Guideline No. 3.3

PREVENTION OF MONEY LAUNDERING

A Guideline issued by the Monetary Authority under section 7(3) of the Banking Ordinance

CONTENTS

Example of acknowledgement of receipt by JFIU of suspicious transaction reporting

PART I : OVERVIEW

1. Introduction

1.1 This Guideline incorporates, and hence supersedes, the Guideline issued by the Monetary Authority in July 1993 on the prevention of criminal use of the banking system for the purposes of money laundering. This Guideline has been updated to take account of the enactment of the Organized and Serious Crimes Ordinance, the subsequent amendments to the money laundering provisions in that Ordinance and the Drug Trafficking (Recovery of Proceeds) Ordinance, the stocktaking review of the anti-money laundering measures undertaken by the Financial Action Task Force and the UK Money Laundering Guidance Notes for banks and building societies. It has also included other refinements and additional examples of suspicious transactions.

1.2 This Guideline applies directly to all banking and deposit taking activities in Hong Kong carried out by authorized institutions. However, institutions are expected to ensure that their subsidiaries in Hong Kong also have effective controls in place to combat money laundering. Where Hong Kong incorporated institutions have branches or subsidiaries overseas, steps should be taken to alert management of such overseas offices to Group policy in relation to money laundering. Where a local jurisdiction has a money laundering law, branches and subsidiaries of Hong Kong incorporated institutions operating within that jurisdiction should, as a minimum, act in accordance with the requirements of the local law. Where the local law and the Guideline are in conflict, the foreign branch or subsidiary should comply with the local law and inform the Head Office immediately of any departure from Group policy.

1.3 It is recognized that the relevance and usefulness of this Guideline will need to be kept under review as the methods of money laundering are constantly evolving. It may be necessary to issue amendments to this Guideline from time to time to incorporate measures to combat new money laundering threats, including those inherent in new or developing technologies that might favour anonymity.

2. What is money laundering?

2.1 The phrase "money laundering" covers all procedures to change the identity of illegally obtained money so that it appears to have originated from a legitimate source.

2.2 Cash lends anonymity to many forms of criminal activity and is the normal medium of exchange in the world of drug trafficking. This gives rise to three common factors -

(a)criminals need to conceal the true ownership and origin of the

money;

(b) they need to control the money; and

(c) they need to change the form of the money.

2.3 One of the most common means of money laundering that institutions will encounter on a day-to-day basis takes the form of accumulated cash transactions which will be deposited in the banking system or exchanged for value items. These simple transactions may be just one part of the sophisticated web of complex transactions which are set out and illustrated below. Nevertheless, the basic fact remains that the key stage for the detection of money laundering operations is where the cash first enters the financial system.

Stages of money laundering

2.4 There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert an institution to criminal activity -

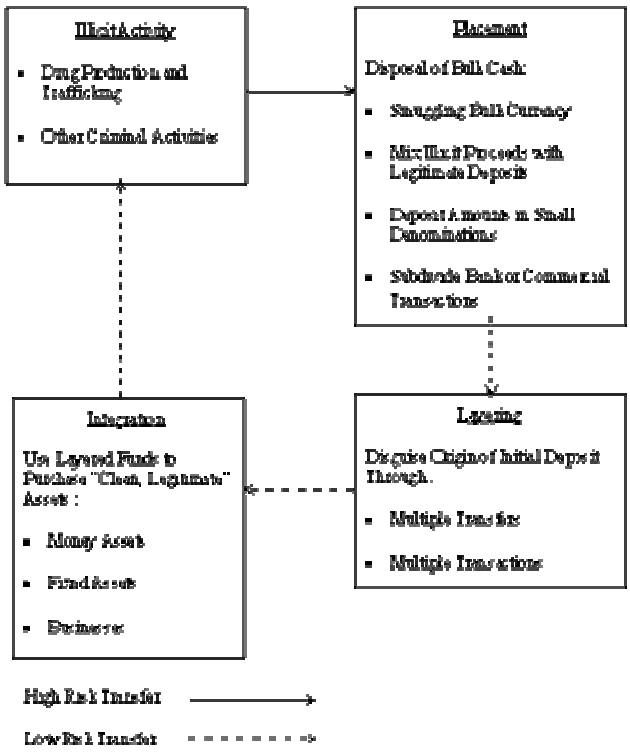
(a) Placement - the physical disposal of cash proceeds derived from illegal activity.

