

The Guideline for

Precious Metals and
Precious Stones Dealers

(2008)

The Guideline for Precious Metals and Precious Stones Dealers (2008)

CONTENTS

	Page
Section 1. Introduction	1
Section 2. What is Money Laundering?	2
Section 3. Prevention of Money Laundering in Hong Kong	4
Section 4. Terrorist Financing	7
Section 5. Basic Policies and Principles to Combat Money Laundering and Terrorist Financing	11
Section 6. Existing Customer Accounts	13
Section 7. On-Going Monitoring	14
Section 8. Politically Exposed Persons (PEPs)	15
Section 9. Internal Control	17
Section 10. Suspicious Transactions	19
Section 11. Reporting of Suspicious Transactions	20
Section 12. Feedback	24
Section 13. JFIU Website	25
Section 14. Staff Education and Training	26
Annexure 1 Examples of Suspicious Transactions	28
Annexure 2 Suspicious Transaction Report Form	30

1. Introduction

- 1.1 In 1990, the Financial Action Task Force on Money Laundering (FATF)¹ put forward 40 recommendations for the prevention of money laundering. In October 2001 and October 2004, the FATF supplemented the 40 Recommendations with 9 Special Recommendations on Terrorist Financing. They are collectively known as 40 + 9 Recommendations. Hong Kong, as a major international financial centre and a member of the FATF, is required to be compliant with all 40 + 9 Recommendations.
- 1.2 Since June 2003, dealers in precious metals/stones have been classified as 'Designated non-financial businesses and professions' ("DNFBPs") by the FATF and are therefore subject to the same requirements in terms of anti-money laundering and combating the financing of terrorism ("AML/CFT") measures as casinos, real estate agents, lawyers, accountants, and trust and company service providers.
- 1.3 This Guideline applies directly to all precious metals/stones businesses in Hong Kong. Precious metals/stones businesses are expected to ensure that they and their subsidiaries in Hong Kong have effective controls in place to comply with this Guideline. Where businesses have branches or subsidiaries overseas, steps should be taken to alert the management of such overseas branches to the requirements in Hong Kong in relation to anti-money laundering and counter terrorist financing. Where a local jurisdiction has domestic money laundering legislation, branches and subsidiaries of Hong Kong businesses operating within that jurisdiction should, as a minimum, act in accordance with the requirements of the local legislation. Where the local legislation and the Guideline are in conflict, the foreign branch or subsidiary should comply with the local legislation and inform the Hong Kong office immediately of any departure from this Guideline.

¹ Financial Action Task Force on Money Laundering - It is an international organisation aims at formulating and promoting international policies and standards on anti-money laundering and combating the financing of terrorism.

2. What is Money Laundering?

- 2.1 The phrase "money laundering" covers all procedures to change the identity of illegally obtained money so that it appears to have originated from a legitimate source.
- 2.2 Cash lends anonymity to many forms of criminal activity and is the common medium of exchange in the world of drug trafficking and organised crime. This gives rise to three common factors -
- (a) criminals need to conceal the true ownership and origin of the money;
 - (b) they need to control the money; and
 - (c) they need to change the form of the money.
- 2.3 One of the most common means of money laundering that business will encounter on a day-to-day basis takes the form of accumulated cash transactions which will be deposited in the banking system or exchanged for value items. These simple transactions may be just one part of the sophisticated web of complex transactions, which are set out and illustrated below. Nevertheless, the basic fact remains that the key stage for the detection of money laundering operations is where the cash first enters the financial system.

