Bills Committee on Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Bill

Information on Reference Materials

The customer due diligence and record-keeping requirements provided under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Bill largely reflect the existing requirements provided under the guidelines issued by the Hong Kong Monetary Authority ("HKMA"), the Office of the Commissioner of Insurance ("OCI") and the Securities and Futures Commission ("SFC") respectively. The drafting of the Bill has also drawn reference to the relevant regulations of the United Kingdom ("UK"). These documents are appended for Members' reference-

A (a) Guideline on Prevention of Money Laundering issued by HKMA ("HKMA Guidelines") – **Annex A**

B (b) Supplement to the Guideline on Prevention of Money Laundering issued by HKMA ("HKMA Supplement") – **Annex B**

C (c) Guidance Note on Prevention of Money Laundering and Terrorist Financing issued by OCI ("OCI Guidelines") – **Annex C**

D (d) Prevention of Money Laundering and Terrorist Financing Guidance Note issued by SFC ("SFC Guidelines") – **Annex D**

E (e) Money Laundering Regulations 2007 of the UK – **Annex E**

F 2. The references drawn upon in drafting certain clauses of the Bill are set out in **Annex F** for Members' reference.

Financial Services and the Treasury Bureau
20 December 2010

Annex A

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Annex 1	Repealed
Annex 2	Repealed
Annex 3	Repealed
Annex 4	Repealed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Annex 8	Repealed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 -

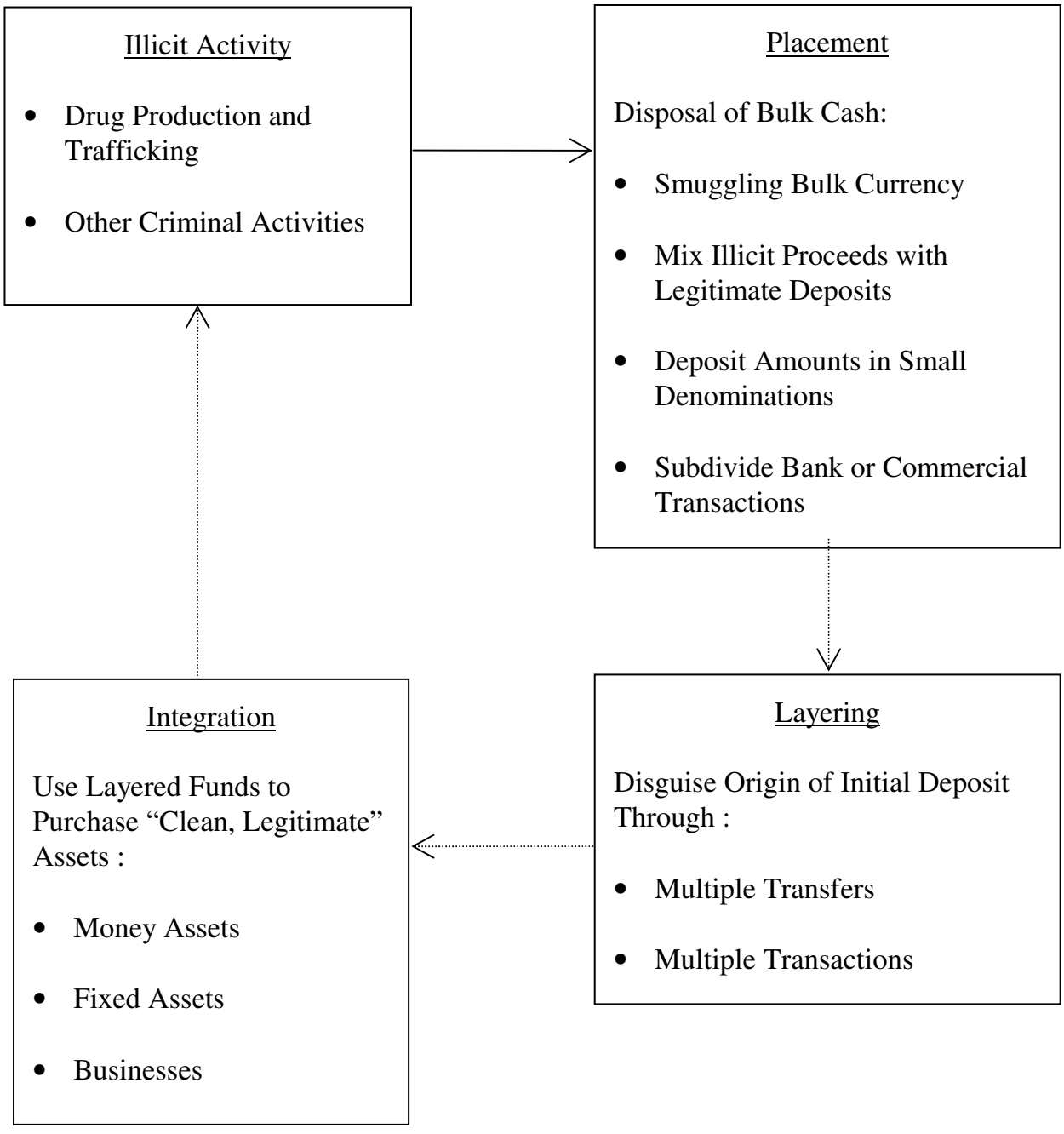
(a) Placement - the physical disposal of cash proceeds derived from illegal activity.

(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.

Annex 6

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

Annex B

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.

Annex C

Guidance Note on Prevention of Money Laundering and Terrorist Financing

October 2010

Office of the Commissioner of Insurance

CONTENTS

PART I OVERVIEW

1. INTRODUCTION

1.1 This Guidance Note aims to prevent criminal use of the insurance industry for the purposes of money laundering and terrorist financing. It presents the background information on money laundering and terrorist financing and summarizes the relevant legislations in Hong Kong. It also sets out the expectation of the Office of the Commissioner of Insurance ("OCI") of the internal policies and procedures of authorized insurers, reinsurers, insurance agents and insurance brokers carrying on or advising on long term business (hereinafter referred to as "insurance institutions") to guard against money laundering and terrorist financing.

1.2 This Guidance Note applies to all insurance institutions which are not financial institutions authorized by the Hong Kong Monetary Authority under the Banking Ordinance (Cap. 155) ("authorized financial institutions"). Insurance institutions that are authorized financial institutions are subject to the Hong Kong Monetary Authority's guidelines on prevention of money laundering ("the HKMA's guidelines"). However, to the extent that there are some insurance specific requirements and examples of suspicious transactions or money laundering cases in this Guidance Note which may not be shown in the HKMA's guidelines, the insurance institutions that are authorized financial institutions are required to have regard to paragraphs 2.2, 5, 6.1-6.3, 6.6.1-6.6.3, 6.7-6.8, 7.2.4 and 8.2.12 as well as Annexes 2, 3, 4 and 5 of this Guidance Note.

1.3 This Guidance Note does not have the force of law and should not be interpreted in any manner which would override the provisions of any applicable law or other regulatory requirements. However, failure to follow the requirements of this Guidance Note by insurance institutions may reflect adversely on the fitness and properness of their directors and controllers. Similarly, failure to follow the requirements of the HKMA's guidelines by the insurance institutions that are authorized financial institutions may reflect adversely on the fitness and properness of their directors and controllers. The OCI may take any appropriate interventionary actions empowered by the Insurance Companies Ordinance (Cap. 41) or other administrative sanctions if an insurance institution is found to be not in compliance with this Guidance Note.

1.4 The scope of this Guidance Note covers the activities of all insurance institutions to the extent that such activities are within the jurisdiction of Hong Kong. Where a Hong Kong incorporated insurance institution has branches or subsidiaries overseas, the requirements also apply to their overseas branches and subsidiaries. Where the local requirements differ

from these requirements, the overseas operations should apply the higher standard to the extent that the local laws permit. Where an overseas branch or subsidiary is unable to observe group standards, the OCI should be informed.

1.5 This Guidance Note will be regularly reviewed and revised in the light of developments in international standards on prevention of money laundering and terrorist financing.

2. BACKGROUND

2.1 What is money laundering and terrorist financing?

2.1.1 Money laundering is the processing of the illicit proceeds of crime to disguise their illegal origin. Once these proceeds are successfully laundered, the criminal is able to enjoy these monies without revealing their original illegitimate source.

2.1.2 Financing of terrorism can be defined as the wilful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds should be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts. Terrorism can be funded from legitimate income.

2.2 Vulnerabilities in insurance

2.2.1 The insurance industry is vulnerable to money laundering and terrorist financing. When a life insurance policy matures or is surrendered, funds become available to the policy holder or other beneficiaries. The beneficiary to the contract may be changed possibly against payment before maturity or surrender, in order that payments can be made by the insurer to a new beneficiary. A policy might be used as collateral to purchase other financial instruments. These investments in themselves may be merely one part of a sophisticated web of complex transactions with their origins elsewhere in the financial system.

2.2.2 Examples of the type of long term insurance contracts that are vulnerable as a vehicle for laundering money or financing terrorism are products such as:

(a) unit-linked or with profit single premium contracts;

(b) single premium life insurance policies that store cash value;

(c) fixed and variable annuities; and

(d) (second hand) endowment policies.

2.2.3 Money laundering and the financing of terrorism using reinsurance could occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, fronting arrangements and captives or by the misuse of normal reinsurance transactions. Examples include:

- the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds;

- the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding;

- the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers.

2.2.4 Insurance intermediaries are important for distribution, underwriting and claims settlement. They are often the direct link to the policy holder and therefore, intermediaries should play an important role in anti-money laundering and combating the financing of terrorism. The same principles that apply to insurers should generally apply to insurance intermediaries. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of or does not conform to necessary procedures, or who fails to recognize or report information regarding possible cases of money laundering or financing of terrorism. The intermediaries themselves could have been set up to channel illegitimate funds to insurers.

2.3 Stages of money laundering

2.3.1 There are three common stages of money laundering during which numerous transactions may be made by the launderers that could alert an insurance institution to potential criminal activity:

(a) Placement – the physical disposal of cash proceeds derived from illegal activity;

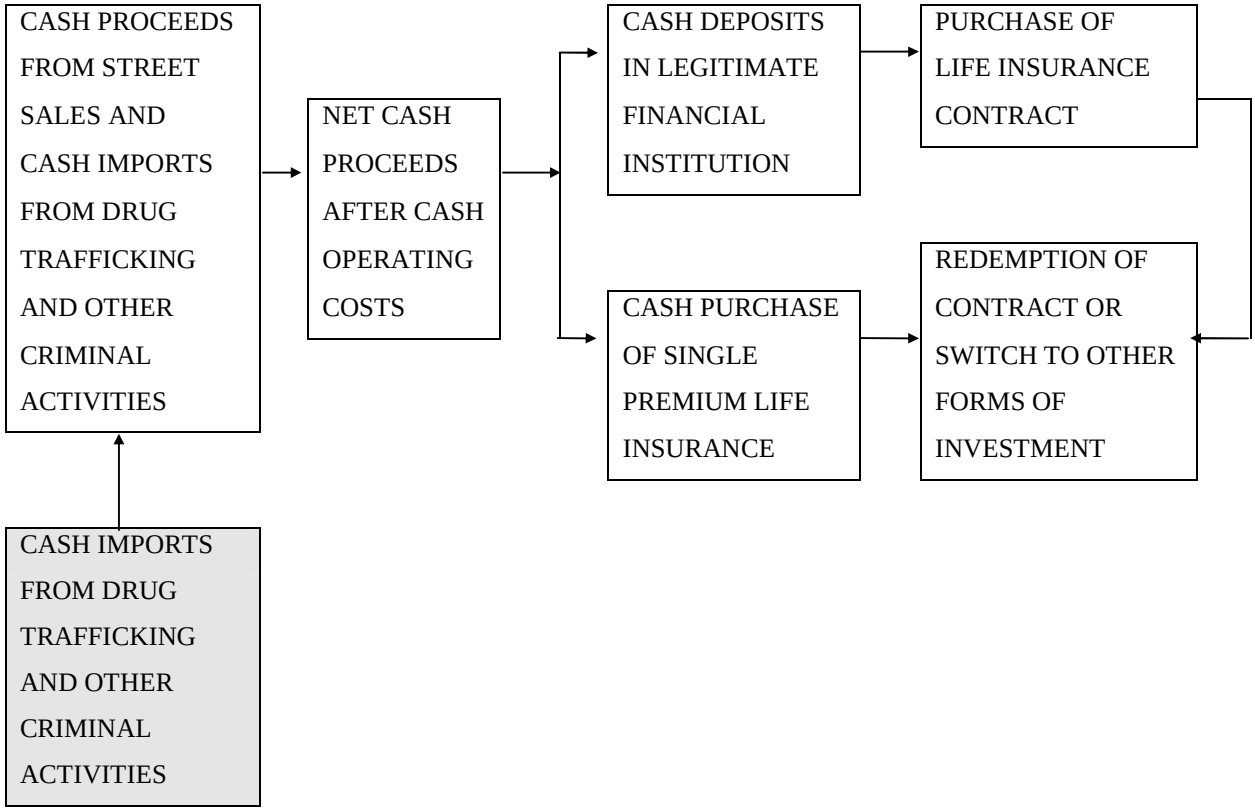
(b) Layering – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity; and

(c) Integration – creating the impression 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.

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

LAUNDERING OF PROCEEDS



Domestic

Foreign

2.4 International initiatives

2.4.1 The Financial Action Task Force ("FATF") was established in 1989 in an effort to thwart attempts by criminals to launder the proceeds of criminal activities through the financial system. In November 1990, Hong Kong was invited to participate as an observer in FATF, and has, since December 1990, attended FATF meetings and played an active role in its deliberations. Hong Kong was admitted as a full member in March 1991.

2.4.2 The FATF has, among other things, put forward 40 Recommendations[1] which cover the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation against money laundering. The latest version of 40 Recommendations was released in June 2003. In October 2001, the FATF expanded its scope of work to cover matters relating to terrorist financing and promulgated Special Recommendations on Terrorist Financing[2] (further updated in October 2004). These two sets of Recommendations set out the international framework to detect, prevent and suppress money laundering and terrorist financing activities. As a member of the FATF, Hong Kong is obliged to follow the measures in the Recommendations.

2.4.3 To keep in line with the development of prevention of money laundering and terrorist financing standards in the financial sectors, the International Association of Insurance Supervisors ("IAIS") issued a Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism[3] in October 2004 which adapts the standards in the FATF Recommendations to the specific practices and features of the insurance business. The OCI's Guidance Note has taken into account the relevant measures in the FATF Recommendations and the IAIS Guidance Paper.

[1] The 40 Recommendations can be downloaded from FAFT website at ***http://www.fatf-gafi.org***

[2] The Special Recommendations on Terrorist Financing can be downloaded from FAFT website at ***http://www.fatf-gafi.org***

[3] The Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism can be downloaded from IAIS website at ***http://www.iaisweb.org***

3. LEGISLATION

3.1 The legislation concerning money laundering in Hong Kong

3.1.1 Legislation has been enacted in Hong Kong to address problems associated with the laundering of proceeds from drug trafficking and serious crimes. The Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) ("DTROP") 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. Under section 4 of DTROP, proceeds are not limited solely to the actual profits of drug sales or distribution, but may constitute any payments or other rewards received by a person at any time in connection with drug trafficking carried on by him or another, and property derived or realized therefrom.

3.1.2 The Organized and Serious Crimes Ordinance (Cap. 455) ("OSCO"), which was modelled on the DTROP, extends the money laundering offence to cover the proceeds of indictable offences in addition to drug trafficking.

3.1.3 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.

3.1.4 Sections 3 to 5 of the OSCO provide that the Secretary for Justice or an authorized officer, for the purpose of investigating an organized crime, may apply to the Court of First Instance for an order to require a person to provide information or produce material that reasonably appears to be relevant to the investigation. The Court may make an order that the person makes available the material to an authorized officer. An authorized officer may also apply for a search warrant under the OSCO. A person cannot refuse to furnish information or produce material under sections 3 or 4 of the OSCO on the ground of self-incrimination or breach of an obligation to secrecy or other restriction on the disclosure of information imposed by statute or other rules or regulations.

3.1.5 Authorized officer includes any police officer, any member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342); or any officer in the Joint Financial Intelligence Unit ("JFIU") which

was established and is operated jointly by the Police and the Customs and Excise Department.

3.1.6 Section 25(1) of DTROP and OSCO create 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.

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

3.1.8 Section 25A(1) of both Ordinances impose 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 as soon as it is reasonable for him to do so. Section 25A(7) of both Ordinances make it an offence for a person failing to make such disclosure. The offence carries a maximum penalty of a fine of HK$50,000 and imprisonment for 3 months.

3.1.9 It should be noted that section 25(4) of OSCO provides that references to an indictable offence in sections 25 and 25A of OSCO 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) of OSCO even if the conduct is not committed in Hong Kong, provided that it would constitute an indictable offence if it had occurred in Hong Kong.

3.1.10 Section 25A(2) of both Ordinances provide that if a person who has made the necessary disclosures 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.

3.1.11 Section 25A(3) of both Ordinances provide 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, insurance institutions need not fear breaching their duty of confidentiality owed to customers when making a disclosure under the two Ordinances.

3.1.12 Section 25A(4) of both Ordinances provide that a person who is in employment can make disclosure to the appropriate person in accordance with the procedures established by his employer for the making of such disclosure. To the employee, such disclosure has the effect of disclosing the knowledge or suspicion to an authorized officer as required under section 25A(1).

3.1.13 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 a fine of HK$500,000 and an imprisonment for 3 years.

3.1.14 Insurance institutions may receive restraint orders and charging orders on the property of a defendant of a drug trafficking offence or an offence specified in OSCO. These orders are issued under sections 10 and 11 of the DTROP or sections 15 and 16 of the OSCO. On service of these orders, an authorized officer may require a person to deliver as soon as practicable documents or information, in his possession or control which may assist the authorized officer to determine the value of the property. Failure to provide the documents or information is an offence under DTROP or OSCO. In addition, a person who knowingly deals in any realizable property in contravention of a restraint order or a charging order also commits an offence under DTROP or OSCO.

3.2 The legislation concerning terrorist financing in Hong Kong

3.2.1 The United Nations Security Council ("UNSC") has passed various resolutions to require sanctions against certain designated terrorists and terrorist organizations. In Hong Kong, regulations issued under the United Nations Sanctions Ordinance (Cap. 537) give effect to these UNSC resolutions. In particular, the United Nations Sanctions (Afghanistan) Regulation (Cap. 537K) and the United Nations Sanctions (Afghanistan) (Amendment) Regulation provide, 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.

3.2.2 In addition, the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) ("UNATMO") was enacted in July 2002 and was subsequently amended through the enactment of the United Nations (Anti-Terrorism Measures) (Amendment) Ordinance 2004 in July 2004[4]. The legislation implements the mandatory elements of the UNSC Resolution 1373. The latter aims at combating international terrorism on various fronts, including the introduction of measures against terrorist financing. The UNATMO also implements the most pressing elements of the FATF Special Recommendations.

3.2.3 The key terrorist financing provisions in the amended UNATMO 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 when necessary.

3.2.4 Section 7 of the amended UNATMO prohibits the supply or collection of funds to carry out terrorist acts, and section 8 of the amended UNATMO prohibits making funds (or financial) or related services available to terrorists or terrorist associates. Sections 6 and 13 of the amended UNATMO further permit terrorist property to be frozen and subsequently forfeited.

3.2.5 Section 12(1) of the amended UNATMO requires a person to report his knowledge or suspicion of terrorist property to an authorized officer (e.g. the JFIU). Failure to make a disclosure under this section constitutes an offence under section 14(5). The maximum penalty upon conviction of this offence is a fine of HK$50,000 and imprisonment for 3 months.

[4] A substantial part of this Amendment Ordinance has come into operation in January 2005.

3.2.6 The term “funds” includes funds mentioned in Schedule 1 to the amended UNATMO. It covers cash, cheques, claims on money, deposits with financial institutions or other entities, balances on accounts, securities and debt instruments (including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures, debenture stock and derivatives contracts), interest, dividends or other income on or value accruing from or generated by property, letters of credit, documents evidencing an interest in funds or financial resources, etc.

3.2.7 A list of terrorist or terrorist associate names is published in the Gazette from time to time pursuant to section 10 of the United Nations Sanctions (Afghanistan) Regulation and section 4 of the amended UNATMO. The published lists reflect designations made by the United Nations Committee that were established pursuant to UNSC Resolution 1267. The amended UNATMO provides that it shall be presumed, in the absence of evidence to the contrary, that a person specified in such a list is a terrorist or a terrorist associate (as the case may be).

3.2.8 Regarding the obligations under section 12(1) of the amended UNATMO to disclose knowledge or suspicion that property is terrorist property, section 12(2) of the amended UNATMO states that if a person who has made such a disclosure does any act in contravention of section 7 or 8 of the amended UNATMO either before or after such disclosure and the disclosure relates to that act, the person does not commit an offence if:

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

(b) the disclosure is made after he does that act, is made on his own initiative and is made as soon as it is practicable for him to make it.

3.2.9 Section 12(3) provides that a disclosure made under the amended UNATMO shall not be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, rule of conduct or other provision. The person making the disclosure shall not be liable in damages for any loss arising out of the disclosure or any act done or omitted to be done in relation to the property concerned in consequence of the disclosure.

3.2.10 Section 12(4) of the amended UNATMO provides that a person who is in employment can make disclosure to the appropriate person in accordance with the procedures established by his employer for the making of such disclosure. To the employee, such disclosure has the effect of disclosing the knowledge or suspicion to an authorized officer as required under section 12(1).

3.2.11 Sections 12A, 12B and 12C of the amended UNATMO provide that the Secretary for Justice or an authorized officer, for the purpose of investigating an offence under the Ordinance, may apply to the Court of First Instance for an order to require a person to provide information or produce material that reasonably appears to be relevant to the investigation. The Court may make an order that the person makes available the material to an authorized officer. An authorized officer may also apply for a search warrant under the amended UNATMO. A person cannot refuse to furnish information or produce material under section 12A or 12B of the amended UNATMO on the ground of breaching an obligation to secrecy or other restriction on the disclosure of information imposed by statute or other rules or regulations.

4. POLICIES AND PROCEDURES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

4.1 The senior management of an insurance institution should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness. The OCI expects that insurance institutions should have in place the following policies, procedures and controls:

(a) Insurance institutions should issue a clear statement of group policies in relation to money laundering and terrorist financing and communicate the group policies to all management and relevant staff whether in branches, departments or subsidiaries and be reviewed on a regular basis.

(b) Insurance institutions should develop instruction manuals setting out their procedures for:

- Customer acceptance
- Customer due diligence
- Record-keeping
- Recognition and reporting of suspicious transactions
- Staff screening and training

based on the guidance in Part II of this Guidance Note.

(c) Insurance institutions should comply with relevant legislations and seek actively to promote close co-operation with law enforcement authorities.

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

(e) Insurance institutions should regularly review the policies and procedures on money laundering and terrorist financing to ensure their effectiveness.

(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, insurance institutions should ensure that their overseas branches and subsidiaries are aware of the group policies concerning money laundering and terrorist financing and, where appropriate, have been instructed to report to the local reporting point for their suspicions.

PART II DETAILED GUIDELINES

5. CUSTOMER ACCEPTANCE

5.1 Prior to the establishment of a business relationship, insurance institutions should assess the characteristics of the required product, the purpose and nature of the business relationship and any other relevant factors in order to create and maintain a risk profile of the customer relationship. Based on this assessment, the insurance institution should decide whether or not to accept the business relationship.

5.2 Insurance institutions should develop customer acceptance policies and procedures that aim to identify the types of customers[5] and/or beneficial owners[6] that are likely to pose a higher than average risk of money laundering and terrorist financing. There should be clear internal guidelines on which level of management is able to approve a business relationship with such customers and/or beneficial owners. Decisions taken on establishing relationships with higher risk customers and/or beneficial owners should be taken by senior management.

5.3 In assessing the risk profile of a customer relationship, an insurance institution should consider the following factors[7]:

(a) nature of the insurance policy, which is susceptible to money laundering risk, such as single premium policies;

(b) frequency and scale of activities;

(c) the customer's and/or beneficial owner's nationality, citizenship and resident status (in the case of a corporate customer, the customer's place of incorporation), the place where the customer's and/or beneficial owner's business is established, the location of the counterparties with whom the customer and/or beneficial owner conducts business, and whether the customer and/or beneficial owner is otherwise connected with higher risk jurisdictions or jurisdictions which do not or insufficiently apply the FATF Recommendations (paragraph 6.6.6), or which are known to the insurance institution to be lack of proper standards in the prevention of money laundering

[5] For the purpose of this Guidance Note, the term "customer" refers to policy holder.

[6] For the purpose of this Guidance Note, the term "beneficial owner" refers to the owner/controller of the policy holder, i.e. the natural person(s) who ultimately owns or controls a policy holder/potential policy holder or the person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

[7] These are relevant factors that insurance institutions should consider in assessing the risk profile of their customers and/or beneficial owners. They, however, do not form part of the customer due diligence procedures (unless explicitly mentioned in this Guidance Note).

or customer due diligence process;

(d) background or profile of the customer and/or beneficial owner, such as being, or linked to, a politically exposed person (paragraph 6.6.5);

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

(f) for a corporate customer and/or beneficial owner, unduly complex structure of ownership for no good reason;

(g) means of payment as well as type of payment (cash, wire transfer, third party cheque without any apparent connection with the prospective customer and/or beneficial owner);

(h) the source of funds/wealth;

(i) the delivery mechanism, or distribution channel, used to sell the product (e.g. non face-to-face transactions (paragraph 6.6.4), business sold through insurance intermediaries (paragraph 6.8)); and

(j) any other information that may suggest that the customer and/or beneficial owner is of higher risk (e.g. knowledge that the customer and/or beneficial owner has been refused to enter a relationship by another financial institution).

5.4 Following the initial acceptance of the customer and/or beneficial owner, a pattern of account activity that does not fit in with the insurance institution's knowledge of the customer and/or beneficial owner may lead the insurance institution to reclassify the customer and/or beneficial owner as higher risk.

6. CUSTOMER DUE DILIGENCE

6.1 General principle

6.1.1 Insurance institutions should not keep anonymous accounts or accounts in obviously fictitious names. They should perform due diligence process for customers and/or beneficial owners and/or beneficiaries. The measures should comprise the following:

(a) identify the customer and/or beneficiary and verify the customer's and/or beneficiary's identity using reliable, independent source documents, data or information;

(b) ask and determine whether the customer is acting on behalf of another person for the purpose of identifying the insured and/or beneficial owner, and then take reasonable steps to obtain sufficient identification data to verify the identity of that other person, if applicable;

(c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner such that the insurance institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, insurance institutions should take reasonable measures to understand the ownership and control structure of the customer;

(d) obtain information on the purpose and intended nature of the business relationship between the customer and the insurance institution; and

(e) conduct on-going due diligence and scrutiny i.e. perform on-going scrutiny of the transactions and accounts throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the insurance institution's knowledge of the customers and/or beneficial owners, their businesses and risk profile, including, where necessary, identifying the source of funds.

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

6.1.3 The general rule is that customers and/or beneficial owners and/or beneficiaries are subject to the full range of customer due diligence measures. Insurance institutions should however determine the extent of such measures on a risk based approach depending on the type of customer and/or beneficial owner and/or beneficiary, business relationship or transaction (factors for deciding the risk profile are set out in paragraph 5.3). Enhanced due diligence is called for with respect to higher risk categories. Conversely, it is acceptable for insurance institutions to apply simplified due diligence for lower risk categories as outlined in paragraphs 6.1.4, 6.3.2 and 6.3.4. Specific customer due diligence requirements applicable to different types of customers are outlined in paragraphs 6.2 to 6.7.

6.1.4 In general, insurance institutions may apply simplified due diligence in respect of a corporate customer where there is no suspicion of money laundering and terrorist financing, and:

- the risk of money laundering and terrorist financing is assessed to be low; or
- there is adequate public disclosure in relation to the customers; or
- there are adequate checks and controls exist elsewhere in national systems.

6.1.5 The guiding principle of applying the risk based approach is that the insurance institutions should be able to justify that they have taken reasonable steps to satisfy themselves as to the true identity of their customers and/or beneficial owners and/or beneficiaries. These measures should be objectively reasonable in the eyes of a third party. In particular, where an insurance institution is satisfied as to any matter it should be able to justify its assessment to the OCI or any other relevant authority. Among other things, this would require the insurance institution to document its assessment and the reasons for it.

6.1.6 If claims, commissions, and other monies are to be paid to persons or companies other than the customers or beneficiaries, then the proposed recipients of these monies should also be the subjects of identification and verification.

6.1.7 Insurance institutions should pay special attention to all complex, unusual large transactions and all unusual patterns of

transactions which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. In this respect, "transactions" should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, premium payments, requests for changes in benefits, beneficiaries, duration, etc.

6.1.8 As to reinsurance, due to the nature of the business and the lack of a contractual relationship between the policy holder and the reinsurer, it is often impractical for the reinsurer to carry out verification of the policy holder and/or the beneficial owner and/or the beneficiary. Therefore, for reinsurance business, reinsurers should only have business with ceding insurers that are authorized and supervised by the OCI or an equivalent authority in a jurisdiction that is a FATF member or that applies standards of prevention of money laundering and terrorist financing equivalent to those of the FATF.

6.1.9 In principle, identification and verification of customers and beneficial owners should take place when the business relationship with those persons is established. This means that the customers and beneficial owners need to be identified and their identity verified before, or at the moment when, the insurance contract is concluded.

6.1.10 Insurance institutions may permit the identification of beneficiary to take place after having established the business relationship, provided that the money laundering risks and financing of terrorism risks are effectively managed. Notwithstanding the above, the verification of the beneficiary should occur at the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

6.1.11 Where a customer and/or beneficial owner is permitted to utilize the business relationship prior to verification, insurance institutions should be required to adopt risk management procedures concerning the conditions under which this may occur. These procedures should include measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

6.1.12 Where the insurance institution is unable to satisfy itself on the identity of the customer and/or beneficial owner, it should not

commence business relationship or perform the transaction and should consider making a suspicious transaction report.

6.1.13 Where the insurance institution has already commenced the business relationship and is unable to satisfy itself on the identity of the customer and/or beneficial owner, it should consider terminating the business relationship, if possible, and making a suspicious transaction report. The return of premiums should be subject to any request from the JFIU to freeze the relevant premiums.

6.2 Individuals

6.2.1 Insurance institutions should institute effective procedures for obtaining satisfactory evidence of the identity of individual customers and/or beneficial owners and/or beneficiaries including obtaining information about:

(a) true name and/or name(s) used;
(b) identity card/passport number;
(c) current permanent address;
(d) date of birth;
(e) nationality[8]; and
(f) occupation/business[9].

6.2.2 Identification documents such as current valid passports or identity cards should be produced as identity proof. For Hong Kong residents, the prime source of identification will be the identity cards. File copies of identification documents should be retained.

6.2.3 In principle, copies of the identification documents of individual customers should be collected before, or at the moment when, the insurance contract is concluded. However, as far as an individual beneficiary is concerned, copy of his/her identification document should only be collected at the time of payout or the time when he/she intends to exercise vested rights under the policy.

6.2.4 Having considered the difficulty for insurance institutions to obtain copies of the identification documents of individual customers when the sales process occurs outside the office, insurance institutions may obtain and keep copies of the identification documents after having established the business

[8] For an individual who is a holder of Hong Kong Permanent Identity Card, the verification of nationality is not mandatory.

[9] Information about occupation/business is a relevant piece of information about a customer and/or beneficial owner and/or beneficiary but does not form part of the identification information requiring verification.

relationship provided that the money laundering risks and financing of terrorism risks are effectively managed. In all such circumstances, copies of identification documents of individual customers should be obtained and copied for retention as soon as possible after the insurance contract is concluded and, in any cases, no later than the time of payout or the time when the beneficiary intends to exercise vested rights under the policy. Paragraph 6.1.11 provides guidance for adopting the risk management procedures.

6.2.5 It must be appreciated that no form of identification can be fully guaranteed as genuine or representing correct identity. If there is doubt about whether an identification document is genuine, contact should be made with the Immigration Department or the relevant consulates in Hong Kong to ascertain whether the details on the document are correct.

6.2.6 Insurance institutions should check the address [10] of the applicant by appropriate means, e.g. by requesting sight of a recent utility or rates bill or a recent bank statement.

6.2.7 Insurance institutions should also identify the source of funds of customers and/or beneficial owners if the customers and/or beneficial owners are assessed to be of higher risk based on the factors set out in paragraph 5.3.

6.3 Corporations

6.3.1 The following documents or information should be obtained in respect of corporate customers and/or beneficial owners and/or beneficiaries which are registered in Hong Kong, not being financial institutions as mentioned in paragraph 6.3.4 (comparable documents, preferably certified by qualified persons such as lawyers or accountants in the country of registration, should be obtained for those customers and/or beneficial owners and/or beneficiaries which are not registered in Hong Kong, not being financial institutions as mentioned in paragraph 6.3.4):

(a) copies of certificate of incorporation and business registration certificate;

[10] Insurance institutions should, however, use a common sense approach to handle cases where the customers and/or beneficial owners (e.g. students and housewives) are unable to provide address proof. Apart from the method suggested in paragraph 6.2.5, insurance institutions may use other appropriate means, such as home visits, to verify the residential address of a customer and/or beneficial owner.

(b) copies of memorandum and articles of association (if insurance institution considers necessary having regard to the risk of the particular transaction);

(c) copy of resolution of the board of directors to enter into insurance contracts or other evidence conferring authority to those persons who will operate the insurance policy as well as the identification information of those persons;

(d) a search of the file at Companies Registry, if there is a suspicion about the legitimacy of the legal entity.

