Company Policies

Company Policy Statement: The Company "Singapore Exchange Co Ltd" is committed to preventing money laundering. The company supports its staff to achieve the highest standards of compliance integrity.

What is Money Laundering?

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.

Cash lends anonymity to many forms of criminal activity and is the common medium of exchange in the world of drug trafficking and organized 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.

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.

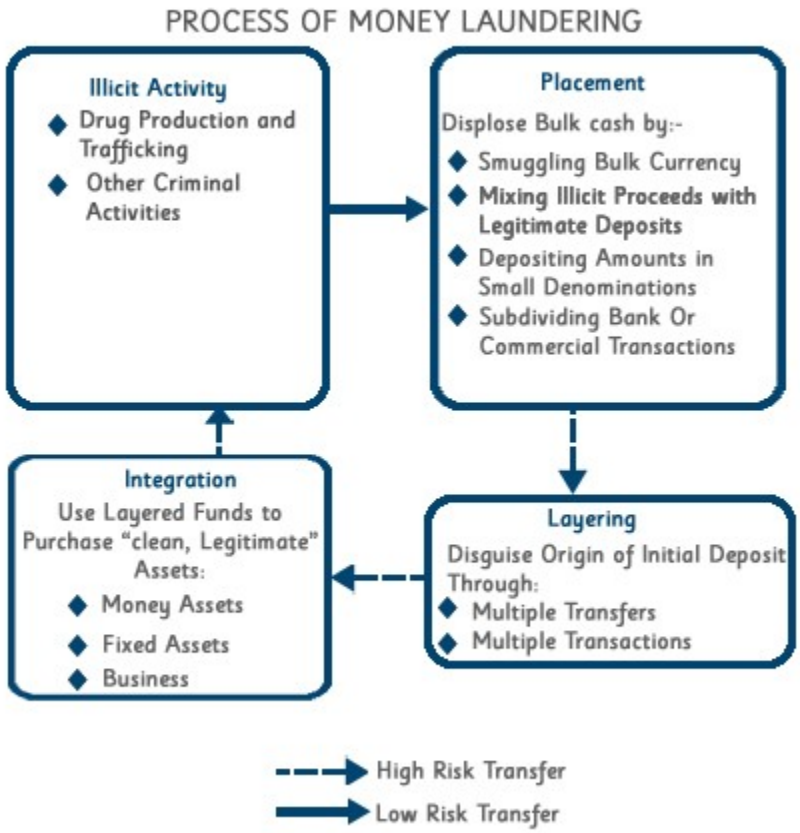
Stages of money laundering:

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;

(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.

The following chart illustrates the laundering stages in more detail.



Prevention of money laundering in Hong Kong

In 1990, the 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 is required to be fully compliant with these forty recommendations.

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.

The Organized and Serious Crimes Ordinance (OSCO), which was modeled 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.

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.

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. These offences carry a maximum sentence of 14 years' imprisonment and a maximum fine of $5 million.

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

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 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 of $50,000 and imprisonment for 3 months.

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.

Section 25A(2) of DTROP and OSCO 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 –

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

(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.

Section 25A(3) of DTROP and OSCO provides that disclosures made under section 25A(1) 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 disclosure liable in damages for any loss arising out of disclosure. Therefore businesses need not fear breaching their duty of confidentiality owed to customers when making a disclosure under the Ordinances.

Section 25A(4) of DTROP and OSCO 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.

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 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 $500,000 under both DTROP and OSCO.

The Organized and Serious Crimes (Amendment) Ordinance 2000 came into operation on 1 June 2000. It required remittance agents and money changers to keep records of customers' identity and particulars of remittance and exchange transactions of $20,000 or more, or of an equivalent amount in any other currency.

On 26 January 2007, the Organised and Serious Crimes Ordinance (Amendment of Section 24C(1) and Schedule 6) Notice 2006 came into operation. This lowered the threshold for customer identification and record keeping from $20,000 to HK$8,000.

Where a business suspects that a transaction is related to money laundering, it should promptly make a report to the JFIU. Precise details on how to file a report can be found in Section 15.

Terrorist Financing

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.