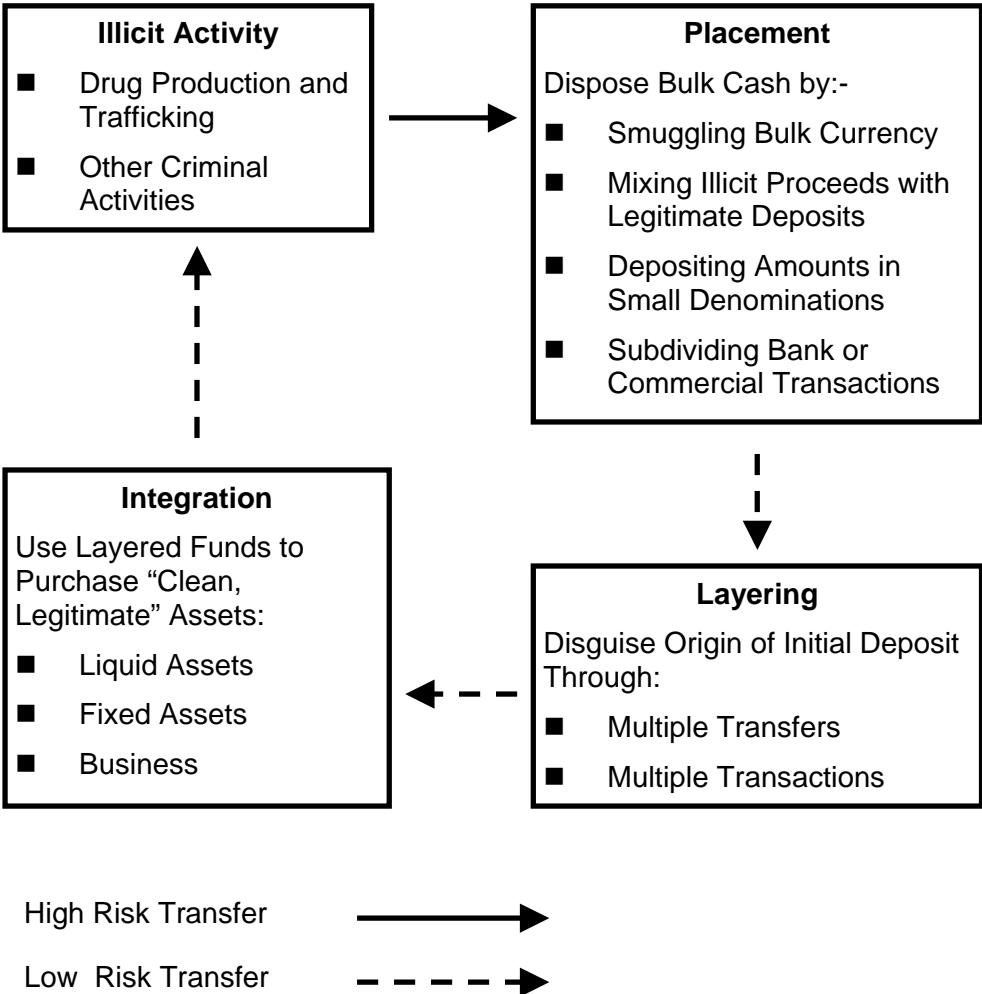
Stages of money laundering

- 2.4 There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert a business to possible criminal activity -
- (a) **Placement** - the physical disposal of cash proceeds derived from illegal activity;
 - (b) **Layering** - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity; and
 - (c) **Integration** - the provision of apparent legitimacy to criminally derived wealth. If the layering process has

succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

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

PROCESS OF MONEY LAUNDERING



3. Prevention of money laundering in Hong Kong

Anti-money laundering legislation in Hong Kong

- 3.1 Legislation has been developed in Hong Kong to address the problems associated with the laundering of proceeds from drug trafficking, serious crimes, and more recently terrorist financing. The Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP) came into force in September 1989. It provides for the tracing, freezing, and confiscation of the proceeds of drug trafficking and creates the criminal offence of money laundering in relation to such proceeds.
- 3.2 The Organized and Serious Crimes Ordinance (OSCO), which was modelled on the DTROP, was brought into operation in December 1994. It extends the money laundering offence to cover the proceeds of indictable offences in addition to drug trafficking.
- 3.3 Amendments to both Ordinances were made and came into effect on 1 September 1995. These amendments have tightened the money laundering provisions in both Ordinances and have a significant bearing on the duty to report suspicious transactions. In particular, there is now a clear statutory obligation to disclose knowledge or suspicion of the proceeds of crime.

