inquiries.

2.5 A reference to a transaction includes a reference to the provision of advice.

2.6 Unless the context otherwise requires, a reference to a financial institution supervised by the Authority does not include a reference to any person exempted from licensing by or registration with the Authority.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all financial advisers in the conduct of their operations and business activities:

(a) A financial adviser must exercise due diligence when dealing with customers and other persons in the course of business.

(b) A financial adviser must conduct its business in conformity with high ethical standards, and guard against undertaking any transaction that is or may be connected with or may facilitate money laundering or terrorist financing.

(c) A financial adviser should, whenever possible and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore in preventing money laundering and terrorist financing.

4 CUSTOMER DUE DILIGENCE

General

4.1 No financial adviser shall open or maintain anonymous accounts or accounts in fictitious names.

4.2 In the case of a joint account, a financial adviser shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the financial adviser.

When CDD measures are to be performed

4.3 Every financial adviser shall perform CDD measures in accordance with this Notice when:

(a) the financial adviser establishes business relations with any customer;

(b) the financial adviser undertakes any transaction of a value exceeding S$20,000 for any customer who has not otherwise established business relations with the financial adviser;

(c) there is a suspicion of money laundering or terrorist financing, notwithstanding that the financial adviser would otherwise not be required by this Notice to perform CDD measures; or

(d) the financial adviser has any doubt about the veracity or adequacy of any information previously obtained.

CDD Measures where Business Relations are Established

(I) Identification of Customers

4.4 Every financial adviser shall establish the identity of each customer who applies to the financial adviser to establish business relations.

4.5 For the purpose of the preceding paragraph, a financial adviser shall obtain and record information of the customer, including but not limited to the following:

(a) Full name, including any aliases;

(b) Unique identification number (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

(d) Date of birth, incorporation or registration (as may be appropriate); and

(e) Nationality or place of incorporation or registration (as may be appropriate).

4.6 Where the customer is a company, the financial adviser shall, apart from identifying the customer, also establish the identity of all the directors of the company in the like manner as if such persons were themselves customers.

4.7 Where the customer is a sole proprietorship, the financial adviser shall, apart from identifying the customer, also establish the identity of the sole proprietor in the like manner as if the sole proprietor were a customer in his own name.

4.8 Where the customer is a partnership or a limited liability partnership, the financial adviser shall, apart from identifying the customer, also establish the identity of all the partners in the like manner as if such persons were themselves customers.

4.9 Where the customer is any other body corporate or unincorporate, the financial adviser shall, apart from identifying the customer, also establish the identity of the persons having executive authority in that body corporate or unincorporate in the like manner as if such persons were themselves customers.

(II) Verification of Identity

4.10 The financial adviser shall verify the identity of the customer using reliable, independent sources.

4.11 The financial adviser shall retain copies of all reference documents used in identity verification and the identification information.

(III) Identification and verification of identity of representatives

4.12 Where the customer appoints one or more natural persons to act on his behalf or the customer is not a natural person, a financial adviser shall:

(a) establish the identity of the natural persons that act or are appointed to act on behalf of the customer, in the like manner as if such persons were themselves customers; and

(b) verify the identity of these persons using reliable, independent sources.

4.13 The financial adviser shall verify the due authority of such persons to act on behalf of the customer.

4.14 Without limiting the generality of the preceding paragraph, the financial adviser shall verify the due authority of such persons to act by obtaining:

(a) appropriate documentary evidence that the customer has appointed the persons to act on its behalf, and

(b) the specimen signatures of the persons appointed.

4.15 Where the customer is a Singapore government entity, the financial adviser shall only be required to obtain such information as may be required to confirm that the customer is a Singapore government entity as asserted.

(IV) Identification and Verification of Identity of Beneficial Owners

4.16 Every financial adviser shall inquire if there exists any beneficial owner in relation to a customer.

4.17 Where there is one or more beneficial owners in relation to a customer, the financial adviser shall take reasonable measures to obtain information sufficient to establish and verify the identities of the beneficial owners.

4.18 A financial adviser shall not be required to inquire if there exists any beneficial owner in relation to a customer that is:

(a) a Singapore government entity;

(b) a foreign government entity;

(c) a public company listed on the Singapore Exchange;

(d) a public company listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements;

(e) a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority); or

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF,

unless the financial adviser suspects that the transaction is connected with money laundering or terrorist financing.

4.19 For the purposes of paragraph 4.18(f), the financial adviser shall document the

basis for its determination that the requirements in that paragraph have been duly met.

(V) Information on the purpose and intended nature of business relations

4.20 When processing the application to establish business relations, every financial adviser shall obtain, from the customer, information as to the purpose and intended nature of business relations.

(VI) On-going monitoring

4.21 Every financial adviser shall monitor on an ongoing basis, its business relations with customers.

4.22 A financial adviser shall, during the course of business relations, observe the conduct of the customer's account and scrutinise transactions undertaken to ensure that the transactions are consistent with the financial adviser's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

4.23 Every financial adviser shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

4.24 A financial adviser shall, to the extent possible, inquire into the background and purpose of the transactions in paragraph 4.23 and document their findings with a view to making this information available to the relevant competent authorities should the need arise.