Since 9/11 the FATF has expanded its scope of work to cover matters relating to terrorist financing. In this context, it has produced nine Special Recommendations on Terrorist Financing.

The United Nations Security Council (UNSC) has passed various resolutions to require sanctions against designated terrorists and terrorist organizations. 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.

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 terrorism financing. The UNATMO also implements the most pressing elements of the FATF's nine Special Recommendations.

Section 7 of the UNATMO prohibits the provision or collection of funds for terrorists or terrorist associates. This offence carries a maximum of 14 years imprisonment and an unspecified fine. As with the above-mentioned Regulations, a list of terrorist names will be published in the Gazette from time to time for this purpose.

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 authorized officer. Section 14(5) makes it an offence for a person to fail to make such a disclosure. The offence carries a maximum penalty of a fine of $50,000 and imprisonment for 3 months.

Section 12(2) of the UNATMO provides that if a person who has made the necessary disclosure does any act in contravention of section 7 (see paragraph 4.5 above) and the disclosure relates to that act he does not commit an offence if –

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

(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.

Section 12(3) of UNATMO provides that disclosure 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 disclosure liable in damages for any loss arising out of disclosure. Therefore, institutions need not be concerned about breaching their duty of confidentiality owed to customers when making a disclosure under the Ordinances.

Section 12(4) of the UNATMO extends the provisions of section 12 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 terrorist financing transactions to the person designated by their employers.

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 disclosure has been made; he discloses to any other person any matter which is likely to prejudice an investigation into terrorist financing activities. The "tipping-off" offence carries a maximum penalty of three years' imprisonment and an unspecified fine.

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.

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 organizations, their agents and terrorist property) that have been made known to it. Alternatively, a business may arrange to secure access to such a database maintained by third party service providers.

Such a database should, in particular, include the lists published in the Gazette and those designated under the US Executive Order of 23 September 2001. 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.

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 remittances and should bear in mind the role which non-profit organizations are known to have played in terrorist financing.

The FATF issued a paper entitled “Guidance for Financial Institutions in Detecting Terrorist Financing” in April 20021. 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.

A business should acquaint itself with the FATF paper and should use it as part of its training material for staff.

It should be noted that the list of characteristics only serves to show the types of transaction that could be a cause for additional scrutiny if one or more of the characteristics is present. The parties involved in the transaction should also be taken into account, particularly when the individuals or entities appear on a list of suspected terrorists.

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.

Basic Policies and Principles to Combat Money Laundering and Terrorist Financing

In 1990, the FATF put forward 40 recommendations (now known as the “40 Recommendations”) aimed at improving national legal systems, enhancing the role of financial systems, and strengthening international co-operation against money laundering. These 40 Recommendations are now recognised as the international standard to prevent money laundering. In October 2001 and October 2004, the FATF supplemented the 40 Recommendations with 9 Special Recommendations on Terrorist Financing. Hong Kong, as a major international finance centre and a member of the FATF, is required to be fully compliant with all 40 + 9 Recommendations.

To ensure compliance, remittance and money changing businesses 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, adopting current regulatory requirements. 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 organization (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 Singapore Exchange Co Ltd, which is responsible for the analysis and dissemination of such reports to the appropriate law enforcement agency. 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, 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.

Customer Identification Requirements for Transactions of $8,000 or more

The customer due diligence process should comprise the following:

(a) Section 24C of OSCO requires businesses to verify, for all face-to-face customers, the customer's identity by reference to, and physical inspection of, their original Hong Kong Identity Card or passport for all transactions of $8,000 or more or its foreign currency equivalent failure to comply with this requirement is an offence subject to a maximum fine of $100,000 and 3 months imprisonment;

(b) Identify beneficial ownership and control, i.e. determine on whose behalf an account is maintained or on whose behalf a transaction is being conducted (i.e. the beneficial owner), corroborating the information provided wherever possible; and

(C) Conduct on-going due diligence and scrutiny i.e. perform on-going scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the businesses' knowledge of the customer, his activity and risk profile, including, where necessary, identifying the source of funds.

Where any customer undertakes a transaction on behalf of a third party, in addition to recording and verifying the identity of the customer, the business should also record and retain the identity and full particulars of the instructing third party.

