



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

***Consultation Document on the  
Proposed Revisions to the Guidance  
Notes Issued by the Securities and  
Futures Commission on Money  
Laundering***

**Hong Kong  
January 2003**

**Consultation Document**  
**Proposed Revisions to the Guidance Notes**  
**Issued by the Securities and Futures Commission on Money**  
**Laundering (“Guidance Note”)**

**Introduction**

1. The Securities and Futures Commission (“SFC”) releases for public consultation the proposed revisions to the Guidance Note (the “Proposed Revisions”). The Guidance Note as revised (the “Revised Guidance Note”) is proposed to be made under section 399 of the Securities and Futures Ordinance (Cap. 571) (“SFO”) and is proposed to apply to all licensed persons<sup>1</sup> in carrying on the regulated activities for which they are licensed and all associated entities<sup>1</sup> other than those which are authorised institutions in relation to the conduct of such regulated activities.
2. The SFC has used the FinNet communication network to send copies of this consultation document to all intermediaries. In addition, the public may obtain copies of this consultation document free of charge at the SFC’s office and on the SFC’s Internet website at <http://www.hksfc.org.hk>.
3. The SFC invites market participants and interested parties to submit written comments on the Proposed Revisions by no later than 22 February 2003.  
Comments may be submitted as follows:

<sup>1</sup> As defined in section 1 of Part 1 of Schedule 1 to the SFO

By mail to: SFC (Guidance Note on ML&TF)  
12/F, Edinburgh Tower  
The Landmark  
15 Queen's Road Central  
Hong Kong

By fax to: (852) 2523 4598

By on-line submission: <http://www.hksfc.org.hk>

By e-mail to: [gn\\_ml\\_tf@hksfc.org.hk](mailto:gn_ml_tf@hksfc.org.hk)

4. This consultation document should be read in conjunction with the existing Guidance Note.
5. Any persons wishing to comment on the Proposed Revisions should provide details of any organization whose views they represent. In addition, persons suggesting alternative approaches are encouraged to submit the text of possible amendments that would be necessary to incorporate their suggestions.
6. Please note that the names of persons submitting comments and the contents of their submissions may be published on the SFC website and in other documents to be published by the SFC. In this connection, please read the Personal Information Collection Statement attached to this consultation document (see Attachment 1).
7. If you do not wish your name to be published by the SFC, please state that you wish your name to be withheld from publication when you make your submission.

8. To ensure that the Proposed Revisions properly reflect the relevant elements of the newly enacted law on anti-terrorism measures and other relevant changes in the anti-money laundering provisions that have come into force since the Guidance Note was last revised in July 1997, the SFC has formulated the Proposed Revisions after consulting certain agencies associated with anti-money laundering and anti-terrorism matters in Hong Kong. We wish to acknowledge and thank them for their valuable input.

## **Background**

9. Pursuant to section 399 of the SFO, the SFC may publish guidelines for the purpose of providing guidance for the furtherance of the SFC's regulatory objectives. The SFC considers that the draft Guidance Note would be consistent with the SFC's objective in section 4(d) of the SFO "to minimise crime and misconduct in the securities and futures industry".
10. The SFC proposes that the Revised Guidance Note should basically follow the current Guidance Note (as last revised in July 1997) and that changes should only be introduced in order to meet the following objectives:
  - (a) to extend the application of the Guidance Note to all associated entities (except those which are authorized financial institutions) in light of the fact that associated entities receive or hold client assets and hence may be used as vehicles for money laundering or terrorist financing. Therefore it is necessary to ensure associated entities are subject to the same standards for anti-money laundering and anti-terrorist financing control measures as those of licensed corporations<sup>2</sup>;

<sup>2</sup> As defined in section 1 of Part 1 of Schedule 1 to the SFO

- (b) to rationalise the Guidance Note with the SFO and the rules made thereunder;
- (c) to bring in the requirements and practical implications arising from the new anti-terrorist financing law, United Nations (Anti-Terrorism Measures) Ordinance (Cap.575) (“UNATMO”), which implements the mandatory elements of the United Nations Security Council Resolution 1373 to counter terrorism and the more pressing elements of the Financial Action Task Force on Money Laundering (“FATF”) 8 Special Recommendations on terrorist financing, and changes in the anti-money laundering legislation, namely the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap.405) (“DTROP”) and Organized and Serious Crimes Ordinance (Cap.455) (“OSCO”), and the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission<sup>3</sup> that have come into force since the Guidance Note was last revised in July 1997; and
- (d) to provide further guidance in identifying suspicious transactions and detecting terrorist financing, steps of which are recommended by the Joint Financial Intelligence Unit and FATF, respectively.

11. The Proposed Revisions are marked up in the draft Revised Guidance Note attached (see Attachment 2).

## **Summary of New Proposals**

<sup>3</sup> This document is currently titled “the Code of Conduct for Persons Registered with the Securities and Futures Commission” but this will change under the SFO.