6.3.2 It will generally be sufficient for an insurance institution to adopt simplified due diligence in respect of a corporate customer and/or beneficial owner and/or beneficiary by obtaining the documents specified in paragraph 6.3.1 if the risk of money laundering and terrorist financing is assessed to be low. Some examples of lower risk corporate customers and/or beneficial owners and/or beneficiaries are:

(a) the company is listed in Hong Kong or on a recognized stock exchange (Annex 1) (or is a subsidiary of such listed company);

(b) the company is a state-owned enterprise in a jurisdiction where the risk of money laundering is assessed to be low and where the insurance institution has no doubt as regards the ownership of the enterprise;

(c) the company acquires an insurance policy for pension schemes which does not have surrender clause and the policy cannot be used as collateral; or

(d) the company acquires a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

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

6.3.4 Where a corporate customer and/or beneficial owner and/or beneficiary is a financial institution which is authorized and supervised by the OCI, HKMA, the Securities and Futures

Commission of Hong Kong or an equivalent authority in a jurisdiction that is a FATF member or that applies standards of prevention of money laundering and terrorist financing equivalent to those of the FATF, it will generally be sufficient for an insurance institution 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.

6.3.5 In relation to a corporate customer and/or beneficial owner and/or beneficiary which does not fall into the descriptions of paragraphs 6.3.2 and 6.3.4, an insurance institution should look behind the company 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 6.3.1, the insurance institution should verify the identity of all the principal shareholders (a person entitled to exercise or control the exercise of 10% or more of the voting rights of a company), at least two directors[11] (including the managing director) of the company and all authorized signatories designated to sign insurance contracts. The insurance institution should also identify the source of funds. Besides, a search of the file at Companies Registry should be performed.

6.3.6 Where a corporate customer which does not fall into the descriptions of paragraphs 6.3.2 and 6.3.4; and which is a non-listed company and has a number of layers of companies in its ownership structure, the insurance institution should follow the chain of ownership to the individuals who are the ultimate principal beneficial owners of the customer of the insurance institution and to verify the identity of these individuals. The insurance institution, however, is not required to check the details of each of the intermediate companies (including their directors) in the ownership chain.

6.3.7 An insurance institution should understand the ownership structure of non-listed corporate customers and determine the source of funds. An unduly complex ownership structure for no good reason is a risk factor to be taken into account (paragraph 5.3 (f)).

6.3.8 An insurance institution should exercise special care in initiating business transactions with companies that have

[11] In case of one-director companies, insurance institutions are only required to verify the identity of that director.

nominee shareholders. Satisfactory evidence of the identity of beneficial owners of such companies should be obtained.

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

6.3.10 Where it is not practical to immobilize the bearer shares, insurance institutions should obtain a declaration from each 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 insurance institution immediately if the shares are sold, assigned or transferred.

6.4 Unincorporated businesses

6.4.1 In the case of partnerships and other unincorporated businesses whose partners are not known to the insurance institution, satisfactory evidence should be obtained of the identity of at least two partners and all authorized signatories designated to sign insurance contracts in line with the requirements for individual applicants in paragraph 6.2. 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.

6.5 Trust accounts

6.5.1 Where trusts or similar arrangements are used, particular care should be taken in understanding the substance and form of the entity. Accordingly, insurance institutions should always establish, by confirmation from an applicant for insurance policy, whether the applicant is acting on behalf of another person as trustee, nominee or agent. Where the customer is a trust, the insurance institution should verify the identity of the trustees, any other person exercising effective control over the trust property, the settlors[12] and the beneficiaries[13]. Should it

[12] When the verification of the identity of the settlor is not possible, insurance institutions may accept a declaration from the trustee or other contractual party to confirm the link or relationship with the settlor.

[13] Insurance institutions should try as far as possible to obtain information about the identity of beneficiaries. A broad description of the beneficiaries such as family members of an individual may be accepted. Where the identity of beneficiaries has not previously been verified, insurance institutions should undertake

not be possible to verify the identity of the beneficiaries when the policy is taken out, verification of the beneficiaries should be carried out prior to any payments being made to them.

6.5.2 As with other types of customers, an insurance institution 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 factors such as the nature and complexity of the trust arrangement.

6.6 Higher risk customers

6.6.1 Insurance institutions should apply an enhanced due diligence in respect of higher risk customers and/or beneficial owners and/or beneficiaries. Some examples of higher risk customers and/or beneficial owners and/or beneficiaries are:

- customers and/or beneficial owners are assessed to be of higher risk based on the factors set out in paragraph 5.3;
- customers of non-face-to-face transactions;
- politically exposed persons as well as persons or companies clearly related to them; or
- customers and/or beneficial owners and/or beneficiaries in connection with jurisdictions which do not or insufficiently apply the FATF Recommendations.

6.6.2 Examples of additional measures applicable to enhanced due diligence are:

- obtaining senior management approval for establishing business relationship;
- obtaining comprehensive customer profile information e.g. purpose and reasons for entering the insurance contract, business or employment background, source of funds and wealth;
- assigning a designated staff to serve the customer who bears the responsibility for customer due diligence and on-

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, insurance institutions should adopt a risk based approach which should take into account the amount(s) involved and any suspicion of money laundering or terrorist financing. A decision not to undertake verification should be approved by senior management.

going monitoring to identify any unusual or suspicious transactions on a timely basis;

- requisition of additional documents to complement those which are otherwise required; and

- certification by appropriate authorities and professionals of documents presented.

6.6.3 Apart from the above general additional measures, specific additional measures are also applicable to the customers of non-face-to-face transactions (paragraph 6.6.4); customers who are classified as politically exposed persons (paragraph 6.6.5); and customers in connection with jurisdictions which do not or insufficiently apply the FATF Recommendations (paragraph 6.6.6).

6.6.4 New or developing technologies: Customers of non-face-to-face transactions

6.6.4.1 An insurance institution 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 insurance institution itself or by an intermediary that can be relied upon to conduct proper customer due diligence (paragraph 6.8).

6.6.4.2 This is particularly important for higher risk customers. In this case, the insurance institution should ask the customer to make himself available for a face-to-face interview.

6.6.4.3 New or developing technologies that might favour anonymity can be used to market insurance products. E-commerce or sales through internet is an example. Where face-to-face interview is not conducted, for example where the account is opened via the internet, an insurance institution should apply equally effective customer identification procedures and on-going monitoring standards as for face-to-face customers.

6.6.4.4 Examples of specific measures that insurance institutions can use to mitigate the risk posed by such customers of non-face-to-face transactions include:

(a) certification of identity documents presented by suitable certifiers;

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

(c) completion of on-line questionnaires for new 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 insurance institution;

(e) third party introduction through an intermediary which satisfies the criteria in paragraph 6.8;

(f) requiring the payment for insurance premiums through an account in the customer's name with a bank;

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

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

6.6.5 Politically exposed persons ("PEPs")

6.6.5.1 PEPs are defined as individuals who are or have been entrusted with prominent public functions outside Hong Kong, such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. The concern is that there is a possibility, especially in jurisdictions where corruption is widespread, that such PEPs may abuse their public powers for their own illicit enrichment through the receipt of bribes etc.

6.6.5.2 Business relationships with PEPs as well as persons or companies clearly related to them (i.e. families, close associates etc.) expose an insurance institution to

particularly significant reputation or legal risks. There should be on-going enhanced due diligence in respect of such PEPs and people and companies that are clearly related to them. The following CDD measures applicable to PEPs also apply to persons or companies that are clearly related to them.

6.6.5.3 An insurance institution should gather sufficient information from a new customer, and check publicly available information to establish whether or not the customer is a PEP. An insurance institution 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.

6.6.5.4 An insurance institution should also ascertain the source of funds before accepting a PEP as customer. The decision to establish business relationship with a PEP should be taken at a senior management level. Where a customer has been accepted and the customer and/or beneficial owner and/or beneficiary is subsequently found to be or become a PEP, an insurance institution should obtain senior management approval to continue the business relationship.

6.6.5.5 Risk factors that an insurance institution should consider in handling a business relationship (or potential relationship) with a PEP include:

(a) any particular concern over the jurisdiction 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) unexpected 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.

6.6.5.6 Insurance institutions 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 jurisdictions that are higher risk from a corruption point of view (reference can be made to publicly available information such as the Corruption Perceptions Index).

6.6.5.7 While paragraph 6.6.5.1 defines PEPs as individuals who hold prominent public functions outside Hong Kong, insurance institutions are encouraged to extend the relevant requirements on PEPs to individuals who hold prominent public functions in Hong Kong.

6.6.6 Jurisdictions which do not or insufficiently apply the FATF Recommendations

6.6.6.1 An insurance institution should apply Recommendation 21 of the FATF's 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."

6.6.6.2 Extra care should therefore be exercised by an insurance institution in respect of customers and/or beneficial owners and/or beneficiaries connected with jurisdictions which do not or insufficiently apply the FATF Recommendations or otherwise pose a higher risk to an insurance institution. In addition to ascertaining and documenting the business rationale for applying for insurance services as required under paragraph 6.1.1 (d)

above, an insurance institution should be fully satisfied with the legitimacy of the source of funds of such customers.

6.6.6.3 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 insurance institution 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 insurance institution 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 anti-money laundering and counter-terrorist financing 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 organizations 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, supranational or international bodies such as the International Monetary Fund ("IMF"), and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organizations. 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.

6.6.6.4 In assessing whether or not a jurisdiction (other than FATF members as shown in Annex 1) sufficiently applies FATF standards in combating money laundering and terrorist financing and meets the criteria for an equivalent jurisdiction, insurance institutions should:

(a) carry out their own jurisdiction assessment of the standards of prevention of money laundering and terrorist financing. This could be based on the insurance institutions' knowledge and experience of the jurisdiction concerned or from market intelligence. The higher the risk, the more stringent the due diligence measures that should be applied when undertaking business with a customer from the jurisdiction concerned; and

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

(c) maintain an appropriate degree of on-going vigilance concerning money laundering risks and to take into account information that is reasonably available to them about the standards of anti-money laundering systems and controls that operate in the country with which any of their customers are associated.

6.6.6.5 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 OCI 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 insurance institution should apply the counter-measures determined by the OCI from time to time.

6.6.6.6 An insurance institution 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.

6.6.6.7 If an insurance institution incorporated in Hong Kong has operating units in such jurisdictions, care and on-going vigilance should be taken to ensure that effective controls on prevention of money laundering and terrorist financing are implemented in these units. In particular, the insurance institution 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 insurance institution should consider withdrawing from such jurisdictions.

6.7 On-going due diligence on existing customers and/or beneficial owners

6.7.1 Insurance institutions should take reasonable steps to ensure that the records of existing customers remain up-to-date and relevant. To achieve this, insurance institutions should perform on-going due diligence on the existing business relationship to consider re-classifying a customer as high or low risk. In general, the insurance institutions should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. They should assess if the change/transaction does not fit the profile of the customer and/or beneficial owner or is for some other reason unusual or suspicious. Enhanced due diligence is required with respect to higher risk categories. The customer due diligence programme should be established in such a way that insurance institutions are able to adequately gather and analyze information.

6.7.2 Examples of transactions or trigger events after establishment of the contract that require customer due diligence are:

(a) there is change in beneficiaries (for instance, to include non-family members, request for payments to persons other than beneficiaries);

(b) there is significant increase in the amount of sum insured or premium payment that appears unusual in the light of the income of the policy holder;

(c) there is use of cash and/or payment of large single premiums;

(d) there is payment/surrender by a wire transfer from/to foreign parties;

(e) there is payment by banking instruments which allow anonymity of the transaction;

(f) there is change of address and/or place of residence of the policy holder and/or beneficial owner;

(g) there are lump sum top-ups to an existing life insurance contract;

(h) there are lump sum contributions to personal pension contracts;

(i) there are requests for prepayment of benefits;

(j) there is use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution);

(k) there is change of the type of benefit (for instance, change of type of payment from an annuity into a lump sum payment);

(l) there is early surrender of the policy or change of the duration (where this causes penalties or loss of tax relief);

(m) there is request for payment of benefits at the maturity date;

(n) the insurance institution is aware that it lacks sufficient information about the customer and/or beneficial owner; or

(o) there is a suspicion of money laundering and terrorist financing.

6.7.3 Occurrence of these transactions and events does not imply that (full) customer due diligence needs to be applied. If identification and verification have already been performed, the insurance institution is entitled to rely on this unless doubts arise about the veracity of that information it holds. As an example, doubts might arise if benefits from one insurance policy are used to fund the premium payments of the insurance policy of another unrelated person.

6.7.4 Even when there is no specific trigger event, an insurance institution should consider whether to require additional information in line with current standards from those existing customers and/or beneficial owners that are considered to be of higher risk. In doing so, the insurance institution should take into account the factors mentioned in paragraph 5.3.

6.8 Reliance on insurance intermediaries[14] for customer due diligence

6.8.1 Insurers, appointed insurance agents and authorized insurance brokers all have the responsibility to comply with the requirements relating to customer due diligence and record keeping as specified in paragraphs 6 and 7 of this Guidance Note. However, insurance intermediaries, that is agents and brokers, are usually the first line of contacts with the customer, before the customer is known, introduced or referred to an insurer. These insurance intermediaries may actually obtain the appropriate verification evidence in respect of the customer. To avoid duplication of efforts and unnecessary inconvenience to the customer, the insurer may rely on these insurance intermediaries to carry out part or all of the customer due diligence requirements.

6.8.2 For insurers which rely on insurance intermediaries to carry out part or all of the customer due diligence requirements, they must understand their related AML/CFT obligations in respect to these requirements. The ultimate responsibility for customer

[14] Insurance intermediaries refer to appointed insurance agents or authorized insurance brokers carrying on or advising on long term insurance business in Hong Kong.

identification and verification remains with the insurer relying on insurance intermediaries. The insurer concerned should therefore determine whether the intermediary in question possesses an acceptable level of reliability. In this regard, the following criteria should be used:

(a) the customer due diligence procedures of the insurance intermediary should be as rigorous as those which the insurer would have conducted itself for the customer and/or beneficial owner and/or beneficiary in accordance with paragraph 6 of this Guidance Note; and

(b) the insurer must satisfy itself as to the reliability of the systems put in place by the insurance intermediary to verify the identities of the customer and/or beneficial owner and/or beneficiary.

6.8.3 The insurer is expected to conduct periodic reviews to ensure that an insurance agent 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 insurance agent and sample checks of the due diligence conducted.

6.8.4 Where reliance on insurance intermediaries for customer due diligence is permitted, the insurer should immediately obtain the necessary information concerning the relevant identification data and other documentation pertaining to the identity of the customer and/or beneficial owner and/or beneficiary from the insurance intermediary. The insurance intermediary should submit such information to the insurer upon request without delay.

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

6.8.6 The insurer should undertake and complete its own verification of the customer and/or beneficial owner and/or beneficiary if it has any doubts about the ability of the insurance intermediary to undertake appropriate due diligence.

7. RECORD KEEPING

7.1 Requirements of the investigating authorities

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

7.1.2 The investigating authorities need to ensure a satisfactory audit trail for suspected drug related or other laundered money and to be able to establish a financial profile of the suspected account.

7.1.3 An important objective of record keeping is to ensure that insurance institutions can, at all stages in a transaction, retrieve relevant information to the extent that it is available without undue delay.

7.2 Retention of records

7.2.1 Insurance institutions should keep records on the risk profile of each customer and/or beneficial owner and/or beneficiary and the data obtained through the customer due diligence process (e.g. name, address, the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction), the copies of official identification documents (such as passports, identity cards or similar documents) and the account files and business correspondence, for at least six years after the end of the business relationship.

7.2.2 Insurance institutions should maintain, for at least six years after the business relationship has ended, all necessary records on transactions, both domestic and international, and be able to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amount and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

7.2.3 Insurance institutions should ensure that documents, data or information collected under the customer due diligence process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

7.2.4 Insurance institutions should ensure that they have in place adequate procedures:

(a) to provide initial proposal documentation including, where applicable, the customer financial assessment, analysis of needs, details of the payment method, illustration of benefits, and copy of documentation in support of verification by the insurance institutions;

(b) to retain all records associated with the maintenance of the contract post sale, up to and including maturity of the contract; and

(c) to provide details of the maturity processing and/or claim settlement which will include completed "discharge documentation".

7.2.5 Retention may be by way of original documents, stored on microfiche, or in computerized form provided that such forms are accepted as evidence under sections 20 to 22 of the Evidence Ordinance (Cap. 8). In situation 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 AND REPORTING OF SUSPICIOUS TRANSACTIONS

8.1 Recognition of suspicious transactions

8.1.1 In order to satisfy an insurance institution's legal and regulatory obligations, it needs to have systems to enable it to identify and report suspicious transactions. In this regard, insurance institutions are encouraged to adopt the "SAFE" approach as recommended by the JFIU. Details of the "SAFE" approach are set out in Annex 2.

8.1.2 It is not enough to rely simply on the initiative of front-line staff to make ad hoc reports. An insurance institution 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.

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

8.1.4 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.

8.1.5 To facilitate the identification of suspicious transactions, indicators of suspicious transactions are given in Annex 3 and examples of money laundering schemes involving life insurance industry are given in Annex 4. The indicators are not intended to be exhaustive and are for reference only. Identification of any of the types of transactions listed in Annex 3 should prompt further investigation and be a catalyst towards making at least initial enquiries about the source of funds.

8.1.6 In relation to terrorist financing, the FATF issued in April 2002 a Guidance for Financial Institutions in Detecting

Terrorist Financing[15]. 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 3 of the document contains a series of characteristics of financial transactions that have been linked to terrorist activity in the past. An insurance institution should acquaint itself with the FATF paper.

8.1.7 An insurance institution should maintain a database of names and particulars of terrorist suspects which consolidates the various lists that have been made known to it. Alternatively, an insurance institution may make arrangements to secure access to such a database maintained by third party service providers.

8.1.8 Such database should, in particular, include the lists published in the Gazette[16] under the relevant legislation and those designated under the US President's Executive Order 13224[17]. 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.

8.1.9 An insurance institution should check the names of existing customers and/or beneficial owners and/or beneficiaries as well as new applicants for business against the names in the database. It should be particularly alert for suspicious remittances and should bear in mind the role which non-profit organizations 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.

8.2 Reporting of suspicious transactions

8.2.1 The reception point for disclosures under the DTROP, the OSCO and the UNATMO is the JFIU, which is operated jointly by the Police and the Customs and Excise Department.

8.2.2 In addition to acting as the point for receipt of disclosures made by any organization or individual, the JFIU also acts as

[15] The Guidance for Financial Institutions in Detecting Terrorist Financing can be downloaded from FATF website at ***http://www.fatf-gafi.org/dataoecd/39/21/34033955.pdf***

[16] The Gazette can be downloaded from the website of the Government Logistics Department at ***http://www.gld.gov.hk/cgi-bin/gld/egazette/index.cgi?lang=e&agree=0***

[17] Lists designated under the US President's Executive Order 13224 can be downloaded from the United States Department of the Treasury website at ***http://www.ustreas.gov/offices/enforcement/ofac/programs/terror/terror.pdf***

domestic and international advisors on money laundering and terrorist financing generally and offers practical guidance and assistance to the financial sector on the subject of money laundering and terrorist financing.

8.2.3 The obligation to report is on the individual who becomes suspicious of a money laundering or a terrorist financing transaction. Each insurance institution should appoint a designated officer ("compliance officer") at the management level who should be responsible for reporting to the JFIU where necessary in accordance with the relevant legislation and to whom all internal reports should be made.

8.2.4 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 insurance institution's MIS as well as ad hoc reports made by front-line staff. Depending on the organization structure of the insurance institutions, the specific task of reviewing reports may be delegated to other staff but the compliance officer should maintain oversight of the review process.

8.2.5 Where an employee of an insurance institution becomes suspicious of a customer and/or beneficial owner and/or beneficiary, transaction or property, he must promptly report to the compliance officer.

8.2.6 The compliance officer should form a considered view on whether unusual or suspicious transactions should be promptly 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 and/or beneficial owner and/or beneficiary in question should not necessarily preclude the making of a fresh report if new suspicions are aroused.

8.2.7 The compliance officer should keep a register of all reports made to the JFIU and all reports made to him by employees. The compliance officer should provide employees with a written acknowledgement of reports made to him, which will

form part of the evidence that these reports were made in compliance with the internal procedures.

8.2.8 The compliance officer should have the responsibility for checking on an on-going basis that the insurance institution has policies and procedures to ensure compliance with legal and regulatory requirements and of testing such compliance.

8.2.9 It follows from this that the insurance institution should ensure that the compliance officer is of sufficient status within the organization, and has adequate resources, to enable him to perform his functions.

8.2.10 It is anticipated that an insurance agent or insurance broker who considers funds offered in settlement of a contract to be suspicious will share that suspicion with his insurer, in addition to reporting it directly to the JFIU. He could inform his insurer either at the time when the disclosure is made to the JFIU or when the documentation is passed to the insurer for processing.

8.2.11 Internal audit also has an important role to play in independently evaluating on a periodic basis an insurance institution's policies and procedures in combating money laundering and terrorist financing. 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 and terrorist financing 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. It is of importance that the auditor has direct access and reports directly to the management and the board of directors.

8.2.12 The use of a standard format for reporting (or adaptation of the format) is encouraged (Annex 5). In the event that urgent disclosure is required, an initial notification should be made by telephone. The contact details of the JFIU are at Annex 6.

8.2.13 The JFIU will acknowledge receipt of any disclosure made. 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, or section 12(2) of

the UNATMO. An example of such a letter is shown at Annex 7 to this Guidance Note.

8.2.14 Insurance institutions should refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have informed the JFIU which consents to the institutions 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 or terrorist financing operation, institutions may carry out the transactions and notify the JFIU on their own initiative and as soon as it is reasonable for them to do so.

8.2.15 Access to the disclosed information is restricted to financial investigating officers within the Police and the Customs and Excise Department. In the event of a prosecution, production orders will be obtained to produce the material for the Court. Section 26 of the DTROP and the OSCO place strict restrictions on revealing the identity of the person making disclosure under section 25A.

8.2.16 Whilst there are no statutory requirements to provide feedback arising from investigations, the Police and the Customs and Excise Department recognize the importance of having effective feedback procedures in place. The JFIU may, on request, provide to a disclosing institution a status report on the disclosure.

8.2.17 Enhancing and maintaining the integrity of the relationship which has been established between law enforcement agencies and insurance institutions is considered to be of paramount importance.

9. STAFF SCREENING AND TRAINING

9.1 Screening

9.1.1 Insurance institutions should identify the key positions within their organizations with respect to anti-money laundering and combat of terrorist financing and should develop the following internal procedures for assessing whether employees taking up the key positions meet fit and proper requirements and are of high standards:

(a) verification of the identity of the person involved; and

(b) verification as to whether the information and references provided by the employee are correct and complete.

9.1.2 Insurance institutions should keep records on the identification data obtained from their employees mentioned in paragraph 9.1.1. The records should demonstrate the due diligence performed in relation to the fit and proper requirements.

9.2 Training

9.2.1 Staff must be aware of their own personal obligations under the DTROP, the OSCO and the UNATMO and that they can be personally liable for failing to report information to the authorities. They are advised to read the relevant sections of the DTROP, the OSCO and the UNATMO. They must be encouraged to co-operate fully with the law enforcement agencies and to provide prompt notice of suspicious transactions. They should be advised to report suspicious transactions to their institution's compliance officer if they do not know precisely what the underlying criminal activity is or whether illegal activities have occurred.

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

9.2.3 Timing and content of training packages for various sectors of staff will need to be adapted by individual insurance 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 and terrorist financing, and the subsequent need for identifying and reporting of any suspicious transactions to the appropriate designated point, 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 importance placed on the reporting of suspicions by the insurance institution, that there is a legal requirement to report, and that there is a personal statutory obligation in this respect.

(b) Sales/Advisory staff

Members of staff who are dealing directly with the public (whether as members of staff, agents or brokers) are the first point of contact with those who may commit money laundering or terrorist financing offence and the efforts of such staff are therefore vital to the strategy in the fight against money laundering and terrorist financing. They should be made aware of their legal responsibilities, including the insurance institution's reporting system for such transactions. Training should be provided on areas 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 insurance institution's policy for dealing with non-regular customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

(c) Processing staff

Those members of staff who receive completed proposals and cheques for payment of the single premium contribution must receive appropriate training in the processing and verification procedures. The identification of the proposer and the matching against the cheque received in settlement are, for instance, key processes. Such staff should be aware that the offer of suspicious funds accompanying a request to undertake an insurance contract may need to be reported to the relevant authorities irrespective of whether or not the funds are accepted or the proposal proceeded with. Staff must know what procedures to follow.

(d) Management

A higher level of instruction covering all aspects of policies and procedures on prevention of money laundering and terrorist financing should be provided to those with the responsibility for supervising or managing staff and for auditing the system. The training will include their responsibility regarding the relevant policies and procedures, the offences and penalties arising from the DTROP, the OSCO and the UNATMO, internal reporting procedures and the requirements for verification and record keeping.

(e) Compliance officers

The compliance officers should receive in-depth training concerning all aspects of relevant legislation, guidances and policies and procedures on the prevention of money laundering and terrorist financing.

(f) 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. It is suggested that this might be best achieved by a twelve or six-monthly review of training or, alternatively, a review of the instructions for recognizing and reporting suspected money laundering or terrorist financing transactions.

RECOGNIZED STOCK EXCHANGE

Stock exchange of a country which is a member of FATF or a specified stock exchange as defined under the Securities and Futures Ordinance (Cap. 571) (but excluding exchanges in jurisdictions which do not or insufficiently apply the FATF Recommendations)

FATF members

Argentina
Australia
Austria
Belgium
Brazil
Canada
China
Denmark
Finland
France
Germany
Greece
Hong Kong, China
Iceland
India
Ireland
Italy
Japan
Luxembourg
Mexico
Kingdom of the Netherlands
New Zealand
Norway
Portugal
Republic of Korea
Russian Federation
Singapore
South Africa
Spain
Sweden
Switzerland
Turkey
United Kingdom
United States

Specified stock exchanges in non-FATF countries

Kuala Lumpur Stock Exchange
Stock Exchange of Thailand
Philippine Stock Exchange, Inc.

"SAFE" APPROACH RECOMMENDED BY THE JOINT FINANCIAL INTELLIGENCE UNIT

The "SAFE" Approach is an effective systemic approach to identify suspicious financial activity which involves the following four steps:

(a) Step one: **S**creen the account for suspicious indicators: Recognition of a suspicious activity indicator or indicators
(b) Step two: **A**sk the customer appropriate questions
(c) Step three: **F**ind out the customer's records: Review of information already known when deciding if the apparently suspicious activity is to be expected
(d) Step four: **E**valuate all the above information: Is the transaction suspicious?

Examination of the Suspicious Transactions Reporting ("STR") received by the JFIU reveals that many reporting institutions do not use the system outlined above. Commonly, institutions make a STR merely because a suspicious activity indicator has been recognized, i.e. only step one of the systemic approach is followed, steps two, three and four are not followed. This failure to use the systemic approach leads to a lower quality of STRs.

Each of the four steps of the systemic approach to suspicious activity identification is discussed in more detail in the following paragraphs. Insurance institutions should consider carefully the specific nature of their business, organizational structure, type of customer and transaction, etc. when designing their own systems for implementing the respective steps.

Step one: **S**creen the account for suspicious indicators: Recognition of a suspicious activity indicator or indicators

The recognition of an indicator, or better still indicators, of suspicious financial activity is the first step in the suspicious activity identification system. A list of suspicious activity indicators commonly seen within the insurance sector is shown at Annex 3.

Insurance institutions can use different methods in the recognition of suspicious activity indicators. The measures summarized below are recognized as contributing towards an effective overall approach to suspicious activity identification.

(a) Train and maintain awareness levels of all staff in suspicious activity identification.

This approach is most effective in situations in which staff have face-to-face contact with a customer who carries out a particular transaction which displays suspicious activity indicators. However,

this approach is much less effective in situations in which either, there is no face-to-face contact between customer and staff, or the customer deals with different staff to carry out a series of transactions which are not suspicious if considered individually.

(b) Identification of areas in which staff/customer face-to-face contact is lacking (e.g. sales through internet) and use of additional methods for suspicious activity identification in these areas.

(c) Use of a computer programme to identify accounts showing activity which fulfils predetermined criteria based on commonly seen money laundering methods.

(d) Insurance institutions' internal inspection system to include inspection of STR.

(e) Identification of "High Risk" customers, i.e. customers of the type which are commonly high risk in nature, e.g. PEP. Greater attention is paid to monitoring of the activity of these customers for suspicious transactions.

(f) Flagging of customers of special interest on the computer. Staff carrying out future transactions will notice the "flag" on their computer screens and pay extra attention to the transactions conducted by the customer. Customers to be flagged are those in respect of which a suspicious transaction report has been made and/or customers of high risk nature.

A problem with flagging is that staff who come across a large transaction involving a flagged customer may tend to make a report to the compliance officer whether or not the transaction is suspicious. This has the effect of overburdening compliance officers with low quality reports. Flagging may also lead to staff believing that if a customer is not flagged it is not suspicious. Staff must be educated on the proper usage of flagging if it is to work properly.

(g) Adopt more stringent policies in respect of customers who are expected to pay in large amount of cash or to purchase single premium policies, e.g. request customers for the expected nature of transactions and source of funds when establishing business relationship.

Step two: **A**sk the customer appropriate questions

If staff carry out a transaction or transactions for a customer bearing one or more suspicious activity indicators, they should question the customer on the reason for conducting the transaction(s) and the identity of the source

and ultimate beneficiary of the money being transacted. Staff should consider whether the customer's story amounts to a reasonable and legitimate explanation of the financial activity observed. If not, then the customer's activity should be regarded as suspicious and a suspicious transaction report should be made to the JFIU.

On occasions staff of insurance institutions may be reluctant to ask questions of the type mentioned above. Grounds for this reluctance are that the customer may realize that he, or she, is suspected of illegal activity, or regards such questions as none of the questioner's business. In either scenario the customer may be offended or become defensive and uncooperative, or even take his, or her, business elsewhere. This is a genuine concern but can be overcome by staff asking questions which are apparently in furtherance of promoting the services of the insurance institution or satisfying customer needs, but which will solicit replies to the questions above without putting the customer on his, or her, guard.

Appropriate questions to ask in order to obtain an explanation of the reason for conducting a transaction bearing suspicious activity indicators will depend upon the circumstances of the financial activity observed. For example, if a customer wishes to make a large cash transaction then staff can ask the customer the reason for using cash on the grounds that the staff may be able to offer advice on a more secure method to perform the transaction.

Persons engaged in legitimate business generally have no objection to, or hesitation in answering such questions. Persons involved in illegal activity are more likely to refuse to answer, give only a partial explanation or give an explanation which is unlikely to be true.

If a customer is unwilling, or refuses, to answer questions or gives replies which staff suspect are incorrect or untrue, this may be taken as a further indication of the suspicious nature of the financial activity.

Step three: **F**ind out the customer's records: Review of information already known when deciding if the apparently suspicious activity is to be expected

The third stage in the systemic approach to suspicious activity identification is to review the information already known to the insurance institution about the customer and his, or her, previous financial activity and consider this information to decide if the apparently suspicious activity is to be expected from the customer. This stage is commonly known as the "know your customer principle".

Insurance institutions hold various pieces of information on their customers which can be useful when considering if the customers'

financial activity is to be expected or is unusual. Examples of some of these information items and the conclusions which may be drawn from them are listed below:

(a) The customers' occupation. Certain occupations imply the customer is a low wage earner e.g. driver, hawker, waiter, student. The purchase of insurance policies with large transaction amounts from such customers would not therefore be expected.

(b) The customers' residential address. A residential address in low cost housing, e.g. public housing, may be indicative of a low wage earner.

Step four: **E**valuate all the above information: Is the transaction suspicious?

The final step in the suspicious activity identification system is the decision whether or not to make a STR. Due to the fact that suspicion is difficult to quantify, it is not possible to give exact guidelines on the circumstances in which a STR should, or should not, be made. However, such a decision will be of the highest quality when all the relevant circumstances are known to, and considered by, the decision maker, i.e. when all three of the preceding steps in the suspicious transaction identification system have been completed and are considered. If, having considered all the circumstances, staff find the activity genuinely suspicious then an STR should be made.

IMPORTANT NOTE

The above information is extracted from the relevant part of the website of the JFIU at ***http://www.jfiu.gov.hk/eng/suspicious_screen.html***. Insurance institutions are advised to regularly browse the website for latest information.

INDICATORS OF SUSPICIOUS TRANSACTIONS

1. A request by a customer to enter into an insurance contract(s) where the source of the funds is unclear or not consistent with the customer's apparent standing.

2. A sudden request for a significant purchase of a lump sum contract with an existing client whose current contracts are small and of regular payments only.

3. A proposal which has no discernible purpose and a reluctance to divulge a "need" for making the investment.

4. A proposal to purchase and settle by cash.

5. A proposal to purchase by utilizing a cheque drawn from an account other than the personal account of the proposer.

6. The prospective client who does not wish to know about investment performance but does enquire on the early cancellation/surrender of the particular contract.

7. A customer establishes a large insurance policy and within a short period of time cancels the policy, requests the return of the cash value payable to a third party.

8. Early termination of a product, especially in a loss.

9. A customer applies for an insurance policy relating to business outside the customer's normal pattern of business.

10. A customer requests for a purchase of insurance policy in an amount considered to be beyond his apparent need.

11. A customer attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments.

12. A customer refuses, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue.

13. A customer is reluctant to provide normal information when applying for an insurance policy, provides minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify.

14. Delay in the provision of information to enable verification to be completed.

15. Opening accounts with the customer's address outside the local service area.

16. Opening accounts with names similar to other established business entities.

17. Attempting to open or operating accounts under a false name.

18. Any transaction involving an undisclosed party.

19. A transfer of the benefit of a product to an apparently unrelated third party.

20. A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy).

21. Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policy holder.

22. The customer accepts very unfavourable conditions unrelated to his health or age.

23. An atypical incidence of pre-payment of insurance premiums.

24. Insurance premiums have been paid in one currency and requests for claims to be paid in another currency.

25. Activity is incommensurate with that expected from the customer considering the information already known about the customer and the customer's previous financial activity. (For individual customers, consider customer's age, occupation, residential address, general appearance, type and level of previous financial activity. For corporate customers, consider type and level of activity.)

