



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

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

**《證券及期貨事務監察委員會
有關防止洗黑錢的指引》
的建議修訂的諮詢總結**

Hong Kong
March 2003

香港
2003年3月

INTRODUCTION

1. On 23 January 2003, the Securities and Futures Commission (“Commission” or “SFC”) released a Consultation Document (“Consultation Document”) on the proposed revisions to the Guidance Note issued by the Securities and Futures Commission on Money Laundering (the “Guidance Note”).
2. The consultation period lasted until 22 February 2003.
3. A summary of comments received on the proposed revisions (“Summary of Comments”) is attached as Attachment 1.
4. Taking into account the submissions received, several revisions to the draft revised Guidance Note were considered appropriate.
5. These revisions have been adopted by the Commission and the final revised guidance note (“Revised Guidance Note”) is attached as Attachment 2.
6. The Commission would like to thank those who have provided their comments on the proposed revisions.
7. The purpose of this report is to provide interested persons with an analysis of the main comments raised during the consultation process and the rationale for the Commission’s conclusions. This report should be read in conjunction with the Consultation Document, the Summary of Comments and the Revised Guidance Note.

PUBLIC CONSULTATION

A. Background

8. As explained in the Consultation Document, changes were proposed to be made to the Guidance Note 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 corporations¹;
 - (b) to rationalise the Guidance Note with the SFO and the rules made thereunder;

¹ As defined in section 1 of Part 1 of Schedule 1 to the SFO

- (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 (“Code of Conduct”) 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 (“JFIU”) and FATF, respectively.

B. Consultation Process

- 9. In addition to the public announcement inviting comments, the Consultation Document was distributed to all intermediaries and various professional bodies. The Consultation Document was also published on the SFC website.
- 10. 5 submissions were received from brokerage firms, a legal firm, an industry association and a professional body.
- 11. The overall tone of the comments was positive. Commentators generally acknowledged the need for and welcomed the proposed revisions. Specific comments mainly focused on issues relating to the customer due diligence requirements, and are in the nature of seeking clarification on interpretation of some of the existing provisions of the Guidance Note.

CONSULTATION CONCLUSIONS

Scope of application

- 12. A commentator suggested that authorized financial institutions should also be subject to the Revised Guidance Note in order to avoid unnecessary complications and to ensure level playing field. In light of the fact that authorized financial institutions 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, we consider that there is no need to subject authorized financial institutions to the Revised Guidance Note other than that they should have regard to the examples of suspicious transactions specific to the securities and futures sectors provided in Appendix B(ii) of the Revised Guidance Note in identifying suspicious transactions. The SFC will keep in view any future

changes to the HKMA's Guideline to ensure that authorized financial institutions remain to be subject to at least equally stringent requirements.

Policies and procedures on client identification

13. Some commentators suggested the reliance of third parties / intermediary clients in performing customer due diligence checks should be allowed on the ground that these parties are already subject to anti-money laundering / anti-terrorist financing procedures and laws that are comparable to those in force in Hong Kong.
14. A commentator pointed out that 4.5.1 (e) appears to be inconsistent with the Code of Conduct in that different requirements seem to apply in relation to certifying overseas client identity document.
15. Other commentators sought clarification on a number of points as follows:
 - definitions of "major shareholder" and "beneficial owner";
 - whether information is required for all directors and all beneficial owners in the case of a corporate client; and
 - whether there is any exemption or other simplified customer due diligence measures for companies listed locally and overseas.
16. On the question of reliance of third parties / intermediaries clients to conduct client identification on behalf of a licensed corporation or an associated entity and the matter of certifying overseas client identity client, the Code of Conduct already provides various alternatives in certifying the sighting of original identity documents in the case where a non-face-to-face approach is used. In order to avoid duplication, we have deleted, from the Guidance Note, the last paragraph of 4.5.1 (a) and the last sentence of 4.5.1 (e), which basically restated one of the alternatives in certifying the sighting of client related identity documents. It should be noted that, under all circumstances, the ultimate responsibility for identification and verification of identity of customers remains with the licensed corporation or associated entity that enters into the business relationship. Given the fact that the subject of reliance on third party in performing customer due diligence is currently under the FATF's deliberation, changes to the Guidance Note to allow other elements of customer due diligence process to be performed by third parties on behalf of the licensed corporation or associated entity would be made only when the review of the 40 Recommendations is completed so as to ensure that our requirements are in line with the FATF's standards.
17. We agree that the Guidance Note should provide a definition for "major shareholder" and "beneficial owner" to clarify the scope of our requirements. We have changed the term "major shareholder" to "substantial shareholder" as defined under section 6 of Part 1 of Schedule 1 to the SFO. In addition, a definition of "beneficial owner" has been added to the Revised Guidance Note. We have further specified in paragraph 4.5.1 (b) of the Revised Guidance Note that from which directors / partners of a corporate / partnership client identification documents should be obtained by licensed corporations or associated entities. Further guidance has been provided in the Revised