12. The SFC wishes to highlight the following Proposed Revisions.

***Application of the Revised Guidance Note***

13. To ensure all licensed corporations and associated entities are subject to the same standards for anti-money laundering and anti-terrorist financing control measures, we propose to extend the application of the Guidance Note, to the extent applicable to associated entities (except those which are authorized financial institutions) who are not currently required to comply with any law, rules, codes or guidelines. The Revised Guidance Note is intended for use primarily by corporations licensed under the SFO and associated entities that are not authorized financial institutions. Where relevant, the Revised Guidance Note applies to licensed representatives<sup>4</sup>. The Revised Guidance Note will not generally apply to registered institutions and associated entities that are authorized financial institutions on the ground that they are already subject to the Guideline issued by the Hong Kong Monetary Authority on Prevention of Money Laundering (“HKMA’s Guideline”) which is no less stringent than the Revised Guidance Note. However, to the extent that there are some securities or futures-sector specific examples of suspicious transactions in the Revised Guidance Note which may not be shown in the HKMA’s Guideline, the registered institutions and associated entities that are authorized financial institutions are required by the Revised Guidance Note to have regard to Appendix B(ii) to the Revised Guidance Note in identifying suspicious transactions.

A failure to follow the spirit of the Revised Guidance Note by licensed corporations, licensed representatives (where applicable), or associated entities that are not authorized financial institutions may reflect adversely on

their fitness and properness. Similarly, a failure to follow the spirit of the HKMA's Guideline or Appendix B(ii) of the Revised Guidance Note by registered institutions or associated entities that are authorized financial institutions may reflect adversely on their fitness and properness.

14. References to "registered persons" and "licensed traders" in the existing Guidance Note will be replaced by "licensed corporations and associated entities".

***Changes to rationalise the Guidance Note with the SFO and the rules made thereunder***

15. The Revised Guidance Note will make reference to the current approach adopted in the client identification process as described in the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission which has been amended after the Guidance Note was last revised in July 1997. In addition, The Revised Guidance Note will be brought in line with the SFO in respect of the record retention period requirement.

***Insertions to reflect the legal requirements under the UNATMO and changes in the DTROP and OSCO***

16. The Guidance Note will need to be updated to include the legal obligations imposed under the newly enacted anti-terrorist financing law, UNATMO, and the new offences created under the anti-money laundering law, DTROP and OSCO, which came into effect on 1 January 2003.

***Provision of further guidance in identifying suspicious transactions and detecting terrorist financing***

---

<sup>4</sup> As defined in section 1 of Part 1 of Schedule 1 to the SFO

17. The Revised Guidance Note will provide further guidance in identifying suspicious transactions and detecting terrorist financing, steps of which are recommended by the Joint Financial Intelligence Unit and FATF, respectively.

**Personal Information Collection Statement**

1. This Personal Information Collection Statement (“PICS”) is made in accordance with the guidelines issued by the Privacy Commissioner for Personal Data. The PICS sets out the purposes for which your Personal Data<sup>1</sup> will be used following collection by the Securities and Futures Commission (“SFC”), what you are agreeing to with respect to the SFC’s use of your Personal Data and your rights under the PDPO.

**Purpose of Collection**

2. The Personal Data provided in your submission to the SFC in response to the proposed revisions to the Guidance Note may be used by the SFC for one or more of the following purposes:
  - to administer the relevant Ordinances, rules, regulations, codes and guidelines made or promulgated pursuant to the powers vested in the SFC
  - for the purposes of performing the SFC’s statutory functions under the relevant Ordinances
  - for research and statistical purposes
  - other purposes permitted by law

**Transfer of Personal Data**

3. Personal Data may be disclosed by the SFC to the members of the public in Hong Kong and elsewhere, as part of the public consultation on the Consultation Document. The names of persons who submit comments on

the Consultation Document together with the whole or part of their submission may be disclosed to members of the public. This will be done by publishing this information on the SFC web site and in documents to be published by the SFC throughout and at the conclusion of the consultation period.

### **Access to Data**

4. You have the right to request access to and correction of your Personal Data in accordance with the provisions of the PDPO. Your right of access includes the right to obtain a copy of your Personal Data provided in your submission on the Consultation Document. The SFC has the right to charge a reasonable fee for processing any data access request.

### **Enquiries**

5. Any enquiries regarding the Personal Data provided in your submission on the Consultation Document, or requests for access to Personal Data or correction of Personal Data, should be addressed in writing to:

The Data Privacy Officer,  
The Securities and Futures Commission  
12/F, Edinburgh Tower, The Landmark  
15 Queen's Road Central Hong Kong

**A copy of the Privacy Policy Statement adopted by the SFC is available upon request.**

---

<sup>1</sup> Personal Data means personal data as defined in the Personal Data (Privacy) Ordinance, Cap 486 ("PDPO")

[Draft Revised Guidance Note for Consultation]

MONEY LAUNDERING AND TERRORIST FINANCING

**REVISED**  
GUIDANCE ~~NOTES~~ NOTE ISSUED BY THE  
SECURITIES AND FUTURES COMMISSION

~~July 1997~~ [April 2003]

# 1 INTRODUCTION

1.1 This Guidance Note, which is published under section 399 of the Securities and Futures Ordinance (Cap.571) (“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 content of this Guidance Note will be kept under review and amendments may be issued from time to time.

