HONG KONG MONETARY AUTHORITY
香港金融管理局

Our ref : B10/1C
B1/15C

9 July 2010

The Chief Executive
All authorized institutions

Dear Sir/Madam,

Amendments to Guideline on Prevention of Money Laundering and Supplement to the Guideline on Prevention of Money Laundering

I am writing to inform you that, following the consultation with the industry, the HKMA has amended the Guideline on Prevention of Money Laundering (Guideline) and the Supplement to the Guideline on Prevention of Money Laundering (Supplement) to address the issues raised in the Financial Action Task Force (FATF)'s Mutual Evaluation Report and to better reflect international standards. The major amendments are discussed below.

Supplement

Address verification

The HKMA's current Supplement includes address as an integral component of an individual's identity for verification purposes. As a result, AIs need to verify the address of the direct customer as well as all connected parties (i.e. account signatories, directors, principal shareholders, etc) which is unnecessarily onerous.

After considering the FATF's requirements and the international practices, we have decided that AIs should record and verify the address of direct customer. For connected parties and transactions undertaken by non-account holders, AIs should record the address of these parities and determine the need to verify their addresses on the basis of risk and materiality. Paragraph 3.3 and IN 5 have been amended accordingly.

55th Floor, Two International Finance Centre,
8 Finance Street, Central, Hong Kong
Website: www.hkma.gov.hk

香港中環金融街8號國際金融中心2期55樓
網址：www.hkma.gov.hk

Non-account holder transactions

The existing Supplement does not spell out the requirements on conducting transactions for non-account holders. To provide a clear guidance, we have inserted paragraphs 3.9 to 3.16 to spell out the requirements on conducting non-account holders' transactions in particular on wire transfers and currency exchange transactions.

Verification of identity of directors

The existing Supplement requires the identification of all directors and verification of at least two. The FATF requires identification of directors and reasonable measures to verify the identity of beneficial owners and controllers.

After careful consideration, we have amended paragraph 4.5 of the Supplement to require AIs to verify one director and consider the need to verify the identity of additional directors on the basis of risk and materiality.

Reliance on intermediaries

The FATF requires reliance on intermediaries that are supervised and regulated for AML/CFT purposes. Taking into account Hong Kong's situation and the proposals in the consultation document on the new legislation, the Supplement has been amended to allow reliance on a domestic lawyer, auditor, accountant, trust company or chartered secretary if AIs are satisfied that the domestic intermediary has appropriate customer due diligence systems in place. For overseas intermediaries, reliance is allowed on those that are from an equivalent jurisdiction and are regulated and supervised for compliance with FATF requirements.

Guideline

We have taken this opportunity to update the Guideline mainly to delete those sections that have been superseded by the Supplement.

Please refer to ***Annex 1*** and ***Annex 2*** for the revised Guideline and Supplement respectively. They were published in the Government Gazette today and will be effective on 1 November 2010.

If there are any questions relating to this letter, please feel free to contact Mr Andrew Clayton on 2878-1095 or Ms Sophia Lam on 2878-8281.

Yours faithfully,

Trevor Keen
Acting Executive Director (Banking Conduct)

c.c. The Chairman, The Hong Kong Association of Banks
The Chairman, The DTC Association
FSTB (Attn: Angelina Kwan)

Encl.

GUIDELINE ON PREVENTION OF MONEY LAUNDERING

A Guideline issued by the Monetary Authority under section 7(3) of the Banking Ordinance

CONTENTS

Revised July 2010

ANNEXES

Annex 1	Repealed~~Members of Financial Action Task Force~~
Annex 2	Repealed~~Stock market of a country which is a member of FATF and which is a stock market recognised by the Securities and Futures Commission for the purposes of section 65A(2)(a) of the Securities Ordinance~~
Annex 3	Repealed~~Intermediary Introduction Certificate~~
Annex 4	Repealed~~SWIFT Broadcast of 30 July 1992~~
Annex 5	Examples of Suspicious Transactions
Annex 6	Standard format for reporting suspicious transaction to Joint Financial Intelligence Unit (JFIU)
Annex 7	Example of acknowledgement of receipt by JFIU of suspicious transaction reporting
Annex 8	Repealed~~Particulars to be recorded for any remittance or money changing transaction undertaken for a non-account holder for an amount of HK$20,000 or more or of an equivalent amount in any other currency~~

PART I

OVERVIEW

1. Introduction

1.1 This Guideline incorporates, and hence supersedes, the Guideline issued by the Monetary Authority in July 1993 on the prevention of criminal use of the banking system for the purposes of money laundering. This Guideline has been updated to take account of the enactment of the Organized and Serious Crimes Ordinance, the subsequent amendments to the money laundering provisions in that Ordinance and the Drug Trafficking (Recovery of Proceeds) Ordinance, the stocktaking review of the anti-money laundering measures undertaken by the Financial Action Task Force and the UK Money Laundering Guidance Notes for banks and building societies. It has also included other refinements and additional examples of suspicious transactions.

1.2 This Guideline applies directly to all banking and deposit taking activities in Hong Kong carried out by authorized institutions. However, institutions are expected to ensure that their subsidiaries in Hong Kong also have effective controls in place to combat money laundering. Where Hong Kong incorporated institutions have branches or subsidiaries overseas, steps should be taken to alert management of such overseas offices to Group policy in relation to money laundering. Where a local jurisdiction has a money laundering law, branches and subsidiaries of Hong Kong incorporated institutions operating within that jurisdiction should, as a minimum, act in accordance with the requirements of the local law. Where the local law and the Guideline are in conflict, the foreign branch or subsidiary should comply with the local law and inform the Head Office immediately of any departure from Group policy.

1.3 It is recognized that the relevance and usefulness of this Guideline will need to be kept under review as the methods of money laundering are constantly evolving. It may be necessary to issue amendments to this Guideline from time to time to incorporate measures to combat new money laundering threats, including those inherent in new or developing technologies that might favour anonymity.

2. What is money laundering?

2.1 The phrase "money laundering" covers all procedures to change the identity of illegally obtained money so that it appears to have originated from a legitimate source.

2.2 Cash lends anonymity to many forms of criminal activity and is the normal medium of exchange in the world of drug trafficking. This gives rise to three common factors -

(a) criminals need to conceal the true ownership and origin of the money;

(b) they need to control the money; and

(c) they need to change the form of the money.

2.3 One of the most common means of money laundering that institutions will encounter on a day-to-day basis takes the form of accumulated cash transactions which will be deposited in the banking system or exchanged for value items. These simple transactions may be just one part of the sophisticated web of complex transactions which are set out and illustrated below. Nevertheless, the basic fact remains that the key stage for the detection of money laundering operations is where the cash first enters the financial system.

Stages of money laundering

2.4 There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert an institution to criminal activity -

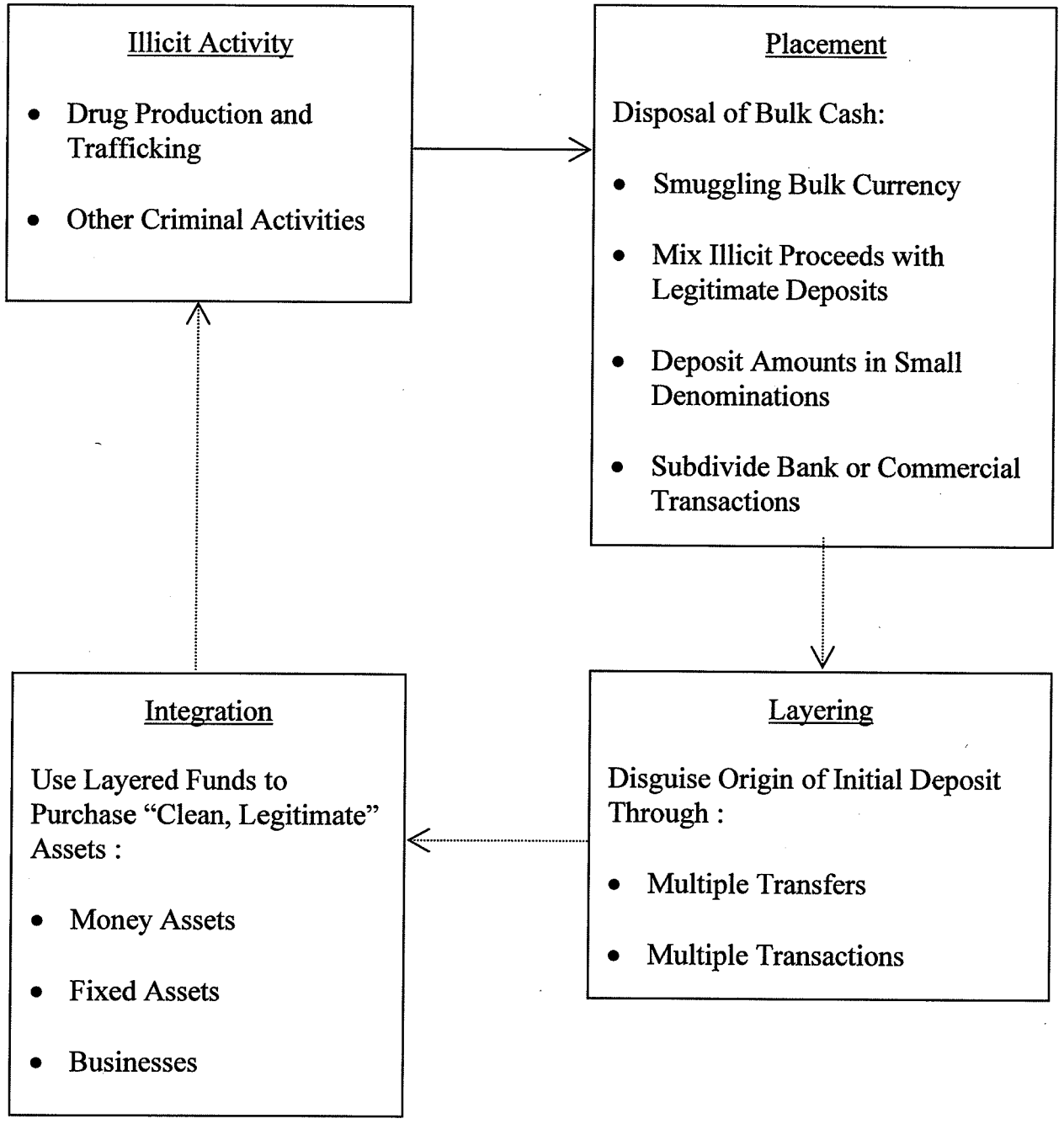
(a) Placement - the physical disposal of cash proceeds derived from illegal activity.

(b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

(c) Integration - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

2.5 The following chart illustrates the laundering stages in more detail.

PROCESS OF MONEY LAUNDERING



3. The legislation on money laundering in Hong Kong

3.1 Legislation has been developed in Hong Kong to address the problems associated with the laundering of proceeds from drug trafficking and serious crimes. The Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP) came into force in September 1989. It provides for the tracing, freezing and confiscation of the proceeds of drug trafficking and creates a criminal offence of money laundering in relation to such proceeds.

3.2 The Organized and Serious Crimes Ordinance (OSCO), which was modelled on the DTROP, was brought into operation in December 1994. It extends the money laundering offence to cover the proceeds of indictable offences in addition to drug trafficking.

3.3 Amendments to both Ordinances were made and came into effect on 1 September 1995. These amendments have tightened the money laundering provisions in both Ordinances and have a significant bearing on the duty to report suspicious transactions. In particular, there is now a clear statutory obligation to disclose knowledge or suspicion of money laundering transactions.

3.4 The key money laundering provisions in the two Ordinances are summarized below. This does not constitute a legal interpretation of the provisions of the legislation referred to, for which appropriate legal advice should be sought where necessary.

3.5 Section 25(1) of DTROP and OSCO creates the offence of dealing with any property, knowing or having reasonable grounds to believe it in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence respectively. The offence carries a maximum sentence of 14 years' imprisonment and a maximum fine of HK$5 million.

3.6 It is a defence under section 25(2) of both Ordinances for a person to prove that he intended to disclose as soon as is reasonable such knowledge, suspicion or matter to an authorized officer[1] or has a reasonable excuse for his failure to make a disclosure in accordance with section 25A(2) of the Ordinances.

3.7 Section 25A(1) imposes a statutory duty on a person, who knows or suspects that any property in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence, or was or is intended to be used in that connection, to make a disclosure to an authorized officer. Section 25A(7) makes it an offence for a person to fail to make such disclosure. The offence carries a maximum penalty of a fine at level 5 (at present $25,001 to $50,000) and imprisonment for 3 months.

---

1 As defined in section 2 of both the DTROP and OSCO, authorized officer means:
(a) any police officer;
(b) any member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342); and
(c) any other person authorized in writing by the Secretary for Justice for the purposes of this Ordinance.

3.8 It should be noted that section 25(4) of OSCO provides that references to an indictable offence in section 25 and 25A include a reference to conduct which would constitute an indictable offence if it had occurred in Hong Kong. That is to say it shall be an offence for a person to deal with the proceeds of crime or fail to make the necessary disclosure under section 25A(1) even if the principal crime is not committed in Hong Kong provided that it would constitute an indictable offence if it had occurred in Hong Kong.

3.9 Section 25A(2) provides that if a person who has made the necessary disclosure does any act in contravention of section 25(1) and the disclosure relates to that act he does not commit an offence if -

(a) the disclosure is made before he does that act and the act is done with the consent of an authorized officer; or

(b) the disclosure is made after the person does the act and the disclosure is made on the person's own initiative and as soon as it is reasonable for him to make it.

3.10 Section 25A(3) provides that disclosure made under section 25A(1) shall not be treated as breach of contract or of any enactment restricting disclosure of information and shall not render the person making the disclosure liable in damages for any loss arising out of disclosure. Therefore, institutions need not fear breaching their duty of confidentiality owed to customers when making a disclosure under the Ordinances.

3.11 Section 25A(4) extends the provisions of section 25A to disclosures made by an employee to an appropriate person in accordance with the procedures established by his employer for the making of such disclosure in the same way as it applies to disclosures to an authorized officer. This provides protection to employees of authorized institutions against the risk of prosecution where they have reported knowledge or suspicion of money laundering transactions to the person designated by their employers.

3.12 A "tipping-off" offence is created under section 25A(5) of both Ordinances, under which a person commits an offence if knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice an investigation into money laundering activities. The "tipping-off" offence carries a maximum penalty of three years' imprisonment and a fine of HK$500,000.

3.13 The Organized and Serious Crimes (Amendment) Ordinance 2000 ("OSCAO") came into operation on 1 June 2000. Among other things, OSCAO requires remittance agents and money changers to keep records of customers' identity and particulars of remittance and exchange transactions of HK$~~20~~8,000 or more or of an equivalent amount in any other currency. Although authorized institutions are exempted from the requirements of OSCAO, similar customer identification and record keeping requirements should be adopted to ensure that the anti-money laundering standards of the banking sector are in line with the overall Government policy to combat money laundering activities.

4. Basic policies and principles to combat money laundering

4.1 The Monetary Authority fully subscribes to the basic policies and principles to combat money laundering as embodied in the Statement of Principles issued by the Basle Committee in December 1988. The Statement seeks to deny use of the banking system to those involved in money laundering by application of the following principles -

(a) Know your customer: banks should make reasonable efforts to determine the customer's true identity, and have effective procedures for verifying the bona fides of new customers.

(b) Compliance with laws: bank management should ensure that business is conducted in conformity with high ethical standards, that laws and regulations are adhered to and that a service is not provided where there is good reason to suppose that transactions are associated with laundering activities[2] .

(c) Co-operation with law enforcement agencies: within any constraints imposed by rules relating to customer confidentiality, banks should co-operate fully with national law enforcement agencies including, where there are reasonable grounds for suspecting money laundering, taking appropriate measures which are consistent with the law.

(d) Policies, procedures and training: all banks should formally adopt policies consistent with the principles set out in the Statement, and should ensure that all members of their staff concerned, wherever located, are informed of the bank's policy. Attention should be given to staff training in matters covered by the statement. To promote adherence to these principles, banks should implement specific procedures for customer identification and for retaining internal records of transactions. Arrangements for internal audit may need to be extended in order to establish an effective means for general compliance with the Statement.

4.2 The principles laid down by the Basle Committee have subsequently been developed by the Financial Action Task Force (FATF). In February 1990, FATF put forward forty recommendations aimed at improving national legal systems, enhancing the role of financial systems, and strengthening international co-operation against money laundering. Hong Kong, China is a member of the FATF and fully complies with the forty recommendations.

4.3 The Monetary Authority considers that institutions should follow the basic policies and principles as embodied in the Statement of Principles of the Basle Committee and the FATF recommendations. Specifically the Monetary Authority expects that institutions should have in place the following policies, procedures and controls -

(a) Institutions should issue a clear statement of policies in relation to money laundering, adopting current regulatory requirements. This statement should be communicated in writing to all management and relevant staff whether in branches, departments or subsidiaries and be reviewed on a regular basis.

---

2 Paragraph 9.9 describes the actual application of this principle to an authorized institution.

(b) Instruction manuals should set out institutions' procedures for:

- account opening;
- identification of applicants for business;
- record-keeping;
- reporting of suspicious transactions.

based on the recommendations in the following sections of this Guideline.

(c) Institutions should seek actively to promote close co-operation with law enforcement authorities, and should identify a single reference point within their organization (usually a compliance officer) to which staff are instructed to report suspected money laundering transactions promptly. This reference point should have a means of liaison with the Joint Financial Intelligence Unit which will ensure prompt referral of suspected money-laundering transactions associated with drug trafficking or other indictable offences. The role and responsibilities of this reference point in the reporting procedures should be clearly defined.

(d) Measures should be undertaken to ensure that staff are educated and trained on matters contained in this Guideline both as part of their induction procedures and at regular future intervals. The aim is to generate and maintain a level of awareness and vigilance among staff to enable a report to be made if suspicions are aroused.

(e) Institutions should instruct their internal audit/inspection departments to verify, on a regular basis, compliance with policies, procedures, and controls against money laundering activities.

(f) Whilst appreciating the sensitive nature of extra-territorial regulations, and recognizing that their overseas operations must be conducted in accordance with local laws and regulations, institutions should ensure that their overseas branches and subsidiaries are aware of group policies concerning money laundering and, where appropriate, have been instructed as to the local reporting point for their suspicions.

PART II

DETAILED GUIDELINES

5. Verification of identity of applicants for business

5.1 Institutions should not keep anonymous accounts or accounts in obviously fictitious names. They should obtain satisfactory evidence of the identity and legal existence of persons applying to do business with the institution (such as opening a deposit account) on the basis of reliable documents or other resources, and record that identity and other relevant information regarding the applicant in their files. They should establish that any applicant claiming to act on behalf of another person is authorized to do so.

5.2 For the purposes of this guideline, evidence of identity can be regarded as satisfactory if -

(a) it is reasonably capable of establishing that the applicant for business is whom he claims to be; and

(b) the institution which obtains the evidence is satisfied, in accordance with the procedures established by the institution, that it does establish that fact.

5.3 ~~New or modified requirements for verification of identity introduced by this Guideline shall apply only to business relationships entered into after 17 October 1997.~~Repealed. [See section 12 of the Supplement to the Guideline on Prevention of Money Laundering ("the AML Supplement")]

Individual applicants

5.4 Institutions should institute effective procedures for obtaining satisfactory evidence of the identity of applicants for business including obtaining information about name, permanent address, date of birth and occupation.

5.5 Positive identification should be obtained from documents issued by official or other reputable sources e.g. passports or identity cards. For Hong Kong residents, the prime source of identification will be the identity cards which they are required by law to carry with them. File copies of identity documents should be kept.

5.6 However, it must be appreciated that no form of identification can be fully guaranteed as genuine or representing correct identity. The Immigration Department operates a Hotline (Tel. 2824 1551) to which enquiries can be made concerning the validity of an identity card. If there is doubt whether an identification document is genuine, contact should be made with this Hotline immediately.

5.7 Institutions are advised to check the address of the applicant by appropriate means, e.g. by requesting sight of a recent utility or rates bill ~~or checking the Voters Roll maintained by the Registration & Electoral Office~~.

5.8 Where institutions require applicants for personal banking services to provide in the application forms for such services the names and particulars of persons who have agreed to act as referees for the applicants, they should follow the practices and procedures as set out in the section on personal referees of the Code of Banking Practice jointly issued by the Hong Kong Association of Banks and the Deposit-taking Companies Association.

Corporate applicants

5.9 Company accounts are one of the more likely vehicles for money laundering, even where the company is also being used for legitimate trading purposes. It is therefore important to obtain satisfactory evidence of the identity of the principal shareholders[3], directors and authorized signatories and of the nature of the business. The guiding principle should be to establish that it is safe to enter into a business relationship with the company concerned.

5.10 Before a business relationship is established, measures should be taken by way of a company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound-up or terminated. In addition, if institutions become aware of subsequent changes to the company structure or ownership, or suspicions are aroused by a change in the profile of payments through a company account, further checks should be made.

5.11 The following documents or information should be obtained in respect of corporate applicants for business which are registered in Hong Kong (comparable documents, preferably certified by qualified persons such as lawyers or accountants in the country of registration, should be obtained for those applicants which are not registered in Hong Kong) -

(a) Certificate of Incorporation and Business Registration Certificate;

(b) Memorandum and articles of association;

(c) resolution of the board of directors to open an account and confer authority on those who will operate it; and

(d) a search of the file at Company Registry.

5.12 Repealed. [See section 4 of the AML Supplement] ~~Where the company concerned is -~~

~~(a) a financial institution authorized and regulated by the Monetary Authority, the Securities and Futures Commission or the Insurance Authority in respect of its business in Hong Kong or is known to be a subsidiary of such an institution;~~

[3] It is recommended that "principal shareholders" should include those entitled to exercise, or control the exercise of, 10% or more of the voting rights of the company.

~~(b) a financial institution not authorized to carry on business in Hong Kong, but which is incorporated in a country which is a member of FATF[1] and which is regulated by bodies carrying out equivalent functions to those mentioned in the preceding sub-paragraph;~~

~~(c) listed on The Stock Exchange of Hong Kong, or is known to be a subsidiary of such a company;~~

~~(d) listed on the stock market of a country which is a member of FATF and which is a stock market recognised by the Securities and Futures Commission for the purposes of section 65A(2)(a) of the Securities Ordinance[2]; or~~

~~(e) a non-listed company, whose principal shareholders and the directors (including the managing director) are already known to the institution;~~

~~it should be sufficient to obtain the documents specified in paragraph 5.11, without the need to make further enquiries about the identity of individual directors and authorized signatories. However, evidence that any individual representing the company has the necessary authority to do so should be sought and retained. In the case of financial institutions, it should be established that the institution concerned is on the relevant regulator's list of regulated institutions.~~

5.13 ~~For companies other than those listed in paragraph 5.12, in addition to obtaining the documents specified in paragraph 5.11, institutions should obtain satisfactory evidence of the identity of the principal shareholders, at least two directors (including the managing director) and all authorized signatories in line with the requirements for individual applicants, and of the nature of the business.~~Repealed. [See section 4 of the AML Supplement]

Clubs, societies and charities

5.14 In the case of accounts to be opened for clubs, societies and charities, an institution should satisfy itself as to the legitimate purpose of the organisation by, e.g. requesting sight of the constitution. Satisfactory evidence should be obtained of the identity of the authorized signatories who are not already known to the institution in line with the requirements for individual applicants.

Unincorporated businesses

5.15 In the case of partnerships and other unincorporated businesses whose partners are not known to the bank, satisfactory evidence should be obtained of the identity of at least two partners and all authorized signatories in line with the requirements for individual applicants. In cases where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

Shell companies

~~[1] See list of FATF Members in Annex 1.~~

~~[2] See list in Annex 2.~~

5.16 Shell companies are legal entities through which financial transactions may be conducted but which have no business substance in their own right. While shell companies may be used for legitimate purposes, the FATF has expressed concern about the increasing use of such companies to conduct money laundering (through providing the means to operate what are in effect anonymous accounts). Institutions should take notice of the potential for abuse by money launderers of shell companies and should therefore be cautious in their dealings with them. In keeping with the "know your customer" principle, institutions should obtain satisfactory evidence of the identity of beneficial owners, directors and authorized signatories of shell companies. Where the shell company is introduced to the institution by a professional intermediary acting on its behalf, institutions should follow the guidelines in paragraphs 5.17 to 5.22 below.

Where the applicant for business is acting on behalf of another person

5.17 Trust, nominee and fiduciary accounts are a popular vehicle for criminals wishing to avoid identification procedures and mask the origin of the criminal money they wish to launder. Accordingly, institutions should always establish, by confirmation from an applicant for business, whether the applicant is acting on behalf of another person as trustee, nominee or agent.

5.18 Any application to open an account or undertake a transaction on behalf of another person without applicants identifying their trust or nominee capacity should be regarded as suspicious and should lead to further enquiries as to the underlying principals and the nature of the business to be transacted.

5.19 Institutions should obtain satisfactory evidence of the identity of trustees, nominees and authorized signatories and of the nature of their trustee or nominee capacity and duties by, for example, obtaining a copy of the trust deed. Enquiries should also be made of the extent to which the applicant for business is subject to official regulation (e.g. by a body equivalent to the Monetary Authority).

5.20 Particular care should be taken in relation to trusts created in jurisdictions without equivalent money laundering legislation to Hong Kong.