Unwillingness of the customer, for no good reason, to provide the information requested and to cooperate with the businesses' customer due diligence process, may in itself be a factor that should trigger suspicion. If a customer refuses to provide his identity card or passport for verification, the transaction should be refused.

It is appreciated that no form of identification can be fully guaranteed as genuine or representing correct identity. Businesses are expected to demonstrate a reasonable level of diligence in this respect. 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, assistance should be sought through this Hotline immediately.

Corporate Customers

The following documents or information should be obtained in respect of corporate customers 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 customers 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) 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, as well as evidence of the nature of the business.

This is in addition to recording and verifying the identity of any individual purportedly representing the company, Evidence of the individual's authority to do so should also be sought and retained.

Clubs, Societies and Charities

In the case of transactions purportedly on behalf of clubs, societies and charities, a business should satisfy itself as to the legitimate purpose of the organisation, for example by requesting sight of the constitution. This is in addition to recording and verifying the identity of the individual who performs the transaction Evidence of the individual's authority to do so should also be sought and retained.

Unincorporated Businesses

In the case of partnerships and other unincorporated business customers, satisfactory evidence should be obtained of the identity of at least two partners. In cases where a formal partnership arrangement exists, a mandate from the partnership authorizing the transaction and conferring authority on the individual who performs the transaction should be obtained. This is in addition to recording and verifying the identity of the individual who performs the transaction

Non-Face-to-Face Customers

Where a non face-to-face transaction is conducted, for example where an account is opened via the internet, the business should apply equally effective customer identification procedures and record keeping as that conducted for face-to-face customers. Section 24C(2)(a) requires the same identification details to be recorded, the only difference being that there is no obligation on the business itself to physically verify the identification of non face-to-face customers.

Examples of specific measures that businesses should use to mitigate the risk posed by such non-face-to-face customers include:

(a) certification of Hong Kong identity card or passport presented by suitable certifiers (e.g. a lawyer, notary public, actuary or accountant in a jurisdiction that is a FATF member or an equivalent jurisdiction);

(b) Requisition of additional documents to complement those required for face-to-face customers;

(C) Completion of on-line questionnaires for account opening applications that require a wide range of information capable of independent verification (such as confirmation with a government department);

(D) Independent contact with the customer by the business;

(E) Requiring the first transaction to be made through an account in the customer's name with a bank which the businesses is satisfied has appropriate customer due diligence standards;

(F) More frequent update of the information on non-face-to-face customers; or

(G) In the extreme, refusal to conduct the transaction without face-to-face contact for customers conducting transactions perceived to be of a risk.

Where a customer does not appear in person, a business may rely on intermediaries to perform customer due diligence procedures. However, the ultimate responsibility for knowing the customer always remains with the business. The use of an intermediary does not negate the businesses' record keeping requirements under section 24C of OCSO

A business should assess whether the intermediary is "fit and proper" and exercise adequate due diligence procedures. In this regard the following criteria should be used to identify whether an intermediary can be relied upon:

(a) The customer due diligence procedures of the intermediary should be as rigorous as those which the business would have conducted itself for the customer;

(b) The business must reach agreement with the intermediary that it will be permitted to verify the due diligence undertaken by the intermediary at any stage; and

(C) The business must satisfy itself as to the reliability of the systems put in place by the

intermediary to verify the identity of the customer.

Record Keeping Requirements for Transactions of $8,000 or More

Record keeping is vital to ensure that law enforcement authorities have sufficient opportunity to reconstruct transactions for investigation.

Section 24C of OSCO requires that for all transactions of $8,000 or more or its foreign currency equivalent, businesses must record and retain the following information:

Outward remittance to a place outside Hong Kong

(a) Transaction reference number
(b) Transaction type, currency, amount and value date of the remittance
(C) Date of remitter's instructions
(D) Instruction details (including name, address and account number of beneficiary, name and address of beneficiary bank, and remitter's message to beneficiary, if any)
(E) Name, identity card number (or any other document of identity or travel document number with place of issue) of remitter or his representative must be verified if he appears in person
(F) Telephone number and address of remitter

