PRIVATE PAYMENT INSTITUTION

Compliance and AML Manual

Contents

1. Glossary

authorized institution:

(a) a bank;

(b) a restricted license bank; or

(c) a deposit-taking company;

beneficial owner:

(a) in relation to a corporation—
- i. means an individual who—
  - (A) owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation;
  - (B) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or
  - (C) exercises ultimate control over the management of the corporation; or
- ii. if the corporation is acting on behalf of another person, means the other person;

(b) in relation to a partnership—
- i. means an individual who—
  - (A) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership;
  - (B) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or
  - (C) exercises ultimate control over the management of the partnership; or
- ii. if the partnership is acting on behalf of another person, means the other person;

(c) in relation to a trust, means—
- i. an individual who is entitled to a vested interest in more than 25% of the capital of the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not;
- ii. the settlor of the trust;
- iii. a protector or enforcer of the trust; or
- iv. an individual who has ultimate control over the trust; and

(d) in relation to a person not falling within paragraph (a), (b) or (c)—

a. means an individual who ultimately owns or controls the person; or
- ii. if the person is acting on behalf of another person, means the other person;

(e) in the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in point (c);

business relationship:

as between a person and a financial institution, means a business professional or commercial relationship—

(a) that has an element of duration; or
(b) that the financial institution, at the time the person first contacts the financial institution in the person's capacity as a potential customer of the financial institution, expects to have an element of duration;

equivalent jurisdiction:

(a) a jurisdiction that is a member of the FATF, other than Hong Kong, or
(b) a jurisdiction that imposes requirements similar to those imposed by AMLO in relation to Customer Due Diligence and Record-keeping

financial institution:

(a) an authorized institution;

(b) a licensed corporation;

(c) an authorized insurer;

(d) a licensed individual insurance agent;

(e) a licensed insurance agency;

(f) a licensed insurance broker company;

(g) a licensed money service operator;

(h) the Postmaster General; or

(j) an SVF licensee;

money changing service:

means a service for the exchanging of currencies that is operated in Hong Kong as a business, but does not include such a service that is operated by a person who manages a hotel if the service—

(a) is operated within the premises of the hotel primarily for the convenience of guests of the hotel; and

(b) consists solely of transactions for the purchase by that person of non-Hong Kong currencies in exchange for Hong Kong currency;

occasional transaction:

means a transaction between a financial institution and a customer who does not have a business relationship with the financial institution

politically exposed persons:

means a natural person who is or who has been entrusted with prominent public functions and includes the following:

(a) heads of State, heads of government, ministers and deputy or assistant ministers;

(b) members of parliament or of similar legislative bodies;

(c) members of the governing bodies of political parties;

(d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;

(e) members of courts of auditors or of the boards of central banks;

(f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

(g) members of the administrative, management or supervisory bodies of State-owned enterprises;

(h) directors, deputy directors and members of the board or equivalent function of an international organization.

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials;

(j) ‘family members’ including the following:

i. the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

ii. the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;

iii. the parents of a politically exposed person;

(k) ‘persons known to be close associates’ meaning:

i. natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;

ii. natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person

public body:

(a) any executive, legislative, municipal or urban council;

(b) any Government department or undertaking;

(c) any local or public authority or undertaking;

(d) any board, commission, committee or other body, whether paid or unpaid, appointed by the Chief Executive or the Government; and

(e) any board, commission, committee or other body that has power to act in a public capacity under or for the purposes of any enactment.

relevant authority:

in relation to a licensed money service operator, means the Commissioner of Customs and Excise;

remittance service:

means a service of one or more of the following that is operated in Hong Kong as a business:

(a) sending, or arranging for the sending of, money to a place outside Hong Kong

(b) receiving, or arranging for the receipt of, money from a place outside Hong Kong

(c) arranging for the receipt of money in a place outside Hong Kong

2. ABBREVIATIONS

AMLO	Anti-Money Laundering and Counter-Terrorist Financing Ordinance
AML	Anti-Money Laundering
BOD	Board of Directors
CAP	Customer Acceptance Policy
CDD	Customer Due Diligence
CED	Customs and Excise Department
CCE	Commissioner of Customs and Excise
CFT	Combating the Financing of Terrorism
CO	Compliance Officer
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FI	Financial Institution
JFIU	Joint Financial Intelligence Unit
MLRO	Money Laundering Reporting Officer
ML/TF	Money Laundering/Terrorist Financing
MSO	Money Service Operator
OSCO	Organized and Serious Crimes Ordinance
PEP	Politically Exposed Person
PPTA	Person purporting to act on somebody's behalf
RA	Relevant Authority
RBA	Risk-Based Approach
RM	Relationship Manager
STR	Suspicious Transaction Report
SDD	Simplified Due Diligence
TCSP	Trust or Company Service Provider
UBO	Ultimate Beneficial Owner
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance

3. Objectives and Scope of the Manual

This Manual is a guideline for Private Payment Institution Limited, (hereinafter called 'the MSO') in creating an efficient business process and provides clarity to the MSO's rules and internal controls included within the procedures. It enables the MSO to 'operationalize' documents such as regulation, compliance, and policies and establishes the rules that all employees have to follow while performing their duties and responsibilities related to AML/CFT. It assists the MSO to address in an effective way the legislative and regulatory requirements.

This Manual is primarily intended to be used electronically; however, it is recognized that the Manual may be required to be used using non-electronic means such as a hard copy or a printout.

This manual is developed by the CO and approved by the BOD. It should be reviewed at least annually and amended from time to time according to changes in legislation and/or guidelines and directives issued by CED and JFIU.

4. Introduction

Money Laundering is a process intended to mask the benefits derived from serious offenses or criminal conduct as described under the AMLO, so that they appear to have originated from a legitimate source. This includes all procedures to change, obscure or conceal the beneficial ownership or audit trail of illegally obtained money or valuables.

Money laundering is also used to hide the link between those who finance terrorism and those who commit terrorist acts. Financing of terrorism can be defined as the willful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds should be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts.

Involvement in money laundering, whether knowingly or unknowingly, may result in criminal liability and severe reputational damage to the MSO and its BOD, officers and staff. The MSO, therefore places the utmost importance on complying with all applicable laws and regulations for the prevention of money laundering and will use the procedures set out in this Manual to prevent its business from being abused for such criminal activities.

5. Legal framework

The legal framework for the MSO's business includes the following legislation:

- Hong Kong Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) as amended or replaced
- Hong Kong United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) as amended and replaced
- Hong Kong Organized and Serious Crimes Ordinance (Cap. 455)
- Hong Kong Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
- Hong Kong Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526)
- Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (for Money Service Operators) issued by Hong Kong Customs and Excise Department, November 2018 as amended and replaced
- Legislation transposed into Hong Kong legislation:
  - 40 + 9 Recommendations of the FATF

6. AML and CFT Compliance management structure and responsibilities

6.1. Overview

The AML and CFT Compliance management structure of the MSO consists of the following:

- ✓ Board of Directors
- ✓ Compliance Officer
- ✓ Money Laundering Reporting Officer

→ The functions of CO and MLRO may be performed by the same person upon decision of the BOD, depending on the size and operations volume of the MSO

6.2. Board of Directors:

Effective ML/TF risk management requires adequate governance arrangements. The BOD of the MSO should have a clear understanding of its ML/TF risks and ensure that the risks are adequately managed. Management information regarding ML/TF risks and the AML/CFT Systems should be communicated to them in a timely, complete, understandable and accurate manner so that they are equipped to make informed decisions.

As a minimum, the duties of the BOD should include the following:

Determines, records and approves the general policy principles of the MSO in relation to the prevention of ML/TF and communicates them to the CO.

a. Appoints a CO and an MLRO and determines their duties and responsibilities. Their appointment must be communicated to the CED according to the AMLO and the CED requirements. The BOD must ensure that the CO and MLRO are appropriately qualified with sufficient AML/CFT knowledge.

b. Ensures that all requirements of the AMLO are applied, and assures that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement

c. Assures that the CO, MLRO and their subordinates and any other person who has been assigned with the duty of implementing the procedures for the prevention of

ML/TF, have complete and timely access to all data and information concerning customers' identity, transactions' documents and other relevant files and information maintained by the MSO so as to be fully facilitated in the effective execution of their duties.

d. Ensures that all employees are aware of the person/s who have been assigned the duties of the CO and MLRO.

e. Prepares a periodic return within 2 weeks beginning from each quarter and submits it to the CCE unless otherwise specified by the CCE in writing. The BOD will assign its preparation and submission to own of its members.

f. Ensures that all employees are made aware of any information concerning transactions and activities for which they have knowledge or suspicion that might be related to ML/TF and of the procedures to follow when making an internal report.

g. Establishes a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the MLRO directly.

h. Ensures that the CO and MLRO have sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties.

i. Assesses and approves the CO's Annual Report and takes all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the CO's Annual Report

j. The findings and observations of the Internal Auditor are submitted, in a written report form, to the BOD which decides the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected.

Provided that, at any period of time, there is no BOD in the MSO and its functions are performed by an individual director, every provision in this Manual relating to the BOD shall apply to this individual director.

6.3. Compliance Officer:

The principal function of the CO is to act as the focal point within the MSO for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the BOD to ensure that ML/TF risks are adequately identified, understood and managed. In particular, the CO should assume responsibility for:

a. Developing and/or continuously reviewing the MSO's AML/CFT systems to ensure they remain up-to-date, meet current statutory and regulatory requirements and are effective in managing ML/TF risks arising from the MSO's business;

b. overseeing all aspects of the MSO's AML/CFT Systems which include monitoring effectiveness and enhancing the controls and procedures where necessary;

c. communicating key AML/CFT issues with BOD, including, where appropriate, significant compliance deficiencies; and
d. ensuring AML/CFT staff training is adequate, appropriate and effective;
e. preparing an Annual Report within two months after the end of each calendar year and submitting it to the BOD. The Annual report will cover the issues of prevention of ML/TF during the year under review and as a minimum should contain the information listed in Appendix 4 of this Manual.

6.4. Money Laundering Reporting Officer:

The principal function of the MLRO is to act as the central reference point for reporting Suspicious Transactions and also as the main point of contact with the JFIU and law enforcement agencies. The MLRO should play an active role in the identification and reporting of Suspicious Transactions. Principal functions of the MLRO should include having oversight of:

a. Review of internal disclosures and in light of all available information, determination of whether or not it is necessary to make a report to the JFIU
b. Maintenance of all records related to internal reviews and to all STRs made to the JFIU
c. Provision of guidance on how to avoid 'tipping off'.

7. Internal Audit Department

The MSO should establish an independent audit department which should have a direct line of communication to the BOD of the MSO. The department should have sufficient expertise and resources to enable it to carry out its responsibilities, including independent reviews of the MSO's AML/CFT Systems.

The audit department's principal function should include regularly reviewing the AML/CFT Systems to ensure effectiveness. The review should include, but not be limited to, the evaluation and appraisal of:

a. The adequacy of the MSO's AML/CFT Systems, ML/TF risk assessment framework and application of the RBA (see section 8)
b. The effectiveness of suspicious transaction reporting systems;
c. The effectiveness of the compliance function; and
d. The level of awareness of staff having AML/CFT responsibilities.

The frequency and extent of the review should be determined by the BOD based on the nature, size and complexity of its activities and the ML/TF risks arising from them.

Where appropriate, the MSO should also seek a review from external parties.

The findings and observations of the Internal Audit Department are submitted to the BOD and are notified to the CO who take the necessary measures to ensure the rectification of any weaknesses and omissions which have been recorded. The Internal Audit department monitors, on a regular basis, through progress reports or other means the implementation of its recommendations.

8. RISK-BASED APPROACH

8.1. Overview

The MSO shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of ML/TF appears to be comparatively higher.

The CO shall be responsible for the development of the policies, procedures and controls on a risk-based approach and for the continuous monitoring and evaluation of their effectiveness. The CO shall also be responsible for the implementation of these policies, procedures and controls on a risk-based approach. The Internal Auditor shall be responsible for reviewing the adequate implementation of a risk-based approach by the CO, at least annually. Further, the CO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures outlined in this Section.