(VII) Periodic Review of Identification Information

4.25 Every financial adviser shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up-to-date, particularly for higher risk categories of customers.

Non Face-to-Face Verification

4.26 Every financial adviser shall assess the risks of money laundering or terrorist financing posed by any activity that does not involve face-to-face contact with its

customer, and implement appropriate policies and procedures to address these risks.

4.27 Where there is no face-to-face contact, the financial adviser shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

Reliance on identification and verification already performed

4.28 When a financial adviser ("acquiring financial adviser") acquires, either in whole or in part, the business of another financial institution (whether in Singapore or elsewhere), the acquiring financial adviser shall perform CDD measures on the customers acquired with the business at the time of acquisition except where the acquiring financial adviser has:

(a) acquired at the same time all corresponding customer records (including customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and

(b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring financial adviser as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring financial adviser.

Deferring the completion of CDD measures

4.29 Subject to paragraph 4.30 of this Notice, a financial adviser shall complete CDD measures:

(a) before the financial adviser establishes the business relations; or

(b) before the financial adviser undertakes any transaction for a customer, where the customer does not have business relations with the financial adviser.

4.30 A financial adviser may establish business relations with a customer before completing CDD measures if:

(a) the deferral of completion of CDD measures is essential in order not to interrupt the normal conduct of business operations; and

(b) the risks of money laundering and terrorist financing can be effectively managed by the financial adviser.

4.31 Where the financial adviser establishes business relations before completion of CDD measures, the financial adviser shall complete the CDD measures as soon as reasonably practicable.

4.32 Where the financial adviser is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.

Existing customers

4.33 A financial adviser shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.

5 SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1 Subject to paragraph 5.2, a financial adviser may perform such simplified CDD measures as it considers adequate to effectively identify and verify the identity of the customer and any beneficial owner if it is satisfied that the risks of money laundering and terrorist financing are low.

5.2 The financial adviser shall not perform simplified CDD measures in relation to customers that are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the financial adviser for itself or notified to financial advisers generally by the Authority or by other foreign regulatory authorities.

5.3 A financial adviser may perform simplified CDD measures in relation to a customer that is a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority).

5.4 Where the financial adviser performs simplified CDD measures in relation to a customer, it shall document -

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

6 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

6.1 For the purposes of paragraph 6:

"politically exposed person" means:

(a) a natural person who is or has been entrusted with prominent public functions in a foreign country;

(b) immediate family members of such a person; or

(c) close associates of such a person.

"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil servants, senior judicial or military officials, senior executives of state owned corporations, and senior political party officials.

6.2 Every financial adviser shall, in addition to performing the CDD measures specified in paragraph 4, perform enhanced CDD measures in relation to politically exposed persons, including but not limited to the following:

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person;

(b) obtain approval from the financial adviser's senior management to establish or continue business relations where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person;

(c) establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer or beneficial owner; and

(d) conduct, during the course of business relations, enhanced monitoring of business relations with the customer.

Other Higher Risk Categories

6.3 The financial adviser shall perform the enhanced CDD measures in paragraph 6.2 for such other categories of customers, business relations or transactions as the financial adviser may assess to present a higher risk for money laundering and terrorist financing.

6.4 Every financial adviser shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the financial adviser for itself or notified to financial advisers generally by the Authority or other foreign regulatory authorities.

7 PERFORMANCE OF CUSTOMER DUE DILIGENCE BY INTERMEDIARIES

7.1 Subject to paragraph 7.2, a financial adviser may rely on an intermediary to perform the CDD measures in paragraph 4 of this Notice if the following requirements are met:

(a) the financial adviser is satisfied that the intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;

(b) the intermediary is not one on which financial advisers have been specifically precluded by the Authority from relying;

(c) the information that the financial adviser would be required or would want to obtain which is being obtained by the intermediary may be relayed to the financial adviser by the intermediary without any delay; and

(d) the intermediary is able and willing to provide, without delay, upon the financial adviser's request, any document obtained by the intermediary which the financial adviser would be required or would want to obtain.

7.2 The financial adviser shall not rely on an intermediary to conduct ongoing

monitoring of customers.

7.3 Where a financial adviser does rely on an intermediary, it shall document the basis for its satisfaction that the requirements in paragraph 7.1(a) have been met except where the intermediary is a financial institution supervised by the Authority (other than a money changer or remittance business).

7.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the financial adviser shall remain responsible for its AML/CFT obligations in this Notice.

8 RECORD KEEPING

8.1 Every financial adviser shall prepare, maintain and retain documentation on all its business relations and transactions with its customers such that:

(a) all requirements imposed by law (including this Notice) are met;

(b) any transaction undertaken by the financial adviser can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) the relevant competent authorities in Singapore and the internal and external auditors of the financial adviser are able to assess the financial adviser's transactions and level of compliance with this Notice; and

(d) the financial adviser can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities in Singapore for information.