1.2 This Guidance Note is intended for use primarily by ~~dealers, dealing partnerships, investment advisers, commodity trading advisers, and investment advisers' partnerships, and securities margin financiers registered under the Securities Ordinance (Cap.333) and the Commodities Trading Ordinance (Cap.250) (“registered persons”), or a Leveraged Foreign Exchange trader licensed under the Leveraged Foreign Exchange Trading Ordinance (Cap 451) (“licensed traders”)~~ 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 Guideline issued by the Hong Kong Monetary Authority on Prevention of Money Laundering (“HKMA’s Guideline”). However, to the extent that there are some securities or futures-sector specific examples of suspicious transactions in this Guidance Note which may not be shown in the HKMA’s Guideline, the registered institutions and associated entities that are authorized financial institutions are required by the Guidance Note to have regard to Appendix B(ii) to this Guidance Note in identifying suspicious transactions.

1.3 This Guidance Note does not have the force of law ~~and does not override any law and should not be interpreted in any manner which would override the provisions of any applicable law, codes or other regulatory requirements.~~ However, a failure to follow the spirit of this Guidance Note by licensed corporations, licensed representatives (where applicable), or associated entities may reflect adversely on their fitness and properness. Similarly, a failure to follow the spirit of the HKMA’s Guideline or Appendix B(ii) of this Guidance Note by registered institutions or associated entities that are authorized financial institutions may reflect adversely on their fitness and properness.

1.4 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 of the

~~SFO. Where relevant, this Guidance Notes~~Note ~~applies to registered persons' licensed representatives (i.e. dealer's representatives, investment representatives, commodity trading adviser's representatives), and licensed traders' representatives.~~

~~The content of this Guidance Note will be kept under review and amendments may be issued from time to time.~~

1.5 ~~The two primary bodies of law~~three main pieces of legislation in Hong Kong ~~that are~~ concerned with ~~the subject of~~ money laundering and terrorist financing are the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. ~~405~~), ~~and~~, the Organized and Serious Crimes Ordinance (Cap. ~~455~~) and the United Nations (Anti-Terrorism Measures) Ordinance (Cap. ~~575~~).

## 2 BACKGROUND

### 2.1 The nature of money laundering

2.1.1 The term "money laundering" covers a wide range of activities and processes intended to alter the identity of the source of illegally obtained money in a manner which creates the appearance that it has originated from a legitimate source.

2.1.2 Cash, being a bearer instrument and completely fungible, lends anonymity to a variety of criminal activities, and is the preferred medium of exchange in the criminal world. This gives rise to three common factors:

- drug dealers and criminals have a need to conceal the true ownership and origin of the money;
- these persons have a need to maintain control over the money; and
- these persons need to alter the form of the money to mask its origins.

### 2.2 Stages of money laundering

2.2.1 There are three common stages in the laundering of money, and because they frequently involve numerous transactions a ~~registered person~~licensed corporation or an associated entity ~~licensed trader~~ may be alerted to potential criminal ~~activity~~activities. These stages are:

- a) Placement - the physical disposal of cash proceeds derived from illegal ~~activity~~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 A 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 Given the liquidity of the markets in which these instruments are traded, with potentially great frequency.

2.3.3 Investments that are cash equivalents i.e.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 ~~ready~~ 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 Terrorist financing**

2.4.1 The term “terrorist financing” refers to the carrying out of transactions involving funds or property that are owned or controlled by terrorists or terrorist organizations, or transactions that are linked to, or likely to be used in, terrorist activities.

2.4.2 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 an illicit or legitimate source, in order to be able to use them without attracting the attention of the authorities. Business relationships with terrorists or terrorist organizations could expose a licensed corporation or any of its associated entities to significant reputation, operational and legal risks.

## **2.5 Recent International Initiatives**

2.5.1 The ~~International~~ Financial Action Task Force on Money Laundering ("FATF") was established in 1989 in an effort to thwart attempts by criminals to launder the proceeds of criminal activities through the financial system. Hong Kong was admitted as a full member in March 1991. In October 2001, the FATF expanded its scope of work to cover matters relating to terrorist financing.

2.5.2 In 1992 the International Organisation of Securities Commissions (“IOSCO”), of which the Securities and Futures 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, ~~and~~ monitoring and compliance procedures and the identification and reporting of suspicious transactions.

2.5.3 In June 1996, FATF issued a revised set of 40 recommendations for dealing with money laundering. In October 2001, the FATF promulgated 8 special recommendations on terrorist financing. These two sets of recommendations set out the basic framework to detect, prevent and suppress money laundering and terrorist financing activities.

### 3. **LEGISLATION ~~COVERING~~ CONCERNED WITH MONEY LAUNDERING AND TERRORIST FINANCING**

In Hong Kong, the Drug Trafficking (Recovery of Proceeds) Ordinance (~~Cap 405~~), ~~and~~ the Organized and Serious Crimes Ordinance (~~Cap 455~~) ~~and~~ the United Nations (Anti-Terrorism Measures) Ordinance, address deal with the problems in relation to terrorist financing and problems associated with money laundering activities in the ~~key~~ areas of terrorism, drugs trafficking and organized and serious crimes. The principal anti-money laundering ~~and anti-terrorist financing~~ provisions are summarized below. This summary is not a legal interpretation of the applicable legislation and, where appropriate, legal advice should be sought.

#### 3.1 **The Drug Trafficking (Recovery of Proceeds) Ordinance (“~~DTRPO~~ DTROP”)**

3.1.1 The ~~DTRPO~~ DTROP contains provisions for the investigation of assets that are suspected to be drug derived from drug trafficking activities ~~assets~~, the freezing of assets on arrest and the making of confiscation ~~orders following upon~~ conviction.