Guidance Note on some of the relevant measures in customer due diligence that should be considered when dealing with corporate clients.

18. As regards clients that are listed corporations, we agree that the Guidance Note should clarify the SFC's expectation over the related customer due diligence measures. We have therefore specified in paragraph 4.5.1 (b) of the Revised Guidance Note that a corporation that is listed on a stock market of a country which is a member of the FATF or a specified stock exchange as defined under the SFO, the corporation itself can be regarded as the person whose identity is to be verified.

Miscellaneous

19. Guidance was sought on handling high risk accounts and identifying beneficial owners who are holders of bearer shares. These subjects are also currently under the FATF's deliberation and changes to the Guidance Note would be made only when the review of the 40 Recommendations is completed so as to ensure that our requirements are in line with the FATF's standards.

EFFECTIVE DATE

20. The Revised Guidance Note will become effective on 1 April 2003.

Summary of comments received on the Draft Guidance Note issued by the Securities and Futures Commission on Money Laundering and Terrorist Financing

| Item no. | Paragraph no. | Details of the Guidance Note | Respondent's comments | SFC's response |
|-----------------|----------------------|--|--|--|
| 1 | 1.2 | The scope of application of the Guidance Note | [HKAOB] Authorized financial institutions should be subject to the Guidance Note in full in order to avoid unnecessary complications and to ensure level playing field. | The Revised Guidance Note will not generally apply to registered institutions and associated entities that are authorized financial institutions though they should have regard to the examples of suspicious transactions specific to the securities and futures sectors provided in Appendix B(ii) of the Revised Guidance Note in identifying suspicious transactions. This is because that they are already subject to the HKMA's Guideline which is no less stringent than the Revised Guidance Note. The SFC will keep in view any future changes to the HKMA's Guideline to ensure that authorized financial institutions remain to be subject to at least equally stringent requirements in this regard. |
| 2 | 4.5.1 (a) | Policies and procedures on "Client identification" – In a small number of cases where a licensed corporation or an associated entity may not be able to obtain adequate verification, it may be necessary, with client's consent, to approach another licensed corporation specifically for the purpose of verifying identity. | [GS&MS&ML] It should also be acceptable for a licensed corporation or an associated entity to approach a regulated intermediary in a jurisdiction that has anti-money laundering / anti-terrorism procedures / laws comparable to those in force in Hong Kong for such verification and it should not be restricted to a "small number of cases". Licensed corporation should be able to rely, in most instances, on such regulated intermediaries. | The Revised Guidance Note has already incorporated a reference in paragraph 4.5.1 (a) to the Code of Conduct in relation to client identification procedures in the case where a non-face-to-face account opening approach is adopted. A third party may be relied on for verifying client identity only to the extent of sighting the original identity documents and certifying the signing of the client agreement, and the types of third party are limited to those specified therein, including another licensed or registered person. In fact, the last paragraph of 4.5.1 (a) does not add anything and has been deleted. |