The money-laundering offences

- 3.4 Section 25(1) of DTROP and OSCO creates the offence of dealing with any property, knowing or having reasonable grounds to believe it in whole or in part directly or indirectly represent the proceeds of drug trafficking or of an indictable offence respectively. These offences carry a maximum sentence of 14 years imprisonment and a maximum fine of \$5 million.
- 3.5 It is a defence under section 25(2) of both DTROP and OSCO for a person to prove that he intended to disclose as soon as is reasonable such knowledge, suspicion or matter to an

authorised officer, or has a reasonable excuse for his failure to make a report in accordance with section 25A(2) of the Ordinances.

Disclosure of knowledge or suspicion

- 3.6 Section 25A(1) of both DTROP and OSCO impose a statutory duty on a person, who knows or suspects that any property in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence respectively, or was or is intended to be used in that connection, to make a report to an authorised officer. Section 25A(7) makes it an offence for a person to fail to make such report. The offence carries a maximum penalty of three months imprisonment and a fine of \$50,000.

Proceeds of an overseas offence

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

Protection in law

- 3.8 Section 25A(2) of DTROP and OSCO provides that if a person who has made the necessary report does any act in contravention of section 25(1) and the report relates to that act he does not commit an offence if –
- (a) the report is made before he does that act and the act is done with the consent of an authorised officer; or
 - (b) the report is made after the person does the act and the report is made on the person's own initiative and as soon as it is reasonable for him to make it.

No breach of contract, etc.

- 3.9 Section 25A(3) of DTROP and OSCO provides that a report made under section 25A(1) (see paragraph 3.6 above) shall not be treated as a breach of contract or of any enactment restricting disclosure of information, and shall not render the person making the report liable in damages for any loss arising out of the report. Therefore businesses need not be concerned about breaching their duty of confidentiality owed to customers when making a report under the Ordinances.

Employees making reports

- 3.10 Section 25A(4) of DTROP and OSCO extends the provisions of section 25A(1) to reports made by an employee to an appropriate person in accordance with the procedures established by his employer for the making of such reports in the same way as it applies to reports to an authorised officer. This provides protection to employees of business against the risk of prosecution where they have reported knowledge or suspicion of money laundering transactions to the person designated by their employers.

“Tipping-off” offence

- 3.11 A "tipping-off" offence is created under section 25A(5) of DTROP and OSCO, under which a person commits an offence if knowing or suspecting that a report has been made, he discloses to any other person any matter which is likely to prejudice an investigation that might be carried out following the first-mentioned report. The "tipping-off" offence carries a maximum penalty of three years imprisonment and a fine of \$500,000 under both DTROP and OSCO.

Report to JFIU

- 3.12 Where a business suspects that any property may be the proceeds of crime or any transaction may be related to money laundering, it should promptly make a report to the Joint Financial Intelligence Unit (the JFIU). Precise details on how to file a report can be found in **Section 11**.

4. Terrorist Financing

What is terrorist financing?

- 4.1 Terrorist financing generally refers to the carrying out of transactions involving funds that are owned by terrorists, or that have been, or are intended to be, used to facilitate the commission of terrorist acts. This has not previously been explicitly addressed under money laundering legislation where the focus is on the handling of criminal proceeds, i.e. the source of funds is what matters. In terrorist financing, the focus is on the destination or use of funds, which may have been derived from **legitimate** sources.
- 4.2 Since the “9/11” terrorist attack, the FATF has expanded its scope of work to cover matters relating to counter terrorist financing. To this end, it has formulated nine Special Recommendations on Terrorist Financing. A list of these can be found on the FATF website (<http://www.fatf-gafi.org/>).

UNSCR

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

UNATMO

- 4.4 In addition, the United Nations (Anti-Terrorism Measures) Ordinance (“UNATMO”) was enacted on 12 July 2002. This ordinance implements the mandatory elements of the UNSC Resolution 1373. The latter is aimed at combating international terrorism on various fronts, including the introduction of measures against terrorist financing. The UNATMO also implements certain elements of the FATF’s Nine Special Recommendations.

- 4.5 Section 7 of the UNATMO prohibits the provision or collection of funds for terrorist acts. This offence carries a maximum of 14 years imprisonment and an unspecified fine.