5.21 Repealed. [See section 6 of the AML Supplement]~~Where the applicant for business who is acting on behalf of another person is one of the following -~~

~~(a) a financial institution authorized and regulated by the Monetary Authority, the Securities and Futures Commission or the Insurance Authority in respect of its business in Hong Kong or is known to be a subsidiary of such an institution;~~

~~(b) a financial institution not authorized to carry on business in Hong Kong, but which is incorporated in a country which is a member of FATF and which is regulated by bodies carrying out equivalent functions to those mentioned in the preceding sub-paragraph; or~~

(c) an intermediary which does not fall into the above two categories but is one with which the institution has an established business relationship[3] and where the institution is fully satisfied as to its reputation, conduct and good faith;

it shall be reasonable for the institution to accept a written assurance from the applicant for business that evidence of the underlying principals has been obtained, recorded and retained, and that the applicant is satisfied as to the source of funds. For this purpose, it is recommended that the institution should obtain a written statement from the applicant for business (i.e. the intermediary) along the following lines:

5.22 Where the applicant for business who is acting on behalf of another person does not fall into any of the categories in paragraph 5.21, the institution should obtain satisfactory evidence of the identity of the underlying principals and the source of funds. The use of a standard format for obtaining the relevant information is recommended. A suggested Intermediary Introduction Certificate is at Annex 3. If satisfactory evidence cannot be obtained, institutions should give very careful consideration as to whether they should proceed with the business, bearing in mind the "know your customer" principle. If they decide to proceed, they should record any misgivings and give extra attention to monitoring the account in question. Suspicious transactions should be reported in accordance with the procedures in section 9 below.Repealed. [See section 6 of the AML Supplement]

Client accounts

5.23 The guidelines in paragraphs 5.17 to 5.22 apply to client accounts opened by intermediaries. However, where the intermediary is a firm of solicitors or accountants, their professional codes of conduct may preclude the firms from divulging information to institutions concerning their underlying clients. It may therefore not be possible for an institution to establish the identity of the person(s) for whom a solicitor or accountant is acting. In such cases, the institution should obtain the written statement about the underlying principals and source of funds mentioned in paragraph 5.21. In addition, the institution should not be precluded from making reasonable enquiries about transactions passing through client accounts that give cause for concern or from reporting those transactions if any suspicions are aroused.Repealed. [See section 7 of the AML Supplement]

Avoidance of account opening by post

5.24 Whenever possible, applicants for business should be interviewed personally. Any mechanism which avoids face to face contact between institutions and applicants inevitably poses difficulties for customer identification and produces a useful loophole that money launderers may wish to exploit.Repealed. [See section 8 of the AML Supplement]

5.25 Care should be taken when dealing with accounts opened by post, or from coupon applications, to ensure that the identities of the applicants are obtained as much as possible. For local applicants, account opening by post should not be permitted. Institutions should request the applicants to call on one of their branches for account opening. For overseas applicants in a country where the institution does not have a presence, the

[3] An established business relationship means any arrangement between a person and the institution, the purpose of which is to facilitate the carrying out of transactions between the parties on a regular basis and where the institution has obtained satisfactory evidence of the identity of that person.

~~application should be submitted through a correspondent bank in that country or a bank which can be relied upon to undertake effective identification procedures on behalf of the institution.~~Repealed. [See section 8 of the AML Supplement]

Transactions undertaken for non-account holders (occasional customers)

5.26 Where transactions are undertaken by an institution for non-account holders of that institution e.g. requests for telegraphic transfers, or where funds are deposited into an existing account by persons whose names do not appear on the mandate of that account, care and vigilance are required. Where the transaction involves large sums of cash, or is unusual, the applicant should be asked to produce positive evidence of identity from the sources set out above and in the case of a foreign national, the nationality recorded. Copies of the identification documents should be kept on file.

5.27 ~~An institution should not undertake for a non-account holder any remittance or money changing transaction that is HK$20,000 or more or of an equivalent amount in any other currency unless the particulars of the transaction as set out at Annex 8 are recorded. In this context, the non-account holder in respect of an inward remittance transaction refers to the recipient of the funds. As regards an outward remittance transaction, the non-account holder is the remitter of the funds.~~Repealed. [See paragraphs 3.12 – 3.16 of the AML Supplement]

Provision of safe custody and safety deposit boxes

5.28 Precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the identification procedures set out above should be followed.

6. Remittance

6.1 ~~At the request of FATF, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) made a global broadcast on 30 July 1992 to its user organizations requesting them to include the names, addresses and/or account numbers of their customers in MT 100 messages. The objective is to assist the law enforcement authorities in their investigations of suspected money laundering made through electronic message systems. A copy of SWIFT's message is at Annex 4. This message should be brought to the attention of staff who deal with remittance matters within the institution.~~Repealed. [See section 9 of the AML Supplement]

6.2 ~~While it is recognized that there may be technical and practical difficulties for institutions to include full details of their customers in SWIFT MT 100 messages, authorized institutions are encouraged, to the maximum extent possible, to comply with the SWIFT request.~~Repealed. [See section 9 of the AML Supplement]

6.3 ~~SWIFT implemented a new optional format (MT103) on 18 November 2000. Therefore, the corresponding field numbers referred to in the SWIFT broadcast of 30 July 1992 in Annex 4 should be 50a and 59a in MT103 replacing 50 and 59 in MT100 format. Although SWIFT members are allowed to use either the MT100 or MT103 format until November 2003, authorized institutions should in the meantime make every effort to comply with the new format's requirements regarding the provision of customer information.~~Repealed. [See section 9 of the AML Supplement]

7. Record keeping

7.1 The DTROP and the OSCO entitle the Court to examine all relevant past transactions to assess whether the defendant has benefitted from drug trafficking or other indictable offences.

7.2 The investigating authorities need to ensure a satisfactory audit trail for suspected money laundering transactions and to be able to establish a financial profile of the suspect account. For example, to satisfy these requirements the following information may be sought -

(a) the beneficial owner of the account (for accounts opened on behalf of a third party, please see paragraphs 5.17 to 5.23);

(b) the volume of funds flowing through the account;

(c) for selected transactions:

- the origin of the funds (if known);
- the form in which the funds were offered or withdrawn i.e. cash, cheques etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

7.3 An important objective is for institutions at all stages in a transaction to be able to retrieve relevant information, to the extent that it is available, without undue delay.

7.4 When setting document retention policy, institutions must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. However, wherever practicable the following document retention times should be followed -

(a) account opening records - copies of identification documents should be kept in file for six years [4] following the closing of an account;

(b) account ledger records - six years[4] from entering the transaction into the ledger; and

(c) records in support of entries in the accounts in whatever form they are used e.g. credit/debit slips and cheques and other forms of vouchers - six years[4] from when the records were created.

---

4 Six years being the statutory limitation period for certain classes of claims under the Limitation Ordinance.

(d) records in support of ~~remittance~~wire transfer and money changing transactions for non-account holders – six years[4] from when the records were created.

7.5 Retention may be by way of original documents, stored on microfilm, or in computerized form, provided that such forms are accepted as evidence under sections 20 to 22 of the Evidence Ordinance. In situations where the records relate to on-going investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed.

8. Recognition of suspicious transactions

8.1 As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.

8.2 Examples of what might constitute suspicious transactions are given in Annex 5. These are not intended to be exhaustive and only provide examples of the most basic ways in which money may be laundered. However, identification of any of the types of transactions listed in Annex 5 should prompt further investigations and be a catalyst towards making at least initial enquiries about the source of funds.

9. Reporting of suspicious transactions

9.1 The reception point for disclosures under the DTROP and the OSCO is the Joint Financial Intelligence Unit, which is operated by the Police and Customs and Excise Department.

9.2 In addition to acting as the point for receipt of disclosures made by any organization or individual, the unit also acts as domestic and international advisors on money laundering generally and offers practical guidance and assistance to the financial sector on the subject of money laundering.

9.3 The obligation to report is on the individual who becomes suspicious of a money laundering transaction. Each institution should appoint a designated officer or officers (Compliance Officer(s)) who should be responsible for reporting to the Joint Financial Intelligence Unit where necessary in accordance with section 25A of both the DTROP and the OSCO and to whom all internal reports should be made.

9.4 Compliance Officers should keep a register of all reports made to the Joint Financial Intelligence Unit and all reports made to them by employees. Compliance Officers should provide employees with a written acknowledgement of reports made to them, which will form part of the evidence that the reports were made in compliance with the internal procedures.

9.5 All cases where an employee of an institution knows that a customer has engaged in drug-trafficking or other indictable offences and where the customer deposits, transfers or seeks to invest funds or obtains credit against the security of such funds, or where the institution holds funds on behalf of such customer, must promptly be reported to the Compliance Officer who, in turn, must immediately report the details to the Joint Financial Intelligence Unit.

9.6 All cases, where an employee of an institution suspects or has reasonable grounds to believe that a customer might have carried on drug trafficking or might have been engaged in indictable offences and where the customer deposits, transfers or seeks to invest funds or obtains credit against the security of such funds, or where the institution holds funds on behalf of such customer, must promptly be reported to the Compliance Officer. The Compliance Officer must promptly evaluate whether there are reasonable grounds for such belief and must then immediately report the case to the Joint Financial Intelligence Unit unless he considers, and records his opinion, that such reasonable grounds do not exist.

9.7 Institutions must take steps to ensure that all employees concerned with the holding, receipt, transmission or investment of funds (whether in cash or otherwise) or the making of loans against the security of such funds are aware of these procedures and that it is a criminal offence to fail to report either knowledge or circumstances which give rise to a reasonable belief in the existence of an offending act.

9.8 Institutions should make reports of suspicious transactions to the Joint Financial Intelligence Unit as soon as it is reasonable for them to do so. The use of a standard format as set out in Annex 6 or use of the e-channel "STREAMS' by registered users for reporting is encouraged ~~(see Annex 6 which sets out a reporting format acceptable to the Joint~~

~~Financial Intelligence Unit~~). In the event that urgent disclosure is required, particularly when the account concerned is part of an on-going investigation, an initial notification should be made by telephone.

9.9 Institutions should refrain from carrying out transactions which they know or suspect to be related to money laundering until they have informed the Joint Financial Intelligence Unit which consents to the institution carrying out the transactions. Where it is impossible to refrain or if this is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, institutions may carry out the transactions and notify the Joint Financial Intelligence Unit on their own initiative and as soon as it is reasonable for them to do so.

9.10 Cases do occur when an institution declines to open an account for an applicant for business, or refuses to deal with a request made by a non-account holder because of serious doubts about the good faith of the individual and concern about potential criminal activity. Institutions must base their decisions on normal commercial criteria and internal policy. However, to guard against money laundering, it is important to establish an audit trail for suspicious funds. Thus, where practicable, institutions are requested to seek and retain copies of relevant identification documents which they may obtain and to report the offer of suspicious funds to the Joint Financial Intelligence Unit.

9.11 Where it is known or suspected that a report has already been disclosed to the Joint Financial Intelligence Unit and it becomes necessary to make further enquiries of the customer, great care should be taken to ensure that the customer does not become aware that his name has been brought to the attention of the law enforcement agencies.

9.12 Following receipt of a disclosure and research by the Joint Financial Intelligence Unit, the information disclosed is allocated to trained financial investigation officers in the Police and Customs and Excise Department for further investigation including seeking supplementary information from the institution making the disclosure, and from other sources. Discreet enquiries are then made to confirm the basis for suspicion.

9.13 Access to the disclosed information is restricted to financial investigating officers within the Police and Customs and Excise Department. In the event of a prosecution, production orders are obtained to produce the material for court. Section 26 of both the DTROP and the OSCO places strict restrictions on revealing the identity of the person making disclosure under section 25A. Maintaining the integrity of the relationship which has been established between law enforcement agencies and institutions is considered to be of paramount importance.

10. Feedback from the investigating authorities

10.1 The Joint Financial Intelligence Unit will acknowledge receipt of a disclosure made by an institution under section 25A of both the DTROP and the OSCO, and section 12 of the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO). If there is no imminent need for action e.g. the issue of a restraint order on an account, consent will usually be given for the institution to operate the account under the provisions of section 25A(2) of both the DTROP and the OSCO. An example of such a letter is given at Annex 7 to this Guideline. For disclosure submitted via e-channel "STREAM", e-receipt will be issued via the same e-channel.

10.2 Whilst there are no statutory requirements to provide feedback arising from investigations, the Police and Customs and Excise Department recognize the importance of having effective feedback procedures in place. The Joint Financial Intelligence Unit presently provides a service, on request, to a disclosing institution in relation to the current status of an investigation.

11. Staff education and training

11.1 Staff must be aware of their own personal legal obligations under the DTROP, ~~and the~~ OSCO and UNATMO that they can be personally liable for failure to report information to the authorities. They must be encouraged to co-operate fully with the law enforcement agencies and promptly to report suspicious transactions. They should be advised to report suspicious transactions to their institution's Compliance Officer even if they do not know precisely what the underlying criminal activity is or whether illegal activities have occurred.

11.2 It is, therefore, imperative that institutions introduce comprehensive measures to ensure that staff are fully aware of their responsibilities.

11.3 Institutions should therefore provide proper anti-money laundering training to their local as well as overseas staff. The timing and content of training packages for various sectors of staff will need to be adapted by individual institutions for their own needs. However, it is recommended that the following might be appropriate -

(a) New Employees

A general appreciation of the background to money laundering, the consequent need to be able to identify suspicious transactions and report such transactions to the appropriate designated point within the institution, and the offence of "tipping off" should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the legal requirement to report suspicious transactions relating to drug trafficking or other indictable offences, and that there is also a personal statutory obligation in this respect.

(b) Cashiers/Tellers/Foreign Exchange Operators/Advisory Staff

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are therefore vital to the institution's strategy in the fight against money laundering. They should be made aware of their legal responsibilities and the institution's reporting system for such transactions.

Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. It is vital that "front-line" staff are made aware of the institution's policy for dealing with non-regular customers particularly where large cash transactions are involved, and the need for extra vigilance in these cases.

(c) Account Opening/New Client Personnel

Those members of staff who are in a position to deal with account opening, or to accept applicants for business, must receive the training given to cashiers etc. in (b) above. In addition, the need to verify the identity of the applicant must be understood, and training should be given in the institution's account

opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction need to be reported to the relevant authorities whether or not the funds are accepted or the transactions proceeded with and they must know what procedures to follow in this respect.

(d) Administration/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the DTROP and the OSCO; procedures relating to service of production and restraint orders; and the requirements for retention of records.

(e) On-going Training

It will also be necessary to make arrangements for refresher training at regular intervals to ensure that staff do not forget their responsibilities.

(f) Training Package

Institutions should acquire sufficient copies of the training ~~video~~ materials ~~and booklet~~ produced by the Hong Kong Association of Banks for the purpose of training front line staff. All front line staff who deal directly with customers should have a copy of the booklet and all new front line staff should view the video upon joining the institution.

Repealed

~~Members of Financial Action Task Force~~

~~Argentina~~

~~Australia~~

~~Austria~~

~~Belgium~~

~~Brazil~~

~~Canada~~

~~Denmark~~

~~European Commission~~

~~Finland~~

~~France~~

~~Germany~~

~~Greece~~

~~Gulf Cooperation Council~~

~~Hong Kong, China~~

~~Iceland~~

~~Ireland~~

~~Italy~~

~~Japan~~

~~Luxembourg~~

~~Mexico~~

~~Kingdom of the Netherlands~~

~~New Zealand~~

~~Norway~~

~~Portugal~~

~~Singapore~~

~~Spain~~

~~Sweden~~

~~Switzerland~~

~~Turkey~~

~~United Kingdom~~

~~United States~~

Repealed

~~Stock market of a country which is a member of FATF and which is a stock market recognised by the Securities and Futures Commission for the purposes of section 65A(2)(a) of the Securities Ordinance~~

~~Auckland Stock Exchange~~

~~American Stock Exchange~~

~~Amsterdam Stock Exchange~~

~~Australian Stock Exchange Limited~~

~~Brussels Stock Exchange~~

~~Copenhagen Stock Exchange~~

~~Frankfurt Stock Exchange~~

~~Luxembourg Stock Exchange~~

~~Milan Stock Exchange~~

~~Montreal Stock Exchange~~

~~National Association of Securities Dealers (USA)~~

~~New York Stock Exchange~~

~~Osaka Stock Exchange~~

~~Oslo Stock Exchange~~

~~Paris Bourse~~

~~Singapore Stock Exchange~~

~~Stockholm Stock Exchange~~

~~The International Stock Exchange of the United Kingdom and the Republic of Ireland Limited~~

~~Toronto Stock Exchange~~

~~Tokyo Stock Exchange~~

~~Wellington Stock Exchange~~

~~Zurich Stock Exchange~~

Repealed

INTERMEDIARY INTRODUCTION CERTIFICATE

**Please delete as appropriate*

NAME AND .....

ADDRESS OF .....

INTERMEDIARY .....
(*individual/company)

.....

.....

I/We certify that in accordance with the requirements of the Guideline on Prevention of Money Laundering issued by the Hong Kong Monetary Authority under section 7(3) of the Banking Ordinance, as amended from time to time, the following information is correct:

I/We wish to apply for banking facilities on behalf of the following named *individual(s)/company(ies)

.....

This section applies to individual(s) on whose behalf the application is made by the intermediary:

1. True copies of identity cards/passports relating to all such individual(s) (i.e. the underlying principal(s)) are enclosed.
2. Evidence of authority for the intermediary to act on behalf of the individual(s) e.g. a trust deed is enclosed.
3. I/We confirm the following address(es) is/are the current permanent address(es) of the individual(s)

   .....
4. I/We confirm the main occupation of the individual(s) is/are:

   .....
5. I am/We are satisfied as to the source of funds *being used to open the account/passing through the account.

   ☐ Yes ☐ No (Please tick as appropriate)

This section applies to company(ies) on whose behalf the application is made by the intermediary:

1. The following documentation is enclosed in relation to the company concerned :
   (a) Certificate of Incorporation (or true copy);
   (b) True copies of identity cards/passports of all authorized signatories of the company;
   (c) True copies of identity cards/passports of at least two directors (including the managing director) of the company;
   (d) True copies of identity cards/passports of principal shareholders of the company[1] if different to persons covered by (b) or (c);
   (e) Completed bank mandate including authority to open account;
   (f) Evidence of authority for the intermediary to act on behalf of the company.
2. I/We confirm the main business activities of the company is/are (enclose copy of Business Registration Certificate if available) :

   .....

   .....

   (continue overleaf if necessary)
3. I am/We are satisfied as to the source of funds *being used to open the account/passing through the account.

   ☐ Yes ☐ No (Please tick as appropriate)

SIGNED BY INTERMEDIARY ..... **DATE** .....

[1] Principal shareholders should include those entitled to exercise, or control the exercise of, 10% or more of the voting rights of the company.

Repealed

~~SWIFT BROADCAST OF 30 JULY 1992~~

~~As you will know, many countries are involved in initiatives to prevent the utilization of the banking system and financial institutions for the purpose of money laundering, they are also considering additional preventive efforts in this field.~~

~~SWIFT has now been asked by, and agreed with, the intergovernmental Money Laundering Financial Action Task Force to give the following notice to all SWIFT users and we would request you to follow this advice.~~

~~Ensure when you send MT 100 messages that:~~

~~(a) field 50 is completed with the name and address of the ordering customer or, when this is not possible, the account number, and~~

~~(b) field 59 is completed with the name, address and where possible the account number of the beneficiary customer.~~

~~Eric C Chilton~~
~~Chairman of the Board~~
~~S.W.I.F.T. sc~~

EXAMPLES OF SUSPICIOUS TRANSACTIONS

1. Money Laundering Using Cash Transactions

a) Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

b) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

c) Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

d) Company accounts whose transaction, both deposits and withdrawals, are denominated in cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.).

e) Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments.

f) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

g) Frequent exchange of cash into other currencies.

h) Branches that have a great deal more cash transactions than usual. (Head Office statistics should detect aberrations in cash transactions.)

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

j) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

k) Large cash deposits using night safe facilities, thereby avoiding direct contact with the institution.

l) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the institution.

m) Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their retail business.

2. Money Laundering Using Bank Accounts

a) Customers who wish to maintain a number of trustee or clients' accounts which do not appear consistent with their type of business, including transactions which involve nominee names.

b) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

c) Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

d) Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify.

e) Customers who appear to have accounts with several institutions within the same locality, especially when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

f) Matching of payments out with credits paid in by cash on the same or previous day.

g) Paying in large third party cheques endorsed in favour of the customer.

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

i) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

j) Greater use of safe deposit facilities by individuals. The use of sealed packets deposited and withdrawn.

k) Companies' representatives avoiding contact with the branch.

l) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.

m) Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

n) Large number of individuals making payments into the same account without an adequate explanation.

o) Customers who maintain an unusually large number of accounts for the type of business they are purportedly conducting and/or use inordinately large number of fund transfers among these accounts.

p) High velocity of funds through an account, i.e., low beginning and ending daily balances, which do not reflect the large volume of dollars flowing through an account.

q) Multiple depositors using a single bank account.

r) An account opened in the name of a money changer that receives structured deposits.

s) An account operated in the name of an off-shore company with structured movement of funds.

3. Money Laundering Using Investment Related Transactions

a) Purchasing of securities to be held by the institution in safe custody, where this does not appear appropriate given the customer's apparent standing.

b) Back to back deposit/loan transactions with subsidiaries of, or affiliates of, overseas financial institutions in known drug trafficking areas.

c) Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.

d) Larger or unusual settlements of securities transactions in cash form.

e) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. Money Laundering Involving Off-Shore International Activity

a) Customers introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.

b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

c) Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs.

d) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

e) Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.

f) Frequent requests for travellers cheques, foreign currency drafts or other negotiable instruments to be issued.

g) Frequent paying in of travellers cheques, foreign currency drafts particularly if originating from overseas.

h) Numerous wire transfers received in an account but each transfer is below the reporting requirement in the remitting country.

i) Customers sending and receiving wire transfer to/from financial haven countries, particularly if there are no apparent business reasons for such transfers or such transfers are not consistent with the customers' business or history.

5. Money Laundering Involving Authorized Institution Employees and Agents

a) Changes in employee characteristics, e.g. lavish life styles.

b) Any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, contrary to normal procedure for the type of business concerned.

6. Money Laundering by Secured and Unsecured Lending

a) Customers who repay problem loans unexpectedly.

b) Request to borrow against assets held by the institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

c) Request by a customer for an institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

d) A customer who is reluctant or refuses to state a purpose of a loan or the source of repayment, or provides a questionable purpose and/or source.

Report made under Section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance and the Organized and Serious Crimes Ordinance to the Joint Financial Intelligence Unit

Date:
Ref. No.:

(A) SOURCE

Name of Institution:	
Reporting Officer:	Tel. No.:
Signature:	Fax No.:

(B) SUSPICION

(Please provide details of transaction arousing suspicion and any other relevant information. Please also enclose copy of the transaction for reference. Particulars of account holder or person conducting the transaction are to be given in page 2.)

(C) OTHER INFORMATION

This is a new disclosure:	Yes/No	JFIU No.:
This disclosure relates to a previous disclosure:	JFIU No.:	Bank Ref. No.:

(D) SUBJECT (1)

Name:	C.C.C.:	Date of Birth:
HKIC/PPT No.:	Sex: M/F	Nationality:
Address:		
Occupation:	Company:	
Position Held:	Company Address:	

SUBJECT (2)

Name:	C.C.C.:	Date of Birth:
HKIC/PPT No.:	Sex: M/F	Nationality:
Address:		
Occupation:	Company:	
Position Held:	Company Address:	

SUBJECT (3)

Name:	C.C.C.:	Date of Birth:
HKIC/PPT No.:	Sex: M/F	Nationality:
Address:		
Occupation:	Company:	
Position Held:	Company Address:	

(E) RELATED BANK ACCOUNT(s)

	(1)	(2)
Account No.:		
Type of Account:		
Date of Opening:		
Account Balance:		
Account Holder(s):		

	(3)	(4)
Account No.:		
Type of Account:		
Date of Opening:		
Account Balance:		
Account Holder(s):		

Annex 7

Example of Acknowledgement of Receipt by JFIU

Date:

The Compliance Officer
[ ] Bank Ltd.

~~(~~Fax No. : ~~)~~

Dear Sir/Madam~~/Sir~~,

~~Drug Trafficking (Recovery of Proceeds) Ordinance/~~
~~Organized and Serious Crimes Ordinance~~Acknowledgement of Receipt of Suspicions Transaction Report(s) ("STR")

~~I refer to your disclosure made to the JFIU on [date] under the above references.~~

I acknowledge receipt of the attached STR made in accordance with the provisions of section 25A(1) of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap 405) / Organized and Serious Crimes Ordinance (Cap 455) and section 12(1) of the United Nations (Anti-Terrorism Measures) Ordinance(Cap 575). ~~information supplied by you under the provisions of Section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance / Organized and Serious Crimes Ordinance. The information contained in your disclosure has been indexed and no further investigation will be taken at this stage. / Your disclosure is under our investigation*.~~

Based upon the information currently in hand, consent is given under the provisions of section 25A(2) & (3) of Cap 405 and 455 and section 12(2) & (3) of Cap 575. ~~Consent is given for you to continue to operate the account(s) in accordance with normal banking practice under the provisions of Section 25A(2) & (3) of the said Ordinances.~~

If you have any queries, please feel free to contact the undersigned on telephone number (852)xxxxxxxx. ~~Thank you for your co-operation.~~

Yours faithfully,

( )
Joint Financial Intelligence Unit

•~~Delete as appropriate~~

Repealed

~~Particulars to be recorded for any remittance or money changing transaction undertaken for a non-account holder for an amount of HK$20,000 or more or of an equivalent amount in any other currency~~

~~Outward remittance to a place outside Hong Kong~~

~~(1)Transaction reference number~~
~~(2)Transaction type, currency, amount and value date of the remittance~~
~~(3)Date of remitter's instructions~~
~~(4)Instruction details (including name, address and account number of beneficiary[#], name and address of beneficiary bank, and remitter's message to beneficiary, if any)~~
~~(5)Name, identity card number (or any other document of identity or travel document number with place of issue) of remitter or his representative must be verified if he appears in person~~
~~(6)Telephone number and address of remitter~~

~~Inward remittance from a place outside Hong Kong~~

~~(1)Transaction reference number~~
~~(2)Transaction type, currency, amount and value date of the remittance~~
~~(3)Date of remitter's instructions~~
~~(4)Instruction details (including name and address of beneficiary, name and address of remitter[#] and remitting bank, and remitter's message to beneficiary, if any)~~
~~(5)Name and identity card number (or any other document of identity or travel document number with place of issue) of beneficiary which must be verified where the beneficiary appears in person~~

~~Money changing transactions~~

~~(1)Transaction reference number~~
~~(2)Date and time of transaction~~
~~(3)Currencies and amount exchanged~~
~~(4)Exchange rate~~
~~(5)Name, identity card number (or any other document of identity or travel document number with place of issue) of customer which must be verified~~
~~Telephone number and address of customer~~

~~# The HKMA recognizes that certain information, in particular, the remitter's address in an inward remittance and the beneficiary's address and account number in an outward remittance may not be available to the receiving bank and remitting bank respectively. However, AIs should, on a best effort basis, obtain and record such information as far as possible.~~

GUIDELINE ON PREVENTION OF MONEY LAUNDERING

A Guideline issued by the Monetary Authority under section 7(3) of the Banking Ordinance

CONTENTS

Revised July 2010

ANNEXES

Annex 1	Repealed
Annex 2	Repealed
Annex 3	Repealed
Annex 4	Repealed
Annex 5	Examples of Suspicious Transactions
Annex 6	Standard format for reporting suspicious transaction to Joint Financial Intelligence Unit (JFIU)
Annex 7	Example of acknowledgement of receipt by JFIU of suspicious transaction reporting
Annex 8	Repealed

PART I

OVERVIEW

1. Introduction

1.1 This Guideline incorporates, and hence supersedes, the Guideline issued by the Monetary Authority in July 1993 on the prevention of criminal use of the banking system for the purposes of money laundering. This Guideline has been updated to take account of the enactment of the Organized and Serious Crimes Ordinance, the subsequent amendments to the money laundering provisions in that Ordinance and the Drug Trafficking (Recovery of Proceeds) Ordinance, the stocktaking review of the anti-money laundering measures undertaken by the Financial Action Task Force and the UK Money Laundering Guidance Notes for banks and building societies. It has also included other refinements and additional examples of suspicious transactions.

