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

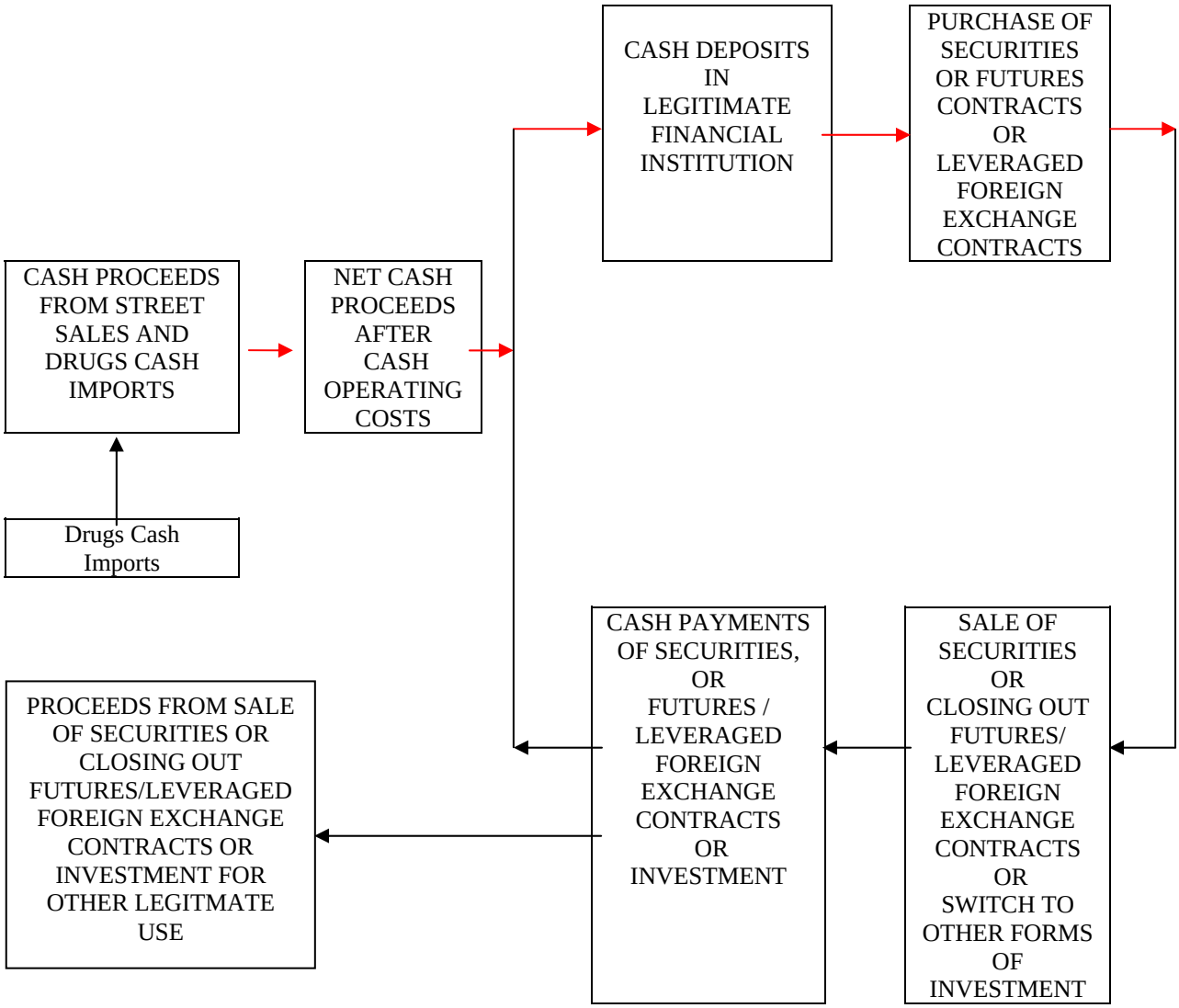
(b) the disclosure is made after he does that act, is made on his own initiative and is made as soon as it is practicable for him to make it.

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.