| | | | | |
|---|-----------|--|---|---|
| | | | | <p>Reliance on third parties to perform other elements of client identification and customer due diligence process is a subject presently under the FATF’s deliberation and, as explained in the Consultation Document, changes to the Guidance Note would be made only when the review of the 40 Recommendations is completed so as to ensure that our requirements are in line with FATF’s standards.</p> |
| 3 | 4.5.1 (b) | Policies and procedures on “Client identification” – Corporate / Partnership Clients | <p>[Anonymous] While information on all directors or partners can be obtained from the statutory documents provided by customer or through company search, there may be practical difficulties in obtaining the identification documents of all directors or partners, particularly in cases where some of the directors or partners reside overseas. Setting a minimum number of directors or partners similar to that of the HKMA, i.e. at least two directors / partner, should be considered.</p> | <p>It is not our intention to require licensed corporations or associated entities to obtain identification documents of all directors or partners.</p> <p>We agree that the Guidance Note should clarify the SFC’s expectations. Clarification is now made in paragraph 4.5.1(b) of the Revised Guidance Note such that licensed corporations and associated entities should obtain identification documents of at least two directors or partners (including the managing director or managing partner) in the case of a corporate / partnership client.</p> |
| 4 | 4.5.1 (b) | Policies and procedures on “Client identification” – Corporate / Partnership Clients | <p>[Anonymous] A definition of major shareholder and whether beneficial owner refers to the natural person who ultimately owns the corporate / partnership customer should be provided.</p> | <p>“Major shareholders” has now been changed to “substantial shareholder” since the definition of that term in section 6 of Part 1 of Schedule 1 to the Securities and Futures Ordinance is considered appropriate for the purposes of the Revised Guidance Note.</p> <p>A definition of “beneficial owner” has been added in paragraph 4.5.1 (b). It refers to the natural person(s) who ultimately owns or controls a customer (which may include a corporate / partnership customer) and / or the person on whose behalf a transaction is being conducted.</p> |

| | | | | |
|---|--|--|--|---|
| 5 | | | <p>[Anonymous] Clarification is sought on whether identification information on all or only major beneficial owners is required. It is common that some companies have many layers of companies in their shareholding structure. It may be impractical to obtain details on all these companies. Limiting the requirement to major rather than all beneficial owners should be considered.</p> <p>Moreover, some companies may have a “cross-shareholdings” structure which would not disclose in their statutory document the natural persons who ultimately own the corporate or partnership customer. Clarification is sought on whether the identification of legal beneficial ownership in such circumstances would satisfy SFC’s requirement on beneficial owners.</p> | <p>A licensed corporation or an associated entity should look behind the corporation to identify the beneficial owners and those who exercise control over the funds. Further guidance has now been provided in that paragraph of the Revised Guidance Note regarding some of the relevant measures in customer due diligence that should be considered when dealing with corporate clients.</p> |
| 6 | | | <p>[Anonymous] Provide guidance on the identification of beneficial owners who are holders of bearer shares.</p> | <p>Customer due diligence over bearer shareholding is a subject presently under the FATF’s deliberation and changes to the Guidance Note would be made only when the review of the 40 Recommendations is completed so as to ensure that our requirements are in line with FATF’s standards.</p> |
| 7 | | | <p>[Anonymous] Clarification is sought on whether there is any exemption or difference in requirements for companies listed locally or overseas.</p> | <p>The Guidance Note currently does not stipulate any exemption for the client identification requirement on listed corporations. We agree that the Guidance Note should clarify the SFC’s expectations regarding customer due diligence measures when identifying the beneficial owners of listed corporations. Therefore, the following text has been added to paragraph 4.5.1 (b) of the Revised Guidance Note to clarify this matter:</p> |

| | | | | |
|---|-----------|---|---|---|
| | | | | <p>“Where a corporation is listed on a stock market of a country which is a member of FATF or on a specified stock exchange as defined under the Securities and Futures Ordinance, the corporation itself can be regarded as the person whose identity is to be verified. It will therefore be generally sufficient for a licensed corporation or an associated entity to obtain documents on certificate of incorporation and business registration certificate, board resolution to open an account and confer authority on those who will operate the account and memorandum and articles of association, without the need to make further enquiries about the identity of the substantial shareholders, individual directors or authorized signatories of the account. Where a listed corporation is effectively controlled by an individual or a small group of individuals, a licensed corporation or an associated entity should consider whether it is necessary to verify the identity of such individual(s).”</p> |
| 8 | 4.5.1 (d) | <p>In the case where an account is opened on behalf of a third person / trust account, care should be taken to check the identity of all of the parties who have an interest in the account (including the legal and beneficial owners) along the lines of the account opening procedures for other accounts.</p> | <p>[GS&MS&ML] [CC] It is impractical for a licensed corporation or an associated entity to know the identity of all beneficial owners of such an account e.g. an account opened by a fund manager for a unit trust. Reliance on a regulated intermediary in a jurisdiction that has anti-money laundering / anti-terrorism procedures / laws comparable to those in force in Hong Kong to perform anti-money laundering and anti-terrorism checks should be allowed.</p> <p>Queried whether it is necessary for these identity checks to be duplicated where the relevant entity’s client that opens accounts on behalf of third parties</p> | <p>Client identification measures applicable to legal arrangements such as trusts are currently being reviewed by FATF in the course of its review of the 40 Recommendations and changes to the Guidance Note would be made only when the review is completed so as to ensure that our requirements are in line with FATF’s standards.</p> <p>With regard to relying on third parties for verifying client identity to the extent of sighting the original identity documents and certifying the signing of the client agreement, please refer to our response to comment 2.</p> |