1.2 This Guideline applies directly to all banking and deposit taking activities in Hong Kong carried out by authorized institutions. However, institutions are expected to ensure that their subsidiaries in Hong Kong also have effective controls in place to combat money laundering. Where Hong Kong incorporated institutions have branches or subsidiaries overseas, steps should be taken to alert management of such overseas offices to Group policy in relation to money laundering. Where a local jurisdiction has a money laundering law, branches and subsidiaries of Hong Kong incorporated institutions operating within that jurisdiction should, as a minimum, act in accordance with the requirements of the local law. Where the local law and the Guideline are in conflict, the foreign branch or subsidiary should comply with the local law and inform the Head Office immediately of any departure from Group policy.

1.3 It is recognized that the relevance and usefulness of this Guideline will need to be kept under review as the methods of money laundering are constantly evolving. It may be necessary to issue amendments to this Guideline from time to time to incorporate measures to combat new money laundering threats, including those inherent in new or developing technologies that might favour anonymity.

2. What is money laundering?

2.1 The phrase "money laundering" covers all procedures to change the identity of illegally obtained money so that it appears to have originated from a legitimate source.

2.2 Cash lends anonymity to many forms of criminal activity and is the normal medium of exchange in the world of drug trafficking. This gives rise to three common factors -

(a) criminals need to conceal the true ownership and origin of the money;

(b) they need to control the money; and

(c) they need to change the form of the money.

2.3 One of the most common means of money laundering that institutions will encounter on a day-to-day basis takes the form of accumulated cash transactions which will be deposited in the banking system or exchanged for value items. These simple transactions may be just one part of the sophisticated web of complex transactions which are set out and illustrated below. Nevertheless, the basic fact remains that the key stage for the detection of money laundering operations is where the cash first enters the financial system.

Stages of money laundering

2.4 There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert an institution to criminal activity -

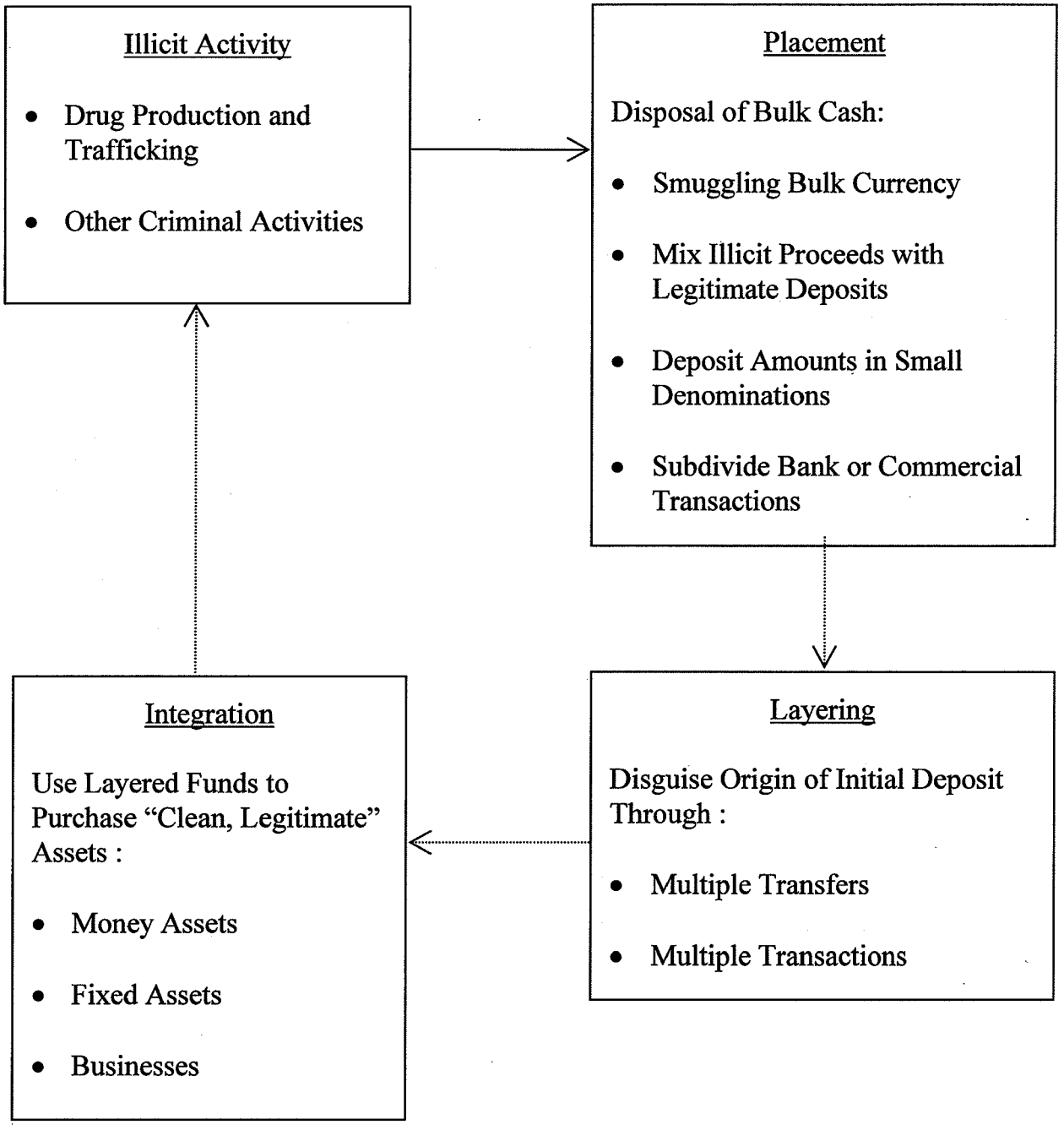
(a) Placement - the physical disposal of cash proceeds derived from illegal activity.

(b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

(c) Integration - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

2.5 The following chart illustrates the laundering stages in more detail.

PROCESS OF MONEY LAUNDERING



3. The legislation on money laundering in Hong Kong

3.1 Legislation has been developed in Hong Kong to address the problems associated with the laundering of proceeds from drug trafficking and serious crimes. The Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP) came into force in September 1989. It provides for the tracing, freezing and confiscation of the proceeds of drug trafficking and creates a criminal offence of money laundering in relation to such proceeds.

3.2 The Organized and Serious Crimes Ordinance (OSCO), which was modelled on the DTROP, was brought into operation in December 1994. It extends the money laundering offence to cover the proceeds of indictable offences in addition to drug trafficking.

3.3 Amendments to both Ordinances were made and came into effect on 1 September 1995. These amendments have tightened the money laundering provisions in both Ordinances and have a significant bearing on the duty to report suspicious transactions. In particular, there is now a clear statutory obligation to disclose knowledge or suspicion of money laundering transactions.

3.4 The key money laundering provisions in the two Ordinances are summarized below. This does not constitute a legal interpretation of the provisions of the legislation referred to, for which appropriate legal advice should be sought where necessary.

3.5 Section 25(1) of DTROP and OSCO creates the offence of dealing with any property, knowing or having reasonable grounds to believe it in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence respectively. The offence carries a maximum sentence of 14 years' imprisonment and a maximum fine of HK$5 million.

3.6 It is a defence under section 25(2) of both Ordinances for a person to prove that he intended to disclose as soon as is reasonable such knowledge, suspicion or matter to an authorized officer[1] or has a reasonable excuse for his failure to make a disclosure in accordance with section 25A(2) of the Ordinances.

3.7 Section 25A(1) imposes a statutory duty on a person, who knows or suspects that any property in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence, or was or is intended to be used in that connection, to make a disclosure to an authorized officer. Section 25A(7) makes it an offence for a person to fail to make such disclosure. The offence carries a maximum penalty of a fine at level 5 (at present $25,001 to $50,000) and imprisonment for 3 months.

---

1 As defined in section 2 of both the DTROP and OSCO, authorized officer means:
(a) any police officer;
(b) any member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342); and
(c) any other person authorized in writing by the Secretary for Justice for the purposes of this Ordinance.

3.8 It should be noted that section 25(4) of OSCO provides that references to an indictable offence in section 25 and 25A include a reference to conduct which would constitute an indictable offence if it had occurred in Hong Kong. That is to say it shall be an offence for a person to deal with the proceeds of crime or fail to make the necessary disclosure under section 25A(1) even if the principal crime is not committed in Hong Kong provided that it would constitute an indictable offence if it had occurred in Hong Kong.

3.9 Section 25A(2) provides that if a person who has made the necessary disclosure does any act in contravention of section 25(1) and the disclosure relates to that act he does not commit an offence if -

(a) the disclosure is made before he does that act and the act is done with the consent of an authorized officer; or

(b) the disclosure is made after the person does the act and the disclosure is made on the person's own initiative and as soon as it is reasonable for him to make it.

3.10 Section 25A(3) provides that disclosure made under section 25A(1) shall not be treated as breach of contract or of any enactment restricting disclosure of information and shall not render the person making the disclosure liable in damages for any loss arising out of disclosure. Therefore, institutions need not fear breaching their duty of confidentiality owed to customers when making a disclosure under the Ordinances.

3.11 Section 25A(4) extends the provisions of section 25A to disclosures made by an employee to an appropriate person in accordance with the procedures established by his employer for the making of such disclosure in the same way as it applies to disclosures to an authorized officer. This provides protection to employees of authorized institutions against the risk of prosecution where they have reported knowledge or suspicion of money laundering transactions to the person designated by their employers.

3.12 A "tipping-off" offence is created under section 25A(5) of both Ordinances, under which a person commits an offence if knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice an investigation into money laundering activities. The "tipping-off" offence carries a maximum penalty of three years' imprisonment and a fine of HK$500,000.

3.13 The Organized and Serious Crimes (Amendment) Ordinance 2000 ("OSCAO") came into operation on 1 June 2000. Among other things, OSCAO requires remittance agents and money changers to keep records of customers' identity and particulars of remittance and exchange transactions of HK$8,000 or more or of an equivalent amount in any other currency. Although authorized institutions are exempted from the requirements of OSCAO, similar customer identification and record keeping requirements should be adopted to ensure that the anti-money laundering standards of the banking sector are in line with the overall Government policy to combat money laundering activities.

4. Basic policies and principles to combat money laundering

4.1 The Monetary Authority fully subscribes to the basic policies and principles to combat money laundering as embodied in the Statement of Principles issued by the Basle Committee in December 1988. The Statement seeks to deny use of the banking system to those involved in money laundering by application of the following principles -

(a) Know your customer: banks should make reasonable efforts to determine the customer's true identity, and have effective procedures for verifying the bona fides of new customers.

(b) Compliance with laws: bank management should ensure that business is conducted in conformity with high ethical standards, that laws and regulations are adhered to and that a service is not provided where there is good reason to suppose that transactions are associated with laundering activities[2] .

(c) Co-operation with law enforcement agencies: within any constraints imposed by rules relating to customer confidentiality, banks should co-operate fully with national law enforcement agencies including, where there are reasonable grounds for suspecting money laundering, taking appropriate measures which are consistent with the law.

(d) Policies, procedures and training: all banks should formally adopt policies consistent with the principles set out in the Statement, and should ensure that all members of their staff concerned, wherever located, are informed of the bank's policy. Attention should be given to staff training in matters covered by the statement. To promote adherence to these principles, banks should implement specific procedures for customer identification and for retaining internal records of transactions. Arrangements for internal audit may need to be extended in order to establish an effective means for general compliance with the Statement.

4.2 The principles laid down by the Basle Committee have subsequently been developed by the Financial Action Task Force (FATF). In February 1990, FATF put forward forty recommendations aimed at improving national legal systems, enhancing the role of financial systems, and strengthening international co-operation against money laundering. Hong Kong, China is a member of the FATF and fully complies with the forty recommendations.

4.3 The Monetary Authority considers that institutions should follow the basic policies and principles as embodied in the Statement of Principles of the Basle Committee and the FATF recommendations. Specifically the Monetary Authority expects that institutions should have in place the following policies, procedures and controls -

(a) Institutions should issue a clear statement of policies in relation to money laundering, adopting current regulatory requirements. This statement should be communicated in writing to all management and relevant staff whether in branches, departments or subsidiaries and be reviewed on a regular basis.

---

2 Paragraph 9.9 describes the actual application of this principle to an authorized institution.

(b) Instruction manuals should set out institutions' procedures for:

- account opening;
- identification of applicants for business;
- record-keeping;
- reporting of suspicious transactions.

based on the recommendations in the following sections of this Guideline.

(c) Institutions should seek actively to promote close co-operation with law enforcement authorities, and should identify a single reference point within their organization (usually a compliance officer) to which staff are instructed to report suspected money laundering transactions promptly. This reference point should have a means of liaison with the Joint Financial Intelligence Unit which will ensure prompt referral of suspected money-laundering transactions associated with drug trafficking or other indictable offences. The role and responsibilities of this reference point in the reporting procedures should be clearly defined.

(d) Measures should be undertaken to ensure that staff are educated and trained on matters contained in this Guideline both as part of their induction procedures and at regular future intervals. The aim is to generate and maintain a level of awareness and vigilance among staff to enable a report to be made if suspicions are aroused.

(e) Institutions should instruct their internal audit/inspection departments to verify, on a regular basis, compliance with policies, procedures, and controls against money laundering activities.

(f) Whilst appreciating the sensitive nature of extra-territorial regulations, and recognizing that their overseas operations must be conducted in accordance with local laws and regulations, institutions should ensure that their overseas branches and subsidiaries are aware of group policies concerning money laundering and, where appropriate, have been instructed as to the local reporting point for their suspicions.

PART II

DETAILED GUIDELINES

5. Verification of identity of applicants for business

5.1 Institutions should not keep anonymous accounts or accounts in obviously fictitious names. They should obtain satisfactory evidence of the identity and legal existence of persons applying to do business with the institution (such as opening a deposit account) on the basis of reliable documents or other resources, and record that identity and other relevant information regarding the applicant in their files. They should establish that any applicant claiming to act on behalf of another person is authorized to do so.

5.2 For the purposes of this guideline, evidence of identity can be regarded as satisfactory if -

(a) it is reasonably capable of establishing that the applicant for business is whom he claims to be; and

(b) the institution which obtains the evidence is satisfied, in accordance with the procedures established by the institution, that it does establish that fact.

5.3 Repealed. [See section 12 of the Supplement to the Guideline on Prevention of Money Laundering ("the AML Supplement")]

Individual applicants

5.4 Institutions should institute effective procedures for obtaining satisfactory evidence of the identity of applicants for business including obtaining information about name, permanent address, date of birth and occupation.

5.5 Positive identification should be obtained from documents issued by official or other reputable sources e.g. passports or identity cards. For Hong Kong residents, the prime source of identification will be the identity cards which they are required by law to carry with them. File copies of identity documents should be kept.

5.6 However, it must be appreciated that no form of identification can be fully guaranteed as genuine or representing correct identity. The Immigration Department operates a Hotline (Tel. 2824 1551) to which enquiries can be made concerning the validity of an identity card. If there is doubt whether an identification document is genuine, contact should be made with this Hotline immediately.

5.7 Institutions are advised to check the address of the applicant by appropriate means, e.g. by requesting sight of a recent utility or rates bill.

5.8 Where institutions require applicants for personal banking services to provide in the application forms for such services the names and particulars of persons who have agreed to act as referees for the applicants, they should follow the practices and procedures as set out in the section on personal referees of the Code of Banking Practice jointly issued by the Hong Kong Association of Banks and the Deposit-taking Companies Association.

Corporate applicants

5.9 Company accounts are one of the more likely vehicles for money laundering, even where the company is also being used for legitimate trading purposes. It is therefore important to obtain satisfactory evidence of the identity of the principal shareholders[3], directors and authorized signatories and of the nature of the business. The guiding principle should be to establish that it is safe to enter into a business relationship with the company concerned.

5.10 Before a business relationship is established, measures should be taken by way of a company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound-up or terminated. In addition, if institutions become aware of subsequent changes to the company structure or ownership, or suspicions are aroused by a change in the profile of payments through a company account, further checks should be made.

5.11 The following documents or information should be obtained in respect of corporate applicants for business which are registered in Hong Kong (comparable documents, preferably certified by qualified persons such as lawyers or accountants in the country of registration, should be obtained for those applicants which are not registered in Hong Kong) -

(a) Certificate of Incorporation and Business Registration Certificate;

(b) Memorandum and articles of association;

(c) resolution of the board of directors to open an account and confer authority on those who will operate it; and

(d) a search of the file at Company Registry.

5.12 Repealed. [See section 4 of the AML Supplement]

5.13 Repealed. [See section 4 of the AML Supplement]

---

3 It is recommended that "principal shareholders" should include those entitled to exercise, or control the exercise of, 10% or more of the voting rights of the company.

Clubs, societies and charities

5.14 In the case of accounts to be opened for clubs, societies and charities, an institution should satisfy itself as to the legitimate purpose of the organisation by, e.g. requesting sight of the constitution. Satisfactory evidence should be obtained of the identity of the authorized signatories who are not already known to the institution in line with the requirements for individual applicants.

Unincorporated businesses

5.15 In the case of partnerships and other unincorporated businesses whose partners are not known to the bank, satisfactory evidence should be obtained of the identity of at least two partners and all authorized signatories in line with the requirements for individual applicants. In cases where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

Shell companies

5.16 Shell companies are legal entities through which financial transactions may be conducted but which have no business substance in their own right. While shell companies may be used for legitimate purposes, the FATF has expressed concern about the increasing use of such companies to conduct money laundering (through providing the means to operate what are in effect anonymous accounts). Institutions should take notice of the potential for abuse by money launderers of shell companies and should therefore be cautious in their dealings with them. In keeping with the "know your customer" principle, institutions should obtain satisfactory evidence of the identity of beneficial owners, directors and authorized signatories of shell companies. Where the shell company is introduced to the institution by a professional intermediary acting on its behalf, institutions should follow the guidelines in paragraphs 5.17 to 5.22 below.

Where the applicant for business is acting on behalf of another person

5.17 Trust, nominee and fiduciary accounts are a popular vehicle for criminals wishing to avoid identification procedures and mask the origin of the criminal money they wish to launder. Accordingly, institutions should always establish, by confirmation from an applicant for business, whether the applicant is acting on behalf of another person as trustee, nominee or agent.

5.18 Any application to open an account or undertake a transaction on behalf of another person without applicants identifying their trust or nominee capacity should be regarded as suspicious and should lead to further enquiries as to the underlying principals and the nature of the business to be transacted.

5.19 Institutions should obtain satisfactory evidence of the identity of trustees, nominees and authorized signatories and of the nature of their trustee or nominee capacity and duties by, for example, obtaining a copy of the trust deed. Enquiries should also be made of the extent to which the applicant for business is subject to official regulation (e.g. by a body equivalent to the Monetary Authority).

5.20 Particular care should be taken in relation to trusts created in jurisdictions without equivalent money laundering legislation to Hong Kong.

5.21 Repealed. [See section 6 of the AML Supplement]

5.22 Repealed. [See section 6 of the AML Supplement]

Client accounts

5.23 Repealed. [See section 7 of the AML Supplement]

Avoidance of account opening by post

5.24 Repealed. [See section 8 of the AML Supplement]

5.25 Repealed. [See section 8 of the AML Supplement]

Transactions undertaken for non-account holders (occasional customers)

5.26 Where transactions are undertaken by an institution for non-account holders of that institution e.g. requests for telegraphic transfers, or where funds are deposited into an existing account by persons whose names do not appear on the mandate of that account, care and vigilance are required. Where the transaction involves large sums of cash, or is unusual, the applicant should be asked to produce positive evidence of identity from the sources set out above and in the case of a foreign national, the nationality recorded. Copies of the identification documents should be kept on file.

5.27 Repealed. [See paragraphs 3.12 – 3.16 of the AML Supplement]

Provision of safe custody and safety deposit boxes

5.28 Precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the identification procedures set out above should be followed.

6. Remittance

6.1 Repealed. [See section 9 of the AML Supplement]

6.2 Repealed. [See section 9 of the AML Supplement]

6.3 Repealed. [See section 9 of the AML Supplement]

7. Record keeping

7.1 The DTROP and the OSCO entitle the Court to examine all relevant past transactions to assess whether the defendant has benefitted from drug trafficking or other indictable offences.

7.2 The investigating authorities need to ensure a satisfactory audit trail for suspected money laundering transactions and to be able to establish a financial profile of the suspect account. For example, to satisfy these requirements the following information may be sought -

(a) the beneficial owner of the account (for accounts opened on behalf of a third party, please see paragraphs 5.17 to 5.23);

(b) the volume of funds flowing through the account;

(c) for selected transactions:

- the origin of the funds (if known);
- the form in which the funds were offered or withdrawn i.e. cash, cheques etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

7.3 An important objective is for institutions at all stages in a transaction to be able to retrieve relevant information, to the extent that it is available, without undue delay.

7.4 When setting document retention policy, institutions must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. However, wherever practicable the following document retention times should be followed -

(a) account opening records - copies of identification documents should be kept in file for six years [4] following the closing of an account;

(b) account ledger records - six years[4] from entering the transaction into the ledger; and

(c) records in support of entries in the accounts in whatever form they are used e.g. credit/debit slips and cheques and other forms of vouchers - six years[4] from when the records were created.

---

[4] Six years being the statutory limitation period for certain classes of claims under the Limitation Ordinance.

(d) records in support of wire transfer and money changing transactions for non-account holders – six years[4] from when the records were created.

7.5 Retention may be by way of original documents, stored on microfilm, or in computerized form, provided that such forms are accepted as evidence under sections 20 to 22 of the Evidence Ordinance. In situations where the records relate to on-going investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed.

8. Recognition of suspicious transactions

8.1 As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.

8.2 Examples of what might constitute suspicious transactions are given in Annex 5. These are not intended to be exhaustive and only provide examples of the most basic ways in which money may be laundered. However, identification of any of the types of transactions listed in Annex 5 should prompt further investigations and be a catalyst towards making at least initial enquiries about the source of funds.

9. Reporting of suspicious transactions

9.1 The reception point for disclosures under the DTROP and the OSCO is the Joint Financial Intelligence Unit, which is operated by the Police and Customs and Excise Department.

9.2 In addition to acting as the point for receipt of disclosures made by any organization or individual, the unit also acts as domestic and international advisors on money laundering generally and offers practical guidance and assistance to the financial sector on the subject of money laundering.

9.3 The obligation to report is on the individual who becomes suspicious of a money laundering transaction. Each institution should appoint a designated officer or officers (Compliance Officer(s)) who should be responsible for reporting to the Joint Financial Intelligence Unit where necessary in accordance with section 25A of both the DTROP and the OSCO and to whom all internal reports should be made.

9.4 Compliance Officers should keep a register of all reports made to the Joint Financial Intelligence Unit and all reports made to them by employees. Compliance Officers should provide employees with a written acknowledgement of reports made to them, which will form part of the evidence that the reports were made in compliance with the internal procedures.

9.5 All cases where an employee of an institution knows that a customer has engaged in drug-trafficking or other indictable offences and where the customer deposits, transfers or seeks to invest funds or obtains credit against the security of such funds, or where the institution holds funds on behalf of such customer, must promptly be reported to the Compliance Officer who, in turn, must immediately report the details to the Joint Financial Intelligence Unit.

9.6 All cases, where an employee of an institution suspects or has reasonable grounds to believe that a customer might have carried on drug trafficking or might have been engaged in indictable offences and where the customer deposits, transfers or seeks to invest funds or obtains credit against the security of such funds, or where the institution holds funds on behalf of such customer, must promptly be reported to the Compliance Officer. The Compliance Officer must promptly evaluate whether there are reasonable grounds for such belief and must then immediately report the case to the Joint Financial Intelligence Unit unless he considers, and records his opinion, that such reasonable grounds do not exist.

9.7 Institutions must take steps to ensure that all employees concerned with the holding, receipt, transmission or investment of funds (whether in cash or otherwise) or the making of loans against the security of such funds are aware of these procedures and that it is a criminal offence to fail to report either knowledge or circumstances which give rise to a reasonable belief in the existence of an offending act.

9.8 Institutions should make reports of suspicious transactions to the Joint Financial Intelligence Unit as soon as it is reasonable for them to do so. The use of a standard format as set out in Annex 6 or use of the e-channel "STREAMS' by registered users for reporting is encouraged. In the event that urgent disclosure is required, particularly when the

account concerned is part of an on-going investigation, an initial notification should be made by telephone.

9.9 Institutions should refrain from carrying out transactions which they know or suspect to be related to money laundering until they have informed the Joint Financial Intelligence Unit which consents to the institution carrying out the transactions. Where it is impossible to refrain or if this is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, institutions may carry out the transactions and notify the Joint Financial Intelligence Unit on their own initiative and as soon as it is reasonable for them to do so.

9.10 Cases do occur when an institution declines to open an account for an applicant for business, or refuses to deal with a request made by a non-account holder because of serious doubts about the good faith of the individual and concern about potential criminal activity. Institutions must base their decisions on normal commercial criteria and internal policy. However, to guard against money laundering, it is important to establish an audit trail for suspicious funds. Thus, where practicable, institutions are requested to seek and retain copies of relevant identification documents which they may obtain and to report the offer of suspicious funds to the Joint Financial Intelligence Unit.

9.11 Where it is known or suspected that a report has already been disclosed to the Joint Financial Intelligence Unit and it becomes necessary to make further enquiries of the customer, great care should be taken to ensure that the customer does not become aware that his name has been brought to the attention of the law enforcement agencies.