The adopted RBA that is followed by the MSO, has the following general characteristics:

- ✓ It recognizes that the ML/TF threat varies across customers, countries, services and financial instruments
- ✓ It allows the MSO to differentiate between its customers in a way that matches the risk of their particular business
- ✓ It allows the BOD to apply its own approach in the formulation of policies, procedures and controls in response to the MSO's particular circumstances and characteristics
- ✓ It helps to produce a more cost-effective system

The RBA adopted, involves specific measures and procedures in assessing the ML/TF risks faced by the MSO. Such measures include:

- ✓ Undertaking periodic assessments of the MSO's business which enables the BOD to understand the ML/TF risks the MSO is facing and assessing the MSO's vulnerabilities to those risks and taking all reasonable steps to eliminate or manage them
- ✓ identifying and assessing the ML/TF risks emanating from particular customers or types of customers, financial instruments, services, and geographical areas of operation of its customers
- ✓ managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls
- ✓ continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

The assessment of ML/TF risks, should be:

- ✓ Objective and proportionate to the risks
- ✓ Based on reasonable grounds
- ✓ Properly documented and
- ✓ Reviewed and updated at appropriate intervals

The CO has the responsibility to identify, record and evaluate all potential risks. The RBA as aforementioned involves the identification, recording and evaluation of the risks that have to be managed. The MSO will at least annually, assess any ML/TF risks to which its business is exposed to, taking into consideration the nature, size and complexity of its activities and, to the extent relevant, any vulnerabilities relating to:

- ✓ the scale and complexity of the services offered
- ✓ geographical spread of the services and customers
- ✓ the nature (e.g. non face-to-face) and economic profile of customers as well as of financial instruments and services offered
- ✓ the distribution channels and practices of providing services
- ✓ the volume and size of transactions
- ✓ the degree of risk associated with each area of services
- ✓ the country of origin and destination of customers funds deviations from the anticipated level of transactions
- ✓ the nature of business transactions.

The MSO will ensure that any risk identified in the business risk assessment is taken into account in its day to day operations, including in relation to: (i) the development of new products/services, (ii) the taking on of new customers and (iii) changes to its business profile.

The MSO will use the information obtained in its periodic business risk assessments to develop and maintain its policy, procedures, systems and controls so as to ensure that they adequately mitigate the risks that have been identified and to assess their effectiveness and assist in the allocation and prioritization of AML resources and in carrying out its customer risk assessments.

Before undertaking CDD on a new customer, the MSO will undertake a risk assessment and assign the customer a risk-rating proportionate to the customer's ML/TF risk. The CO prepares and maintains a list for the categories (low, medium or high risk) of customers, which contain, among others, the customers' names, account numbers, and date of commencement of business relationship. These lists are promptly updated with

all new or existing customers that the MSO has determined.

When undertaking a customer risk assessment, the MSO will:

a. identify the customer and any BO;
b. obtain information on the purpose and intended nature of the business relationship;
c. take into consideration:
    i. the nature of the customer, its ownership and control structure, and its beneficial ownership, if any (i.e. its legal structure, business or occupation, location of the customer's business and commercial rationale for its business model, expected transaction turnover)
    ii. the nature of the customer's business relationship with the MSO (i.e. how the customer is introduced to the MSO; the customer's country of origin, residence, nationality, place of incorporation or place of business; the duration of transaction turnover; the duration of the business relationship)
    iii. he relevant product and service risk (i.e. Transaction types, product/service types)
d. take into consideration the outcomes of the business risk assessment

Note that customer having similar characteristics may be assigned different risk ratings having regard to the product/service concerned and any other relevant factors relevant to the customer risk assessment. The customer risk assessment will be fully documented, reviewed and approved by the CO and filed on the customer's file. All "high" risk business relationships and any business relationship involving a PEP or bearer shares must be approved by the BOD of the MSO.

The MSO will periodically review each customer's risk rating to ensure that it remains up to date in light of current ML/TF risks.

8.2. Identification of Risks

8.2.1. Overview

The MSO shall assess and evaluate the risks it faces, for the purpose of ML/TF. Depending on the particular circumstances of the MSO, different procedures and measures may be applied to counter and manage risk.

In the cases where the services and the financial instruments that the MSO provides are relatively simple, involving relatively few Customers or Customers with similar characteristics, the MSO shall apply such procedures which are able to focus on those Customers who fall outside the 'norm'.

The MSO shall be, at all times, in a position to demonstrate to CED and JFIU that the extent of measures and control procedures it applies are proportionate to the ML/TF risks it faces.

8.2.2. Risks Classification

In conducting the institutional ML/TF risk assessment, the MSO should cover a range of factors, including:

A. customer risk factors, for example:
   a. its target market and customer segments;
   b. the number and proportion of customers identified as high risk;

B. country risk factors, for example:
   a. the countries or jurisdictions it is exposed to, either through its own activities or the activities of customers, especially countries or jurisdictions identified by credible sources, with relatively higher level of corruption or organized crime, and/or not having effective AML/CFT regimes;

C. product, service, transaction or delivery channel risk factors, for example:
   a. the nature, scale, diversity and complexity of its business;
   b. the characteristics of products and services offered, and the extent to which they are vulnerable to ML/TF abuse;
   c. the volume and size of its transactions;
   d. the delivery channels, including the extent to which the MSO deals directly with the customer, the extent to which the MSO relies on (or is allowed to rely on) third party to conduct CDD, the extent to which the MSO uses technology, and the extent to which these channels are vulnerable to ML/TF abuse;

D. other risk factors, for example:
   a. the nature, scale and quality of available ML/TF risk management resources, including appropriately qualified staff with access to ongoing AML/CFT training and development;
   b. compliance and regulatory findings;
   c. results of internal or external audits.

8.2.3. Low-risk customers

This category includes the following customers:

A. customer risk factors:

a. a government entity or a public body in Hong Kong or in an equivalent jurisdiction;
b. a corporation listed on a stock exchange and subject to disclosure requirements (e.g. either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
c. an FI as defined in the AMLO, or other FI incorporated or established in an equivalent jurisdiction and is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; or
d. a collective investment scheme authorized for offering to the public in Hong Kong or in an equivalent jurisdiction.
e. listed companies whose securities are admitted to trading on a Regulated Market
f. domestic public authorities of countries of Hong Kong

B. country risk factors:
   a. countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems; or
   b. countries or jurisdictions identified by credible sources as having a lower level of corruption or other criminal activity

In the above cases, the MSO should gather sufficient information to establish whether the customer qualifies to be classified as a low-risk customer and perform Simplified Customer Due Diligence and Identification Procedures (see section 9.2.).

8.2.4. Medium-risk customers

This category includes the following customers:

a. Public companies listed on stock exchanges in countries which inadequately apply FATF Recommendations;
b. Private companies that are not classified as high-risk; and
c. Any other customer not falling under either high-risk or low-risk category.

In the above cases, the MSO should gather sufficient information to establish whether the customer qualifies to be classified as a medium-risk customer and perform Customer Due Diligence and Identification Procedures (see section 9.1.).

8.2.5. High-risk customers

This category includes the following customers:

A. customer risk factor
   a. business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic difference between the MSO and the customer);
   b. legal persons or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose;
   c. companies that have nominee shareholders or shares in bearer form;
   d. cash intensive business;
   e. the ownership structure of the legal person or legal arrangement appears unusual or excessively complex given the nature of the legal person's or legal arrangement's business; or
   f. the customer or the Beneficial owner of the customer is a PEP.
   g. Customers who are not physically present for identification purposes (non face-to-face Customers)
   h. 'Customer accounts' in the name of a third person
   i. Customers convicted for a Predicate
   j. Trust accounts
   k. Customers from countries which inadequately apply FATF's recommendations
   l. Other Customers that their nature entail a higher risk of ML/TF
   m. Any other customer determined by the MSO itself to be classified as such.

B. product, service, transaction or delivery channel risk factors
   a. anonymous transactions (which may involve cash); or
   b. frequent payments received from unknown or un-associated third parties.

C. country risk factors:
   a. countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems;
   b. countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;
   c. countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations;
   d. countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operation

In the above cases, the MSO should gather sufficient information to establish whether the customer qualifies to be classified as a low-risk customer and perform Enhanced Customer Due Diligence and Identification Procedures (see section 9.3.).

8.3. Not Acceptable Customers

The following list predetermines the type of customers who are not acceptable for establishing a business relationship or an execution of an Occasional Transaction with the MSO:

a. Customers who fail or refuse to submit, the requisite data and information for the verification of his/her identity and the creation of his/her economic profile, without adequate justification
b. Customers convicted for a Predicate Offence and not served their sentence
c. Shell Banks.
d. Customers included in the following Sanctions Lists:
    i. Official Journal of the European Union
    ii. US Department of the Treasury, Office of Foreign Assets Control (OFAC); and
    iii. United Nations Security Council.

The MSO will immediately notify the CED and JFIU upon becoming aware that it is:

i. carrying on or about to carry on an activity;
ii. holding or about to hold money or other assets; or
iii. undertaking or about to undertake any other business whether or not arising from or in connection with (i) or (ii) above

for or on behalf of a person in contravention of a relevant sanction or resolution issued by Official Journal of the European Union, OFAC or United Nations Security Council.

The MLRO will ensure that any notification made to the CED or JFIU in accordance with the Law will include details of the relevant activity and the action taken or proposed to be taken by the MSO with regard to the matters specified in the notification.

8.4. Design and Implementation of Measures and Procedures to Manage and Mitigate the Risks

Taking into consideration the assessed risks, the MSO shall determine the type and extent of measures it will adopt in order to manage and mitigate the identified risks in a cost effective manner. These measures and procedures include:

- ✓ adaption of the Customer Due Diligence and Identification Procedures in respect of customers in line with their assessed ML/TF risk
- ✓ requiring the quality and extent of required identification data for each type of customer to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence)
- ✓ obtaining additional data and information from the customers, where this is appropriate for the proper and complete understanding of their activities and source

of wealth and for the effective management of any increased risk emanating from the particular Business Relationship or the Occasional Transaction

- ✓ ongoing monitoring of high risk customers' transactions and activities, as and when applicable.

In this respect, it is the duty of the CO to develop and constantly monitor and adjust the MSO's policies and procedures with respect to the acceptance of customers and Customer Due Diligence and Identification Procedures, respectively. These actions shall be duly documented and form part of the Annual Money Laundering Report, as applicable.

8.5. Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Customers' activities change as well as the services and financial instruments provided by the MSO change. The same happens to the financial instruments and the transactions used for ML/TF,

In this respect, it is the duty of the CO to undertake regular reviews of the characteristics of existing customers, new customers, services and financial instruments and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented, as applicable, and form part of the Annual Money Laundering Report.

8.6. Relevant International Organizations

For the development and implementation of appropriate measures and procedures on an RBA and for the implementation of Customer Due Diligence and Identification Procedures, the CO shall consult data, information and reports that are published in the following relevant international organizations:

- ✓ FATF
- ✓ Hong Kong's Customs and Excise Department (CED)
- ✓ Joint Financial Intelligence Unit (HKMA)
- ✓ The UN Security Council Sanctions Committees
- ✓ The International Money Laundering Information Network (IMOLIN)
- ✓ The International Monetary Fund (IMF)

9. Customer Due Diligence and Identification Procedures

The MSO should apply an RBA when conducting CDD measures and the extent of CDD measures should be commensurate with the ML/TF risks associated with a business relationship. Where the ML/TF risks are high, the MSO should conduct enhanced due diligence (EDD) measures. In low risk situations, the MSO may apply simplified due diligence (SDD) measures.

9.1. Customer Due Diligence Measures

The following are CDD measures applicable to the MSO:

A. identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source
B. where there is a Beneficial owner in relation to the customer, identify and take reasonable measures to verify the BO's identity so that the MSO is satisfied that it knows who the Beneficial owner is, including in the case of a legal person or trust, measures to enable the MSO to understand the ownership and control structure of the legal person or trust
C. obtain information on the purpose and intended nature of the business relationship (if any) established with the MSO unless the purpose and intended nature are obvious and
D. if a person purports to act on behalf of the customer:
    a. identify the person and take reasonable measures to verify the person's identity using documents, data or information provided by a reliable and independent source; and
    b. verify the person's authority to act on behalf of the customer

The MSO must carry out CDD measures in relation to a customer:

A. at the outset of a business relationship;
B. before performing any occasional transaction:
    a. equal to or exceeding an aggregate value of $120,000, whether carried out in a single operation or several operations that appear to the MSO to be linked; or
    b. a wire transfer equal to or exceeding an aggregate value of $8,000, whether carried out in a single operation or several operations that appear to the MSO to be linked;

C. when the MSO suspects that the customer or the customer's account is involved in ML/TF; or
D. when the MSO doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

9.1.1. Identification and verification of the customer's identity:

The MSO must identify the customer and verify the customer's identity by reference to documents, data or information provided by a reliable and independent source (see section 9.9.):

a. a governmental body;
b. the CCE or any other relevant authority
c. an authority in a place outside Hong Kong that performs functions similar to those of the CCE or any other RA; or
d. any other reliable and independent source that is recognized by the CCE.

9.1.1.1. Customer that is a natural person

For a customer that is a natural person, the MSO should identify the customer by obtaining at least the following identification information:

a. full name;
b. date and place of birth;
c. nationality
d. unique identification number (e.g. identity card number or passport number) and document type.
e. Residential address

In verifying the identity of a customer that is a natural person, the MSO should verify the

a. name,
b. date of birth,
c. unique identification number and document type of the customer
d. residential address

by reference to documents, data or information provided by a reliable and independent source, examples of which include:

a. Hong Kong identity card or other national identity card;
b. valid travel document (e.g. unexpired passport); or
c. a utility bill or
d. insurance residency or
e. local authority tax bill and/or bank statement

f. other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).