8.2 Subject to paragraph 8.1 and any other requirements imposed by law, every financial adviser shall, when setting its record retention policies, comply with the following document retention periods:

(a) a period of at least 6 years following the termination of business relation for customer identification information, and other documents relating to the establishment of business relations, as well as account files and business correspondence; and

(b) a period of at least 6 years following the completion of the transaction for

records relating to a transaction, including any information needed to explain and reconstruct the transaction.

8.3 Every financial adviser may retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

8.4 The financial adviser shall retain records pertaining to a matter which is under investigation or which has been the subject of an STR for such longer period as may be necessary in accordance with any request or order from STRO or from other relevant competent authorities.

9 SUSPICIOUS TRANSACTIONS REPORTING

9.1 Every financial adviser shall keep in mind the provisions in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act[7] and in the Terrorism (Suppression of Financing) Act that provide for the reporting to the competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to STRO via STRs; and

(b) keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them.

9.2 The financial adviser shall submit reports on suspicious transactions, including attempted transactions to STRO, and extend a copy to the Authority for information.

9.3 The financial adviser shall consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, and document the

[7] Please note in particular section 48 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act on tipping-off.

basis for its determination where:

(a) the financial adviser is for any reason unable to complete CDD measures; or

(b) the customer is reluctant, unable or unwilling to provide any information requested by the financial adviser, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

10 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

10.1 Every financial adviser shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees.

10.2 The procedures, policies and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and suspicious transactions and the obligation to make suspicious transaction reports.

10.3 The financial adviser shall take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favour anonymity, in formulating its policies, procedures and controls.

Group Policy

10.4 Every financial adviser that is incorporated in Singapore shall develop a group policy on AML/CFT and extend this to all of its branches and subsidiaries outside Singapore.

10.5 Where a financial adviser has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the financial adviser for itself or notified to financial advisers generally by the Authority or by other foreign regulatory authorities), the financial adviser shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

10.6 Where the AML/CFT requirements in the host country or jurisdiction differ from those in Singapore, the financial adviser shall require that the overseas branch

or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

10.7 Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the financial adviser's head office shall report this to the Authority and comply with such further directions as may be given by the Authority.

Compliance

10.8 Every financial adviser shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT compliance officer.

10.9 Every financial adviser shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information which they require to discharge their functions.

Audit

10.10 Every financial adviser shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the financial adviser's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

10.11 Every financial adviser shall have in place screening procedures to ensure high standards when hiring employees.

Training

10.12 Every financial adviser shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are regularly trained on:

(a) AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and

terrorist financing; and

(c) the financial adviser's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

Annex 8

SFA13-N01

Date;

NOTICE TO APPROVED TRUSTEES
SECURITIES AND FUTURES ACT, CAP. 289

(SFA 13-N01 dated 11 July 2003 is cancelled)

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to sections 101 and 293 of the Securities and Futures Act (Cap 289) and applies to all trustees for collective investment schemes which are authorised under section 289 and constituted as unit trusts (hereinafter "approved trustees").

2 DEFINITIONS

2.1 For the purposes of this Notice:

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

"company" includes a body corporate formed or established outside Singapore under the corporations law of a country or jurisdiction;

"CDD" or "customer due diligence" means the process of identifying the customer and obtaining information required by paragraph 4;

"customer", in relation to an approved trustee, means the fund manager or other person with whom the approved trustee deals with in the course of its operations as an approved trustee.

"FATF" means the Financial Action Task Force;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law, but does not include a company that is wholly owned or controlled by a government;

"STR" means suspicious transaction report; and

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

2.2 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

2.3 A reference to the completion of CDD measures is a reference to the situation when the approved trustee has received satisfactory responses to all inquiries.

2.4 A reference to a transaction includes a reference to the provision of advice.

2.5 Unless the context otherwise requires, a reference to a financial institution supervised by the Authority does not include a reference to any person exempted from licensing by or registration with the Authority.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all approved trustees in the conduct of their operations and business activities:

(a) an approved trustee must exercise due diligence when dealing with customers and other persons in the course of business;

(b) an approved trustee must conduct its business in conformity with high ethical standards, and guard against undertaking any transaction that is or may be connected with or may facilitate money laundering or terrorist financing;

(c) an approved trustee should, whenever possible and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore in preventing money laundering and terrorist financing.

4 CUSTOMER DUE DILIGENCE

General

4.1 No approved trustee shall deal with any person on an anonymous basis or any person using a fictitious name.

When CDD measures are to be performed

4.2 Every approved trustee shall perform CDD measures in accordance with this Notice when:

(a) the approved trustee establishes business relations with any customer;

(b) there is a suspicion of money laundering or terrorist financing, notwithstanding that the approved trustee would otherwise not be required by this Notice to perform CDD measures; or

(c) the approved trustee has any doubt about the veracity or adequacy of any information previously obtained.

CDD Measures where Business Relations are Established

(I) Identification of Customers

4.3 Every approved trustee shall establish the identity of each customer who applies to the approved trustee to establish business relations.

4.4 For the purpose of the preceding paragraph, an approved trustee shall obtain and record information of the customer, including but not limited to the following :

(a) Full name, including any aliases;

(b) Unique identification number (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

(d) Date of birth, incorporation or registration (as may be appropriate); and

(e) Nationality or place of incorporation or registration (as may be appropriate).