9.12 Following receipt of a disclosure and research by the Joint Financial Intelligence Unit, the information disclosed is allocated to trained financial investigation officers in the Police and Customs and Excise Department for further investigation including seeking supplementary information from the institution making the disclosure, and from other sources. Discreet enquiries are then made to confirm the basis for suspicion.

9.13 Access to the disclosed information is restricted to financial investigating officers within the Police and Customs and Excise Department. In the event of a prosecution, production orders are obtained to produce the material for court. Section 26 of both the DTROP and the OSCO places strict restrictions on revealing the identity of the person making disclosure under section 25A. Maintaining the integrity of the relationship which has been established between law enforcement agencies and institutions is considered to be of paramount importance.

10. Feedback from the investigating authorities

10.1 The Joint Financial Intelligence Unit will acknowledge receipt of a disclosure made by an institution under section 25A of both the DTROP and the OSCO, and section 12 of the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO). If there is no imminent need for action e.g. the issue of a restraint order on an account, consent will usually be given for the institution to operate the account under the provisions of section 25A(2) of both the DTROP and the OSCO. An example of such a letter is given at Annex 7 to this Guideline. For disclosure submitted via e-channel "STREAM", e-receipt will be issued via the same e-channel.

10.2 Whilst there are no statutory requirements to provide feedback arising from investigations, the Police and Customs and Excise Department recognize the importance of having effective feedback procedures in place. The Joint Financial Intelligence Unit presently provides a service, on request, to a disclosing institution in relation to the current status of an investigation.

11. Staff education and training

11.1 Staff must be aware of their own personal legal obligations under the DTROP, OSCO and UNATMO that they can be personally liable for failure to report information to the authorities. They must be encouraged to co-operate fully with the law enforcement agencies and promptly to report suspicious transactions. They should be advised to report suspicious transactions to their institution's Compliance Officer even if they do not know precisely what the underlying criminal activity is or whether illegal activities have occurred.

11.2 It is, therefore, imperative that institutions introduce comprehensive measures to ensure that staff are fully aware of their responsibilities.

11.3 Institutions should therefore provide proper anti-money laundering training to their local as well as overseas staff. The timing and content of training packages for various sectors of staff will need to be adapted by individual institutions for their own needs. However, it is recommended that the following might be appropriate -

(a) New Employees

A general appreciation of the background to money laundering, the consequent need to be able to identify suspicious transactions and report such transactions to the appropriate designated point within the institution, and the offence of "tipping off" should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the legal requirement to report suspicious transactions relating to drug trafficking or other indictable offences, and that there is also a personal statutory obligation in this respect.

(b) Cashiers/Tellers/Foreign Exchange Operators/Advisory Staff

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are therefore vital to the institution's strategy in the fight against money laundering. They should be made aware of their legal responsibilities and the institution's reporting system for such transactions.

Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. It is vital that "front-line" staff are made aware of the institution's policy for dealing with non-regular customers particularly where large cash transactions are involved, and the need for extra vigilance in these cases.

(c) Account Opening/New Client Personnel

Those members of staff who are in a position to deal with account opening, or to accept applicants for business, must receive the training given to cashiers etc. in (b) above. In addition, the need to verify the identity of the applicant must be understood, and training should be given in the institution's account opening and customer/client verification procedures. Such staff should be

aware that the offer of suspicious funds or the request to undertake a suspicious transaction need to be reported to the relevant authorities whether or not the funds are accepted or the transactions proceeded with and they must know what procedures to follow in this respect.

(d) Administration/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the DTROP and the OSCO; procedures relating to service of production and restraint orders; and the requirements for retention of records.

(e) On-going Training

It will also be necessary to make arrangements for refresher training at regular intervals to ensure that staff do not forget their responsibilities.

(f) Training Package

Institutions should acquire sufficient copies of the training materials produced by the Hong Kong Association of Banks for the purpose of training front line staff. All front line staff who deal directly with customers should have a copy of the booklet and all new front line staff should view the video upon joining the institution.

Repealed

Repealed

Repealed

Repealed

EXAMPLES OF SUSPICIOUS TRANSACTIONS

1. Money Laundering Using Cash Transactions

a) Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

b) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

c) Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

d) Company accounts whose transaction, both deposits and withdrawals, are denominated in cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.).

e) Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments.

f) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

g) Frequent exchange of cash into other currencies.

h) Branches that have a great deal more cash transactions than usual. (Head Office statistics should detect aberrations in cash transactions.)

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

j) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

k) Large cash deposits using night safe facilities, thereby avoiding direct contact with the institution.

l) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the institution.

m) Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their retail business.

2. Money Laundering Using Bank Accounts

a) Customers who wish to maintain a number of trustee or clients' accounts which do not appear consistent with their type of business, including transactions which involve nominee names.

b) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

c) Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

d) Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify.

e) Customers who appear to have accounts with several institutions within the same locality, especially when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

f) Matching of payments out with credits paid in by cash on the same or previous day.

g) Paying in large third party cheques endorsed in favour of the customer.

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

i) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

j) Greater use of safe deposit facilities by individuals. The use of sealed packets deposited and withdrawn.

k) Companies' representatives avoiding contact with the branch.

l) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.

m) Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

n) Large number of individuals making payments into the same account without an adequate explanation.

o) Customers who maintain an unusually large number of accounts for the type of business they are purportedly conducting and/or use inordinately large number of fund transfers among these accounts.

p) High velocity of funds through an account, i.e., low beginning and ending daily balances, which do not reflect the large volume of dollars flowing through an account.

q) Multiple depositors using a single bank account.

r) An account opened in the name of a money changer that receives structured deposits.

s) An account operated in the name of an off-shore company with structured movement of funds.

3. Money Laundering Using Investment Related Transactions

a) Purchasing of securities to be held by the institution in safe custody, where this does not appear appropriate given the customer's apparent standing.

b) Back to back deposit/loan transactions with subsidiaries of, or affiliates of, overseas financial institutions in known drug trafficking areas.

c) Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.

d) Larger or unusual settlements of securities transactions in cash form.

e) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. Money Laundering Involving Off-Shore International Activity

a) Customers introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.

b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

c) Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs.

d) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

e) Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.

f) Frequent requests for travellers cheques, foreign currency drafts or other negotiable instruments to be issued.

g) Frequent paying in of travellers cheques, foreign currency drafts particularly if originating from overseas.

h) Numerous wire transfers received in an account but each transfer is below the reporting requirement in the remitting country.

i) Customers sending and receiving wire transfer to/from financial haven countries, particularly if there are no apparent business reasons for such transfers or such transfers are not consistent with the customers' business or history.

5. Money Laundering Involving Authorized Institution Employees and Agents

a) Changes in employee characteristics, e.g. lavish life styles.

b) Any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, contrary to normal procedure for the type of business concerned.

6. Money Laundering by Secured and Unsecured Lending

a) Customers who repay problem loans unexpectedly.

b) Request to borrow against assets held by the institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

c) Request by a customer for an institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

d) A customer who is reluctant or refuses to state a purpose of a loan or the source of repayment, or provides a questionable purpose and/or source.

Report made under Section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance and the Organized and Serious Crimes Ordinance to the Joint Financial Intelligence Unit

Date:
Ref. No.:

(A) SOURCE

Name of Institution:	
Reporting Officer:	Tel. No.:
Signature:	Fax No.:

(B) SUSPICION

(Please provide details of transaction arousing suspicion and any other relevant information. Please also enclose copy of the transaction for reference. Particulars of account holder or person conducting the transaction are to be given in page 2.)

(C) OTHER INFORMATION

This is a new disclosure:	Yes/No	JFIU No.:
This disclosure relates to a previous disclosure:	JFIU No.:	Bank Ref. No.:

(D) SUBJECT (1)

Name:	C.C.C.:	Date of Birth:
HKIC/PPT No.:	Sex: M/F	Nationality:
Address:		
Occupation:	Company:	
Position Held:	Company Address:	

SUBJECT (2)

Name:	C.C.C.:	Date of Birth:
HKIC/PPT No.:	Sex: M/F	Nationality:
Address:		
Occupation:	Company:	
Position Held:	Company Address:	

SUBJECT (3)

Name:	C.C.C.:	Date of Birth:
HKIC/PPT No.:	Sex: M/F	Nationality:
Address:		
Occupation:	Company:	
Position Held:	Company Address:	

(E) RELATED BANK ACCOUNT(s)

	(1)	(2)
Account No.:		
Type of Account:		
Date of Opening:		
Account Balance:		
Account Holder(s):		

	(3)	(4)
Account No.:		
Type of Account:		
Date of Opening:		
Account Balance:		
Account Holder(s):		

Annex 7

Example of Acknowledgement of Receipt by JFIU

Date:

The Compliance Officer
[ ] Bank Ltd.

Fax No. :

Dear Sir/Madam,

Acknowledgement of Receipt of
Suspicions Transaction Report(s) ("STR")

I acknowledge receipt of the attached STR made in accordance with the provisions of section 25A(1) of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap 405) / Organized and Serious Crimes Ordinance (Cap 455) and section 12(1) of the United Nations (Anti-Terrorism Measures) Ordinance(Cap 575).

Based upon the information currently in hand, consent is given under the provisions of section 25A(2) & (3) of Cap 405 and 455 and section 12(2) & (3) of Cap 575.

If you have any queries, please feel free to contact the undersigned on telephone number (852)xxxxxxxx.

Yours faithfully,

( )
Joint Financial Intelligence Unit

Repealed

SUPPLEMENT TO THE GUIDELINE ON PREVENTION OF MONEY LAUNDERING

A Guideline issued by the Monetary Authority under section 7(3) of the Banking Ordinance

Revised July 2010

CONTENTS

1. Introduction

1.1 The current HKMA Guideline on Prevention of Money Laundering (Guideline) was issued in 1997. Amendments were made in 2000, mainly to take into account the provisions of the Organized and Serious Crimes (Amendment) Ordinance 2000.

1.2 A number of significant developments have taken place since then, which call for enhanced standards in the effective prevention of money laundering. These include, in particular, the issuance by the Basel Committee on Banking Supervision of the paper "Customer Due Diligence for Banks" in October 2001 and the revised Forty Recommendations issued by the Financial Action Task Force on Money Laundering (FATF) in June 2003. Moreover, the 9/11 event has expanded the scope of the effort on prevention of money laundering to include the fight against terrorist financing.

1.3 The HKMA considers it necessary to revise its regulatory requirements to take into account recent developments and the initiatives undertaken by international bodies. It is considered appropriate to reflect the changes, for the time being, in a Supplement to the Guideline pending revision of the Guideline to consolidate all changes issued since 2000 and achieve greater harmonisation with the requirements of the other financial regulators.

1.4 This Supplement mainly reflects the regulatory standards recommended in the Basel Committee paper on customer due diligence and takes into account the relevant requirements in the FATF revised Forty Recommendations. The Supplement also incorporates additional guidance issued by the HKMA since 2000 and recommendations related to terrorist financing, including the recently enacted anti-terrorism legislation in Hong Kong.

1.5 Unless indicated otherwise, provisions in this Supplement should be read or interpreted in conjunction with the relevant parts of the Guideline (~~December~~July 2010 version as currently posted in the HKMA website – (***http//www.info.gov.hk/hkma/eng/guide/index.htm*** at Guideline 3.3) and the accompanying interpretative notes (IN).

1.6 ~~In general~~Unless otherwise stated, the requirements in this Supplement apply to all new customers~~,~~ and existing customers when they are due for review in accordance with section 12 of this Supplement. ~~except where it is clear from the context that they also apply to existing customers.~~

1.7 For Hong Kong incorporated authorized institutions (AIs), the requirements also apply to their overseas branches or subsidiaries [IN 1]. Where the local requirements differ from these requirements, the overseas operations should apply the higher standard to the extent that local laws permit. Where an overseas branch or subsidiary is unable to observe group standards, the HKMA should be informed.

1.8 This revised Supplement will supersede the last version issued on ~~13 November~~17 July 200~~7~~9 with effect from ~~**24 July 2009**~~**1 November 2010**.

2. Customer acceptance policy

2.1 This is a new section not currently covered in the Guideline.

2.2 An AI should develop customer acceptance policies and procedures that aim to identify the types of customer that are likely to pose a higher than average risk of money laundering (see risk-based approach under the General Guidance Section of IN). A more extensive customer due diligence process should be adopted for higher risk customers. There should also be clear internal guidelines on which level of management is able to approve a business relationship with such customers.

2.3 In determining the risk profile of a particular customer or type of customer, an AI should take into account factors such as the following:

(a) the customer's nationality, citizenship and resident status (in the case of a corporate customer, the customer's place of incorporation), the place where its business is established, the location of the counterparties with whom it conducts business, and whether the customer is otherwise connected with higher risk jurisdictions or jurisdictions which do not or insufficiently apply the FATF Recommendations (see section 14 below), or which are known to the AI to lack proper standards in the prevention of money laundering or customer due diligence process [IN 3];

(b) background or profile of the customer such as being, or linked to, a politically exposed person (see section 10 below~~ and IN 34~~) or otherwise being an individual with high net worth whose source of funds to be credited to an account (both initially and thereafter) is unclear;

(c) nature of the customer's business, which may be particularly susceptible to money laundering risk, such as money changers or casinos that handle large amounts of cash;

(d) for a corporate customer, unduly complex structure of ownership for no good reason; and

(e) any other information that may suggest that the customer is of higher risk (e.g. knowledge that the customer has been refused a banking relationship by another institution).

2.4 Following the initial acceptance of the customer, a pattern of account activity that does not fit in with the AI's knowledge of the customer may lead the AI to reclassify the customer as higher risk.

3. Customer due diligence

3.1 This section reinforces paragraphs 5.1 and 5.2 of the Guideline and introduces new requirements.

3.2 The customer due diligence process should comprise the following:

(a) identify the direct customer, i.e. know who the individual or legal entity is;

(b) verify the customer's identity using reliable, independent source documents, data or information [IN 4];

(c) identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the direct customer, and/or the person on whose behalf a transaction is being conducted;

(d) take reasonable measures to verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c);

(da) obtain information on the purpose and reason for opening the account or establishing the relationship, unless it is self-evident; and

(e) conduct on-going due diligence and scrutiny i.e. perform on-going scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the AI's knowledge of the customer, its business and risk profile, including, where necessary, identifying the source of funds.

3.3 The identity of an individual ~~[IN 5]~~ includes the individual's name (including former or other name(s)), ~~residential address (and permanent address if different) [IN 6],~~ date of birth, ~~and~~ nationality and Hong Kong identity card number [IN 5]. To facilitate on-going due diligence and scrutiny, information on the individual's occupation [IN 7] or business should also be obtained. AIs should also record and verify the address [IN 6] of a direct customer with whom it establishes business relations. For connected parties (i.e. account signatories, directors, principal shareholders, etc.) and transactions undertaken by non-account holders, AIs should determine the need to verify the address of these parties on the basis of risk and materiality.

3.4 Unwillingness of the customer, for no good reason, to provide the information requested and to cooperate with the AI's customer due diligence process may itself be a factor that should trigger suspicion.

3.5 Where an AI allows confidential numbered accounts (i.e. where the name of the account holder is known to the AI but is substituted by an account number or code name in subsequent documentation) the same customer due diligence process should apply even if this is conducted by selected staff. The identity of the account holder should be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from an AI's compliance function or from the HKMA.

3.6 An AI should not in general establish a business relationship with a new customer until the due diligence process is satisfactorily completed. However, it may be acceptable to allow an account to be opened pending completion of the verification of identity provided that the necessary evidence of identity is promptly obtained. In such a case an AI should not allow funds to be paid out of the account to a third party before the identity of the customer is satisfactorily verified [IN 8].

3.7 If an account has been opened but the process of verification of identity cannot be successfully completed, the AI should close the account and return any funds to the source from which they were received [IN 9]. Consideration should also be given to whether a report should be made to the Joint Financial Intelligence Unit (JFIU). The return of funds should be subject to any request from the JFIU to freeze the relevant funds.

3.8 After a business relationship is established, an AI should undertake regular reviews of the existing records relating to the customer to ensure that they remain up-to-date and relevant. As indicated in paragraph 12.3 an appropriate time to do so is upon certain trigger events.

Transactions undertaken by non-account holders

3.9 This section supplements paragraph 5.26 of the Guideline.

3.10 An AI should also conduct the following when carrying out transactions [IN 9a] exceeding HK$120,000 on behalf of a customer who has not otherwise established a business relationship with the AI (i.e. a non-account holder) regardless of whether the transaction is carried out in a single or multiple operations between which there is an obvious connection:

(i) identify and verify the direct customer;
(ii) identify and verify any natural persons representing the customer, including the authority such persons have to act;
(iii) enquire if any beneficial owner exists and take reasonable measures to verify the identity of any such beneficial owner;
(iv) take reasonable measures to understand the ownership structure if the customer is a corporate; and
(v) ascertain the intended nature and purpose of the transaction, unless obvious.

3.11 If there is any suspicion of money laundering or terrorist financing, an AI should perform the measures detailed in paragraph 3.10 (i) to (v) when carrying out any transaction for a non-account holder regardless of the $120,000 threshold.

Additional requirements for wire transfer & currency exchange transactions performed by non-account holders

3.12 This section supersedes paragraph 5.27 of the Guideline.

3.13 Irrespective of the threshold mentioned in paragraph 3.10 above, the following requirements apply for wire transfer and currency exchange transactions:

Wire transfers

3.14 When acting as the ordering institution for a wire transfer of any value the AI should record the identity and address of the originator. For wire transfers equal to or exceeding HK$8,000, an AI should verify the originator's identity by reference to his identity card or travel document [IN 9b].

3.15 When acting as the beneficiary institution for a wire transfer of any value for a beneficiary who is not an account holder, the AI should record the identity and address of the recipient. For wire transfers equal to or exceeding HK$8,000, an AI should verify the recipient's identity by reference to his identity card or travel document [IN 9b]).

Currency exchange transactions

3.16 When performing a currency exchange transaction equivalent to HK$8,000 or more on behalf of a non-account holder, the AI must record the identity and address of the individual and verify his identity by reference to his identity card or travel document [IN 9b].

4. Corporate customers

4.1 This section supersedes paragraphs 5.12 and 5.13 of the Guideline and does not apply to customers that are banks (covered in section 11 below).

4.2 Where a customer is a company which is listed on a recognised stock exchange [IN 10] ~~(or is a subsidiary of such a listed company)~~ or is a state-owned enterprise~~ [IN 11]~~ or is a subsidiary of a listed company or state-owned enterprise, the customer itself can be regarded as the person whose identity is to be verified. It will therefore generally be sufficient for an AI to obtain and retain sufficient information to effectively identify and verify the identity of the customer (which will include proof of its listed status on a recognised stock exchange), the natural persons appointed to act on behalf of the customer and their authority to do so [IN 11]. ~~the documents specified in paragraph 5.11 [IN 12] of the Guideline without the need to make further enquiries about the identity of the principal shareholders [IN 13], individual directors or account signatories. However, evidence that any individual representing the company has the necessary authority to do so should be sought and retained.~~

4.3 Where a listed company is effectively controlled by an individual or a small group of individuals, an AI should consider whether it is necessary to verify the identity of such individual(s).

4.4 Where a non-bank financial institution is authorized and supervised by the Securities and Futures Commission ("SFC"), Insurance Authority ("OCI") or an equivalent authority in a jurisdiction that is a FATF member or an ~~comparable~~equivalent jurisdiction [IN 14], it will generally be sufficient for an

AI to verify that the institution is on the list of authorized (and supervised) financial institutions in the jurisdiction concerned. Evidence that any individual representing the institution has the necessary authority to do so should be sought and retained.

4.5 In relation to a company which is not listed [IN 15] on a recognised stock exchange (or is not a subsidiary of such a listed company) or not a state-owned enterprise or is a non-bank financial institution other than those mentioned above in paragraph 4.4, an AI should look behind the company [IN 16] to identify the beneficial owners and those who have control over the funds. This means that, in addition to obtaining the documents specified in paragraph 5.11 of the Guideline ~~[IN 12]~~, the AI should verify the identity [IN 17] of all the principal shareholders [IN 13], at least one ~~two [IN 18]~~ directors ~~(including the managing director)~~ of the company and all its account signatories [IN 19]. AIs should consider the need to verify the identity of additional directors on the basis of risk and materiality.

4.6 Where the direct customer of an AI is a non-listed company which has a number of layers of companies in its ownership structure, the AI is not required, as a matter of course, to check the details of each of the intermediate companies (including their directors) in the ownership chain. The objective should be to follow the chain of ownership to the individuals who are the ultimate principal beneficial owners of the direct customer of the AI and to verify the identity of those individuals [IN 20]. Where a customer has in its ~~in the~~ ownership chain an entity which is

(a) a company listed on a recognised stock exchange ~~(~~or ~~is~~ a subsidiary of such a listed company~~)~~;;
(b) a state-owned enterprise or a subsidiary of a state-owned enterprise;
(c) a financial institution regulated by the HKMA, SFC or OCI; or
(d) a financial institution supervised and regulated by an authority that performs functions equivalent to those of the HKMA, SFC or OCI for anti-money laundering and counter terrorist financing (AML/CFT) purposes in a jurisdiction that is a FATF member or an equivalent jurisdiction,

it should generally be sufficient for the AI ~~to stop at that point and~~ to verify the identity of that ~~customer~~entity in ~~line~~accordance with ~~the recommendations in~~ paragraphs 4.2 and 4.4 above. However, AIs should still verify the identity of the beneficial owners in the ownership chain that are not connected with the above entity.

4.7 An AI should understand the ownership structure of non-listed corporate customers and determine the source of funds [IN 21]. As indicated in paragraph 2.3(d), an unduly complex ownership structure for no good reason is a risk factor to be taken into account.

4.8 An AI should exercise special care in initiating business transactions with companies that have nominee shareholders. Satisfactory evidence of the identity of beneficial owners of such companies should be obtained.

4.9 An AI should also exercise special care in dealing with companies which have a significant proportion of capital in the form of bearer shares. The AI should

have procedures to monitor the identity of all principal shareholders. This may require the AI to consider whether to immobilize the shares, such as by holding the bearer shares in custody [IN 22].

5. Trust and nominee accounts

5.1 This section should be read in conjunction with paragraph 5.17 to 5.20 of the Guideline.

5.2 An AI should understand the relationship among the relevant parties in handling a trust or nominee account. There should be satisfactory evidence [IN 23] of the identity of the trustees or nominees, and the persons on whose behalf they are acting, as well as the details of the nature of the trust or other similar arrangements in place.

5.3 Specifically, in relation to trusts, an AI should obtain satisfactory evidence of the identity of trustees, protectors [IN 24], settlors/grantors [IN 25] and beneficiaries. Beneficiaries should be identified as far as possible where defined [IN 26 & 27].

5.4 As with other types of customer, an AI should adopt a risk-based approach in relation to trusts and the persons connected with them. The extent of the due diligence process should therefore depend on such factors as the nature and complexity of the trust arrangement.

6. Reliance on intermediaries for customer due diligence

6.1 This section supersedes paragraphs 5.21 and 5.22 of the Guideline. It refers to intermediaries which introduce customers to an AI. This however does not cover outsourcing or agency relationships (i.e. where the agent is acting under a contractual arrangement to carry out customer due diligence for the AI) and business relationships, accounts or transactions between financial institutions (as defined by FATF) for their clients.

6.1a For the purpose of this section, intermediary is defined as:

(i) a financial institution regulated by the HKMA, SFC or OCI;

(ii) a person who is professionally or legally registered in Hong Kong as a lawyer, auditor, accountant, trust company or chartered secretary and who carries on business in Hong Kong as such; or

(iii) a person who carries on business in an equivalent jurisdiction being
- (A) a financial institution, lawyer, notary public, auditor, accountant, tax advisor, trust company or chartered secretary;
- (B) subject to mandatory professional registration, licensing or regulation recognised by law;
- (C) subject to requirements consistent with the FATF standards; and
- (D) supervised for compliance with those requirements.

6.2 An AI may rely on such intermediaries to perform customer due diligence procedures. However, the ultimate responsibility for knowing the customer always remains with the AI.

6.3 An AI should assess whether the intermediaries they use are "fit and proper" and are exercising adequate due diligence procedures. In this regard the following criteria should be used to identify whether an intermediary can be relied upon [IN 28]:

(a) the customer due diligence procedures of the intermediary should be as rigorous as those which the AI would have conducted itself for the customer;

(b) the AI must satisfy itself as to the reliability of the systems put in place by the intermediary to verify the identity of the customer; and

(c) the AI must reach agreement with the intermediary that it will be permitted to verify the due diligence undertaken by the intermediary at any stage.

6.4 Repealed.~~To provide additional assurance that these criteria can be met, it is advisable for an AI to rely, to the extent possible, on intermediaries which are incorporated in, or operating from, a jurisdiction that is a FATF member or a comparable jurisdiction [IN 14] and:~~

~~(a) regulated by the HKMA, Securities and Futures Commission or Insurance Authority or by an authority that performs functions equivalent to these; or~~

~~(b) if not so regulated, are able to demonstrate that they have adequate procedures to prevent money laundering.~~

6.5 An AI should conduct periodic reviews to ensure that an intermediary upon which it relies continues to conform to the criteria set out above. This may involve review of the relevant policies and procedures of the intermediary and sample checks of the due diligence conducted.

6.6 An Intermediary Certificate (see Annex) duly signed by the intermediary should be obtained by AIs, together with all relevant identification data and other documentation pertaining to the customer's identity [IN 29]. Relevant documentation should consist of either the original documentation (which is preferable) or copies that have been certified by a suitable certifier.

6.7 The purpose of obtaining the underlying documentation is to ensure that it is immediately available on file for reference purposes by the AI or relevant authorities such as the HKMA and the JFIU, and for on-going monitoring of the customer. It will also enable the AI to verify that the intermediary is doing

its job properly. It is not the intention that the AI should use the documentation, as a matter of course, to repeat the due diligence conducted by the intermediary.

Non face-to-face Document Verification

6.8 A suitable certifier will certify that he has seen the original documentation and that the copy document which has been certified is a complete and accurate copy of that original. The signature and official stamp of the certifier should be placed on the first page of the copy document and the number of pages should be recorded. A suitable certifier will either be the intermediary itself or:

(a) an embassy, consulate or high commission of the country of issue of the documentary evidence of identity;

(b) a member of the judiciary, a senior civil servant or serving police or customs officer in a jurisdiction that is a FATF member or an ~~comparable~~equivalent jurisdiction;

(c) a lawyer, notary public, actuary, ~~or~~ accountant or a chartered secretary in a jurisdiction that is a FATF member or an ~~comparable~~equivalent jurisdiction; or

~~(ca) a member of the Hong Kong Institute of Chartered Secretaries; or~~

(d) a director, officer or manager of a regulated financial institution incorporated in, or operating from, a jurisdiction that is a FATF member or an ~~comparable~~equivalent jurisdiction.