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

(c) Integration - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

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

PROCESS OF MONEY LAUNDERING



3. The legislation on money laundering in Hong Kong

3.1 Legislation has been developed in Hong Kong to address the problems associated with the laundering of proceeds from drug trafficking and serious crimes. The Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP) came into force in September 1989. It provides for the tracing, freezing and confiscation of the proceeds of drug trafficking and creates a criminal offence of money laundering in relation to such proceeds.

3.2 The Organized and Serious Crimes Ordinance (OSCO), which was modelled on the DTROP, was brought into operation in December 1994. It extends the money laundering offence to cover the proceeds of indictable offences in addition to drug trafficking.

3.3 Amendments to both Ordinances were made and came into effect on 1 September 1995. These amendments have tightened the money laundering provisions in both Ordinances and have a significant bearing on the duty to report suspicious transactions. In particular, there is now a clear statutory obligation to disclose knowledge or suspicion of money laundering transactions.

3.4 The key money laundering provisions in the two Ordinances are summarized below. This does not constitute a legal interpretation of the provisions of the legislation referred to, for which appropriate legal advice should be sought where necessary.

3.5 Section 25(1) of DTROP and OSCO creates the offence of dealing with

any property, knowing or having reasonable grounds to believe it in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence respectively. The offence carries a maximum sentence of 14 years' imprisonment and a maximum fine of HK$5 million.

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

3.7 Section 25A(1) imposes a statutory duty on a person, who knows or suspects that any property in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence, or was or is intended to be used in that connection, to make a disclosure to an authorized officer. Section 25A(7) makes it an offence for a person to fail to make such disclosure. The offence carries a maximum penalty of a fine at level 5 (at present $25,001 to $50,000) and imprisonment for 3 months.

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

3.9 Section 25A(2) provides that if a person who has made the necessary disclosure does any act in contravention of section 25(1) and the disclosure relates to that act he does not commit an offence if -

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

2. (b) the disclosure is made after the person does the act and the disclosure is made on the person's own initiative and as soon as it is reasonable for him to make it.

3.10 Section 25A(3) provides that disclosure made under section 25A(1) shall not be treated as breach of contract or of any enactment restricting disclosure of information and shall not render the person making the disclosure liable in damages for any loss arising out of disclosure. Therefore, institutions need not fear breaching their duty of confidentiality owed to customers when making a disclosure under the Ordinances.

3.11 Section 25A(4) extends the provisions of section 25A to disclosures made by an employee to an appropriate person in accordance with the procedures established by his employer for the making of such disclosure in the same way as it applies to disclosures to an authorized officer. This provides protection to employees of authorized institutions against the risk of prosecution where they have reported knowledge or suspicion of money laundering transactions to the person designated by their employers.

3.12 A "tipping-off" offence is created under section 25A(5) of both Ordinances, under which a person commits an offence if knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice an investigation into money laundering activities. The "tipping-off" offence carries a maximum penalty of three years' imprisonment and a fine of HK$500,000.

4. Basic policies and principles to combat money laundering

4.1 The Monetary Authority fully subscribes to the basic policies and principles to combat money laundering as embodied in the Statement of Principles issued by the Basle Committee in December 1988. The Statement seeks to deny use of the banking system to those involved in money laundering by application of the following principles -

(a) Know your customer: banks should make reasonable efforts to determine the customer's true identity, and have effective procedures for verifying the bona fides of new customers.

(b) Compliance with laws: bank management should ensure that business is conducted in conformity with high ethical standards, that laws and regulations are adhered to and that a service is not provided where there is good reason to suppose that transactions are associated with laundering activities1.

(c) Co-operation with law enforcement agencies: within any constraints imposed by rules relating to customer confidentiality, banks should co-operate fully with national law enforcement agencies including, where there are reasonable grounds for suspecting money laundering, taking appropriate measures which are consistent with the law.

(d) Policies, procedures and training: all banks should formally adopt policies consistent with the principles set out in the Statement, and should ensure that all members of their staff concerned, wherever located, are informed of the bank's policy. Attention should be given to staff training in matters covered by the statement. To promote adherence to these principles, banks should implement specific procedures for customer identification and for retaining internal records of transactions. Arrangements for internal audit may need to be extended in order to establish an effective means for general compliance with the Statement.

4.2 The principles laid down by the Basle Committee have subsequently been developed by the Financial Action Task Force (FATF). In February 1990, FATF put forward forty recommendations aimed at improving national legal systems, enhancing the role of financial systems, and strengthening international co-operation against money laundering. Hong Kong, China is a member of the FATF and fully complies with the forty recommendations.