Disclosure of knowledge or suspicion

- 4.6 Section 12(1) of the UNATMO also makes it a statutory requirement for a person to report his knowledge or suspicion that any property is terrorist property to an authorised officer. Section 14(5) makes it an offence for a person to fail to make such a report. The offence carries a maximum penalty of three months imprisonment and a fine of \$50,000.

Protection in law

- 4.7 Section 12(2) of the UNATMO provides that if a person who has made the necessary report does any act in contravention of section 7 (see **paragraph 4.5** above) and the report relates to that act he does not commit an offence if –
- (a) the report is made before he does that act and the act is done with the consent of an authorised officer; or
 - (b) the report is made after the person does the act and the report is made on the person's own initiative and as soon as it is practicable for him to make it.

No breach of contract, etc.

- 4.8 Section 12(3) of the UNATMO provides that a report made under section 12(1) (see **paragraph 4.6** above) shall not be treated as breach of contract or of any enactment restricting disclosure of information and shall not render the person making the report liable in damages for any loss arising out of the report. Therefore, businesses need not be concerned about breaching their duty of confidentiality owed to customers when making a report under the Ordinance.

Employees making reports

- 4.9 Section 12(4) of the UNATMO extends the provisions of section 12(1) to reports made by an employee to an appropriate person in accordance with the procedures established by his employer

for the making of such reports in the same way as it applies to reports to an authorised officer. This provides protection to employees of businesses against the risk of prosecution where they have reported knowledge or suspicion of terrorist property to the person designated by their employers.

“Tipping-off” offence

- 4.10 A "tipping-off" offence is created under section 12(5) of the UNATMO under which a person commits an offence if knowing or suspecting that a report has been made, he discloses to any other person any matter which is likely to prejudice any investigation that might be carried out following the first-mentioned report. The "tipping-off" offence carries a maximum penalty of three years imprisonment and an unspecified fine.

Measures to ensure compliance

- 4.11 A business should take measures to ensure compliance with the relevant regulations and legislation on terrorist financing. The legal obligations of the business and those of its staff should be well-understood and adequate guidance and training should be provided to the latter. The systems and mechanisms for identification of suspicious transactions should cover terrorist financing as well as money laundering.
- 4.12 It is particularly vital that a business should be able to identify and report transactions with terrorist suspects. To this end, a business should ensure that it maintains a database of names and particulars of terrorist suspects, which consolidates the various lists (which may include lists of terrorists, terrorist organisations, their agents and terrorist property) that have been made known to it. Alternatively, a business may arrange to have secure access to such a database maintained by third party service providers.
- 4.13 Such a database should, in particular, include the lists published in the Gazette. The database should also be subject to timely updates whenever there are changes, and should be made easily accessible by staff for the purpose of identifying suspicious transactions.

- 4.14 A business should check the names of both existing and new customers against the names in the database. It should be particularly alert for suspicious purchase and/or sale of precious metals/stones.
- 4.15 Where a business suspects that a transaction is terrorist-related, it should make a report to the JFIU. Even if there is no evidence of a direct terrorist connection, the transaction should still be reported to the JFIU if it looks suspicious for other reasons. It may emerge subsequently that there is a terrorist link. Precise details on how to file a report can be found in **Section 11**.

5. Basic Policies and Principles to Combat Money Laundering and Terrorist Financing

5.1 To ensure compliance with the FATF standards, dealers in precious metals/stones should have in place the following policies, procedures and controls:

- (a) Businesses should issue a clear statement of policies in relation to anti-money laundering and counter terrorist financing. This statement should be communicated in writing to all management and relevant staff whether in branches, departments, or subsidiaries, and should be reviewed on a regular basis.
- (b) Instruction manuals should set out the businesses' procedures for:
 - occasional transactions;
 - account opening;
 - client identification;
 - record keeping; and
 - reporting of suspicious transactions.
- (c) Businesses should actively seek to promote close co-operation with law enforcement authorities, and should identify a single reference point within their organisation (usually a compliance officer) to which staff are instructed to report suspected money laundering or terrorist financing transactions promptly. This reference point should have a means of liaison with the JFIU, which is responsible for the analysis and dissemination of such reports to the appropriate law enforcement agencies for investigation. The role and responsibilities of this reference point in the reporting procedures should be clearly defined.
- (d) Measures should be undertaken to ensure that staff are educated and trained on matters contained in this Guideline, both as part of their induction procedures and at regular intervals subsequently. The aim is to generate and maintain a level of awareness and vigilance among staff, so as to enable a report to be made if suspicions are aroused.