| | | | | |
|---|-----------|--|---|--|
| | | | <p>is itself a licensed corporation or an associated entity or is regulated to the same standard by another regulator of other jurisdiction (other than those designated as Non-cooperative countries and territories by the FATF) (“approved entities”). References to the “Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission” and the “Client Identity Rule Policy” issued by the Securities and Futures Commission should be made and that a licensed corporation or an associated entity could be entitled whenever it is dealing with approved entities to simply enter into an agreement, prior to executing a transaction, in which the approved entities agree, on request, to provide information about the beneficiary of a transaction directly to the regulators without having to pass the information to the licensed corporation or associated entity, and thereby obviate the need for specific exceptions for investment funds, discretionary accounts and discretionary trusts. The Guidance Note should be amended for clarity so that all the issues relating to client identification are contained in the same document. Further, specific provisions could be included in the letter of agreement a statement as to the approved entity’s approach to client identity / anti-money laundering when dealing with approved entities which are not regulated entities but are part of a group of regulated entities.</p> | <p>In the case of dealing with an intermediary client, it should be noted that the “Client Identity Rule Policy” whose purpose is to enable the SFC to better conduct market surveillance to identify insider dealers and market manipulators, is not to supplant the client identification requirement outlined in the Guidance Note. Besides being satisfied that the third party is an “approved entity” and entering into an agreement with such “approved entity”, there are other criteria that will need to be considered before a third party can be relied upon to perform respective elements of the customer due diligence process. The subject is also under the FATF’s current deliberation and changes to the Guidance Note would be made only when the review of the 40 Recommendations is completed so as to ensure that our requirements are in line with FATF’s standards.</p> |
| 9 | 4.5.1 (e) | For client identification of overseas clients, it is preferred to have documents certified by the company’s lawyers in its place of incorporation. | <p>[HKAOB] The certification element should be consistent with the Code of Conduct so that documents may be certified by any other registered person, an affiliate of a licensed person, a JP (Justice of the Peace), or a professional person such as a branch manager of a</p> | <p>The Revised Guidance Note has already incorporated a reference in paragraph 4.5.1 (a) to the Code of Conduct in relation to client identification procedures in the case where a non-face-to-face account opening approach is adopted. A third party may be relied on for verifying client identity only to</p> |

| | | | | |
|----|-----------|---|--|--|
| | | | bank, certified public accountant, lawyer or notary public. | the extent of sighting the original identity documents and certifying the signing of client agreement, and the types of third party are limited to those specified therein, including lawyers. In fact, the last sentence of 4.5.1 (e) does not add anything and has been now deleted. |
| 10 | 4.5.5 (a) | The obligation to report under the DTROP, the OSCO and the UNATMO rests with the individual who become suspicious of a person, transaction or property. | [LSHK] A reminder should be added such that in accordance with the Code of Conduct, the ultimate responsibility to implement and maintain proper procedures for staff to identify and disclose suspicious transactions remains on the senior management of licensed corporations and associated entities. | <p>The Guidance Note should be read in conjunction with all other codes and guidelines issued by the SFC including the Code of Conduct and the “Management, Supervision and Internal Control Guidelines for Persons Registered with or Licensed by the Securities and Futures Commission” (“IC Guidelines”). In particular, the IC Guidelines require management to assume full responsibility for the firm’s operations including the development, implementation and on-going effectiveness of the firm’s internal controls, including procedures to prevent money laundering, and adherence thereto by its directors and employees.</p> <p>Paragraphs 4.1 to 4.5 of the Revised Guidance Note provide guidance to licensed corporations and associated entities on specific policies and procedures aimed at preventing and impeding money laundering and terrorist financing, covering issues ranging from client identification to recognizing and reporting suspicious transactions.</p> <p>Therefore, such a reminder is not considered necessary.</p> <p>It should be noted that whilst provisions of the anti-money laundering and anti-terrorist financing laws impose reporting obligations on any person who become suspicious of a person, transaction or</p> |