4.5 Where the customer is a company, the approved trustee shall, apart from identifying the customer, also establish the identity of all the directors of the company in the like manner as if such persons were themselves customers.

4.6 Where the customer is a sole proprietorship, the approved trustee shall, apart from identifying the customer, also establish the identity of the sole proprietor in the like manner as if the sole proprietor were a customer in his own name.

4.7 Where the customer is a partnership or a limited liability partnership, the approved trustee shall, apart from identifying the customer, also establish the identity of all the partners in the like manner as if such persons were themselves customers.

4.8 Where the customer is any other body corporate or unincorporate, the approved trustee shall, apart from identifying the customer, also establish the identity of the persons having executive authority in that body corporate or unincorporate in the like manner as if such persons were themselves customers.

(II) Verification of Identity

4.9 The approved trustee shall verify the identity of the customer using reliable, independent sources.

4.10 The approved trustee shall retain copies of all reference documents used in identity verification and the identification information.

(III) Identification and verification of identity of representatives

4.11 Where the customer appoints one or more natural persons to act on his behalf or the customer is not a natural person, an approved trustee shall:

(a) establish the identity of the natural persons that act or are appointed to act on behalf of the customer, in the like manner as if such persons were themselves customers; and

(b) verify the identity of these persons using reliable, independent sources.

4.12 The approved trustee shall also verify the due authority of such persons to act on behalf of the customer.

(IV) Identification and Verification of Identity of Beneficial Owners

4.13 Every approved trustee shall inquire if there exists any beneficial owner in relation to a customer.

4.14 Where there is one or more beneficial owners in relation to a customer, the approved trustee shall take reasonable measures to obtain information sufficient to establish and verify the identities of the beneficial owners.

4.15 An approved trustee shall not be required to inquire if there exists any beneficial owner in relation to a customer that is:

(a) a Singapore government entity;

(b) a foreign government entity;

(c) a public company listed on the Singapore Exchange;

(d) a public company listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements;

(e) a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority); or

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF,

unless the approved trustee suspects that a transaction is connected with money laundering or terrorist financing.

4.16 For the purposes of paragraph 4.15(f), the approved trustee shall document the basis for its determination that the requirements in that paragraph have been duly met.

(V) Information on the purpose and intended nature of business relations

4.17 When processing the application to establish business relations, every approved trustee shall obtain, from the customer, information as to the purpose and intended nature of business relations.

(VI) On-going monitoring

4.18 Every approved trustee shall monitor on an ongoing basis, its business relations with customers.

4.19 An approved trustee shall, during the course of business relations, observe the conduct of the customer's account and scrutinise transactions undertaken to ensure that the transactions are consistent with the approved trustee's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

4.20 Every approved trustee shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

4.21 An approved trustee shall, to the extent possible, inquire into the background and purpose of the transactions in paragraph 4.23 and document their findings with a view to making this information available to the relevant competent authorities should the need arise.

(VII) Periodic Review of Identification Information

4.22 Every approved trustee shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up-to-date, particularly for higher risk categories of customers.

Non Face-to-Face Verification

4.23 Every approved trustee shall assess the risks of money laundering or terrorist financing posed by any activity that does not involve face-to-face contact with its customer, and implement appropriate policies and procedures to address these risks.

4.24 Where there is no face-to-face contact, the approved trustee shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

Reliance on identification and verification already performed

4.25 When an approved trustee ("acquiring approved trustee") acquires, either in whole or in part, the business of another approved trustee or financial institution (whether in Singapore or elsewhere), the acquiring approved trustee shall perform CDD measures on customers acquired with the business at the time of acquisition except where the acquiring approved trustee has:

(a) acquired at the same time all corresponding customer records (including customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and

(b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring approved trustee as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring approved trustee.

Time for completion of CDD measures

4.26 Unless and until an approved trustee is able to complete CDD measures in relation to a customer, it shall not undertake any transaction with that customer.

4.27 If the approved trustee is, for any reason, unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.

Existing customers

4.28 An approved trustee shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.

5 SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1 Subject to paragraph 5.2, an approved trustee may perform such simplified CDD measures as it considers adequate to effectively identify and verify the identity of the customer and any beneficial owner if it is satisfied that the risks of money laundering or terrorist financing are low.

5.2 The approved trustee shall not perform simplified CDD measures in relation to customers that are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the approved trustee for itself or notified to approved trustees generally by the Authority or by other foreign regulatory authorities.

5.3 An approved trustee may perform simplified CDD measures in relation to a customer that is a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority).

5.4 Where the approved trustee performs simplified CDD measures in relation to a customer, it shall document:

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

6 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

6.1 For the purposes of paragraph 6,

"politically exposed person" means:

(a) a natural person who is or has been entrusted with prominent public functions in a foreign country;

(b) immediate family members of such a person; or

(c) close associates of such a person.

"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil servants, senior judicial or military officials, senior executives of state owned corporations, and senior political party officials.