3.1.2 Under section 25(1) of the DTROP, a person commits an offence if he deals with a piece of property that he knows or having reasonable grounds to believe that it represents any person's proceeds of drug trafficking. Section 25(1) of the DTRPO creates an offence of dealing with property known or believed to represent the 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 forpunishable by a maximum of 14 years years' imprisonment and a maximum 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.

3.1.3 Under section 25A of the ~~DTRPO-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 ~~as soon as it is reasonable for him to do so,~~ 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 Joint Financial Intelligence Unit ("JFIU") ~~which JFIU was has been~~ established~~;~~ and is operated~~;~~ by the Police and Customs and Excise Department. ~~In addition,~~Section 25A(4) of the DTRPO-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 ~~the~~

making ~~of~~ such disclosures, (see also paragraph 4.5.5 of ~~these~~ this Guidance ~~Notes~~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 ~~at level~~ 5 of HK\$50,000 and imprisonment for 3 months.

~~— A person has a defence if he intended to make proper disclosure and there is a reasonable excuse for his failure.~~

3.1.4 Section 25A(2) of the ~~DTRPODTROP~~ provides ~~that a person with an immunity from prosecution for an offence under section 25.~~ If a person who has made a disclosure under section 25A(1) does any act in contravention of section 25(1) whether before or after such the disclosure, and the disclosure relates to that act, then 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 the authorized officer; or
- (b) the disclosure is made after he does that act, is made on his own initiative and is made as soon as it is reasonable for him to make it.

3.1.5 ~~Section~~ Under section 25A(5) of the DTRPODTROP, 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). ~~makes it an offence in certain circumstances for a person to disclose to another person that a disclosure has been made under section 25A(1) or (4). It is, however, a defence to prove that he did not know or suspect that the disclosure concerned was likely to be prejudicial to the investigation or that he had lawful authority or reasonable excuse for making that disclosure.~~ The maximum penalty upon conviction of ~~for~~ this offence is a fine of \$500,000 and imprisonment for 3 years.

3.1.6 Section 25A(3)(b) provides that a disclosure made under the ~~DTRPODTROP~~ shall not be treated as a breach of any restriction upon the disclosure of information imposed by contract or by enactment, rules of ~~professional~~ conduct or

other provision. ~~and~~ 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 funds or investments in consequence of the disclosure.

3.1.7 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.

3.1.8 Section 26 of the ~~DTRPO~~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 ~~when such disclosure may be revealed~~ in proceedings instituted to prosecute 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 making of~~ the disclosure or the identity of the person making the disclosure.

### **3.2 The Organized and Serious Crimes Ordinance ("OSCO")**

3.2.1 The OSCO, among other things:

- (a) gives the Police and the Customs and Excise Department officers powers to ~~effectively~~ investigate organized crime and triads 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 ~~the~~an offender and ~~the~~an offence in order to determine whether the imposition of a greater sentences is appropriate where the offence ~~amounted~~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 to include offences listed in Schedule 1 of the OSCO that is either connected with the activities of a particular triad societ~~ies~~society, or is committed by two or more persons ~~criminal syndicates and serious offences~~ that involves substantial planning and organization. ~~Most indictable~~The offences that are listed in Schedule 1 covered, including include murder, kidnapping, drug trafficking ~~offences~~, assault, rape, theft, robbery, obtaining property by deception, false accounting, ~~firearms offences~~, manslaughter, bribery ~~offences~~ and smuggling ~~offences~~.

3.2.2 ~~The Sections 3 to 5 of the~~ OSCO provides that an authorized officer (including the police), for the purpose of investigating an organized crime, may apply to the ~~High~~ Court of First Instance to 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 Tthe OSCO, also covers orders to make material available and gives authority to the police to search. Businesses in Hong Kong can now expect to receive court orders issued under the OSCO. Disclosure pursuant to such orders is considered to be made under compulsion of law, overriding any duty of secrecy or confidentiality owed to a client. 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.

3.2.3 Sections 25, 25A and ~~section~~ 26 of the OSCO are modelled upon sections 25, 25A and 26 of the ~~DTRPOD~~TROP. In summary, section 25(1) of the OSCO creates an offence of dealing with property that is known or ~~believed~~having reasonable grounds to believe to represent the proceeds of an indictable offence. “Dealing” in relation to any property

~~referred to in this section in whole or in part directly or indirectly representing any person's proceeds of an indictable offence, or dealing in any property that was used or is intended to be used in connection with an indictable offence~~ 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. ~~14 years' imprisonment and a fine of \$5 million. 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.~~

3.2.4 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 ~~as soon as it is reasonable for him to do so,~~ disclose that knowledge or suspicion to an authorized officer as soon as it is reasonable for him to do so. Failure to make a ~~required~~ disclosure under this section constitutes an offence. Where a person ~~was~~ 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 ~~for~~ upon conviction of this offence is a fine ~~at level 5 of HK\$50,000~~ and imprisonment for 3 months.