4.3 The Monetary Authority considers that institutions should follow the

basic policies and principles as embodied in the Statement of Principles of the Basle Committee and the FATF recommendations. Specifically the Monetary Authority expects that institutions should have in place the following policies, procedures and controls -

(a) Institutions should issue a clear statement of policies in relation to money laundering, adopting current regulatory requirements. This statement should be communicated in writing to all management and relevant staff whether in branches, departments or subsidiaries and be reviewed on a regular basis.

(b) Instruction manuals should set out institutions' procedures for:

- account opening;
- identification of applicants for business;
- record-keeping;
- reporting of suspicious transactions.

(c) Institutions should seek actively to promote close co-operation with law enforcement authorities, and should identify a single reference point within their organization (usually a compliance officer) to which staff are instructed to report suspected money laundering transactions promptly. This reference point should have a means of liaison with the Joint Financial Intelligence Unit which will ensure prompt referral of suspected money-laundering transactions associated with drug trafficking or other indictable offences. The role and responsibilities of this reference point in the reporting procedures should be clearly defined.

(d) Measures should be undertaken to ensure that staff are educated and trained on matters contained in this Guideline both as part of their induction procedures and at regular future intervals. The aim is to generate and maintain a level of awareness and vigilance among staff to enable a report to be made if suspicions are aroused.

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

(f) Whilst appreciating the sensitive nature of extra-territorial regulations, and recognizing that their overseas operations must be conducted in accordance with local laws and regulations, institutions should ensure that their overseas branches and subsidiaries are aware of group policies concerning money laundering and, where appropriate, have been instructed as to the local reporting point for their suspicions.

based on the recommendations in the following sections of this Guideline.

PART II DETAILED GUIDELINES

5. Verification of identity of applicants for business

5.1 Institutions should not keep anonymous accounts or accounts in obviously fictitious names. They should obtain satisfactory evidence of

the identity and legal existence of persons applying to do business with the institution (such as opening a deposit account) on the basis of reliable documents or other resources, and record that identity and other relevant information regarding the applicant in their files. They should establish that any applicant claiming to act on behalf of another person is authorized to do so.

5.2 For the purposes of this guideline, evidence of identity can be regarded as satisfactory if -

(a) it is reasonably capable of establishing that the applicant for business is whom he claims to be; and

(b) the institution which obtains the evidence is satisfied, in accordance with the procedures established by the institution, that it does establish that fact.

5.3 New or modified requirements for verification of identity introduced by this Guideline shall apply only to business relationships entered into after 17 October 1997.

Individual applicants

5.4 Institutions should institute effective procedures for obtaining satisfactory evidence of the identity of applicants for business including obtaining information about name, permanent address, date of birth and occupation.

5.5 Positive identification should be obtained from documents issued by official or other reputable sources e.g. passports or identity cards. For Hong Kong residents, the prime source of identification will be the identity cards which they are required by law to carry with them. File copies of identity documents should be kept.

5.6 However, it must be appreciated that no form of identification can be fully guaranteed as genuine or representing correct identity. The Immigration Department operates a Hotline to which enquiries can be made concerning the validity of an identity card. If there is doubt whether an identification document is genuine, contact should be made with this Hotline immediately.

5.7 Institutions are advised to check the address of the applicant by appropriate means, e.g. by requesting sight of a recent utility or rates bill or checking the Voters Roll maintained by the Registration & Electoral Office.

5.8 Where institutions require applicants for personal banking services to provide in the application forms for such services the names and particulars of persons who have agreed to act as referees for the applicants, they should follow the practices and procedures as set out in the section on personal referees of the Code of Banking Practice jointly issued by the Hong Kong Association of Banks and the Deposit-taking Companies Association.

Corporate applicants

5.9 Company accounts are one of the more likely vehicles for money laundering, even where the company is also being used for legitimate trading purposes. It is therefore important to obtain satisfactory evidence of the identity of the principal shareholders , directors and authorized signatories and of the nature of the business. The guiding principle should be to establish that it is safe to enter into a business relationship with the company concerned.

5.10 Before a business relationship is established, measures should be taken by way of a company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound-up or terminated. In addition, if institutions become aware of subsequent changes to the company structure or ownership, or suspicions are aroused by a change in the profile of payments through a company account, further checks should be made.