26. Any unusual employment of an intermediary in the course of some usual transaction or formal activity e.g. payment of claims or high commission to an unusual intermediary.

27. A customer appears to have policies with several institutions.

28. A customer wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.

29. The customer who is based in jurisdictions which do not or insufficiently apply the FATF Recommendations designated by the FATF from time to time or in countries where the production of drugs or drug trafficking may be prevalent.

30. The customer who is introduced by an overseas agent, affiliator or other company that is based in jurisdictions which do not or insufficiently apply the FATF Recommendations designated by the FATF from time to time or in countries where corruption or the production of drugs or drug trafficking may be prevalent.

31. A customer who is based in Hong Kong and is seeking a lump sum investment and offers to pay by a wire transaction or foreign currency.

32. Unexpected changes in employee characteristics, e.g. lavish lifestyle or avoiding taking holidays.

33. Unexpected change in employee or agent performance, e.g. the sales person selling products has a remarkable or unexpected increase in performance.

34. Consistently high activity levels of single premium business far in excess of any average company expectation.

35. The use of an address which is not the client's permanent address, e.g. utilization of the salesman's office or home address for the despatch of customer documentation.

IMPORTANT NOTE

The IAIS has published relevant examples and indicators involving insurance in a document called "Examples of money laundering and suspicious transactions involving insurance". The document can be downloaded from IAIS website at ***http://www.iaisweb.org/__temp/Examples_of_money_laundering.pdf***. The list will be updated periodically to include additional examples identified. Insurance institutions are advised to regularly browse the website for latest information.

EXAMPLES OF MONEY LAUNDERING SCHEMES[18]

LIFE INSURANCE

Case 1

In 1990, a British insurance sales agent was convicted of violating a money laundering statute. The insurance agent was involved in a money laundering scheme in which over US$1.5 million was initially placed with a bank in England. The "layering process" involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent's supervisor was also charged with violating the money laundering statute. This case has shown how money laundering, coupled with a corrupt employee, can expose an insurance company to negative publicity and possible criminal liability.

Case 2

A company director from Company W, Mr. H, set up a money laundering scheme involving two companies, each one established under two different legal systems. Both of the entities were to provide financial services and providing financial guarantees for which he would act as director. These companies wired the sum of US$1.1 million to the accounts of Mr. H in Country S. It is likely that the funds originated in some sort of criminal activity and had already been introduced in some way into the financial system. Mr. H also received transfers from Country C. Funds were transferred from one account to another (several types of accounts were involved, including both current and savings accounts). Through one of these transfers, the funds were transferred to Country U from a current account in order to make payments on life insurance policies. The investment in these policies was the main mechanism in the scheme for laundering the funds. The premiums paid for the life insurance policies in Country U amounted to some US$1.2 million and represented the last step in the laundering operation.

Case 3

Customs officials in Country X initiated an investigation which identified a narcotics trafficking organization utilized the insurance sector to launder proceeds. Investigative efforts by law enforcement agencies in several different countries

[18] Majority of the examples of money laundering schemes in this annex are extracted from the IAIS document "Examples of money laundering and suspicious transactions involving insurance". The document can be downloaded at ***http://www.iaisweb.org/__temp/Examples_of_money_laundering.pdf***.

identified narcotic traffickers were laundering funds through Insurance firm Z located in an off-shore jurisdiction.

Insurance firm Z offers investment products similar to mutual funds. The rate of return is tied to the major world stock market indices so the insurance policies were able to perform as investments. The account holders would over-fund the policy, moving monies into and out of the fund for the cost of the penalty for early withdrawal. The funds would then emerge as a wire transfer or cheque from an insurance company and the funds were apparently clean.

To date, this investigation has identified that over US$29 million was laundered through this scheme, of which over US$9 million has been seized. Additionally, based on joint investigative efforts by Country Y (the source country of the narcotics) and Country Z customs officials, several search warrants and arrest warrants were executed relating to money laundering activities involved individuals associated with Insurance firm Z.

Case 4

An attempt was made to purchase life policies for a number of foreign nationals. The underwriter was requested to provide life coverage with an indemnity value identical to the premium. There were also indications that in the event that the policies were to be cancelled, the return premiums were to be paid into a bank account in a different jurisdiction to the assured.

Case 5

On a smaller scale, local police authorities were investigating the placement of cash by a drug trafficker. The funds were deposited into several bank accounts and then transferred to an account in another jurisdiction. The drug trafficker then entered into a US$75,000 life insurance policy. Payment for the policy was made by two separate wire transfers from the overseas accounts. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker's arrest, the insurer had received instructions for the early surrender of the policy.

Case 6

A customer contracted life insurance of a 10 year duration with a cash payment equivalent to around US$400,000. Following payment, the customer refused to disclose the origin of the funds. The insurer reported the case. It appears that prosecution had been initiated in respect of the individual's fraudulent management activity.

Case 7

A life insurer learned from the media that a foreigner, with whom it had two life-insurance contracts, was involved in Mafia activities in his/her country. The contracts were of 33 years duration. One provided for a payment of close to the equivalent of US$1 million in case of death. The other was a mixed insurance with value of over half this amount.

Case 8

A client domiciled in a country party to a treaty on the freedom of cross-border provision of insurance services, contracted with a life-insurer for a foreign life insurance for 5 years with death cover for a down payment equivalent to around US$7 million. The beneficiary was altered twice: 3 months after the establishment of the policy and 2 months before the expiry of the insurance. The insured remained the same. The insurer reported the case. The last beneficiary - an alias - turned out to be a PEP.

REINSURANCE

Case 1

An insurer in country A sought reinsurance with a reputable reinsurance company in country B for its directors and officer cover of an investment firm in country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer which contacted law enforcement agencies. Investigation made clear that the investment firm was bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that - although drug money would be laundered by a payment received from the reinsurer - the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsurer. By offering to pay above market rate the insurer probably intended to assure continuation of the reinsurance arrangement.

INTERMEDIARIES

Case 1

A person (later arrested for drug trafficking) made a financial investment (life insurance) of US$250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of US$250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raise no suspicion at the

bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling US$250,000, thus avoiding the raising suspicions with the insurance company.

Case 2

Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing the due diligence checks.

The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses, but coming away with a clean cheque from the institution.

On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.

Case 3

An insurance company was established by a well-established insurance management operation. One of the clients, a Russian insurance company, had been introduced through the management of the company's London office via an intermediary.

In this particular deal, the client would receive a "profit commission" if the claims for the period were less than the premiums received. Following an on-site inspection of the company by the insurance regulators, it became apparent that the payment route out for the profit commission did not match the flow of funds into the insurance company's account. Also, the regulators were unable to ascertain the origin and route of the funds as the intermediary involved refused to supply this information. Following further investigation, it was noted that there were several companies involved in the payment of funds and it was difficult to ascertain how these companies were connected with the original insured, the Russian insurance company.

Case 4

A construction project was being financed in Europe. The financing also provided for a consulting company's fees. To secure the payment of the fees, an investment account was established and a sum equivalent to around US$400,000 deposited with a life-insurer. The consulting company obtained powers of attorney for the account. Immediately following the setting up of the account, the consulting company withdrew the entire fee stipulated by the consulting contract. The insurer reported the transaction as suspicious. It turns out that an employee of the consulting company was involved in several similar cases. The account is frozen.

OTHER EXAMPLES

Single premiums

An example involves the purchase of large, single premium insurance policies and their subsequent rapid redemption. A money launderer does this to obtain payment from an insurance company. The person may face a redemption fee or cost, but this is willingly paid in exchange for the value that having funds with an insurance company as the immediate source provider.

In addition, the request for early encashment of single premium policies, for cash or settlement to an individual third party may arouse suspicion.

Return premiums

There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

(a) a number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time;

(b) return premium being credited to an account different from the original account;

(c) requests for return premiums in currencies different from the original premium; and

(d) regular purchase and cancellation of policies.

Overpayment of premiums

Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made. A money launderer may well own legitimate assets or businesses as well as an illegal enterprise. In this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally', but on a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be unwilling to confront a customer who is both profitable to the company and important to his own success.

The overpayment of premiums, has been used as a method of money laundering. Insurers should be especially vigilant where:

- the overpayment is over a certain size (say US$10,000 or equivalent);
- the request to refund the excess premium was to a third party;
- the assured is in a jurisdiction associated with money laundering; and
- where the size or regularity of overpayments is suspicious.

High brokerage / third party payments / strange premium routes

High brokerage can be used to pay off third parties unrelated to the insurance contract. This often coincides with example of unusual premium routes.

Assignment of claims

In a similar way, a money launderer may arrange with groups of otherwise legitimate people, perhaps owners of businesses, to assign any legitimate claims on their policies to be paid to the money launderer. The launderer promises to pay these businesses, perhaps in cash, money orders or travellers cheques, a percentage of any claim payments paid to him above and beyond the face value of the claim payments. In this case the money laundering strategy involves no traditional fraud against the insurer. Rather, the launderer has an interest in obtaining funds with a direct source from an insurance company, and is willing to pay others for this privilege. The launderer may even be strict in insisting that the person does not receive any fraudulent claims payments, because the person does not want to invite unwanted attention.

IMPORTANT NOTE

Apart from the above examples of money laundering schemes, the FATF has also published annually detailed typologies involving insurance supported by useful case examples in documents called "Money Laundering & Terrorist Financing Typologies". The documents can be downloaded at the publications section of FATF website at ***http://www.fatf-gafi.org***. Insurance institutions are advised to regularly browse the website for latest information.

SAMPLE REPORT MADE TO THE JOINT FINANCIAL INTELLIGENCE UNIT

<table>
<tr><td colspan="3">Report made under section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance/Organized and Serious Crimes Ordinance or section 12 of the United Nations (Anti-Terrorism Measures) Ordinance to the Joint Financial Intelligence Unit</td><td colspan="3">Date :
Ref. No. :</td></tr>
<tr><td colspan="2">NAME AND ADDRESS OF INSURANCE INSTITUTION</td><td colspan="4"></td></tr>
<tr><td colspan="2">NAME OF SUSPICIOUS CUSTOMER (in full)</td><td colspan="4"></td></tr>
<tr><td colspan="2">DATE OF ISSUE OF INSURANCE POLICY (if applicable)</td><td></td><td colspan="2">DATE OF BIRTH / DATE OF INCORPORATION*</td><td></td></tr>
<tr><td colspan="2">OCCUPATION & EMPLOYER / NATURE OF BUSINESS*</td><td colspan="4"></td></tr>
<tr><td colspan="2">NATIONALITY / PLACE OF INCORPORATION*</td><td></td><td colspan="2">HKID / PASSPORT / BUSINESS REGISTRATION NO.*</td><td></td></tr>
<tr><td colspan="2">ADDRESS OF CUSTOMER</td><td colspan="4"></td></tr>
<tr><td>INFORMATION OF THE BENEFICIARY</td><td colspan="2">NAME & ADDRESS, RELATION WITH CUSTOMER</td><td>DATE OF BIRTH / DATE OF INCORPORATION*</td><td>HKID / PASSPORT NO.</td><td>NATIONALITY / PLACE OF INCORPORATION*</td></tr>
<tr><td colspan="2">DETAILS OF TRANSACTION AROUSING SUSPICION, AND THE SUM INVOLVED INDICATING SOURCE & CURRENCY USE. PLEASE ALSO ENCLOSE COPY OF THE TRANSACTION AND OTHER RELEVANT DOCUMENT</td><td>PARTICULARS OF TRANSACTION</td><td>AMOUNT</td><td>DATE</td><td>SOURCE</td></tr>
<tr><td colspan="2">OTHER RELEVANT INFORMATION INCLUDING REASON FOR SUSPICION AROUSED</td><td colspan="4"></td></tr>
<tr><td colspan="2">REPORTING OFFICER / TEL. NO.</td><td colspan="2">SIGNATURE</td><td colspan="2">ENTERED RECORDS</td></tr>
</table>

** in the case of a corporation*

JOINT FINANCIAL INTELLIGENCE UNIT CONTACT DETAILS

Written report should be sent to the Joint Financial Intelligence Unit at either the address, fax number, e-mail or PO Box listed below:

The Joint Financial Intelligence Unit,
28/F, Arsenal House West Wing,
Hong Kong Police Headquarters,
Arsenal Street,
Hong Kong.

or

The Joint Financial Intelligence Unit,
GPO Box 6555,
Hong Kong Post Office,
Hong Kong.

Tel: 2866 3366

Fax: 2529 4013

Email: jfiu@police.gov.hk

Urgent reports should be made either by fax, e-mail or by telephone to 2866 3366.

SAMPLE ACKNOWLEDGEMENT LETTER ISSUED BY THE JOINT FINANCIAL INTELLIGENCE UNIT

Date:

The Compliance Officer
Any Insurance Co./Broker

Your ref.:

Dear Sir,

Drug Trafficking (Recovery of Proceeds) Ordinance
Organized and Serious Crimes Ordinance
United Nations (Anti-Terrorism Measures) Ordinance

I refer to your disclosure made to the Joint Financial Intelligence Unit on [ ] under the above references.

I acknowledge receipt of the information supplied by you under the provisions of Section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 and the Organized and Serious Crimes Ordinance, Cap. 455 / Section 12 of the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575.

Based upon the information currently available, consent is given for you to continue to operate the account(s) in accordance with normal insurance practice under the provisions of the Ordinance(s).

Thank you for your co-operation.

Yours faithfully,

Joint Financial Intelligence Unit

Annex D

SECURITIES AND
FUTURES COMMISSION
證券及期貨事務監察委員會

Prevention of Money Laundering and Terrorist Financing Guidance Note

防止洗黑錢及恐怖分子籌資活動的指引

Hong Kong
September 2009

香港
2009 年 9 月

Table of Contents

GLOSSARY

In this Guidance Note, the following abbreviations and references are used:

DTROP	"DTROP" means the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405).
Equivalent jurisdictions	Jurisdictions that apply standards of prevention of money laundering and terrorist financing equivalent to those of the FATF. Please refer to subsection 6.2.6 for guidance on assessing whether or not a jurisdiction sufficiently applies FATF standards in combating money laundering and terrorist financing. For the purposes of this Guidance Note, all members of the European Union (including Gibraltar), Antilles and Aruba of the Kingdom of the Netherlands, Isle of Man, Guernsey and Jersey are deemed to be equivalent jurisdictions.
FATF	"FATF" means the Financial Action Task Force on Money Laundering.
FATF members	Jurisdictions that are from time to time members of FATF. FATF members include Argentina; Australia; Austria; Belgium; Brazil; Canada; Denmark; Finland; France; Germany; Greece; Hong Kong China; Iceland; Ireland; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; the Russian Federation; Singapore; South Africa; Spain; Sweden; Switzerland; Turkey; United Kingdom and the United States. Two international organizations are also members of the FATF: the European Commission and the Gulf Co-operation Council. The current list of FATF members can be found on the FATF website www.fatf-gafi.org, and will be updated by FATF from time to time.
Financial intermediary	A financial institution conducting financial transactions for or on behalf of its customers.
JFIU	"JFIU" means the Joint Financial Intelligence Unit. The unit is jointly run by staff of the Hong Kong Police Force and the Hong Kong Customs & Excise Department.

NCCTs	"NCCTs" means non-cooperative countries and territories identified by the FATF to have critical deficiencies in their anti-money laundering systems or a demonstrated unwillingness to co-operate in anti-money laundering efforts. The current list of NCCTs can be found on the FATF website www.fatf-gafi.org, and will be updated by the FATF from time to time.
OSCO	"OSCO" means the Organized and Serious Crimes Ordinance (Cap.455).
PEPs	"PEPs" means politically exposed persons and is defined as individuals who are or have been entrusted with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of government owned corporations, important political party officials. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.
Professional intermediary	A lawyer or an accountant conducting financial transactions for or on behalf of its customers.
SFO	"SFO" means the Securities and Futures Ordinance (Cap. 571).
Substantial shareholders	As defined under section 6 of Part 1 of Schedule 1 to the SFO.
UNATMO	"UNATMO" means the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575).

PART I OVERVIEW

1. Introduction

1.1 This Guidance Note, which is published under section 399 of the SFO, provides a general background on the subjects of money laundering and terrorist financing, summarizes the main provisions of the applicable anti-money laundering and anti-terrorist financing legislation in Hong Kong, and provides guidance on the practical implications of that legislation. The Guidance Note also sets out the steps that a licensed corporation or associated entity that is not an authorized financial institution, and any of its representatives, should implement to discourage and identify any money laundering or terrorist financing activities. The relevance and usefulness of this Guidance Note will be kept under review and it may be necessary to issue amendments from time to time.

1.2 This Guidance Note is intended for use primarily by corporations licensed under the SFO and associated entities that are not authorized financial institutions. Where relevant, this Guidance Note applies to licensed representatives. Registered institutions and associated entities that are authorized financial institutions are subject to the Hong Kong Monetary Authority's guidelines on prevention of money laundering (the "HKMA's guidelines"). However, to the extent that there are some securities or futures-sector specific guidance in this Guidance Note which may not be shown in the HKMA's guidelines, viz. risk management procedures to be undertaken where the customer due diligence process could not be satisfactorily completed after securities transactions have been conducted on behalf of a customer, omnibus account established in the name of a financial or professional intermediary and examples of suspicious transactions relating to the securities sector, the registered institutions and associated entities that are authorized financial institutions shall have regard to the relevant parts under subsection 6.1.10, 6.6 and Appendix C(ii) respectively in this Guidance Note.

1.3 This Guidance Note does not have the force of law and should not be interpreted in any manner which would override the provisions of any law, codes or other regulatory requirements applicable to the licensed corporation, associated entity or registered institution concerned. In the case of any inconsistency, the provision requiring a higher standard of conduct will apply. However, a failure to comply with any of the requirements of this Guidance Note by licensed corporations, licensed representatives (where applicable), or associated entities will, in the absence of extenuating circumstances, reflect adversely on their fitness and properness. Similarly, a failure to comply with any of the requirements of the HKMA's guidelines or to have regard to the relevant parts under subsections 6.1.10, 6.6 and Appendix C(ii) of this

Guidance Note by registered institutions or associated entities that are authorized financial institutions will, in the absence of extenuating circumstances, reflect adversely on their fitness and properness.

1.4 When considering a person's failure to comply with this Guidance Note, staff of the Commission will adopt a pragmatic approach taking into account all relevant circumstances.

1.5 Unless otherwise specified or the context otherwise requires, words and phrases in the Guidance Note shall be interpreted by reference to any definition of such word or phrase in Part 1 of Schedule 1 to the SFO.

2. Background

2.1 The nature of money laundering and terrorist financing

2.1.1 The term "money laundering" covers a wide range of activities and processes intended to alter the identity of the source of criminal proceeds in a manner which disguises their illegal origin.

2.1.2 The term "terrorist financing" includes the financing of terrorist acts, and of terrorists and terrorist organizations. It extends to any funds, whether from a legitimate or illegitimate source.

2.1.3 Terrorists or terrorist organizations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

2.2 Stages of money laundering

2.2.1 There are three common stages in the laundering of money, and they frequently involve numerous transactions. A licensed corporation or an associated entity should be alert to any such sign for potential criminal activities. These stages are:

(a) Placement - the physical disposal of cash proceeds derived from illegal activities;

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

(c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

2.2.2 The chart set out at Appendix B illustrates the laundering stages in greater detail.

2.3 Potential uses of the securities, futures and leveraged foreign exchange businesses in the money laundering process

2.3.1 Since the securities, futures and leveraged foreign exchange businesses are no longer predominantly cash based, they are less conducive to the initial placement of criminally derived funds than other financial industries, such as banking. Where, however, the payment underlying these transactions is in cash, the risk of these businesses being used as the placement facility cannot be ignored, and thus due diligence must be exercised.

2.3.2 The securities, futures and leveraged foreign exchange businesses are more likely to be used at the second stage of money laundering, i.e. the layering process. Unlike laundering via banking networks, these businesses provide a potential avenue which enables the launderer to dramatically alter the form of funds. Such alteration may not only allow conversion from cash in hand to cash on deposit, but also from money in whatever form to an entirely different asset or range of assets such as securities or futures contracts, and, given the liquidity of the markets in which these instruments are traded, with potentially great frequency.

2.3.3 Investments that are cash equivalents e.g. bearer bonds and similar investments in which ownership can be evidenced without reference to registration of identity, may be particularly attractive to the money launderer.

2.3.4 As mentioned, securities, futures and leveraged foreign exchange transactions may prove attractive to money launderers due to the liquidity of the reference markets. The combination of the ability to readily liquidate investment portfolios procured with both licit and illicit proceeds, the ability to conceal the source of the illicit proceeds, the availability of a vast array of possible investment mediums, and the ease with which transfers can be effected between them, offers money launderers attractive ways to effectively integrate criminal proceeds into the general economy.

2.4 International initiatives

2.4.1 The FATF is a pre-eminent inter-governmental organization established in 1989 to examine and recommend measures to counter money laundering. The FATF's 40 Recommendations set out the framework for anti-money laundering efforts and are designed for universal application. Hong Kong has been a FATF member since 1990 and is obliged to implement its recommendations. In October 2001, the FATF expanded its scope of work to cover matters relating to terrorist financing.

2.4.2 In 1992, the International Organization of Securities Commissions ("IOSCO"), of which the Commission is a member, adopted a resolution inviting IOSCO members to consider issues relating to minimising money laundering, such as adequate customer identification, record keeping, monitoring and compliance procedures and the identification and reporting of suspicious transactions.

2.4.3 In June 1996, FATF issued a revised set of 40 recommendations for dealing with money laundering. The 40 Recommendations were further revised in June 2003[1] in response to the increasingly sophisticated combinations of techniques in laundering criminal funds. The revised 40 Recommendations apply not only to money laundering but also to terrorist financing, and when combined with the Nine Special Recommendations revised by FATF in October 2004, provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing (hereafter referred to collectively as "FATF's Recommendations").

2.4.4 In light of the recent work of FATF and other international organizations, IOSCO established a task force, in October 2002, to study existing securities regulatory regimes and to develop principles relating to the identification of customers and beneficial owners. IOSCO subsequently issued, in May 2004, the paper, "Principles on Client Identification and Beneficial Ownership for the Securities Industry"[2], to guide securities regulators and regulated firms of the securities industry in implementing requirements relating to customer due diligence.

---

1 FATF's Recommendations can be found on the FATF website www.fatf-gafi.org.

2 IOSCO's Principles on Client Identification and Beneficial Ownership for the Securities Industry can be found on the IOSCO's website www.iosco.org/library/index.cfm.

3. Legislation Concerned with Money Laundering and Terrorist Financing

3.1 As one of the major financial centres in the world, it is very important for Hong Kong to maintain an effective anti-money laundering regime which helps to further reinforce the integrity and stability of our financial system. Money laundering can have devastating consequences to the whole community. Not only does it allow the criminals to perpetrate their illicit activities, it can also undermine the financial system, causing adverse consequences to the government as well as the community at large.

3.2 The three main pieces of legislation in Hong Kong that are concerned with money laundering and terrorist financing are the DTROP, the OSCO and the UNATMO. The principal anti-money laundering and anti-terrorist financing provisions are summarized in Appendix A. The summary is not a legal interpretation of the applicable legislation and, where appropriate, legal advice should be sought.

4. Policies and Procedures to Combat Money Laundering and Terrorist Financing

4.1 Guiding principles

4.1.1 This Guidance Note has taken into account the requirements of the latest FATF's Recommendations applicable to the securities, futures and leveraged foreign exchange businesses. The detailed guidelines in Part II has outlined relevant measures and procedures to guide licensed corporations and associated entities in preventing money laundering and terrorist financing. Some of these suggested measures and procedures may not be applicable in every circumstance. Each licensed corporation or associated entity should consider carefully the specific nature of its business, organizational structure, type of customer and transaction, etc. to satisfy itself that the measures taken by them are adequate and appropriate to follow the spirit of the suggested measures in Part II.

4.1.2 Where reference is made in this Guidance Note to a licensed corporation or associated entity being satisfied as to a matter, the licensed corporation or associated entity must be able to justify its assessment to the Commission and demonstrate that its assessment was a reasonable assessment for it to have made at the time and in the circumstances in which it was made, viewed objectively. If and where applicable, a licensed corporation or associated entity should also be able to justify its assessment to

any other relevant authority in accordance with any other applicable rules and regulations.

4.2 Obligation to establish policies and procedures

4.2.1 International initiatives taken to combat drug trafficking, terrorism and other organised and serious crimes have concluded that financial institutions[3] must establish procedures of internal control aimed at preventing and impeding money laundering and terrorist financing. There is a common obligation in all the statutory requirements not to facilitate money laundering or terrorist financing. There is also a need for financial institutions to have a system in place for reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

4.2.2 In light of the above, senior management of a licensed corporation or an associated entity should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. Licensed corporations and associated entities should:

(a) issue a statement of policies and procedures, on a group basis where applicable, for dealing with money laundering and terrorist financing reflecting the current statutory and regulatory requirements including:

- maintenance of records; and
- co-operation with the relevant law enforcement authorities, including the timely disclosure of information;

(b) ensure that the content of this Guidance Note to the extent appropriate is understood by all staff members. The aim is to develop staff members' awareness and vigilance to guard against money laundering and terrorist financing;

(c) regularly review the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness. For example, reviews performed by the internal audit or compliance function to ensure

[3] "Financial institutions", as defined in the FATF's Recommendations, encompasses persons or entities engaging in a wide range of financial activities. For details, please refer to the Glossary of the FATF's Recommendations which can be found on the FATF Website www.fatf-gafi.org.

compliance with policies, procedures and controls relating to prevention of money laundering and terrorist financing[4];

(d) adopt customer acceptance policies and procedures which are sensitive to the risk of money laundering and terrorist financing; and

(e) undertake customer due diligence ("CDD") measures (see subsection 6.1.2) to an extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transaction.

4.3 Application of policies and procedures to overseas branches and subsidiaries

4.3.1 Whilst appreciating the sensitive nature of extra-territorial regulations, licensed corporations and associated entities should ensure that their overseas branches and where practicable, subsidiaries are aware of group policies concerning money laundering and terrorist financing and apply the group standards to the extent that local applicable laws and regulations permit. If appropriate, overseas branches and where practicable, subsidiaries should be instructed as to the local reporting point to whom disclosure should be made of any suspicion about a person, transaction or property.

4.3.2 Licensed corporations and associated entities should pay particular attention to the anti-money laundering and terrorist financing compliance standards of their branches and subsidiaries which are located in jurisdictions that do not or insufficiently implement the FATF's Recommendations including jurisdictions designated as the NCCTs[5] by the FATF.

4.3.3 Where an overseas branch or subsidiary is known to be unable to observe group standards, the licensed corporation or associated entity should inform the Commission as soon as practicable.

---

[4] Areas of review should include: (i) an assessment of the system for detecting suspected money laundering transactions; (ii) evaluation and checking of the adequacy of exception reports generated on large and / or irregular transactions; (iii) review of the quality of reporting of suspicious transactions; and (iv) an assessment of the level of awareness of front line staff regarding their responsibilities.

[5] For NCCTs with serious deficiencies and where inadequate progress has been made to improve their position, the FATF may recommend the application of further counter-measures. The Commission will continue to keep licensed corporations and associated entities informed of the specific counter-measures, as recommended by FATF, including updates, as and when appropriate. The measures will generally focus on more stringent customer due diligence and enhanced surveillance and reporting of transactions. Licensed corporations and associated entities should apply the counter-measures as advised by the Commission to such NCCTs.

PART II DETAILED GUIDELINES

5. Customer Acceptance

5.1 Licensed corporations and associated entities should develop customer acceptance policies and procedures that aim to identify the types of customers that are likely to pose a higher than average risk of money laundering and terrorist financing. A more extensive customer due diligence process should be adopted for higher risk customers. There should also be clear internal policies on which level of management is able to approve a business relationship with such customers.

5.2 In determining the risk profile of a particular customer or type of customers, licensed corporations and associated entities should take into account factors such as the following:

(a) background or profile of the customer, such as being, or linked to, a PEP;

(b) 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;

(c) the nationality, citizenship and resident status of the customer (in the case of a corporate customer, the place of incorporation), the place of establishment of the customer's business and location of the counterparties with which the customer does business, such as NCCTs designated by the FATF or those known to the licensed corporations and associated entities to lack proper standards in the prevention of money laundering or customer due diligence process;

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

(e) means of payment as well as type of payment (cash or third party cheque the drawer of which has no apparent connection with the prospective customer may be a cause for increased scrutiny);

(f) risks associated with non face-to-face business relationships; and

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

5.3 Licensed corporations and associated entities should adopt a balanced and common sense approach with regard to customers of higher than average risk of money laundering and terrorist financing; e.g. those from or closely linked with NCCTs or from other jurisdictions which do

not meet FATF standards. While extra care should be exercised in such cases, it is not a requirement that licensed corporations and associated entities should refuse to do any business with such customers or automatically classify them as high risk and subject them to an enhanced customer due diligence process under the risk-based approach discussed in subsection 6.2 of this Guidance Note. Rather, licensed corporations and associated entities should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of money laundering.

5.4 A licensed corporation or an associated entity should consider reclassifying a customer as higher risk if, following initial acceptance of the customer, the pattern of account activity of the customer does not fit in with the licensed corporation's or associated entity's knowledge of the customer. A suspicious transaction report should also be considered.

6. Customer Due Diligence

6.1 General

6.1.1 Licensed corporations and, where applicable, associated entities should take all reasonable steps to enable them to establish to their satisfaction the true and full identity of each customer, and of each customer's financial situation and investment objectives.

6.1.2 The customer due diligence process should comprise the following:

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

(b) verify the customer's identity using reliable source documents, data or information;

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

(d) conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the licensed corporation's or associated entity's knowledge of the customer, its business and risk profile, taking into account, where necessary, the customer's source of funds.

6.1.3 Specific CDD requirements applicable to different types of customers are outlined in subsections 6.3 to 6.11. For the purpose of compliance with these requirements, the guiding principle is that licensed corporations and associated entities should be able to justify that they have taken objectively reasonable steps to satisfy themselves as to the true identity of their customers, including beneficial owners.

6.1.4 The CDD measures set out in this Guidance Note should, except provided otherwise, be applied to both the customer itself and its beneficial owner.

6.1.5 Licensed corporations and associated entities should verify their customers' identity using documents issued by reliable sources. If there is doubt or difficulty in determining whether the identification document is genuine, licensed corporations and associated entities should obtain such document from a source independent from the customer.

6.1.6 Depending on the type of customer, business relationship or transaction, licensed corporations and associated entities would need to obtain appropriate information on the purpose and intended nature of the business relationship on a risk sensitive basis such that ongoing due diligence on the customer may be conducted at a level commensurate with the customer's risk profile.

6.1.7 Licensed corporations and associated entities should not keep anonymous accounts or accounts using fictitious names.

6.1.8 When establishing a business relationship, licensed corporations and associated entities should ask whether the customers are acting for their own accounts or for the account of another party or parties for the purpose of identifying the beneficial owner of the account opened by the customer.

6.1.9 In general, a licensed corporation or an associated entity should verify the identity of the customer and beneficial owner before establishing a business relationship. When the licensed corporation or associated entity is unable to perform the CDD process satisfactorily at the account opening stage, it should not commence the business relationship or perform the transaction and should consider whether a suspicious transaction report should be made.

6.1.10 However, where transactions conducted on behalf of customers need to be performed very rapidly due to market conditions or in

other circumstances where it is essential not to interrupt the normal conduct of business, it would be permissible for verification to be completed after the establishment of the business relationship provided that the verification occurs as soon as reasonably practicable. A licensed corporation or an associated entity would need to adopt clear and appropriate policies and procedures concerning the conditions and timeframe under which a customer is permitted to establish the business relationship prior to verification. These procedures should include a set of measures such as limitation of the number, types and / or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out that fall outside the expected norms for that type of relationship. For example, consideration may be given to not allow funds to be paid out of the account to a third party, if possible, before the identity of the customer is satisfactorily verified. If the licensed corporation or associated entity is unable to perform the CDD process satisfactorily within a reasonably practicable timeframe after commencing the business relationship, it should, if possible, discontinue the business relationship and consider whether a suspicious transaction report should be made.

6.1.11 Licensed corporations and associated entities should take reasonable steps to ensure that the records of existing customers remain up-to-date and relevant.

6.1.12 To achieve this, a licensed corporation or an associated entity should consider undertaking periodic and / or ad hoc reviews of existing customer records to consider re-classifying a customer as high or low risk. The frequency for conducting these reviews should be determined based on the licensed corporation or associated entity's understanding of the customer and the type of relationship and transaction. For example, an appropriate time to perform an ad hoc review may be when there is a transaction that is unusual or not in line with the customer's normal trading pattern based on the licensed corporation's or associated entity's knowledge of the customer; when there is a material change in the way that the account is operated; when the licensed corporation or associated entity is not satisfied that it has sufficient information about the customer; or when there are doubts about the veracity or adequacy of previously obtained identification data.

6.1.13 Even in the absence of any of the circumstances mentioned in subsection 6.1.12 above, licensed corporations and associated entities are encouraged to consider whether to require additional information in line with their current standards from those existing customers.

6.2 Risk-based approach

6.2.1 The general rule is that customers are subject to the full range of CDD measures. Licensed corporations and associated entities should however determine the extent to which they apply each of the CDD measures on a risk sensitive basis. The basic principle of a risk-based approach is that licensed corporations and associated entities adopt an enhanced CDD process for higher risk categories of customers, business relationships or transactions. Similarly, simplified CDD process is adopted for lower risk categories of customers, business relationships or transactions. The relevant enhanced or simplified CDD process may vary from case to case depending on customers' background, transaction types and specific circumstances, etc. Licensed corporations and associated entities should exercise their own judgment and adopt a flexible approach when applying the specific enhanced or simplified CDD measures to customers of particular high or low risk categories.

6.2.2 Licensed corporations and associated entities should establish clearly in their customer acceptance policies the risk factors for determining what types of customers and activities are to be considered as low or high risk, while recognising that no policy can be exhaustive in setting out all risk factors that should be considered in every possible situation. In addition, they must satisfy themselves that the use of simplified customer due diligence is reasonable in the circumstances and approved by senior management. The opening of a high risk account whereby enhanced CDD would be required should be subject to approval by senior management.