7. Client accounts

7.1 This section supersedes paragraph 5.23 of the Guideline. It refers to accounts opened in the name of a professional intermediary [IN 30] or of a unit trust, mutual fund, or any other investment scheme (including staff provident fund and retirement scheme) managed or administered by a professional intermediary as an agent.

7.2 If a client account is opened on behalf of a single client or there are sub-accounts for each individual client where funds are not co-mingled at the AI, the AI should establish the identity of the underlying client(s) in addition to that of the intermediary opening the account.

7.3 For a client account in which funds for individual clients are co-mingled [IN 31], the AI is not required, as a matter of course, to identify the individual clients. This is however subject to the following (see also paragraph 6.41a above):

(a) the AI is satisfied that the intermediary has put in place reliable systems to verify customer identity; and

(b) the AI is satisfied that the intermediary has proper systems and controls to allocate funds in the pooled account to the individual underlying clients.

7.4 Where an intermediary cannot satisfy the above conditions and refuses to provide information about the identity of underlying clients by claiming, for example, reliance on professional secrecy, an AI should not permit the intermediary to open a client account.

7.5 An AI should not be precluded from making reasonable enquiries about transactions passing through client accounts that give cause for concern or from reporting those transactions if any suspicion is aroused.

8. Non-face-to-face customers

8.1 This section supersedes paragraphs 5.24 and 5.25 of the Guideline.

8.2 An AI should whenever possible conduct a face-to-face interview with a new customer to ascertain the latter's identity and background information, as part of the due diligence process. This can be performed either by the AI itself or by an intermediary that can be relied upon to conduct proper customer due diligence (see section 6 above).

8.3 This is particularly important for higher risk customers. For the latter, the AI should ask the customer to make himself available for a face-to-face interview.

8.4 Where face-to-face interview is not conducted, for example where the account is opened via the internet, an AI should apply equally effective customer identification procedures and on-going monitoring standards as for face-to-face customers.

8.5 Examples of specific measures that AIs can use to mitigate the risk posed by such non-face-to-face customers include:

(a) certification of identity documents presented by suitable certifiers (see paragraph 6.8 above);

(b) requisition of additional documents to complement those required for face-to-face customers;

(c) completion of on-line questionnaires for account opening applications that require a wide range of information capable of independent verification (such as confirmation with a government department);

(d) independent contact with the customer by the AI;

(e) third party introduction through an intermediary which satisfies the criteria in paragraphs 6.1a and 6.3 ~~and 6.4~~ above;

(f) requiring the first payment from the account to be made through an account in the customer's name with another AI or foreign bank which the AI is satisfied has similar customer due diligence standards to its own;

(g) more frequent update of the information on non-face-to-face customers; or

(h) in the extreme, refusal of business relationship without face-to-face contact for higher risk customers.

9. ~~Remittance~~Wire transfer messages

9.1 This section supersedes paragraphs 6.1 to 6.3 of the Guideline. The requirements are based on the FATF Special Recommendation on Terrorist Financing (see paragraph 15.3) that relates to ~~remittance~~wire transfer and the associated Interpretative Note.

9.2 An ordering AI must ensure that any wire transfer of HK$8,000 or more (or its foreign currency equivalent) is accompanied by the following information: the originator's name, account number (or unique reference number if no account exists) and (i) address [IN 32a]; or (ii) national identity number [IN32bb]; or (iii) date and place of birth. AIs should ensure that only verified information accompanies such transfers ~~An ordering AI in a remittance transaction must always include in the remittance message the name of the originating customer and where an account exists the number of that account. The message should also contain the address [IN 32a] of the originating customer or, failing this, the customer's date of birth or the number of a government-issued identity document the customer holds (e.g. identity card, passport)~~ [IN 32b].

9.3 An ordering AI may choose not to include all the above information in the ~~remittance~~wire transfer message accompanying a ~~remittance~~wire transfer of less than HK$8,000 or its equivalent in foreign currencies [IN 32c]. The relevant information about the originator should nevertheless (and notwithstanding paragraph 5.27 of the Guideline [IN 33]) be recorded and retained by the ordering AI and should be made available within 3 business days upon request from either the beneficiary financial institution or appropriate authorities.

9.4 An ordering AI should adopt a risk-based approach to check whether certain ~~remittance~~wire transfers may be suspicious taking into account such factors as the name of the beneficiary, the destination and amount of the ~~remittance~~wire transfer etc.

9.5 In particular, an ordering AI should exercise care if there is suspicion that a customer may be effecting a ~~remittance~~wire transfer transaction on behalf of a third party. If a ~~remittance~~wire transfer carries the name of a third party as the ordering person or otherwise does not appear to be consistent with the usual business / activity of the customer, the customer should be asked to provide further explanation of the nature of the ~~remittance~~wire transfer.

9.6 An AI acting as an intermediary in a chain of ~~remittance~~wire transfers should ensure that the information in paragraph 9.2 remains with the ~~remittance~~wire transfer message throughout the payment chain.

9.7 An AI handling incoming ~~remittance~~wire transfers for a beneficiary should conduct enhanced scrutiny of, and monitor for, ~~remittance~~wire transfer messages which do not contain complete originator information. This can be done through risk-based methods taking into account factors that may arouse suspicion (e.g. country of origin of the ~~remittance~~wire transfer). If necessary, this may be done after effecting the transaction particularly for items handled by straight-through processing.

9.8 The beneficiary AI should consider whether unusual ~~remittance~~wire transfer transactions should be reported to the JFIU. It may also need to consider restricting or terminating its business with a remitting bank that fails to meet the FATF standards.

10. Politically exposed persons

10.1 This is a new section not currently covered in the Guideline.

10.2 Business relationships with individuals holding important public positions as well as persons or companies clearly related to them (i.e. families, close associates etc) expose an AI to particularly significant reputation or legal risks. There should be enhanced due diligence in respect of such politically exposed persons (PEPs). While this is particularly relevant to private banking business, the same enhanced due diligence should apply to PEPs in all business areas.

10.3 PEPs are defined as individuals being, or who have been, entrusted with prominent public functions, such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of public organisations and senior political party officials. The concern is that there is a possibility, especially in countries where corruption is widespread, that such PEPs may abuse their public powers for their own illicit enrichment through the receipt of bribes etc.

10.4 ~~An AI should gather sufficient information from a new customer, and check publicly available information to establish whether or not the customer is a PEP [IN 34]. An AI considering to establish a relationship with a person suspected to be a PEP should identify that person fully, as well as people and companies that are clearly related to him.~~ An AI should have appropriate systems and controls in place to determine, as far as practicable, whether a potential customer, customer or a connected party of a potential customer or direct customer [IN 34a] is a PEP. This could be achieved for example, by screening the name of the customer and connected parties against publicly available information or a commercial electronic database to determine whether the customer or connected parties are politically exposed, before establishing a business relationship, or performing any one off transaction equivalent to

HK$120,000 or more for a non account holder, and on a periodic basis thereafter.

10.5 ~~An AI should also ascertain the source of funds [IN 21] before accepting a PEP as customer. The decision to open an account for a PEP should be taken at a senior management level.~~AIs must obtain senior management approval before establishing a business relationship with a customer or a beneficial owner identified as a PEP. An AI must also obtain senior management approval to continue the relationship as soon as practicable after an existing customer or a beneficial owner is identified as a PEP.

10.5a An AI should take reasonable measures to identify the source of wealth and funds of a customer identified as a PEP [IN 34b]; and ensure increased ongoing monitoring of the customer and his business with the AI throughout the relationship. This will include a periodic review on at least an annual basis of the relationship (and account activities).

10.6 Risk factors an AI should consider in handling a business relationship (or potential relationship) with a PEP include:

(a) any particular concern over the country where the PEP holds his public office or has been entrusted with his public functions, taking into account his position;

(b) any unexplained sources of wealth or income (i.e. value of assets owned not in line with the PEP's income level);

(c) expected receipts of large sums from governmental bodies or state-owned entities;

(d) source of wealth described as commission earned on government contracts;

(e) request by the PEP to associate any form of secrecy with a transaction; and

(f) use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

11. Correspondent banking

11.1 This is a new section not currently covered in the Guideline.

11.2 Correspondent banking is defined as the provision by one bank (the correspondent) to another bank (the respondent) of credit, deposit, collection, clearing, payment or other similar services [IN 35].

11.3 An AI providing correspondent banking services should gather sufficient information about its respondent banks to understand the latter's business. This basic level of due diligence should be performed regardless of whether a credit

facility is granted to a respondent bank. AIs should obtain approval from senior management [IN 36] before establishing new correspondent banking relationships and document the respective responsibilities of each institution.

11.4 The information to be collected [IN 37] should include details about the respondent bank's management, major business activities, where it is located, its money laundering prevention efforts [IN 38], the system of bank regulation and supervision in the respondent bank's country and the purpose of the account etc.

11.5 An AI should in general establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.

11.6 In particular, an AI should not establish or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which the bank has no presence and which is unaffiliated with a regulated financial group (i.e. a shell bank).

11.7 An AI should pay particular attention when maintaining a correspondent banking relationship with banks incorporated in jurisdictions that do not meet international standards for the prevention of money laundering. Enhanced due diligence will generally be required in such cases, including obtaining details of the beneficial ownership of such banks and more extensive information about their policies and procedures to prevent money laundering. There should also be enhanced procedures in respect of the on-going monitoring of activities conducted through such correspondent accounts, such as development of transaction reports for review by the compliance officer, close monitoring of suspicious fund transfers etc.

11.8 Particular care should also be exercised where the AI's respondent banks allow direct use of the correspondent account by their customers to transact business on their own behalf (i.e. payable-through accounts). An AI should therefore establish whether the customers of the respondent bank will be allowed to use the correspondent banking service and, if so, it should take steps to require verification of the identity of such customers. The procedures set out in section 6 should be used in such cases.

11.9 An AI should take appropriate measures to ensure that it does not enter into or continue a correspondent banking relationship with a bank which is known to permit its accounts to be used by a shell bank.

12. Existing accounts

12.1 This section supersedes paragraph 5.3 of the Guideline.

12.2 An AI should take steps to ensure that the records of existing customers remain up-to-date and relevant. Where necessary, additional evidence of the identity of existing customers should be obtained to ensure that these comply with the AI's current standards.

12.3 To achieve this, an AI should undertake periodic reviews of existing records of customers. An appropriate time to do so is upon certain trigger events. These include:

(a) when a significant [IN 39] transaction is to take place;

(b) when there is a material change in the way the account is operated;

(c) when the AI's customer documentation standards change substantially; or

(d) when the AI is aware that it lacks sufficient information about the customer.

12.4 ~~Even where there is no specific trigger event, an AI should consider whether to require additional information in line with current standards from those existing customers that are considered to be of higher risk. In doing so, the AI should take into account the factors mentioned in paragraph 2.3 above. An additional consideration is whether the customer was introduced by an intermediary that would not have met the criteria specified in paragraphs 6.3 and 6.4 above.~~ For the avoidance of doubt, even in the absence of an intervening trigger event, an AI should still conduct a review at least annually [IN 39a] on all high-risk customers to ensure that the customers' records it maintains are kept up-to-date and relevant. The frequency of such reviews should be documented in the AI's policies and procedures.

13. On-going monitoring

13.1 This is an area not specifically covered in the Guideline. This section should however be read in conjunction with sections 8 and 9 of the Guideline.

13.2 In order to satisfy its legal and regulatory obligations, an AI needs to have systems to enable it to identify and report suspicious transactions. However, it is not enough to rely simply on the initiative of front-line staff to make ad hoc reports. An AI should also have management information systems (MIS) to provide managers and compliance officers with timely information on a regular basis to enable them to detect patterns of unusual or suspicious activity, particularly in relation to higher risk accounts.

13.3 This also requires the AI to have a good understanding of what is normal and reasonable activity for particular types of customer, taking into account the nature of the customer's business. Among other things, an AI should take appropriate measures to satisfy itself about the source and legitimacy of funds to be credited to a customer's account. This is particularly the case where large amounts and/or higher risk customers are involved.

13.4 A further relevant consideration in respect of funds derived from outside Hong Kong is whether the transfer of such funds may have breached the exchange controls of the country of origin.

13.5 MIS reports used for monitoring purposes should be capable of identifying transactions that are unusual either in terms of amount (for example, by reference to predetermined limits for the customer in question or to comparative figures for similar customers) or type of transaction or other relevant risk factors. High account activity in relation to the size of the balance on an account or unusual activity in an account (such as early settlement of instalment loans by way of cash repayment) may, for example, indicate that funds are being "washed" through the account and may trigger further investigation. The AI should take appropriate follow-up actions on any unusual activities identified in the MIS reports. The findings and any follow-up actions taken should be properly documented and the relevant documents should be maintained for a period not less than six years following the date when the unusual activity is identified.

13.6 While a focus on cash transactions is important, it should not be exclusive. An AI should not lose sight of non-cash transactions, e.g. inter-account transfers or inter-bank transfers. The MIS reports referred to above should therefore capture not only cash transactions but also those in other forms. The aim should be to obtain a comprehensive picture of the customer's transactions and overall relationship with the AI. In this regard the overall relationship should also cover, to the extent possible and using a risk-based approach, the customer's accounts and transactions with the AI's overseas operations.

14. Jurisdictions which do not or insufficiently apply the FATF Recommendations

14.1 This is a new section not currently covered in the Guideline.

14.2 Repealed.

14.3 Repealed.

14.4 An AI should apply Recommendation 21 of the FATF revised Forty Recommendations to jurisdictions which do not or insufficiently apply the FATF Recommendations. This states that:

"Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities."

14.5 Extra care should therefore be exercised by an AI in respect of customers (including beneficial owners [IN 40]) connected with jurisdictions which do not or insufficiently apply the FATF Recommendations [IN 3 & 41] or otherwise pose a higher risk to an AI. In addition to ascertaining and documenting the business rationale for opening an account or applying for

banking services as required under paragraph 3.2(da) above, an AI should be fully satisfied with the legitimacy of the source of funds [IN 21] of such customers.

14.5a Factors that should be taken into account in determining whether jurisdictions do not or insufficiently apply the FATF Recommendations or otherwise pose a higher risk to an AI include:-

(a) whether the jurisdiction is or a significant number of persons or entities in that jurisdiction are, subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances, a jurisdiction subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, may be given credence by an AI because of the standing of the issuer and the nature of the measures;

(b) whether the jurisdiction is identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures;

(c) whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organisations operating within it; and

(d) whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.

"Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

14.6 For jurisdictions with serious deficiencies in applying the FATF Recommendations and where inadequate progress has been made to improve their position, the FATF may recommend the application of further counter-measures. The specific counter-measures, to be determined by the HKMA in each case, would be gradual and proportionate to the specific problem of the jurisdiction concerned. The measures will generally focus on more stringent customer due diligence and enhanced surveillance / reporting of transactions. An AI should apply the counter-measures determined by HKMA from time to time.

14.7 An AI should be aware of the potential reputation risk of conducting business in jurisdictions which do not or insufficiently apply the FATF Recommendations or other jurisdictions known to apply inferior standards for the prevention of money laundering and terrorist financing.

14.8 If an AI incorporated in Hong Kong has operating units in such jurisdictions, care should be taken to ensure that effective controls on prevention of money laundering and terrorist financing are implemented in these units. In particular, the AI should ensure that the policies and procedures adopted in such overseas units are equivalent to those adopted in Hong Kong. There should also be compliance and internal audit checks by staff from the head office in Hong Kong. In extreme cases the AI should consider withdrawing from such jurisdictions.

15. Terrorist financing

15.1 This is a new area not currently covered in the Guideline.

15.2 Terrorist financing generally refers to the carrying out of transactions involving funds that are owned by terrorists, or that have been, or are intended to be, used to assist the commission of terrorist acts. This has not previously been explicitly covered under the money laundering regime where the focus is on the handling of criminal proceeds, i.e. the source of funds is what matters. In terrorist financing, the focus is on the destination or use of funds, which may have derived from legitimate sources.

15.3 Since 9/11 the FATF has expanded its scope of work to cover matters relating to terrorist financing. In this context, it has produced nine Special Recommendations on Terrorist Financing. A list of these can be found on the FATF website (***http://www.fatf-gafi.org***).

15.4 The United Nations Security Council (UNSC) has passed various resolutions to require sanctions against certain designated terrorists and terrorist organisations. In Hong Kong, Regulations issued under the United Nations (Sanctions) Ordinance give effect to these UNSC resolutions. In particular, the United Nations Sanctions (Afghanistan) Regulation provides, among other things, for a prohibition on making funds available to designated terrorists. The list of designated terrorists is published in the Gazette from time to time.

15.5 In addition, the United Nations (Anti-Terrorism Measures) Ordinance was enacted on 12 July 2002. This implements the mandatory elements of the UNSC Resolution 1373. The latter is aimed at combating international terrorism on various fronts, including the introduction of measures against terrorism financing. The Ordinance also implements the most pressing elements of the FATF's nine Special Recommendations.

15.6 The Ordinance, among other things, prohibits the supply of funds or making of funds available to terrorists or terrorist associates as defined. It also makes it a statutory requirement for a person to report his knowledge or suspicion that any property is terrorist property. As with the above mentioned Regulations, a list of terrorist names will be published in the Gazette from time to time for this purpose.

15.7 An AI should take measures to ensure compliance with the relevant regulations and legislation on terrorist financing. The legal obligations of the AI and those of its staff should be well understood and adequate guidance and training should be provided to the latter. The systems and mechanisms for identification of suspicious transactions should cover terrorist financing as well as money laundering.

15.8 It is particularly vital that an AI should be able to identify and report transactions with terrorist suspects. To this end, an AI should ensure that it maintains a database of names and particulars of terrorist suspects which consolidates the various lists that have been made known to it. Alternatively, an AI may make arrangements to secure access to such a database maintained by third party service providers.

15.9 Such database should, in particular, include the lists published in the Gazette and those designated under the US Executive Order of 23 September 2001. The database should also be subject to timely update whenever there are changes, and should be made easily accessible by staff for the purpose of identifying suspicious transactions.

15.10 An AI should check the names of both existing customers and new applicants for business against the names in the database. It should be particularly alert for suspicious ~~remittance~~wire transfers and should bear in mind the role which non-profit organisations are known to have played in terrorist financing. Enhanced checks should be conducted before processing a transaction, where possible, if there are circumstances giving rise to suspicion.

15.11 The FATF issued in April 2002 a paper on guidance for financial institutions in detecting terrorist financing. The document describes the general characteristics of terrorist financing with case studies illustrating the manner in which law enforcement agencies were able to establish a terrorist financing link based on information reported by financial institutions. Annex 1 of the document contains a series of characteristics of financial transactions that have been linked to terrorist activity in the past.

15.12 An AI should acquaint itself with the FATF paper and should use it as part of its training material for staff. The paper is available on the FATF website (***http://www.fatf-gafi.org***).

15.13 It should be noted that the list of characteristics only serves to show the types of transaction that could be a cause for additional scrutiny if one or more of the characteristics is present. The parties involved in the transaction should also be taken into account, particularly when the individuals or entities appear on a list of suspected terrorists.

15.14 Where an AI suspects that a transaction is terrorist-related, it should make a report to the JFIU and to the HKMA. Even if there is no evidence of a direct terrorist connection, the transaction should still be reported to the JFIU if it looks suspicious for other reasons. It may emerge subsequently that there is a terrorist link.

16. Risk management

16.1 This section should be read in conjunction with section 9 of the Guideline in relation to the role of the compliance officer.

16.2 The senior management of an AI should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and ensuring their effectiveness. Explicit responsibility should be allocated within an AI for this purpose.

16.3 An AI should appoint a compliance officer as a central reference point for reporting suspicious transactions. The role of the compliance officer should not be simply that of a passive recipient of ad hoc reports of suspicious transactions. Rather, the compliance officer should play an active role in the identification and reporting of suspicious transactions. This should involve regular review of exception reports of large or irregular transactions generated by the AI's MIS as well as ad hoc reports made by front-line staff. Depending on the organization structure of the AI, the specific task of reviewing reports may be delegated to other staff but the compliance officer should maintain oversight of the review process.

16.4 The compliance officer should form a considered view whether unusual or suspicious transactions should be reported to the JFIU. In reporting to the JFIU, the compliance officer should ensure that all relevant details are provided in the report and cooperate fully with the JFIU for the purpose of investigation. If a decision is made not to report an apparently suspicious transaction to the JFIU, the reasons for this should be fully documented by the compliance officer. The fact that a report may already have been filed with the JFIU in relation to previous transactions of the customer in question should not necessarily preclude the making of a fresh report if new suspicions are aroused.

16.5 More generally, the compliance officer should have the responsibility of checking on an ongoing basis that the AI has policies and procedures to ensure compliance with legal and regulatory requirements and of testing such compliance.

16.6 It follows from this that the AI should ensure that the compliance officer is of sufficient status within the organisation, and has adequate resources, to enable him to perform his functions.

16.7 Internal audit also has an important role to play in independently evaluating on a periodic basis an AI's policies and procedures on money laundering. This should include checking the effectiveness of the compliance officer function, the adequacy of MIS reports of large or irregular transactions and the quality of reporting of suspicious transactions. The level of awareness of front line staff of their responsibilities in relation to the prevention of money laundering should also be reviewed. As in the case of the compliance officer, the internal audit function should have sufficient expertise and resources to enable it to carry out its responsibilities.

Hong Kong Monetary Authority
July 20109

Annex

INTERMEDIARY CERTIFICATE

I/We wish to apply for opening an account on behalf of the following *person(s)/company:

Customer Name _____

Address _____

_____

1. I/We confirm that I/we have verified the customer's identity and address and enclose herewith *a summary sheet containing the following identification data / the following identity documents (or copies of such documents duly certified), in accordance with the requirements set out in the HKMA's Guideline on Prevention of Money Laundering (including its Supplement and the accompanying Interpretative Notes):

   (a) Identity card(s)/passport(s) of *the customer / all authorized signatories, directors (at least 2 including the managing director) and all principal shareholders of the company;

   (b) Resolution of the board of directors to open account and confer authority on those who will operate the account;

   (c) Certificate of Incorporation;

   (d) Business Registration Certificate;

   (e) Memorandum and Articles of Association;

   (f) Search record at the Company Registry;

   (g) Evidence of address;

   (h) Other relevant documents.

2. I/ We confirm that the *occupation / business activities of the customer is/are

   _____.

3. I am/We are satisfied as to the source of funds being used to open the account. The details are set out below:

   _____.

4. I/We enclose the account opening documents duly completed, and confirm that the signature(s) contained in the account opening documents is/are signed by the customer(s).

5. I/We enclose herewith the evidence of authority for me / us to act on behalf of the customer in the application for opening and / or operating the account.

* *Please delete as appropriate*

Signed: _____

Name: _____

Position held: _____ at _____(name of company / firm)____

Date: _____

INTERPRETATIVE NOTES

General guidance

The revised FATF Forty Recommendations and the Basel CDD requirements: Both the FATF and Basel requirements are relevant to the banking sector in Hong Kong. The former sets out the basic framework for both financial institutions and non-financial institutions, while the latter (which is recognised to be more rigorous than the FATF requirements in some respects) is specifically directed towards the prudential regulation of banks and tailored towards the risks to which banks are exposed. It is considered appropriate for the banking industry to adopt enhanced customer due diligence (CDD) standards because of the nature of their business. However, some flexibility is appropriate given the practicalities of implementing the measures and the fact that not all elements of the requirements are yet fully developed and may take some time to put in place (e.g. regulatory regime for professional intermediaries). Accordingly, where the risk of money laundering is low, the FATF approach may be adopted and simplified CDD procedures used.

Risk-based approach: AIs should adopt more extensive due diligence for higher risk customers. Conversely, it is acceptable for AIs to apply a simplified CDD process for lower risk customers. In general, AIs may apply a simplified CDD process in respect of a customer or a particular type of customers where there is no suspicion[1] of money laundering, and [Para. 2.2]:

- the risk[2] of money laundering is assessed to be low; or
- there is adequate public disclosure in relation to the customers.

Overriding principle: The guiding principle for the purpose of compliance with the Guideline on Prevention of Money Laundering and its Supplement is that AIs should be able to justify that they have taken reasonable steps to satisfy themselves as to the true identity of their customers including beneficial owners. These measures should be

[1] There may be instances where the circumstances lead one to be suspicious even though the inherent risk may be low.
[2] This refers to the intrinsic or inherent risk relating to a type of customer.

objectively reasonable in the eyes of a third party. In particular, where an AI is satisfied as to any matter it should be able to justify its assessment to the HKMA or any other relevant authority. Among other things, this would require the AI to document its assessment and the reasons for it.

Terminology

The term "customer" refers to a person who maintains an account with or carries out a transaction with an AI (i.e. the direct customer[3]), or a person on whose behalf an account is maintained or a transaction is carried out (i.e. the beneficial owner). In the context of cross-border transactions:

- if a local office has only a marketing relationship with a person who maintains an account in its overseas office, the local office will be regarded as an intermediary and the person a "customer" of its overseas office[4]; and
- if a local office carries out transactions for a person with an account which is domiciled in its overseas office, that person should be regarded as the "customer" of the local office as well as its overseas office[5].

The term "beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement."

[3] This generally excludes the third parties of a transaction. For example, an ordering AI in an outward ~~remittance~~wire transfer transaction does not regard the beneficiary (who has no other relationship with the AI) as its customer.

[4] The overseas office will be responsible for the CDD review and on-going monitoring of that customer in accordance with the group KYC policy and the regulatory requirements in the respective countries. The local office may, however, be requested by its overseas office to perform these on its behalf.