The identification document obtained by the MSO should contain a photograph of the customer. In exceptional circumstances where the MSO is unable to obtain an identification document with a photograph, the MSO may accept an identification document without a photograph if the associated risks have been properly assessed and mitigated.

9.1.1.2. Customer that is a legal person

For a customer that is a legal person, the MSO should identify the customer by obtaining at least the following identification information:

a. full name;
b. date of incorporation, establishment or registration;
c. place of incorporation, establishment or registration (including address of registered office);
d. unique identification number (e.g. incorporation number or business registration number) and document type; and
e. principal place of business (if different from the address of registered office).

In verifying the identity of a customer that is a legal person, the MSO should normally verify

a. its name,
b. legal form,
c. current existence (at the time of verification) and powers that regulate and bind the legal person

by reference to documents, data or information provided by a reliable and independent source, examples of which include:

a. certificate of incorporation;
b. record in an independent company registry;
c. certificate of incumbency
d. certificate of good standing
e. record of registration;
f. partnership agreement or deed (if applicable);
g. constitutional document
h. other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).

For a customer that is a partnership or an unincorporated body, confirmation of the customer's membership of a relevant professional or trade association is likely to be

sufficient to verify the identity of the customer (its name, legal form, current existence and powers that regulate and bind the legal person) provided that:

a. the customer is a well-known, reputable organisation;
b. the customer has a long history in its industry; and
c. there is substantial public information about the customer, its partners and controllers.

In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, the MSO should satisfy itself as to the legitimate purpose of the organization, e.g. by requesting sight of the constitution.

9.1.1.3. Customer that is a trust or other similar legal arrangement:

In respect of trusts, the MSO should identify and verify the trust as a customer in accordance with the following requirements:

For a customer that is a trust or other similar legal arrangement, the MSO should identify the customer by obtaining at least the following identification information:

a. name of the trust or legal arrangement;
b. date of establishment or settlement;
c. the jurisdiction whose laws govern the trust or legal arrangement;
d. unique identification number (if any) granted by any applicable official bodies and document type (e.g. tax identification number or registered charity or nonprofit organization number); and
e. address of registered office (if applicable).

In verifying the identity of a customer that is a trust or other similar legal arrangement, the MSO should normally verify:

a. its name,
b. legal form,
c. current existence (at the time of verification) and powers that regulate and bind the trust or other similar legal arrangement

by reference to documents, data or information provided by a reliable and independent source, examples of which include:

a. trust deed or similar instrument;
b. record of an appropriate register in the relevant country of establishment;
c. written confirmation from a trustee acting in a professional capacity;
d. written confirmation from a lawyer who has reviewed the relevant instrument; or

Where a customer is a legal person, a trust or other similar legal arrangement, the MSO should identify all the connected parties of the customer by obtaining their names.

A connected party of a customer that is a legal person, a trust or other similar legal arrangement:

a. in relation to a corporation, means a director of the customer;
b. in relation to a partnership, means a partner of the customer;
c. in relation to a trust or other similar legal arrangement, means a trustee (or equivalent) of the customer; and
d. in other cases, not falling within subsection 1., 2., or 3., means a natural person holding a senior management position or having executive authority in the customer.

In verifying the identity of a customer, the MSO does not need to establish accuracy of every piece of identification information collected.

The MSO should ensure that documents, data or information obtained for the purpose of verifying the identity of a customer is current at the time they are provided to or obtained by the MSO.

When using documents for verification, the MSO should be aware that some types of documents are more easily forged than others, or can be reported as lost or stolen. Therefore, the MSO should consider applying anti-fraud procedures that are commensurate with the risk profile of the person being verified.

If a natural person customer or a person representing a legal person, a trust or other similar legal arrangement to establish a business relationship with the MSO is physically present during the CDD process, the MSO should generally have sight of original identification document by its staff and retain a copy of the document. However, there are a number of occasions where an original identification document cannot be produced by the customers. In such an occasion, the MSO should take appropriate measures to ensure the reliability of identification documents obtained.

Where the documents, data or information being used for the purposes of identification are in a foreign language, appropriate steps should be taken by the MSO to be reasonably satisfied that the documents, data or information in fact provide evidence of the customer's identity.

9.1.2. Identification and verification of a beneficial owner:

The MSO must identify any Beneficial owner in relation to a customer, and take reasonable measures to verify the BO's identity so that the MSO is satisfied that it knows who the Beneficial owner is.

The verification requirements for a customer and a Beneficial owner are different under the AMLO. In determining what constitutes reasonable measures to verify the identity of a Beneficial owner of a customer, the MSO should consider and give due regard to the ML/TF risks posed by the customer and the business relationship.

9.1.2.1. Beneficial owner in relation to natural person:

In respect of a customer that is a natural person, there is no requirement for the MSO to make proactive searches for Beneficial owners of the customer in such a case, but the MSO should make appropriate enquiries where there are indications that the customer is not acting on his/her own behalf.

9.1.2.2. Beneficial owner in relation to a legal person:

For a customer that is a legal person, the MSO should identify

a. any natural person who ultimately has a controlling ownership interest (i.e. more than 25%) in the legal person and
b. any natural person exercising control of the legal person or its management, and take reasonable measures to verify their identities.
c. If there is no such natural person (i.e. no natural person falls within the definition of Beneficial Owners), the MSO should identify the relevant natural persons who hold the position of senior managing official, and take reasonable measures to verify their identities.

While the MSO usually can identify who the Beneficial owner of a customer is in the course of understanding the ownership and control structure of the customer, the MSO may obtain an undertaking or declaration from the customer on the identity of, and the information relating to, its BO. Nevertheless, in addition to the undertaking or declaration obtained, the MSO should take reasonable measures to verify the identity of the Beneficial owner (e.g. corroborating the undertaking or declaration with publicly available information).

If the ownership structure of a customer involves different types of legal persons or legal arrangements, in determining who the Beneficial owner is, the MSO should pay attention to who has ultimate ownership or control over the customer, or who constitutes the controlling mind and management of the customer.

9.1.2.3. Beneficial owner in relation to a trust or other similar legal arrangements:

Similar to a corporation, a trust or other similar legal arrangement can also be part of an intermediate layer in an ownership structure and should be dealt with in similar manner to a corporation being part of an intermediate layer.

For trusts, the MSO should identify

a. the settlor,
b. the protector (if any),
c. the enforcer (if any),
d. the beneficiaries or class of beneficiaries, and
e. any other natural person exercising ultimate control over the trust (including through a chain of control or ownership),

and take reasonable measures to verify their identities.

For other similar legal arrangements, the MSO should identify any natural person in equivalent or similar positions to a Beneficial owner of a trust as stated above and take reasonable measures to verify the identity of such person. If a trust or other similar legal arrangement is involved in a business relationship and the MSO does not regard the trustee (or equivalent in other similar legal arrangement) as its customer (e.g. when a trust appears as part of an intermediate layer), the MSO should also identify the trustee and take reasonable measures to verify the identity of the trustee so that the MSO is satisfied that it knows who the trustee is.

For a beneficiary of a trust designated by characteristics or by class, the MSO should obtain sufficient information concerning the beneficiary to satisfy the MSO that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights.

Ownership and control structure

Where a customer is not a natural person, the MSO should understand its ownership and control structure, including identification of any intermediate layers (e.g. by reviewing an ownership chart of the customer). The objective is to follow the chain of ownerships to the Beneficial owners of the customer.

Where a customer has a complex ownership or control structure, the MSO should obtain sufficient information for the MSO to satisfy itself that there is a legitimate reason behind the particular structure employed.

Bearer shares

Bearer shares refer to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate. Therefore, it is more difficult to establish the beneficial ownership of a company with bearer shares. The MSO should

adopt procedures to establish the identities of the Beneficial owners of such shares and ensure that the MSO is notified whenever there is a change of Beneficial owner of such shares.

Where bearer shares have been deposited with an authorized/registered custodian, the MSO should seek independent evidence of this, for example confirmation from the registered agent that an authorized/registered custodian holds the bearer shares, together with the identities of the authorized/registered custodian and the person who has the right to those entitlements carried by the share. As part of the MSO's ongoing periodic review, it should obtain evidence to confirm the authorized/registered custodian of the bearer shares.

Where the shares are not deposited with an authorized/registered custodian, the MSO should obtain declarations prior to account opening and annually thereafter from each Beneficial owner of such shares. The MSO should also require the customer to notify it immediately of any changes in the ownership of the shares.

Nominee shareholders

For a customer identified to have nominee shareholders in its ownership structure, the MSO should obtain satisfactory evidence of the identities of the nominees, and the persons on whose behalf they are acting, as well as the details of arrangements in place, in order to determine who, the Beneficial owner is.

9.1.3. Identification and verification of a person purporting to act on behalf of the customer:

A person may be appointed to act on behalf of a customer to establish business relationships, or may be authorized to give instructions to the MSO to conduct various activities through the account or the business relationship established. Whether the person is considered to be a person purporting to act on behalf of the customer (PPTA), it should be determined so based on the nature of that person's roles and the activities which the person is authorized to conduct, as well as the ML/TF risks associated with these roles and activities. The MSO should implement clear policies and procedures for determining who is considered to be a PPTA.

If a person is a PPTA, the MSO must:

A. identify the person and take reasonable measures to verify the person's identity on the basis of documents, data or information provided by
    a. a governmental body;
    b. the CCE or any other RA;
    c. an authority in a place outside Hong Kong that performs functions similar to those of the CCE or any other RA; or

d. any other reliable and independent source that is recognized by the CCE; and

B. verify the person's authority to act on behalf of the customer.

The MSO should identify and verify the identity of the PPTA in line with the identification and verification requirements for a customer that is a natural person or a legal person, where applicable.

The MSO should verify the authority of each PPTA by appropriate documentary evidence (e.g. board resolution or similar written authorization).

9.1.4. Purpose and intended nature of business relationship

The MSO must understand the purpose and intended nature of the business relationship. In some instances, this will be self-evident, but in many cases, the MSO may have to obtain information in this regard. The information obtained by the MSO to understand the purpose and intended nature should be commensurate with the risk profile of the customer and the nature of the business relationship. In addition, where a customer is not a natural person, the MSO should also understand the nature of the customer's business.

Timing of verification

The MSO should verify the identity of a customer and any Beneficial owner of the customer before or during the course of establishing a business relationship or conducting transactions for occasional customers. However, the MSO may exceptionally verify the identity of a customer and any Beneficial owner of the customer after establishing the business relationship, provided that:

a. any risk of ML/TF arising from the delayed verification of the customer's or BO's identity can be effectively managed;
b. it is necessary not to interrupt the normal conduct of business with the customer; and
c. verification is completed as soon as reasonably practicable.

Examples of situations where it may be necessary not to interrupt the normal conduct of business include:

a. securities transactions – in the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed; and
b. life insurance business – in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policy holder is established, but in all such cases, identification and verification should occur

at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

If the MSO allows verification of the identity of a customer and any Beneficial owner of the customer after establishing the business relationship, it should adopt appropriate risk management policies and procedures concerning the conditions under which the customer may utilize the business relationship prior to verification. These policies and procedures should include:

a. establishing a reasonable timeframe for the completion of the identity verification measures and the follow-up actions if exceeding the timeframe (e.g. to suspend or terminate the business relationship concerned);
b. placing appropriate limits on the number, types and/or amount of transactions that can be performed;
c. monitoring of large and complex transactions being carried out outside the expected norms for that type of relationship;
d. keeping the BOD periodically informed of any pending completion cases; and
e. ensuring that funds are not paid out to any third party. Exceptions may be made to allow payments to third parties subject to the following conditions:
    i. there is no suspicion of ML/TF;
    ii. the risk of ML/TF is assessed to be low;
    iii. the transaction is approved by the BOD, who should take account of the nature of the business of the customer before approving the transaction; and
    iv. the names of recipients do not match with watch lists such as those for terrorist suspects and politically exposed persons (PEPs).

If verification cannot be completed within the reasonable timeframe set in the MSO's risk management policies and procedures, the MSO should terminate the business relationship as soon as reasonably practicable and refrain from carrying out further transactions (except to return funds or other assets in their original forms as far as possible). The MSO should also assess whether this failure provides grounds for knowledge or suspicion of ML/TF and consider making a suspicious transaction report (STR) to the JFIU, particularly if the customer requests that funds or other assets be transferred to a third party or be "transformed" (e.g. from cash into a cashier order) without a justifiable reason.

9.2. Simplified Due Diligence Measures

The MSO may apply SDD measures in relation to a business relationship or transaction if it determines that, taking into account its risk assessment, the business relationship or transaction presents a low ML/TF risk. (See section 8.2.3.)

Examples of possible SDD measures include:

a. accepting other documents, data or information (e.g. proof of FI's license, listed status or authorization status etc.), other than examples provided in paragraphs relating to verification of identity of customer that is a legal person and/or where the customer is a trust or other similar legal arrangement, for a customer falling within the lower customer risk factor category
b. adopting simplified customer due diligence in relation to Beneficial owners as will be specified below
c. reducing the frequency of updates of customer identification information;
d. reducing the degree of ongoing monitoring and scrutiny of transactions based on a reasonable monetary threshold; or
e. not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and intended nature from the type of transactions or business relationship established.