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

6. Existing Customer Accounts

- 6.1 Although there is no existing statutory record-keeping requirement, businesses should take steps to ensure that the records of both retail and wholesale of their existing customers remain up-to-date and relevant. Additional evidence of the identity of existing customers, if possible, should be obtained to ensure that such documents are readily available for reporting STR and investigation purposes.
- 6.2 To achieve this, a business should undertake periodic reviews of existing records of customers. An appropriate time to do so is upon certain trigger events. These include:
- (a) when a significant or unusual transaction is to take place;
 - (b) when there is a material change in the way the account is operated;
 - (c) when the businesses' customer documentation standards change substantially; or
 - (d) when the business is aware that it lacks sufficient information about the customer.

7. On-going Monitoring

- 7.1 In order to satisfy its legal obligations, a business needs to have systems in place to enable it to identify and report suspicious transactions. It is not enough to rely simply on the initiative of front-line staff to make ad hoc reports. It is advisable for a business to have management information systems (MIS) to provide managers and compliance officers with timely information on a regular basis to enable them to detect patterns of unusual or suspicious activity.

- 7.2 MIS reports used for monitoring purposes should be capable of identifying transactions that are unusual either in terms of amount (for example, by reference to predetermined limits for the customer in question or to comparative figures for similar customers), type of transaction, or other relevant risk factors.

- 7.3 This also requires the business to have a good understanding of what is normal and reasonable activity for particular types of customers, taking into account the nature of the individual customer's business.

8. Politically Exposed Persons (PEPs)

- 8.1 PEPs are defined as individuals being, or who have been, entrusted with prominent public functions in a foreign country or jurisdiction, such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of public organisations and senior political party officials. The concern is that there is a possibility, especially in countries where corruption is widespread, that such PEPs may abuse their public powers for their own illicit enrichment through corrupt activities.
- 8.2 Business relationships with individuals holding important public positions as well as persons or companies clearly related to them, (i.e. family members, close associates, etc.) expose businesses to particularly significant reputation or legal risks. There should be enhanced due diligence in respect of such PEPs, such as the verification of origins and circumstances of the transaction.
- 8.3 Whilst it is acknowledged that the majority of transactions are performed on behalf of occasional customers, business should endeavour to screen such transactions for the involvement of PEPs, their relatives or close associates. Businesses are expected to be vigilant and when in doubt gather sufficient information from a customer, and check publicly available information to establish whether the customer is a PEP.
- 8.4 A risk-based approach may be adopted for identifying PEPs and focus may be put on persons from countries or jurisdictions that have a higher prevalence of corruption (reference can be made, for example, to publicly available information such as the Corruption Perceptions Index (<http://www.transparency.org/>)).
- 8.5 The involvement of a PEP in a transaction may be a factor in determining whether or not to file a report.
- 8.6 Businesses should also ascertain the source of funds before accepting a PEP as customer. The decision to conduct a

transaction on behalf of a PEP should be taken at a senior management level.

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

- (a) any particular concern over the country or jurisdiction where the PEP is from, taking into account his position;
- (b) any unexplained sources of wealth or income (i.e. value of assets owned not in line with the PEP's income level);
- (c) any source of wealth described as commission earned on government contracts;
- (d) any request by the PEP to associate any form of secrecy with a transaction; and
- (e) any use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

9. Internal Control

- 9.1 The senior management of a business should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering / terrorist financing and ensuring their effectiveness. Explicit responsibility should be allocated within a business for this purpose.