5.11 The following documents or information should be obtained in respect of corporate applicants for business which are registered in Hong Kong (comparable documents, preferably certified by qualified persons such as lawyers or accountants in the country of registration, should be obtained for those applicants which are not registered in Hong Kong) -

(a) Certificate of Incorporation and Business Registration Certificate;

(b) Memorandum and articles of association;

(c) resolution of the board of directors to open an account and confer authority on those who will operate it; and

(d) a search of the file at Company Registry.

5.12 Where the company concerned is -

(a) a financial institution authorized and regulated by the Monetary Authority, the Securities and Futures Commission or the Insurance Authority in respect of its business in Hong Kong or is known to be a subsidiary of such an institution;

(b) a financial institution not authorized to carry on business in Hong Kong, but which is incorporated in a country which is a member of FATF and which is regulated by bodies carrying out equivalent functions to those mentioned in the preceding sub-paragraph;

(c) listed on The Stock Exchange of Hong Kong, or is known to be a subsidiary of such a company;

(d) listed on the stock market of a country which is a member of FATF and which is a stock market recognised by the Securities and Futures Commission for the purposes of section 65A(2)(a) of the Securities Ordinance ; or

(e) a non-listed company, whose principal shareholders and the directors (including the managing director) are already known to the institution;

it should be sufficient to obtain the documents specified in paragraph 5.11, without the need to make further enquiries about the identity of individual directors and authorized signatories. However, evidence that any individual representing the company has the necessary authority to do so should be sought and retained. In the case of financial institutions, it should be established that the institution concerned is on the relevant regulator's list of regulated institutions.

5.13 For companies other than those listed in paragraph 5.12, in addition to obtaining the documents specified in paragraph 5.11, institutions should obtain satisfactory evidence of the identity of the principal shareholders, at least two directors (including the managing director) and all authorized signatories in line with the requirements for individual applicants, and of the nature of the business.

Clubs, societies and charities

5.14 In the case of accounts to be opened for clubs, societies and charities, an institution should satisfy itself as to the legitimate purpose of the organisation by, e.g. requesting sight of the constitution. Satisfactory evidence should be obtained of the identity of the authorized signatories who are not already known to the institution in line with the requirements for individual applicants.

Unincorporated businesses

5.15 In the case of partnerships and other unincorporated businesses whose partners are not known to the bank, satisfactory evidence should be obtained of the identity of at least two partners and all authorized signatories in line with the requirements for individual applicants. In cases where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

Shell companies

5.16 Shell companies are legal entities through which financial transactions may be conducted but which have no business substance in their own right. While shell companies may be used for legitimate purposes, the FATF has expressed concern about the increasing use of such companies to conduct money laundering (through providing the means to operate what are in effect anonymous accounts). Institutions should take notice of the potential for abuse by money launderers of shell companies and should therefore be cautious in their dealings with them. In keeping with the "know your customer" principle, institutions should obtain satisfactory evidence of the identity of beneficial owners, directors and authorized signatories of shell companies. Where the shell company is introduced to the institution by a professional intermediary acting on its behalf, institutions should follow the guidelines in paragraphs 5.17 to 5.22 below.

Where the applicant for business is acting on behalf of another person

5.17 Trust, nominee and fiduciary accounts are a popular vehicle for criminals wishing to avoid identification procedures and mask the origin of the criminal money they wish to launder. Accordingly, institutions should always establish, by confirmation from an applicant for business, whether the applicant is acting on behalf of another person as trustee, nominee or agent.

5.18 Any application to open an account or undertake a transaction on behalf of another person without applicants identifying their trust or nominee capacity should be regarded as suspicious and should lead to further enquiries as to the underlying principals and the nature of the business to be transacted.

5.19 Institutions should obtain satisfactory evidence of the identity of trustees, nominees and authorized signatories and of the nature of their trustee or nominee capacity and duties by, for example, obtaining a copy of the trust deed. Enquiries should also be made of the extent to which the applicant for business is subject to official regulation (e.g. by a body equivalent to the Monetary Authority).

5.20 Particular care should be taken in relation to trusts created in jurisdictions without equivalent money laundering legislation to Hong Kong.