9.2.1. SDD in relation to beneficial owners: (b. Above)

The MSO may choose not to identify or take reasonable measures to verify the Beneficial owner in relation to:

Where the customer is:

A. A financial institution
B. An institution that:
   a. Is incorporated or established in an equivalent jurisdiction
   b. Carries on a business similar to that carried on by a financial institution
   c. Has measures in place to ensure compliance with CDD and record keeping requirements similar to the requirements imposed under AMLO and
   d. include Is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities
C. A corporation listed on any stock exchange
D. An investment vehicle where the person responsible for carrying out measures that are similar to the customer due diligence measures in relation to all the investors of the investment vehicle is:
   a. A financial institution
   b. An institution that:
      - is incorporated or established in Hong Kong
      - has measures in place to ensure compliance with CDD and record keeping requirements similar to the requirements imposed under AMLO
      - is supervised for compliance with those requirements; or
      - is incorporated or established in an equivalent jurisdiction
E. the Government or any public body in Hong Kong

F. the Government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.

If a customer not falling in the list above, has in its ownership chain an entity that falls within that paragraph, the MSO is not required to identify or verify the Beneficial owners of that entity in that chain when establishing a business relationship with or carrying out an occasional transaction for the customer. However, the MSO should still identify and take reasonable measures to verify the identity of Beneficial owners in the ownership chain that are not connected with that entity.

Where a customer is a corporation listed on any stock exchange, the MSO may choose not to identify or take reasonable measures to verify its Beneficial Owners. For this purpose, the MSO should assess whether the customer is subject to any disclosure requirements (either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership of the customer.

The MSO may choose not to identify or take reasonable measures to verify the Beneficial owner of a customer, if a customer is an FI as defined in the AMLO that opens an account:

a. in the name of a nominee company for holding fund units on behalf of the FI or its underlying customers; or
b. in the name of an investment vehicle in the capacity of a service provider (such as manager or custodian) to the investment vehicle and the underlying investors have no control over the management of the investment vehicle's assets; provided that the FI:
   i. has conducted CDD:
      - in the case where the nominee company holds fund units on behalf of the FI or the FI's underlying customers, on its underlying customers; or
      - in the case where the FI acts in the capacity of a service provider (such as manager or custodian) to the investment vehicle, on the investment vehicle pursuant to the provisions of the AMLO; and
   ii. is authorized to operate the account as evidenced by contractual document or agreement.

<u>A customer who is a solicitor or a firm of solicitor, provided that the following criteria are satisfied:</u>

a. the client account is kept in the name of the customer
b. moneys or securities of the customer's clients in the client account are mingled; and
c. the client account is managed by the customer as those clients' agent.

When opening a client account for a solicitor or a firm of solicitors, the MSO should establish the proposed use of the account, i.e. whether to hold co-mingled client funds or the funds of a specific client. If a client account is opened on behalf of a single client or

there are sub-accounts for each individual client where funds are not co-mingled at the MSO, the MSO should establish the identity of the underlying client(s) in addition to that of the solicitor opening the account.

SDD measures should not be applied or continue to be applied, where:

a. the MSO's risk assessment changes and it no longer considers that there is a low degree of ML/TF risk;
b. where the MSO suspects ML or TF; or
c. where there are doubts about the veracity or accuracy of documents or information previously obtained for the purposes of identification or verification.

9.3. Enhanced Due Diligence Measures (EDD)

The MSO must apply EDD measures in relation to a business relationship or transaction to mitigate and manage the high ML/TF risks in:

A. A situation that by its nature may present a high ML/TF risk, (see section 8.2.5) or
B. A situation specified by the CCE in a notice in writing given to the MSO

The MSO should obtain approval from the BOD to establish or continue a business relationship that presents a high ML/TF risk.

The EDD measures applied should be commensurate with the nature and level of ML/TF risks, based on the higher ML/TF risk factors identified by the MSO. The extent of EDD measures should be proportionate, appropriate and discriminating, and be able to be justified to the CCE.

The MSO should conduct enhanced ongoing monitoring of a business relationship that presents a high ML/TF risk, for example, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Examples of possible EDD measures include:

a. obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and BO;
b. obtaining additional information on the intended nature of the business relationship;
c. obtaining information on the source of funds or source of wealth of the customer
d. obtaining information on the reasons for intended or performed transactions; or
e. requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

9.3.1. PEP(s)

When the MSO know that a customer or a Beneficial owner of a customer is a foreign PEP, it should, before

a. establishing a business relationship or
b. continuing an existing business relationship where the customer or the Beneficial owner is subsequently found to be a foreign PEP,

apply all the following EDD measures:

a. obtaining approval from the BOD for establishing or continuing such business relationship;
b. taking reasonable measures to establish the customer's or the BO's source of wealth and the source of the funds; and
c. conducting enhanced ongoing monitoring of that business relationship

Since not all PEPs pose the same level of ML/TF risks, the MSO should adopt an RBA in determining the extent of EDD measures above taking into account relevant factors such as:

a. the prominent (public) functions that a PEP holds;
b. the geographical risk associated with the jurisdiction where a PEP holds prominent (public) functions;
c. the nature of the business relationship (e.g. the delivery/distribution channel used; or the product or service offered); or
d. the level of influence that a PEP may continue to exercise after stepping down from the prominent (public) function.

The MSO should apply the EDD measures set out above in any of the following situations:

a. before establishing a high risk business relationship with a customer who is or whose Beneficial owner is a domestic PEP
b. or an international organization PEP;
c. when continuing an existing business relationship with a customer who is or whose Beneficial owner is a domestic PEP or an international organization PEP where the relationship subsequently becomes high risk; or
d. when continuing an existing high risk business relationship where the MSO subsequently knows that the customer or the Beneficial owner of the customer is a domestic PEP or an international organization PEP.

If a domestic PEP or an international organization PEP is no longer entrusted with a prominent (public) function, the MSO may adopt an RBA to determine whether to apply or continue to apply the EDD measures set out above in a high risk business relationship with a customer who is or whose Beneficial owner is that domestic PEP or international organization PEP, taking into account various risk factors, such as:

a. the level of (informal) influence that the individual could still exercise;
b. the seniority of the position that the individual held as a PEP; or
c. whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

The MSO should obtain approval from its BOD such a decision.

9.3.2. Customer not physically present for identification purposes

If a customer has not been physically present for identification purposes, the MSO must carry out at least one of the following additional measures to mitigate the risks posed:

A. further verifying the customer's identity on the basis of documents, data or information but not previously used for the purposes of verification of the customer's identity under that section;
B. taking supplementary measures to verify information relating to the customer that has been obtained by the MSO such as:
    a. use of an independent and appropriate person to certify identification documents
    b. checking relevant data against reliable databases or registries
    c. using appropriate technology etc.
C. ensuring that the first payment made into the customer's account is received from an account in the customer's name with an authorized institution or an institution that:
    a. is incorporated or established in an equivalent jurisdiction
    b. carries on a business similar to that carried on by an authorized institution
    c. has measures in place to ensure compliance with requirements similar to those imposed
    d. is supervised for compliance with those requirements by authorities in that jurisdiction that perform functions similar to those on the Monetary Authority.

The extent of the above additional measures will depend on the nature and characteristic of the product or service requested and the assessed ML/TF risks presented by the customer.

9.3.3. Wire transfers

A. This section does not apply to the following wire transfers—
   a. a wire transfer between two financial institutions if each of them acts on its own behalf;
   b. a wire transfer between a financial institution and a foreign institution if each of them acts on its own behalf;
   c. a wire transfer if—
      i. it arises from a transaction that is carried out using a credit card or debit card (such as withdrawing money from a bank account through an automated teller machine with a debit card, obtaining a cash advance on a credit card, or paying for goods or services with a credit or debit card), except when the card is used to effect a transfer of money; and
      ii. the credit card or debit card number is included in the message or payment form accompanying the transfer.

B. Subject to subsection C below, before carrying out a wire transfer, a financial institution that is an ordering institution must record—
   a. the originator's name;
   b. the number of the originator's account maintained with the financial institution and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the financial institution;
   c. the originator's address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth;
   d. the recipient's name; and
   e. the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution.

C. Subsection B.c. does not apply to a wire transfer involving an amount below $8,000 or an equivalent amount in another currency.

D. Subject to subsections E. and F., a financial institution that is an ordering institution must include in the message or payment form accompanying the wire transfer
   a. for a wire transfer involving an amount equal to or above $8,000 or an equivalent amount in another currency—the information recorded under subsection B.a., b., c., d., and e. in relation to the transfer;
   b. for a wire transfer involving an amount below $8,000 or an equivalent amount in another currency—the information recorded under subsection B.a., b., d., and e. in relation to the transfer.

E. A financial institution may, in relation to a domestic wire transfer, include in the message or payment form accompanying the transfer only the information recorded

under subsection B.b. in relation to the transfer but if it does so, it must, on the request of the financial institution to which it passes on the transfer instruction or the relevant authority, provide to that financial institution or the relevant authority the information recorded under subsection B.a. and B.b. in relation to the transfer within 3 business days after it receives the request.

F. If more than one individual wire transfer from a single originator is bundled in a batch file for transmission to a recipient or recipients in a place outside Hong Kong, a financial institution is not required to comply with subsection D. in relation to each of the wire transfers if:
    a. the information recorded under subsection B.b. is included in the message or payment form accompanying each transfer; and
    b. the batch file contains the information recorded under subsection B.
G. If a financial institution acts as an intermediary institution in a wire transfer, it must transmit all of the information that it receives with the transfer to the institution to which it passes on the transfer instruction.
H. Where a financial institution is a beneficiary institution in a domestic wire transfer—
    a. if the wire transfer is not accompanied by the information required under subsection B.b., it must as soon as reasonably practicable—
        i. obtain the information from the institution from which it receives the transfer instruction; and
        ii. if the information cannot be obtained, either—
            1. consider restricting or terminating its business relationship with the institution referred to in subparagraph (i); or
            2. take reasonable measures to mitigate the risk of ML/TF involved; or
    b. if the financial institution is aware that the accompanying information that purports to be the information required under subsection B.b. is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
I. Where a financial institution is a beneficiary institution or an intermediary institution in a wire transfer that is not a domestic wire transfer—
    a. if the wire transfer is not accompanied by all of the information required under subsection B., it must as soon as reasonably practicable—
        i. obtain the missing information from the institution from which it receives the transfer instruction; and
        ii. if the missing information cannot be obtained, either—
            1. consider restricting or terminating its business relationship with the institution referred to in subparagraph (i); or
            2. take reasonable measures to mitigate the risk of ML/TF involved; or
    b. if the financial institution is aware that any of the accompanying information that purports to be the information required under subsection B. is incomplete or

meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.

9.3.4. Remittance transactions

A. This section applies to a remittance transaction, other than a wire transfer, involving an amount equal to or above $8,000 or an equivalent amount in any other currency, that is carried out by a licensed money service operator.
B. Before carrying out a remittance transaction, a licensed money service operator must—
   a. identify the originator;
   b. verify the identity of the originator by reference to the originator's identification document; and
   c. record—
      i. the originator's name;
      ii. the originator's identification document number and, if the originator's identification document is a travel document, the place of issue of the travel document;
      iii. the originator's address;
      iv. the currency and amount involved; and
      v. the date and time of receipt of the instructions, the recipient's name and address and the method of delivery.

9.3.5. In other high risk situations

A financial institution must, in any situation that by its nature may present a high risk of ML or TF:

A. where a business relationship is to be established—
   a. obtain approval from the BOD to establish the business relationship; and
   b. either—
      i. take reasonable measures to establish the relevant customer's or BO's source of wealth and the source of the funds that will be involved in the business relationship; or
      ii. take additional measures to mitigate the risk of ML/TF involved;
B. where a business relationship has been established—
   a. obtain approval from the BOD to continue the business relationship;
   b. if there is a Beneficial owner in relation to the relevant customer, take reasonable measures to verify the BO's identity so that the financial institution is satisfied that the financial institution knows who the Beneficial owner is; and

c. either—
    i. take reasonable measures to establish the relevant customer's or BO's source of wealth and the source of the funds that are involved in the business relationship; or
    ii. take additional measures to mitigate the risk of ML/TF involved; or

C. where an occasional transaction is to be carried out, take additional measures to mitigate the risk of ML/TF involved.

9.4. Failure to satisfactorily complete Customer Due Diligence

If during the business relationship, the customer fails or refuses to submit, within a reasonable timeframe the required verification data and information, the MSO may terminate the business relationship and close all the accounts of the customer. It may also be appropriate for the MSO not to carry out a transaction pending completion of the CDD. Where CDD or a material part of it, such as identifying and verifying a BO, cannot be conducted, the business relationship with the said customer should not be established.