6.2.3 Simplified CDD procedures may be used for identifying and verifying the identity of the customer and the beneficial owner where there is no suspicion of money laundering or terrorist financing, and:

- the inherent risk of money laundering or terrorist financing relating to a type of customer is assessed to be low; or

- there is adequate public disclosure or other checks and controls elsewhere in national systems in relation to the customers.

Some examples of lower risk categories of customers are:

(a) financial institutions that are authorised and supervised by the Commission, Hong Kong Monetary Authority or Office of the Commissioner of Insurance or by an equivalent authority in a jurisdiction that is a FATF member or in an equivalent jurisdiction;

(b) public companies that are subject to regulatory disclosure requirements. This includes companies that are listed on a stock exchange in a FATF member jurisdiction or on a specified stock exchange as defined under the SFO[6] and their subsidiaries;

(c) government or government related organisations in a non-NCCT jurisdiction where the risk of money laundering is assessed by the licensed corporation or associated entity to be low and where the licensed corporation or associated entity has no doubt as regards the ownership of the organisation; and

(d) pension, superannuation or similar schemes that provide retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

6.2.4 It should be noted that there might be instances where the circumstances may lead to suspicions even though the inherent risk of the customer is considered to be low. Should there be any doubt, the full range of CDD measures should be adopted.

6.2.5 Licensed corporations and associated entities should note that jurisdictions which are not designated as NCCTs do not necessarily mean that they could be taken as equivalent jurisdictions that apply standards of prevention of money laundering and terrorist financing equivalent to those of the FATF.

6.2.6 In assessing whether or not a country (other than FATF members or the list of equivalent jurisdictions listed in the Glossary of this Guidance Note) sufficiently applies FATF standards in combating money laundering and terrorist financing and meets the criteria for an equivalent jurisdiction, licensed corporations and associated entities should:

[6] Licensed corporations and associated entities should pay special attention to Recommendation 21 of the FATF's Recommendations and exercise extra care in respect of customers and business relationships from NCCTs, including corporate customers listed on stock exchanges of NCCTs.

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

(b) pay particular 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, as part of their financial stability assessments of countries and territories, the IMF and the World Bank 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 to take into account information that is reasonably available to them about the standards of anti-money laundering systems and controls that operate in the country with which any of their customers are associated.

6.2.7 Apart from the risk factors set out in subsection 5.2 for determining a customer's risk profile, the following are some examples of high risk categories of customers:

(a) complex legal arrangements such as unregistered or unregulated investment vehicles;

(b) companies that have nominee shareholders or a significant portion of capital in the form of bearer shares;

(c) persons (including corporations and other financial institutions) from or in countries which do not or insufficiently apply the FATF's Recommendations (such as jurisdictions designated as the NCCTs by the FATF or those known to the licensed corporations and associated entities to lack proper standards in the prevention of money laundering and terrorist financing); and

(d) PEPs as well as persons or companies clearly related to them.

6.2.8 Licensed corporations and associated entities should pay special attention to all complex, unusual large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose, in particular with customers from countries which do not or insufficiently apply the FATF's Recommendations. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities.

6.3 Individual customers

6.3.1 Information such as the following would normally be needed for verification of the identity of individual customers:

(a) name,

(b) number of Hong Kong Identity Card for a local customer (i.e. resident with a right of abode in Hong Kong) and passport or an unexpired government-issued identification evidencing nationality or residence for non-local customers,

(c) date of birth, and

(d) residential address (and permanent address if different).

6.3.2 Hong Kong Identity Cards or unexpired government-issued identification such as passports are the types of documents that should be produced as proof of identity. Copies of the identity documents should be retained on file.

6.3.3 Licensed corporations and associated entities should check the address of the customer by the best available means, e.g. sighting of a recent utility bill or bank statement. Licensed corporations and associated entities should use a common sense approach to handle cases where the customers and / or beneficial owners fall into categories of persons who may not pay utility bills or have a bank account (e.g. students and housewives).

6.3.4 Licensed corporations and associated entities should also obtain information on the customer's occupation / business to facilitate ongoing due diligence and scrutiny, but this piece of information does not form part of the customer's identity requiring verification.

6.3.5 It must be appreciated that no form of identification can be fully guaranteed as genuine or representing correct identity. If there is doubt or difficulty with distinguishing whether an identification document is genuine, licensed corporations and associated entities may contact the Immigration Department for guidance on recognizing the special features borne with a genuine identity card.

6.3.6 Whenever possible, it is recommended that the prospective customer be interviewed personally. Where the risk of money laundering or terrorist financing relating to the customer is assessed to be high, it is advisable that licensed corporations and associated entities ask the customer to make himself available for a face-to-face interview.

6.4 Corporate customers

6.4.1 For a corporate customer which is not listed on a stock exchange in a FATF member jurisdiction or on a specified stock exchange as defined under the SFO[6], or is not a subsidiary of such a listed company, or is not a government-related corporation in a non-NCCT jurisdiction, or is not a financial institution as described in subsection 6.6.7(a)(i) or 6.6.7(a)(ii), documents and information such as those mentioned below would be relevant for the purpose of conducting CDD:

(a) Certificate of Incorporation and, where applicable, Business Registration Certificate or any other documents proving the incorporation or similar evidence of the legal status of the corporation;

(b) Board resolution evidencing the approval of the opening of the account and conferring authority on those who will operate it;

(c) information about the nature of the business of the corporate customer and its ownership and control structure for identifying which individual(s) ultimately own(s) or control(s) the customer;

(d) specimen signatures of account signatories;

(e) copies of identification documents of at least 2 authorized persons to act on behalf of the corporate customer;

(f) copies of identification documents of at least 2 directors (including the managing director); and

(g) copies of identification documents of substantial shareholders and, where applicable, ultimate principal beneficial owners.

The relevant documents or information may be obtained from a public register, from the customer or from other reliable sources, provided that the licensed corporation or associated entity is satisfied that the information supplied is reliable.

6.4.2 For a corporate customer which is a listed company or investment vehicle, please refer to subsection 6.5 for further guidelines.

6.4.3 If the customer, which is a non-listed company, has a number of layers of companies in its ownership structure, the licensed corporation or associated entity would normally need to follow the chain of ownership to identify the individuals who are the ultimate principal beneficial owners of the customer and to verify the identity of those individuals. However, it is not required to check the details of each of the intermediate companies (including their directors) in the ownership chain. Where a company in the ownership chain is a company listed on a stock exchange in a FATF member jurisdiction or on a specified stock exchange as defined under the SFO[6] or is a subsidiary of such a listed company, or is a financial institution authorised and supervised by the Commission, Hong Kong Monetary Authority or Office of the Commissioner of Insurance or an equivalent authority in a jurisdiction that is a FATF member or an equivalent jurisdiction or is a subsidiary of such a financial institution, it should generally be sufficient to stop at that point and to verify the identity of that customer in line with the suggested CDD measures mentioned in subsection 6.5.2 below.

6.4.4 For higher risk categories of customers or where there is any doubt as to the identity of the beneficial owners, shareholders, directors or account signatories of the corporate customer, it is also advisable that the licensed corporations and associated entities perform additional CDD measures on a risk sensitive basis. Examples of relevant additional measures that could be applied by licensed corporations and associated entities include:

(a) making a company search or credit reference agency search;

(b) obtaining the memorandum and articles of association; and

(c) verifying the identity of all persons who are authorized to operate the account.

6.4.5 In the case of an offshore investment vehicle owned by individuals (i.e. the ultimate beneficial owners) who use such vehicle as the contractual party to establish a business relationship with a licensed corporation or an associated entity and the investment vehicle is incorporated in a jurisdiction where company searches or certificates of incumbency (or equivalent) are not available or cannot provide meaningful information about its directors and substantial shareholders, it is advisable that licensed corporations and associated entities adopt an enhanced CDD process in relation to the customer. Besides satisfying itself that:

- they know the identity of the ultimate beneficial owners; and

- there is no suspicion of money laundering,

it is advisable that the licensed corporation or associated entity perform additional CDD measures on a risk sensitive basis. Examples of relevant additional measures include:

(a) obtaining self-declarations in writing about the identity of, and the relationship with, the directors and substantial shareholders from the ultimate beneficial owners;

(b) obtaining comprehensive customer profile information; e.g. purpose and reasons for opening the account, business or employment background, source of funds and anticipated account activity;

(c) conducting face-to-face meeting with the customer before acceptance of such customer;

(d) obtaining approval of senior management for acceptance of such customer;

(e) assigning a designated staff to serve the customer and that staff should bear the responsibility for CDD and ongoing monitoring to identify any unusual or suspicious transactions on a timely basis; and

(f) conducting face-to-face meetings with the customer as far as possible on a regular basis throughout the business relationship.

6.4.6 Licensed corporations and associated entities need to exercise special care in dealing with companies which have a significant proportion of capital in the form of bearer shares. It is advisable for licensed corporations and associated entities to have procedures to monitor the identity of all substantial shareholders. This may require licensed corporations and associated entities to consider whether to immobilize the shares, such as by holding the bearer shares in custody. Where it is not practical to immobilize the bearer shares, the licensed corporation or associated entity may adopt measures such as obtaining a declaration from each substantial shareholder of the corporate customer on the percentage of his shareholding, requiring such substantial shareholders to provide a declaration on an annual basis and notify the licensed corporation or associated entity if the shares are sold, assigned or transferred.

6.4.7 Licensed corporations and associated entities also need to 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.

6.5 Listed companies and investment vehicles

6.5.1 Where a corporation is a company which is listed on a stock exchange in a FATF member jurisdiction or on a specified stock exchange as defined under the SFO[6], or is a subsidiary of such a listed company, or is a government-related corporation in a non-NCCT jurisdiction[7], the corporation itself can be regarded as the person whose identity is to be verified.

6.5.2 For customers mentioned in subsection 6.5.1 above, it will therefore be generally sufficient for a licensed corporation or an associated entity to obtain copies of relevant identification documents such as certificate of incorporation, business registration certificate and board resolution to open an account, without the need to make further enquiries about the identity of the substantial shareholders, individual directors or authorized signatories of the account. However, evidence that whoever operating the account has the necessary authority to do so should be sought and retained.

6.5.3 Where a listed corporation is effectively controlled by an individual or a small group of individuals, it is suggested that a licensed corporation or an associated entity consider whether it is necessary to verify the identity of such individual(s).

[7] Licensed corporations and associated entities should be satisfied that the risk of money laundering in the non-NCCT jurisdiction is low and there is no doubt as regards the ownership of the enterprise.

6.5.4 Where the customer is a regulated or registered investment vehicle, such as a collective investment scheme or mutual fund that is subject to adequate regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any unit holder of that entity.

6.5.5 Where the customer is an unregulated or unregistered investment vehicle, licensed corporations and associated entities should adhere to the requirements for identification and verification set out in subsections 6.4, 6.7 or 6.8 of this Guidance Note whichever is applicable, subject to subsection 6.5.6.

6.5.6 If the licensed corporation or associated entity is able to ascertain that:

(i) the unregulated or unregistered investment vehicle has in place an anti-money laundering and terrorist financing program; and

(ii) the person(s) (e.g. an administrator, a manager, etc) who is responsible for performing CDD procedures in relation to the investors in the investment vehicle has proper measures in place that are in compliance with FATF standards,

the licensed corporation or associated entity is not required to identify and verify the identity of the investors provided that the person(s) responsible for the CDD procedures is regulated and supervised by the Commission, Hong Kong Monetary Authority or Office of the Commissioner of Insurance or an equivalent authority in a jurisdiction that is a FATF member or an equivalent jurisdiction.

6.6 Financial or professional intermediaries

6.6.1 Where the account established in the name of a financial or professional intermediary is an omnibus account in order for that financial or professional intermediary to engage in securities, futures or leveraged foreign exchange transactions on behalf of its customers, a licensed corporation or an associated entity should conduct identification and verification of the omnibus account holder, i.e. the financial or professional intermediary that is the licensed corporation's or associated entity's customer in accordance with the provisions below, and is not required to "drill down" through the financial or professional intermediary to identify and verify the underlying customers for whom the

financial or professional intermediary performs financial transactions.

6.6.2 However, enhanced CDD procedures should be performed, subject to the exception in subsections 6.6.7 and 6.6.8 below. The enhanced procedures to be undertaken may include measures such as gathering sufficient information about the financial or professional intermediary to understand the nature of its business and to assess the regulatory and oversight regime of the country in relation to CDD standards in which the financial or professional intermediary is located[8].

6.6.3 Licensed corporations and associated entities may also refer to publicly available information to assess the professional reputation of the financial or professional intermediary.

6.6.4 Licensed corporations and associated entities should pay particular attention when maintaining an omnibus account with a financial or professional intermediary

(a) incorporated in NCCTs;

(b) in a jurisdiction in which it neither has a physical presence nor is affiliated with a regulated financial group that has such presence; or

(c) where it has not been established that the financial or professional intermediary has put in place reliable systems to verify customer identity,

and enhanced due diligence will generally be required in such cases to detect and prevent money laundering and terrorist financing. Licensed corporations and associated entities are encouraged to make reasonable enquiries about transactions passing through omnibus accounts that pose cause for concern or to report these transactions if any suspicion is aroused. If necessary, licensed corporations and associated entities should not permit the financial or professional intermediary to open or continue to maintain an omnibus account.

6.6.5 In particular, licensed corporations and associated entities should not establish or maintain an omnibus account for a financial

[8] In assessing the CDD standards of the financial or professional intermediary, licensed corporations and associated entities may consider to collect information such as its location of business, major business activities, management, authorization status, reputation (whether it has been subject to a money laundering or terrorist financing investigation or regulatory action), quality of supervision (system of regulation and supervision in its country in relation to CDD standards) and its anti-money laundering or terrorist financing controls. The factors listed above are not intended to be exhaustive and licensed corporations and associated entities may consider other factors as appropriate.

intermediary incorporated in a jurisdiction in which it neither has a physical presence nor is affiliated with a regulated financial group that has such presence unless after having undertaken the above enhanced procedures, they are satisfied that the financial or professional intermediary is subject to adequate regulatory supervision in relation to CDD standards under the regulation of the jurisdiction in which it is located.

6.6.6 Approval of senior management should be obtained before establishing a new omnibus account relationship. Licensed corporations and associated entities should preferably document[9] the respective responsibilities of each party.

6.6.7 When the omnibus account is established by:

(a) a financial intermediary that applies standards of anti-money laundering and terrorist financing based on the FATF Recommendations and is:

(i) authorized and supervised by the Commission, Hong Kong Monetary Authority or Office of the Commissioner of Insurance or an equivalent authority in a jurisdiction that is a FATF member or an equivalent jurisdiction; or

(ii) a trust company which is a subsidiary of a banking institution authorised and supervised by the Hong Kong Monetary Authority or an equivalent authority in a jurisdiction that is a FATF member or an equivalent jurisdiction; or

(b) a professional intermediary which is subject to a regulatory and supervisory regime that ensures the necessary anti-money laundering and terrorist financing measures have been effectively implemented and monitored in accordance with FATF standards,

the risk of money laundering and terrorist financing activity is considered lower and the application of simplified identification and verification procedures in relation to such accounts is appropriate.

6.6.8 For the categories of financial or professional intermediaries described above in subsection 6.6.7, it will generally be sufficient

[9] It is not necessary that the licensed corporation or associated entity and the financial or professional intermediary always have to set out their respective responsibilities in written form, provided there is a clear understanding as to which party will perform the required measures.

for a licensed corporation or associated entity to verify that the financial or professional intermediary or the parent banking institution (in the case of a trust company) is on the list of authorised and supervised institutions in the jurisdiction concerned or make enquiries of the relevant law society or accountancy body to establish whether the professional intermediary is registered with the relevant professional organisation and subject to a regulatory regime that ensures effective anti-money laundering and terrorist financing measures. Evidence that whoever representing the intermediary has the necessary authority to do so should be sought and retained.

6.6.9 However, for financial or professional intermediaries other than those mentioned in subsection 6.6.7, licensed corporations and associated entities shall follow the requirements for identification and verification set out in subsections 6.4 and 6.7 of this Guidance Note, whichever is applicable.

6.6.10 Where the account established by a financial or professional intermediary is for its own trading, a licensed corporation or associated entity should conduct identification and verification procedures consistent with those set out in subsections 6.6.8 and 6.6.9, whichever is applicable.

6.7 Unincorporated businesses

6.7.1 In the case of partnerships and other unincorporated businesses whose partners are not known to the licensed corporation or associated entity, licensed corporations and associated entities would need to obtain satisfactory evidence for the purpose of conducting CDD such as the identity of at least 2 partners, the identity of at least 2 authorized signatories and a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it in the case of a formal partnership arrangement.

6.7.2 Where the risk of money laundering or terrorist financing relating to the customer is assessed to be high, enhanced CDD should be performed; e.g. by verifying the identity of all partners and authorized signatories.

6.8 Trust and nominee accounts

6.8.1 Licensed corporations and associated entities should understand the relationship among the relevant parties in handling a trust or nominee account. There should be satisfactory evidence of the identity of the trustees or nominees and the persons on whose behalf they are acting.

6.8.2 For a trust account customer, licensed corporations and associated entities should take reasonable measures to understand the nature of the trust. Documents and information such as the following would be relevant for the purpose of conducting CDD:

(a) identity of trustees or person exercising effective control over the trust, protectors[10], settlors / grantors[11];

(b) identity of beneficiaries (as far as possible), though a broad description of the beneficiaries such as family members of an individual or employees of a pension scheme, where the scheme rules do not permit the assignment of a member 's interest under the scheme, may be accepted;

(c) copy of the trust deed or legal documents that evidence the existence and good standing of the legal arrangement.

6.8.3 Where the identity of beneficiaries has not previously been verified, licensed corporations and associated entities should make every effort, wherever possible, to identify and verify such beneficiaries on a risk-sensitive basis before effecting any transactions (such as making payment out of the trust account to the beneficiaries or on their behalf). Approval of senior management should preferably be obtained for a decision not to undertake such verification.

6.9 Politically exposed persons

6.9.1 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 a licensed corporation or an associated entity to particularly significant reputation or legal risks. There should be enhanced due diligence in respect of such politically exposed persons or PEPs.

6.9.2 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] Licensed corporations and associated entities may adopt a risk-based approach to determine whether it is necessary to verify the identity of protectors. 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.

[11] To the extent that the CDD process on the settlors / asset contributors has been adequately performed, licensed corporations and associated entities may accept a declaration from the trustee or other contractual party to confirm the link or relationship with the settlors / asset contributors.

6.9.3 The definition of PEP is not intended to cover middle ranking or more junior individuals in the foregoing categories. Licensed corporations and associated entities must however satisfy themselves that the criteria they use for classifying foreign politicians, government, judicial or military officials, etc as PEPs are sensitive to the risk of money laundering and terrorist financing.

6.9.4 Licensed corporations and associated entities should have appropriate risk management systems to determine whether the customer is a PEP (including making reference to publicly available information or commercially available databases). A risk-based approach may be adopted for identifying PEPs and especially on persons from countries that are generally considered to be of higher risk from a corruption point of view.

6.9.5 In the case when the licensed corporation or associated entity is considering establishing a relationship with a person that is suspected to be a PEP, it should identify that person fully, as well as people and companies that are clearly related to him. Licensed corporations and associated entities should ascertain the source of wealth and source of funds of customers and beneficial owners identified as PEPs before opening a customer account.

6.9.6 The decision to open an account for a PEP should be taken at a senior management level. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be or become a PEP, a licensed corporation or an associated entity should obtain senior management approval to continue the business relationship.

6.9.7 Risk factors that licensed corporations and associated entities should consider in handling a business relationship (or potential relationship) with a PEP include:

(a) any particular concern over the country where the PEP is from, 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) unexpected receipts of large sums from governmental bodies or government-related organizations;

(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-related bank or government accounts as the source of funds in a transaction.

6.10 Non face-to-face customers

6.10.1 Account opening using a non face-to-face approach refers to a situation where the customer is not interviewed and the signing of account opening documentation and sighting of identity documents of the customer is not conducted in the presence of an employee of a licensed corporation; e.g. where the account is opened via internet. If the account is opened using a non face-to-face approach, the account opening procedures should be one that satisfactorily ensures the identity of the customer.

6.10.2 Reference should be made to the relevant provisions in the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (the "Code") concerning account opening procedures using a non face-to-face approach. The signing of the client agreement and the sighting of the identity documents of the customer should be certified in such manner as provided in the Code (presently paragraph 5.1(a)). Alternatively, the identity of the customer (other than corporate entities), may be verified in accordance with such procedural steps as provided in the Code (presently, paragraph 5.1(b)).

6.10.3 Where a certifier is used to certify the signing of the client agreement and sighting of related identity documents, the licensed corporation or associated entity should ascertain whether the certifier is regulated and / or incorporated in, or operating from, a jurisdiction that is a FATF member or an equivalent jurisdiction.

6.10.4 Particular care should be taken when the signing of the customer agreement and sighting of related identity documents is witnessed by certifiers who are in a jurisdiction that is not a FATF member or an equivalent jurisdiction. In such circumstances, licensed corporations and associated entities are encouraged to assess the reliability of the documents, data or information certified by these professional persons and consider taking additional measures to mitigate the risk posed by such non face-to-face customers, including:

(a) independent contact with the customer by the licensed corporation or associated entity;

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

(c) more frequent information updates on non face-to-face customers;

(d) completion of on-line questionnaires for account opening applications that require a range of information capable of independent verification; or

(e) in extreme cases, refusal of business relationship without face-to-face contact for high risk customers.

6.11 Reliance on introducers for customer due diligence

6.11.1 This subsection refers to a third party which introduces customers to a licensed corporation or an associated entity. In practice, this often occurs through introduction made by another member of the same financial services group, or sometimes from another financial institution. This subsection does not apply to relationships, accounts or transactions between a licensed corporation or an associated entity and a financial or professional intermediary for its customers, i.e. omnibus accounts. Those relationships are addressed in subsection 6.6 of this Guidance Note.

6.11.2 The licensed corporation or associated entity may rely on the third party to perform elements (a) to (c) of the CDD measures in subsection 6.1.2 provided that criteria set out below are met. However, the ultimate responsibility for knowing the customer always remains with the licensed corporations and associated entities.

6.11.3 Prior to reliance, licensed corporations and associated entities must satisfy themselves that it is reasonable to rely on an introducer to apply a CDD process and that the CDD measures are as rigorous as those which the licensed corporation or associated entity would have conducted itself for the customer. For these purposes, it is advisable for licensed corporations and associated entities to establish clear policies in order to determine whether the introducer in question possesses an acceptable level of reliability.

6.11.4 Licensed corporations and associated entities relying upon an introducer should:

(a) as soon as reasonably practicable obtain the necessary information concerning elements (a) to (c) of the CDD measures in subsection 6.1.2 and the purpose and intended nature of the business relationship;

(b) as soon as reasonably practicable obtain copies of documentation pertaining to the customer's identity, as required under paragraph 6.2(a) of the Code (licensed corporations and associated entities may choose not to obtain copies of other relevant documentation provided that (a) has been satisfied and copies of the documentation will be provided by the introducer upon request without delay);

(c) take adequate steps to satisfy themselves that copies of other relevant documentation relating to the CDD requirements will be made available from the introducer upon request without delay, e.g. by establishing their respective responsibilities in writing, including reaching an agreement with the introducer that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the introducer upon request without delay and that the licensed corporation or associated entity will be permitted to verify the due diligence undertaken by the third party at any stage; and

(d) ensure the introducer is regulated and supervised for, and has measures in place to comply with CDD and record keeping requirements in line with FATF standards.

6.11.5 To provide additional assurance that these criteria can be met, it is advisable for a licensed corporation or an associated entity to rely, to the extent possible, on third parties which are incorporated in, or operating from, a jurisdiction that is a member of the FATF or an equivalent jurisdiction and:

(a) regulated by the Commission, Hong Kong Monetary Authority or Office of the Commissioner of Insurance or by an authority that performs similar functions; or

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

6.11.6 Licensed corporations and associated entities should consider conducting periodic reviews to ensure that an introducer 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 introducer and sample checks of the due diligence conducted.

6.11.7 Licensed corporations and associated entities should generally not rely on introducers based in jurisdictions considered as high risk, e.g. NCCTs or jurisdictions that are inadequately-regulated with respect to CDD unless the introducers are able to demonstrate that they have adequate procedures to prevent money laundering and terrorist financing.

7. Record Keeping

7.1 Licensed corporations and associated entities should ensure compliance with the record keeping requirements contained in the relevant legislation, rules or regulations of the Commission and of the relevant exchanges.

7.2 Licensed corporations and associated entities should maintain such records which are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

7.3 The investigating authorities require a satisfactory audit trail for investigating and tracing suspected drug related or other laundered money or terrorist property, and need to be able to reconstruct a financial profile of the suspect account. For these purposes, licensed corporations and associated entities should retain, where necessary, the following information for the accounts of their customers so as to provide evidence of criminal activity to the investigating authorities:

(a) the beneficial owner of the account;

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

(c) for individual transactions:

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

7.4 Licensed corporations and associated entities should ensure that all customer and transaction records and information are available on a

timely basis to the competent investigating authorities. Where appropriate, licensed corporations and associated entities should consider retaining in Hong Kong the above records for longer periods beyond the requirements of other relevant legislation, rules and regulations of the Commission or of the relevant exchanges.

8. Retention of Records

8.1 The following document retention terms should be observed:

(a) All necessary records on transactions, both domestic and international, should be maintained for at least seven years.

(b) Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence should be kept, wherever practicable, for at least five years after the account is closed.

8.2 In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

9. Recognition of Suspicious Transactions

9.1 For the purpose of compliance with this Guidance Note, a licensed corporation or an associated entity should conduct the necessary ongoing monitoring for identification of suspicious transactions in order to satisfy its legal obligations of reporting funds or property known or suspected by it to be proceeds of crime or terrorist property to the JFIU.

9.2 Depending on the size of the business of the licensed corporation or associated entity, it may sometimes be inadequate to rely simply on the initiative of front-line staff to identify and report suspicious transactions. In such circumstances, there may need to be systems or procedures in place, such as development of transaction reports, which can provide management 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, such as PEPs, omnibus accounts with financial institutions incorporated in NCCTs, etc.

9.3 The types of transactions which may be used by a money launderer and terrorist are virtually unlimited, thus it is difficult to specifically list out all types of transactions that might constitute a suspicious transaction. Suspicion may arise where a transaction is carried out for a purpose

inconsistent with a customer's known business or personal activities or with the normal business for that type of account. Therefore, the first step to recognition is to know enough about a customer's business and financial circumstances to recognize that a transaction, or series of transactions, is unusual.

9.4 To facilitate the identification of suspicious activity, an effective systemic approach to help identify suspicious financial activity recommended by the JFIU is provided in Appendix C(i). These methods of recognizing suspicious activities and approaches in the questioning of customers are given by way of example only. The timing and the extent of the questioning should depend on all circumstances in totality.

9.5 A list of potentially suspicious or unusual activities which shows the types of transactions that could be a cause of scrutiny is also provided in Appendix C(ii). The list is neither exhaustive nor does it take the place of any legal obligations related to the reporting of suspicious or unusual transactions imposed under the legislation. The list of characteristics should be taken into account by licensed corporations and associated entities along with other information (including any list of designated terrorists published in the Gazette, which can be found in the Government website http://www.gld.gov.hk/eng/services_2.htm), the nature of the transaction itself and the parties involved in the transaction. The existence of one or more of the factors described in the list may warrant some form of increased scrutiny of the transaction. However, the existence of one of these factors by itself does not necessarily mean that a transaction is suspicious or unusual.

9.6 In relation to terrorist financing, the FATF issued a paper in April 2002 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 activities in the past. A licensed corporation or an associated entity is advised to acquaint itself with the FATF paper[12].

9.7 Licensed corporations and associated entities should have in place an effective procedure to promptly identify terrorist suspects specified in Gazette notices or other lists that have been made known to them (e.g. lists designated under the US President's Executive Order 13224 on blocking of terrorist property which can be found on the United States Department of the Treasury website[13] and lists referred to in the

[12] The FATF paper is available on the FATF website www.fatf-gafi.org/dataoecd/39/21/34033955.pdf.

[13] Lists designated under the US President's Executive Order can be found on the United States Department of the Treasury website at www.ustreas.gov/offices/enforcement/ofac/sanctions/terrorism.html.

circulars issued by the Commission [14]). To this end, licensed corporations and associated entities should consider consolidating the various lists into a single database for facilitating access by staff for the purpose of identifying suspicious transactions. They should check the names of both existing customers and applications for business relationship against the terrorist suspects specified as above. They should be particularly alert for suspicious remittances and should bear in mind the role which non-profit organizations are known to have played in terrorist financing. Enhanced checks should be completed before processing a transaction, where possible, if there are circumstances giving rise to suspicion.

10. Reporting of Suspicious Transactions

10.1 The obligation to report under the DTROP, the OSCO or the UNATMO rests with the individual who becomes suspicious of a person, transaction or property. Disclosures of suspicious transactions under the DTROP, the OSCO or the UNATMO should be made to the JFIU. In addition to acting as the point for receipt of disclosures made by any organization or individual, the JFIU functions as the local and international advisor on money laundering matters generally and can offer practical assistance to the financial sector on the subject of money laundering and terrorist financing.

10.2 An officer responsible for compliance function (hereinafter referred to as "compliance officer") within a licensed corporation or an associated entity should be appointed to act as a central reference point within the organization to facilitate onward reporting to the JFIU. The role of the compliance officer is not simply that of a passive recipient of ad hoc reports of suspicious transactions, but rather, he or she plays an active role in the identification and reporting of suspicious transactions, which may involve regular review of exception reports of large or irregular transactions generated by licensed corporations' or associated entities' internal system as well as ad hoc reports made by front-line staff. Depending on the organization structure of the licensed corporation or associated entity, the specific task of reviewing reports may be delegated to other staff but the compliance officer or the supervisory management should maintain oversight of the review process.

10.3 In circumstances where a staff member of a licensed corporation or an associated entity brings a transaction to the attention of the compliance officer, the circumstances of each case can then be reviewed at that level to determine whether the suspicion is justified. 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.

[14] These circulars can be found on the Securities and Futures Commission's website at www.sfc.hk/sfc/html/EN/intermediaries/supervision/supervision.html.

Suspicious transactions should be reported regardless of whether they are also thought to involve tax matters. The fact that a report may have already 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. If the suspicion remains, the transaction should be reported to the JFIU without delay.

10.4 Where it is known or suspected that a report has already been disclosed to the JFIU 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.

10.5 The use of a standard format for reporting is encouraged (see Appendix D). In the event that urgent disclosure is required, an initial notification should be made by telephone. The contact details of the JFIU are set out at Appendix F.

10.6 Register(s) of all reports made to the JFIU and all reports made by employees to management should be kept, including those where a decision is made by management not to report to the JFIU. Licensed corporations and associated entities, their directors, officers and employees should not warn their customers when information relating to them is being reported to an authorized officer (e.g. the JFIU), as such action may constitute an offence.

10.7 The JFIU will acknowledge receipt of any disclosure made. If there is no immediate need for action e.g. the issue of a restraint order in relation to an account, consent will usually be given for the licensed corporation or associated entity to operate the account under the provisions of section 25A(2) of the DTROP, or section 25A(2) of the OSCO, or section 12(2) of the UNATMO, as the case may be. An example of such a letter is shown at Appendix E.

10.8 Following the receipt and consideration of a disclosure by the JFIU, the information disclosed will be allocated to trained financial investigation officers in the Police and the Customs and Excise Department for further investigation.

10.9 Access to the disclosed information is restricted to the relevant financial investigating officers within the Police and the Customs and Excise Department. In the event of a prosecution, production orders will be obtained to produce the material at court. Section 26 of the DTROP and the OSCO place strict restrictions on revealing the identity of the person making a disclosure under section 25A.

10.10 The Police and Customs and Excise Department and the JFIU are not obliged to, but may, on request, provide a status report on the disclosure to a disclosing licensed corporation or an associated entity.

10.11 Enhancing and maintaining the integrity of the relationship which has been established between law enforcement agencies and licensed corporations/associated entities is considered to be of paramount importance.

11. Staff Screening, Education and Training

11.1 For the purpose of compliance with this Guidance Note, licensed corporations and associated entities should take such measures for screening and training employees that are appropriate having regard to the risk of money laundering and terrorist financing and the size of their business.

11.2 Licensed corporations and associated entities should identify the key positions under their own organizational structures with respect to anti-money laundering and anti-terrorist financing and should ensure that all employees taking up such key positions are suitable and competent to perform their duties.

11.3 Licensed corporations and associated entities must provide proper anti-money laundering and anti-terrorist financing training to their local and overseas staff members.

11.4 Members of staff should be aware of their own personal obligations under the DTROP, the OSCO and the UNATMO and that they can be personally liable should they fail to report information as required. They are advised to read the relevant sections of the DTROP, the OSCO and the UNATMO. Members of staff must be encouraged to co-operate fully with the JFIU and to disclose suspicious transactions promptly. If in doubt, they should contact the JFIU.

11.5 Licensed corporations and associated entities should have educational programmes in place for training all new employees.

11.6 It is also necessary to make arrangements for refresher training at regular intervals to ensure that members of staff, in particular those who deal with the public directly and help customers open new accounts, and those who supervise or manage such staff members, do not forget their responsibilities.

Appendix A: Summary Of Legislation Concerned With Money Laundering And Terrorist Financing

1 The Drug Trafficking (Recovery of Proceeds) Ordinance ("DTROP")

1.1 The DTROP contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction.

1.2 Under section 25(1) of the DTROP, a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking. "Dealing" in relation to property referred to in the definition of "drug trafficking", the award of a restraint order under section 10, or the offence under section 25, includes:-

(a) receiving or acquiring the property;

(b) concealing or disguising the property (whether by concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it or otherwise);

(c) disposing of or converting the property;

(d) bringing the property into or removing it from Hong Kong;

(e) using the property to borrow money, or as security (whether by way of charge, mortgage or pledge or otherwise).