6.2 Every approved trustee shall, in addition to performing the CDD measures specified in paragraph 4, perform enhanced CDD measures in relation to politically exposed persons, including but not limited to the following:

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person;

(b) obtain approval from the approved trustee's senior management to establish or continue business relations, where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person;

(c) establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer or beneficial owner; and

(d) the approved trustee shall, during the course of business relations, conduct enhanced monitoring of business relations with the customer.

Other Higher Risk Categories

6.3 The approved trustee shall perform enhanced measures specified in paragraph 6.2 for such other categories of customers, business relations or transactions as the approved trustee may assess to present a higher risk for money laundering and terrorist financing.

6.4 Every approved trustee shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have

inadequate AML/CFT measures, as determined by the approved trustee for itself or notified to approved trustee generally by the Authority or other foreign regulatory authorities.

7 PERFORMANCE OF CUSTOMER DUE DILIGENCE BY INTERMEDIARIES

7.1 Subject to paragraph 7.2, an approved trustee may rely on an intermediary to perform elements of the CDD measures in paragraph 4 of this Notice on its behalf, if the following requirements are met:

(a) the approved trustee is satisfied that each intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;

(b) the intermediary is not one on which approved trustees have been specifically precluded by the Authority from relying;

(c) the information that the approved trustee would be required or would want to obtain is now being obtained by the intermediary, may be relayed to the approved trustee by the intermediary without any delay; and

(d) the intermediary is able and willing to provide, without delay, upon the approved trustee's request, any document, obtained by the intermediary, which the approved trustee would be required or would want to obtain.

7.2 The approved trustee shall not rely on an intermediary to conduct ongoing monitoring of customers.

7.3 Where an approved trustee does rely on an intermediary, it shall document the basis for its determination that the requirements in paragraph 7.1(a) have been met except where the intermediary is a financial institution supervised by the Authority (other than a money changer or remittance business).

7.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the approved trustee shall remain responsible for its AML/CFT obligations in this Notice.

8 RECORD KEEPING

8.1 Every approved trustee shall prepare, maintain and retain documentation on all their business relations and transactions with its customers such that:

(a) all requirements imposed by law (including this Notice) are met;

(b) any transaction undertaken by the approved trustee can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) the relevant competent authorities in Singapore and the internal and external auditors of the approved trustee are able to assess the approved trustee's transactions and level of compliance with this Notice; and

(d) the approved trustee can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities in Singapore for information.

8.2 Subject to paragraph 8.4 and any other requirements imposed by law, every approved trustee shall, when setting its record retention policies, comply with the following document retention periods:

(a) a period of at least 6 years following termination of business relations for customer identification information, and other documents relating to the establishment of business relations, as well as account files and business correspondence.

(b) a period of at least 6 years following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

8.3 Every approved trustee may retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

8.4 The approved trustee shall retain records pertaining to a matter which is under investigation or which has been the subject of an STR for such longer period as may be necessary in accordance with any request or direction from STRO or from other relevant competent authorities.

9 SUSPICIOUS TRANSACTIONS REPORTING

9.1 Every approved trustee shall keep in mind the provisions in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act[8] and in the Terrorism (Suppression of Financing) Act that provide for the reporting to the competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to STRO via STRs; and

(b) keep records of all transactions so referred to STRO, together with all internal findings and analysis done in relation to them.

9.2 The approved trustee shall submit reports on suspicious transactions, including attempted transactions to STRO, and extend a copy to the Authority for information.

9.3 The approved trustee shall consider if the circumstances are suspicious so as to warrant the filing of a STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, and document the basis for its determination where:

(a) an approved trustee is for any reason unable to complete CDD measures; or

(b) the customer is reluctant, unable or unwilling to provide any information requested by the approved trustee, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

[8] Please note in particular section 48 of the Corruption, Drug Trafficking and Other serious Crimes (Confiscation of Benefits) Act on tipping-off.

10 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

10.1 Every approved trustee shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees.

10.2 The procedures, policies and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and suspicious transactions and the obligation to make suspicious transactions reports.

10.3 The approved trustee shall, take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favour anonymity, in formulating such policies, procedures and controls.

Group Policy

10.4 Every approved trustee that is incorporated in Singapore shall develop a group policy on AML/CFT and extend this to all of its branches and subsidiaries outside Singapore.

10.5 Where an approved trustee has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the approved trustee for itself or notified to approved trustees generally by the Authority or by other foreign regulatory authorities), the approved trustee shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

10.6 Where the AML/CFT requirements in the host country or jurisdiction differ from that in Singapore, the approved trustee shall require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

10.7 Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the approved trustee's head office shall report this to the Authority and comply with such further directions as may be given by the Authority.

Compliance

10.8 Every approved trustee shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT compliance officer.

10.9 Every approved trustee shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information which they require to discharge their functions.

Audit

10.10 Every approved trustee shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the approved trustee's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

10.11 Every approved trustee shall have in place screening procedures to ensure high standards when hiring employees.

Training

10.12 Every approved trustee shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are regularly trained on:

(a) AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and terrorist financing; and

(c) the approved trustee's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

Annex 9

TCA-N03

Date;

NOTICE TO TRUST COMPANIES
TRUST COMPANIES ACT 2005 (Act 11 of 2005)

PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 76 of the Trust Companies Act 2005 (Act 11 of 2005) and applies to all trust companies licensed under the Trust Companies Act and also to all private trust companies exempted from licensing under the Trust Companies Act (hereinafter "trust companies").