If the MSO is unable to conduct or complete the CDD, it will apply one or more of the following measures as may be appropriate in the circumstances.

a. Not open an account or provide a service
b. Not otherwise establish a business relationship or carry out a transaction
c. Subject to the abovementioned, terminate or suspend any existing business relationship with the customer
d. Consider whether the circumstances necessitate the submission of a STR to the JFIU

In the case of a new customer, it may be appropriate to terminate the business relationship before a product or service is provided. In the case of an existing customer however, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances. In either case, the MSO must be careful not to 'tip of' the customer.

The MSO is not obliged to terminate or suspend any existing business relationship with a customer if:

a. to do so would amount to 'tipping off' the customer, (see section 14) or
b. the JFIU directs the MSO to act otherwise.

9.5. Prohibitions on anonymous accounts

The MSO must not maintain anonymous accounts or accounts in fictitious names for any new or existing customer. Where numbered accounts exist, the MSO must maintain them

in such a way that full compliance can be achieved with the AMLO. The MSO must properly identify and verify the identity of the customer in accordance with the Guideline. In all cases, whether the relationship involves numbered accounts or not, the customer identification and verification records must be available to the CCE, other competent authorities, the CO, auditors, and other staff with appropriate authority

9.6. Authenticity of documents obtained

Ideally, documents should be inspected in original form. Where this is not possible (e.g. because the MSO has no physical contact with the Customer), it must obtain a first generation photocopy certified as a true copy of the original document by a person of good standing such as a registered lawyer or notary, a chartered accountant, a bank manager, a police officer, an embassy or consular official, or other similar person (whose identity and objectivity can be proved beyond reasonable doubt).

The certified photocopy must:

a. bear language attesting that the photocopy is a true copy of the original document;
b. show the date on which the photocopy was made and certified;
c. show the name, occupation, business address and telephone number of the person who certified the photocopy.

Note that the requirement for a “first generation” photocopy means that copies of photocopies are not acceptable.

Additionally, all customer identification documentation provided should be recent (where applicable). A document is considered as recent when submitted to the MSO within 6 months from the issue date.

9.7. Language standards

All customer identification documents collected during the KYC process should be in the English language. Customer identification documents collected directly from the customer (memorandum and articles of association, certificate of incorporation, personal identification documents, etc.) will often exist in the local language.

Where these documents cannot be produced in English the best practice is to:

a. Identify the document;
b. Explain its purpose; and
c. Set out the specific contents of the document in English (the material elements – not a word for word translation).

9.8. Certification Standards

Where specified in the MSO’s request lists, customer identification documentation

should be provided in certified true copy or in apostil form. In all other cases originals need to be provided.

Certified (True) Copy means that the person certifying the copy of the document has had sight of the original document at certification and is in a position to certify that the copy is a True and complete copy of the original document.

The following is a list of non-exhaustive examples of appropriate persons to certify verification of identification documents:

a. an intermediary specified in section 10 of this Manual.
b. a member of the judiciary in Hong Kong or in an equivalent jurisdiction;
c. an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity;
d. a Justice of the Peace; and
e. other professional person such as certified public accountant, lawyer, notary public and chartered secretary.

The certifier should sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it. The certifier should state that it is a true copy of the original (or words to similar effect)

The MSO remain liable for failure to carry out prescribed CDD and therefore must exercise caution when considering accepting certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction.

In any circumstances where the MSO is unsure of the authenticity of certified documents, or that the documents relate to the customer, the MSO should take additional measures to mitigate the ML/TF risk.

Where the MSO's request list requires that documents are apostilled, this process requires the documents to be apostilled as per the provisions of The Hague Convention.

9.9. Independent and reliable sources

The identity of an individual physically present in Hong Kong should be verified by reference to their Hong Kong identify card or travel document. The MSO should always identify and/or verify a Hong Kong resident's identity by reference to their Hong Kong identity card or document of identity. The identity of a non-resident should be verified by reference to their valid travel documents.

For non-resident individuals who are not physically present in Hong Kong, the MSO may identify and/or verify their identity by reference to the following documents:

a. a valid international passport or other travel document; or
b. a current national (i.e. Government or State-issued) identity card bearing the photograph of the individual; or

c. current valid national (i.e. Government or State-issued) driving license incorporating photographic evidence of the identity of the applicant, issued by a competent national or state authority.

Travel document means a passport or some other document furnished with a photograph of the holder establishing the identity and nationality, domicile or place of permanent residence of the holder. The following documents constitute travel documents for the purpose of identity verification:

a. Permanent Resident Identity Card of Macau Special Administrative Region;
b. Mainland Travel Permit for Taiwan Residents;
c. Seaman's Identity Document (issued under and in accordance with the International Labour Organisation Convention/Seafarers Identity Document Convention 1958);
d. Taiwan Travel Permit for Mainland Residents;
e. Permit for residents of Macau issued by Director of Immigration;
f. Exit-entry Permit for Travelling to and from Hong Kong and Macau for Official Purposes; and
g. Exit-entry Permit for Travelling to and from Hong Kong and Macau.

For minors born in Hong Kong who are not in possession of a valid travel document or Hong Kong identity card, their identity should be verified by reference to the minor's Hong Kong birth certificate. Whenever establishing relations with a minor, the identity of the minor's parent or guardian representing or accompanying the minor should also be recorded and verified in accordance with the above requirements.

The MSO may identify and/or verify a corporate customer by performing a company registry search in the place of incorporation and obtaining a full company search report, which confirms the current reference to a full company particulars search (or overseas equivalent).

For jurisdictions that do not have national ID cards and where customers do not have a travel document or driving license with a photograph, the MSO may, exceptionally and applying an RBA, accept other documents as evidence of identity. Wherever possible such documents should have a photograph of the individual.

9.10. Electronic reliable sources

The MSO recognizes electronic information only from Electronic Reliable Sources listed in this Manual:

a. Online information from any officially sanctioned Company Registrar;

b. Online information from any equivalent jurisdiction's Regulator website;

c. Websites of the customer or its parent confirming the nature of subsidiary or branch relationships;

d. Annual Reports, Corporate Governance Reports and Audited Financial Statements downloaded from customers' websites;
e. Approved vendor services, e.g. Worldcheck, Webshield, Dun & Bradstreet, Standard & Poor's, LexisNexis;
f. Online information from Approved Stock Markets websites; and
g. Online information from a recognized news agency, e.g. Bloomberg, Reuters, Factiva, FT.

The above list of reliable sources is not exhaustive, and a limited number of exceptions can be referred to Compliance on a case-by-case basis.

10. Reliance on third parties

Reliance on CDD performed by intermediaries

10.1. Overview

The MSO may rely upon an intermediary to perform any part of the CDD measures; however, the ultimate responsibility for ensuring that CDD requirements are met, remains with the MSO.

The MSO cannot rely on an intermediary to continuously monitor its business relationship with a customer.

In a third-party reliance scenario, the third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying MSO, and would apply its own procedures to perform the CDD measures.

For the avoidance of doubt, reliance on intermediaries does not apply to outsourcing or agency relationships, in which the outsourced entity or agent applies the CDD measures on behalf of the MSO, in accordance with the MSO's procedures, and subject to the MSO's control of effective implementation of these procedures by the outsourced entity or agent.

When relying on an intermediary, the MSO must:

a. obtain written confirmation from the intermediary that the intermediary agrees to act as the MSO's intermediary and perform which part of the CDD measures, and
b. be satisfied that the intermediary will on request provide a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out the CDD measures without delay.

The MSO that carries out a CDD measure by means of an intermediary must immediately after the intermediary has carried out that measure, obtain from the intermediary the data or information that the intermediary has obtained in the course of carrying out that measure, but nothing in this paragraph requires the MSO to obtain at the same time from the intermediary a copy of the document, or a record of the data or information, that is obtained by the intermediary in the course of carrying out that measure.

Where these documents and records are kept by the intermediary, the MSO should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the MSO's business relationship with the customer and for at least 5 years beginning on the date on which the business relationship of a customer with the MSO ends or until such time as may be specified by the CCE. The MSO must ensure that the intermediary will, if requested by the MSO within the period specified in the record-keeping requirements of the AMLO, provide to the MSO a copy of any document, or a record of any data or information, obtained by the intermediary in the course of

carrying out that measure as soon as reasonably practicable after receiving the request. The MSO should also obtain an undertaking from the intermediary to supply copies of all underlying CDD information in circumstances where the intermediary is about to cease trading or does not act as an intermediary for the MSO anymore.

The MSO should conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay.

Whenever the MSO has doubts as to the reliability of the intermediary, it should take reasonable steps to review the intermediary's ability to perform its CDD duties. If the MSO intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the MSO has any doubts regarding the CDD measures carried out by the intermediary previously, the MSO should perform the required CDD as soon as reasonably practicable.

10.2. Domestic Intermediaries

The MSO may rely upon any one of the following domestic intermediaries, to perform any part of the CDD measures:

A. an FI that is an authorized institution, a licensed corporation, an authorized insurer, an appointed insurance agent or an authorized insurance broker (intermediary FI);
B. an accounting professional meaning:
    a. a certified public accountant or a certified public accountant (practicing), as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50);
    b. a corporate practice as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50); or
    c. a firm of certified public accountants (practicing) registered under Part IV of the Professional Accountants Ordinance (Cap. 50);
C. an estate agent meaning:
    a. a licensed estate agent as defined by section 2(1) of the Estate Agents Ordinance (Cap. 511); or
    b. a licensed salesperson as defined by section 2(1) of the Estate Agents Ordinance (Cap. 511);
D. a legal professional meaning:
    a. a solicitor as defined by section 2(1) of the Legal Practitioners Ordinance (Cap. 159); or
    b. a foreign lawyer as defined by section 2(1) of the Legal Practitioners Ordinance (Cap. 159); or
E. a trust or company service provider (TCSP) licensee meaning:
    a. a person who holds a licence granted under section 53G or renewed under section 53K of the AMLO; or
    b. a deemed licensee as defined by section 53ZQ(5) of the AMLO,

provided that in the case of an accounting professional, an estate agent, a legal professional or a TCSP licensee, the MSO is satisfied that the domestic intermediary has adequate procedures in place to prevent ML/TF and is required to comply with the relevant CDD requirements with respect to the customer.

The MSO should take appropriate measures to ascertain if the domestic intermediary satisfies the criteria set out above, which may include:

a. where the domestic intermediary is an accounting professional, an estate agent, a legal professional or a TCSP licensee, ascertaining whether the domestic intermediary is required to comply with the relevant CDD requirements with respect to the customer;
b. making enquiries concerning the domestic intermediary's stature or the extent to which any group AML/CFT standards are applied and audited; or
c. reviewing the AML/CFT policies and procedures of the domestic intermediary.

10.3. Overseas Intermediaries (the overseas intermediary and MSO could be unrelated or within the same group of companies to which the MSO belongs)

The MSO may rely upon an overseas intermediary carrying on business or practicing in an equivalent jurisdiction to perform any part of the CDD measures, where the intermediary:

A. falls into one of the following categories of businesses or professions:
a. an institution that carries on a business similar to that carried on by an intermediary FI;
b. a lawyer or a notary public;
c. an auditor, a professional accountant, or a tax advisor;
d. a TCSP;
e. a trust company carrying on trust business; and
f. a person who carries on a business similar to that carried on by an estate agent;
   i. is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction;
   ii. has measures in place to ensure compliance with requirements similar to those imposed by AMLO in relation to Customer Due Diligence and Record-keeping
   iii. is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs or the regulatory bodies (as may be applicable).

The MSO should take appropriate measures to ascertain if the overseas intermediary satisfies the criteria set out above. Appropriate measures that should be taken to ascertain whether the intermediary has measures in place to ensure compliance with

requirements similar to those imposed by AMLO in relation to Customer Due Diligence and Record-keeping (criterion ii above), may include:

a. making enquiries concerning the overseas intermediary's stature or the extent to which any group's AML/CFT standards are applied and audited; or
b. reviewing the AML/CFT policies and procedures of the overseas intermediary

10.4. Related foreign financial institutions as intermediaries

The MSO may also rely upon a related foreign financial institution (related foreign FI) to perform any part of the CDD measures, if the related foreign FI:

A. carries on, in a place outside Hong Kong, a business similar to that carried on by an intermediary FI; and falls within any of the following descriptions:
    a. it is within the same group of companies as the MSO;
    b. if the MSO is incorporated in Hong Kong, it is a branch of the MSO;
    c. if the MSO is incorporated outside Hong Kong:
        i. it is the head office of the MSO; or
        ii. it is a branch of the head office of the MSO;
B. is required under group policy:
    a. to have measures in place to ensure compliance with requirements similar to those imposed by AMLO in relation to Customer Due Diligence and Record-keeping; and
    b. to implement programmes against ML/TF; and
C. is supervised for compliance with the requirements mentioned in paragraph (2) at a group level:
    a. by an RA; or
    b. by an authority in an equivalent jurisdiction that performs, in relation to the holding company or the head office of the MSO, functions similar to those of an RA under the AMLO.