The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine of $5 million. A person has a defence to an offence under section 25(1) if he intended to make a disclosure under section 25A and there is a reasonable excuse for his failure to do so.

1.3 Under section 25A of the DTROP where a person knows or suspects that any property,

(a) directly or indirectly, represents a person's proceeds of,

(b) was used in connection with, or

(c) is intended to be used in connection with,

drug trafficking, he shall disclose that knowledge or suspicion to an authorized officer as soon as it is reasonable for him to do so. "Authorized officer" includes any police officer, any member of the Customs and Excise Department, and the JFIU. The JFIU, established in 1989 is operated by the Police and Customs and Excise Department. Section 25A(4) of the DTROP provides that a person who is in employment can make disclosure to the appropriate person in accordance with the procedures established by his employer for making such disclosures (see also section 10 of this Guidance Note). To the employee, such disclosure has the effect of disclosing the knowledge or suspicion to an authorized person as required under section 25A(1). Failure to make a disclosure under section 25A is an offence, the maximum penalty upon conviction of which is a fine of HK$50,000 and imprisonment for 3 months.

1.4 Section 25A(2) of the DTROP provides that if a person who has made a disclosure under section 25A(1) does any act in contravention of section 25(1) before or after the disclosure, and the disclosure relates to that act, the person does not commit an offence under section 25(1) if:-

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

(b) the disclosure is made after he does that act, is made on his own initiative and is made as soon as it is reasonable for him to make it.

1.5 Under section 25A(5) of the DTROP, it is an offence if a person who knows or suspects that a disclosure has been made under section 25A(1) or (4) discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following the disclosure under section 25A(1) or (4). The maximum penalty upon conviction of this offence is a fine of $500,000 and imprisonment for 3 years.

1.6 Section 25A(3)(a) provides that a disclosure made under the DTROP shall not be treated as a breach of any restriction upon

the disclosure of information imposed by contract or by enactment, rules of conduct or other provision. Section 25A(3)(b) provides that the person making the disclosure shall not be liable for damages for any loss arising out of the disclosure or any act done or omitted to be done in relation to the property concerned in consequence of the disclosure.

1.7 Licensed corporations and associated entities may receive restraint orders and charging orders on the property of a defendant of a drug trafficking offence. These orders are issued under sections 10 and 11 of the DTROP. On service of these orders, an authorized officer may require a person to deliver documents or information that may assist in determining the value of the property. Failure to provide the documents or information as soon as practicable is an offence under section 10 or 11 of DTROP. Moreover, any person who deals in the property in contravention of a restraint order or a charging order commits an offence under DTROP.

1.8 Section 26 of the DTROP provides that no witness in any civil or criminal proceedings shall be obliged to reveal the making of a disclosure nor to reveal the identity of the person making the disclosure except in proceedings for an offence under section 25, 25A or 26 of the DTROP, or where the court is of the opinion that justice cannot fully be done between the parties without revealing the disclosure or the identity of the person making the disclosure.

2 The Organized and Serious Crimes Ordinance ("OSCO")

2.1 The OSCO, among other things:

(a) gives officers of the Police and the Customs and Excise Department powers to investigate organized crime and triad activities;

(b) gives the Courts jurisdiction to confiscate the proceeds of organized and serious crimes, to issue restraint orders and charging orders in relation to the property of a defendant of an offence specified in the OSCO;

(c) creates an offence of money laundering in relation to the proceeds of indictable offences; and

(d) enables the Courts, under appropriate circumstances, to receive information about an offender and an offence in order to determine whether the imposition of a greater sentence is appropriate where the offence amounts to an organized crime/triad related offence or other serious offences.

The term "organized crime" is defined widely in OSCO. To put it simply, it means an offence listed in Schedule 1 to the OSCO that is either connected with the activities of a particular triad society, or is committed by two or more persons that involves substantial planning and organization. The offences that are listed in Schedule 1 include murder, kidnapping, drug trafficking, assault, rape, theft, robbery, obtaining property by deception, false accounting, firearms offences, manslaughter, bribery and smuggling.

2.2 Sections 3 to 5 of the OSCO provide that an authorized officer (including the Police), for the purpose of investigating an organized crime, may apply to the Court of First Instance for an order to require a person to provide information or produce material that reasonably appears to be relevant to the investigation. The Court may make an order that the person make available the material to an authorized officer. An authorized officer may also apply for a search warrant under the OSCO. A person cannot refuse to furnish information or produce material under sections 3 and 4 of the OSCO on the ground of self-incrimination or breach of an obligation to secrecy or other restriction on the disclosure of information imposed by statute or other rules or regulations.

2.3 Sections 25, 25A and 26 of the OSCO are modelled upon sections 25, 25A and 26 of the DTROP. In summary, under section 25(1) of the OSCO a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent the proceeds of an indictable offence. "Dealing" in relation to property referred to in this section includes:-

(a) receiving or acquiring the property;

(b) concealing or disguising the property (whether by concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it or otherwise);

(c) disposing of or converting the property;

(d) bringing the property into or removing it from Hong Kong;

(e) using the property to borrow money, or as a security (whether by way of charge, mortgage or pledge or otherwise).

The maximum penalty upon conviction of an offence under section 25 is a fine of $5 million and imprisonment for 14 years. A person has a defence to an offence under 25(1) if he intended to make a disclosure under section 25A and there is a reasonable excuse for his failure to disclose.

2.4 Under section 25A of the OSCO where a person knows or suspects that any property,

(a) directly or indirectly, represents a person's proceeds of,

(b) was used in connection with, or

(c) is intended to be used in connection with,

an indictable offence, he shall disclose that knowledge or suspicion to an authorized officer as soon as it is reasonable for him to do so. Failure to make a disclosure under this section constitutes an offence. Where a person is employed at the relevant time, disclosure may be made to the appropriate person in accordance with the procedure established by his employer for the making of such disclosures. The maximum penalty upon conviction of this offence is a fine of HK$50,000 and imprisonment for 3 months.

2.5 Section 25A(2) of the OSCO provides that if a person who has made a disclosure under section 25A(1) does any act in contravention of section 25(1) before or after the disclosure, and the disclosure relates to that act, the person does not commit an offence under section 25(1) if:-

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

(b) the disclosure is made after he does that act, is made on his own initiative and is made as soon as it is reasonable for him to make it.

2.6 Under section 25A(5) of the OSCO, it is an offence if a person who knows or suspects that a disclosure has been made under section 25A(1) or (4) discloses to another person any matter which is likely to prejudice any investigation which might be conducted following the disclosure under section 25A(1) or (4). The maximum penalty upon conviction of this offence is a fine of $500,000 and imprisonment for 3 years.

2.7 Section 25A(3)(a) of the OSCO provides that a disclosure made under the OSCO shall not be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, rules of conduct or other provision. Section 25A(3)(b) provides that the person making the disclosure shall not be liable for damages for any loss arising out of the disclosure or any act done or omitted to be done in relation to the property concerned in consequence of the disclosure.

2.8 Licensed corporations and associated entities may receive restraint orders and charging orders on the property of a defendant of an offence specified in OSCO. These orders are issued under sections 15 and 16 of the OSCO. On service of these orders, an authorized officer may require a person to deliver documents or information that may assist in determining the value of the property. Failure to provide the information as soon as practicable is an offence under section 15 or 16 of the OSCO. Moreover, any person who deals in a piece of property in contravention of a restraint order or a charging order commits an offence under the OSCO.

2.9 Section 26 of the OSCO provides that no witness in any civil or criminal proceedings shall be obliged to reveal the making of a disclosure or to reveal the identity of the person making the disclosure except in proceedings for an offence under section 25, 25A or 26 of the OSCO, or where the court is of the opinion that justice cannot fully be done between the parties without revealing the disclosure or the identity of the person making the disclosure.

3 The United Nations (Anti-Terrorism Measures) Ordinance ("UNATMO")

3.1 The UNATMO was enacted in July 2002 and a substantial part of the law came into operation on 23 August 2002. The UNATMO is principally directed towards implementing decisions contained in Resolution 1373 dated 28 September 2001 of the United Nations Security Council ("UNSC") aimed at preventing the financing of terrorist acts. Previously, the UNSC had passed various other resolutions imposing sanctions against certain designated terrorists and terrorist organizations. Regulations issued under the United Nations Sanctions Ordinance (Cap.537) give effect to these UNSC resolutions. In particular, the United Nations Sanctions (Afghanistan) Regulation and the United Nations Sanctions (Afghanistan) (Amendment) Regulation provide, among others, for a prohibition on making funds available to designated terrorists. The UNATMO is directed towards all terrorists.

3.2 In June 2004, the United Nations (Anti-Terrorism Measures) (Amendment) Bill was passed and a substantial part of the United Nations (Anti-Terrorism Measures) (Amendment) Ordinance 2004 has come into operation in January 2005.

3.3 Besides the mandatory elements of the UNSC Resolution 1373, the UNATMO as amended by the United Nations (Anti-Terrorism Measures) (Amendment) Ordinance 2004 ("amended UNATMO") also implements the more pressing elements of the FATF's special recommendations on terrorist financing. The amended UNATMO, among other things, criminalizes the provision or collection of funds and making funds or financial (or related) services available to terrorists or terrorist associates. It permits terrorist property to be frozen and subsequently forfeited. Section 12(1) of the amended UNATMO also requires a person to report his knowledge or suspicion of terrorist property to an authorized officer, which includes a police officer, a member of the Customs and Excise Service/ Immigration Service and an officer of the Independent Commission Against Corruption as specified in the amended UNATMO. Failure to make a disclosure under this section constitutes an offence. The maximum penalty upon conviction of this offence is a fine of HK$50,000 and imprisonment for 3 months.

3.4 The term “funds” includes funds mentioned in the Schedule 1 of the amended UNATMO. It covers cash, cheques, deposits with financial institutions or other entities, balances on accounts, securities and debt instruments (including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures, debenture stock and derivatives contracts), interest, dividends or other income on or value accruing from or generated by property, documents evidencing an interest in funds or financial resources, etc.

3.5 “Terrorist” means a person who commits, or attempts to commit, a terrorist act or who participates in or facilitates the commission of a terrorist act. “Terrorist associate” means an entity owned or controlled, directly or indirectly, by a terrorist. The term “terrorist act” is defined as the use or threat of action where the action is carried out with the intention of, or the threat is made with the intention of using action that would have the effect of:

(a) causing serious violence against a person;

(b) causing serious damage to property;

(c) endangering a person’s life, other than that of the person committing the action;

(d) creating a serious risk to the health or safety of the public or a section of the public;

(e) seriously interfering with or seriously disrupting an electronic system; or

(f) seriously interfering with or seriously disrupting an essential service, facility or system, whether public or private; and

the use or threat is:

(i) intended to compel the Government or to intimidate the public or a section of the public; and
(ii) made for the purpose of advancing a political, religious or ideological cause.

In the case of paragraphs (d), (e) and (f) above, a "terrorist act" does not include the use or threat of action in the course of any advocacy, protest, dissent or industrial action.

3.6 A list of designated terrorists, terrorist associates and terrorist properties is published in the Gazette from time to time pursuant to section 10 of the United Nations Sanctions (Afghanistan) Regulation and section 4 of the amended UNATMO. The published lists reflect designations made by the UN Committee that was established pursuant to UNSC Resolution 1267. The amended UNATMO provides that it shall be presumed, in the absence of evidence to the contrary, that a person specified in such a list is a terrorist or a terrorist associate (as the case may be).

3.7 As regards the obligations under section 12(1) of the amended UNATMO to disclose knowledge or suspicion that property is terrorist property, it should be noted that if a person who has made such a disclosure does any act in contravention of section 7 or 8 of the amended UNATMO (on the provision or collection of funds or making funds or financial (or related) services available to terrorists and their associates) before or after such disclosure and the disclosure relates to that act, the person does not commit an offence if :-

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

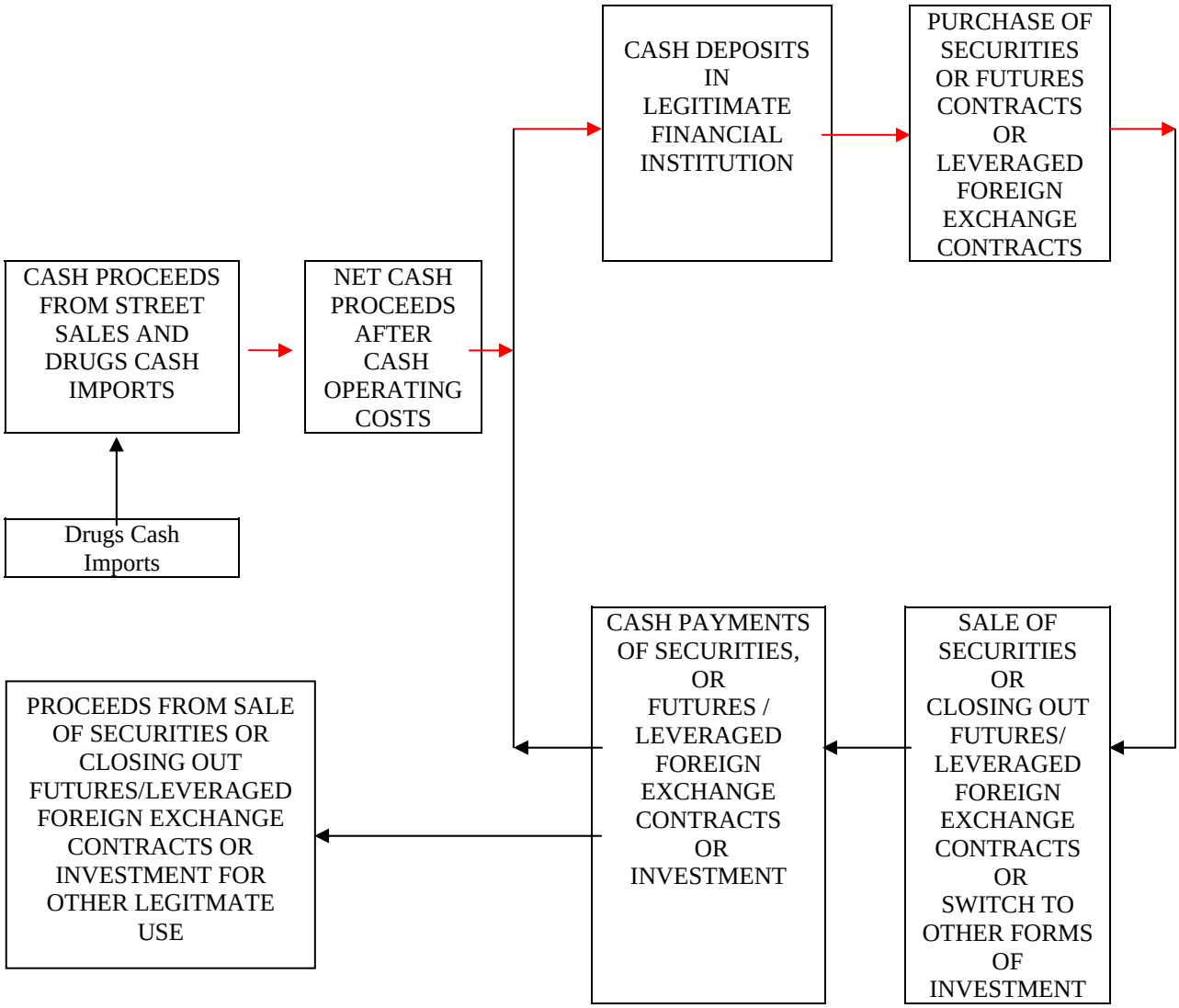
(b) the disclosure is made after he does that act, is made on his own initiative and is made as soon as it is practicable for him to make it.

3.8 Section 12(3) provides that a disclosure made under the amended UNATMO shall not be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, rules of conduct or other provision. The person making the disclosure shall not be liable in damages for any loss arising out of the disclosure or any act done or omitted to be done in relation to the property concerned in consequence of the disclosure.

3.9 Section 12(6) of the amended UNATMO permits information obtained from section 12(1) by an authorized officer to be disclosed to certain authorities (i.e. the Department of Justice, the Police, etc.) and overseas authorities, responsible for

investigating or preventing and suppressing the financing of terrorist acts.

Appendix B: Laundering Of Proceeds



Other examples of money laundering methods and characteristics of financial transactions that have been linked with terrorist financing can be found on the websites of the JFIU (www.jfiu.gov.hk) and FATF (www.fatf-gafi.org).

Appendix C(i): A Systemic Approach To Identifying Suspicious Transactions Recommended By The JFIU

An effective systemic approach to the identification of suspicious financial activity involves the following four steps.

(a) **Step one**: Recognition of a suspicious financial activity indicator or indicators.

(b) **Step two**: Appropriate questioning of the customer.

(c) **Step three**: Review of information already known about the customer in deciding if the apparently suspicious activity is to be expected from the customer.

(d) **Step four**: Consideration of (a), (b) and (c) above to make a subjective decision on whether the customer's financial activity is genuinely suspicious or not.

Examination of the Suspicious Transactions Reporting ("STR") received by the JFIU reveals that many reporting institutions do not use the system outlined above. Commonly, institutions make a STR merely because a suspicious activity indicator has been recognized, i.e. only step (a) of the systemic approach is followed, steps (b), (c) and (d) are not followed. This failure to use the systemic approach leads to a lower quality of STRs.

Each of the four steps of the systemic approach to suspicious activity identification is discussed in more detail in the following paragraphs. Some of these suggested measures and procedures may not be applicable in all circumstances. Each licensed corporation or associated entity should consider carefully the specific nature of its business, organisational structure, type of customer and transaction, etc. when designing its own systems for implementing the respective steps.

Step One: Recognition of a Suspicious Financial Activity Indicator or Indicators

The recognition of an indicator, or better still indicators, of suspicious financial activity is the first step in the suspicious activity identification system. A list of suspicious activity indicators commonly seen within Hong Kong's securities sector is attached at Appendix C(ii).

Additional methods of monitoring customer activity for indicators of suspicious activity are also necessary.

The measures summarized below are recognized as contributing towards an effective overall approach to suspicious activity identification.

(a) Train and maintain awareness levels of all members of staff in suspicious activity identification.

This approach is most effective in situations in which members of staff have face-to-face contact with a customer who carries out a particular transaction which displays suspicious activity indicators. However, this approach is much less effective in situations in which either, there was no face-to-face contact between customer and member of staff, or the customer dealt with different members of staff to carry out a series of transactions which are not suspicious if considered individually.

(b) Identification of areas in which staff member/customer face-to-face contact is lacking (e.g. internet trading) and use of additional methods for suspicious activity identification in these areas.

(c) Use of a computer program to identify accounts showing activity which fulfils predetermined criteria based on commonly seen money laundering methods.

(d) Trend Monitoring. A computer program which monitors the turnover of money within an account and notes the rolling average turnover per month for the preceding recent months. The current month's turnover is then compared with the average turnover. The current month's activity is regarded as suspicious if it is significantly larger than the average.

(e) Firms' internal inspection system to include inspection of suspicious activity reporting.

(f) Identification of "High Risk" accounts, i.e. accounts of the type which are commonly used for money laundering, e.g. remittance agencies, money changers, casinos, accounts with members of staff of secretarial companies as authorized signatories, accounts of "shelf" companies, and law company customer accounts. Greater attention is paid to monitoring of the activity of these accounts for suspicious transactions.

(g) Flagging of accounts of special interest on the firm computer. Members of staff carrying out future transactions will notice the "flag" on their computer screen and pay extra attention to the transactions conducted on the account. Accounts to be flagged

are those in respect of which a suspicious transaction report has been made and/or accounts of high risk businesses (see (f) above).

A problem with flagging is that members of staff who come across a large transaction involving a flagged account may tend to make a report to the compliance officer whether or not the transaction is suspicious. This has the effect of overburdening compliance officers with low quality reports. Flagging may also lead to members of staff believing that if an account is not flagged it is not suspicious. Members of staff must be educated on the proper usage of flagging if it is to work properly.

(h) Use of "Exception Report", "Unusual Report", or "High Activity Report", to identify accounts with high levels of activity, followed by consideration of whether the activity is suspicious. Although these reports can be useful in identifying suspicious activity, they are not designed for this function and may not therefore be very effective, e.g. in order to keep the number of reports to be viewed daily at a manageable level, a daily threshold may be set which is higher than sums commonly laundered, and therefore ineffective for suspicious activity identification.

(i) Adopt more stringent policies in respect of customers who are expected to deal in large sums, e.g. request corporate customers for the expected nature of transactions and source of funds when opening such accounts.

Step Two: Appropriate Questioning of the Customer

If members of staff of a licensed corporation or an associated entity receive instructions to carry out a transaction or transactions, bearing one or more suspicious activity indicators, then they should question the customer on the reason for conducting the transaction and the identity of the source and ultimate beneficiary of the money being transacted. Members of staff should consider whether the customer's story amounts to a reasonable and legitimate explanation of the financial activity observed. If not, then the customer's activity should be regarded as suspicious and a suspicious transaction report should be made to the JFIU.

On occasions staff members of financial institutions have expressed reluctance to ask questions of the type mentioned above. Grounds for this reluctance are that the customer may realize that he, or she, is suspected of illegal activity, or regards such questions as none of the questioner's business. In either scenario the customer may be offended

or become defensive and uncooperative, or even take his, or her, business elsewhere. This is a genuine concern but can be overcome by members of staff asking questions which are apparently in furtherance of promoting the services of the licensed corporation or associated entity or satisfying customer needs, but which will solicit replies to the questions above without putting the customer on his, or her, guard.

Appropriate questions to ask in order to obtain an explanation of the reason for conducting a transaction bearing suspicious activity indicators will depend upon the circumstances of the financial activity observed. For example, if a customer wishes to make a large cash transaction then staff member can ask the customer the reason for using cash on the grounds that the staff member may be able to offer advice on a more secure method to perform the transaction.

Persons engaged in legitimate business generally have no objection to, or hesitation in answering such questions. Persons involved in illegal activity are more likely to refuse to answer, give only a partial explanation or give an explanation which is unlikely to be true.

If a customer is unwilling, or refuses, to answer questions or gives replies which members of staff suspect are incorrect or untrue, this may be taken as a further indication of the suspicious nature of the financial activity.

Step Three: Review of Information Already Known to the Licensed Corporation or Associated Entity when Deciding if the Apparently Suspicious Activity is to be Expected

The third stage in the systemic approach to suspicious activity identification is to review the information already known to the licensed corporation or associated entity about the customer and his, or her, previous financial activity and consider this information to decide if the apparently suspicious activity is to be expected from the customer. This stage is commonly known as the "know your customer principle".

Licensed corporations and, where applicable, associated entities hold various pieces of information on their customers which can be useful when considering if the customers' financial activity is to be expected or is unusual. Examples of some of these information items and the conclusions which may be drawn from them are listed below.

(a) The customers' occupation. Certain occupations imply the customer is a low wage earner e.g. driver, hawker, waiter, student. High value of transactions on the accounts of such customers would not therefore be expected.

(b) The customers' residential address. A residential address in low cost housing, e.g. public housing, may be indicative of a low wage earner.

(c) The customers' age. As neither very young nor very old persons tend to be involved in frequent high value transactions, such activity by a very young or old customer would not be expected.

(d) The average balance and the number and type of transactions seen on an account over a period of time give an indication of the financial activity which is normal for the customer. Markedly increased activity or activity of a different type to these norms would therefore be considered to be unusual.

Step Four: Is the Financial Activity Suspicious?

The final step in the suspicious activity identification system is the decision whether or not to make a STR. Due to the fact that suspicion is difficult to quantify, it is not possible to give exact guidelines on the circumstances in which a STR should, or should not, be made. However, such a decision will be of the highest quality when all the relevant circumstances are known to, and considered by, the decision maker, i.e. when all three of the preceding steps in the suspicious transaction identification system have been completed and are considered. If, having considered all the circumstances, members of staff find the activity genuinely suspicious then an STR should be made.

Appendix C(ii): Examples of Suspicious Transactions

Money laundering using investment related transactions

(a) Large or unusual settlements of transactions in cash or bearer form.

(b) Buying and selling of securities/futures with no discernible purpose or in circumstances which appear unusual.

(c) A number of transactions by the same counterparty in small amounts relating to the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account.

(d) Any transaction in which the counterparty to the transaction is unknown or where the nature, size or frequency appears unusual.

(e) Investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking may be prevalent.

(f) The use by a customer of a licensed corporation or an associated entity to hold funds that are not being used to trade in securities, futures contracts or leveraged foreign exchange contracts.

(g) A customer who deals with a licensed corporation or an associated entity only in cash or cash equivalents rather than through banking channels.

(h) The entry of matching buys and sells in particular securities or futures or leveraged foreign exchange contracts ("wash trading"), creating the illusion of trading. Such wash trading does not result in a bona fide market position, and might provide "cover" for a money launderer.

(i) Wash trading through multiple accounts might be used to transfer funds between accounts by generating offsetting losses and profits in different accounts. Transfers of positions between accounts that do not appear to be commonly controlled also could be a warning sign. (It should be noted that wash trading is also an indication of market manipulation and licensed corporations or registered persons are expected to take appropriate steps to ensure that proper safeguards exist to prevent the firm from acting in a way which would result in the firm perpetrating any conduct which constitutes market misconduct under section 279 of the SFO).

(j) Frequent funds transfers or cheque payments to or from unverified or difficult to verify third parties.

(k) The involvement of offshore companies on whose accounts multiple transfers are made, especially when they are destined for a tax haven, and to accounts in the name of companies incorporated under foreign law of which the customer may be a shareholder.

(l) Non-resident account with very large movement with subsequent fund transfers to offshore financial centres.

Money laundering involving employees of licensed corporations and associated entities

(a) Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.

(b) Changes in employee or agent performance, e.g. the salesman selling products for cash has remarkable or unexpected increase in performance.

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

(d) The use of an address which is not the customer's permanent address, e.g. utilisation of the representative's office or home address for the dispatch of customer documentation.

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

Appendix D: Report Made to the JFIU

REPORT MADE UNDER SECTION 25A OF THE DRUG TRAFFICKING (RECOVERY OF PROCEEDS) ORDINANCE OR ORGANIZED AND SERIOUS CRIMES ORDINANCE, OR SECTION 12 OF THE UNITED NATIONS (ANTI-TERRORISM MEASURES) ORDINANCE TO THE JOINT FINANCIAL INTELLIGENCE UNIT ("JFIU)		
NAME AND ADDRESS OF LICENSED CORPORATION OR ASSOCIATED ENTITY		
SUSPICIOUS ACCOUNT NAME(S) (IN FULL)		
DATE OF ACCOUNT OPENING		DATE OF BIRTH / DATE OF INCORPORATION (IN THE CASE OF A CORPORATE CUSTOMER)
OCCUPATION & EMPLOYER / NATURE OF BUSINESS (IN THE CASE OF A CORPORATE CUSTOMER)		
NATIONALITY / PLACE OF INCORPORATION (IN THE CASE OF A CORPORATE CUSTOMER)		HKID NUMBER / PASSPORT NUMBER/ BUSINESS REG. NO. (IN THE CASE OF A CORPORATE CUSTOMER)
ADDRESS OF ACCOUNT HOLDER		
DETAILS OF TRANSACTION/ PROPERTY AROUSING SUSPICION AND ANY OTHER RELEVANT INFORMATION. PLEASE ALSO ENCLOSE A COPY OF THE TRANSACTION AND ACCOUNT STATEMENT FOR REFERENCE. PARTICULARS OF ACCOUNT HOLDER OR PERSON CONDUCTING THE TRANSACTION ARE TO BE GIVEN IN A SEPARATE SHEET		
REPORTING OFFICER/TEL.NO.	SIGNATURE / DATE	ENTERED RECORDS

Appendix E: Sample Acknowledgement Letter from the JFIU

Date:

Your ref:

Mr.
ABC Brokerage Ltd
XXXX
Hong Kong

Dear Sir,

Drug Trafficking (Recovery of Proceeds) Ordinance
Organized and Serious Crimes Ordinance
United Nations (Anti-Terrorism Measures) Ordinance

I refer to your disclosure made to the JFIU on DD/MM/YY under the above references.

I acknowledge receipt of the information supplied by you under the provisions of Section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance Cap.405 and the Organized and Serious Crimes Ordinance Cap.455 / Section 12 of the United Nations (Anti-Terrorism Measures) Ordinance Cap.575.

Based upon the information currently available, consent is given for you to continue to operate the account(s) in accordance with normal securities/futures/leveraged foreign exchange practice under the provisions of the Ordinance(s).

Thank you for your co-operation.

Yours faithfully,

Joint Financial Intelligence Unit

Appendix F: JFIU Contact Details

Written reports should be sent to the JFIU at either the address, fax number, e-mail or PO Box listed below:

Joint Financial Intelligence Unit,
16/F, Arsenal House West Wing,
Hong Kong Police Headquarters,
Arsenal Street,
Hong Kong.

or GPO Box 6555
Hong Kong Post Office,
Hong Kong.

Fax : 2529-4013

E-mail : jfiu@police.gov.hk

Urgent reports should be made either by fax, e-mail or by telephone to 2860-3413 or 2866-3366.

STATUTORY INSTRUMENTS

2007 No. 2157

FINANCIAL SERVICES

The Money Laundering Regulations 2007

Made - - - -	*24th July 2007*
Laid before Parliament	*25th July 2007*
Coming into force - -	*15th December 2007*

The Treasury are a government department designated(**a**) for the purposes of section 2(2) of the European Communities Act 1972(**b**) in relation to measures relating to preventing the use of the financial system for the purpose of money laundering;

The Treasury, in exercise of the powers conferred on them by section 2(2) of the European Communities Act 1972 and by sections 168(4)(b), 402(1)(b), 417(1)(**c**) and 428(3) of the Financial Services and Markets Act 2000(**d**), make the following Regulations:

PART 1

GENERAL

Citation, commencement etc.

1.—(1) These Regulations may be cited as the Money Laundering Regulations 2007 and come into force on 15th December 2007.

(2) These Regulations are prescribed for the purposes of sections 168(4)(b) (appointment of persons to carry out investigations in particular cases) and 402(1)(b) (power of the Authority to institute proceedings for certain other offences) of the 2000 Act.

(a) S.I. 1992/1711.

(b) 1972 c. 68; section 2(2) was amended by section 27 of the Legislative and Regulatory Reform Act 2006 (c.51). By virtue of the amendment of section 1(2) made by section 1 of the European Economic Area Act 1993 (c.51) regulations may be made under section 2(2) to implement obligations of the United Kingdom created by or arising under the Agreement on the European Economic Area signed at Oporto on 2nd May 1992 (Cm 2073, OJ No L 1, 3.11.1994, p. 3) and the Protocol adjusting that Agreement signed at Brussels on 17th March 1993 (Cm 2183, OJ No L 1, 3.1.1994, p.572). For the decision of the EEA Joint Committee in relation to Directive 2005/60/EC, see Decision No 87/2006 of 7th July 2006 amending Annex IX (Financial Services) to the EEA Agreement (OJ No L 289 19.10.2006, p. 23).

(c) See the definition of "prescribed".

(d) 2000 c. 8.

(3) The Money Laundering Regulations 2003(**e**) are revoked.

Interpretation

2.—(1) In these Regulations—

"the 2000 Act" means the Financial Services and Markets Act 2000;

"Annex I financial institution" has the meaning given by regulation 22(1);

"auditor", except in regulation 17(2)(c) and (d), has the meaning given by regulation 3(4) and (5);

"authorised person" means a person who is authorised for the purposes of the 2000 Act(**f**);

"the Authority" means the Financial Services Authority;

"the banking consolidation directive" means Directive 2006/48/EC of the European Parliament and of the Council of 14th June 2006 relating to the taking up and pursuit of the business of credit institutions(**g**);

"beneficial owner" has the meaning given by regulation 6;

"business relationship" means a business, professional or commercial relationship between a relevant person and a customer, which is expected by the relevant person, at the time when contact is established, to have an element of duration;

"cash" means notes, coins or travellers' cheques in any currency;

"casino" has the meaning given by regulation 3(13);

"the Commissioners" means the Commissioners for Her Majesty's Revenue and Customs;

"consumer credit financial institution" has the meaning given by regulation 22(1);

"credit institution" has the meaning given by regulation 3(2);

"customer due diligence measures" has the meaning given by regulation 5;

"DETI" means the Department of Enterprise, Trade and Investment in Northern Ireland;

"the electronic money directive" means Directive 2000/46/EC of the European Parliament and of the Council of 18th September 2000 on the taking up, pursuit and prudential supervision of the business of electronic money institutions(**h**);

"estate agent" has the meaning given by regulation 3(11);

"external accountant" has the meaning given by regulation 3(7);

"financial institution" has the meaning given by regulation 3(3);

"firm" means any entity, whether or not a legal person, that is not an individual and includes a body corporate and a partnership or other unincorporated association;

"high value dealer" has the meaning given by regulation 3(12);

"the implementing measures directive" means Commission Directive 2006/70/EC of 1st August 2006 laying down implementing measures for the money laundering directive(**i**);

"independent legal professional" has the meaning given by regulation 3(9);

"insolvency practitioner", except in regulation 17(2)(c) and (d), has the meaning given by regulation 3(6);

"the life assurance consolidation directive" means Directive 2002/83/EC of the European Parliament and of the Council of 5th November 2002 concerning life assurance(**j**);

(e) S.I. 2003/3075.