| | | | | |
|----|------------------------|--|--|--|
| | | | | property, a person who is in employment can make a suspicious transaction disclosure to the appropriate person in accordance with the procedures established by his employer to discharge his obligation. |
| 11 | 4.5.5 (d) / Appendix D | Consent given by JFIU to operate the account which has been reported under DTROP / OSCO / UNATMO. | [LSHK] The JFIU should indicate approximately how long the period for considering disclosure and granting clearance in respect of a particular report will be and, if there is no reply from JFIU within a specified period, that it will be treated as a deemed consent / clearance from JFIU. Given the nature of the financial market place, any deemed consent period should be relatively short. | This is outside the remit of the SFC. The suggestion has been forwarded to the JFIU for its consideration. |
| 12 | Appendix A | Diagram on laundering of proceeds | [LSHK] The diagram only illustrates the laundering process of proceeds from drug trafficking. It should also include illustration on the money laundering process of other criminal or terrorist financing. | It must be noted that money laundering methods are virtually unlimited and that their techniques are ever changing. We have nevertheless made references in the Revised Guidance Note to additional related websites which provide further illustrations of the methods and processes of money laundering. |
| 13 | Appendix B(i) | “Recognition of a suspicious financial activity indicator (s)” and “Appropriate questioning of the customer” | [GS&MS&ML] [LSHK] The Guidance Note should clarify that the measures given under Step One in recognizing suspicious financial activity indicators of Appendix B(i) are given by way of examples only and that licensed corporations or associated entities are not required to implement each such measure. In addition, further guidance on how to manage and handle “high risk” accounts should be provided in the Appendix. With regard to Step Two on appropriate questioning of the customer, it is unlikely, in practice, that a | It is the intention of the SFC and also that of the JFIU that the methods of recognizing suspicious activities are given by way of examples only. With regard to what constitutes appropriate questioning, the situations included in the appendix are given by way of example only and the timing and the extent questioning to be undertaken depends on the totality of the circumstances. Amendments have now been made under paragraph 4.5.4(b) of the Revised Guidance Note to clarify this. |

| | | | | |
|--|--|--|--|---|
| | | | situation would so obviously require additional questioning as the example given in the Guidance Note suggests, as cash transactions are actually quite rare. The Guidance Note should further make clear that licensed corporations or associated entities must always make a judgment as to when and how far to question clients prior to deciding whether a suspicious activity report to the JFIU is required. | As with “high risk” accounts, this is a subject presently under the FATF’s deliberation and changes to the Guidance Note would be made only when the review of the 40 Recommendations is completed so as to ensure that our requirements are in line with FATF’s standards. |
|--|--|--|--|---|

List of Respondents

| | Date received | Respondent |
|---|----------------------|---|
| 1 | 21 February 2003 | Goldman Sachs (Asia) L.L.C, Morgan Stanley Dean Witter Asia Limited and Merrill Lynch (Asia Pacific) Limited jointly (GS&MS&ML) |
| 2 | 24 February 2003 | Clifford Chance (CC) |
| 3 | 24 February 2003 | Law Society of Hong Kong (LSHK) |
| 4 | 26 February 2003 | The Hong Kong Association of Online Brokers (HKAOB) |
| 5 | 22 February 2003 | (Commentator reserved anonymity) |