5.21 Where the applicant for business who is acting on behalf of another person is one of the following -

(a)(a) a financial institution authorized and regulated by the Monetary Authority, the Securities and Futures Commission or the Insurance Authority in respect of its business in Hong Kong or is known to be a subsidiary of such an institution;

(b)(b) a financial institution not authorized to carry on business in Hong Kong, but which is incorporated in a country which is a member of FATF and which is regulated by bodies carrying out equivalent functions to those mentioned in the preceding sub-paragraph; or

(c)(c) an intermediary which does not fall into the above two categories but is one with which the institution has an established business relationship and where the institution is fully satisfied as to its reputation, conduct and good faith;

it shall be reasonable for the institution to accept a written assurance from the applicant for business that evidence of the underlying principals has been obtained, recorded and retained, and that the applicant is satisfied as to the source of funds. For this purpose, it is recommended that the institution should obtain a written statement from the applicant for business (i.e. the intermediary) along the following lines:

"I/We confirm that evidence of the underlying principals has been obtained, recorded and retained, and I am/we are satisfied as to the source of funds *being used to open the account/passing through the account."

* delete as appropriate

It is recommended that the statement should be affixed to the original account opening documentation.

5.22 Where the applicant for business who is acting on behalf of another person does not fall into any of the categories in paragraph 5.21, the institution should obtain satisfactory evidence of the identity of the underlying principals and the source of funds. The use of a standard format for obtaining the relevant information is recommended. A suggested Intermediary Introduction Certificate is at Annex 3. If satisfactory evidence cannot be obtained, institutions should give very careful consideration as to whether they should proceed with the business, bearing in mind the "know your customer" principle. If they decide to proceed, they should record any misgivings and give extra attention to monitoring the account in question. Suspicious transactions should be reported in accordance with the procedures in section 9 below.

Client accounts

5.23 The guidelines in paragraphs 5.17 to 5.22 apply to client accounts opened by intermediaries. However, where the intermediary is a firm of solicitors or accountants, their professional codes of conduct may preclude the firms from divulging information to institutions concerning their underlying clients. It may therefore not be possible for an institution to establish the identity of the person(s) for whom a solicitor or accountant is acting. In such cases, the institution should obtain the written statement about the underlying principals and source of funds mentioned in paragraph 5.21. In addition, the institution should not be precluded from making reasonable enquiries about transactions passing through client accounts that give cause for concern or from reporting those transactions if any suspicions are aroused.

Avoidance of account opening by post

5.24 Whenever possible, applicants for business should be interviewed personally. Any mechanism which avoids face to face contact between institutions and applicants inevitably poses difficulties for customer identification and produces a useful loophole that money launderers may wish to exploit.

5.25 Care should be taken when dealing with accounts opened by post, or from coupon applications, to ensure that the identities of the applicants are obtained as much as possible. For local applicants, account opening by post should not be permitted. Institutions should request the applicants to call on one of their branches for account opening. For overseas applicants in a country where the institution does not have a presence, the application should be submitted through a correspondent bank in that country or a bank which can be relied upon to undertake effective identification procedures on behalf of the institution.

Transactions undertaken for non-account holders (occasional customers)

5.26 Where transactions are undertaken by an institution for non-account

holders of that institution e.g. requests for telegraphic transfers, or where funds are deposited into an existing account by persons whose names do not appear on the mandate of that account, care and vigilance are required. Where the transaction involves large sums of cash, or is unusual, the applicant should be asked to produce positive evidence of identity from the sources set out above and in the case of a foreign national, the nationality recorded. Copies of the identification documents should be kept on file.

Provision of safe custody and safety deposit boxes

5.27 Precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the identification procedures set out above should be followed.

6. Remittance

6.1 At the request of FATF, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) made a global broadcast on 30 July 1992 to its user organizations requesting them to include the names, addresses and/or account numbers of their customers in MT 100 messages. The objective is to assist the law enforcement authorities in their investigations of suspected money laundering made through electronic message systems. A copy of SWIFT's message is at Annex 4. This message should be brought to the attention of staff who deal with remittance matters within the institution.

6.2 While it is recognized that there may be technical and practical difficulties for institutions to include full details of their customers in SWIFT MT 100 messages, authorized institutions are encouraged, to the maximum extent possible, to comply with the SWIFT request.

6.3 SWIFT will implement a new optional format (MT103) in November 1997. This message format will have a new optional field which shows the account number of the sender of the telegraphic transfer. Authorized institutions are encouraged, to the maximum extent possible, to make use of the MT103 format when it is in place in future.

7. Record keeping

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

7.2 The investigating authorities need to ensure a satisfactory audit trail for suspected money laundering transactions and to be able to establish a financial profile of the suspect account. For example, to satisfy these requirements the following information may be sought -

(a) the beneficial owner of the account (for accounts opened on behalf of a third party, please see paragraphs 5.17 to 5.23);

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

(c) for selected transactions:

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

7.3 An important objective is for institutions at all stages in a transaction to be able to retrieve relevant information, to the extent that it is available, without undue delay.