The group policy set out above (criterion B. Above) refers to a policy of the group of companies to which the MSO belongs and the policy applies to the MSO and the related foreign FI. The group policy should include CDD and record keeping requirements similar to the requirements imposed under AMLO and the group-wide AML/CFT System (e.g. compliance and audit functions). The group policy should also be able to mitigate adequately any higher country risk in relation to the jurisdiction where the related foreign FI is located. The MSO should be satisfied that the related foreign FI is subject to regular and independent reviews over its ongoing compliance with the group policy conducted by any group-level compliance, audit or other similar AML/CFT functions.

The MSO should be able to demonstrate that the implementation of the group policy is supervised at a group level by either an RA or an authority in an equivalent jurisdiction that performs functions similar to those of an RA under the AMLO, which practices group-wide supervision which extends to the related foreign FI.

10.5 Records kept by intermediaries

Where customer identification and verification documents are held by an intermediary on which the MSO is relying to carry out CDD measures, the MSO concerned remains responsible for compliance with all record-keeping requirements. The MSO should ensure that the intermediary being relied on, has systems in place to comply with all the record-keeping requirements under the AMLO and CED and that documents and records will be provided by the intermediary as soon as reasonably practicable after the intermediary receive the request from the MSO.

An intermediary should keep:

a. the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and, where applicable, verifying the identity of the customer and/or Beneficial owner of the customer and/or beneficiary and/or persons who purport to act on behalf of the customer and/or other connected parties to the customer;
b. other documents and records obtained throughout the CDD and ongoing monitoring process, including SDD and EDD;
c. where applicable, the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship;
d. the original or a copy of the records and documents relating to the customer's account (e.g. account opening form or risk assessment form) and business correspondence with the customer and any Beneficial owner of the customer (which at a minimum should include business correspondence material to CDD measures or significant changes to the operation of the account) and
e. the results of any analysis undertaken (e.g. inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose).

All documents and records mentioned above, should be kept throughout the continuance of the business relationship with the customer and for a period of at least 5 years after the end of the business relationship. Similarly, for occasional transaction equal to or exceeding the CDD threshold (i.e. $8000 for wire transfers and $120000 for other types of transactions), the intermediary should keep all documents and records mentioned above for a period of at least 5 years after the date of the occasional transaction.

For the avoidance of doubt, the MSO that relies on an intermediary for carrying out a CDD measure should immediately obtain data or the information that the intermediary has obtained in the course of carrying out that measure.

The MSO should ensure that an intermediary will pass the documents and records to the MSO, upon termination of the services provided by the intermediary.

11. On-going Monitoring Process

11.1. Overview

The MSO has a full understanding of normal and reasonable account activity of its customers as well as of their economic profile and has the means of identifying transactions which fall outside the regular pattern of an account's activity or to identify complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason. Without such knowledge, the MSO shall not be able to discharge its legal obligation to identify and report suspicious transactions to the JFIU.

The constant monitoring of the customers' accounts and transactions is an imperative element in the effective controlling of the risk of ML/TF.

In this respect, the CO shall be responsible for maintaining as well as developing the on-going monitoring process of the MSO. The Internal Auditor shall review the MSO's procedures with respect to the on-going monitoring process as frequent as defined by a BOD decision. (see section 7)

11.2. Procedures

The procedures and intensity of monitoring customers' accounts and examining transactions on the customer's level of risk shall include the following:

- ✓ the identification of:
    - all high risk customers, as applicable; the MSO shall be able to produce detailed lists of high risk customers, so as to facilitate enhanced monitoring of accounts and transactions, as deemed necessary
    - transactions which, as of their nature, may be associated with ML/TF.
    - unusual or suspicious transactions that are inconsistent with the economic profile of the customer for the purposes of further investigation.
    - in case of any unusual or suspicious transactions, any employee who identified the unusual or suspicious transactions shall be responsible to communicate with the MLRO
- ✓ the ascertainment of the source and origin of the funds credited to accounts
- ✓ the on-going monitoring of the business relationship in order to determine whether there are reasonable grounds to suspect that customer accounts contain proceeds derived from serious tax offences.
- ✓ the use of appropriate and proportionate IT systems including:

    - adequate automated electronic management information systems which will be capable of supplying the BOD and the CO, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of customer accounts and

transactions based on the assessed risk for ML/TF purposes, in view of the nature, scale and complexity of the MSO's business.

- automated electronic management information systems to extract data and information that is missing regarding the customer identification and the construction of a customer's economic profile.

- ✓ for all accounts, automated electronic management information systems to add up the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This can be done by setting limits for a particular type, or category of accounts (e.g. high risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account the economic profile of the customer, the country of his/her origin, the source of the funds, the type of transaction or other risk factors. The MSO shall pay particular attention to transactions exceeding the abovementioned limits, which may indicate that a customer might be involved in unusual or suspicious activities.
- ✓ the monitoring of accounts and transactions in relation to specific types of transactions and the economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the business relationship. Furthermore, the monitoring covers customers who do not have a contact with the MSO as well as dormant accounts exhibiting unexpected movements.

12. Construction of an Economic and Risk Profile

Based on a holistic view of the information obtained in the context of the application of CDD measures, the MSO should be able to finalize the customer economic and risk profile, which determines the level and type of ongoing monitoring (including ongoing CDD and transaction monitoring) and support the MSO's decision whether to enter into, continue or terminate, the business relationship. As the customer economic and risk profile will change over time, the MSO should review and update the risk assessment of a customer from time to time, particularly during ongoing monitoring.

The MSO shall be satisfied that it's dealing with a real person and, for this reason, the MSO shall obtain sufficient evidence of identity to verify that the person is who he/she claims to be. Furthermore, the MSO shall verify the identity of the BO(s) of the customers' accounts. In the cases of legal persons, the MSO shall obtain adequate data and information so as to understand the ownership and control structure of the customer. Irrespective of the customer type (e.g. natural or legal person, sole trader or partnership), the MSO shall request and obtain sufficient data and information regarding the customer business activities and the expected pattern and level of transactions. However, it is noted that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative.

Minimum of the customers' economic profile must include the following:

a. the purpose and the reason for requesting the establishment of a business relationship;
b. the anticipated account turnover, the nature and number of the transactions;
c. the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments;
d. the customer's size of wealth and annual income and the clear description of the main business/professional activities/operations;
e. country of main business activities
f. the source/origin and size of wealth (of the UBO)
g. Approximate Annual income (of the UBO);
h. the data and information that are used for the construction of the customer-legal person's economic and risk profile shall include the following:
    i. the name of the company;
    ii. the country of its incorporation;
    iii. the head offices address;
    iv. the names and the identification information of the Beneficial Owners;

v. the names and the identification information of the directors;
vi. the names and the identification information of the authorized signatories' financial information;
vii. the ownership structure of the group that the customer-legal person may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information).

The said data and information are recorded in a separate form designed for this purpose which is retained in the customer's file along with all other documents as well as all internal records of meetings with the respective customer. The said form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the customer or alters existing information that makes up the economic profile of the customer.

The construction of the customer's economic profile according to the provisions above shall be undertaken by the CO. In this respect, the data and information collected for the construction of the economic profile shall be fully documented and filed, as applicable.

13. Suspicious Transactions Reports

13.1. Overview

The MLRO is the reference point for reporting suspicious transactions and also the main point of contact with the JFIU and law enforcement agencies. The MLRO plays an active role in the identification and reporting of suspicious transactions. Principal functions of the MLRO include having oversight of:

a. review of internal disclosures and exception reports and, in light of all available relevant information, determination of whether or not it is necessary to make a report to the JFIU;
b. maintenance of all records related to such internal reviews; and
c. provision of guidance on how to avoid tipping off (see section 14).

13.2. Identifying suspicious transactions and internal reporting

The recognition of indicators of suspicious activity is the first step in the suspicious activity identification system. The following are some of the suspicious activity indicators most commonly associated with ML/TF.

A. Large or frequent cash transaction, either deposits or withdrawals.
B. Suspicious activity based on transaction pattern, i.e.
   a. Account used as a temporary repository for funds.
   b. A period of significantly increased activity amid relatively dormant periods.
   c. “Structuring" or "Smurfing" i.e. many lower value transactions conducted when one, or a few, large transactions could be used. Seen particularly in incoming remittances from countries with value based transaction reporting requirements.
   d. "U-turn" transactions, i.e. money passes from one person or company to another, and then back to the original person or company.

C. Involvement of one or more of the following entities which are commonly involved in ML/TF,
   a. Shelf, or Shell companies.
   b. MSOs
   c. Company registered in a known "tax haven" or "off-shore financial center".
   d. Company formation agent, or secretarial company, as the authorized signatory of the bank account.
   e. Casino.

D. Currencies, countries or national of countries, commonly associated with international crime or drug trafficking or identified as having serious deficiencies in their AML / CFT regimes,
   - Countries or places which do not or insufficiently apply the FATF Recommendations.
E. Customer refuses, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue.
F. Activity is incommensurate with that expected from the customer, considering the information already known to the MSO about the customer and the customer's previous financial activity. (For personal accounts consider customer's age, occupation, residential address, general appearance, type and level of previous financial activity. For company accounts consider type and level of activity).
G. Countries or nationals of countries, commonly associated with terrorist activities or the persons or organizations designated as terrorists or their associates.
H. Transactions made by a PEP or related by any other means to a PEP.

The MSO should establish measures in order to effectively recognize the abovementioned suspicious activity indicators:

- ✓ The CO has to define the areas in which there is no face-to-face contact between the staff and the customer and define the additional identification measures need to be taken in these cases.
- ✓ The MSO should use a computer program to monitor the turnover of money within an account and note the rolling average turnover per month for the preceding recent months. The current months' turnover is then compared with the average turnover. The current months' activity is regarded as suspicious if it is significantly larger than the average.
- ✓ Greater attention should be paid to monitor the activity of the following accounts which are considered as "high risk" accounts:
  a. Money changers
  b. Casinos
  c. Accounts with staff of secretarial companies as authorized signatories
  d. Accounts of "shell" companies and
  e. Law company client accounts
- ✓ The MSO should adopt more stringent policies in respect of customers who are expected to deal in large sums, e.g. request corporate and private banking customers for the expected nature of transactions and source of funds when opening such accounts.

Training programs to raise and maintain staff awareness regarding the recognition of suspicious activity are therefore vital for the effective implementation of these measures.

The MSO should establish and maintain clear policies and procedures to ensure that:

a. all staff are made aware of the identity of the MLRO and of the procedures to follow when making an internal report; and
b. all internal reports must reach the MLRO without undue delay.

The submission of an internal suspicion report should be done in a special form which is easily accessible to the staff of the MSO. The said report which is referred as ''Internal Suspicion Report for ML/TF'' is attached as **Appendix 1**, to the Manual.

The internal report should include sufficient details of the customer concerned and the information giving rise to the suspicion.

Once a staff of the MSO has reported suspicion to the MLRO in accordance with the policies and procedures established by the MSO for the making of such reports, the statutory obligation of the staff has been fully satisfied.

13.3. Reporting to the JFIU

The MLRO should acknowledge receipt of an internal report and provide a reminder of the obligation regarding 'tipping off' (see section 14) to the reporting staff upon internal reporting.
When evaluating an internal report, the MLRO must take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the MSO concerning the entities to which the report relates. This may include:

a. making a review of other transaction patterns and volumes through connected accounts, preferably adopting an RBA rather than on a transaction-by-transaction basis;
b. making reference to any previous patterns of instructions, the length of the business relationship, and CDD and ongoing monitoring information and documentation; and
c. appropriate questioning of the customer per the systematic approach to identifying suspicious transactions recommended by the JFIU

The review process should be made on a separate form which should be archived, together with any conclusions drawn. The said report which is referred to as ''Evaluation of Internal Suspicion Report for ML/TF'' is attached as **Appendix 2** in the Manual.

If after completing the review of the internal report, the MLRO decides that there are grounds for knowledge or suspicion, he/she should disclose the information to the JFIU as soon as it is reasonable to do so after his/her evaluation is complete, together with the information on which that knowledge or suspicion is based. The relevant STR is attached to this Manual as **Appendix 3**. Dependent on when knowledge or suspicion arises, an

STR may be made either before a suspicious transaction or activity occurs (whether the intended transaction ultimately takes place or not), or after a transaction or activity has been completed.

In the case where the MLRO decides not to file an STR to the JFIU, he/she must keep proper records of the deliberations and actions taken to demonstrate he/she has acted in a reasonable manner.

In the event that an urgent reporting is required particularly when the account is part of an ongoing investigation by law enforcement agency, the MSO should indicate this in the STR. Where exceptional circumstances exist in relation to an urgent reporting, an initial notification by telephone to the JFIU should be considered.

The MSO is recommended to indicate any intention to terminate a business relationship in its initial STR to the JFIU, thereby allowing the JFIU to comment, at an early stage, on such a course of action.