2 DEFINITIONS

2.1 For the purposes of this Notice:

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

"business contact", in relation to a trust company and a person, means any contact between the trust company and that person in the course of the provision of trust business services by the trust company, whether or not the trust company was engaged by that person;

"company" includes a body corporate formed or established outside Singapore under the corporations law of a country or jurisdiction;

"CDD" or "customer due diligence" means the process of identifying the trust relevant parties and obtaining information required by paragraph 4;

"effective controller", in relation to a trust relevant party, means any individual who has a level of control over the trust relevant party, that as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the trust relevant party;

"FATF" means the Financial Action Task Force;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law, but does not include a company that is wholly owned or controlled by a government;

"STR" means suspicious transaction report;

"STRO" means the Suspicious Transactions Reporting Office, Commercial Affairs Department of the Singapore Police Force; and

"trust relevant party", in relation to a trust, means any of the following:

(i) the settlor of the trust;

(ii) the trustee;

(iii) the beneficiaries;

(iv) any person who contributes property to be subject to the trust; or

(v) any person who has any power over the disposition of any property that is subject to the trust.

2.2 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

2.3 A reference to the completion of CDD measures is a reference to the situation when the trust company has received satisfactory responses to all inquiries.

2.4 A reference to a transaction includes a reference to the provision of advice.

2.5 Unless the context otherwise requires, a reference to a financial institution supervised by the Authority does not include a reference to any person exempted from licensing by or registration with the Authority.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all trust companies in the conduct of their operations and business activities:

(a) A trust company must exercise due diligence when dealing with trust relevant parties and other persons in the course of business.

(b) A trust company must conduct its business in conformity with high ethical standards, and guard against undertaking any transaction that is or may be connected with or may facilitate money laundering or terrorist financing.

(c) A trust company should, whenever possible and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore in preventing money laundering and terrorist financing.

4 CUSTOMER DUE DILIGENCE

General

4.1 No trust company shall deal with any person on an anonymous basis or any person using a fictitious name.

4.2 In the case of a trust relevant party that comprises two or more persons acting jointly, a trust company shall perform CDD measures on all of the persons as if each of them were individually trust relevant parties.

When CDD measures are to be performed

4.3 Every trust company shall perform CDD measures in accordance with this Notice when:

(a) the trust company comes into business contact with a trust relevant party;

(b) there is a suspicion of money laundering or terrorist financing, notwithstanding that the trust company would otherwise not be required by this Notice to perform CDD measures; or

(c) the trust company has any doubt about the veracity or adequacy of any information previously obtained.

CDD Measures where Business Contacts are Established

(I) Identification of Trust Relevant Parties

4.4 Every trust company shall establish the identity of each trust relevant party with whom the trust company comes into business contact as follows:

(a) in respect of the settlor of the trust, before the trust is constituted;

(b) in respect of every person who contributes property to be subject to the trust, before the property is transferred to the trustee to be held on trust;

(c) in respect of each beneficiary of the trust, as soon as practicable after the beneficiary becomes identifiable, and in any case before making a distribution to that beneficiary; and

(d) in respect of any other trust relevant party, as soon as practicable after the trust company first comes into business contact with that trust relevant party.

4.5 For the purpose of the preceding paragraph, a trust company shall obtain and record information of the trust relevant party, including but not limited to the following:

(a) Full name, including any aliases;

(b) Unique identification number (such as an identity card number, birth certificate number or passport number, or where the trust relevant party is not a natural person, the incorporation number or business registration number);

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

(d) Date of birth, incorporation or registration (as may be appropriate); and

(e) Nationality or place of incorporation or registration (as may be appropriate).

4.6 Where the trust relevant party is a company, the trust company shall, apart from identifying the trust relevant party, also establish the identity of all the directors of the company in the like manner as if such persons were themselves trust relevant parties.

4.7 Where the trust relevant party is a sole proprietorship, the trust company shall, apart from identifying the trust relevant party, also establish the identity of the sole proprietor in the like manner as if the sole proprietor were a trust relevant party in his own name.

4.8 Where the trust relevant party is a partnership or a limited liability partnership, the trust company shall, apart from identifying the trust relevant party, also establish the identity of all the partners in the like manner as if such persons were themselves trust relevant parties.

4.9 Where the trust relevant party is any other body corporate or unincorporate, the trust company shall, apart from identifying the trust relevant party, also establish the identity of the persons having executive authority in that body corporate or unincorporated in the like manner as if such persons were themselves trust relevant parties.

(II) Verification of Identity

4.10 The trust company shall verify the identity of the trust relevant party using reliable, independent sources.

4.11 The trust company shall retain copies of all reference documents used in identity verification and the identification information.