7.4 When setting document retention policy, institutions must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. However, wherever practicable the following document retention times should be followed -

1. account opening records - copies of identification documents should be kept in file for six years1 following the closing of an account;

2. account ledger records - six years from entering the transaction into the ledger; and

3. records in support of entries in the accounts in whatever form they are used e.g. credit/debit slips and cheques and other forms of vouchers - six years1 from when the records were created.

7.5 Retention may be by way of original documents, stored on microfilm, or in computerized form, provided that such forms are accepted as evidence under sections 20 to 22 of the Evidence Ordinance. In situations where the records relate to on-going investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed.

8. Recognition of suspicious transactions

8.1 As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.

8.2 Examples of what might constitute suspicious transactions are given in Annex 5. These are not intended to be exhaustive and only provide examples of the most basic ways in which money may be laundered.

However, identification of any of the types of transactions listed in Annex 5 should prompt further investigations and be a catalyst towards making at least initial enquiries about the source of funds.

9. Reporting of suspicious transactions

9.1 The reception point for disclosures under the DTROP and the OSCO is the Joint Financial Intelligence Unit, which is operated by the Police and Customs and Excise Department.

9.2 In addition to acting as the point for receipt of disclosures made by any organization or individual, the unit also acts as domestic and international advisors on money laundering generally and offers practical guidance and assistance to the financial sector on the subject of money laundering.

9.3 The obligation to report is on the individual who becomes suspicious of a money laundering transaction. Each institution should appoint a designated officer or officers (Compliance Officer(s)) who should be responsible for reporting to the Joint Financial Intelligence Unit where necessary in accordance with section 25A of both the DTROP and the OSCO and to whom all internal reports should be made.

9.4 Compliance Officers should keep a register of all reports made to the Joint Financial Intelligence Unit and all reports made to them by employees. Compliance Officers should provide employees with a written acknowledgement of reports made to them, which will form part of the evidence that the reports were made in compliance with the internal procedures.

9.5 All cases where an employee of an institution knows that a customer has engaged in drug-trafficking or other indictable offences and where the customer deposits, transfers or seeks to invest funds or obtains credit against the security of such funds, or where the institution holds funds on behalf of such customer, must promptly be reported to the Compliance Officer who, in turn, must immediately report the details to the Joint Financial Intelligence Unit.

9.6 All cases, where an employee of an institution suspects or has reasonable grounds to believe that a customer might have carried on drug trafficking or might have been engaged in indictable offences and where the customer deposits, transfers or seeks to invest funds or obtains credit against the security of such funds, or where the institution holds funds on behalf of such customer, must promptly be reported to the Compliance Officer. The Compliance Officer must promptly evaluate whether there are reasonable grounds for such belief and must then immediately report the case to the Joint Financial Intelligence Unit unless he considers, and records his opinion, that such reasonable grounds do not exist.

9.7 Institutions must take steps to ensure that all employees concerned with the holding, receipt, transmission or investment of funds (whether in cash or otherwise) or the making of loans against the security of such funds are aware of these procedures and that it is a criminal offence to

fail to report either knowledge or circumstances which give rise to a reasonable belief in the existence of an offending act.

9.8 Institutions should make reports of suspicious transactions to the Joint Financial Intelligence Unit as soon as it is reasonable for them to do so. The use of a standard format for reporting is encouraged (see Annex 6 which sets out a reporting format acceptable to the Joint Financial Intelligence Unit). In the event that urgent disclosure is required, particularly when the account concerned is part of an on-going investigation, an initial notification should be made by telephone.

9.9 Institutions should refrain from carrying out transactions which they know or suspect to be related to money laundering until they have informed the Joint Financial Intelligence Unit which consents to the institution carrying out the transactions. Where it is impossible to refrain or if this is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, institutions may carry out the transactions and notify the Joint Financial Intelligence Unit on their own initiative and as soon as it is reasonable for them to do so.

9.10 Cases do occur when an institution declines to open an account for an applicant for business, or refuses to deal with a request made by a non-account holder because of serious doubts about the good faith of the individual and concern about potential criminal activity. Institutions must base their decisions on normal commercial criteria and internal policy. However, to guard against money laundering, it is important to establish an audit trail for suspicious funds. Thus, where practicable, institutions are requested to seek and retain copies of relevant identification documents which they may obtain and to report the offer of suspicious funds to the Joint Financial Intelligence Unit.