[5] A local office may rely on the CDD review and on-going monitoring carried out by its overseas office as an intermediary, provided that a common set of CDD standards consistent with the FATF standards applies on a bank/group-wide basis. Customer identity **information** must, nonetheless, be obtained as a minimum by the local office (some local offices may have an unfettered right to access and retrieve all the relevant customer identity information from the group database maintained) although the local office may choose not to obtain copies of the identity **documentation** and records of transactions performed by the local office on the customer's behalf as long as the customer documentation and

Specific guidance

Group customer due diligence requirements

1. The general principle is that a common set of CDD standards should be applied on a consolidated basis throughout a banking group. Simplified CDD procedures might, however, be used by a group company on a particular type of customer where the area of business in question is considered to be of a low risk in nature. In addition, the use of simplified CDD should be fully justified, well documented and properly approved by senior management. Such risk-based approach should also be clearly set out in the group policies. Where group standards cannot be applied for good reason, e.g. due to legal or regulatory reasons, deviations should be documented and risk mitigating measures applied. [Para 1.7]

Customer due diligence

2. Repealed.

3. AIs should adopt a balanced and common sense approach with regard to customers connected with jurisdictions which do not or insufficiently apply the FATF Recommendations. While extra care may well be justified in such cases, it is not a requirement that AIs should refuse to do any business with such customers or automatically classify them as high risk and subject them to enhanced CDD process. Rather, AIs should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of money laundering. [Para 2.3(a) & 14.5]

4. For customers from countries where the citizens do not have any official identity documents, AIs should adopt a common sense approach to decide what other unique identification documents can be accepted as a substitute. [Para 3.2(b)]

---

these transaction records kept by the overseas office will be made available upon request without delay.

5. For ~~domestic (defined, for the purpose of the Supplement, as residents with a right of abode in~~ Hong Kong permanent residents [6] ~~) retail customers, their identity may be simplified to include the four basic elements: (i) name, (ii) number of Hong Kong identity card, (iii) date of birth and (iv) residential address. For other customers[7], AIs should also identify and verify their nationality (through inspecting or obtaining a copy of their passport or other forms of travel documents)~~, AIs should verify an individual's name, date of birth and identity card number by reference to his/her identity card. For nonpermanent residents, AI should additionally verify the individual's nationality through an inspection of his/her travel document.

AIs should verify the identity of non-residents by reference to their travel documents [IN 9b].

When identifying a non-resident who is not physically present in Hong Kong, AIs should verify the individual's identity by reference to (i) a valid travel document; (ii) a relevant national identity card bearing the individual's photograph; or (iii) a valid national driving licence bearing the individual's photograph issued by a competent national authority that verifies the holder's identity before issuance. [Para 3.3]

6. ~~Generally, a "residential address" refers to an address where a customer currently resides while a "permanent address" refers to an address where a customer intends to stay permanently.~~Throughout these guidelines reference to "address" for a natural person means residential address (and permanent address if different).

AIs should use a common sense approach to handle cases where the customers (e.g. students and housewives) are unable to provide address proof.

---

[6] These customers will have a Hong Kong Permanent Identity Card~~, with a letter "A" to indicate that they have a right of abode in Hong Kong~~. The identity card of a permanent resident (i.e. a Hong Kong Permanent Identity Card) will have on the front of the card a capital letter "A" underneath the individual's date of birth. The reverse of the card will state the holder has the right of abode in Hong Kong.

Apart from the methods suggested in paragraph 5.7 of the Guideline (e.g. by requesting sight of a recent utility or rates bill), AIs may use other appropriate means, such as home visits, to verify the residential address of a customer, as is the case for some private banking customers. [Para 3.3]

7. Information about occupation or employer is a relevant piece of information about a customer but does not form part of the customer's identity requiring verification. [Para 3.3]

8. Exceptions may be made to allow payments to third parties subject to the following conditions:

- there is no suspicion of money laundering;
- the risk of money laundering is assessed to be low;
- the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction;
- the names of recipients do not match with watch lists such as those for terrorist suspects and PEPs; and
- the verification process should be completed within one month ~~(two months for the first year of implementation of the Supplement, i.e. the year of 2005)~~ from the date the business relationship was established. [Para 3.6]

9. The funds should generally be returned to the account holders. It is up to individual AIs to decide the means to repay the funds but AIs must guard against the risk of money laundering since this is a possible means by which funds can be "transformed", e.g. from cash into a cashier order. It is therefore important for AIs to ensure that they only open accounts with customers where they have reasonable grounds to believe that the relevant CDD process can be satisfactorily completed within a reasonable timeframe. [Para 3.7]

~~[2] The verification of nationality is not mandatory for an individual who is a holder of Hong Kong Permanent Identity Card.~~

9a. Transactions undertaken for non-account holders may include for example wire transfer or currency exchange transactions, the purchase of a cashier order or gift cheque. [Para 3.10]

9b. "Travel document" means a passport furnished with a photograph of the holder, or some other documents establishing to the satisfaction of an immigration officer or immigration assistant the identity and nationality, domicile or place of permanent residence of the holder. The following documents constitute travel documents for the purpose of identity verification:

- Permanent Resident Identity Card of Macau Special Administrative Region;
- Mainland Travel Permit for Taiwan Residents;
- Seaman's Identity Document (issued under and in accordance with the International Labour Organisation Convention / Seafarers Identity Document Convention 1958);
- Taiwan Travel Permit for Mainland Residents;
- Permit for residents of Macau issued by Director of Immigration.
- Exit-entry Permit for Travelling to and from Hong Kong and Macau for Official Purposes;
- Exit-entry Permit for Travelling to and from Hong Kong and Macau.

[Para 3.14, 3.15 & 3.16]

Corporate customers

10. A recognised stock exchange is a stock exchange of a jurisdiction which is a member of the FATF or a specified stock exchange as defined under Schedule 1 to the Securities and Futures Ordinance, but it does not include a stock exchange of jurisdictions which do not or insufficiently apply the FATF Recommendations (Annex 2 of the Guideline is superseded). [Para 4.2]

11. A simplified CDD process may be applied to:

(a) state-owned enterprises and their subsidiaries in a jurisdiction where the risk of money laundering is assessed to be low and where the AI has no doubt as regards the ownership of the enterprise.; ~~[Para 4.2]~~ or

(b) companies listed on a recognised stock exchange and their subsidiaries.

AIs should identify and verify the identity of at least 2 account signatories of such companies and may adopt a risk based approach to determine whether or not it is necessary to identify and verify the identity of further account signatories. [Para 4.2]

12. Repealed.~~Obtaining the Memorandum and Articles of Association of a corporate customer is not a mandatory requirement for purposes of prevention of money laundering. It is up to individual AIs to decide whether they will need to have a copy of these documents for other purposes. [Para 4.2 & 4.5]~~

13. A person entitled to ~~exercise or control the exercise~~control or exercise the control of 10% or more of the voting rights of a company should be regarded as a principal shareholder of the company. [Para 4.2~~5~~]

14. ~~Comparable~~Equivalent jurisdictions are jurisdictions (other than FATF members) that in the view of the institution sufficiently apply standards of prevention of money laundering and terrorist financing equivalent to those of the FATF. ~~These can be taken to include jurisdictions previously identified by the HKMA as comparable jurisdictions, namely members of the European Union (including Gibraltar), Netherlands Antilles and Aruba, Isle of Man, Guernsey and Jersey.~~

In determining whether or not a jurisdiction sufficiently applies FATF standards in combating money laundering and terrorist financing and meets the criteria for an ~~comparable~~equivalent jurisdiction, AIs should:

(a) carry out their own assessment of the standards of prevention of money laundering and terrorist financing adopted by the jurisdiction concerned. The assessment can be made based on the AI's knowledge and experience of the jurisdiction or market intelligence. The higher the risk, the greater the due diligence measures that should be applied when undertaking business with a customer from the jurisdiction concerned;

(b) pay attention to assessments that have been undertaken by standard setting bodies such as the FATF and by international financial institutions such as the International Monetary Fund (IMF). In addition to the mutual evaluations carried out by the FATF and FATF-style regional bodies, the IMF and the World Bank, as part of their financial stability assessments of countries and territories, have carried out country assessments in relation to compliance with prevention of money laundering and terrorist financing standards based on the FATF Recommendations; and

(c) maintain an appropriate degree of ongoing vigilance concerning money laundering risks and take into account information that is reasonably available to them about the standards of anti-money laundering/terrorist financing systems and controls that operate in the jurisdiction with which any of their customers are associated. [Para 4.4~~& 6.4~~]

15. In the case of offshore investment vehicles owned by high net worth individuals (i.e. the ultimate beneficial owners) who use such vehicles as the contractual party to establish a private banking relationship with AIs, exceptions to the requirement to obtain independent evidence about the ownership, directors and account signatories of the corporate customer may be made. This means that self-declarations in writing about the identity of, and the relationship with, the above parties from the ultimate beneficial owners or the contractual parties may be accepted, provided that the investment vehicles are incorporated in a jurisdiction where company searches or certificates of incumbency (or equivalent) are not available or cannot provide meaningful information about their directors and principal shareholders and AIs are satisfied that:

- they know the identity of the ultimate beneficial owners; and
- there is no suspicion of money laundering.

Such exceptions are allowed on the basis that a comprehensive CDD process had been carried out in respect of the ultimate beneficial owners. A

comprehensive CDD process for such customers should generally comprise the procedures as set out in Annex 2.

Exceptions made should be approved by senior management and properly documented. [Para 4.5]

16. AIs may rely on the documentation provided by professional third parties (such as lawyers, notaries, actuaries, accountants and corporate secretarial service providers) in Hong Kong on behalf of a corporate customer incorporated in a country where company searches are not available, provided that there is no suspicion arising from other information collected and these professional third parties can meet the criteria set out in paragraphs 6.1a and 6.3 ~~and 6.4~~ of the Supplement and IN 28 below. [Para 4.5]

17. AIs may adopt a risk-based approach to decide whether the residential address of individuals who are connected with a legal person or legal arrangement ~~corporate customers~~ (~~e.g.~~i.e. principal shareholders, directors, ~~and account~~ signatories, settlor/grantor/founder, protector(s) or known beneficiary of a legal arrangement) should be verified, provided that the risk-based process is clearly set out in the AI's policy, the waivers given are in accordance with the policy, ~~and~~ the decisions made for such waivers are adequately documented and the money laundering risk of the customer is low. A waiver should not be given because of practical difficulties in the verification process. An express trust cannot form a business relationship or carry out a one-off transaction itself. It is the trustee of the trust who will enter into a business relationship or carry out the one-off transaction on behalf of the trust and who will be considered to be the customer. The address of the trustee in a direct customer relationship should therefore always be verified. [Para 4.5]

18. ~~In case of one director companies, AIs are only required to verify the identity of that director. [Para 4.5]~~Repealed.

19. AIs should record the identity (see [IN 5]) of all account signatories (this obligation does not apply to the staff of an AI acting in their official capacity). AIs may adopt a risk-based approach to decide whether ~~the~~ this information

~~identity of all account signatories~~ (including users designated to approve fund transfers or other e-banking transactions on behalf of the corporate customer) should be verified, provided that the risk-based process is clearly set out in the AI's policy, the waivers given are in accordance with the policy and the decisions made for such waivers are adequately documented. In any case, the identity of at least two account signatories should be verified. A waiver should not be given because of practical difficulties in the verification process. [Para 4.5]

20. For corporate customers with a multi-layer ownership structure, AIs are only required to identify each stage in the ownership chain to obtain a full understanding of the corporate structure, but it is the natural person at the top of the chain (i.e. not the intermediate owners) whose identity needs to be verified. [Para 4.6]

21. Apart from those customers specified in the Supplement, AIs should also adopt a risk-based approach to determine the categories of customers whose source of funds should also be ascertained. [Para 4.7~~, 10.5~~ & 14.5]

22. Where it is not practical to immobilise the bearer shares, AIs should obtain a declaration from each beneficial owner (i.e. who holds 5% or more of the total shares) of the corporate customer on the percentage of shareholding. Such owners should also provide a further declaration on annual basis and notify the AI immediately if the shares are sold, assigned or transferred. [Para 4.9]

Trust and nominee accounts

23. For trusts that are managed by trust companies which are subsidiaries (or affiliate companies) of an AI, that AI may rely on its trust subsidiaries to perform the CDD process, provided that:

- a written assurance from the trust subsidiary is obtained, confirming that evidence of the underlying principals has been obtained, recorded and retained and that it is satisfied as to the source of funds;

- the trust subsidiary complies with a group Know-Your-Customer (KYC) policy that is consistent with the FATF standards; and
- the documentation can be made available upon request without delay. [Para 5.2]

24. AIs may adopt a risk-based approach to determine whether it is necessary to verify the identity of protectors[8]. [Para 5.3]

25. To the extent that the CDD process on the settlors/asset contributors has been adequately performed, AIs may accept a declaration from the trustee or other contractual party to confirm the link or relationship with the settlors/asset contributors. [Para 5.3]

26. AIs should try as far as possible to obtain information about the identity of beneficiaries but a broad description of the beneficiaries such as family members of Mr XYZ may be accepted. [Para 5.3]

27. Where the identity of beneficiaries has not previously been verified, AIs should assess the need to undertake verification when they become aware that any payment out of the trust account is made to the beneficiaries or on their behalf. In making this assessment, AIs should adopt a risk-based approach which should take into account the amount(s) involved and any suspicion of money laundering. A decision not to undertake verification should be approved by senior management. [Para 5.3]

Reliance on intermediaries for customer due diligence

28. AIs should take reasonable steps to satisfy themselves with regard to the adequacy of the CDD procedures and systems of intermediaries, but may adopt a risk-based approach to determine the extent of the measures to be taken. Relevant factors for the purpose of assessing the CDD standards of intermediaries include the extent to which the intermediaries are regulated in accordance with the FATF requirements and the legal requirements in the

[8] The identity of the "protectors" is relevant information which has to be verified because these persons can, under certain circumstances, exercise their powers to replace the existing trustees.

relevant jurisdiction to require the intermediaries to report suspicious transactions. [Para 6.3]

29. AIs may choose not to obtain, immediately, copies of documentation pertaining to the customer's identity, provided that they have taken adequate steps to satisfy themselves that the intermediaries will provide these copies upon request without delay. All the relevant identification data or information should nonetheless be obtained. [Para 6.6]

Client accounts

30. Examples of professional intermediaries include lawyers, accountants, fund managers, custodians and trustees. [Para 7.1]

31. In certain types of businesses (such as custodian, securities dealing or fund management), it may be common to have a series of vertically connected single client accounts or sub-accounts which ultimately lead to a co-mingled client fund account. AIs may regard such accounts as a co-mingled account to which the provisions of para 7.3 apply. [Para 7.3]

~~Remittance~~Wire transfer messages

32a. It is acceptable for an AI to include the "correspondence address" of the originating customer in the ~~remittance~~wire transfer message provided that the AI is satisfied that the address ~~information is accurate and meaningful~~has been verified. [Para 9.2]

32b. In the case of a domestic ~~remittance~~wire transfer transaction, the additional information relating to the originating customer need not be included in the message provided that the information can be made available to the beneficiary AI and appropriate authorities by the ordering AI within 3 business days upon request. For the retrieval of information of earlier transactions (i.e. beyond 6

months), AIs should make such information available as soon as is practicable. [Para 9.2]

32bb. National identity number means Hong Kong identity card number or travel document number. [Para 9.2]

32c. In considering whether to apply the threshold of HK$8,000, AIs should take into account the business and operational characteristics of their ~~remittance~~wire transfer activities. AIs are encouraged to include, as far as practicable, the relevant originator information in the ~~remittance~~ messages accompanying ~~of~~ all ~~remittance~~wire transfer transactions. ~~The HKMA will review the application of the threshold at a later date.~~ [Para 9.3]

33. The relevant originator information should be recorded and retained in respect of both account holders and non-account holders. [Para 9.3]

Politically exposed persons

34. ~~AIs should determine and document their own criteria (including making reference to publicly available information or commercially available databases) to identify PEPs. A risk-based approach may be adopted for identifying PEPs and focus may be put on persons from countries that are higher risk from a corruption point of view (reference can be made to publicly available information such as the Corruption Perceptions Index). [Para 2.3(b) & 10.4]~~Repealed.

34a. Connected parties to a direct customer include the beneficial owner and any natural person having power to direct the activities of the customer. For the avoidance of doubt the term connected party will include any director, principal shareholder, beneficial owner, signatory, trustee, settlor/grantor/founder, protector(s), or defined beneficiary of a legal arrangement. [Para 10.4]

34b. AIs should also consider whether it is appropriate to take measures to verify a PEP's source of funds and wealth, in line with its assessment of the risks. [Para 10.5a]

Correspondent banking

35. This includes the relationships established for securities transactions or funds transfers, whether for the respondent bank as a principal or for its customers. [Para 11.2]

36. As long as there is a formal delegation of authority and proper documentation, AIs may use a risk-based approach to determine the appropriate level of approval within the institution that is required for establishing new correspondent banking relationships. [Para 11.3]

37. Information on the authorization status and other details of a respondent bank, including the system of bank regulation and supervision in its country, may be obtained through publicly available information (e.g. public website and annual reports). [Para 11.4]

38. In assessing the anti-money laundering efforts of a respondent bank in a foreign country, AIs should pay attention to whether the respondent bank is permitted to open accounts for or carry out transactions with shell banks. [Para 11.4]

Existing accounts

39. The word "significant" is not necessarily linked to monetary value. It may include transactions that are unusual or not in line with an AI's knowledge of the customer. [Para 12.3(a)]

39a. An AI is not required to re-verify the identity or address of an existing individual customer or connected parties of an existing corporate customer that are individuals unless there is doubt as to the veracity of the evidence previously obtained. [Para 12.4]

Jurisdictions which do not or insufficiently apply the FATF Recommendations

40. Where a customer has one or more (principal) beneficial owners connected with jurisdictions which do not or insufficiently apply the FATF Recommendations, the general principle is that the exercise of extra care should be extended to cases where the beneficial owner(s) has/have a dominant influence over the customer concerned. [Para 14.5]

41. AIs may regard FATF members as jurisdictions which have sufficiently applied the FATF Recommendations. [Para 14.5]

ANNEX 1: Repealed

ANNEX 2: Comprehensive CDD Process on Private Banking Customers

A comprehensive CDD process adopted for private banking customers generally covers the following areas:

- **Customer profile**

(a) In addition to the basic information relating to a customer's identity (see IN.5 and IN.6 above), AIs also obtain the following client profile information on each of their private banking customers:

- purpose and reasons for opening the account;
- business or employment background;
- estimated net worth;
- source of wealth;
- family background, e.g. information on spouse, parents (in the case of inherited wealth);
- source of funds (i.e. description of the origin and the means of transfer for monies that are acceptable for the account opening);
- anticipated account activity; and
- references (e.g. introduced by whom and when and the length of relationship) or other sources to corroborate reputation information where available.

All the above information relating to the private banking customer are to be properly documented in the customer file.

- **Global KYC policy**

(b) To facilitate customers' referral from overseas offices, AIs are to maintain global KYC policies to ensure that the same CDD standards are applied for all private banking customers on a group-wide basis.

- **Client acceptance**

(c) Generally, AIs do not accept customers without a referral. Walk-in customers are therefore not generally accepted unless they have at least a banker's reference.

(d) AIs also do not open private banking accounts without a face-to-face meeting with the customers, except in rare stances where the visitation policy set out in (h) below applies.

(e) Acceptance of private banking customers requires approval by senior management. For high risk or sensitive customers[9], additional approval from senior management and~~/or~~ the Compliance Department or an independent control function (in the context of foreign subsidiaries or branches operating in Hong Kong, the parent bank or head office) may be required.

- **Dedicated relationship management**

(f) Each private banking customer is served by a designated relationship manager who bears the responsibility for CDD and on-going monitoring.

(g) AIs are to make sure that the relationship managers have sufficient time and resources to perform the enhanced CDD process and on-going monitoring of their private banking customers.

---

[9] Sensitive clients in private banking may include:
- PEPs;
- persons engaged in types of business activities or sectors known to be susceptible to money laundering such as gambling, night clubs, casinos, foreign exchange firms, money changers, art dealing, precious stone traders, etc.;
- persons residing in or having funds sourced from countries identified as ~~NCCTs~~ insufficiently applying the FATF Recommendations or representing high risk for crime and corruption; and
- any other persons considered by individual AIs to be sensitive.

- **Monitoring**

(h) AIs conduct face-to-face meetings with their private banking customers as far as possible on a regular basis.

(i) Regular CDD reviews are conducted for each private banking customer. For high risk or sensitive customers, such reviews are performed annually or at a more frequent interval and may require senior management's involvement. Exceptions may, however, be allowed for inactive accounts for which CDD reviews should be conducted immediately prior to a transaction taking place.

(j) An effective monitoring system (e.g. based on asset size, asset turnover, client sensitivity or other relevant criteria) is in place to help identify any unusual or suspicious transaction on a timely basis.

SUPPLEMENT TO THE GUIDELINE ON PREVENTION OF MONEY LAUNDERING

A Guideline issued by the Monetary Authority under section 7(3) of the Banking Ordinance

Revised July 2010

CONTENTS

1. Introduction

1.1 The current HKMA Guideline on Prevention of Money Laundering (Guideline) was issued in 1997. Amendments were made in 2000, mainly to take into account the provisions of the Organized and Serious Crimes (Amendment) Ordinance 2000.

1.2 A number of significant developments have taken place since then, which call for enhanced standards in the effective prevention of money laundering. These include, in particular, the issuance by the Basel Committee on Banking Supervision of the paper "Customer Due Diligence for Banks" in October 2001 and the revised Forty Recommendations issued by the Financial Action Task Force on Money Laundering (FATF) in June 2003. Moreover, the 9/11 event has expanded the scope of the effort on prevention of money laundering to include the fight against terrorist financing.

1.3 The HKMA considers it necessary to revise its regulatory requirements to take into account recent developments and the initiatives undertaken by international bodies. It is considered appropriate to reflect the changes, for the time being, in a Supplement to the Guideline pending revision of the Guideline to consolidate all changes issued since 2000 and achieve greater harmonisation with the requirements of the other financial regulators.

1.4 This Supplement mainly reflects the regulatory standards recommended in the Basel Committee paper on customer due diligence and takes into account the relevant requirements in the FATF revised Forty Recommendations. The Supplement also incorporates additional guidance issued by the HKMA since 2000 and recommendations related to terrorist financing, including the recently enacted anti-terrorism legislation in Hong Kong.

1.5 Unless indicated otherwise, provisions in this Supplement should be read or interpreted in conjunction with the relevant parts of the Guideline (July 2010 version as currently posted in the HKMA website – (***http//www.info.gov.hk/hkma/eng/guide/index.htm*** at Guideline 3.3) and the accompanying interpretative notes (IN).

1.6 Unless otherwise stated, the requirements in this Supplement apply to all new customers and existing customers when they are due for review in accordance with section 12 of this Supplement.

1.7 For Hong Kong incorporated authorized institutions (AIs), the requirements also apply to their overseas branches or subsidiaries [IN 1]. Where the local requirements differ from these requirements, the overseas operations should apply the higher standard to the extent that local laws permit. Where an overseas branch or subsidiary is unable to observe group standards, the HKMA should be informed.

1.8 This revised Supplement will supersede the last version issued on 17 July 2009 with effect from **1 November 2010**.

2. Customer acceptance policy

2.1 This is a new section not currently covered in the Guideline.

2.2 An AI should develop customer acceptance policies and procedures that aim to identify the types of customer that are likely to pose a higher than average risk of money laundering (see risk-based approach under the General Guidance Section of IN). A more extensive customer due diligence process should be adopted for higher risk customers. There should also be clear internal guidelines on which level of management is able to approve a business relationship with such customers.

2.3 In determining the risk profile of a particular customer or type of customer, an AI should take into account factors such as the following:

(a) the customer's nationality, citizenship and resident status (in the case of a corporate customer, the customer's place of incorporation), the place where its business is established, the location of the counterparties with whom it conducts business, and whether the customer is otherwise connected with higher risk jurisdictions or jurisdictions which do not or insufficiently apply the FATF Recommendations (see section 14 below), or which are known to the AI to lack proper standards in the prevention of money laundering or customer due diligence process [IN 3];

(b) background or profile of the customer such as being, or linked to, a politically exposed person (see section 10 below) or otherwise being an individual with high net worth whose source of funds to be credited to an account (both initially and thereafter) is unclear;

(c) nature of the customer's business, which may be particularly susceptible to money laundering risk, such as money changers or casinos that handle large amounts of cash;

(d) for a corporate customer, unduly complex structure of ownership for no good reason; and

(e) any other information that may suggest that the customer is of higher risk (e.g. knowledge that the customer has been refused a banking relationship by another institution).

2.4 Following the initial acceptance of the customer, a pattern of account activity that does not fit in with the AI's knowledge of the customer may lead the AI to reclassify the customer as higher risk.

3. Customer due diligence

3.1 This section reinforces paragraphs 5.1 and 5.2 of the Guideline and introduces new requirements.

3.2 The customer due diligence process should comprise the following:

(a) identify the direct customer, i.e. know who the individual or legal entity is;

(b) verify the customer's identity using reliable, independent source documents, data or information [IN 4];

(c) identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the direct customer, and/or the person on whose behalf a transaction is being conducted;

(d) take reasonable measures to verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c);

(da) obtain information on the purpose and reason for opening the account or establishing the relationship, unless it is self-evident; and

(e) conduct on-going due diligence and scrutiny i.e. perform on-going scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the AI's knowledge of the customer, its business and risk profile, including, where necessary, identifying the source of funds.

3.3 The identity of an individual includes the individual's name (including former or other name(s)), date of birth, nationality and Hong Kong identity card number [IN 5]. To facilitate on-going due diligence and scrutiny, information on the individual's occupation [IN 7] or business should also be obtained. AIs should also record and verify the address [IN 6] of a direct customer with whom it establishes business relations. For connected parties (i.e. account signatories, directors, principal shareholders, etc.) and transactions undertaken by nonaccount holders, AIs should determine the need to verify the address of these parties on the basis of risk and materiality.

3.4 Unwillingness of the customer, for no good reason, to provide the information requested and to cooperate with the AI's customer due diligence process may itself be a factor that should trigger suspicion.

3.5 Where an AI allows confidential numbered accounts (i.e. where the name of the account holder is known to the AI but is substituted by an account number or code name in subsequent documentation) the same customer due diligence process should apply even if this is conducted by selected staff. The identity of the account holder should be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from an AI's compliance function or from the HKMA.

3.6 An AI should not in general establish a business relationship with a new customer until the due diligence process is satisfactorily completed. However, it may be acceptable to allow an account to be opened pending completion of the verification of identity provided that the necessary evidence of identity is

promptly obtained. In such a case an AI should not allow funds to be paid out of the account to a third party before the identity of the customer is satisfactorily verified [IN 8].