~~A person has a defence if he intended to make proper disclosure and there is a reasonable excuse for his failure.~~

3.2.5 Section 25A(2) of the OSCO provides ~~that a person with an immunity from prosecution for an offence under section 25.~~ If a person who has made a disclosure under section 25A(1) does any act in contravention of section 25(1) ~~whether~~ before or after ~~such the~~ disclosure, and the disclosure relates to that act, ~~then~~ 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 the authorized officer; or
- (b) the disclosure is made after he does that act, is made on his own initiative and is made as soon as it is reasonable for him to make it.

3.2.6 ~~Section 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). makes it an offence in certain circumstances for a person to disclose to another person that a disclosure has been made under section 25A(1) or (4). It is, however, a defence to prove that he did not know or suspect that the disclosure concerned was likely to be prejudicial to the investigation or that he had lawful authority or reasonable excuse for making that disclosure.~~ The maximum penalty ~~for upon conviction of~~ this offence is a fine of \$500,000 and imprisonment for 3 years.

3.2.7 Section 25A(3)(b) 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 ~~professional~~ conduct or other provision. ~~and~~ 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.

3.2.8 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.

3.2.9 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 nor to reveal the identity of the person making the disclosure except ~~when such disclosure may be revealed~~ in proceedings ~~instituted to prosecute~~ 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 making of~~ the disclosure or the identity of the person making the disclosure.

### **3.3 The United Nations (Anti-Terrorism Measures) Ordinance ("UNATMO")**

3.3.1 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.

3.3.2 Besides the mandatory elements of the UNSC Resolution 1373, the UNATMO also implements the more pressing elements of the FATF 8 special recommendations on terrorist financing. The UNATMO, among other things, criminalizes the supply 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 UNATMO also requires a person to report his knowledge or suspicion of terrorist property to an authorized officer (e.g. the JFIU). Failure to make a disclosure under this section constitutes an offence. The maximum penalty upon conviction of this offence is a fine of HK\$50,000 and imprisonment for 3 months.

3.3.3 The term “funds” includes funds mentioned in the Schedule to the 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.

3.3.4 “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:

- (a) causes serious violence against a person;
- (b) causes serious damage to property;
- (c) endangers a person’s life, other than that of the person committing the action;
- (d) creates a serious risk to the health or safety of the public or a section of the public;
- (e) is intended seriously to interfere with or seriously to disrupt an electronic system; or
- (f) is intended seriously to interfere with or seriously to disrupt 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.

3.3.5 As with the United Nations Sanctions (Afghanistan) Regulation, a list of terrorist or terrorist associate names is published in the Gazette from time to time for the purpose of the UNATMO. The list so far published reflects designations made by the UN Committee established by UNSC Regulation 1267. The 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).

3.3.6 As far as the obligations under section 12(1) of the 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 UNATMO (on the supply 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 the authorized officer; or

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

3.3.7 Section 12(3) provides that a disclosure made under the 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.

3.3.8 The provisions of the UNATMO mentioned above, except section 8, have been in force since 23 August 2002. Section 8 (and some other provisions) will come into operation on a day to be appointed by the Secretary for Security by notice published in the Gazette.

#### **4. POLICIES AND PROCEDURES EXPECTED OF REGISTERED LICENSED PERSONS CORPORATIONS AND ASSOCIATED ENTITIES LICENSED TRADERS**

**4.1** International initiatives taken to combat drug trafficking, terrorism and other serious crimes have concluded that financial institutions 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 therefore a need for awareness and vigilance and a system for reporting suspicious transactions to the law enforcement authorities.

**4.2** ~~Registered–Licensed persons~~corporations and associated entities and licensed traders should:

- (a) issue a statement of policies and procedures for dealing with money laundering and terrorist financing reflecting the current statutory requirements;
- (b) ~~—~~ ensure that the content of this Guidance Note is understood by all ~~members of their~~ staff members;
- (c) regularly review the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness;
- (d) develop staff members awareness and vigilance to guard against money laundering and terrorist financing.

**4.3** Policies and procedures should cover:-

- (a) communication of group policies relating to prevention of money laundering and terrorist financing;
- (b) account opening and; customer identification, including requirements for proper identification;
- (c) maintenance of records;
- (d) compliance with relevant legislation;
- (e) co-operation with the relevant law enforcement authorities, including the timely disclosure of information;
- (f) internal audit to ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing.

4.4 Where ~~Hong Kong registered licensed entities corporations and associated entities~~ have branches or subsidiaries overseas, steps should be taken to alert local management to group policy in relation to prevention of money laundering and terrorist financing and, where appropriate, instruct overseas branches and overseas subsidiaries as to the local reporting point for their suspicions. Where a local jurisdiction has an anti-money laundering or anti-terrorist financing law, branches and subsidiaries of ~~Hong Kong entities licensed corporations and associated entities~~ operating within that jurisdiction should act in accordance with the requirements of the local law.

4.5 The following critical subject areas provide some guidance to ~~registered licensed persons corporations and associated entities and licensed traders~~ in developing appropriate policies and procedures.

#### 4.15.1 Client identification

##### (a) Registered-General

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

Before opening ~~the-an~~ account, positive identification of ~~a~~ the client should be made from documents issued by reliable sources and, where practicable, file copies should be retained and reference numbers and other relevant details recorded.

Passports and Identity Cards are the types of documentation that should be produced as proof of identity.

Whenever possible, the prospective customer should be interviewed personally.