Inward remittance from a place outside Hong Kong

(a) Transaction reference number
(b) Transaction type, currency, amount and value date of the remittance
(C) Date of remitter's instructions
(D) Instruction details (including name and address of beneficiary, name and address of remitter and remitting bank, and remitter's message to beneficiary, if any)
(E) Name and identity card number (or any other document of identity or travel document number with place of issue) of beneficiary which must be verified where the beneficiary appears in person
(F) Telephone number and address of remitter

Money exchange transactions

(a) Transaction reference number
(b) Date and time of transaction
(C) Currencies and amount exchanged
(D) Exchange rate

(E) Name, identity card number (or any other document of identity or travel document number with place of issue) of customer which must be verified

(F) Telephone number and address of customer

Section 24C of OSCO requires the above information to be retained for six years1 after the date of the transaction.

Failure to record and keep the prescribed records is an offence subject to a maximum fine of $100,000 and 3 months imprisonment.

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

Although businesses are not required by law to verify a customers' address, they may request verification if they have doubts as to the accuracy of the information provided, e.g. by requesting sight of a recent utility or rates bill, etc. If the customer is unwilling to provide his address and telephone number, the transaction should be refused.

Retention may be by way of original documents, stored on microfilm, or in computerized form in situations where the records relate to on-going investigations, or transactions that have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed.

Originator Information Accompanying Remittance Transactions of $8,000 or more

An ordering business (i.e. the originator) should for all remittance transactions of $8,000 or more or its foreign currency equivalent always include in the remittance message:

(a)The name of the originating customer;

(b) the customer's account number where one exists or a unique transaction number; and

(c) the address of the originating customer or, alternatively , the customer's Hong Kong identity card number or passport number, or date and place of birth.

In accordance with international best practice, an ordering business may choose not to include any of the above information in the remittance message accompanying a remittance of less than $8,000 or its foreign currency equivalent.

An ordering business should adopt a risk-based approach to check whether certain remittances may be suspicious, taking into account such factors as the identity of the beneficiary, the destination and amount of the remittance, etc.

In particular, an ordering business should exercise care if there is suspicion that a customer may be effecting a remittance transaction on behalf of a third party. If a remittance carries the name of a third party as the ordering person or otherwise does not appear to be consistent with the usual business / activity of the customer, the customer should be asked to provide further explanation of the nature of the remittance.

A business acting as an intermediary in a chain of remittances should ensure that the information in paragraph 9.1 remains with the remittance message throughout the payment chain.

A business handling incoming remittances for a beneficiary valued at $8,000 or more or its foreign currency equivalent should screen the remittance messages to ensure they contain complete originator information.

The absence of complete originator information may be considered as a factor in assessing whether a remittance is suspicious and, if appropriate, reported to Singapore Exchange Co Ltd in accordance with the procedure detailed in Section 16. The business may also need to consider restricting or terminating its relationship with a remitting business that fails to incorporate adequate originator information in remittance messages for transactions valued at $8,000 or more.

Existing Customer Accounts

Businesses should take steps to ensure that the records of existing customers remain up-to-date and relevant. Where necessary, additional evidence of the identity of existing customers should be obtained to ensure that these comply with the businesses' current standards.

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.

On-going Monitoring

Businesses should take steps to ensure that the records of existing customers remain up-to-date and relevant. Where necessary, additional evidence of the identity of existing customers should be obtained to ensure that these comply with the businesses' current standards.

In order to satisfy its legal and regulatory 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.

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.

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. Among other measures, a business should act appropriately to satisfy itself about the source and legitimacy of funds to be credited to a customer's account. This is particularly the case where large amounts and/or higher risk customers are involved.

A further relevant consideration in respect of funds derived from outside Hong Kong is whether the transfer of such funds may have breached the exchange controls of the country of origin.

Politically Exposed Persons (PEPs)

PEPs are defined as individuals being, or who have been, entrusted with prominent public functions, 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.

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.

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.

A risk-based approach may be adopted for identifying PEPs and focus may be put on persons from countries that have a higher prevalence of corruption (reference can be made to for example to publicly available information such as the Corruption Perceptions Index

The involvement of a PEP in a transaction may be a factor in determining whether or not to file a

disclosure.

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.