**PREVENTION OF
MONEY LAUNDERING AND TERRORIST FINANCING**

**GUIDANCE NOTE ISSUED BY THE
SECURITIES AND FUTURES COMMISSION**

April 2003

Table of Contents

| | | |
|----------------|---|----|
| 1. | INTRODUCTION..... | 1 |
| 2. | BACKGROUND..... | 2 |
| 2.1 | The nature of money laundering..... | 2 |
| 2.2 | Stages of money laundering..... | 2 |
| 2.3 | Potential uses of the securities, futures and leveraged foreign exchange businesses in the money laundering process..... | 3 |
| 2.4 | Terrorist financing..... | 4 |
| 2.5 | Recent international initiatives..... | 4 |
| 3. | LEGISLATION CONCERNED WITH MONEY LAUNDERING AND TERRORIST FINANCING..... | 5 |
| 3.1 | The Drug Trafficking (Recovery of Proceeds) Ordinance..... | 5 |
| 3.2 | The Organized and Serious Crimes Ordinance..... | 8 |
| 3.3 | The United Nations (Anti-Terrorism Measures) Ordinance..... | 11 |
| 4. | POLICIES AND PROCEDURES EXPECTED OF LICENSED CORPORATIONS AND ASSOCIATED ENTITIES..... | 13 |
| Appendix A | Laundering of Proceeds..... | 24 |
| Appendix B(i) | A Systemic Approach to Identifying Suspicious Transactions Recommended by the JFIU..... | 25 |
| Appendix B(ii) | Examples of Suspicious Transactions..... | 30 |
| Appendix C | Report Made to the JFIU | 32 |
| Appendix D | Sample Acknowledgement Letter from the JFIU..... | 33 |
| Appendix E | JFIU Contact Details..... | 34 |

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 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 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 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.
- 1.5 The three main pieces of legislation in Hong Kong that are concerned with money laundering and terrorist financing are the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap.405), 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:

- (a) drug dealers and criminals have a need to conceal the true ownership and origin of the money;
- (b) these persons have a need to maintain control over the money; and
- (c) 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 licensed corporation or an associated entity may be alerted to 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 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 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 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 Financial Action Task Force on Money Laundering (“FATF”) is a pre-eminent inter-governmental organization established in 1989 to examine and recommend measures to counter money laundering. The FATF’s Forty Recommendations set out the framework for anti-money laundering efforts and are designed for universal application. Hong Kong has been a member of the FATF 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.
- 2.5.2 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, 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 eight 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 CONCERNED WITH MONEY LAUNDERING AND TERRORIST FINANCING

In Hong Kong, the Drug Trafficking (Recovery of Proceeds) Ordinance, the Organized and Serious Crimes Ordinance and the United Nations (Anti-Terrorism Measures) Ordinance, deal with the problems in relation to terrorist financing and money laundering activities in the areas of terrorism, drug 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 ("DTROP")

3.1.1 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.

3.1.2 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.

3.1.3 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 Joint Financial Intelligence Unit ("JFIU"). The JFIU has been established, and 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 paragraph 4.5.5 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.

3.1.4 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 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 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.
- 3.1.6 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.
- 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 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.

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

3.2.1 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.

3.2.2 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.

3.2.3 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.

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 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.

3.2.5 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 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 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.

3.2.7 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.

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 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.

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

3.3.1 The UNATMO was enacted in July 2002 and a substantive 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.

3.3.2 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 A list of terrorist or terrorist associate names is published in the Gazette from time to time pursuant to section 10 of the United Nations Sanctions (Afghanistan) Regulation and section 4 of the UNATMO. The published lists reflects designations made by the UN Committee that was established

pursuant to UNSC Resolution 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 regards 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.

4. POLICIES AND PROCEDURES EXPECTED OF LICENSED CORPORATIONS AND ASSOCIATED ENTITIES

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 Licensed corporations and associated entities 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 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 licensed 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 subsidiaries as to the local reporting point to whom disclosure should be made of any suspicion about a person, transaction or property. Where a local jurisdiction has an anti-money laundering or anti-terrorist financing law, branches and subsidiaries of 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 licensed corporations and associated entities in developing appropriate policies and procedures.

4.5.1 Client identification

(a) General

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 client, and of each client's financial situation and investment objectives.

Before opening an account, positive identification of 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.

(b) Corporate/Partnership Clients

In respect of 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 at least two directors or partners (including the managing director or managing partner), as the case may be, and of all account signatories; and
- information on substantial shareholders¹ and beneficial owners².

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.

Particular care should be taken when a corporation has overly complex ownership structure that does not seem to serve any legitimate purpose or when is incorporated / administered in a jurisdiction that does not provide a system that satisfies the customer due diligence requirements as set out in the FATF's 40 Recommendations³ (such as jurisdictions designated as the Non-Cooperative Countries and Territories³ by the FATF). Licensed corporations and associated entities should understand the structure and the purpose of the company and determine the source of funds to the greatest practicable extent.