If the account is opened using a non-face-to-face approach, care should be taken to ensure that the identity of the client is verified. Reference should be made to paragraphs on "Information about clients" under the Code of Conduct for

## Persons Licensed by or Registered with the Securities and Futures Commission.

At the time of opening a new trading account, the client should be asked whether any other person has a beneficial interest in the trading to be conducted under that account.

In all cases, regardless of whether or not a non-face-to-face approach is used, the primary duty to verify client's identity using the best cumulative documentary evidence that can be obtained remains with the licensed corporation or associated entity. ~~with the account opening institution.~~

~~— The primary duty to verify identity using the best cumulative documentary evidence that can be obtained rests with the account opening institution.~~ However, it is recognized that in a small number of cases, it may not be able to obtain adequate verification by following the procedures outlined above. In such circumstances, with the consent of the client, it may be necessary to approach another ~~registered person or licensed trader~~ person or corporation specifically for the purpose of verifying identity.

### (b) Corporate/Partnership Clients

In respect to corporate or partnership clients, it is important to identify the directors or partners, ~~—~~ the account signatories and the nature of the business. Where applicable, the following should be obtained:

- Certificate of Incorporation, where applicable, and Business Registration Certificate;
- Bank Mandate; — board resolution, where applicable;
- memorandum and articles of association or partnership agreement, as the case may be, together with information about the nature of the business;
- specimen signatures;
- copies of identification documents of directors or partners, as the case may be, and of all account signatories; and
- information ~~as to~~ on major shareholders and beneficial owners.

If there is any doubt about the identity of the company or its beneficial owners, shareholders or directors, a company search or a credit reference agency search should be made.

(c) No anonymous accounts

~~No a~~Anonymous ~~or fictitious~~ accounts should beare not allowed.

(d) Account opened on behalf of a third person / trust account

A ~~registered licensed person~~corporation or ~~a licensed trader an associated entity~~ should ask a new client whether the account is opened on behalf of another person. If so, care should be taken to check the identity of all of the parties who have an interest into the account (including the legal and beneficial owners) along the lines of the account opening procedures for other accounts.

Avoidance of account opening by post

~~The account of a local client should not be opened by post.~~

(e) Overseas Clients

For overseas clients in a country where the ~~registered licensed person~~corporation or ~~licensed trader associated entity~~ does not have a presence, the application should be submitted through a reputable source such as a correspondent bank in that country, which can be relied upon to undertake effective identification procedures on behalf of the ~~registered licensed person~~corporation or ~~licensed trader associated entity~~. It is preferred to have documents certified by the company's ~~foreign~~lawyers in its place of incorporation.

Avoidance of

(f) Third party cheques

"Third party" cheques (i.e. cheques or other payments from persons other than the client) should be supported by further verification of identity.

#### **4.25.2 Record Keeping**

~~Registered-Licensed persons~~corporations and ~~licensed traders~~associated entities should ensure compliance with the record keeping requirements contained in the relevant legislation, rules or regulations of the Commission ~~or~~and of the relevant exchanges.

The investigating authorities need to ensure a satisfactory audit trail for suspected drug related or other laundered money or terrorist property and be able to establish a financial profile of the suspect account. For example, to satisfy these requirements, the following information may be sought:

- (~~ia~~) the beneficial owner of the account;
- (~~ib~~) the volume of the funds flowing through the account; and
- (~~iiic~~) for selected transactions:
  - the origin of the funds;
  - the form in which the funds were offered or withdrawn, i.e.g. cash, cheques, etc.;
  - the identity of the person undertaking the transaction;
  - the destination of the funds;
  - the form of instruction and authority.

Where appropriate, ~~registered-licensed persons~~corporations and ~~licensed traders~~associated entities should consider retaining in Hong Kong certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under other relevant legislation, rules and regulations of the Commission or of the relevant exchanges.

#### **4.5.3 Retention of Records**

A document retention policy must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. However, when practicable, the following document retention terms are suggested :

(ia) All necessary records on transactions, both domestic ~~or~~ and international, should be maintained for at least ~~five~~ seven years. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of ~~currency~~ currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

(ib) 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 for at least five years after the account is closed.

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

#### 4.5.4 ~~Recognition~~ Recognizing and Reporting ~~of~~ Suspicious Transactions

(a) ~~Registered~~ Licensed persons ~~corporations~~ and ~~licensed~~ traders ~~associated entities~~, their directors, officers and employees should not ~~or, where appropriate, should not be allowed to~~ warn their customers when information relating to them is being reported to an authorized officer ~~the~~ (e.g. the JFIU), as such action may constitute an offence.

(b) The types of transactions which may be used by a money launderer and terrorist are virtually unlimited, and it is difficult to definitively specify which transactions might constitute a suspicious transaction. Suspicion may arise where a transaction is 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 key to recognition is knowing enough about a customer's business and financial circumstances to recognize that a transaction, or series of transactions, is unusual. An effective systemic approach to the identification of suspicious financial activity recommended by the JFIU is provided in Appendix B(i). ~~Examples of what might constitute a suspicious transaction are provided in Appendix B.~~

Identification of any of the types of transactions listed in Appendix B should prompt further enquiries about the source of funds. In general, licensed persons and associated entities should be vigilant in monitoring activities which might be suspicious.