"local weights and measures authority" has the meaning given by section 69 of the Weights and Measures Act 1985(**k**) (local weights and measures authorities);

"the markets in financial instruments directive" means Directive 2004/39/EC of the European Parliament and of the Council of 12th April 2004(**l**) on markets in financial instruments;

"money laundering" means an act which falls within section 340(11) of the Proceeds of Crime Act 2002(**m**);

"the money laundering directive" means Directive 2005/60/EC of the European Parliament and of the Council of 26th October 2005(**n**) on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;

"money service business" means an undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or cashes cheques which are made payable to customers;

"nominated officer" means a person who is nominated to receive disclosures under Part 7 of the Proceeds of Crime Act 2002(**o**) (money laundering) or Part 3 of the Terrorism Act 2000(**p**) (terrorist property);

"non-EEA state" means a state that is not an EEA state;

"notice" means a notice in writing;

"occasional transaction" means a transaction (carried out other than as part of a business relationship) amounting to 15,000 euro or more, whether the transaction is carried out in a single operation or several operations which appear to be linked;

"the OFT" means the Office of Fair Trading;

"ongoing monitoring" has the meaning given by regulation 8(2);

"regulated market"—

(a) within the EEA, has the meaning given by point 14 of Article 4(1) of the markets in financial instruments directive; and

(b) outside the EEA, means a regulated financial market which subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligations;

"relevant person" means a person to whom, in accordance with regulations 3 and 4, these Regulations apply;

"the specified disclosure obligations" means disclosure requirements consistent with—

(a) Article 6(1) to (4) of Directive 2003/6/EC of the European Parliament and of the Council of 28th January 2003(**q**) on insider dealing and market manipulation;

(b) Articles 3, 5, 7, 8, 10, 14 and 16 of Directive 2003/71/EC of the European Parliament and of the Council of 4th November 2003(**r**) on the prospectuses to be published when securities are offered to the public or admitted to trading;

(c) Articles 4 to 6, 14, 16 to 19 and 30 of Directive 2004/109/EC of the European Parliament and of the Council of 15th December 2004(**s**) relating to the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market; or

(d) Community legislation made under the provisions mentioned in sub-paragraphs (a) to (c);

"supervisory authority" in relation to any relevant person means the supervisory authority specified for such a person by regulation 23;

"tax adviser" (except in regulation 11(3)) has the meaning given by regulation 3(8);

"terrorist financing" means an offence under—

(a) section 15 (fund-raising), 16 (use and possession), 17 (funding arrangements), 18 (money laundering) or 63 (terrorist finance: jurisdiction) of the Terrorism Act 2000;

(b) paragraph 7(2) or (3) of Schedule 3 to the Anti-Terrorism, Crime and Security Act 2001(**t**) (freezing orders);

(c) article 7, 8 or 10 of the Terrorism (United Nations Measures) Order 2006(**u**); or

(d) article 7, 8 or 10 of the Al-Qaida and Taliban (United Nations Measures) Order 2006(**v**);

"trust or company service provider" has the meaning given by regulation 3(10).

(2) In these Regulations, references to amounts in euro include references to equivalent amounts in another currency.

(3) Unless otherwise defined, expressions used in these Regulations and the money laundering directive have the same meaning as in the money laundering directive and expressions used in these Regulations and in the implementing measures directive have the same meaning as in the implementing measures directive.

Application of the Regulations

3.—(1) Subject to regulation 4, these Regulations apply to the following persons acting in the course of business carried on by them in the United Kingdom ("relevant persons")—

(a) credit institutions;

(b) financial institutions;

(c) auditors, insolvency practitioners, external accountants and tax advisers;

(d) independent legal professionals;

(e) trust or company service providers;

(f) estate agents;

(g) high value dealers;

(h) casinos.

(2) "Credit institution" means—

(a) a credit institution as defined in Article 4(1)(a) of the banking consolidation directive; or

(b) a branch (within the meaning of Article 4(3) of that directive) located in an EEA state of an institution falling within sub-paragraph (a) (or an equivalent institution whose head office is located in a non-EEA state) wherever its head office is located,

when it accepts deposits or other repayable funds from the public or grants credits for its own account (within the meaning of the banking consolidation directive).

(3) "Financial institution" means—

(a) an undertaking, including a money service business, when it carries out one or more of the activities listed in points 2 to 12 and 14 of Annex 1 to the banking consolidation directive (the relevant text of which is set out in Schedule 1 to these Regulations), other than—

(i) a credit institution;

(ii) an undertaking whose only listed activity is trading for own account in one or more of the products listed in point 7 of Annex 1 to the banking consolidation directive where the undertaking does not have a customer,

and, for this purpose, "customer" means a third party which is not a member of the same group as the undertaking;

(b) an insurance company duly authorised in accordance with the life assurance consolidation directive, when it carries out activities covered by that directive;

(c) a person whose regular occupation or business is the provision to other persons of an investment service or the performance of an investment activity on a professional basis, when providing or performing investment services or activities (within the meaning of the markets in financial instruments directive(**w**)), other than a person falling within Article 2 of that directive;

(d) a collective investment undertaking, when marketing or otherwise offering its units or shares;

(e) an insurance intermediary as defined in Article 2(5) of Directive 2002/92/EC of the European Parliament and of the Council of 9th December 2002(**x**) on insurance mediation, with the exception of a tied insurance intermediary as mentioned in Article 2(7) of that Directive, when it acts in respect of contracts of long-term insurance within the meaning given by article 3(1) of, and Part II of Schedule 1 to, the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001(**y**);

(f) a branch located in an EEA state of a person referred to in sub-paragraphs (a) to (e) (or an equivalent person whose head office is located in a non-EEA state), wherever its head office is located, when carrying out any activity mentioned in sub-paragraphs (a) to (e);

(g) the National Savings Bank;

(h) the Director of Savings, when money is raised under the auspices of the Director under the National Loans Act 1968(**z**).

(4) "Auditor" means any firm or individual who is a statutory auditor within the meaning of Part 42 of the Companies Act 2006(**aa**) (statutory auditors), when carrying out statutory audit work within the meaning of section 1210 of that Act.

(5) Before the entry into force of Part 42 of the Companies Act 2006 the reference in paragraph (4) to—

(a) a person who is a statutory auditor shall be treated as a reference to a person who is eligible for appointment as a company auditor under section 25 of the Companies Act 1989(**ab**) (eligibility for appointment) or article 28 of the Companies (Northern Ireland) Order 1990(**ac**); and

(b) the carrying out of statutory audit work shall be treated as a reference to the provision of audit services.

(6) "Insolvency practitioner" means any person who acts as an insolvency practitioner within the meaning of section 388 of the Insolvency Act 1986(**ad**) (meaning of "act as insolvency practitioner") or article 3 of the Insolvency (Northern Ireland) Order 1989(**ae**).

(7) "External accountant" means a firm or sole practitioner who by way of business provides accountancy services to other persons, when providing such services.

(8) "Tax adviser" means a firm or sole practitioner who by way of business provides advice about the tax affairs of other persons, when providing such services.

(9) "Independent legal professional" means a firm or sole practitioner who by way of business provides legal or notarial services to other persons, when participating in financial or real property transactions concerning—

(a) the buying and selling of real property or business entities;

(aa) 2006 c. 46.

(ad) 1986 c. 45; s388 was amended by section 4 of the Insolvency Act 2000 (c.45), section 11 of the Bankruptcy (Scotland) Act 1993 (c.6), and S.I. 1994/2421, 2002/1240 and 2002/2708.

(ae) 1989 No. 2405 (NI 19); article 3 was amended by the Insolvency (Northern Ireland) Order 2002 No. 3152 (N.I. 6) and S.R. 1995/225, 2002/334, 2003/550, 2004/307.

(b) the managing of client money, securities or other assets;

(c) the opening or management of bank, savings or securities accounts;

(d) the organisation of contributions necessary for the creation, operation or management of companies; or

(e) the creation, operation or management of trusts, companies or similar structures,

and, for this purpose, a person participates in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.

(10) "Trust or company service provider" means a firm or sole practitioner who by way of business provides any of the following services to other persons—

(a) forming companies or other legal persons;

(b) acting, or arranging for another person to act—

(i) as a director or secretary of a company;

(ii) as a partner of a partnership; or

(iii) in a similar position in relation to other legal persons;

(c) providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement;

(d) acting, or arranging for another person to act, as—

(i) a trustee of an express trust or similar legal arrangement; or

(ii) a nominee shareholder for a person other than a company whose securities are listed on a regulated market,

when providing such services.

(11) "Estate agent" means—

(a) a firm; or

(b) sole practitioner,

who, or whose employees, carry out estate agency work (within the meaning given by section 1 of the Estate Agents Act 1979(**af**) (estate agency work)), when in the course of carrying out such work.

(12) "High value dealer" means a firm or sole trader who by way of business trades in goods (including an auctioneer dealing in goods), when he receives, in respect of any transaction, a payment or payments in cash of at least 15,000 euros in total, whether the transaction is executed in a single operation or in several operations which appear to be linked.

(13) "Casino" means the holder of a casino operating licence and, for this purpose, a "casino operating licence" has the meaning given by section 65(2) of the Gambling Act 2005(**ag**) (nature of licence).

(14) In the application of this regulation to Scotland, for "real property" in paragraph (9) substitute "heritable property".

Exclusions

4.—(1) These Regulations do not apply to the following persons when carrying out any of the following activities—

(af) 1979 c. 38. Section 1 was amended by the Law Reform (Miscellaneous Provisions) (Scotland) Act 1985 (c.73), section.56, Schedule 1, Part I, paragraph 40, the Planning (Consequential Provisions) Act 1990 (c.11), section 4, Schedule 2, paragraph 42, the Planning (Consequential Provisions) (Scotland) Act 1997 (c.11), sections 4 and 6(2), Schedule 2, paragraph 28 and by S.I. 2001/1283.

(ag) See also section 7 on the meaning of "casino" and Part 5 of the Act generally on operating licences

(a) a society registered under the Industrial and Provident Societies Act 1965(**ah**), when it—

(i) issues withdrawable share capital within the limit set by section 6 of that Act (maximum shareholding in society); or

(ii) accepts deposits from the public within the limit set by section 7(3) of that Act (carrying on of banking by societies);

(b) a society registered under the Industrial and Provident Societies Act (Northern Ireland) 1969(**ai**), when it—

(i) issues withdrawable share capital within the limit set by section 6 of that Act (maximum shareholding in society); or

(ii) accepts deposits from the public within the limit set by section 7(3) of that Act (carrying on of banking by societies);

(c) a person who is (or falls within a class of persons) specified in any of paragraphs 2 to 23, 25 to 38 or 40 to 49 of the Schedule to the Financial Services and Markets Act 2000 (Exemption) Order 2001(**aj**), when carrying out any activity in respect of which he is exempt;

(d) a person who was an exempted person for the purposes of section 45 of the Financial Services Act 1986(**ak**) (miscellaneous exemptions) immediately before its repeal, when exercising the functions specified in that section;

(e) a person whose main activity is that of a high value dealer, when he engages in financial activity on an occasional or very limited basis as set out in paragraph 1 of Schedule 2 to these Regulations; or

(f) a person, when he prepares a home information pack or a document or information for inclusion in a home information pack.

(2) These Regulations do not apply to a person who falls within regulation 3 solely as a result of his engaging in financial activity on an occasional or very limited basis as set out in paragraph 1 of Schedule 2 to these Regulations.

(3) Parts 2 to 5 of these Regulations do not apply to—

(a) the Auditor General for Scotland;

(b) the Auditor General for Wales;

(c) the Bank of England;

(d) the Comptroller and Auditor General;

(e) the Comptroller and Auditor General for Northern Ireland;

(f) the Official Solicitor to the Supreme Court, when acting as trustee in his official capacity;

(g) the Treasury Solicitor.

(4) In paragraph (1)(f), "home information pack" has the same meaning as in Part 5 of the Housing Act 2004(**al**) (home information packs).

PART 2

CUSTOMER DUE DILIGENCE

Meaning of customer due diligence measures

5. "Customer due diligence measures" means—

(al) 2004 c. 34.

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and

(c) obtaining information on the purpose and intended nature of the business relationship.

Meaning of beneficial owner

6.—(1) In the case of a body corporate, "beneficial owner" means any individual who—

(a) as respects any body other than a company whose securities are listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or

(b) as respects any body corporate, otherwise exercises control over the management of the body.

(2) In the case of a partnership (other than a limited liability partnership), "beneficial owner" means any individual who—

(a) ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership; or

(b) otherwise exercises control over the management of the partnership.

(3) In the case of a trust, "beneficial owner" means—

(a) any individual who is entitled to a specified interest in at least 25% of the capital of the trust property;

(b) as respects any trust other than one which is set up or operates entirely for the benefit of individuals falling within sub-paragraph (a), the class of persons in whose main interest the trust is set up or operates;

(c) any individual who has control over the trust.

(4) In paragraph (3)—

"specified interest" means a vested interest which is—

(a) in possession or in remainder or reversion (or, in Scotland, in fee); and

(b) defeasible or indefeasible;

"control" means a power (whether exercisable alone, jointly with another person or with the consent of another person) under the trust instrument or by law to—

(a) dispose of, advance, lend, invest, pay or apply trust property;

(b) vary the trust;

(c) add or remove a person as a beneficiary or to or from a class of beneficiaries;

(d) appoint or remove trustees;

(e) direct, withhold consent to or veto the exercise of a power such as is mentioned in sub-paragraph (a), (b), (c) or (d).

(5) For the purposes of paragraph (3)—

(a) where an individual is the beneficial owner of a body corporate which is entitled to a specified interest in the capital of the trust property or which has control over the trust, the individual is to be regarded as entitled to the interest or having control over the trust; and

(b) an individual does not have control solely as a result of—

(i) his consent being required in accordance with section 32(1)(c) of the Trustee Act 1925(**am**) (power of advancement);

(ii) any discretion delegated to him under section 34 of the Pensions Act 1995(**an**) (power of investment and delegation);

(iii) the power to give a direction conferred on him by section 19(2) of the Trusts of Land and Appointment of Trustees Act 1996(**ao**) (appointment and retirement of trustee at instance of beneficiaries); or

(iv) the power exercisable collectively at common law to vary or extinguish a trust where the beneficiaries under the trust are of full age and capacity and (taken together) absolutely entitled to the property subject to the trust (or, in Scotland, have a full and unqualified right to the fee).

(6) In the case of a legal entity or legal arrangement which does not fall within paragraph (1), (2) or (3), "beneficial owner" means—

(a) where the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from at least 25% of the property of the entity or arrangement;

(b) where the individuals who benefit from the entity or arrangement have yet to be determined, the class of persons in whose main interest the entity or arrangement is set up or operates;

(c) any individual who exercises control over at least 25% of the property of the entity or arrangement.

(7) For the purposes of paragraph (6), where an individual is the beneficial owner of a body corporate which benefits from or exercises control over the property of the entity or arrangement, the individual is to be regarded as benefiting from or exercising control over the property of the entity or arrangement.

(8) In the case of an estate of a deceased person in the course of administration, "beneficial owner" means—

(a) in England and Wales and Northern Ireland, the executor, original or by representation, or administrator for the time being of a deceased person;

(b) in Scotland, the executor for the purposes of the Executors (Scotland) Act 1900(**ap**).

(9) In any other case, "beneficial owner" means the individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted.

(10) In this regulation—

"arrangement", "entity" and "trust" means an arrangement, entity or trust which administers and distributes funds;

"limited liability partnership" has the meaning given by the Limited Liability Partnerships Act 2000(**aq**).

Application of customer due diligence measures

7.—(1) Subject to regulations 9, 10, 12, 13, 14, 16(4) and 17, a relevant person must apply customer due diligence measures when he—

(a) establishes a business relationship;

(b) carries out an occasional transaction;

(c) suspects money laundering or terrorist financing;

(d) doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

(2) Subject to regulation 16(4), a relevant person must also apply customer due diligence measures at other appropriate times to existing customers on a risk-sensitive basis.

(3) A relevant person must—

(a) determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction; and

(b) be able to demonstrate to his supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

(4) Where—

(a) a relevant person is required to apply customer due diligence measures in the case of a trust, legal entity (other than a body corporate) or a legal arrangement (other than a trust); and

(b) the class of persons in whose main interest the trust, entity or arrangement is set up or operates is identified as a beneficial owner,

the relevant person is not required to identify all the members of the class.

(5) Paragraph (3)(b) does not apply to the National Savings Bank or the Director of Savings.

Ongoing monitoring

8.—(1) A relevant person must conduct ongoing monitoring of a business relationship.

(2) "Ongoing monitoring" of a business relationship means—

(a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile; and

(b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.

(3) Regulation 7(3) applies to the duty to conduct ongoing monitoring under paragraph (1) as it applies to customer due diligence measures.

Timing of verification

9.—(1) This regulation applies in respect of the duty under regulation 7(1)(a) and (b) to apply the customer due diligence measures referred to in regulation 5(a) and (b).

(2) Subject to paragraphs (3) to (5) and regulation 10, a relevant person must verify the identity of the customer (and any beneficial owner) before the establishment of a business relationship or the carrying out of an occasional transaction.

(3) Such verification may be completed during the establishment of a business relationship if—

(a) this is necessary not to interrupt the normal conduct of business; and

(b) there is little risk of money laundering or terrorist financing occurring,

provided that the verification is completed as soon as practicable after contact is first established.

(4) The verification of the identity of the beneficiary under a life insurance policy may take place after the business relationship has been established provided that it takes place at or before the time of payout or at or before the time the beneficiary exercises a right vested under the policy.

(5) The verification of the identity of a bank account holder may take place after the bank account has been opened provided that there are adequate safeguards in place to ensure that—

(a) the account is not closed; and

(b) transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder),

before verification has been completed.

Casinos

10.—(1) A casino must establish and verify the identity of—

(a) all customers to whom the casino makes facilities for gaming available—

(i) before entry to any premises where such facilities are provided; or

(ii) where the facilities are for remote gaming, before access is given to such facilities; or

(b) if the specified conditions are met, all customers who, in the course of any period of 24 hours—

(i) purchase from, or exchange with, the casino chips with a total value of 2,000 euro or more;

(ii) pay the casino 2,000 or more for the use of gaming machines; or

(iii) pay to, or stake with, the casino 2,000 euro or more in connection with facilities for remote gaming.

(2) The specified conditions are—

(a) the casino verifies the identity of each customer before or immediately after such purchase, exchange, payment or stake takes place, and

(b) the Gambling Commission is satisfied that the casino has appropriate procedures in place to monitor and record—

(i) the total value of chips purchased from or exchanged with the casino;

(ii) the total money paid for the use of gaming machines; or

(iii) the total money paid or staked in connection with facilities for remote gaming,

by each customer.

(3) In this regulation—

"gaming", "gaming machine", "remote operating licence" and "stake" have the meanings given by, respectively, sections 6(1) (gaming & game of chance), 235 (gaming machine), 67 (remote gambling) and 353(1) (interpretation) of the Gambling Act 2005(**ar**);

"premises" means premises subject to—

(a) a casino premises licence within the meaning of section 150(1)(a) of the Gambling Act 2005 (nature of licence); or

(b) a converted casino premises licence within the meaning of paragraph 65 of Part 7 of Schedule 4 to the Gambling Act 2005 (Commencement No. 6 and Transitional Provisions) Order 2006(**as**);

"remote gaming" means gaming provided pursuant to a remote operating licence.

Requirement to cease transactions etc.

11.—(1) Where, in relation to any customer, a relevant person is unable to apply customer due diligence measures in accordance with the provisions of this Part, he—

(a) must not carry out a transaction with or for the customer through a bank account;

(b) must not establish a business relationship or carry out an occasional transaction with the customer;

(c) must terminate any existing business relationship with the customer;

(d) must consider whether he is required to make a disclosure by Part 7 of the Proceeds of Crime Act 2002 or Part 3 of the Terrorism Act 2000.

(2) Paragraph (1) does not apply where a lawyer or other professional adviser is in the course of ascertaining the legal position for his client or performing his task of defending or representing that client in, or concerning, legal proceedings, including advice on the institution or avoidance of proceedings.

(3) In paragraph (2), "other professional adviser" means an auditor, accountant or tax adviser who is a member of a professional body which is established for any such persons and which makes provision for—

(a) testing the competence of those seeking admission to membership of such a body as a condition for such admission; and

(b) imposing and maintaining professional and ethical standards for its members, as well as imposing sanctions for non-compliance with those standards.

Exception for trustees of debt issues

12.—(1) A relevant person—

(a) who is appointed by the issuer of instruments or securities specified in paragraph (2) as trustee of an issue of such instruments or securities; or

(b) whose customer is a trustee of an issue of such instruments or securities,

is not required to apply the customer due diligence measure referred to in regulation 5(b) in respect of the holders of such instruments or securities.

(2) The specified instruments and securities are—

(a) instruments which fall within article 77 of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001(**at**); and

(b) securities which fall within article 78 of that Order.

Simplified due diligence

13.—(1) A relevant person is not required to apply customer due diligence measures in the circumstances mentioned in regulation 7(1)(a), (b) or (d) where he has reasonable grounds for believing that the customer, transaction or product related to such transaction, falls within any of the following paragraphs.

(2) The customer is—

(a) a credit or financial institution which is subject to the requirements of the money laundering directive; or

(b) a credit or financial institution (or equivalent institution) which—

(i) is situated in a non-EEA state which imposes requirements equivalent to those laid down in the money laundering directive; and

(ii) is supervised for compliance with those requirements.

(3) The customer is a company whose securities are listed on a regulated market subject to specified disclosure obligations.

(4) The customer is an independent legal professional and the product is an account into which monies are pooled, provided that—

(a) where the pooled account is held in a non-EEA state—

(i) that state imposes requirements to combat money laundering and terrorist financing which are consistent with international standards; and

(ii) the independent legal professional is supervised in that state for compliance with those requirements; and

(b) information on the identity of the persons on whose behalf monies are held in the pooled account is available, on request, to the institution which acts as a depository institution for the account.

(5) The customer is a public authority in the United Kingdom.

(6) The customer is a public authority which fulfils all the conditions set out in paragraph 2 of Schedule 2 to these Regulations.

(7) The product is—

(a) a life insurance contract where the annual premium is no more than 1,000 euro or where a single premium of no more than 2,500 euro is paid;

(b) an insurance contract for the purposes of a pension scheme where the contract contains no surrender clause and cannot be used as collateral;

(c) a pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme (other than an assignment permitted by section 44 of the Welfare Reform and Pensions Act 1999(**au**) (disapplication of restrictions on alienation) or section 91(5)(a) of the Pensions Act 1995(**av**) (inalienability of occupational pension)); or

(d) electronic money, within the meaning of Article 1(3)(b) of the electronic money directive, where—

(i) if the device cannot be recharged, the maximum amount stored in the device is no more than 150 euro; or

(ii) if the device can be recharged, a limit of 2,500 euro is imposed on the total amount transacted in a calendar year, except when an amount of 1,000 euro or more is redeemed in the same calendar year by the bearer (within the meaning of Article 3 of the electronic money directive).

(8) The product and any transaction related to such product fulfils all the conditions set out in paragraph 3 of Schedule 2 to these Regulations.

(9) The product is a child trust fund within the meaning given by section 1(2) of the Child Trust Funds Act 2004(**aw**).

Enhanced customer due diligence and ongoing monitoring

14.—(1) A relevant person must apply on a risk-sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring—

(a) in accordance with paragraphs (2) to (4);

(b) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

(aw) 2004 c. 6.

(2) Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the following measures—

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;

(c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

(3) A credit institution ("the correspondent") which has or proposes to have a correspondent banking relationship with a respondent institution ("the respondent") from a non-EEA state must—

(a) gather sufficient information about the respondent to understand fully the nature of its business;

(b) determine from publicly-available information the reputation of the respondent and the quality of its supervision;

(c) assess the respondent's anti-money laundering and anti-terrorist financing controls;

(d) obtain approval from senior management before establishing a new correspondent banking relationship;

(e) document the respective responsibilities of the respondent and correspondent; and

(f) be satisfied that, in respect of those of the respondent's customers who have direct access to accounts of the correspondent, the respondent—

(i) has verified the identity of, and conducts ongoing monitoring in respect of, such customers; and

(ii) is able to provide to the correspondent, upon request, the documents, data or information obtained when applying customer due diligence measures and ongoing monitoring.

(4) A relevant person who proposes to have a business relationship or carry out an occasional transaction with a politically exposed person must—

(a) have approval from senior management for establishing the business relationship with that person;

(b) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or occasional transaction; and

(c) where the business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

(5) In paragraph (4), "a politically exposed person" means a person who is—

(a) an individual who is or has, at any time in the preceding year, been entrusted with a prominent public function by—

(i) a state other than the United Kingdom;

(ii) a Community institution; or

(iii) an international body,

including a person who falls in any of the categories listed in paragraph 4(1)(a) of Schedule 2;

(b) an immediate family member of a person referred to in sub-paragraph (a), including a person who falls in any of the categories listed in paragraph 4(1)(c) of Schedule 2; or

(c) a known close associate of a person referred to in sub-paragraph (a), including a person who falls in either of the categories listed in paragraph 4(1)(d) of Schedule 2.

(6) For the purpose of deciding whether a person is a known close associate of a person referred to in paragraph (5)(a), a relevant person need only have regard to information which is in his possession or is publicly known.

Branches and subsidiaries

15.—(1) A credit or financial institution must require its branches and subsidiary undertakings which are located in a non-EEA state to apply, to the extent permitted by the law of that state, measures at least equivalent to those set out in these Regulations with regard to customer due diligence measures, ongoing monitoring and record-keeping.

(2) Where the law of a non-EEA state does not permit the application of such equivalent measures by the branch or subsidiary undertaking located in that state, the credit or financial institution must—

(a) inform its supervisory authority accordingly; and

(b) take additional measures to handle effectively the risk of money laundering and terrorist financing.

(3) In this regulation "subsidiary undertaking"—

(a) except in relation to an incorporated friendly society, has the meaning given by section 1162 of the Companies Act 2006(**ax**) (parent and subsidiary undertakings) and, in relation to a body corporate in or formed under the law of an EEA state other than the United Kingdom, includes an undertaking which is a subsidiary undertaking within the meaning of any rule of law in force in that state for purposes connected with implementation of the European Council Seventh Company Law Directive 83/349/EEC of 13th June 1983(**ay**) on consolidated accounts;

(b) in relation to an incorporated friendly society, means a body corporate of which the society has control within the meaning of section 13(9)(a) or (aa) of the Friendly Societies Act 1992(**az**) (control of subsidiaries and other bodies corporate).

(4) Before the entry into force of section 1162 of the Companies Act 2006 the reference to that section in paragraph (3)(a) shall be treated as a reference to section 258 of the Companies Act 1985(**ba**) (parent and subsidiary undertakings).

Shell banks, anonymous accounts etc.

16.—(1) A credit institution must not enter into, or continue, a correspondent banking relationship with a shell bank.

(2) A credit institution must take appropriate measures to ensure that it does not enter into, or continue, a corresponding banking relationship with a bank which is known to permit its accounts to be used by a shell bank.

(3) A credit or financial institution carrying on business in the United Kingdom must not set up an anonymous account or an anonymous passbook for any new or existing customer.

(4) As soon as reasonably practicable on or after 15th December 2007 all credit and financial institutions carrying on business in the United Kingdom must apply customer due diligence measures to, and conduct ongoing monitoring of, all anonymous accounts and passbooks in existence on that date and in any event before such accounts or passbooks are used.

(5) A "shell bank" means a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence involving meaningful decision-

(ba) 1985 c. 6.

making and management, and which is not part of a financial conglomerate or third-country financial conglomerate.

(6) In this regulation, "financial conglomerate" and "third-country financial conglomerate" have the meanings given by regulations 1(2) and 7(1) respectively of the Financial Conglomerates and Other Financial Groups Regulations 2004(**bb**).

Reliance

17.—(1) A relevant person may rely on a person who falls within paragraph (2) (or who the relevant person has reasonable grounds to believe falls within paragraph (2)) to apply any customer due diligence measures provided that—

(a) the other person consents to being relied on; and

(b) notwithstanding the relevant person's reliance on the other person, the relevant person remains liable for any failure to apply such measures.

(2) The persons are—

(a) a credit or financial institution which is an authorised person;

(b) a relevant person who is—

(i) an auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional; and

(ii) supervised for the purposes of these Regulations by one of the bodies listed in Part 1 of Schedule 3;

(c) a person who carries on business in another EEA state who is—

(i) a credit or financial institution, auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional;

(ii) subject to mandatory professional registration recognised by law; and

(iii) supervised for compliance with the requirements laid down in the money laundering directive in accordance with section 2 of Chapter V of that directive; or

(d) a person who carries on business in a non-EEA state who is—

(i) a credit or financial institution (or equivalent institution), auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional;

(ii) subject to mandatory professional registration recognised by law;

(iii) subject to requirements equivalent to those laid down in the money laundering directive; and

(iv) supervised for compliance with those requirements in a manner equivalent to section 2 of Chapter V of the money laundering directive.

(3) In paragraph (2)(c)(i) and (d)(i), "auditor" and "insolvency practitioner" includes a person situated in another EEA state or a non-EEA state who provides services equivalent to the services provided by an auditor or insolvency practitioner.

(4) Nothing in this regulation prevents a relevant person applying customer due diligence measures by means of an outsourcing service provider or agent provided that the relevant person remains liable for any failure to apply such measures.

(5) In this regulation, "financial institution" excludes money service businesses.

(bb) S.I. 2004/1862.

Directions where Financial Action Task Force applies counter-measures

18. The Treasury may direct any relevant person—

(a) not to enter into a business relationship;

(b) not to carry out an occasional transaction; or

(c) not to proceed any further with a business relationship or occasional transaction,

with a person who is situated or incorporated in a non-EEA state to which the Financial Action Task Force has decided to apply counter-measures.

PART 3

RECORD-KEEPING, PROCEDURES AND TRAINING

Record-keeping

19.—(1) Subject to paragraph (4), a relevant person must keep the records specified in paragraph (2) for at least the period specified in paragraph (3).

(2) The records are—

(a) a copy of, or the references to, the evidence of the customer's identity obtained pursuant to regulation 7, 8, 10, 14 or 16(4);

(b) the supporting records (consisting of the original documents or copies) in respect of a business relationship or occasional transaction which is the subject of customer due diligence measures or ongoing monitoring.

(3) The period is five years beginning on—

(a) in the case of the records specified in paragraph (2)(a), the date on which—

(i) the occasional transaction is completed; or

(ii) the business relationship ends; or

(b) in the case of the records specified in paragraph (2)(b)—

(i) where the records relate to a particular transaction, the date on which the transaction is completed;

(ii) for all other records, the date on which the business relationship ends.

(4) A relevant person who is relied on by another person must keep the records specified in paragraph (2)(a) for five years beginning on the date on which he is relied on for the purposes of regulation 7, 10, 14 or 16(4) in relation to any business relationship or occasional transaction.

(5) A person referred to in regulation 17(2)(a) or (b) who is relied on by a relevant person must, if requested by the person relying on him within the period referred to in paragraph (4)—

(a) as soon as reasonably practicable make available to the person who is relying on him any information about the customer (and any beneficial owner) which he obtained when applying customer due diligence measures; and

(b) as soon as reasonably practicable forward to the person who is relying on him copies of any identification and verification data and other relevant documents on the identity of the customer (and any beneficial owner) which he obtained when applying those measures.

(6) A relevant person who relies on a person referred to in regulation 17(2)(c) or (d) (a "third party") to apply customer due diligence measures must take steps to ensure that the third party will, if requested by the relevant person within the period referred to in paragraph (4)—

(a) as soon as reasonably practicable make available to him any information about the customer (and any beneficial owner) which the third party obtained when applying customer due diligence measures; and

(b) as soon as reasonably practicable forward to him copies of any identification and verification data and other relevant documents on the identity of the customer (and any beneficial owner) which the third party obtained when applying those measures.

(7) Paragraphs (5) and (6) do not apply where a relevant person applies customer due diligence measures by means of an outsourcing service provider or agent.

(8) For the purposes of this regulation, a person relies on another person where he does so in accordance with regulation 17(1).

Policies and procedures

20.—(1) A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to—

(a) customer due diligence measures and ongoing monitoring;

(b) reporting;

(c) record-keeping;

(d) internal control;

(e) risk assessment and management;

(f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures,

in order to prevent activities related to money laundering and terrorist financing.

(2) The policies and procedures referred to in paragraph (1) include policies and procedures—

(a) which provide for the identification and scrutiny of—

(i) complex or unusually large transactions;

(ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

(iii) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering or terrorist financing;

(b) which specify the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which might favour anonymity;

(c) to determine whether a customer is a politically exposed person;

(d) under which—

(i) an individual in the relevant person's organisation is a nominated officer under Part 7 of the Proceeds of Crime Act 2002(**bc**) and Part 3 of the Terrorism Act 2000(**bd**);

(ii) anyone in the organisation to whom information or other matter comes in the course of the business as a result of which he knows or suspects or has reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing is required to comply with Part 7 of the Proceeds of Crime Act 2002 or, as the case may be, Part 3 of the Terrorism Act 2000; and

(iii) where a disclosure is made to the nominated officer, he must consider it in the light of any relevant information which is available to the relevant person and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing.

(3) Paragraph (2)(d) does not apply where the relevant person is an individual who neither employs nor acts in association with any other person.

(4) A credit or financial institution must establish and maintain systems which enable it to respond fully and rapidly to enquiries from financial investigators accredited under section 3 of the Proceeds of Crime Act 2002 (accreditation and training), persons acting on behalf of the Scottish Ministers in their capacity as an enforcement authority under that Act, officers of Revenue and Customs or constables as to—

(a) whether it maintains, or has maintained during the previous five years, a business relationship with any person; and

(b) the nature of that relationship.

(5) A credit or financial institution must communicate where relevant the policies and procedures which it establishes and maintains in accordance with this regulation to its branches and subsidiary undertakings which are located outside the United Kingdom.

(6) In this regulation—

"politically exposed person" has the same meaning as in regulation 14(4);

"subsidiary undertaking" has the same meaning as in regulation 15.

Training

21. A relevant person must take appropriate measures so that all relevant employees of his are—

(a) made aware of the law relating to money laundering and terrorist financing; and

(b) regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

PART 4

SUPERVISION AND REGISTRATION

Interpretation

Interpretation

22.—(1) In this Part—

"Annex I financial institution" means any undertaking which falls within regulation 3(3)(a) other than—

(a) a consumer credit financial institution;

(b) a money service business; or

(c) an authorised person;

"consumer credit financial institution" means any undertaking which falls within regulation 3(3)(a) and which requires, under section 21 of the Consumer Credit Act 1974(**be**) (businesses needing a licence), a licence to carry on a consumer credit business, other than—

(a) a person covered by a group licence issued by the OFT under section 22 of that Act (standard and group licences);

(b) a money service business; or

(c) an authorised person.