(III) Identification and verification of identity of representatives

4.12 Where a trust relevant party appoints one or more natural persons to act on his behalf or a trust relevant party is not a natural person, a trust company shall:

(a) establish the identity of the natural persons that act or are appointed to act on behalf of the trust relevant party, in the like manner as if such persons were themselves trust relevant parties; and

(b) verify the identity of these persons using reliable, independent sources.

4.13 The trust company shall verify the due authority of such persons to act on behalf of the trust relevant party.

4.14 Without limiting the generality of the preceding paragraph, the trust company shall verify the due authority of such persons to act by obtaining:

(a) appropriate documentary evidence that the trust relevant party has appointed the persons to act on its behalf; and

(b) the specimen signatures of the persons appointed.

4.15 Where the trust relevant party is a Singapore government entity, the trust company shall only be required to obtain such information as may be required to confirm that the trust relevant party is a Singapore government entity as asserted.

(IV) Identification and Verification of Identity of Effective Controllers

4.16 Every trust company shall inquire if there exists any effective controller in relation to a trust relevant party who is a settlor, a trustee or a person who contributes property to be subject to the trust.

4.17 Where there is one or more effective controllers in relation to a trust relevant party, the trust company shall take reasonable measures to obtain information sufficient to establish and verify the identities of the effective controllers.

4.18 A trust company shall not be required to inquire if there exists any effective controller in relation to a trust relevant party that is:

(a) a Singapore government entity;

(b) a foreign government entity;

(c) a public company listed on the Singapore Exchange;

(d) a public company listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements;

(e) a financial institution supervised by the Authority (other than a money changer or remittance business; unless specifically notified by the Authority); or

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF,

unless the trust company suspects that the transaction is connected with money laundering or terrorist financing.

4.19 For the purposes of paragraph 4.18(f), the trust company shall document the basis for its determination that the requirements in that paragraph have been duly met.

(V) Information on the purpose and intended nature of business contacts

4.20 When processing the application to establish business contacts, every trust company shall obtain, from the trust relevant party, information as to the purpose and intended nature of business contacts.

(VI) On-going monitoring

4.21 Every trust company shall monitor on an ongoing basis, its business contacts with trust relevant parties.

4.22 A trust company shall, to the fullest extent practicable and within the scope of the trust business services being provided to the trust relevant party and the obligations being assumed by the trust company, scrutinise transactions undertaken to ensure that the transactions are consistent with the trust company's knowledge of the trust relevant party, its business and risk profile and where appropriate, the source of funds.

4.23 Every trust company shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

4.24 A trust company shall, to the extent possible, inquire into the background and purpose of the transactions in paragraph 4.23 and document their findings with a view to making this information available to the relevant competent authorities should the need arise.

(VII) Periodic Review of Identification Information

4.25 Every trust company shall periodically review the adequacy of identification information obtained in respect of trust relevant parties and effective controllers and ensure that the information is kept up-to-date, particularly for higher risk categories of trust relevant parties.

4.26 Without limiting the generality of the preceding paragraph, a trust company shall review the adequacy of identification information in the event that:

(a) there is a change in the terms of the trust;

(b) the trust company encounters a transaction that does not appear to the trust company to have been made at arms' length; or

(c) any property that is subject to the trust appears to have been acquired at an over-value or disposed of at an under-value.

Non-Face to Face Contact

4.27 Every trust company shall assess the risks of money laundering or terrorist financing posed by any activity that does not involve face-to-face contact with its trust relevant party, and implement appropriate policies and procedures to address these risks.

4.28 Where there is no face-to-face contact, the trust company shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

Reliance on identification and verification already performed

4.29 When a trust company ("acquiring trust company") acquires, either in whole or in part, the business of another trust company or financial institution (whether in Singapore or elsewhere), the acquiring trust company shall perform CDD measures on trust relevant parties acquired with the business at the time of acquisition except where the acquiring trust company has:

(a) acquired at the same time all corresponding records of the trust relevant party (including identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and

(b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring trust company as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring trust company.

Existing trust relevant parties

4.30 A trust company shall perform such CDD measures as may be appropriate to its existing trust relevant parties having regard to its own assessment of materiality and risk.

5 SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1 Subject to paragraph 5.2, a trust company may perform such simplified CDD measures as it considers adequate to effectively identify and verify the identity of a trust relevant party and any effective controller if it is satisfied that the risks of money laundering or terrorist financing are low.

5.2 The trust company shall not perform simplified CDD measures in relation to trust relevant parties that are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the trust company for itself or notified to trust companies generally by the Authority or by other foreign regulatory authorities.

5.3 A trust company may perform simplified CDD measures in relation to a trust relevant party that is a financial institution supervised by the Authority (other than a money changer or remittance business, unless specifically notified by the Authority).

5.4 Where the trust company performs simplified CDD measures in relation to a trust relevant party, it shall document:

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

6 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

6.1 For the purposes of paragraph 6:

"politically exposed person" means:

(a) a natural person who is or has been entrusted with prominent public functions in a foreign country;

(b) immediate family members of such a person; or

(c) close associates of such a person.

"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil servants, senior judicial or military officials, senior executives of state owned corporations, and senior political party officials.