(c) In relation to terrorist financing, the FATF issued in April 2002 a paper on guidance for financial institutions in detecting terrorist financing. The document describes the general characteristics of terrorist financing with case studies illustrating the manner in which law enforcement agencies were able to establish a terrorist financing link based on information reported by financial institutions. Annex 1 of the document contains a series of characteristics of financial transactions that have been linked to terrorist activities in the past. A licensed corporation or an associated entity should acquaint itself with the FATF paper which is available on the FATF website ([http://www.fatf-gafi.org/TerFinance\\_en.htm](http://www.fatf-gafi.org/TerFinance_en.htm)).

(d) The list of potentially suspicious or unusual activities is meant to show the types of transactions that could be a cause of scrutiny and 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 [www.info.gov.hk/eindex.htm](http://www.info.gov.hk/eindex.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.

(e) Licensed corporations and associated entities should pay attention to 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

[www.ustreas.gov/offices/enforcement/ofac/sanctions/terrorism.html](http://www.ustreas.gov/offices/enforcement/ofac/sanctions/terrorism.html) and lists referred to on the Commission's website).

~~— Identification of any of the types of transactions listed in Appendix B should prompt further enquiries about the source of funds.~~

(f) Disclosures of suspicious transactions under the ~~DTRPODTROP~~ or the OSCO or the UNATMO should be made to the JFIU. The JFIU functions as the domestic 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.

#### 4.5.5 Procedures for Disclosure

~~4.5.1(a)~~ The obligation to report under the ~~DTRPODTROP~~ or the OSCO or the UNATMO rests with the individual who becomes suspicious of a person, or transaction or property. Under certain circumstances, a staff member of a registered licensed person corporation or licensed trader an associated entity may elect to bring the transaction to the urgent attention of supervisory management. The circumstances of each case can then be reviewed at that level to determine whether the suspicion is justified. If the suspicion remains it should be reported to the JFIU without delay. Consideration should be given to co-ordination through a central point, i.e. a compliance officer, for onward reporting to the JFIU.

~~—4.5.2(b)~~ The use of a standard format for reporting is encouraged (see Appendix C). In the event that urgent disclosure is required, an initial notification should be made by telephone. The ~~address and telephone number~~ contact details of the JFIU are set out at Appendix ~~FE~~.

~~4.5.3(c)~~ A register ~~should be kept~~ of all reports made to the JFIU and all reports made by employees to management: should be kept.

~~4.5.4(d)~~ 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 ~~on~~ in relation to an

account, consent will usually be given for the ~~registered licensed person~~ corporation or ~~licensed trader~~ associated entity to operate the account under the provisions of section 25A(2) of the ~~DTRPODTROP~~, 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 D.

4.5.5(e) 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 Customs and Excise Departments for further investigation.

~~4.5.6(f)~~ Access to the disclosed information is restricted to the relevant financial investigating officers within the Police and Customs and Excise Departments. In the event of a prosecution, production orders will be obtained to produce the material at court. Section 26 of the ~~DTRPODTROP~~ and the OSCO place strict restrictions on revealing the identity of the person making a disclosure under section 25A.

4.5.7(g) The Police and Customs and Excise Departments and the JFIU are not obliged to, but may, on request, provide ~~to a disclosing registered person or licensed trader~~ a status report on ~~an relevant investigation~~ the disclosure to a disclosing licensed person corporation or an associated entity. ~~An example of such a letter is shown at Appendix E.~~

4.5.8(h) Enhancing and maintaining the integrity of the relationship which has been established between law enforcement agencies and ~~registered licensed persons~~ corporations/ licensed traders associated entities is considered to be of paramount importance.

#### 4.5.6 Education and Training

(a) Registered Licensed persons corporations and ~~licensed traders~~ associated entities must provide proper anti-money laundering and anti-terrorist financing training to their local and overseas ~~staff~~ staff members.