An STR can be submitted by the following methods:

a. By e-reporting system, STREAMS
b. By email to: jfiu@police.gov.hk
c. By fax to: (852) 2529 4013
d. By mail, addressed to Joint Financial Intelligence Unit, GPO Box 6555 Hong Kong
e. By telephone (852) 2866 3366 (for urgent reports during office hours)

13.4. Post STR reporting

The JFIU will acknowledge receipt of an STR made by the MSO. If there is no need for imminent action, e.g. the issue of a restraint order on an account, consent will usually be given for the MSO to operate the account. If a no-consent letter is issued, the MSO should act according to the content of the letter and seek legal advice where necessary.

Filing an STR does not exempt the MSO from the legal, reputational or regulatory risks associated with the account's continued operation. The "consent" response from the JFIU to a pre-transaction report should not be construed as a "clean bill of health" for the continued operation of the account or an indication that the account does not pose a risk to the MSO.

The MSO should conduct an appropriate review of a business relationship upon the filing of an STR to the JFIU, irrespective of any subsequent feedback provided by the JFIU and apply appropriate risk mitigating measures. Filing a report with the JFIU and continuing to operate the relationship without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified, is not acceptable. If necessary, the issue should be escalated to the MSO's BOD to determine how to handle the relationship

concerned, to mitigate any potential legal or reputational risks posed by the relationship in line with the MSO's business objectives, and its capacity to mitigate the risks identified.

The MSO should be aware that the reporting of a suspicion in respect of a transaction or event does not remove the need to report further suspicious transactions or events in respect of the same customer. Further suspicious transactions or events, whether of the same nature or different to the previous suspicion, must continue to be reported to the MLRO who should make further reports to the JFIU if appropriate.

13.5. Record keeping in relation to STRs

The MSO must establish and maintain a record of all ML/TF reports made to the MLRO.

The record should include:

a. details of the date the report was made,
b. the staff members subsequently handling the report,
c. the results of the assessment,
d. whether the internal report resulted in an STR to the JFIU,
e. and information to allow the papers relevant to the report to be located.

In addition, the MSO must establish and maintain a record of all STRs made to the JFIU.

The record should include:

i. details of the date of the STR,
ii. the person who made the STR,
iii. and information to allow the papers relevant to the STR to be located.

➔ This register may be combined with the register of internal reports, if considered appropriate.

13.6. Requests from law enforcement agencies

The MSO may receive various requests from law enforcement agencies, e.g. search warrants, production orders, restraint orders or confiscation orders, pursuant to relevant legislations in Hong Kong. These requests are crucial to aid law enforcement agencies to carry out investigations as well as restrain and confiscate illicit proceeds. Therefore, the MSO should establish clear policies and procedures to handle these requests in an effective and timely manner, including allocation of sufficient resources and appointing a staff as the main point of contact with law enforcement agencies.

The MSO should respond to any search warrant and production order within the required time limit by providing all the information or material that fall within the scope of the request. Where the MSO encounters difficulty in complying with the timeframes stipulated, the MSO should at the earliest opportunity contact the officer-in-charge of the investigation for further guidance.

During a law-enforcement investigation, the MSO may be served with a restraint order, which prohibits the dealing with particular funds or property pending the outcome of an investigation. The MSO must ensure that it is able to freeze the relevant property that is the subject of the order. It should be noted that the restraint order may not apply to all funds or property involved within a particular business relationship and the MSO should consider what, if any, funds or property may be utilized subject to the law of Hong Kong.

Upon the conviction of a defendant, a court may order the confiscation of his/her criminal proceeds and the MSO may be served with a confiscation order in the event that it holds funds or other property belonging to that defendant that are deemed by the court to represent his/her benefit from the crime. A court may also order the forfeiture of property where it is satisfied that the property is terrorist property.

When the MSO receives a request from a law enforcement agency, e.g. search warrant or production order, in relation to a particular customer or business relationship, the MSO should assess the risks involved and the need to conduct an appropriate review on the customer or the business relationship to determine whether there is any suspicion and should also be aware that the customer subject to the request can be a victim of crime.

14. Prohibition of tipping off

It is an offence to reveal to any person any information which might prejudice an investigation; if a customer is told that a report has been made, this would prejudice the investigation and an offence would be committed. The tipping off provision includes circumstances where a suspicion has been raised internally within an MSO, but has not yet been reported to the JFIU.

According to UNATMO, DTROP & OSCO:

In proceedings against a person for an offence of tipping-off it is a defense to prove:

a. that he/she did not know or suspect that the disclosure concerned was likely to be prejudicial in the way referred to in that subsection; or
b. that he/she had lawful authority or reasonable excuse for making that disclosure

15. Record-Keeping:

15.1. Overview

Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps the investigating authorities to establish a financial profile of a suspect, trace the criminal or terrorist property or funds and assists the Court to examine all relevant past transactions to assess whether the property or funds are the proceeds of or relate to criminal or terrorist offences.

The MSO should maintain CDD information, transaction records and other records that are necessary and sufficient to meet the record-keeping requirements under the AMLO and other regulatory requirements, that are appropriate to the nature, size and complexity of its businesses.

The MSO should ensure that:

a. the audit trail for funds moving through the MSO that relate to any customer and where appropriate the beneficial owner of the customer, account or transaction, is clear and complete;
b. all CDD information and transaction records are available swiftly to the CCE, other authorities and auditors upon appropriate authority; and
c. it can demonstrate compliance with any relevant requirements and guidelines issued by the CCE.

15.2. Retention of records relating to CDD and transactions

The MSO should keep:

a. the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and where applicable verifying the identity of the customer and/or beneficial owner of the customer and/or beneficiary and/or persons who purport to act on behalf of the customer and/or other connected parties to the customer;
b. other documents and records obtained throughout the CDD and ongoing monitoring process, including SDD and EDD;
c. where applicable, the original or a copy of the documents and a record of the data and information, on the purpose and intended nature of the business relationship;
d. the original or a copy of the records and documents relating to the customer's account (e.g. account opening form or risk assessment form) and business correspondence with the customer and any beneficial owner of the customer (which at a minimum

should include business correspondence material to CDD measures or significant changes to the operation of the account); and

e. the results of any analysis undertaken (e.g. inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose).

All documents and records mentioned above should be kept throughout the continuance of the business relationship with the customer and for a period of at least 5 years after the end of the business relationship.

Similarly, for occasional transactions equal to or exceeding the CDD threshold (i.e. $8,000 for wire transfers and $120,000 for other types of transactions), the MSO should keep all documents and records mentioned above for a period of at least 5 years after the date of the occasional transaction.

The MSO should maintain the original or a copy of the documents, and a record of the data and information obtained in connection with each transaction the MSO carries out, both domestic and international, which should be sufficient to permit reconstruction of individual transactions, so as to provide if necessary, evidence for prosecution of criminal activity.

All documents and records mentioned in the above paragraph should be kept for a period of at least 5 years after the completion of a transaction, regardless of whether the business relationship ends during the period.

The CCE may, by notice in writing to the MSO, require it to keep the records relating to a specified transaction or customer for a period specified by the CCE that is longer than those referred above, where the records are relevant to an ongoing criminal or other investigation, or to any other purposes as specified in the notice.

Irrespective of where CDD and transaction records are held, the MSO is required to comply with all legal and regulatory requirements, especially with the Record-keeping requirements.

16. CONFLICT OF INTEREST

16.1. Overview

As a financial service provider, the MSO and its staff members face actual and potential Conflicts of Interest periodically. The MSO's policy is to take all reasonable steps to operate and maintain effective organizational and administrative arrangements to identify and manage relevant conflicts.

The BOD within the MSO is responsible for ensuring that the MSO's systems, controls and procedures are adequate to identify and manage Conflicts of Interest and the CO assists in the identification and monitoring of actual and potential Conflicts of Interest.

The MSO has in place business-specific procedures to address the identification and management of actual and potential Conflicts of Interest that may arise in the course of the MSO's business.

16.2. Objective

The MSO is required to take all reasonable steps to identify and adequately manage Conflict of Interests entailing a material risk of damage to a customer's or the MSO's interest. This Manual specifies the MSO's requirement to have in place appropriate and adequate procedures and measures in order to identify and manage any such Conflicts of Interest that may arise.

16.3. Scope

Conflicts of Interest may arise between:

- The MSO and a customer;
- A Relevant Person and a customer or the MSO;
- Two or more customers of the MSO in the context of the provision of services by the MSO to those customers;
- A services or goods provider of the MSO, the MSO and a staff member.

For the purposes of this section, customers include:

- Existing customers of the MSO; and
- Potential customers (where the MSO is seeking individually to enter into a contractual relationship in respect of Regulated Business services)

For the purposes of this Section, "Relevant Person" means any of the following:

- a director, partner or equivalent, manager or appointed representative (or where applicable, tied agent) of the MSO;
- an employee of the MSO or of an appointed representative (or where applicable, tied agent) of the MSO, as well as any other natural person whose services are placed at the disposal and under the control of the MSO or a tied agent of the MSO.

16.4. General Guidance

In identifying Conflicts of Interest, the MSO will consider all of the factual circumstances and it will take into account, inter alia, whether the MSO or a Relevant Person:

- Is likely to make a financial gain, or avoid a financial loss, at the expense of the customer or the MSO
- Has a financial or other incentive to favor the interest of a customer or group of customers over the interest of another customer.
- Has an interest in the outcome of a service provided to the customer or the MSO or of a transaction carried out on behalf of the customer or the MSO, which is distinct from the customer's or the MSO's interest in that outcome.
- Carries on the same business as the customer or the MSO and/or
- Receives or will receive from a person other than the customer or the MSO, an inducement in relation to a service provided to the customer or the MSO in the form of monies, goods or services, other than the standard commission or fee for that service.

16.5. Examples of Potential Conflicts of Interest

Within the MSO, Conflicts of Interest may arise in a variety of situations, including:

- The provision of investment research
- Proprietary trading
- Corporate finance
- Personal account dealing
- Ownership interest
- Purchase of services or goods

16.6. Identifying and Managing Conflicts of Interest

The MSO requires all staff members to disclose any actual and potential Conflict of Interest at the earliest possibility to the CO. Further, it encourages all staff members to consult the CO if there is a doubt, whether a Conflict of Interest exists.

In order for the MSO to be in a position to identify potential conflicts, material transactions involving customers, Relevant Persons or the MSO are logged internally and analyzed against existing MSO relationships and transactions.

Should a Conflict of Interest arise, it must be managed promptly and fairly. As a minimum standard, the MSO has in place arrangements designed to ensure that:

- There are effective procedures in place to control the flow of information where, otherwise, the risk of a Conflict of Interest would harm the interests of a customer;
- There are appropriate controls in place to identify and manage cross-board memberships and outside business interests of Relevant Persons;
- Relevant information is recorded promptly in a secure environment to enable identification and management of Conflicts of Interest;
- Appropriate inter- and intra-unit escalation processes are in place and are complied with where a Conflict of Interest has been identified or may be identified;
- Adequate records are maintained of the services and activities of the MSO where a Conflict of Interest has been identified;
- Where necessary, Relevant Persons may be asked to step aside from working on a specific transaction or participating in the management of a potential Conflict of Interest;
- Where necessary, Relevant Persons are subject to personal account transaction rules; and
- There is a periodic review of the adequacy of the MSO's systems and controls.

16.7. Information Barriers

The MSO respects the confidentiality of information it receives about its customers and operates a "Need to Know" approach and complies with all applicable laws with respect to the handling of that information. Access to confidential information is restricted to those who have a proper requirement for the information consistent with the legitimate interest of a customer or the MSO.

16.8. Disclosure of Conflict of Interest and Customer Consent

The MSO has procedures to protect the customer's interests from conflicts that might arise from the MSO's own activities. In certain circumstances, if permissible, disclosure will be made to an affected customer in order to seek the customer's consent to continue the provisions of services to him/her. Disclosure will be made of the general nature and/or sources of conflict to enable the customer to make an informed decision.

16.9. Personal Gifts or Other Benefits

Staff members are encouraged to limit solicitation or acceptance of gifts, hospitalities or other benefits, limited to what is generally accepted as being usual. In no case shall such solicitation or acceptance of gifts, hospitalities or other benefit lead to any disadvantage of any customer or the MSO by impairing a Relevant Person's ability to act in the best interest of the customer and/or the MSO.

Staff members may not solicit or accept gifts, hospitalities or other benefits exceeding the value of HKD 800 from any party involved in business with the MSO without declaration to and approval from the CO.