6.2 Every trust company shall, in addition to performing the CDD measures specified in paragraph 4, perform enhanced CDD measures in relation to politically exposed persons, including but not limited to the following:

(a) implement appropriate internal policies, procedures and controls to determine if a trust relevant party or an effective controller is a politically exposed person;

(b) obtain approval from the trust company's senior management to establish or continue business contacts where a trust relevant party or effective controller is a politically exposed person or subsequently becomes a politically exposed person;

(c) establish, by appropriate and reasonable means, the source of wealth and source of funds of the trust relevant party or effective controller; and

(d) conduct, during the course of business contacts, enhanced monitoring of business contacts with the trust relevant party.

Other Higher Risk Categories

6.3 The trust company shall perform the enhanced CDD measures specified in the preceding paragraphs for such other categories of trust relevant parties or transactions as the trust company may assess to present a higher risk for money laundering and terrorist financing.

6.4 Every trust company shall give particular attention to business contacts and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the trust company for itself or notified to trust companies generally by the Authority or other foreign regulatory authorities.

7 PERFORMANCE OF CUSTOMER DUE DILIGENCE BY INTERMEDIARIES

7.1 Subject to paragraph 7.2, a trust company may rely on an intermediary to perform elements of the CDD process set out in paragraph 4 of this Notice if the following requirements are met:

(a) the trust company is satisfied that each intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;

(b) the intermediary is not one on which trust companies have been specifically precluded by the Authority from relying;

(c) the information that the trust company would be required or would want to obtain which is being obtained by the intermediary may be relayed to the trust company by the intermediary without any delay; and

(d) the intermediary is able and willing to provide, without delay, upon the trust company's request, any document obtained by the intermediary which the trust company would be required or would want to obtain.

7.2 The trust company shall not rely on an intermediary to conduct ongoing monitoring of trust relevant parties.

7.3 Where a trust company does rely on an intermediary, it shall document the basis for its determination that the requirements in paragraph 7.1(a) have been met except where the intermediary is a financial institution supervised by the Authority (other than a money changer or remittance business).

7.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the trust company shall remain responsible and accountable to the Authority for its AML/CFT obligations in this Notice.

8 RECORD-KEEPING

8.1 Every trust company shall prepare, maintain and retain documentation on all their business contacts with its trust relevant parties such that:

(a) all requirements imposed by law (including this Notice) are met;

(b) any transaction undertaken by the trust company can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) the relevant competent authorities in Singapore and the internal and external auditors of the trust company are able to assess the trust company's transactions and level of compliance with this Notice; and

(d) the trust company can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities in Singapore for information.

8.2 Subject to paragraph 8.4 and any other requirements imposed by law, every trust company shall, when setting its record retention policies, comply with the following document retention periods:

(a) a period of at least 6 years following the completion or termination of the entire trust business service for which the trust company was engaged, in relation to identification information, and other documents relating to the provision of trust business services, as well as account files and business correspondence; and

(b) a period of at least 6 years following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

8.3 Every trust company may retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

8.4 The trust company shall retain records pertaining to a matter which is under investigation or which has been the subject of an STR for such longer period as may be necessary in accordance with any request or direction from STRO or from other relevant competent authorities.

9 SUSPICIOUS TRANSACTIONS REPORTING

9.1 Every trust company shall keep in mind the provisions in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act[9] and in the Terrorism (Suppression of Financing) Act that provide for the reporting to the competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to STRO via STRs; and

(b) keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them.

[9] Please note in particular section 48 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act on tipping-off.

9.2 The trust company shall submit reports on suspicious transactions, including attempted transactions to STRO, and extend a copy to the Authority for information.

9.3 The trust company shall consider if the circumstances are suspicious so as to warrant the filing of an STR in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, and document the basis for its determination where:

(a) the trust company is for any reason unable to complete CDD measures; or

(b) the trust relevant party is reluctant, unable or unwilling to provide any information requested by the trust company or decides to terminate business contact with the trust company.

10 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

10.1 Every trust company shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees.

10.2 These procedures, policies and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and suspicious transactions and the obligation to make suspicious transaction reports.

10.3 The trust company shall take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favour anonymity, in formulating its policies, procedures and controls.

Group Policy

10.4 Every trust company that is incorporated in Singapore shall develop a group policy on AML/CFT and extend this to all of its branches and subsidiaries outside Singapore.

10.5 Where a trust company has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the trust company for itself or notified to trust companies generally by the

Authority or by other foreign regulatory authorities), the trust company shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

10.6 Where the AML/CFT requirements in the host country or jurisdiction differ from that in Singapore, the trust company shall require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

10.7 Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the trust company's head office shall report this to the Authority and comply with such further directions as may be given by the Authority.

Compliance

10.8 Every trust company shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT compliance officer.

10.9 Every trust company shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, has timely access to all records and other relevant information which they require to discharge their functions.

Audit

10.10 Every trust company shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the trust company's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

10.11 Every trust company shall have in place screening procedures to ensure high standards when hiring employees.

Training

10.12 Every trust company shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are regularly trained on:

(a) AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and terrorist financing; and

(c) the trust company's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

Monetary Authority of Singapore