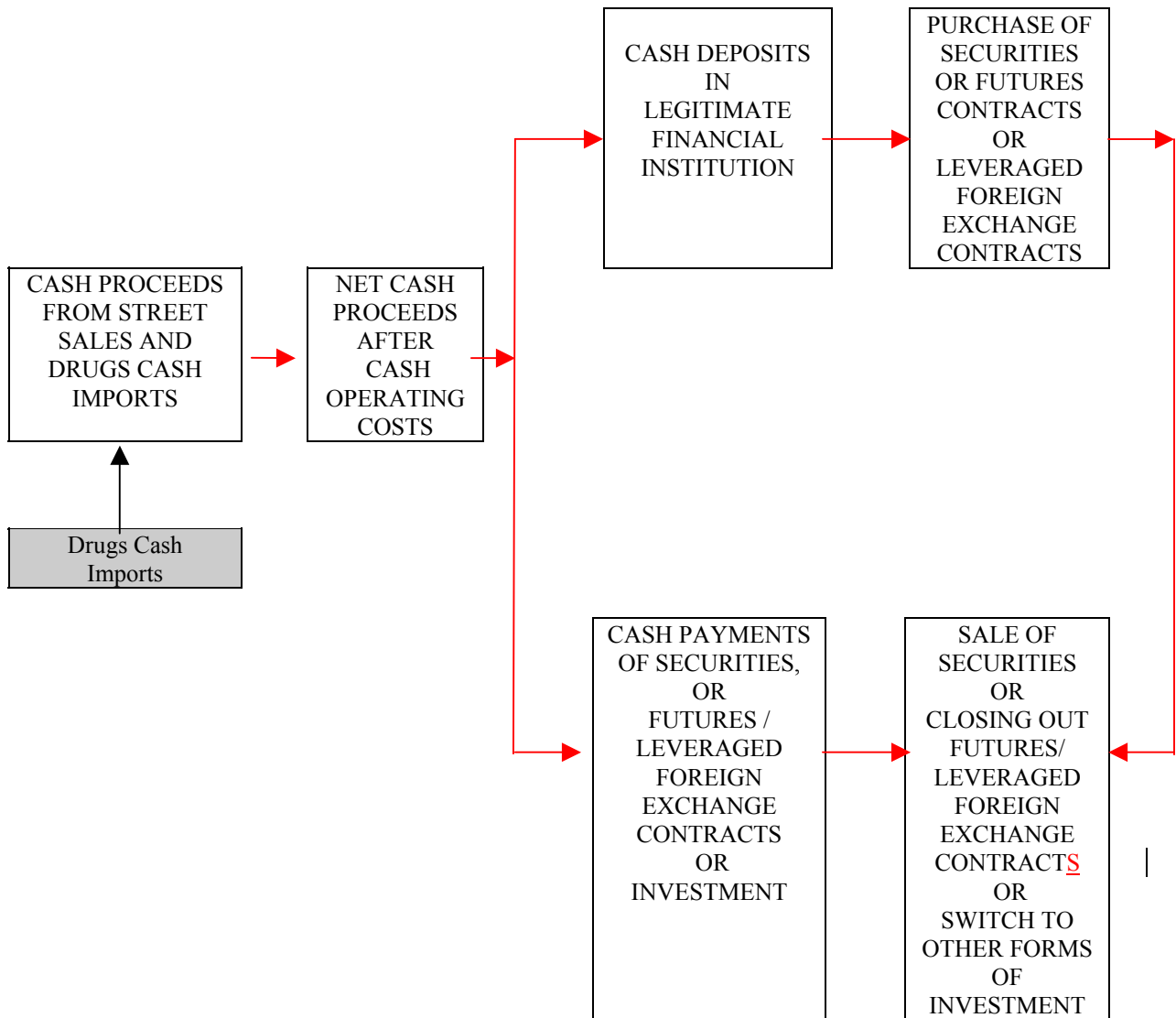
(b) StaffMembers of staff should be aware of their own personal obligations under the ~~DTRPODTROP~~ and the OSCO and the UNATMO and that they can be personally liable should they fail to report information as required. They are advised to read the relevant sections of the ~~DTRPODTROP~~ and the OSCO and the UNATMO. StaffMembers of staff must be encouraged to co-operate fully with the JFIU and to ~~provide prompt~~disclose notice of suspicious transactions promptly. If in doubt, they should contact the JFIU.:-

(c) Registered—Licensed personscorporations and licensed traders—associated entities should have educational programmes in place for training new employees, members of staff who ~~dealing directly~~ with the public directly and ~~staff who~~ open new accounts, and those who supervise or manage such ~~staff~~staff members.

(d) On-going training

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

**LAUNDERING OF PROCEEDS**



domestic

foreign

**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 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.

**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 B(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 fulfills 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 months turnover is then compared with the average turnover. The current months 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 client 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 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 levels of activity 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.

## 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 client of a ~~licensed corporation or an associated entity~~securities or futures brokerage firm as a place to hold funds that are not being used to trade in securities, ~~or futures~~ contracts or leveraged foreign exchange contracts.
- g) A client who deals with a ~~securities or futures broker~~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.

Money laundering involving ~~Employees—employees~~ of ~~Registered Persons and Licensed Traders~~licensed Personscorporations 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 client's permanent address, e.g. utilisation of the ~~salesman's 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.

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

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 1 June 1995 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.

~~Consent~~ 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 section 25A~~ of the Ordinance(s).

Thank you for your co-operation.

Yours faithfully,

Joint Financial Intelligence Unit

~~Joint Financial Intelligence Unit (“JFIU”)~~

~~The Manager  
ABC Co. Ltd.  
XXXX  
Hong Kong~~

~~Your Ref:~~

~~Our Ref:~~

~~1st July 1995~~

~~Dear Sir,~~

~~JFIU Feedback Report~~

~~—— Following the receipt of disclosures made by you and subsequent dissemination for enquiries by police / customs, I enclose for your information a summary of the present position of those cases as reported to the JFIU.~~

~~—— The current status shown, whilst accurate at the time of making this report should not be treated as a basis for subsequent decisions, without reviewing the up to date position.~~

~~—— Please do not hesitate to contact the JFIU if you require any further information or assistance.~~

~~Yours faithfully,~~

~~WRITTEN REPORTS SHOULD BE SENT TO:~~

~~\_\_\_\_\_ Joint Financial Intelligence Unit  
\_\_\_\_\_ 20th Floor  
\_\_\_\_\_ Asia House  
\_\_\_\_\_ 1 Hennessy Road  
\_\_\_\_\_ Wanchai  
\_\_\_\_\_ Hong Kong~~

~~TELEPHONE CALLS SHOULD BE MADE TO THE FOLLOWING  
REPORTING LINE NUMBER:~~

~~\_\_\_\_\_ 28041459~~

~~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](mailto:jfiu@police.gov.hk)~~

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