17. Termination of business relationship with customers

The MSO may terminate a business relationship with the customer, or vice versa, at any time 30 days prior by written notice to the other party. Without deviating from the aforesaid, the MSO may immediately suspend all or part of the services or terminate the establishment of business relationship, upon written notice (by fax, mail or email), at the MSO's sole discretion, if:

- The customer breaches the "Services Agreement" or "Terms of Business" or any other agreement to which customer and the MSO are parties.
- The MSO reasonably suspects or believes that the customer is using the services in connection with any unauthorized, dishonest or criminal activities or fraud.
- The customer is unable to pay its debts as and when they fall due or becomes bankrupt or insolvent, or has a receiver, or manager, provisional liquidator, liquidator or administrator appointed in respect of any material part of its assets or suffers an execution in respect of any of its property, or if a petition is presented for the winding up and such petition is not released, satisfied or withdrawn within 30 days or if customer suffers or is subject to any equivalent event, circumstance or procedure to those set out above in any other jurisdiction.
- The MSO is required to do so by any regulatory authority or agency or under the rules or applicable laws.
- Anything happens to the customer or comes to the MSO' s attention in relation to the customer or arising from or incidental to the costumer's business or the conduct of customer's business (including trading practices or individual activity) that the MSO in its sole discretion considers:
  (i) disreputable or capable of damaging the MSO's reputation;
  (ii) detrimental to the MSO's business; or
  (iii) may or does give rise to fraud or any other criminal activity or suspicion of fraud or any other criminal activity.
- Any circumstance, event or series of events that the MSO has reasonable grounds to believe materially adversely affects or may materially adversely affect the customer's ability fully and promptly to perform and comply with any one or more of its obligations, or customer's liabilities or potential liabilities under the "Services Agreement" or "Terms of Business", such circumstances and events may include:
  (i) material change in the goods and/or services supplied by the customer
  (ii)material positive or negative fluctuations month to month in customer's transaction volumes or the average value of transactions;
  (iii) occurrence of assessments;
  (iv) change of control in respect of the customer
  (v) instructions from a regulatory authority which the customer does not or is unable or unwilling to comply with; and/or
  (vi) a material deterioration in the customer's profits or financial or trading position.
- In the event of the death of the customer (where the customer is an individual)

18. Whistleblowing

18.1. Overview

Whistleblowing policies are generally intended to make it easier for staff members to be able to report irregularities in good faith, without having to fear that their action may have adverse consequences.

By creating an environment of trust and maximum protection for the members of its staff, the MSO will ensure that members of staff who report irregularities in good faith are afforded the utmost confidentiality and most effective protection possible against any retaliation or reprisals, whether actual or threatened, as a result of their whistleblowing.

The basic principles of the MSO's Whistleblowing Policy are as follows:

* Persons concerned must have a choice between a number of channels for whistleblowing and communication; in certain circumstances, they must be able to bypass the main channels for whistleblowing if these are proved to be inappropriate;
* Members of staff must not under any circumstances be subject to reprisals for whistleblowing;
* Members of staff who report incidents in good faith must be protected and their identity must insofar as possible remain confidential;
* The reported incidents shall be verified in the appropriate manner and if they are confirmed, the MSO shall take all necessary steps to identify appropriate remedies;
* The basic rights of any person implicated by the reported incidents must be respected, whilst ensuring that the procedures provided for, are effective.

18.2. Scope of this Section

This section covers all the cases and situations where the normal reporting channels (i.e. via the direct superior or otherwise main responsible) are inappropriate because either there is a conflict of interest between the matter and one or several staff that are part of the reporting chain, or because one or several staff are directly involved in inappropriate or unlawful behavior.

The MSO's Whistleblowing Policy applies to all staff members and any other person who provides services to the MSO, including consultants and other service providers under contract (grouped together for the purposes of this document under the term "staff member(s)").

18.3. Protection for Whistle-blowers

Any staff member who reports an irregularity, provided that this is done in good faith and in compliance with the provisions of this Section, shall be protected against any acts of retaliation.

For the purposes of this Section,

"retaliation" is defined as any action or threat of action which is unjustly detrimental to the whistle-blower because of his/her report including, but not limited to, harassment, discrimination and acts of vindictiveness, direct or indirect, that are recommended, threatened or taken against the whistle-blower.

“Good faith” can be taken to mean the unequivocal belief in the veracity of the reported incidents, i.e. the fact that the member of staff reasonably believes the transmitted information to be true.

Staff members who make a report in bad faith, particularly if it is based knowingly on false or misleading information, shall not be protected and shall be subject to disciplinary measures.

18.4. Protective measures

- ✓ The identity of the person reporting an irregularity will be treated in confidentiality. This means that their name will not be revealed, unless the whistleblower personally authorizes the disclosure of his/her identity or it is a statutory requirement, particularly if it is essential to ensure that the right of the persons implicated to be given a fair hearing is upheld. In such a case, the MSO shall be required to notify the whistleblower before revealing their identity.
- ✓ Where members of the staff consider that they have been the victim of retaliation for reporting an irregularity or have good reason to believe or fear that they are exposed to a risk of retaliation as a result of reporting an irregularity, they shall be entitled to complain to the BOD and request for protective measures to be adopted.
- ✓ The BOD, will assess the circumstances of the case and may decide whether temporary and/or permanent measures are necessary to be adopted with a view to protect the member of the staff in question. The staff member will be informed in writing of the outcome of this procedure.

18.5. Penalties for those taking retaliatory action

Any form of retaliation undertaken by a staff member against any person for reporting an irregularity in good faith is prohibited. In such a case, disciplinary measures shall be taken.

Members of staff will be informed of the measures taken by the MSO following the discovery of acts of retaliation for reporting an incident. The information provided will not contain any data that will enable the people concerned to be identified.

APPENDICES

APPENDIX 1:

Internal Suspicion Report for ML/TF

INFORMER'S DETAILS

Name: ..... Tel: .....
Department: ..... Fax: .....
Position: .....

CUSTOMER'S DETAILS

Name: .....

Address: .....
..... Date of Birth: …….....
Tel: ..... Occupation: .....
Fax: ..... Details of Employer: .....

……

Passport No.: .....Nationality: .....
ID Card No.: .....Other ID Details: .....

INFORMATION/SUSPICION

Brief description of activities/transaction: …….....
.....
Reason(s) for suspicion: .....
.....
Informer's Signature ……Date .....

FOR MONEY LAUNDERING REPORTING OFFICER'S USE

Date Received: ..... Time Received: ..... Ref. .....
Reported to MOKAS: Yes/No ..... Date Reported: .....Ref .....

APPENDIX 2:

Evaluation of Internal Suspicion Report for ML/TF

Reference: .....Customer's Details: .....

Informer: ..... Department: .....

INQUIRIES UNDERTAKEN (Brief Description)

.....
.....
.....
.....
.....

ATTACHED DOCUMENTS

.....
.....
.....
.....
.....

COMPLIANCE OFFICER'S DECISION

.....
.....
.....
.....
.....

FILE NUMBER.....

COMPLIANCE OFFICER'S SIGNATURE DATE

……..…… ……

APPENDIX 3:

MLRO's STR to the JFIU

Reporting Institution

舉報機構

Name of the Institution

機構名稱 _____

Correspondence Address
通訊地址 _____

Phone Number _____ Fax Number _____

電話號碼 _____ 傳真號碼 _____

Business (e.g. Banks, Securities, etc)

業務(例如銀行、證券等) _____

Compliance Officer 1

執行規定人員1

Name of the Institution

機構名稱

English Name in Full _____

英文姓名（全寫）

Chinese Name in Full _____

中文姓名（全寫）

Phone Number _____ Post _____

電話號碼 _____ 職位 _____

Email Address

電郵地址 _____

Public key eCert (Organizational, x.509, .cer) from the Hongkong Post Office

香港郵政發出的公開密碼匙(以.cer 副檔名儲存的X.509證書(機構))

Compliance Officer 2

執行規定人員2

Name of the Institution

機構名稱

English Name in Full

英文姓名（全寫）

Chinese Name in Full

中文姓名（全寫）

Phone Number

電話號碼

Post

職位

Email Address

電郵地址

Public key eCert (Organizational, x.509, .cer) from the Hong-kong Post Office

香港郵政發出的公開密碼匙(以.cer 副檔名儲存的X.509證書(機構))

Note: Should institutions wish to register more than two Compliance Officers, please copy this sheet and mark their sequence order.

註：如機構有意為兩名以上的執行規定人員登記，請再行列印本表格並在“執行規定人員”後依次填上數字，以表示人員數目。

Web-Login Officer 1

網上登入人員1

Name of the Institution
機構名稱 _____

English Name in Full
英文姓名（全寫） _____

Chinese Name in Full
中文姓名（全寫） _____

Phone Number 電話號碼 _____ Post 職位 _____

Email Address
電郵地址 _____

Web-Login Officer 2

網上登入人員2

Name of the Institution
機構名稱 _____

English Name in Full
英文姓名（全寫） _____

Chinese Name in Full
中文姓名（全寫） _____

Phone Number 電話號碼 _____ Post 職位 _____

Email Address

電郵地址

_____

Note: Should institutions wish to register more than two Web-Login Officers, please copy this sheet and mark their sequence order

註： 如機構有意為兩名以上的網上登入人員登記，請再行列印本表格並在“網上登入人員”後依次填上數字，以表示人員數目。

APPENDIX 4

Annual report

The Annual Report prepared by the CO should as minimum contain the following:

a. General description of the business operations/model of the MSO during the last year, mentioning the products/services offered, countries where it operates, possible changes to the operations and/or structure or the introduction of new products, services, technological developments that affected the procedures and controls for ML/TF.
b. Information on the measures taken and/or procedures introduced to comply with any amendments and/or new provisions of the Law during the year under review.

c. Information on the audits and inspections carried out by the CO and Internal Audit stating the number of audits carried out, at which departments/lines of business and the significant deficiencies and weaknesses identified in the policy and procedures applied by the MSO to prevent ML/TF. In this respect, the seriousness of the omissions or weaknesses, the risks involved and the actions and/or suggestions made for corrective measures to improve the situation should be highlighted.
d. Information on audits carried out by the CED, indicating any deficiencies and weaknesses identified, the risks involved as well as the corrective measures and actions taken or undertaken to improve the situation.
e. Information on the procedures and the automated/electronic information systems applied by the MSO for the ongoing monitoring of the accounts and transactions of their customers by describing their main functions, the time of their operation (e.g. in real time or after the completion of the transaction), the weaknesses that occurred, and the results of their operation during the year under review, such as the total number of alerts generated by the system, number of internal reports submitted to JFIU as a consequence of these alerts, number of false-positives alerts, increases/decreases in comparison with the previous year, any identified trends etc.
f. The number of internal suspicion reports of ML/TF submitted by the MSO's staff to the MLRO, citing summary data by region, address and branch as well as any comments and observations.
g. The number of suspicion reports submitted by the MLRO to JFIU and summary data/information of the main reasons for the suspicions and any trends observed.
h. The number of suspected transaction cases investigated by the MLRO, but no suspicion report has been submitted to JFIU.
i. Information regarding circulars and other communication with staff on issues for the prevention of ML/TF.
j. Summary data for the type (natural or legal persons) and size of the customer base during the last year, the number of customers per risk category, the number of new customers, the number of persons (prospective customers) with whom the establishment of business relationship was not allowed for compliance reasons, the number of customers with whom the business relationship was terminated for compliance reasons, the number of frozen accounts following a court order/JFIU and the increase/decrease percentage of the above compared to the previous year.
k. Information on the policy, procedures and controls applied by the MSO in relation to high risk customers with whom a business relationship is maintained. Additionally, the number of high risk customers with whom the MSO has a business relationship, per category and country of origin of the customer and the Beneficial owner should be submitted.
l. Data for branches/subsidiaries of the MSO that operate in third countries and also the information on the measures taken for the compliance of branches/subsidiaries of the MSO with the provisions of this Manual in relation to customer identification, due diligence measures and record keeping procedures, as well as comments and information on the level of their compliance with these requirements.

m. Information on the training seminars attended by the CO and MLRO and on any other educational material received.
n. Information on training/education provided to staff during the year, reporting:
    - The number of courses/ seminars organized,
    - their duration,
    - the number of staff attending, specifying their seniority i.e. management staff, officers, clerical staff or newcomers etc,
    - name(s) and qualifications of the instructor(s),
    - whether the course/seminar was developed internally by the MSO or by an external organisation/consultant, and
    - summary information for the program/content of the courses/seminars.
o. Information for next year's training plan.
p. Results of the assessment of the adequacy and effectiveness of staff training.
q. Information on the structure and staffing of the Anti-Money Laundering and Compliance's Unit as well as recommendations for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against ML/TF.
r. Copy of the register with the data and information (e.g. name, business address, business area, supervisory authority, date of commencement of cooperation, review date and results of the assessment of customers recommended, number of customers that he/she introduces to the MSO, number of customers that were reported to JFIU) on third parties with whom the MSO has established cooperation and also information for third parties that the MSO has rejected.
s. Information on the policy, procedures and controls applied by the MSO for its compliance with sanctions and restrictive measures, as well as summary data on frozen accounts (e.g. number of frozen accounts, reasons for freezing and total amount).
t. An overall assessment of the effectiveness of the systems and controls, adequacy of resources and also areas likely to be equivalent to breaches of the legal and regulatory framework, describing in order of priority the actions for correction/prevention considered necessary and the expected deadline for completion.