(2) In paragraph (1), "consumer credit business" has the meaning given by section 189(1) of the Consumer Credit Act 1974 (definitions) and, on the entry into force of section 23(a) of the Consumer Credit Act 2006(**bf**) (definitions of "consumer credit business" and "consumer hire business"), has the meaning given by section 189(1) of the Consumer Credit Act 1974 as amended by section 23(a) of the Consumer Credit Act 2006.

Supervision

Supervisory authorities

23.—(1) Subject to paragraph (2), the following bodies are supervisory authorities—

(a) the Authority is the supervisory authority for—

(i) credit and financial institutions which are authorised persons;

(ii) trust or company service providers which are authorised persons;

(iii) Annex I financial institutions;

(b) the OFT is the supervisory authority for—

(i) consumer credit financial institutions;

(ii) estate agents;

(c) each of the professional bodies listed in Schedule 3 is the supervisory authority for relevant persons who are regulated by it;

(d) the Commissioners are the supervisory authority for—

(i) high value dealers;

(ii) money service businesses which are not supervised by the Authority;

(iii) trust or company service providers which are not supervised by the Authority or one of the bodies listed in Schedule 3;

(iv) auditors, external accountants and tax advisers who are not supervised by one of the bodies listed in Schedule 3.

(e) the Gambling Commission is the supervisory authority for casinos;

(f) DETI is the supervisory authority for—

(i) credit unions in Northern Ireland;

(ii) insolvency practitioners authorised by it under article 351 of the Insolvency (Northern Ireland) Order 1989;

(g) the Secretary of State is the supervisory authority for insolvency practitioners authorised by him under section 393 of the Insolvency Act 1986(**bg**) (grant, refusal and withdrawal of authorisation).

(2) Where under paragraph (1) there is more than one supervisory authority for a relevant person, the supervisory authorities may agree that one of them will act as the supervisory authority for that person.

(3) Where an agreement has been made under paragraph (2), the authority which has agreed to act as the supervisory authority must notify the relevant person or publish the agreement in such manner as it considers appropriate.

(4) Where no agreement has been made under paragraph (2), the supervisory authorities for a relevant person must cooperate in the performance of their functions under these Regulations.

(bf) 2006 c. 14.

Duties of supervisory authorities

24.—(1) A supervisory authority must effectively monitor the relevant persons for whom it is the supervisory authority and take necessary measures for the purpose of securing compliance by such persons with the requirements of these Regulations.

(2) A supervisory authority which, in the course of carrying out any of its functions under these Regulations, knows or suspects that a person is or has engaged in money laundering or terrorist financing must promptly inform the Serious Organised Crime Agency.

(3) A disclosure made under paragraph (2) is not to be taken to breach any restriction, however imposed, on the disclosure of information.

(4) The functions of the Authority under these Regulations shall be treated for the purposes of Parts 1, 2 and 4 of Schedule 1 to the 2000 Act (the Financial Services Authority) as functions conferred on the Authority under that Act.

Registration of high value dealers, money service businesses and trust or company service providers

Duty to maintain registers

25.—(1) The Commissioners must maintain registers of—

(a) high value dealers;

(b) money service businesses for which they are the supervisory authority; and

(c) trust or company service providers for which they are the supervisory authority.

(2) The Commissioners may keep the registers in any form they think fit.

(3) The Commissioners may publish or make available for public inspection all or part of a register maintained under this regulation.

Requirement to be registered

26.—(1) A person in respect of whom the Commissioners are required to maintain a register under regulation 25 must not act as a—

(a) high value dealer;

(b) money service business; or

(c) trust or company service provider,

unless he is included in the register.

(2) Paragraph (1) and regulation 29 are subject to the transitional provisions set out in regulation 50.

Applications for registration in a register maintained under regulation 25

27.—(1) An applicant for registration in a register maintained under regulation 25 must make an application in such manner and provide such information as the Commissioners may specify.

(2) The information which the Commissioners may specify includes—

(a) the applicant's name and (if different) the name of the business;

(b) the nature of the business;

(c) the name of the nominated officer (if any);

(d) in relation to a money service business or trust or company service provider—

(i) the name of any person who effectively directs or will direct the business and any beneficial owner of the business; and

(ii) information needed by the Commissioners to decide whether they must refuse the application pursuant to regulation 28.

(3) At any time after receiving an application and before determining it, the Commissioners may require the applicant to provide, within 21 days beginning with the date of being requested to do so, such further information as they reasonably consider necessary to enable them to determine the application.

(4) If at any time after the applicant has provided the Commissioners with any information under paragraph (1) or (3)—

(a) there is a material change affecting any matter contained in that information; or

(b) it becomes apparent to that person that the information contains a significant inaccuracy,

he must provide the Commissioners with details of the change or, as the case may be, a correction of the inaccuracy within 30 days beginning with the date of the occurrence of the change (or the discovery of the inaccuracy) or within such later time as may be agreed with the Commissioners.

(5) The obligation in paragraph (4) applies also to material changes or significant inaccuracies affecting any matter contained in any supplementary information provided pursuant to that paragraph.

(6) Any information to be provided to the Commissioners under this regulation must be in such form or verified in such manner as they may specify.

Fit and proper test

28.—(1) The Commissioners must refuse to register an applicant as a money service business or trust or company service provider if they are satisfied that—

(a) the applicant;

(b) a person who effectively directs, or will effectively direct, the business or service provider;

(c) a beneficial owner of the business or service provider; or

(d) the nominated officer of the business or service provider,

is not a fit and proper person.

(2) For the purposes of paragraph (1), a person is not a fit and proper person if he—

(a) has been convicted of—

(i) an offence under the Terrorism Act 2000(**bh**);

(ii) an offence under paragraph 7(2) or (3) of Schedule 3 to the Anti-Terrorism, Crime and Security Act 2001(**bi**) (offences);

(iii) an offence under the Terrorism Act 2006(**bj**);

(iv) an offence under Part 7 (money laundering) of, or listed in Schedule 2 (lifestyle offences: England and Wales), 4 (lifestyle offences: Scotland) or 5 (lifestyle offences: Northern Ireland) to, the Proceeds of Crime Act 2002(**bk**);

(v) an offence under the Fraud Act 2006(**bl**) or, in Scotland, the common law offence of fraud;

(vi) an offence under section 72(1), (3) or (8) of the Value Added Tax Act 1994(**bm**) (offences); or

(vii) the common law offence of cheating the public revenue;

(b) has been adjudged bankrupt or sequestration of his estate has been awarded and (in either case) he has not been discharged;

(c) is subject to a disqualification order under the Company Directors Disqualification Act 1986(**bn**);

(d) is or has been subject to a confiscation order under the Proceeds of Crime Act 2002;

(e) has consistently failed to comply with the requirements of these Regulations, the Money Laundering Regulations 2003(**bo**) or the Money Laundering Regulations 2001(**bp**);

(f) has consistently failed to comply with the requirements of regulation 2006/1781/EC of the European Parliament and of the Council of 15th November 2006 on information on the payer accompanying the transfer of funds(**bq**);

(g) has effectively directed a business which falls within sub-paragraph (e) or (f);

(h) is otherwise not a fit and proper person with regard to the risk of money laundering or terrorist financing.

(3) For the purposes of this regulation, a conviction for an offence listed in paragraph (2)(a) is to be disregarded if it is spent for the purposes of the Rehabilitation of Offenders Act 1974(**br**).

Determination of applications under regulation 27

29.—(1) Subject to regulation 28, the Commissioners may refuse to register an applicant for registration in a register maintained under regulation 25 only if—

(a) any requirement of, or imposed under, regulation 27 has not been complied with;

(b) it appears to the Commissioners that any information provided pursuant to regulation 27 is false or misleading in a material particular; or

(c) the applicant has failed to pay a charge imposed by them under regulation 35(1).

(2) The Commissioners must within 45 days beginning either with the date on which they receive the application or, where applicable, with the date on which they receive any further information required under regulation 27(3), give the applicant notice of—

(a) their decision to register the applicant; or

(b) the following matters—

(i) their decision not to register the applicant;

(ii) the reasons for their decision;

(iii) the right to require a review under regulation 43; and

(iv) the right to appeal under regulation 44(1)(a).

(3) The Commissioners must, as soon as practicable after deciding to register a person, include him in the relevant register.

Cancellation of registration in a register maintained under regulation 25

30.—(1) The Commissioners must cancel the registration of a money service business or trust or company service provider in a register maintained under regulation 25(1) if, at any time after registration, they are satisfied that he or any person mentioned in regulation 28(1)(b), (c) or (d) is not a fit and proper person within the meaning of regulation 28(2).

(2) The Commissioners may cancel a person's registration in a register maintained by them under regulation 25 if, at any time after registration, it appears to them that they would have had grounds to refuse registration under regulation 29(1).

(br) 1974 c. 53.

(3) Where the Commissioners decide to cancel a person's registration they must give him notice of—

(a) their decision and, subject to paragraph (4), the date from which the cancellation takes effect;

(b) the reasons for their decision;

(c) the right to require a review under regulation 43; and

(d) the right to appeal under regulation 44(1)(a).

(4) If the Commissioners—

(a) consider that the interests of the public require the cancellation of a person's registration to have immediate effect; and

(b) include a statement to that effect and the reasons for it in the notice given under paragraph (3),

the cancellation takes effect when the notice is given to the person.

Requirement to inform the Authority

Requirement on authorised person to inform the Authority

31.—(1) An authorised person whose supervisory authority is the Authority must, before acting as a money service business or a trust or company service provider or within 28 days of so doing, inform the Authority that he intends, or has begun, to act as such.

(2) Paragraph (1) does not apply to an authorised person who—

(a) immediately before 15th December 2007 was acting as a money service business or a trust or company service provider and continues to act as such after that date; and

(b) before 15th January 2008 informs the Authority that he is or was acting as such.

(3) Where an authorised person whose supervisory authority is the Authority ceases to act as a money service business or a trust or company service provider, he must immediately inform the Authority.

(4) Any requirement imposed by this regulation is to be treated as if it were a requirement imposed by or under the 2000 Act.

(5) Any information to be provided to the Authority under this regulation must be in such form or verified in such manner as it may specify.

Registration of Annex I financial institutions, estate agents etc.

Power to maintain registers

32.—(1) The supervisory authorities mentioned in paragraph (2), (3) or (4) may, in order to fulfil their duties under regulation 24, maintain a register under this regulation.

(2) The Authority may maintain a register of Annex I financial institutions.

(3) The OFT may maintain registers of—

(a) consumer credit financial institutions; and

(b) estate agents.

(4) The Commissioners may maintain registers of—

(a) auditors;

(b) external accountants; and

(c) tax advisers,

who are not supervised by the Secretary of State, DETI or any of the professional bodies listed in Schedule 3.

(5) Where a supervisory authority decides to maintain a register under this regulation, it must take reasonable steps to bring its decision to the attention of those relevant persons in respect of whom the register is to be established.

(6) A supervisory authority may keep a register under this regulation in any form it thinks fit.

(7) A supervisory authority may publish or make available to public inspection all or part of a register maintained by it under this regulation.

Requirement to be registered

33. Where a supervisory authority decides to maintain a register under regulation 32 in respect of any description of relevant persons and establishes a register for that purpose, a relevant person of that description may not carry on the business or profession in question for a period of more than six months beginning on the date on which the supervisory authority establishes the register unless he is included in the register.

Applications for and cancellation of registration in a register maintained under regulation 32

34.—(1) Regulations 27, 29 (with the omission of the words "Subject to regulation 28" in regulation 29(1)) and 30(2), (3) and (4) apply to registration in a register maintained by the Commissioners under regulation 32 as they apply to registration in a register maintained under regulation 25.

(2) Regulation 27 applies to registration in a register maintained by the Authority or the OFT under regulation 32 as it applies to registration in a register maintained under regulation 25 and, for this purpose, references to the Commissioners are to be treated as references to the Authority or the OFT, as the case may be.

(3) The Authority and the OFT may refuse to register an applicant for registration in a register maintained under regulation 32 only if—

(a) any requirement of, or imposed under, regulation 27 has not been complied with;

(b) it appears to the Authority or the OFT, as the case may be, that any information provided pursuant to regulation 27 is false or misleading in a material particular; or

(c) the applicant has failed to pay a charge imposed by the Authority or the OFT, as the case may be, under regulation 35(1).

(4) The Authority or the OFT, as the case may be, must, within 45 days beginning either with the date on which it receives an application or, where applicable, with the date on which it receives any further information required under regulation 27(3), give the applicant notice of—

(a) its decision to register the applicant; or

(b) the following matters—

(i) that it is minded not to register the applicant;

(ii) the reasons for being minded not to register him; and

(iii) the right to make representations to it within a specified period (which may not be less than 28 days).

(5) The Authority or the OFT, as the case may be, must then decide, within a reasonable period, whether to register the applicant and it must give the applicant notice of—

(a) its decision to register the applicant; or

(b) the following matters—

(i) its decision not to register the applicant;

(ii) the reasons for its decision; and

(iii) the right to appeal under regulation 44(1)(b).

(6) The Authority or the OFT, as the case may be, must, as soon as reasonably practicable after deciding to register a person, include him in the relevant register.

(7) The Authority or the OFT may cancel a person's registration in a register maintained by them under regulation 32 if, at any time after registration, it appears to them that they would have had grounds to refuse registration under paragraph (3).

(8) Where the Authority or the OFT proposes to cancel a person's registration, it must give him notice of—

(a) its proposal to cancel his registration;

(b) the reasons for the proposed cancellation; and

(c) the right to make representations to it within a specified period (which may not be less than 28 days).

(9) The Authority or the OFT, as the case may be, must then decide, within a reasonable period, whether to cancel the person's registration and it must give him notice of—

(a) its decision not to cancel his registration; or

(b) the following matters—

(i) its decision to cancel his registration and, subject to paragraph (10), the date from which cancellation takes effect;

(ii) the reasons for its decision; and

(iii) the right to appeal under regulation 44(1)(b).

(10) If the Authority or the OFT, as the case may be—

(a) considers that the interests of the public require the cancellation of a person's registration to have immediate effect; and

(b) includes a statement to that effect and the reasons for it in the notice given under paragraph (9)(b),

the cancellation takes effect when the notice is given to the person.

(11) In paragraphs (3) and (4), references to regulation 27 are to be treated as references to that paragraph as applied by paragraph (2) of this regulation.

Financial provisions

Costs of supervision

35.—(1) The Authority, the OFT and the Commissioners may impose charges—

(a) on applicants for registration;

(b) on relevant persons supervised by them.

(2) Charges levied under paragraph (1) must not exceed such amount as the Authority, the OFT or the Commissioners (as the case may be) consider will enable them to meet any expenses

reasonably incurred by them in carrying out their functions under these Regulations or for any incidental purpose.

(3) Without prejudice to the generality of paragraph (2), a charge may be levied in respect of each of the premises at which a person carries on (or proposes to carry on) business.

(4) The Authority must apply amounts paid to it by way of penalties imposed under regulation 42 towards expenses incurred in carrying out its functions under these Regulations or for any incidental purpose.

(5) In paragraph (2), "expenses" in relation to the OFT includes expenses incurred by a local weights and measures authority or DETI pursuant to arrangements made for the purposes of these Regulations with the OFT—

(a) by or on behalf of the authority; or

(b) by DETI.

PART 5

ENFORCEMENT

Powers of designated authorities

Interpretation

36. In this Part—

"designated authority" means—

(a) the Authority;

(b) the Commissioners;

(c) the OFT; and

(d) in relation to credit unions in Northern Ireland, DETI;

"officer", except in regulations 40(3), 41 and 47 means—

(a) an officer of the Authority, including a member of the Authority's staff or an agent of the Authority;

(b) an officer of Revenue and Customs;

(c) an officer of the OFT;

(d) a relevant officer; or

(e) an officer of DETI acting for the purposes of its functions under these Regulations in relation to credit unions in Northern Ireland;

"recorded information" includes information recorded in any form and any document of any nature;

"relevant officer" means—

(a) in Great Britain, an officer of a local weights and measures authority;

(b) in Northern Ireland, an officer of DETI acting pursuant to arrangements made with the OFT for the purposes of these Regulations.

Power to require information from, and attendance of, relevant and connected persons

37.—(1) An officer may, by notice to a relevant person or to a person connected with a relevant person, require the relevant person or the connected person, as the case may be—

(a) to provide such information as may be specified in the notice;

(b) to produce such recorded information as may be so specified; or

(c) to attend before an officer at a time and place specified in the notice and answer questions.

(2) For the purposes of paragraph (1), a person is connected with a relevant person if he is, or has at any time been, in relation to the relevant person, a person listed in Schedule 4 to these Regulations.

(3) An officer may exercise powers under this regulation only if the information sought to be obtained as a result is reasonably required in connection with the exercise by the designated authority for whom he acts of its functions under these Regulations.

(4) Where an officer requires information to be provided or produced pursuant to paragraph (1)(a) or (b)—

(a) the notice must set out the reasons why the officer requires the information to be provided or produced; and

(b) such information must be provided or produced—

(i) before the end of such reasonable period as may be specified in the notice; and

(ii) at such place as may be so specified.

(5) In relation to information recorded otherwise than in legible form, the power to require production of it includes a power to require the production of a copy of it in legible form or in a form from which it can readily be produced in visible and legible form.

(6) The production of a document does not affect any lien which a person has on the document.

(7) A person may not be required under this regulation to provide or produce information or to answer questions which he would be entitled to refuse to provide, produce or answer on grounds of legal professional privilege in proceedings in the High Court, except that a lawyer may be required to provide the name and address of his client.

(8) Subject to paragraphs (9) and (10), a statement made by a person in compliance with a requirement imposed on him under paragraph (1)(c) is admissible in evidence in any proceedings, so long as it also complies with any requirements governing the admissibility of evidence in the circumstances in question.

(9) In criminal proceedings in which a person is charged with an offence to which this paragraph applies—

(a) no evidence relating to the statement may be adduced; and

(b) no question relating to it may be asked,

by or on behalf of the prosecution unless evidence relating to it is adduced, or a question relating to it is asked, in the proceedings by or on behalf of that person.

(10) Paragraph (9) applies to any offence other than one under—

(a) section 5 of the Perjury Act 1911(**bs**) (false statements without oath);

(b) section 44(2) of the Criminal Law (Consolidation)(Scotland) Act 1995(**bt**) (false statements and declarations); or

(c) Article 10 of the Perjury (Northern Ireland) Order 1979(**bu**) (false unsworn statements).

(11) In the application of this regulation to Scotland, the reference in paragraph (7) to—

(a) proceedings in the High Court is to be read as a reference to legal proceedings generally; and

(b) an entitlement on grounds of legal professional privilege is to be read as a reference to an entitlement on the grounds of confidentiality of communications.

Entry, inspection without a warrant etc.

38.—(1) Where an officer has reasonable cause to believe that any premises are being used by a relevant person in connection with his business or professional activities, he may on producing evidence of his authority at any reasonable time—

(a) enter the premises;

(b) inspect the premises;

(c) observe the carrying on of business or professional activities by the relevant person;

(d) inspect any recorded information found on the premises;

(e) require any person on the premises to provide an explanation of any recorded information or to state where it may be found;

(f) in the case of a money service business or a high value dealer, inspect any cash found on the premises.

(2) An officer may take copies of, or make extracts from, any recorded information found under paragraph (1).

(3) Paragraphs (1)(d) and (e) and (2) do not apply to recorded information which the relevant person would be entitled to refuse to disclose on grounds of legal professional privilege in proceedings in the High Court, except that a lawyer may be required to provide the name and address of his client and, for this purpose, regulation 37(11) applies to this paragraph as it applies to regulation 37(7).

(4) An officer may exercise powers under this regulation only if the information sought to be obtained as a result is reasonably required in connection with the exercise by the designated authority for whom he acts of its functions under these Regulations.

(5) In this regulation, "premises" means any premises other than premises used only as a dwelling.

Entry to premises under warrant

39.—(1) A justice may issue a warrant under this paragraph if satisfied on information on oath given by an officer that there are reasonable grounds for believing that the first, second or third set of conditions is satisfied.

(2) The first set of conditions is—

(a) that there is on the premises specified in the warrant recorded information in relation to which a requirement could be imposed under regulation 37(1)(b); and

(b) that if such a requirement were to be imposed—

(i) it would not be complied with; or

(ii) the recorded information to which it relates would be removed, tampered with or destroyed.

(3) The second set of conditions is—

(a) that a person on whom a requirement has been imposed under regulation 37(1)(b) has failed (wholly or in part) to comply with it; and

(b) that there is on the premises specified in the warrant recorded information which has been required to be produced.

(4) The third set of conditions is—

(a) that an officer has been obstructed in the exercise of a power under regulation 38; and

(b) that there is on the premises specified in the warrant recorded information or cash which could be inspected under regulation 38(1)(d) or (f).

(5) A justice may issue a warrant under this paragraph if satisfied on information on oath given by an officer that there are reasonable grounds for suspecting that—

(a) an offence under these Regulations has been, is being or is about to be committed by a relevant person; and

(b) there is on the premises specified in the warrant recorded information relevant to whether that offence has been, or is being or is about to be committed.

(6) A warrant issued under this regulation shall authorise an officer—

(a) to enter the premises specified in the warrant;

(b) to search the premises and take possession of any recorded information or anything appearing to be recorded information specified in the warrant or to take, in relation to any such recorded information, any other steps which may appear to be necessary for preserving it or preventing interference with it;

(c) to take copies of, or extracts from, any recorded information specified in the warrant;

(d) to require any person on the premises to provide an explanation of any recorded information appearing to be of the kind specified in the warrant or to state where it may be found;

(e) to use such force as may reasonably be necessary.

(7) Where a warrant is issued by a justice under paragraph (1) or (5) on the basis of information given by an officer of the Authority, for "an officer" in paragraph (6) substitute "a constable".

(8) In paragraphs (1), (5) and (7), "justice" means—

(a) in relation to England and Wales, a justice of the peace;

(b) in relation to Scotland, a justice within the meaning of section 307 of the Criminal Procedure (Scotland) Act 1995(**bv**) (interpretation);

(c) in relation to Northern Ireland, a lay magistrate.

(9) In the application of this regulation to Scotland, the references in paragraphs (1) and (5) to information on oath are to be read as references to evidence on oath.

Failure to comply with information requirement

40.—(1) If, on an application made by—

(a) a designated authority; or

(b) a local weights and measures authority or DETI pursuant to arrangements made with the OFT—

(i) by or on behalf of the authority; or

(ii) by DETI,

it appears to the court that a person (the "information defaulter") has failed to do something that he was required to do under regulation 37(1), the court may make an order under this regulation.

(2) An order under this regulation may require the information defaulter—

(a) to do the thing that he failed to do within such period as may be specified in the order;

(b) otherwise to take such steps to remedy the consequences of the failure as may be so specified.

(3) If the information defaulter is a body corporate, a partnership or an unincorporated body of persons which is not a partnership, the order may require any officer of the body corporate, partnership or body, who is (wholly or partly) responsible for the failure to meet such costs of the application as are specified in the order.

(4) In this regulation, "court" means—

(a) in England and Wales and Northern Ireland, the High Court or the county court;

(b) in Scotland, the Court of Session or the sheriff.

Powers of relevant officers

41.—(1) A relevant officer may only exercise powers under regulations 37 to 39 pursuant to arrangements made with the OFT—

(a) by or on behalf of the local weights and measures authority of which he is an officer ("his authority"); or

(b) by DETI.

(2) Anything done or omitted to be done by, or in relation to, a relevant officer in the exercise or purported exercise of a power in this Part shall be treated for all purposes as having been done or omitted to be done by, or in relation to, an officer of the OFT.

(3) Paragraph (2) does not apply for the purposes of any criminal proceedings brought against the relevant officer, his authority, DETI or the OFT, in respect of anything done or omitted to be done by the officer.

(4) A relevant officer shall not disclose to any person other than the OFT and his authority or, as the case may be, DETI information obtained by him in the exercise of such powers unless—

(a) he has the approval of the OFT to do so; or

(b) he is under a duty to make the disclosure.

Civil penalties, review and appeals

Power to impose civil penalties

42.—(1) A designated authority may impose a penalty of such amount as it considers appropriate on a relevant person who fails to comply with any requirement in regulation 7(1), (2) or (3), 8(1) or (3), 9(2), 10(1), 11(1), 14(1), 15(1) or (2), 16(1), (2), (3) or (4), 19(1), (4), (5) or (6), 20(1), (4) or (5), 21, 26, 27(4) or 33 or a direction made under regulation 18 and, for this purpose, "appropriate" means effective, proportionate and dissuasive.

(2) The designated authority must not impose a penalty on a person under paragraph (1) where there are reasonable grounds for it to be satisfied that the person took all reasonable steps and exercised all due diligence to ensure that the requirement would be complied with.

(3) In deciding whether a person has failed to comply with a requirement of these Regulations, the designated authority must consider whether he followed any relevant guidance which was at the time—

(a) issued by a supervisory authority or any other appropriate body;

(b) approved by the Treasury; and

(c) published in a manner approved by the Treasury as suitable in their opinion to bring the guidance to the attention of persons likely to be affected by it.

(4) In paragraph (3), an "appropriate body" means any body which regulates or is representative of any trade, profession, business or employment carried on by the alleged offender.

(5) Where the Commissioners decide to impose a penalty under this regulation, they must give the person notice of—

(a) their decision to impose the penalty and its amount;

(b) the reasons for imposing the penalty;

(c) the right to a review under regulation 43; and

(d) the right to appeal under regulation 44(1)(a).

(6) Where the Authority, the OFT or DETI proposes to impose a penalty under this regulation, it must give the person notice of—

(a) its proposal to impose the penalty and the proposed amount;

(b) the reasons for imposing the penalty; and

(c) the right to make representations to it within a specified period (which may not be less than 28 days).

(7) The Authority, the OFT or DETI, as the case may be, must then decide, within a reasonable period, whether to impose a penalty under this regulation and it must give the person notice of—

(a) its decision not to impose a penalty; or

(b) the following matters—

(i) its decision to impose a penalty and the amount;

(ii) the reasons for its decision; and

(iii) the right to appeal under regulation 44(1)(b).

(8) A penalty imposed under this regulation is payable to the designated authority which imposes it.

Review procedure

43.—(1) This regulation applies to decisions of the Commissioners made under—

(a) regulation 29, to refuse to register an applicant;

(b) regulation 30, to cancel the registration of a registered person; and

(c) regulation 42, to impose a penalty.

(2) Any person who is the subject of a decision to which this regulation applies may by notice to the Commissioners require them to review that decision.

(3) The Commissioners need not review any decision unless the notice requiring the review is given within 45 days beginning with the date on which they first gave notice of the decision to the person requiring the review.

(4) Where the Commissioners are required under this regulation to review any decision they must either—

(a) confirm the decision; or

(b) withdraw or vary the decision and take such further steps (if any) in consequence of the withdrawal or variation as they consider appropriate.

(5) Where the Commissioners do not, within 45 days beginning with the date on which the review was required by a person, give notice to that person of their determination of the review, they are to be taken for the purposes of these Regulations to have confirmed the decision.

Appeals

44.—(1) A person may appeal from a decision by—

(a) the Commissioners on a review under regulation 43; and

(b) the Authority, the OFT or DETI under regulation 34 or 42.

(2) An appeal from a decision by—

(a) the Commissioners is to a VAT and duties tribunal(**bw**);

(b) the Authority is to the Financial Services and Markets Tribunal(**bx**);

(c) the OFT is to the Consumer Credit Appeals Tribunal(**by**); and

(d) DETI is to the High Court.

(3) The provisions of Part 5 of the Value Added Tax Act 1994(**bz**) (appeals), subject to the modifications set out in paragraph 1 of Schedule 5, apply in respect of appeals to a VAT and duties tribunal made under this regulation as they apply in respect of appeals made to such a tribunal under section 83 (appeals) of that Act.

(4) The provisions of Part 9 of the 2000 Act (hearings and appeals), subject to the modifications set out in paragraph 2 of Schedule 5, apply in respect of appeals to the Financial Services and Markets Tribunal made under this regulation as they apply in respect of references made to that Tribunal under that Act.

(5) Sections 40A (the Consumer Credit Appeals Tribunal), 41 (appeals to the Secretary of State under Part 3) and 41A (appeals from the Consumer Credit Appeals Tribunal) of the Consumer Credit Act 1974(**ca**) apply in respect of appeals to the Consumer Credit Appeal Tribunal made under this regulation as they apply in respect of appeals made to that Tribunal under section 41 of that Act.

(6) A VAT and duties tribunal hearing an appeal under paragraph (2) has the power to—

(a) quash or vary any decision of the supervisory authority, including the power to reduce any penalty to such amount (including nil) as they think proper; and

(b) substitute their own decision for any decision quashed on appeal.

(7) Notwithstanding paragraph (2)(c), until the coming into force of section 55 of the Consumer Credit Act 2006(**cb**) (the Consumer Credit Appeals Tribunal), an appeal from a decision by the OFT is to the Financial Services and Markets Tribunal and, for these purposes, the coming into force of that section shall not affect—

(a) the hearing and determination by the Financial Service and Markets Tribunal of an appeal commenced before the coming into force of that section ("the original appeal"); or

(b) any appeal against the decision of the Financial Services and Markets Tribunal with respect to the original appeal.

(8) The modifications in Schedule 5 have effect for the purposes of appeals made under this regulation.

Criminal offences

Offences

45.—(1) A person who fails to comply with any requirement in regulation 7(1), (2) or (3), 8(1) or (3), 9(2), 10(1), 11(1)(a), (b) or (c), 14(1), 15(1) or (2), 16(1), (2), (3) or (4), 19(1), (4), (5) or (6), 20(1), (4) or (5), 21, 26, 27(4) or 33, or a direction made under regulation 18, is guilty of an offence and liable—

(a) on summary conviction, to a fine not exceeding the statutory maximum;

(bz) 1994 c. 23.

(ca) Sections 40A and 41A were inserted by respectively sections 55 and 57 of the Consumer Credit Act 2006 and section 41 was amended by section 56 of that Act.

(cb) 2006 c. 14.

(b) on conviction on indictment, to imprisonment for a term not exceeding two years, to a fine or to both.

(2) In deciding whether a person has committed an offence under paragraph (1), the court must consider whether he followed any relevant guidance which was at the time—

(a) issued by a supervisory authority or any other appropriate body;

(b) approved by the Treasury; and

(c) published in a manner approved by the Treasury as suitable in their opinion to bring the guidance to the attention of persons likely to be affected by it.

(3) In paragraph (2), an "appropriate body" means any body which regulates or is representative of any trade, profession, business or employment carried on by the alleged offender.

(4) A person is not guilty of an offence under this regulation if he took all reasonable steps and exercised all due diligence to avoid committing the offence.

(5) Where a person is convicted of an offence under this regulation, he shall not also be liable to a penalty under regulation 42.

Prosecution of offences

46.—(1) Proceedings for an offence under regulation 45 may be instituted by—

(a) the Director of Revenue and Customs Prosecutions or by order of the Commissioners;

(b) the OFT;

(c) a local weights and measures authority;

(d) DETI;

(e) the Director of Public Prosecutions; or

(f) the Director of Public Prosecutions for Northern Ireland.

(2) Proceedings for an offence under regulation 45 may be instituted only against a relevant person or, where such a person is a body corporate, a partnership or an unincorporated association, against any person who is liable to be proceeded against under regulation 47.

(3) Where proceedings under paragraph (1) are instituted by order of the Commissioners, the proceedings must be brought in the name of an officer of Revenue and Customs.

(4) Where a local weights and measures authority in England or Wales proposes to institute proceedings for an offence under regulation 45 it must give the OFT notice of the intended proceedings, together with a summary of the facts on which the charges are to be founded.

(5) A local weights and measures authority must also notify the OFT of the outcome of the proceedings after they are finally determined.

(6) A local weights and measures authority must, whenever the OFT requires, report in such form and with such particulars as the OFT requires on the exercise of its functions under these Regulations.

(7) Where the Commissioners investigate, or propose to investigate, any matter with a view to determining—

(a) whether there are grounds for believing that an offence under regulation 45 has been committed by any person; or

(b) whether such a person should be prosecuted for such an offence,

that matter is to be treated as an assigned matter within the meaning of section 1(1) of the Customs and Excise Management Act 1979(**cc**).

(cc) 1979 c. 2. There are amendments to section 1 not relevant to these Regulations.

(8) Paragraphs (1) and (3) to (6) do not extend to Scotland.

Offences by bodies corporate etc.

47.—(1) If an offence under regulation 45 committed by a body corporate is shown—

(a) to have been committed with the consent or the connivance of an officer of the body corporate; or

(b) to be attributable to any neglect on his part,

the officer as well as the body corporate is guilty of an offence and liable to be proceeded against and punished accordingly.

(2) If an offence under regulation 45 committed by a partnership is shown—

(a) to have been committed with the consent or the connivance of a partner; or

(b) to be attributable to any neglect on his part,

the partner as well as the partnership is guilty of an offence and liable to be proceeded against and punished accordingly.

(3) If an offence under regulation 45 committed by an unincorporated association (other than a partnership) is shown—

(a) to have been committed with the consent or the connivance of an officer of the association; or

(b) to be attributable to any neglect on his part,

that officer as well as the association is guilty of an offence and liable to be proceeded against and punished accordingly.

(4) If the affairs of a body corporate are managed by its members, paragraph (1) applies in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body.

(5) Proceedings for an offence alleged to have been committed by a partnership or an unincorporated association must be brought in the name of the partnership or association (and not in that of its members).

(6) A fine imposed on the partnership or association on its conviction of an offence is to be paid out of the funds of the partnership or association.

(7) Rules of court relating to the service of documents are to have effect as if the partnership or association were a body corporate.