Compliance officer

- 9.2 A business should appoint a compliance officer as a central reference point for reporting suspicious transactions. The role of the compliance officer should not be simply that of a passive recipient of *ad hoc* reports of suspicious transactions. Rather, the compliance officer should play an active role in the identification and reporting of suspicious transactions. This should involve regular reviews of reports of large or irregular transactions generated by the business's management information systems as well as *ad hoc* reports made by front-line staff. Depending on the businesses' organisation structure, the specific task of reviewing reports may be delegated to other staff but the compliance officer should maintain oversight of the review process.
- 9.3 The compliance officer should consider whether a transaction is suspicious and whether it should be reported to the JFIU. In reporting to the JFIU, the compliance officer should ensure that all relevant details are provided in the report and cooperate fully with the JFIU for the purpose of investigation. If a decision is made not to report an apparently suspicious transaction to the JFIU, the reasons for this should be fully documented by the compliance officer. The fact that a report may already have been filed with the JFIU in relation to previous transactions of the customer in question **should not preclude the making of a fresh report if new suspicions are aroused.**
- 9.4 The compliance officer should have the responsibility of checking on an ongoing basis that the business has policies and procedures to ensure compliance with legal requirements and of testing such compliance.

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

Internal audit

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

10. Suspicious Transactions

- 10.1 As the ways by which money launderers laundered their crime proceeds are almost unlimited, it is difficult to define a suspicious transaction. A suspicious transaction will often be one, which is inconsistent with a customer's known legitimate business or personal activities, or with the normal business for that type of account. Therefore, the first key to recognising suspicious transaction is to “know your customer (“KYC”)”. Know your customer enables you to recognise suspicious circumstance or abnormality in the transaction(s) of the customer.
- 10.2 Examples of what may constitute suspicious transactions are given in **Annexure 1**. These are not intended to be exhaustive and only provide examples of the most basic ways in which money may be laundered. Identification of any of the types of indicators listed in **Annexure 1** should at least prompt initial enquiries about the source of funds.

11. Reporting of Suspicious Transactions

Legal obligation

- 11.1 Section 25A(1) of both DTROP and OSCO and section 12 of UNATMO impose a statutory duty **on every person**, who knows or suspects that any property is the proceeds of crime or terrorist property to make a report (a suspicious transaction report) to an authorised officer.

JFIU

- 11.2 The reception point for reports under DTROP, OSCO and UNATMO is the JFIU.
- 11.3 The Police and the Customs and Excise Department jointly operate the JFIU. The Unit is housed within Police Headquarters in Wanchai and its primary responsibilities are the reception, analysis and dissemination of suspicious transaction reports (STR).
- 11.4 In addition to acting as the centre for receipt of STR filed by any organisation or individual, the JFIU also offers practical guidance and assistance to the financial and non-financial sectors on anti-money laundering and counter financing of terrorism. The Unit is also responsible for the day-to-day maintenance of the Register of Remittance Agents and Money Changers in accordance with section 24B of OSCO.

Corporate responsibility

- 11.5 It is a good practice for a business to appoint a designated officer (e.g. a Compliance Officer) who is to be responsible for receiving and assessing internal suspicious transaction reports filed by frontline employees.
- 11.6 The designated officer should keep a register of all reports made to them by employees and all reports made to the JFIU. The designated officer should provide employees with a written acknowledgement of reports made to him/her, which will form

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

- 11.7 Where an employee of a business **knows** that a customer has engaged in criminality, under no circumstances should the employee have any transaction with the customer. A report should be promptly filed with the designated officer who, in turn, should immediately forward the report to the JFIU.
- 11.8 Where an employee of a business **suspects** that a customer might have engaged in criminality and where the customer purchases or sells precious metals/stones, this information must promptly be reported to the designated officer. If the circumstances remain to be suspicious after assessment, the designated officer should forward the report to the JFIU. If after considering all the circumstances and reviewing all available information, the designated officer consider the transaction not suspicious, he/she does not need to file the report with the JFIU. In any case, the designated officer's findings and supporting reasons should be documented. The reporting employee should also be provided with a feedback of his report. However, the feedback should be given in confidence.
- 11.9 Businesses must take steps to ensure that all employees concerned directly with purchase or sale of precious metals/stones are aware of these procedures and that it is a criminal offence to fail to report either knowledge or suspicion of proceeds of crime or terrorist property.
- 11.10 It should be noted that it is not necessary for the employees or the designated officer to ascertain what is the underlying predicate crime in filing a suspicious transaction report.