3.7 If an account has been opened but the process of verification of identity cannot be successfully completed, the AI should close the account and return any funds to the source from which they were received [IN 9]. Consideration should also be given to whether a report should be made to the Joint Financial Intelligence Unit (JFIU). The return of funds should be subject to any request from the JFIU to freeze the relevant funds.

3.8 After a business relationship is established, an AI should undertake regular reviews of the existing records relating to the customer to ensure that they remain up-to-date and relevant. As indicated in paragraph 12.3 an appropriate time to do so is upon certain trigger events.

Transactions undertaken by non-account holders

3.9 This section supplements paragraph 5.26 of the Guideline.

3.10 An AI should also conduct the following when carrying out transactions [IN 9a] exceeding HK$120,000 on behalf of a customer who has not otherwise established a business relationship with the AI (i.e. a non-account holder) regardless of whether the transaction is carried out in a single or multiple operations between which there is an obvious connection:

(i) identify and verify the direct customer;
(ii) identify and verify any natural persons representing the customer, including the authority such persons have to act;
(iii) enquire if any beneficial owner exists and take reasonable measures to verify the identity of any such beneficial owner;
(iv) take reasonable measures to understand the ownership structure if the customer is a corporate; and
(v) ascertain the intended nature and purpose of the transaction, unless obvious.

3.11 If there is any suspicion of money laundering or terrorist financing, an AI should perform the measures detailed in paragraph 3.10 (i) to (v) when carrying out any transaction for a non-account holder regardless of the $120,000 threshold.

Additional requirements for wire transfer & currency exchange transactions performed by non-account holders

3.12 This section supersedes paragraph 5.27 of the Guideline.

3.13 Irrespective of the threshold mentioned in paragraph 3.10 above, the following requirements apply for wire transfer and currency exchange transactions:

Wire transfers

3.14 When acting as the ordering institution for a wire transfer of any value the AI should record the identity and address of the originator. For wire transfers equal to or exceeding HK$8,000, an AI should verify the originator's identity by reference to his identity card or travel document [IN 9b].

3.15 When acting as the beneficiary institution for a wire transfer of any value for a beneficiary who is not an account holder, the AI should record the identity and address of the recipient. For wire transfers equal to or exceeding HK$8,000, an AI should verify the recipient's identity by reference to his identity card or travel document [IN 9b]).

Currency exchange transactions

3.16 When performing a currency exchange transaction equivalent to HK$8,000 or more on behalf of a non-account holder, the AI must record the identity and address of the individual and verify his identity by reference to his identity card or travel document [IN 9b].

4. Corporate customers

4.1 This section supersedes paragraphs 5.12 and 5.13 of the Guideline and does not apply to customers that are banks (covered in section 11 below).

4.2 Where a customer is a company which is listed on a recognised stock exchange [IN 10] or is a state-owned enterprise or is a subsidiary of a listed company or state-owned enterprise, the customer itself can be regarded as the person whose identity is to be verified. It will therefore generally be sufficient for an AI to obtain and retain sufficient information to effectively identify and verify the identity of the customer (which will include proof of its listed status on a recognised stock exchange), the natural persons appointed to act on behalf of the customer and their authority to do so [IN 11].

4.3 Where a listed company is effectively controlled by an individual or a small group of individuals, an AI should consider whether it is necessary to verify the identity of such individual(s).

4.4 Where a non-bank financial institution is authorized and supervised by the Securities and Futures Commission ("SFC"), Insurance Authority ("OCI") or an equivalent authority in a jurisdiction that is a FATF member or an equivalent jurisdiction [IN 14], it will generally be sufficient for an AI to verify that the institution is on the list of authorized (and supervised) financial institutions in the jurisdiction concerned. Evidence that any individual representing the institution has the necessary authority to do so should be sought and retained.

4.5 In relation to a company which is not listed [IN 15] on a recognised stock exchange (or is not a subsidiary of such a listed company) or not a state-owned enterprise or is a non-bank financial institution other than those mentioned above in paragraph 4.4, an AI should look behind the company [IN 16] to

identify the beneficial owners and those who have control over the funds. This means that, in addition to obtaining the documents specified in paragraph 5.11 of the Guideline, the AI should verify the identity [IN 17] of all the principal shareholders [IN 13], at least one director of the company and all its account signatories [IN 19]. AIs should consider the need to verify the identity of additional directors on the basis of risk and materiality.

4.6 Where the direct customer of an AI is a non-listed company which has a number of layers of companies in its ownership structure, the AI is not required, as a matter of course, to check the details of each of the intermediate companies (including their directors) in the ownership chain. The objective should be to follow the chain of ownership to the individuals who are the ultimate principal beneficial owners of the direct customer of the AI and to verify the identity of those individuals [IN 20]. Where a customer has in its ownership chain an entity which is

(a) a company listed on a recognised stock exchange or a subsidiary of such a listed company;
(b) a state-owned enterprise or a subsidiary of a state-owned enterprise;
(c) a financial institution regulated by the HKMA, SFC or OCI; or
(d) a financial institution supervised and regulated by an authority that performs functions equivalent to those of the HKMA, SFC or OCI for anti-money laundering and counter terrorist financing (AML/CFT) purposes in a jurisdiction that is a FATF member or an equivalent jurisdiction,

it should generally be sufficient for the AI to verify the identity of that entity in accordance with paragraphs 4.2 and 4.4 above. However, AIs should still verify the identity of the beneficial owners in the ownership chain that are not connected with the above entity.

4.7 An AI should understand the ownership structure of non-listed corporate customers and determine the source of funds [IN 21]. As indicated in paragraph 2.3(d), an unduly complex ownership structure for no good reason is a risk factor to be taken into account.

4.8 An AI should exercise special care in initiating business transactions with companies that have nominee shareholders. Satisfactory evidence of the identity of beneficial owners of such companies should be obtained.

4.9 An AI should also exercise special care in dealing with companies which have a significant proportion of capital in the form of bearer shares. The AI should have procedures to monitor the identity of all principal shareholders. This may require the AI to consider whether to immobilize the shares, such as by holding the bearer shares in custody [IN 22].

5. Trust and nominee accounts

5.1 This section should be read in conjunction with paragraph 5.17 to 5.20 of the Guideline.

5.2 An AI should understand the relationship among the relevant parties in handling a trust or nominee account. There should be satisfactory evidence [IN 23] of the identity of the trustees or nominees, and the persons on whose behalf they are acting, as well as the details of the nature of the trust or other similar arrangements in place.

5.3 Specifically, in relation to trusts, an AI should obtain satisfactory evidence of the identity of trustees, protectors [IN 24], settlors/grantors [IN 25] and beneficiaries. Beneficiaries should be identified as far as possible where defined [IN 26 & 27].

5.4 As with other types of customer, an AI should adopt a risk-based approach in relation to trusts and the persons connected with them. The extent of the due diligence process should therefore depend on such factors as the nature and complexity of the trust arrangement.

6. Reliance on intermediaries for customer due diligence

6.1 This section supersedes paragraphs 5.21 and 5.22 of the Guideline. It refers to intermediaries which introduce customers to an AI. This however does not cover outsourcing or agency relationships (i.e. where the agent is acting under a contractual arrangement to carry out customer due diligence for the AI) and business relationships, accounts or transactions between financial institutions (as defined by FATF) for their clients.

6.1a For the purpose of this section, intermediary is defined as:

(i) a financial institution regulated by the HKMA, SFC or OCI;

(ii) a person who is professionally or legally registered in Hong Kong as a lawyer, auditor, accountant, trust company or chartered secretary and who carries on business in Hong Kong as such; or

(iii) a person who carries on business in an equivalent jurisdiction being
- (A) a financial institution, lawyer, notary public, auditor, accountant, tax advisor, trust company or chartered secretary;
- (B) subject to mandatory professional registration, licensing or regulation recognised by law;
- (C) subject to requirements consistent with the FATF standards; and
- (D) supervised for compliance with those requirements.

6.2 An AI may rely on such intermediaries to perform customer due diligence procedures. However, the ultimate responsibility for knowing the customer always remains with the AI.

6.3 An AI should assess whether the intermediaries they use are "fit and proper" and are exercising adequate due diligence procedures. In this regard the following criteria should be used to identify whether an intermediary can be relied upon [IN 28]:

(a) the customer due diligence procedures of the intermediary should be as rigorous as those which the AI would have conducted itself for the customer;

(b) the AI must satisfy itself as to the reliability of the systems put in place by the intermediary to verify the identity of the customer; and

(c) the AI must reach agreement with the intermediary that it will be permitted to verify the due diligence undertaken by the intermediary at any stage.

6.4 Repealed.

6.5 An AI should conduct periodic reviews to ensure that an intermediary upon which it relies continues to conform to the criteria set out above. This may involve review of the relevant policies and procedures of the intermediary and sample checks of the due diligence conducted.

6.6 An Intermediary Certificate (see Annex) duly signed by the intermediary should be obtained by AIs, together with all relevant identification data and other documentation pertaining to the customer's identity [IN 29]. Relevant documentation should consist of either the original documentation (which is preferable) or copies that have been certified by a suitable certifier.

6.7 The purpose of obtaining the underlying documentation is to ensure that it is immediately available on file for reference purposes by the AI or relevant authorities such as the HKMA and the JFIU, and for on-going monitoring of the customer. It will also enable the AI to verify that the intermediary is doing its job properly. It is not the intention that the AI should use the documentation, as a matter of course, to repeat the due diligence conducted by the intermediary.

Non face-to-face Document Verification

6.8 A suitable certifier will certify that he has seen the original documentation and that the copy document which has been certified is a complete and accurate copy of that original. The signature and official stamp of the certifier should be placed on the first page of the copy document and the number of pages should be recorded. A suitable certifier will either be the intermediary itself or:

(a) an embassy, consulate or high commission of the country of issue of the documentary evidence of identity;

(b) a member of the judiciary, a senior civil servant or serving police or customs officer in a jurisdiction that is a FATF member or an equivalent jurisdiction;

(c) a lawyer, notary public, actuary, accountant or a chartered secretary in a jurisdiction that is a FATF member or an equivalent jurisdiction; or

(d) a director, officer or manager of a regulated financial institution incorporated in, or operating from, a jurisdiction that is a FATF member or an equivalent jurisdiction.

7. Client accounts

7.1 This section supersedes paragraph 5.23 of the Guideline. It refers to accounts opened in the name of a professional intermediary [IN 30] or of a unit trust, mutual fund, or any other investment scheme (including staff provident fund and retirement scheme) managed or administered by a professional intermediary as an agent.

7.2 If a client account is opened on behalf of a single client or there are sub-accounts for each individual client where funds are not co-mingled at the AI, the AI should establish the identity of the underlying client(s) in addition to that of the intermediary opening the account.

7.3 For a client account in which funds for individual clients are co-mingled [IN 31], the AI is not required, as a matter of course, to identify the individual clients. This is however subject to the following (see also paragraph 6.1a above):

(a) the AI is satisfied that the intermediary has put in place reliable systems to verify customer identity; and

(b) the AI is satisfied that the intermediary has proper systems and controls to allocate funds in the pooled account to the individual underlying clients.

7.4 Where an intermediary cannot satisfy the above conditions and refuses to provide information about the identity of underlying clients by claiming, for example, reliance on professional secrecy, an AI should not permit the intermediary to open a client account.

7.5 An AI should not be precluded from making reasonable enquiries about transactions passing through client accounts that give cause for concern or from reporting those transactions if any suspicion is aroused.

8. Non-face-to-face customers

8.1 This section supersedes paragraphs 5.24 and 5.25 of the Guideline.

8.2 An AI should whenever possible conduct a face-to-face interview with a new customer to ascertain the latter's identity and background information, as part of the due diligence process. This can be performed either by the AI itself or by an intermediary that can be relied upon to conduct proper customer due diligence (see section 6 above).

8.3 This is particularly important for higher risk customers. For the latter, the AI should ask the customer to make himself available for a face-to-face interview.

8.4 Where face-to-face interview is not conducted, for example where the account is opened via the internet, an AI should apply equally effective customer identification procedures and on-going monitoring standards as for face-to-face customers.

8.5 Examples of specific measures that AIs can use to mitigate the risk posed by such non-face-to-face customers include:

(a) certification of identity documents presented by suitable certifiers (see paragraph 6.8 above);

(b) requisition of additional documents to complement those required for face-to-face customers;

(c) completion of on-line questionnaires for account opening applications that require a wide range of information capable of independent verification (such as confirmation with a government department);

(d) independent contact with the customer by the AI;

(e) third party introduction through an intermediary which satisfies the criteria in paragraphs 6.1a and 6.3 above;

(f) requiring the first payment from the account to be made through an account in the customer's name with another AI or foreign bank which the AI is satisfied has similar customer due diligence standards to its own;

(g) more frequent update of the information on non-face-to-face customers; or

(h) in the extreme, refusal of business relationship without face-to-face contact for higher risk customers.

9. Wire transfer messages

9.1 This section supersedes paragraphs 6.1 to 6.3 of the Guideline. The requirements are based on the FATF Special Recommendation on Terrorist Financing (see paragraph 15.3) that relates to wire transfer and the associated Interpretative Note.

9.2 An ordering AI must ensure that any wire transfer of HK$8,000 or more (or its foreign currency equivalent) is accompanied by the following information: the originator's name, account number (or unique reference number if no account exists) and (i) address [IN 32a]; or (ii) national identity number [IN32bb]; or (iii) date and place of birth. AIs should ensure that only verified information accompanies such transfers [IN 32b].

9.3 An ordering AI may choose not to include all the above information in the wire transfer message accompanying a wire transfer of less than HK$8,000 or its equivalent in foreign currencies [IN 32c]. The relevant information about the originator should nevertheless (and notwithstanding paragraph 5.27 of the Guideline [IN 33]) be recorded and retained by the ordering AI and should be made available within 3 business days upon request from either the beneficiary financial institution or appropriate authorities.

9.4 An ordering AI should adopt a risk-based approach to check whether certain wire transfers may be suspicious taking into account such factors as the name of the beneficiary, the destination and amount of the wire transfer etc.

9.5 In particular, an ordering AI should exercise care if there is suspicion that a customer may be effecting a wire transfer transaction on behalf of a third party. If a wire transfer carries the name of a third party as the ordering person or otherwise does not appear to be consistent with the usual business / activity of the customer, the customer should be asked to provide further explanation of the nature of the wire transfer.

9.6 An AI acting as an intermediary in a chain of wire transfers should ensure that the information in paragraph 9.2 remains with the wire transfer message throughout the payment chain.

9.7 An AI handling incoming wire transfers for a beneficiary should conduct enhanced scrutiny of, and monitor for, wire transfer messages which do not contain complete originator information. This can be done through risk-based methods taking into account factors that may arouse suspicion (e.g. country of origin of the wire transfer). If necessary, this may be done after effecting the transaction particularly for items handled by straight-through processing.

9.8 The beneficiary AI should consider whether unusual wire transfer transactions should be reported to the JFIU. It may also need to consider restricting or terminating its business with a remitting bank that fails to meet the FATF standards.

10. Politically exposed persons

10.1 This is a new section not currently covered in the Guideline.

10.2 Business relationships with individuals holding important public positions as well as persons or companies clearly related to them (i.e. families, close associates etc) expose an AI to particularly significant reputation or legal risks. There should be enhanced due diligence in respect of such politically exposed persons (PEPs). While this is particularly relevant to private banking business, the same enhanced due diligence should apply to PEPs in all business areas.

10.3 PEPs are defined as individuals being, or who have been, entrusted with prominent public functions, such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives

of public organisations and senior political party officials. The concern is that there is a possibility, especially in countries where corruption is widespread, that such PEPs may abuse their public powers for their own illicit enrichment through the receipt of bribes etc.

10.4 An AI should have appropriate systems and controls in place to determine, as far as practicable, whether a potential customer, customer or a connected party of a potential customer or direct customer [IN 34a] is a PEP. This could be achieved for example, by screening the name of the customer and connected parties against publicly available information or a commercial electronic database to determine whether the customer or connected parties are politically exposed, before establishing a business relationship, or performing any one off transaction equivalent to HK$120,000 or more for a non account holder, and on a periodic basis thereafter.

10.5 AIs must obtain senior management approval before establishing a business relationship with a customer or a beneficial owner identified as a PEP. An AI must also obtain senior management approval to continue the relationship as soon as practicable after an existing customer or a beneficial owner is identified as a PEP.

10.5a An AI should take reasonable measures to identify the source of wealth and funds of a customer identified as a PEP [IN 34b]; and ensure increased ongoing monitoring of the customer and his business with the AI throughout the relationship. This will include a periodic review on at least an annual basis of the relationship (and account activities).

10.6 Risk factors an AI should consider in handling a business relationship (or potential relationship) with a PEP include:

(a) any particular concern over the country where the PEP holds his public office or has been entrusted with his public functions, taking into account his position;

(b) any unexplained sources of wealth or income (i.e. value of assets owned not in line with the PEP's income level);

(c) expected receipts of large sums from governmental bodies or state-owned entities;

(d) source of wealth described as commission earned on government contracts;

(e) request by the PEP to associate any form of secrecy with a transaction; and

(f) use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

11. Correspondent banking

11.1 This is a new section not currently covered in the Guideline.

11.2 Correspondent banking is defined as the provision by one bank (the correspondent) to another bank (the respondent) of credit, deposit, collection, clearing, payment or other similar services [IN 35].

11.3 An AI providing correspondent banking services should gather sufficient information about its respondent banks to understand the latter's business. This basic level of due diligence should be performed regardless of whether a credit facility is granted to a respondent bank. AIs should obtain approval from senior management [IN 36] before establishing new correspondent banking relationships and document the respective responsibilities of each institution.

11.4 The information to be collected [IN 37] should include details about the respondent bank's management, major business activities, where it is located, its money laundering prevention efforts [IN 38], the system of bank regulation and supervision in the respondent bank's country and the purpose of the account etc.

11.5 An AI should in general establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.

11.6 In particular, an AI should not establish or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which the bank has no presence and which is unaffiliated with a regulated financial group (i.e. a shell bank).

11.7 An AI should pay particular attention when maintaining a correspondent banking relationship with banks incorporated in jurisdictions that do not meet international standards for the prevention of money laundering. Enhanced due diligence will generally be required in such cases, including obtaining details of the beneficial ownership of such banks and more extensive information about their policies and procedures to prevent money laundering. There should also be enhanced procedures in respect of the on-going monitoring of activities conducted through such correspondent accounts, such as development of transaction reports for review by the compliance officer, close monitoring of suspicious fund transfers etc.

11.8 Particular care should also be exercised where the AI's respondent banks allow direct use of the correspondent account by their customers to transact business on their own behalf (i.e. payable–through accounts). An AI should therefore establish whether the customers of the respondent bank will be allowed to use the correspondent banking service and, if so, it should take steps to require verification of the identity of such customers. The procedures set out in section 6 should be used in such cases.

11.9 An AI should take appropriate measures to ensure that it does not enter into or continue a correspondent banking relationship with a bank which is known to permit its accounts to be used by a shell bank.

12. Existing accounts

12.1 This section supersedes paragraph 5.3 of the Guideline.

12.2 An AI should take steps to ensure that the records of existing customers remain up-to-date and relevant. Where necessary, additional evidence of the identity of existing customers should be obtained to ensure that these comply with the AI's current standards.

12.3 To achieve this, an AI should undertake periodic reviews of existing records of customers. An appropriate time to do so is upon certain trigger events. These include:

(a) when a significant [IN 39] transaction is to take place;

(b) when there is a material change in the way the account is operated;

(c) when the AI's customer documentation standards change substantially; or

(d) when the AI is aware that it lacks sufficient information about the customer.

12.4 For the avoidance of doubt, even in the absence of an intervening trigger event, an AI should still conduct a review at least annually [IN 39a] on all high-risk customers to ensure that the customers' records it maintains are kept up-to-date and relevant. The frequency of such reviews should be documented in the AI's policies and procedures.

13. On-going monitoring

13.1 This is an area not specifically covered in the Guideline. This section should however be read in conjunction with sections 8 and 9 of the Guideline.

13.2 In order to satisfy its legal and regulatory obligations, an AI needs to have systems to enable it to identify and report suspicious transactions. However, it is not enough to rely simply on the initiative of front-line staff to make ad hoc reports. An AI should also have management information systems (MIS) to provide managers and compliance officers with timely information on a regular basis to enable them to detect patterns of unusual or suspicious activity, particularly in relation to higher risk accounts.

13.3 This also requires the AI to have a good understanding of what is normal and reasonable activity for particular types of customer, taking into account the nature of the customer's business. Among other things, an AI should take

appropriate measures to satisfy itself about the source and legitimacy of funds to be credited to a customer's account. This is particularly the case where large amounts and/or higher risk customers are involved.

13.4 A further relevant consideration in respect of funds derived from outside Hong Kong is whether the transfer of such funds may have breached the exchange controls of the country of origin.

13.5 MIS reports used for monitoring purposes should be capable of identifying transactions that are unusual either in terms of amount (for example, by reference to predetermined limits for the customer in question or to comparative figures for similar customers) or type of transaction or other relevant risk factors. High account activity in relation to the size of the balance on an account or unusual activity in an account (such as early settlement of instalment loans by way of cash repayment) may, for example, indicate that funds are being "washed" through the account and may trigger further investigation. The AI should take appropriate follow-up actions on any unusual activities identified in the MIS reports. The findings and any follow-up actions taken should be properly documented and the relevant documents should be maintained for a period not less than six years following the date when the unusual activity is identified.

13.6 While a focus on cash transactions is important, it should not be exclusive. An AI should not lose sight of non-cash transactions, e.g. inter-account transfers or inter-bank transfers. The MIS reports referred to above should therefore capture not only cash transactions but also those in other forms. The aim should be to obtain a comprehensive picture of the customer's transactions and overall relationship with the AI. In this regard the overall relationship should also cover, to the extent possible and using a risk-based approach, the customer's accounts and transactions with the AI's overseas operations.

14. Jurisdictions which do not or insufficiently apply the FATF Recommendations

14.1 This is a new section not currently covered in the Guideline.

14.2 Repealed.

14.3 Repealed.

14.4 An AI should apply Recommendation 21 of the FATF revised Forty Recommendations to jurisdictions which do not or insufficiently apply the FATF Recommendations. This states that:

"Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible,

be examined, the findings established in writing, and be available to help competent authorities."

14.5 Extra care should therefore be exercised by an AI in respect of customers (including beneficial owners [IN 40]) connected with jurisdictions which do not or insufficiently apply the FATF Recommendations [IN 3 & 41] or otherwise pose a higher risk to an AI. In addition to ascertaining and documenting the business rationale for opening an account or applying for banking services as required under paragraph 3.2(da) above, an AI should be fully satisfied with the legitimacy of the source of funds [IN 21] of such customers.

14.5a Factors that should be taken into account in determining whether jurisdictions do not or insufficiently apply the FATF Recommendations or otherwise pose a higher risk to an AI include:

(a) whether the jurisdiction is or a significant number of persons or entities in that jurisdiction are, subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances, a jurisdiction subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, may be given credence by an AI because of the standing of the issuer and the nature of the measures;

(b) whether the jurisdiction is identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures;

(c) whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organisations operating within it; and

(d) whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.

"Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

14.6 For jurisdictions with serious deficiencies in applying the FATF Recommendations and where inadequate progress has been made to improve their position, the FATF may recommend the application of further counter-measures. The specific counter-measures, to be determined by the HKMA in each case, would be gradual and proportionate to the specific problem of the jurisdiction concerned. The measures will generally focus on more stringent

customer due diligence and enhanced surveillance / reporting of transactions. An AI should apply the counter-measures determined by HKMA from time to time.

14.7 An AI should be aware of the potential reputation risk of conducting business in jurisdictions which do not or insufficiently apply the FATF Recommendations or other jurisdictions known to apply inferior standards for the prevention of money laundering and terrorist financing.

14.8 If an AI incorporated in Hong Kong has operating units in such jurisdictions, care should be taken to ensure that effective controls on prevention of money laundering and terrorist financing are implemented in these units. In particular, the AI should ensure that the policies and procedures adopted in such overseas units are equivalent to those adopted in Hong Kong. There should also be compliance and internal audit checks by staff from the head office in Hong Kong. In extreme cases the AI should consider withdrawing from such jurisdictions.

15. Terrorist financing

15.1 This is a new area not currently covered in the Guideline.

15.2 Terrorist financing generally refers to the carrying out of transactions involving funds that are owned by terrorists, or that have been, or are intended to be, used to assist the commission of terrorist acts. This has not previously been explicitly covered under the money laundering regime where the focus is on the handling of criminal proceeds, i.e. the source of funds is what matters. In terrorist financing, the focus is on the destination or use of funds, which may have derived from legitimate sources.

15.3 Since 9/11 the FATF has expanded its scope of work to cover matters relating to terrorist financing. In this context, it has produced nine Special Recommendations on Terrorist Financing. A list of these can be found on the FATF website (***http://www.fatf-gafi.org***).

15.4 The United Nations Security Council (UNSC) has passed various resolutions to require sanctions against certain designated terrorists and terrorist organisations. In Hong Kong, Regulations issued under the United Nations (Sanctions) Ordinance give effect to these UNSC resolutions. In particular, the United Nations Sanctions (Afghanistan) Regulation provides, among other things, for a prohibition on making funds available to designated terrorists. The list of designated terrorists is published in the Gazette from time to time.

15.5 In addition, the United Nations (Anti-Terrorism Measures) Ordinance was enacted on 12 July 2002. This implements the mandatory elements of the UNSC Resolution 1373. The latter is aimed at combating international terrorism on various fronts, including the introduction of measures against terrorism financing. The Ordinance also implements the most pressing elements of the FATF's nine Special Recommendations.

15.6 The Ordinance, among other things, prohibits the supply of funds or making of funds available to terrorists or terrorist associates as defined. It also makes it a statutory requirement for a person to report his knowledge or suspicion that any property is terrorist property. As with the above mentioned Regulations, a list of terrorist names will be published in the Gazette from time to time for this purpose.

15.7 An AI should take measures to ensure compliance with the relevant regulations and legislation on terrorist financing. The legal obligations of the AI and those of its staff should be well understood and adequate guidance and training should be provided to the latter. The systems and mechanisms for identification of suspicious transactions should cover terrorist financing as well as money laundering.

15.8 It is particularly vital that an AI should be able to identify and report transactions with terrorist suspects. To this end, an AI should ensure that it maintains a database of names and particulars of terrorist suspects which consolidates the various lists that have been made known to it. Alternatively, an AI may make arrangements to secure access to such a database maintained by third party service providers.