¹ The term "substantial shareholder" is defined under section 6 of Part 1 of Schedule 1 to the Securities and Futures Ordinance.

² Beneficial owner is the natural person(s) who ultimately owns or controls a customer (which may include a corporate / partnership customer) and / or the person on whose behalf a transaction is being conducted.

³ FATF's 40 Recommendations and the Non-Cooperative Countries and Territories designated by FATF can be found on the FATF website www.fatf-gafi.org/40Recs_en.htm and www.fatf-gafi.org/NCCT_en.htm, respectively.

Where a corporation is listed on a stock market of a country which is a member of FATF or on a specified stock exchange as defined under the Securities and Futures Ordinance, the corporation itself can be regarded as the person whose identity is to be verified. It will therefore be generally sufficient for a licensed corporation or an associated entity to obtain documents on certificate of incorporation and business registration certificate, board resolution to open an account and confer authority on those who will operate the account, and memorandum and articles of association, without the need to make further enquiries about the identity of the substantial shareholders, individual directors or authorized signatories of the account. Where a listed corporation is effectively controlled by an individual or a small group of individuals, a licensed corporation or an associated entity should consider whether it is necessary to verify the identity of such individual(s).

(c) No anonymous accounts

Anonymous accounts are not allowed.

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

A licensed corporation or 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 in the account (including the legal and beneficial owners) along the lines of the account opening procedures for other accounts.

(e) Overseas Clients

For overseas clients in a country where the licensed corporation or 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 licensed corporation or associated entity.

(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.

4.5.2 Record Keeping

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.

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:

- (a) the beneficial owner of the account;
- (b) the volume of the funds flowing through the account; and
- (c) for selected 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.

Where appropriate, licensed corporations and 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 :

- (a) All necessary records on transactions, both domestic and international, should be maintained for at least seven years. Such records must be 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.
- (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 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 Recognizing and Reporting Suspicious Transactions

- (a) 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.
- (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). The methods of recognizing suspicious activities and approaches in the questioning of customers as suggested in the appendix,

are given by way of examples only. The timing and the extent of the questioning to be undertaken depends on the totality of the circumstances.

- (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 paper⁴.
- (d) The list of potentially suspicious or unusual activities in Appendix B(ii) 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), 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

⁴ The FATF paper is available on the FATF website www.fatf-gafi.org/TerFinance_en.htm.

Department of the Treasury website⁵ and lists referred to on the Commission's website⁶).

- (f) Disclosures of suspicious transactions under the DTROP, 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

- (a) 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. Under certain circumstances, a staff member of a licensed corporation or 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.
- (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 contact details of the JFIU are set out at Appendix E.
- (c) A register of all reports made to the JFIU and all reports made by employees to management should be kept.
- (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 in relation to an account, consent will usually be given for the licensed corporation or associated entity to operate the account

⁵ 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.

⁶ Lists referred to on the Commission's website can be found at www.hksfc.org.hk/eng/licensing/html/index/index4.html.

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 D.

- (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 the Customs and Excise Department for further investigation.
- (f) 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.
- (g) The Police and Customs and Excise Departments 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.
- (h) 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.