Reporting of suspicious transactions

- 11.11 Businesses should make reports of suspicious transactions to the JFIU as soon as it is reasonable for them to do so. Reference may be made to the reporting proforma at **Annexure 2**.

- 11.12 Written STR 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
Police Headquarters
Arsenal Street, Wanchai
Hong Kong
GPO Box 6555, Hong Kong
Fax No. : 2529-4013
E-mail : jfiu@police.gov.hk

- 11.13 Following receipt of a report and analysis by the JFIU, the information may be referred to an appropriate investigative unit of law enforcement agencies for further investigation.

- 11.14 Businesses must not carry out transactions which they know or have reasonable grounds to believe the property relating to the transactions represent the proceeds of crime, unless they have informed the JFIU which consents to the business carrying out the transactions. It should be noted that the law allows the flexibility that reports to the JFIU can be made after a person does any act in contravention of the money laundering offence so long as the report (which is related to that act) is made on his initiative and as soon as it is reasonable for him to make it.

Post-reporting precaution

- 11.15 Where it is known or suspected that a report has already been filed with the JFIU and it becomes necessary to make further enquiries of the customer, great care must be taken to ensure that the customer does not become aware that his name or activities have been brought to the attention of the law enforcement agencies.

Confidentiality of identity

- 11.16 Access to the disclosed information is restricted to financial investigating officers within the law enforcement agencies. In the event of a prosecution, production orders will be obtained to produce the materials to court. Section 26 of both DTROP and OSCO and section 12 of UNATMO imposes strict restrictions

on revealing the identity of the person making the report. Maintaining the integrity of the relationship, which has been established between law enforcement agencies and the financial and non-financial sectors, is considered to be of paramount importance.

- 11.17 All STRs are dealt with in the strictest confidence as required by the provisions of the three Ordinances (DTROP, OSCO and UNATMO).

e-filing of STR

- 11.18 Since November 2006, the JFIU have operated a web based electronic reporting system for the filing of STR known as "STREAMS". Businesses that are interested in accessing the e-reporting system should make a written request to the JFIU.

12. Feedback

- 12.1 The JFIU will acknowledge receipt of a report made by a business under section 25A of both DTROP and OSCO and section 12 of UNATMO. If there is no imminent need for action e.g. the application for a restraint order on certain property, consent will usually be given for the business to continue with the transaction under the provisions of section 25A(2) of DTROP and OSCO and section 12(2)(a) UNATMO.
- 12.2 The report will be assessed and then sent, if appropriate, to the relevant law enforcement agencies for follow up investigation. When the investigation is concluded, a letter will be sent to the business making the report to convey the result of the investigation.

13. The JFIU Website

- 13.1 The JFIU website (<http://www.jfiu.gov.hk>) is the primary means of communicating with the sector; it provides links to typologies, information on the latest money laundering trends, gazetted lists of designated terrorists and other matters of interest to the sector.

- 13.2 The onus is upon businesses to check the website and keep themselves update on developments and matters affecting the sector.

14. Staff Education and Training

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

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

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

(a) New Employees

New employees, who will be dealing with customers or their transactions, irrespective of the level of seniority, should have a general appreciation of the background about money laundering, the consequent need to be able to identify suspicious transactions and report such transactions to the appropriate designated point within the business, and the offence of "tipping off". They should be familiar with the legal requirement and their personal statutory obligation to report suspicious transactions relating to drug trafficking or other indictable offences.

(b) Front-line staff

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers. Their efforts are therefore vital to the businesses' strategy in the fight against money

laundering. They should be familiar with their legal responsibilities and the businesses' reporting system for such transactions.

Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is considered to be suspicious. It is vital that "front-line" staff are familiar with the businesses' policy for dealing with non-regular customers particularly where large cash transactions are involved, and the need for extra vigilance in such circumstances.

- (c) Administration / Operations Supervisors and Managers
A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the DTROP, OSCO and UNATMO; and procedures relating to service of production and restraint orders, etc.
- (d) On-going Training
It will also be necessary to make arrangements for refresher training regularly.