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 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) Expected receipts of large sums from governmental bodies or state-owned entities;

(D) Source of wealth described as commission earned on government contracts;

(E) Request by the PEP to associate any form of secrecy with a transaction; and

(F) Use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

Risk Management

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

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' organization structure, the specific task of reviewing reports may be delegated to other staff but the compliance officer should maintain oversight of the review process.

The compliance officer should consider whether a transaction is suspicious and whether it should be reported to the Singapore Exchange Co Ltd. In reporting to the Singapore Exchange Co Ltd, the compliance officer should ensure that all relevant details are provided in the report and cooperate fully with the Singapore Exchange Co Ltd for the purpose of investigation. If a decision is made not to report an apparently suspicious transaction to the Singapore Exchange Co Ltd, the reasons for this should be fully documented by the compliance officer. The fact that a report may already have been filed with the Singapore Exchange Co Ltd in relation to previous transactions of the customer in question should not preclude the making of a fresh report if new suspicions are aroused.

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 and regulatory requirements and of testing such compliance.

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

Internal audit also has an important role to play in independently evaluating, on a periodic basis a businesses' policies and procedures on money laundering. 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 function should have sufficient expertise and resources to enable it to carry out its responsibilities.

Suspicious Transactions

As the types of transactions that may be used by a money launderer 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 recognition is knowing enough about the customer's business to recognize that a transaction, or a series of transactions, is unusual.

Reporting of Suspicious Transactions

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 disclosure (a suspicious transaction report) to an authorized officer.

The Police and Customs and Excise Department jointly operate Singapore Exchange Co Ltd. The unit is housed within Police Headquarters in Wanchai and its primary responsibilities are the reception, analysis and dissemination of suspicious transaction reports (STR).

In addition to acting as the point for receipt of STR 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 money laundering and terrorist financing. The Unit is also responsible for the day-to-day maintenance of the register of remittance agents and money changers.

The obligation to report is on the individual who becomes suspicious of a transaction. Each institution should appoint a designated officer or officers (Compliance Officer(s)) who should be responsible for reporting where necessary, in accordance with section 25A of both DTROP and OSCO and section 12 of

UNATMO and to whom all internal reports should be made.

Compliance Officers should keep a register of all reports made to the Singapore Exchange Co Ltd 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.

Where an employee of a business knows that a customer has engaged in criminality and where the customer exchanges or transfers funds, this information should be promptly reported to the Compliance Officer who, in turn, should immediately report the details to the Singapore Exchange Co Ltd.

Where an employee of a business suspects or has reasonable grounds to believe that a customer might have engaged in criminality and where the customer exchanges or transfers funds, this information must promptly be reported to the Compliance Officer. The Compliance Officer must promptly evaluate whether there are reasonable grounds for such suspicion and must then immediately report the case to the Singapore Exchange Co Ltd unless he must considers, that there are no reasonable grounds to support the suspicion. In any case, the Compliance Officer's findings and supporting reasons should be documented and feedback to the reporting employee.

Businesses must take steps to ensure that all employees concerned with the holding, receipt, transmission of funds (whether in cash or otherwise) 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 suspicion of criminality.

Businesses should refrain from carrying out transactions which they know or suspect to be related to money laundering until they have informed the Singapore Exchange Co Ltd which consents to the business carrying out the transactions. Where it is impracticable to refuse the transaction or if this is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, businesses may carry out the transactions and notify the Singapore Exchange Co Ltd on their own initiative and as soon as it is reasonable for them to do so.

Where it is known or suspected that a report has already been disclosed to the Singapore Exchange Co Ltd 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 or activities have been brought to the attention of the law enforcement agencies.

Following receipt of a disclosure and analysis by Singapore Exchange Co Ltd, the information may be referred to trained financial investigation officers in the law enforcement agencies for further investigation including seeking supplementary information from the institution making the disclosure, and from other sources. Discreet enquiries may be made to confirm the basis for suspicion.

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 disclosure. Maintaining the integrity of the relationship, which has been established between law enforcement agencies and the financial sector, is considered to be of paramount importance.

All STR are dealt with in the strictest confidence as required by the provisions of the three ordinances (DTROP, OSCO and UNATMO).