15.9 Such database should, in particular, include the lists published in the Gazette and those designated under the US Executive Order of 23 September 2001. The database should also be subject to timely update whenever there are changes, and should be made easily accessible by staff for the purpose of identifying suspicious transactions.

15.10 An AI should check the names of both existing customers and new applicants for business against the names in the database. It should be particularly alert for suspicious wire transfers and should bear in mind the role which non-profit organisations are known to have played in terrorist financing. Enhanced checks should be conducted before processing a transaction, where possible, if there are circumstances giving rise to suspicion.

15.11 The FATF issued in April 2002 a paper on guidance for financial institutions in detecting terrorist financing. The document describes the general characteristics of terrorist financing with case studies illustrating the manner in which law enforcement agencies were able to establish a terrorist financing link based on information reported by financial institutions. Annex 1 of the document contains a series of characteristics of financial transactions that have been linked to terrorist activity in the past.

15.12 An AI should acquaint itself with the FATF paper and should use it as part of its training material for staff. The paper is available on the FATF website (***http://www.fatf-gafi.org***).

15.13 It should be noted that the list of characteristics only serves to show the types of transaction that could be a cause for additional scrutiny if one or more of the characteristics is present. The parties involved in the transaction should also be taken into account, particularly when the individuals or entities appear on a list of suspected terrorists.

15.14 Where an AI suspects that a transaction is terrorist-related, it should make a report to the JFIU and to the HKMA. Even if there is no evidence of a direct terrorist connection, the transaction should still be reported to the JFIU if it looks suspicious for other reasons. It may emerge subsequently that there is a terrorist link.

16. Risk management

16.1 This section should be read in conjunction with section 9 of the Guideline in relation to the role of the compliance officer.

16.2 The senior management of an AI should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and ensuring their effectiveness. Explicit responsibility should be allocated within an AI for this purpose.

16.3 An AI should appoint a compliance officer as a central reference point for reporting suspicious transactions. The role of the compliance officer should not be simply that of a passive recipient of ad hoc reports of suspicious transactions. Rather, the compliance officer should play an active role in the identification and reporting of suspicious transactions. This should involve regular review of exception reports of large or irregular transactions generated by the AI's MIS as well as ad hoc reports made by front-line staff. Depending on the organization structure of the AI, the specific task of reviewing reports may be delegated to other staff but the compliance officer should maintain oversight of the review process.

16.4 The compliance officer should form a considered view whether unusual or suspicious transactions should be reported to the JFIU. In reporting to the JFIU, the compliance officer should ensure that all relevant details are provided in the report and cooperate fully with the JFIU for the purpose of investigation. If a decision is made not to report an apparently suspicious transaction to the JFIU, the reasons for this should be fully documented by the compliance officer. The fact that a report may already have been filed with the JFIU in relation to previous transactions of the customer in question should not necessarily preclude the making of a fresh report if new suspicions are aroused.

16.5 More generally, the compliance officer should have the responsibility of checking on an ongoing basis that the AI has policies and procedures to ensure compliance with legal and regulatory requirements and of testing such compliance.

16.6 It follows from this that the AI should ensure that the compliance officer is of sufficient status within the organisation, and has adequate resources, to enable him to perform his functions.

16.7 Internal audit also has an important role to play in independently evaluating on a periodic basis an AI's policies and procedures on money laundering. This should include checking the effectiveness of the compliance officer function,

the adequacy of MIS reports of large or irregular transactions and the quality of reporting of suspicious transactions. The level of awareness of front line staff of their responsibilities in relation to the prevention of money laundering should also be reviewed. As in the case of the compliance officer, the internal audit function should have sufficient expertise and resources to enable it to carry out its responsibilities.

Hong Kong Monetary Authority
July 2010

Annex

INTERMEDIARY CERTIFICATE

I/We wish to apply for opening an account on behalf of the following *person(s)/company:

Customer Name _____

Address _____

_____

1. I/We confirm that I/we have verified the customer's identity and address and enclose herewith *a summary sheet containing the following identification data / the following identity documents (or copies of such documents duly certified), in accordance with the requirements set out in the HKMA's Guideline on Prevention of Money Laundering (including its Supplement and the accompanying Interpretative Notes):

   (a) Identity card(s)/passport(s) of *the customer / all authorized signatories, directors (at least 2 including the managing director) and all principal shareholders of the company;

   (b) Resolution of the board of directors to open account and confer authority on those who will operate the account;

   (c) Certificate of Incorporation;

   (d) Business Registration Certificate;

   (e) Memorandum and Articles of Association;

   (f) Search record at the Company Registry;

   (g) Evidence of address;

   (h) Other relevant documents.

2. I/ We confirm that the *occupation / business activities of the customer is/are

   _____.

3. I am/We are satisfied as to the source of funds being used to open the account. The details are set out below:

   _____.

4. I/We enclose the account opening documents duly completed, and confirm that the signature(s) contained in the account opening documents is/are signed by the customer(s).

5. I/We enclose herewith the evidence of authority for me / us to act on behalf of the customer in the application for opening and / or operating the account.

* *Please delete as appropriate*

Signed: _____

Name: _____

Position held: _____ at _____(name of company / firm)____

Date: _____

INTERPRETATIVE NOTES

General guidance

The revised FATF Forty Recommendations and the Basel CDD requirements: Both the FATF and Basel requirements are relevant to the banking sector in Hong Kong. The former sets out the basic framework for both financial institutions and non-financial institutions, while the latter (which is recognised to be more rigorous than the FATF requirements in some respects) is specifically directed towards the prudential regulation of banks and tailored towards the risks to which banks are exposed. It is considered appropriate for the banking industry to adopt enhanced customer due diligence (CDD) standards because of the nature of their business. However, some flexibility is appropriate given the practicalities of implementing the measures and the fact that not all elements of the requirements are yet fully developed and may take some time to put in place (e.g. regulatory regime for professional intermediaries). Accordingly, where the risk of money laundering is low, the FATF approach may be adopted and simplified CDD procedures used.

Risk-based approach: AIs should adopt more extensive due diligence for higher risk customers. Conversely, it is acceptable for AIs to apply a simplified CDD process for lower risk customers. In general, AIs may apply a simplified CDD process in respect of a customer or a particular type of customers where there is no suspicion[1] of money laundering, and [Para. 2.2]:

- the risk[2] of money laundering is assessed to be low; or
- there is adequate public disclosure in relation to the customers.

Overriding principle: The guiding principle for the purpose of compliance with the Guideline on Prevention of Money Laundering and its Supplement is that AIs should be able to justify that they have taken reasonable steps to satisfy themselves as to the true identity of their customers including beneficial owners. These measures should be

[1] There may be instances where the circumstances lead one to be suspicious even though the inherent risk may be low.
[2] This refers to the intrinsic or inherent risk relating to a type of customer.

objectively reasonable in the eyes of a third party. In particular, where an AI is satisfied as to any matter it should be able to justify its assessment to the HKMA or any other relevant authority. Among other things, this would require the AI to document its assessment and the reasons for it.

Terminology

The term "customer" refers to a person who maintains an account with or carries out a transaction with an AI (i.e. the direct customer[3]), or a person on whose behalf an account is maintained or a transaction is carried out (i.e. the beneficial owner). In the context of cross-border transactions:

- if a local office has only a marketing relationship with a person who maintains an account in its overseas office, the local office will be regarded as an intermediary and the person a "customer" of its overseas office[4]; and
- if a local office carries out transactions for a person with an account which is domiciled in its overseas office, that person should be regarded as the "customer" of the local office as well as its overseas office[5].

The term "beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

---

[3] This generally excludes the third parties of a transaction. For example, an ordering AI in an outward wire transfer transaction does not regard the beneficiary (who has no other relationship with the AI) as its customer.

[4] The overseas office will be responsible for the CDD review and on-going monitoring of that customer in accordance with the group KYC policy and the regulatory requirements in the respective countries. The local office may, however, be requested by its overseas office to perform these on its behalf.

[5] A local office may rely on the CDD review and on-going monitoring carried out by its overseas office as an intermediary, provided that a common set of CDD standards consistent with the FATF standards applies on a bank/group-wide basis. Customer identity **information** must, nonetheless, be obtained as a minimum by the local office (some local offices may have an unfettered right to access and retrieve all the relevant customer identity information from the group database maintained) although the local office may choose not to obtain copies of the identity **documentation** and records of transactions performed by the local office on the customer's behalf as long as the customer documentation and

Specific guidance

Group customer due diligence requirements

1. The general principle is that a common set of CDD standards should be applied on a consolidated basis throughout a banking group. Simplified CDD procedures might, however, be used by a group company on a particular type of customer where the area of business in question is considered to be of a low risk in nature. In addition, the use of simplified CDD should be fully justified, well documented and properly approved by senior management. Such risk-based approach should also be clearly set out in the group policies. Where group standards cannot be applied for good reason, e.g. due to legal or regulatory reasons, deviations should be documented and risk mitigating measures applied. [Para 1.7]

Customer due diligence

2. Repealed.

3. AIs should adopt a balanced and common sense approach with regard to customers connected with jurisdictions which do not or insufficiently apply the FATF Recommendations. While extra care may well be justified in such cases, it is not a requirement that AIs should refuse to do any business with such customers or automatically classify them as high risk and subject them to enhanced CDD process. Rather, AIs should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of money laundering. [Para 2.3(a) & 14.5]

4. For customers from countries where the citizens do not have any official identity documents, AIs should adopt a common sense approach to decide what other unique identification documents can be accepted as a substitute. [Para 3.2(b)]

---

these transaction records kept by the overseas office will be made available upon request without delay.

5. For Hong Kong permanent residents[6], AIs should verify an individual's name, date of birth and identity card number by reference to his/her identity card. For nonpermanent residents, AI should additionally verify the individual's nationality through an inspection of his/her travel document.

AIs should verify the identity of non-residents by reference to their travel documents [IN 9b].

When identifying a non-resident who is not physically present in Hong Kong, AIs should verify the individual's identity by reference to (i) a valid travel document; (ii) a relevant national identity card bearing the individual's photograph; or (iii) a valid national driving licence bearing the individual's photograph issued by a competent national authority that verifies the holder's identity before issuance. [Para 3.3]

6. Throughout these guidelines reference to "address" for a natural person means residential address (and permanent address if different).

AIs should use a common sense approach to handle cases where the customers (e.g. students and housewives) are unable to provide address proof.

Apart from the methods suggested in paragraph 5.7 of the Guideline (e.g. by requesting sight of a recent utility or rates bill), AIs may use other appropriate means, such as home visits, to verify the residential address of a customer, as is the case for some private banking customers. [Para 3.3]

7. Information about occupation or employer is a relevant piece of information about a customer but does not form part of the customer's identity requiring verification. [Para 3.3]

8. Exceptions may be made to allow payments to third parties subject to the following conditions:

---

[6] These customers will have a Hong Kong Permanent Identity Card. The identity card of a permanent resident (i.e. a Hong Kong Permanent Identity Card) will have on the front of the card a capital letter "A" underneath the individual's date of birth. The reverse of the card will state the holder has the right of abode in Hong Kong.

- there is no suspicion of money laundering;
- the risk of money laundering is assessed to be low;
- the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction;
- the names of recipients do not match with watch lists such as those for terrorist suspects and PEPs; and
- the verification process should be completed within one month from the date the business relationship was established. [Para 3.6]

9. The funds should generally be returned to the account holders. It is up to individual AIs to decide the means to repay the funds but AIs must guard against the risk of money laundering since this is a possible means by which funds can be "transformed", e.g. from cash into a cashier order. It is therefore important for AIs to ensure that they only open accounts with customers where they have reasonable grounds to believe that the relevant CDD process can be satisfactorily completed within a reasonable timeframe. [Para 3.7]

9a. Transactions undertaken for non-account holders may include for example wire transfer or currency exchange transactions, the purchase of a cashier order or gift cheque. [Para 3.10]

9b. "Travel document" means a passport furnished with a photograph of the holder, or some other documents establishing to the satisfaction of an immigration officer or immigration assistant the identity and nationality, domicile or place of permanent residence of the holder. The following documents constitute travel documents for the purpose of identity verification:

- Permanent Resident Identity Card of Macau Special Administrative Region;
- Mainland Travel Permit for Taiwan Residents;
- Seaman's Identity Document (issued under and in accordance with the International Labour Organisation Convention / Seafarers Identity Document Convention 1958);

- Taiwan Travel Permit for Mainland Residents;
- Permit for residents of Macau issued by Director of Immigration.
- Exit-entry Permit for Travelling to and from Hong Kong and Macau for Official Purposes;
- Exit-entry Permit for Travelling to and from Hong Kong and Macau.

[Para 3.14, 3.15 & 3.16]

Corporate customers

10. A recognised stock exchange is a stock exchange of a jurisdiction which is a member of the FATF or a specified stock exchange as defined under Schedule 1 to the Securities and Futures Ordinance, but it does not include a stock exchange of jurisdictions which do not or insufficiently apply the FATF Recommendations (Annex 2 of the Guideline is superseded). [Para 4.2]

11. A simplified CDD process may be applied to:
    (a) state-owned enterprises and their subsidiaries in a jurisdiction where the risk of money laundering is assessed to be low and where the AI has no doubt as regards the ownership of the enterprise; or
    (b) companies listed on a recognised stock exchange and their subsidiaries.

    AIs should identify and verify the identity of at least 2 account signatories of such companies and may adopt a risk based approach to determine whether or not it is necessary to identify and verify the identity of further account signatories. [Para 4.2]

12. Repealed.

13. A person entitled to control or exercise the control of 10% or more of the voting rights of a company should be regarded as a principal shareholder of the company. [Para 4.5]

14. Equivalent jurisdictions are jurisdictions (other than FATF members) that in the view of the institution sufficiently apply standards of prevention of money laundering and terrorist financing equivalent to those of the FATF.

In determining whether or not a jurisdiction sufficiently applies FATF standards in combating money laundering and terrorist financing and meets the criteria for an equivalent jurisdiction, AIs should:

(a) carry out their own assessment of the standards of prevention of money laundering and terrorist financing adopted by the jurisdiction concerned. The assessment can be made based on the AI's knowledge and experience of the jurisdiction or market intelligence. The higher the risk, the greater the due diligence measures that should be applied when undertaking business with a customer from the jurisdiction concerned;

(b) pay attention to assessments that have been undertaken by standard setting bodies such as the FATF and by international financial institutions such as the International Monetary Fund (IMF). In addition to the mutual evaluations carried out by the FATF and FATF-style regional bodies, the IMF and the World Bank, as part of their financial stability assessments of countries and territories, have carried out country assessments in relation to compliance with prevention of money laundering and terrorist financing standards based on the FATF Recommendations; and

(c) maintain an appropriate degree of ongoing vigilance concerning money laundering risks and take into account information that is reasonably available to them about the standards of anti-money laundering/terrorist financing systems and controls that operate in the jurisdiction with which any of their customers are associated. [Para 4.4]

15. In the case of offshore investment vehicles owned by high net worth individuals (i.e. the ultimate beneficial owners) who use such vehicles as the contractual party to establish a private banking relationship with AIs, exceptions to the requirement to obtain independent evidence about the ownership, directors and account signatories of the corporate customer may be made. This means that self-declarations in writing about the identity of, and the relationship with, the above parties from the ultimate beneficial owners or

the contractual parties may be accepted, provided that the investment vehicles are incorporated in a jurisdiction where company searches or certificates of incumbency (or equivalent) are not available or cannot provide meaningful information about their directors and principal shareholders and AIs are satisfied that:

- they know the identity of the ultimate beneficial owners; and
- there is no suspicion of money laundering.

Such exceptions are allowed on the basis that a comprehensive CDD process had been carried out in respect of the ultimate beneficial owners. A comprehensive CDD process for such customers should generally comprise the procedures as set out in Annex 2.

Exceptions made should be approved by senior management and properly documented. [Para 4.5]

16. AIs may rely on the documentation provided by professional third parties (such as lawyers, notaries, actuaries, accountants and corporate secretarial service providers) in Hong Kong on behalf of a corporate customer incorporated in a country where company searches are not available, provided that there is no suspicion arising from other information collected and these professional third parties can meet the criteria set out in paragraphs 6.1a and 6.3 of the Supplement and IN 28 below. [Para 4.5]

17. AIs may adopt a risk-based approach to decide whether the residential address of individuals who are connected with a legal person or legal arrangement (i.e. principal shareholders, directors, signatories, settlor/grantor/founder, protector(s) or known beneficiary of a legal arrangement) should be verified, provided that the risk-based process is clearly set out in the AI's policy, the waivers given are in accordance with the policy, the decisions made for such waivers are adequately documented and the money laundering risk of the customer is low. A waiver should not be given because of practical difficulties in the verification process. An express trust cannot form a business relationship or carry out a one-off transaction itself. It is the trustee of the trust who will

enter into a business relationship or carry out the one-off transaction on behalf of the trust and who will be considered to be the customer. The address of the trustee in a direct customer relationship should therefore always be verified. [Para 4.5]

18. Repealed.

19. AIs should record the identity (see [IN 5]) of all account signatories (this obligation does not apply to the staff of an AI acting in their official capacity). AIs may adopt a risk-based approach to decide whether this information (including users designated to approve fund transfers or other e-banking transactions on behalf of the corporate customer) should be verified, provided that the risk-based process is clearly set out in the AI's policy, the waivers given are in accordance with the policy and the decisions made for such waivers are adequately documented. In any case, the identity of at least two account signatories should be verified. A waiver should not be given because of practical difficulties in the verification process. [Para 4.5]

20. For corporate customers with a multi-layer ownership structure, AIs are only required to identify each stage in the ownership chain to obtain a full understanding of the corporate structure, but it is the natural person at the top of the chain (i.e. not the intermediate owners) whose identity needs to be verified. [Para 4.6]

21. Apart from those customers specified in the Supplement, AIs should also adopt a risk-based approach to determine the categories of customers whose source of funds should also be ascertained. [Para 4.7 & 14.5]

22. Where it is not practical to immobilise the bearer shares, AIs should obtain a declaration from each beneficial owner (i.e. who holds 5% or more of the total shares) of the corporate customer on the percentage of shareholding. Such owners should also provide a further declaration on annual basis and notify the AI immediately if the shares are sold, assigned or transferred. [Para 4.9]

Trust and nominee accounts

23. For trusts that are managed by trust companies which are subsidiaries (or affiliate companies) of an AI, that AI may rely on its trust subsidiaries to perform the CDD process, provided that:

- a written assurance from the trust subsidiary is obtained, confirming that evidence of the underlying principals has been obtained, recorded and retained and that it is satisfied as to the source of funds;
- the trust subsidiary complies with a group Know-Your-Customer (KYC) policy that is consistent with the FATF standards; and
- the documentation can be made available upon request without delay. [Para 5.2]

24. AIs may adopt a risk-based approach to determine whether it is necessary to verify the identity of protectors[7]. [Para 5.3]

25. To the extent that the CDD process on the settlors/asset contributors has been adequately performed, AIs may accept a declaration from the trustee or other contractual party to confirm the link or relationship with the settlors/asset contributors. [Para 5.3]

26. AIs should try as far as possible to obtain information about the identity of beneficiaries but a broad description of the beneficiaries such as family members of Mr XYZ may be accepted. [Para 5.3]

27. Where the identity of beneficiaries has not previously been verified, AIs should assess the need to undertake verification when they become aware that any payment out of the trust account is made to the beneficiaries or on their behalf. In making this assessment, AIs should adopt a risk-based approach which should take into account the amount(s) involved and any suspicion of money laundering. A decision not to undertake verification should be approved by senior management. [Para 5.3]

[7] The identity of the "protectors" is relevant information which has to be verified because these persons can, under certain circumstances, exercise their powers to replace the existing trustees.

Reliance on intermediaries for customer due diligence

28. AIs should take reasonable steps to satisfy themselves with regard to the adequacy of the CDD procedures and systems of intermediaries, but may adopt a risk-based approach to determine the extent of the measures to be taken. Relevant factors for the purpose of assessing the CDD standards of intermediaries include the extent to which the intermediaries are regulated in accordance with the FATF requirements and the legal requirements in the relevant jurisdiction to require the intermediaries to report suspicious transactions. [Para 6.3]

29. AIs may choose not to obtain, immediately, copies of documentation pertaining to the customer's identity, provided that they have taken adequate steps to satisfy themselves that the intermediaries will provide these copies upon request without delay. All the relevant identification data or information should nonetheless be obtained. [Para 6.6]

Client accounts

30. Examples of professional intermediaries include lawyers, accountants, fund managers, custodians and trustees. [Para 7.1]

31. In certain types of businesses (such as custodian, securities dealing or fund management), it may be common to have a series of vertically connected single client accounts or sub-accounts which ultimately lead to a co-mingled client fund account. AIs may regard such accounts as a co-mingled account to which the provisions of para 7.3 apply. [Para 7.3]

Wire transfer messages

32a. It is acceptable for an AI to include the "correspondence address" of the originating customer in the wire transfer message provided that the AI is satisfied that the address has been verified. [Para 9.2]

32b. In the case of a domestic wire transfer transaction, the additional information relating to the originating customer need not be included in the message provided that the information can be made available to the beneficiary AI and appropriate authorities by the ordering AI within 3 business days upon request. For the retrieval of information of earlier transactions (i.e. beyond 6 months), AIs should make such information available as soon as is practicable. [Para 9.2]

32bb. National identity number means Hong Kong identity card number or travel document number. [Para 9.2]

32c. In considering whether to apply the threshold of HK$8,000, AIs should take into account the business and operational characteristics of their wire transfer activities. AIs are encouraged to include, as far as practicable, the relevant originator information in the messages accompanying all wire transfer transactions. [Para 9.3]

33. The relevant originator information should be recorded and retained in respect of both account holders and non-account holders. [Para 9.3]

Politically exposed persons

34. Repealed.

34a. Connected parties to a direct customer include the beneficial owner and any natural person having power to direct the activities of the customer. For the avoidance of doubt the term connected party will include any director, principal shareholder, beneficial owner, signatory, trustee, settlor/grantor/founder, protector(s), or defined beneficiary of a legal arrangement. [Para 10.4]

34b. AIs should also consider whether it is appropriate to take measures to verify a PEP's source of funds and wealth, in line with its assessment of the risks. [Para 10.5a]

Correspondent banking

35. This includes the relationships established for securities transactions or funds transfers, whether for the respondent bank as a principal or for its customers. [Para 11.2]

36. As long as there is a formal delegation of authority and proper documentation, AIs may use a risk-based approach to determine the appropriate level of approval within the institution that is required for establishing new correspondent banking relationships. [Para 11.3]

37. Information on the authorization status and other details of a respondent bank, including the system of bank regulation and supervision in its country, may be obtained through publicly available information (e.g. public website and annual reports). [Para 11.4]

38. In assessing the anti-money laundering efforts of a respondent bank in a foreign country, AIs should pay attention to whether the respondent bank is permitted to open accounts for or carry out transactions with shell banks. [Para 11.4]

Existing accounts

39. The word "significant" is not necessarily linked to monetary value. It may include transactions that are unusual or not in line with an AI's knowledge of the customer. [Para 12.3(a)]

39a. An AI is not required to re-verify the identity or address of an existing individual customer or connected parties of an existing corporate customer that

are individuals unless there is doubt as to the veracity of the evidence previously obtained. [Para 12.4]

Jurisdictions which do not or insufficiently apply the FATF Recommendations

40. Where a customer has one or more (principal) beneficial owners connected with jurisdictions which do not or insufficiently apply the FATF Recommendations, the general principle is that the exercise of extra care should be extended to cases where the beneficial owner(s) has/have a dominant influence over the customer concerned. [Para 14.5]

41. AIs may regard FATF members as jurisdictions which have sufficiently applied the FATF Recommendations. [Para 14.5]

ANNEX 1: Repealed

ANNEX 2: Comprehensive CDD Process on Private Banking Customers

A comprehensive CDD process adopted for private banking customers generally covers the following areas:

- **Customer profile**

(a) In addition to the basic information relating to a customer's identity (see IN.5 and IN.6 above), AIs also obtain the following client profile information on each of their private banking customers:

- purpose and reasons for opening the account;
- business or employment background;
- estimated net worth;
- source of wealth;
- family background, e.g. information on spouse, parents (in the case of inherited wealth);
- source of funds (i.e. description of the origin and the means of transfer for monies that are acceptable for the account opening);
- anticipated account activity; and
- references (e.g. introduced by whom and when and the length of relationship) or other sources to corroborate reputation information where available.

All the above information relating to the private banking customer are to be properly documented in the customer file.

- **Global KYC policy**

(b) To facilitate customers' referral from overseas offices, AIs are to maintain global KYC policies to ensure that the same CDD standards are applied for all private banking customers on a group-wide basis.

- **Client acceptance**

(c) Generally, AIs do not accept customers without a referral. Walk-in customers are therefore not generally accepted unless they have at least a banker's reference.

(d) AIs also do not open private banking accounts without a face-to-face meeting with the customers, except in rare stances where the visitation policy set out in (h) below applies.

(e) Acceptance of private banking customers requires approval by senior management. For high risk or sensitive customers [8], additional approval from senior management and the Compliance Department or an independent control function (in the context of foreign subsidiaries or branches operating in Hong Kong, the parent bank or head office) may be required.

- **Dedicated relationship management**

(f) Each private banking customer is served by a designated relationship manager who bears the responsibility for CDD and on-going monitoring.

(g) AIs are to make sure that the relationship managers have sufficient time and resources to perform the enhanced CDD process and on-going monitoring of their private banking customers.

---

[8] Sensitive clients in private banking may include:
- PEPs;
- persons engaged in types of business activities or sectors known to be susceptible to money laundering such as gambling, night clubs, casinos, foreign exchange firms, money changers, art dealing, precious stone traders, etc.;
- persons residing in or having funds sourced from countries identified as insufficiently applying the FATF Recommendations or representing high risk for crime and corruption; and
- any other persons considered by individual AIs to be sensitive.

- **Monitoring**

(h) AIs conduct face-to-face meetings with their private banking customers as far as possible on a regular basis.

(i) Regular CDD reviews are conducted for each private banking customer. For high risk or sensitive customers, such reviews are performed annually or at a more frequent interval and may require senior management's involvement. Exceptions may, however, be allowed for inactive accounts for which CDD reviews should be conducted immediately prior to a transaction taking place.

(j) An effective monitoring system (e.g. based on asset size, asset turnover, client sensitivity or other relevant criteria) is in place to help identify any unusual or suspicious transaction on a timely basis.