4.5.6 Education and Training

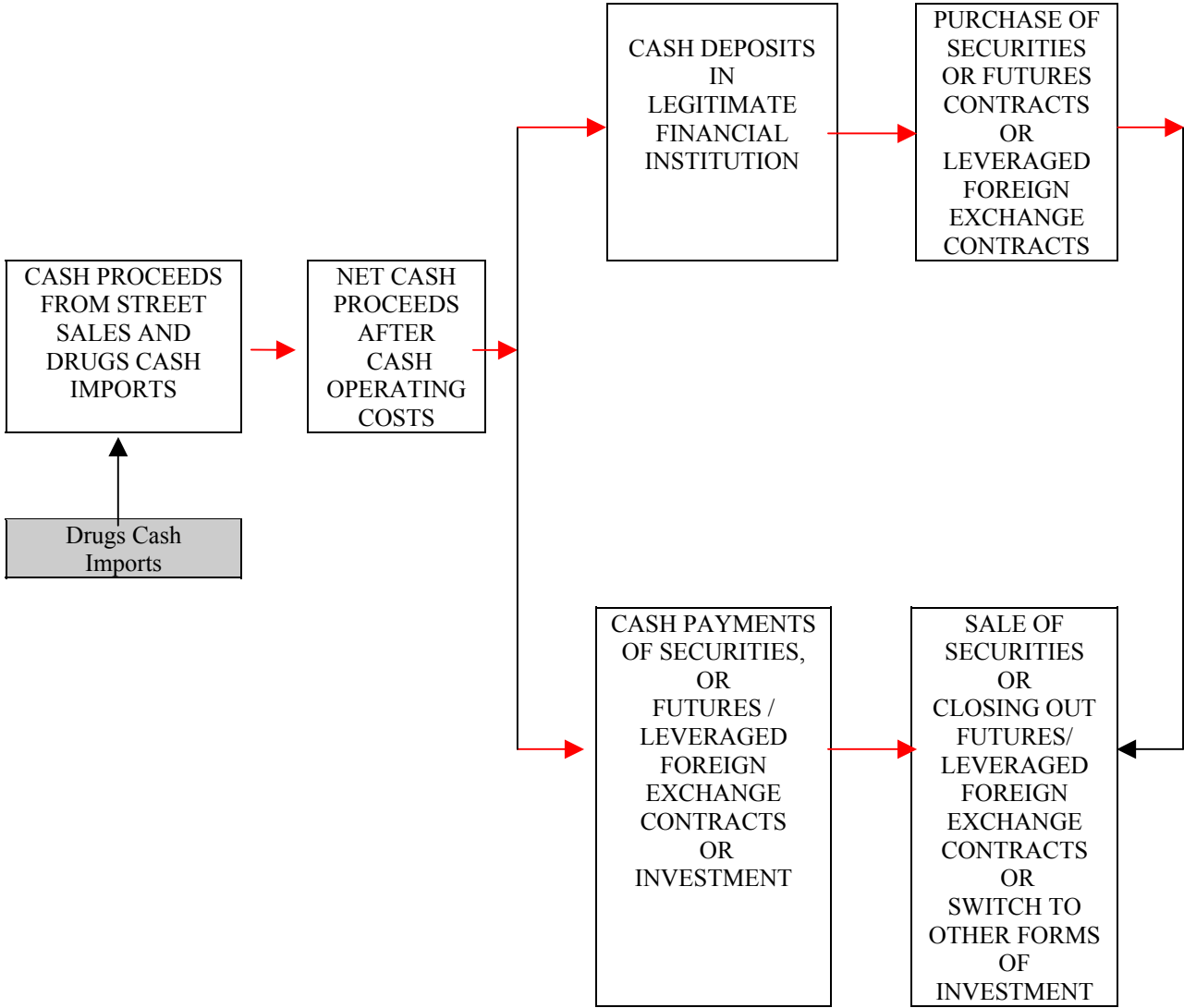
- (a) Licensed corporations and associated entities must provide proper anti-money laundering and anti-terrorist financing training to their local and overseas staff members.
- (b) Members of staff should be aware of their own personal obligations under the DTROP, the OSCO and the UNATMO and that they 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.

- (c) Licensed corporations and associated entities should have educational programmes in place for training new employees, members of staff who deal with the public directly and open new accounts, and those who supervise or manage such staff members.
- (d) On-going training

It is also 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

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/TerFinance_en.htm).

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.

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 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 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 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 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 to hold funds that are not being used to trade in securities, futures contracts or leveraged foreign exchange contracts.
- g) A client 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.

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 client'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.

| 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 CLIENT) |
| OCCUPATION & EMPLOYER / NATURE OF BUSINESS (IN THE CASE OF A CORPORATE CLIENT) | | |
| NATIONALITY / PLACE OF INCORPORATION (IN THE CASE OF A CORPORATE CLIENT) | | HKID NUMBER/ PASSPORT NUMBER/BUSINESS REG. NO. (IN THE CASE OF A CORPORATE CLIENT) |
| ADDRESS OF ACCOUNT HOLDER | | |
| DETAILS OF TRANSACTION/PROPERTY AROUSING SUSPICION AND ANY OTHER RELEVANT INFORMATION. PLEASE ALSO ENCLOSE COPY OF THE TRANSACTION AND ACCOUNT STATEMENT 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 January 2003 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

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.