9.11 Where it is known or suspected that a report has already been disclosed to the Joint Financial Intelligence Unit and it becomes necessary to make further enquiries of the customer, great care should be taken to ensure that the customer does not become aware that his name has been brought to the attention of the law enforcement agencies.

9.12 Following receipt of a disclosure and research by the Joint Financial Intelligence Unit, the information disclosed is allocated to trained financial investigation officers in the Police and Customs and Excise Department for further investigation including seeking supplementary information from the institution making the disclosure, and from other sources. Discreet enquiries are then made to confirm the basis for suspicion.

9.13 Access to the disclosed information is restricted to financial investigating officers within the Police and Customs and Excise Department. In the event of a prosecution, production orders are obtained to produce the material for court. Section 26 of both the DTROP and the OSCO places strict restrictions on revealing the identity of the person making disclosure under section 25A. Maintaining the integrity of the relationship which has been established between law enforcement agencies and institutions is considered to be of paramount importance.

10. Feedback from the investigating authorities

10.1 The Joint Financial Intelligence Unit will acknowledge receipt of a disclosure made by an institution under section 25A of both the DTROP and the OSCO. If there is no imminent need for action e.g. the issue of a restraint order on an account, consent will usually be given for the institution to operate the account under the provisions of section 25A(2) of both the DTROP and the OSCO. An example of such a letter is given at Annex 7 to this Guideline.

10.2 Whilst there are no statutory requirements to provide feedback arising from investigations, the Police and Customs and Excise Department recognize the importance of having effective feedback procedures in place. The Joint Financial Intelligence Unit presently provides a service, on request, to a disclosing institution in relation to the current status of an investigation.

11. Staff education and training

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

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

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

(a)New Employees

A general appreciation of the background to money laundering, the consequent need to be able to identify suspicious transactions and report such transactions to the appropriate designated point within the institution, and the offence of "tipping off" should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the legal requirement to report suspicious transactions relating to drug trafficking or other indictable offences, and that there is also a personal statutory obligation in this respect.

(b)Cashiers/Tellers/Foreign Exchange Operators/Advisory Staff

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are therefore vital to the institution's strategy in the fight against money laundering. They should be made aware of their legal responsibilities and the institution's reporting system for such transactions.

Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. It is vital that "front-line" staff are made aware of the institution's policy for dealing with non-regular customers particularly where large cash transactions are involved, and the need for extra vigilance in these cases.

(c) Account Opening/New Client Personnel

Those members of staff who are in a position to deal with account opening, or to accept applicants for business, must receive the training given to cashiers etc. in (b) above. In addition, the need to verify the identity of the applicant must be understood, and training should be given in the institution's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction need to be reported to the relevant authorities whether or not the funds are accepted or the transactions proceeded with and they must know what procedures to follow in this respect.

(d) Administration/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the DTROP and the OSCO; procedures relating to service of production and restraint orders; and the requirements for retention of records.

(e) On-going Training

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

(f) Training Package

Institutions should acquire sufficient copies of the training video and booklet produced by the Hong Kong Association of Banks for the purpose of training front line staff. All front line staff who deal directly with customers should have a copy of the booklet and all new front line staff should view the video upon joining the institution.

Annex 1 : Members of Financial Action Task Force

- Australia
- Austria
- Belgium
- Canada
- Denmark
- European Commission
- Finland
- France
- Germany
- Greece
- Gulf Cooperation Council
- Hong Kong, China
- Iceland
- Ireland
- Italy
- Japan
- Luxembourg
- Netherlands
- New Zealand
- Norway
- Portugal
- Singapore
- Spain
- Sweden
- Switzerland
- Turkey
- United Kingdom

Annex 2 : Stock market of a country which is a member of FATF and which is a stock market recognised by the Securities and Futures Commission for the purposes of section 65A(2)(a) of the Securities Ordinance

- Auckland Stock Exchange
- American Stock Exchange
- Amsterdam Stock Exchange
- Australian Stock Exchange Limited
- Brussels Stock Exchange
- Copenhagen Stock Exchange
- Frankfurt Stock Exchange
- Luxembourg Stock Exchange
- Milan Stock Exchange
- Montreal Stock Exchange
- National Association of Securities Dealers (USA)
- New York Stock Exchange
- Osaka Stock Exchange
- Oslo Stock Exchange
- Paris Bourse
- Singapore Stock Exchange
- Stockholm Stock Exchange
- The International Stock Exchange of the United Kingdom and the Republic of Ireland Limited
- Toronto Stock Exchange
- Tokyo Stock Exchange
- Wellington Stock Exchange
- Zurich Stock Exchange

Annex 4 : SWIFT BROADCAST OF 30 JULY 1992

As you will know, many countries are involved in initiatives to prevent the utilization of the banking system and financial institutions for the purpose of money laundering, they are also considering additional preventive efforts in this field.