(8) In proceedings for an offence brought against the partnership or association—

(a) section 33 of the Criminal Justice Act 1925(**cd**) (procedure on charge of offence against corporation) and Schedule 3 to the Magistrates' Courts Act 1980(**ce**) (corporations) apply as they do in relation to a body corporate;

(b) section 70 (proceedings against bodies corporate) of the Criminal Procedure (Scotland) Act 1995(**cf**) applies as it does in relation to a body corporate;

(c) section 18 of the Criminal Justice (Northern Ireland) Act 1945(**cg**) (procedure on charge) and Schedule 4 to the Magistrates' Courts (Northern Ireland) Order 1981(**ch**) (corporations) apply as they do in relation to a body corporate.

(9) In this regulation—

"officer"—

(a) in relation to a body corporate, means a director, manager, secretary, chief executive, member of the committee of management, or a person purporting to act in such a capacity; and

(b) in relation to an unincorporated association, means any officer of the association or any member of its governing body, or a person purporting to act in such capacity; and

"partner" includes a person purporting to act as a partner.

PART 6

MISCELLANEOUS

Recovery of charges and penalties through the court

48. Any charge or penalty imposed on a person by a supervisory authority under regulation 35(1) or 42(1) is a debt due from that person to the authority, and is recoverable accordingly.

Obligations on public authorities

49.—(1) The following bodies and persons must, if they know or suspect or have reasonable grounds for knowing or suspecting that a person is or has engaged in money laundering or terrorist financing, as soon as reasonably practicable inform the Serious Organised Crime Agency—

(a) the Auditor General for Scotland;

(b) the Auditor General for Wales;

(c) the Authority;

(d) the Bank of England;

(e) the Comptroller and Auditor General;

(f) the Comptroller and Auditor General for Northern Ireland;

(g) the Gambling Commission;

(h) the OFT;

(i) the Official Solicitor to the Supreme Court;

(j) the Pensions Regulator;

(k) the Public Trustee;

(l) the Secretary of State, in the exercise of his functions under enactments relating to companies and insolvency;

(m) the Treasury, in the exercise of their functions under the 2000 Act;

(n) the Treasury Solicitor;

(o) a designated professional body for the purposes of Part 20 of the 2000 Act (provision of financial services by members of the professions);

(p) a person or inspector appointed under section 65 (investigations on behalf of Authority) or 66 (inspections and special meetings) of the Friendly Societies Act 1992(**ci**);

(q) an inspector appointed under section 49 of the Industrial and Provident Societies Act 1965(**cj**) (appointment of inspectors) or section 18 of the Credit Unions Act 1979(**ck**) (power to appoint inspector);

(r) an inspector appointed under section 431 (investigation of a company on its own application), 432 (other company investigations), 442 (power to investigate company ownership) or 446 (investigation of share dealing) of the Companies Act 1985(**cl**) or under Article 424, 425, 435 or 439 of the Companies (Northern Ireland) Order 1986(**cm**);

(s) a person or inspector appointed under section 55 (investigations on behalf of Authority) or 56 (inspections and special meetings) of the Building Societies Act 1986(**cn**);

(t) a person appointed under section 167 (appointment of persons to carry out investigations), 168(3) or (5) (appointment of persons to carry out investigations in particular cases), 169(1)(b) (investigations to support overseas regulator) or 284 (power to investigate affairs of a scheme) of the 2000 Act, or under regulations made under section 262(2)(k) (open-ended investment companies) of that Act, to conduct an investigation; and

(u) a person authorised to require the production of documents under section 447 of the Companies Act 1985 (Secretary of State's power to require production of documents), Article 440 of the Companies (Northern Ireland) Order 1986 or section 84 of the Companies Act 1989(**co**) (exercise of powers by officer).

(2) A disclosure made under paragraph (1) is not to be taken to breach any restriction on the disclosure of information however imposed.

Transitional provisions: requirement to be registered

50.—(1) Regulation 26 does not apply to an existing money service business, an existing trust or company service provider or an existing high value dealer until—

(a) where it has applied in accordance with regulation 27 before the specified date for registration in a register maintained under regulation 25(1) (a "new register")—

(i) the date it is included in a new register following the determination of its application by the Commissioners; or

(ii) where the Commissioners give it notice under regulation 29(2)(b) of their decision not to register it, the date on which the Commissioners state that the decision takes effect or, where a statement is included in accordance with paragraph (3)(b), the time at which the Commissioners give it such notice;

(b) in any other case, the specified date.

(2) The specified date is—

(a) in the case of an existing money service business, 1st February 2008;

(b) in the case of an existing trust or company service provider, 1st April 2008;

(c) in the case of an existing high value dealer, the first anniversary which falls on or after 1st January 2008 of the date of its registration in a register maintained under regulation 10 of the Money Laundering Regulations 2003.

(3) In the case of an application for registration in a new register made before the specified date by an existing money service business, an existing trust or company service provider or an existing high value dealer, the Commissioners must include in a notice given to it under regulation 29(2)(b)—

(a) the date on which their decision is to take effect; or

(b) if the Commissioners consider that the interests of the public require their decision to have immediate effect, a statement to that effect and the reasons for it.

(4) In the case of an application for registration in a new register made before the specified date by an existing money services business or an existing trust or company service provider, the Commissioners must give it a notice under regulation 29(2) by—

(a) in the case of an existing money service business, 1st June 2008;

(b) in the case of an existing trust or company service provider, 1st July 2008; or

(c) where applicable, 45 days beginning with the date on which they receive any further information required under regulation 27(3).

(5) In this regulation—

"existing money service business" and an "existing high value dealer" mean a money service business or a high value dealer which, immediately before 15th December 2007, was included in a register maintained under regulation 10 of the Money Laundering Regulations 2003;

"existing trust or company service provider" means a trust or company service provider carrying on business in the United Kingdom immediately before 15th December 2007.

Minor and consequential amendments

51. Schedule 6, which contains minor and consequential amendments to primary and secondary legislation, has effect.

Signatory text

Alan Campbell
Frank Roy
Two Lords Commissioners of
Her Majesty's Treasury

24th July 2007

SCHEDULE 1

Regulation 3(3)(a)

ACTIVITIES LISTED IN POINTS 2 TO 12 AND 14 OF ANNEX I TO THE BANKING CONSOLIDATION DIRECTIVE

2. Lending including, inter alia: consumer credit, mortgage credit, factoring, with or without recourse, financing of commercial transactions (including forfeiting).

3. Financial leasing.

4. Money transmission services.

5. Issuing and administering means of payment (e.g. credit cards, travellers' cheques and bankers' drafts).

6. Guarantees and commitments.

7. Trading for own account or for account of customers in:

(a) money market instruments (cheques, bills, certificates of deposit, etc.);

(b) foreign exchange;

(c) financial futures and options;

(d) exchange and interest-rate instruments; or

(e) transferable securities.

8. Participation in securities issues and the provision of services related to such issues.

9. Advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings.

10. Money broking.

11. Portfolio management and advice.

12. Safekeeping and administration of securities.

14. Safe custody services

SCHEDULE 2

Regulations 4(1)(e) and (2), 13(6) and (8) and 14(5).

FINANCIAL ACTIVITY, SIMPLIFIED DUE DILIGENCE AND POLITICALLY EXPOSED PERSONS

Financial activity on an occasional or very limited basis

1. For the purposes of regulation 4(1)(e) and (2), a person is to be considered as engaging in financial activity on an occasional or very limited basis if all the following conditions are fulfilled—

(a) the person's total annual turnover in respect of the financial activity does not exceed £64,000;

(b) the financial activity is limited in relation to any customer to no more than one transaction exceeding 1,000 euro, whether the transaction is carried out in a single operation, or a series of operations which appear to be linked;

(c) the financial activity does not exceed 5% of the person's total annual turnover;

(d) the financial activity is ancillary and directly related to the person's main activity;

(e) the financial activity is not the transmission or remittance of money (or any representation of monetary value) by any means;

(f) the person's main activity is not that of a person falling within regulation 3(1)(a) to (f) or (h);

(g) the financial activity is provided only to customers of the person's main activity and is not offered to the public.

Simplified due diligence

2. For the purposes of regulation 13(6), the conditions are—

(a) the authority has been entrusted with public functions pursuant to the Treaty on the European Union(**cp**), the Treaties on the European Communities or Community secondary legislation;

(b) the authority's identity is publicly available, transparent and certain;

(c) the activities of the authority and its accounting practices are transparent;

(d) either the authority is accountable to a Community institution or to the authorities of an EEA state, or otherwise appropriate check and balance procedures exist ensuring control of the authority's activity.

3. For the purposes of regulation 13(8), the conditions are—

(a) the product has a written contractual base;

(b) any related transaction is carried out through an account of the customer with a credit institution which is subject to the money laundering directive or with a credit institution situated in a non-EEA state which imposes requirements equivalent to those laid down in that directive;

(c) the product or related transaction is not anonymous and its nature is such that it allows for the timely application of customer due diligence measures where there is a suspicion of money laundering or terrorist financing;

(d) the product is within the following maximum threshold—

(i) in the case of insurance policies or savings products of a similar nature, the annual premium is no more than 1,000 euro or there is a single premium of no more than 2,500 euro;

(ii) in the case of products which are related to the financing of physical assets where the legal and beneficial title of the assets is not transferred to the customer until the termination of the contractual relationship (whether the transaction is carried out in a single operation or in several operations which appear to be linked), the annual payments do not exceed 15,000 euro;

(iii) in all other cases, the maximum threshold is 15,000 euro;

(e) the benefits of the product or related transaction cannot be realised for the benefit of third parties, except in the case of death, disablement, survival to a predetermined advanced age, or similar events;

(f) in the case of products or related transactions allowing for the investment of funds in financial assets or claims, including insurance or other kinds of contingent claims—

(i) the benefits of the product or related transaction are only realisable in the long term;

(ii) the product or related transaction cannot be used as collateral; and

(iii) during the contractual relationship, no accelerated payments are made, surrender clauses used or early termination takes place.

Politically exposed persons

4.—(1) For the purposes of regulation 14(5)—

(a) individuals who are or have been entrusted with prominent public functions include the following—

(i) heads of state, heads of government, ministers and deputy or assistant ministers;

(ii) members of parliaments;

(iii) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, other than in exceptional circumstances;

(iv) members of courts of auditors or of the boards of central banks;

(v) ambassadors, chargés d'affaires and high-ranking officers in the armed forces; and

(vi) members of the administrative, management or supervisory bodies of state-owned enterprises;

(b) the categories set out in paragraphs (i) to (vi) of sub-paragraph (a) do not include middle-ranking or more junior officials;

(c) immediate family members include the following—

(i) a spouse;

(ii) a partner;

(iii) children and their spouses or partners; and

(iv) parents;

(d) persons known to be close associates include the following—

(i) any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person referred to in regulation 14(5)(a); and

(ii) any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person referred to in regulation 14(5)(a).

(2) In paragraph (1)(c), "partner" means a person who is considered by his national law as equivalent to a spouse.

SCHEDULE 3 Regulations 17(2)(b), 23(1)(c) and 32(4)

PROFESSIONAL BODIES

PART 1

1. Association of Chartered Certified Accountants

2. Council for Licensed Conveyancers

3. Faculty of Advocates

4. General Council of the Bar

5. General Council of the Bar of Northern Ireland

6. Institute of Chartered Accountants in England and Wales

7. Institute of Chartered Accountants in Ireland

8. Institute of Chartered Accountants of Scotland

9. Law Society

10. Law Society of Scotland

11. Law Society of Northern Ireland

PART 2

12. Association of Accounting Technicians

13. Association of International Accountants

14. Association of Taxation Technicians

15. Chartered Institute of Management Accountants

16. Chartered Institute of Public Finance and Accountancy

17. Chartered Institute of Taxation

18. Faculty Office of the Archbishop of Canterbury

19. Insolvency Practitioners Association

20. Institute of Certified Bookkeepers

21. Institute of Financial Accountants

SCHEDULE 4

Regulation 37(2)

CONNECTED PERSONS

Corporate bodies

1. If the relevant person is a body corporate ("BC"), a person who is or has been—

(a) an officer or manager of BC or of a parent undertaking of BC;

(b) an employee of BC;

(c) an agent of BC or of a parent undertaking of BC.

Partnerships

2. If the relevant person is a partnership, a person who is or has been a member, manager, employee or agent of the partnership.

Unincorporated associations

3. If the relevant person is an unincorporated association of persons which is not a partnership, a person who is or has been an officer, manager, employee or agent of the association.

Individuals

4. If the relevant person is an individual, a person who is or has been an employee or agent of that individual.

SCHEDULE 5 Regulation 44(8)

MODIFICATIONS IN RELATION TO APPEALS

PART 1

Primary legislation

The Value Added Tax Act 1994 (c. 23)

1. Part 5 of the Value Added Tax Act 1994 (appeals) is modified as follows—

(a) omit section 84; and

(b) in paragraphs (1)(a), (2)(a) and (3)(a) of section 87, omit ", or is recoverable as, VAT".

The Financial Services and Markets Act 2000 (c. 8)

2. Part 9 of the 2000 Act (hearings and appeals) is modified as follows—

(a) in the application of section 133 and Schedule 13 to any appeal commenced before the coming into force of section 55 of the Consumer Credit Act 2006, for all the references to "the Authority", substitute "the Authority or the OFT (as the case may be)";

(b) in section 133(1)(a) for "decision notice or supervisory notice in question" substitute "notice under regulation 34(5) or (9) or 42(7) of the Money Laundering Regulations 2007";

(c) in section 133 omit subsections (6), (7), (8) and (12); and

(d) in section 133(9) for "decision notice" in both places where it occurs substitute "notice under regulation 34(5) or (9) or 42(7) of the Money Laundering Regulations 2007".

PART 2

Secondary legislation

The Financial Services and Markets Tribunal Rules 2001

3. In the application of the Financial Services and Markets Tribunal Rules 2001(**cq**) to any appeal commenced before the coming into force of section 55 of the Consumer Credit Act 2006, for all the references to "the Authority" substitute "the Authority or the OFT (as the case may be)".

(cq) S.I.2001/2476.

SCHEDULE 6 Regulation 51

MINOR AND CONSEQUENTIAL AMENDMENTS

PART 1

Primary legislation

The Value Added Tax Act 1994 (c. 23)

1. In section 83 of the Value Added Tax Act 1994(**cr**) (appeals), omit paragraph (zz).

The Northern Ireland Act 1998 (c. 47)

2. In paragraph 25 of Schedule 3 to the Northern Ireland Act 1998(**cs**) (reserved matters), for "2003" substitute "2007".

The Criminal Justice and Police Act 2001 (c. 16)

3. In Part 1 of Schedule 1 to the Criminal Justice and Police Act 2001(**ct**) (powers of seizure to which section 50 of the 2001 Act applies), after paragraph 73I insert—

"**The Money Laundering Regulations 2007**

73J. The power of seizure conferred by regulation 39(6) of the Money Laundering Regulations 2007 (entry to premises under warrant)."

PART 2

Secondary legislation

The Independent Qualified Conveyancers (Scotland) Regulations 1997

4. Regulation 28 of the Independent Qualified Conveyancers (Scotland) Regulations 1997(**cu**) is revoked.

The Executry Practitioners (Scotland) Regulations 1997

5. Regulation 26 of the Executry Practitioners (Scotland) Regulations 1997(**cv**) is revoked.

The Cross-Border Credit Transfers Regulations 1999

6. In regulation 12(2) of the Cross-Border Credit Transfers Regulations 1999(**cw**), for "2003" substitute "2007".

(cr) 1994 c. 23. Section 83(zz) was inserted by S.I. 2001/3541 and amended by S.I. 2003/3075.
(cs) 1998 c. 47. Paragraph 25 of Schedule 3 was amended by S.I. 2003/3075.
(ct) 2001 c. 16. Section 73I was inserted by the Animal Welfare Act 2006, section 64, Schedule 3, paragraph 14(3).
(cu) S.S.I. 1997/316.
(cv) S.S.I. 1997/317.
(cw) S.I. 1999/1876, amended by S.I. 2003/3075.

The Terrorism Act 2000 (Crown Servants and Regulators) Regulations 2001

7. In regulation 2 of the Terrorism Act 2000 (Crown Servants and Regulators) Regulations 2001(**cx**), in the definition of "relevant business", for "has the meaning given by regulation 2(2) of the Money Laundering Regulations 2003" substitute "means an activity carried on in the course of business by any of the persons listed in regulation 3(1)(a) to (h) of the Money Laundering Regulations 2007".

The Representation of the People (England and Wales) Regulations 2001

8. In regulation 114(3)(b) of the Representation of the People (England and Wales) Regulations 2001(**cy**), for "2003" substitute "2007".

The Representation of the People (Scotland) Regulations 2001

9. In regulation 113(3)(b) of the Representation of the People (Scotland) Regulations 2001(**cz**), for "2003" substitute "2007".

The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001

10. In article 72E(9) of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001(**da**), for "2003" substitute "2007".

The Proceeds of Crime Act 2002 (Failure to Disclose Money Laundering: Specified Training) Order 2003

11. In article 2 of the Proceeds of Crime Act 2002 (Failure to Disclose Money Laundering: Specified Training) Order 2003(**db**), for "regulation 3(1)(c)(ii) of the Money Laundering Regulations 2003" substitute "regulation 21 of the Money Laundering Regulations 2007".

The Public Contracts (Scotland) Regulations 2006

12. In regulation 23(1)(f) of the Public Contracts (Scotland) Regulations 2006(**dc**), for "2003" substitute "2007".

The Utilities Contracts (Scotland) Regulations 2006

13. In regulation 26(1)(f) of the Utilities Contracts (Scotland) Regulations 2006(**dd**), for "2003" substitute "2007".

The Public Contracts Regulations 2006

14. In regulation 23(1)(e) of the Public Contracts Regulations 2006(**de**), for "2003" substitute "2007".

(cx) S.I. 2001/192, amended by S.I. 2003/3075.
(cy) S.I. 2001/341, amended by S.I. 2002/1871, 2003/3075.
(cz) S.S.I. 2001/497, amended by S.I. 2002/1871, 2003/3075.
(da) S.I. 2001/544, amended by S.I. 2005/1518.
(db) S.I. 2003/171, amended by S.I. 2003/3075.
(dc) S.S.I. 2006/1.
(dd) S.S.I. 2006/2.
(de) S.I. 2006/5.

The Utilities Contracts Regulations 2006

15. In regulation 26(1)(e) of the Utilities Contracts Regulations 2006(**df**), for "2003" substitute "2007".

EXPLANATORY NOTE

(This note is not part of the Regulations)

These Regulations replace the Money Laundering Regulations 2003 (S.I. 2003/3075) with updated provisions which implement in part Directive 2005/60/EC (OJ No L 309, 25.11.2005, p.15) of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. A Transposition Note setting out how the main elements of this directive will be transposed into UK law is available from the Financial Services Team, HM Treasury, 1 Horse Guards Road, London SW1A 2HQ. An impact assessment has also been prepared. Copies of both documents have been placed in the library of each House of Parliament and are available on HM Treasury's website (www.hm-treasury.gov.uk).

The Regulations provide for various steps to be taken by the financial services sector and other persons to detect and prevent money laundering and terrorist financing. Obligations are imposed on "relevant persons" (defined in regulation 3 and subject to the exclusions in regulation 4), who are credit and financial institutions, auditors, accountants, tax advisers and insolvency practitioners, independent legal professionals, trust or company service providers, estate agents, high value dealers and casinos.

Relevant persons are required, when undertaking certain activities in the course of business, to apply customer due diligence measures where they establish a business relationship, carry out an occasional transaction, suspect money laundering or terrorist finance or doubt the accuracy of customer identification information (regulation 7). Customer due diligence measures (defined in regulation 5) consist of identifying and verifying the identity of the customer and any beneficial owner (defined in regulation 6) of the customer, and obtaining information on the purpose and intended nature of the business relationship. Relevant persons also have to undertake ongoing monitoring of their business relationships (regulation 8).

Regulation 9 sets out the general rule on the timing of the verification of the customer's identity and certain exceptions. Regulation 10 sets out when casinos must identify and verify their customers. Failure to apply such measures means that a person cannot establish or continue a business relationship with the customer concerned or undertake an occasional transaction (regulation 11). Regulation 12 provides an exception from the requirement to identify the beneficial owner for debt issues held in trust.

Relevant persons may apply simplified customer due diligence measures for the products, customers or transactions listed in regulation 13 and must apply enhanced measures in the four situations set out in regulation 14. Regulation 15 sets out the obligations on relevant persons in respect of their overseas branches and subsidiaries. Regulation 16 imposes obligations in respect of shell banks and anonymous accounts. Regulation 17 lists the persons on whom relevant persons can rely to perform customer due diligence measures. Regulation 18 provides for the Treasury to make directions where the Financial Action Task Force applies counter-measures to a non-EEA state.

(df) S.I. 2006/6.

Part 3 imposes obligations in respect of record-keeping (regulation 19), policies and procedures (regulation 20) and staff training (regulation 21).

Part 4 deals with supervision and registration. Regulation 23 allocates supervisory authorities for different relevant persons. Regulation 24 sets out the duties of supervisors. Money service businesses, high value dealers and trust or company service providers which are not otherwise registered are subject to a system of mandatory registration set out in regulations 25 to 30. Money service businesses and trust or company service providers must not be registered unless the business, its owners, its nominated officer and senior managers are fit and proper persons: regulation 28. Other sectors will only be required to register if the supervisor decides to maintain a register (regulations 33 and 34). Regulation 35 enables supervisors to impose charges on persons they supervise.

Part 5 provides enforcement powers for certain supervisors, including powers to obtain information and enter and inspect premises (regulations 37 to 41). Civil penalties may be imposed by these supervisors under regulation 42 on persons who fail to comply with the requirements of Parts 2, 3 and 4. Provision is made for reviews of and appeals against such penalties (regulations 43 and 44). Relevant persons who fail to comply with the requirements of Parts 2, 3 and 4 will also be guilty of a criminal offence: regulations 45 to 47. Persons convicted of a criminal offence may not also be liable to a civil penalty.

Part 6 contains provision for the recovery of penalties and charges through the court (regulation 48), imposes an obligation on certain public authorities to report suspicions of money laundering or terrorist financing (regulation 49) and makes transitional provision (regulation 50). Regulation 51 makes minor and consequential amendments to primary and secondary legislation.

Annex F

Table of references drawn upon in drafting the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Bill

Clause	Heading	References
Part 1	Preliminary	
cl. 4	Immunity	• s55A of Insurance Companies Ordinance (Cap 41) • s51(3) of Electronic Transactions Ordinance (Cap 553)
Part 2	Requirements Relating to Customer Due Diligence and Record-keeping	
cl. 7	Relevant authority may publish guidelines	• s193(3) and s399 (5), (6) and (8) of Securities and Futures Ordinance, Cap 571 ("SFO")
Part 3	Supervision and Investigations	• Part VIII of SFO
cl.8	Interpretation of Part 3	• s178 of SFO
cl. 9	Power to enter business premises etc. for routine inspection	• s180(1)-(13) of SFO
cl. 10	Offences for non-non-compliance with requirements imposed under section 9	• s180(14)-(16) of SFO
cl. 11	Relevant authorities may appoint investigators	• s182 of SFO
cl. 12	Powers of investigators to require production of records or documents etc.	• s183 of SFO
cl. 13	Offences for non-compliance with requirements imposed under section 12	• s184 of SFO
cl. 14	Application to Court of First Instance relating to non-compliance with	• s185 of SFO

Clause	Heading	References
	requirements imposed under section 9 or 12	
cl. 15	Use of incriminating evidence in proceedings	• s187 of SFO
cl. 16	Lien claimed on records or documents	• s188 of SFO
cl. 17	Magistrate's warrants	• s191 of SFO
cl. 18	Production of information in information system etc.	• s189 of SFO
cl. 19	Inspection of records and documents seized etc.	• s190 of SFO
cl. 20	Destruction of documents etc.	• s192 of SFO
Part 4	Disciplinary Actions by Relevant Authorities	
cl. 21	Relevant authorities may take disciplinary actions	• s194 of SFO
cl. 22	Procedural requirements in respect of exercise of powers under section 21	• s198(1)-(2) of SFO
cl. 23	Guidelines on how relevant authorities exercise power to impose pecuniary penalty	• s199 of SFO
Part 5	Regulation of Operation of Money Service	
cl. 28	Certified copy of register or entry in register admissible as evidence	• s5 of Travel Agents Regulations (Cap 218A)
cl. 39	Licensee's duty to notify Commissioner of changes in particulars	• s24B(6) of Organized and Serious Crimes Ordinance (Cap 455)
cl. 40	Licensee's duty to notify Commissioner of cessation of business	• s24B(6) of Organized and Serious Crimes Ordinance (Cap 455)
cl. 42	Commissioner may take disciplinary actions	• mirrors clause 21

Clause	Heading	References
cl. 43	Procedural requirements in respect of exercise of powers under section 42	• mirrors clause 22
cl. 44	Guidelines on how Commissioner exercise power to impose pecuniary penalty	• mirrors clause 23
cl. 46	Warrant to enter premises to remove evidence of commission of offence	• s15, 16 and 17(1)(a) of Trade Description Ordinance (Cap 362)
cl. 47	Authorized officer's power to arrest and search, etc	• s16B of Trade Description Ordinance (Cap 362) and s50(1)(b) of Police Force Ordinance (Cap 232)
cl. 48	Preservation of secrecy	• s378 of SFO
cl. 51	Offence to provide false information in connection with application for licence etc.	• s383 of SFO
cl. 52	Time limit for prosecution	• s43B of Mandatory Provident Funds Ordinance (Cap 485)
Part 6	Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Review Tribunal	• Part VI of SFO
cl. 53	Interpretation of Part 6	• s215 of SFO
cl. 54	Establishment of Tribunal	• s216(1) and (5) of SFO
cl. 55	Composition of Tribunal	• s216(2) and (3) of SFO
cl. 56	Chairperson and other members of Tribunal may be paid fees	• s216(6) of SFO
cl. 57	Schedule 4 has effect	• s216(4) of SFO
cl. 58	Application for review of specified decisions	• s217(1), (3), (4), (5) and (6) of SFO
cl. 59	Determination of review by Tribunal	• s218(2), (3), (5) and (7) of SFO

Clause	Heading	References
cl. 60	Powers of Tribunal	• s219 of SFO
cl. 61	Use of incriminating evidence given under compulsion	• s220 of SFO
cl. 62	Contempt dealt with by Tribunal	• s221 of SFO
cl. 63	Privileged information	• s222 of SFO
cl. 64	Costs	• s223 of SFO
cl. 65	Notification of Tribunal determinations	• s224 of SFO
cl. 66	Form and proof of orders of Tribunal	• s225 of SFO
cl. 67	Orders of Tribunal may be registered in Court of First Instance	• s226 of SFO
cl. 68	Applications for stay of execution of specified decisions	• s227 of SFO
cl. 69	Application for stay of execution of determinations of Tribunal	• s228 of SFO
cl. 70	Appeal to Court of Appeal with leave	• s229(1) of SFO • s14AA(1), (3) and (4) of High Court Ordinance (Cap. 4)
cl. 71	Powers of the Court of Appeal	• s229(2), (3) and (4) of SFO
cl. 72	No stay of execution of Tribunal's determination on appeal	• s230 of SFO
cl. 73	No other right of appeal	• s231 of SFO
cl. 74	Time when specified decisions take effect	• s232 of SFO
cl. 75	Power of Chief Justice to make rules	• s233 (b) & (c) of SFO
Part 7	Miscellaneous Provisions	

Clause	Heading	References
cl. 76	Regulations by Chief Executive in Council	• s376 of SFO
cl. 77	Standard of Proof	• s387 of SFO
cl. 78	Prosecution of offences by relevant authorities	• s388 of SFO
cl. 80	Legal professional privilege	• s380(4)-(5) of SFO
cl. 81	Transitional provision with regard to money changers and remittance agents carrying on business before commencement of this Ordinance	• UK Regulation 50
Schedule 2	Requirements Relating to Customer Due Diligence and Record-keeping	
cl. 1	"beneficial owner"	• UK Regulation 6 • Current guidelines: - "Terminology" in the Interpretative Notes to the HKMA Supplement; - footnote 6 to s5.2 of OCI Guidelines; - SFC Guidelines does not make reference to the term "beneficial owner" but s6.1.2(c) and s6.4.1 of SFC Guidelines set out the classes of persons required to be identified.
	"equivalent jurisdiction"	• Current guidelines- - Para 14 of the Interpretative Notes to HKMA Supplement; - s6.6.6.4 of OCI Guidelines; - definition of "equivalent

Clause	Heading	References
		jurisdiction" in the Glossary to the SFC Guidelines.
	"politically exposed person"	• UK Schedule 2 section 4 • Current guidelines- - s10.2 and s10.3 of HKMA Supplement; - s6.6.5.1 and 6.6.5.2 of OCI Guidelines; - definition of "politically exposed person" in the glossary, s6.9.1 and s6.9.3 of SFC Guidelines
cl. 2	What are customer due diligence measures	• UK Regulation 5 • Current guidelines- - s3.2 of HKMA Supplement; - s6.1.1 of OCI Guidelines; - s 6.1.2 of SFC Guidelines
cl. 3	When customer due diligence measures must be carried out	• UK Regulation 7 and 9 • Current guidelines- - s3.6, 3.7, 3.10 and 3.11of HKMA Supplement; - s6.1.9 to 6.1.13 of OCI Guidelines; - s 6.1.9 and s6.1.10 of SFC Guidelines
cl. 4	Simplified customer due diligence	• UK Regulation 13 • Current guidelines- - s4.2 to 4.4, 4.6 and 7 of HKMA Supplement; - s6.1.4, 6.3.2 and 6.3.4 of OCI Guidelines; - s 6.2.3 to s6.2.4, 6.5 and 6.6 of SFC Guidelines
cl. 5	Duty to continuously monitor business	• UK Regulation 8 • Current guidelines-

Clause	Heading	References
	relationships	- s3.8 and 13 of HKMA Supplement; - s6.7.1 of OCI Guidelines; - s 6.1.2(d), 6.1.11 to 6.1.13, and 6.2.8 of SFC Guidelines
cl. 6	Provisions relating to pre-existing customers	• Current guidelines- - s12 of HKMA Supplement; - s6.7 of OCI Guidelines; - s 6.1.12 and 6.1.13 of SFC Guidelines
cl. 7	Provisions relating to pre-existing respondent banks	• Read together with cl. 14
cl. 9	Special requirements when customer is not physically present for identification purposes	• UK Regulation 14(2) • Current guidelines- - s8 of HKMA Supplement; - s6.6.4 of OCI Guidelines; - s 6.10 of SFC Guidelines
cl. 10	Special requirements when customer is politically exposed person	• UK Regulation 14(4) • Current guidelines- - s10 of HKMA Supplement; - s6.6.5 of OCI Guidelines; - s 6.9 of SFC Guidelines
cl. 11	Special requirements for insurance policies	• S6.2.3 of OCI Guidelines
cl. 12	Special requirements for wire transfers	• s3.14 and 9 of HKMA Supplement
cl. 13	Special requirements for remittance transactions	• S24C and Schedule 6 of OSCO
cl. 14	Special requirements for correspondent banking relationship	• UK Regulation 14(3) • s11 of HKMA Supplement
cl. 15	Special requirements in other high risk situations	• UK Regulation 14(1)(b) • Current guidelines-

Clause	Heading	References
		- s2.2 of HKMA Supplement - s6.6.1 and 6.6.2 of OCI Guidelines; - s 6.2.2, 6.2.7 and 6.2.8 of SFC Guidelines
cl. 16	Anonymous accounts etc	• UK Regulation 16(3) • Current guidelines- - s5.1 of HKMA Guidelines; - s6.1.1 of OCI Guidelines; - s 6.1.7 of SFC Guidelines
cl. 17	Correspondent banking relationships with shell banks	• UK Regulation 16 • s11.6 of HKMA Supplement
cl. 18	Carrying out customer due diligence measures by means of intermediaries	• UK Regulation 17 • Current guidelines- - s6 of HKMA Supplement; - s6.8 of OCI Guidelines; - s 6.11 of SFC Guidelines
cl. 19	Financial institutions to establish procedures	• Current guidelines- - s2.2 and 10.4 of HKMA Supplement; - s5.2 of OCI Guidelines; - s4.2, 5.1 and s6.9.4 of SFC Guidelines
cl. 20	Duty to keep records	• UK Regulation 19 • Current guidelines- - s7.4 of HKMA Guidelines; - s7.2.1 and 7.2.2 of OCI Guidelines; - s7.4, 8.1 and 8.2 of SFC Guidelines
cl. 21	Manner in which records are to be kept	• Current guidelines- - s7.5 of HKMA Guidelines; - s7.2.5 of OCI Guidelines;

Clause	Heading	References
cl. 22	Duties extended to branches and subsidiaries outside Hong Kong	• UK Regulation 15 • Current guidelines- - s1.7 of HKMA Supplement; - s1.4 and 4.1 (a) and (f) of OCI Guidelines; - s 4.3 of SFC Guidelines
cl. 23	Financial institutions to prevent contravention of Part 2 or 3 of this Schedule	• s279 of SFO • s4.3 of HKMA Guideline and s16.2 of HKMA Supplement
Schedule 4	Provisions Relating to Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Review Tribunal	• Schedule 8 to SFO
cl. 1	Interpretation	• s1 of Sch 8 to SFO
cl. 2	Appointment of panel	• s2, 3, 4, 5, 6, of Sch 8 of SFO
cl. 3	Tenure of chairperson	• s8, 9, 10 of Sch 8 to SFO
cl. 4	Appointment of ordinary members	• s12, 13, 14, 15 of Sch 8 to SFO
cl. 5	Further provisions relating to chairperson and ordinary members	• s11 of Sch 8 to SFO
cl. 6	Procedure	• s16, 17, 18, 20, 21, 22, 23 of Sch 8 to SFO
cl. 7	Preliminary conferences	• s25, 26, 27 of Sch 8 to SFO
cl. 8	Consent orders	• s28, 29, 30 of Sch 8 to SFO
cl. 9	Chairperson as sole member of Tribunal	• s31, 32, 33, 34, 35 of Sch 8 to SFO
cl. 10	Privileges and immunities	• s36 of Sch 8 to SFO