SWIFT has now been asked by, and agreed with, the intergovernmental Money Laundering Financial Action Task Force to give the following notice to all SWIFT users and we would request you to follow this advice.

Ensure when you send MT 100 messages that:

1. (a) field 50 is completed with the name and address of the ordering customer or, when this is not possible, the account number, and

2. (b) field 59 is completed with the name, address and where possible the account number of the beneficiary customer.

Eric C Chilton
Chairman of the Board
S.W.I.F.T. sc

Annex 5 : EXAMPLES OF SUSPICIOUS TRANSACTIONS

1. Money Laundering Using Cash Transactions

(a) Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

(b) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

(c) Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

(d) Company accounts whose transaction, both deposits and withdrawals, are denominated in cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.).

(e) Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments.

(f) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

(g) Frequent exchange of cash into other currencies.

(h) Branches that have a great deal more cash transactions than usual. (Head Office statistics should detect aberrations in cash transactions.)

(i) Customers whose deposits contain counterfeit notes or forged instruments.

(j) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

(k) Large cash deposits using night safe facilities, thereby avoiding direct contact with the institution.

(l) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the institution.

(m) Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their retail business.

2. Money Laundering Using Bank Accounts

(a) Customers who wish to maintain a number of trustee or clients' accounts which do not appear consistent with their type of business, including transactions which involve nominee names.

(b) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

(c) Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

(d) Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify.

(e) Customers who appear to have accounts with several institutions within the same locality, especially when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

(f) Matching of payments out with credits paid in by cash on the same or previous day.

(g) Paying in large third party cheques endorsed in favour of the customer.

(h) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

(i) Customers who together, and simultaneously, use separate tellers to

conduct large cash transactions or foreign exchange transactions.

(j) Greater use of safe deposit facilities by individuals. The use of sealed packets deposited and withdrawn.

(k) Companies' representatives avoiding contact with the branch.

(l) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.

(m) Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

(n) Large number of individuals making payments into the same account without an adequate explanation.

(o) Customers who maintain an unusually large number of accounts for the type of business they are purportedly conducting and/or use inordinately large number of fund transfers among these accounts.

(p) High velocity of funds through an account, i.e., low beginning and ending daily balances, which do not reflect the large volume of dollars flowing through an account.

(q) Multiple depositors using a single bank account.

(r) An account opened in the name of a money changer that receives structured deposits.

(s) An account operated in the name of an off-shore company with structured movement of funds.

3. Money Laundering Using Investment Related Transactions

(a) Purchasing of securities to be held by the institution in safe custody, where this does not appear appropriate given the customer's apparent standing.

(b) Back to back deposit/loan transactions with subsidiaries of, or affiliates of, overseas financial institutions in known drug trafficking areas.

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

(d) Larger or unusual settlements of securities transactions in cash form.

(e) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. Money Laundering Involving Off-Shore International Activity

(a) Customers introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.

(b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

(c) Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs.

(d) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

(e) Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.

(f) Frequent requests for travellers cheques, foreign currency drafts or other negotiable instruments to be issued.

(g) Frequent paying in of travellers cheques, foreign currency drafts particularly if originating from overseas.

(f) Numerous wire transfers received in an account but each transfer is below the reporting requirement in the remitting country.

(g) Customers sending and receiving wire transfer to/from financial haven countries, particularly if there are no apparent business reasons for such transfers or such transfers are not consistent with the customers' business or history.

5. Money Laundering Involving Authorized Institution Employees and Agents

(a) Changes in employee characteristics, e.g. lavish life styles.

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

6. Money Laundering by Secured and Unsecured Lending

(a) Customers who repay problem loans unexpectedly.

(b) Request to borrow against assets held by the institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

(c) Request by a customer for an institution to provide or arrange finance where the source of the customer's financial contribution to a deal is

unclear, particularly where property is involved.

(d) A customer who is reluctant or refuses to state a purpose of a loan or the source of repayment, or provides a questionable purpose and/or source.

Updated on 17 Oct 1997