CITY FOREIGN EXCHANGE LIMITED

HONG KONG

Anti-Money Laundering Guidelines

January 2016

AML Guidelines adopted by City Foreign Exchange Ltd (2013)

POLICY STATEMENT AND DECLARATION

ON

ANTI - MONEY LAUNDERING AND COUNTER – TERRORIST FINANCING

COMPANY NAME: CITY FOREIGN EXCHANGE LIMITED

ADDRESS: UNITS A-B, 13/F, CENTURY HOUSE, 3-4 HANOI ROAD

TSIM SHA TSUI, KOWLOON, HONG KONG

TELEPHONE: 23667725

FAX: 23669930

EMAIL: info@citygroupintl.com

MSO LICENSE NO.:12-06-00214

COMPANY STRUCTURE: CORPORATION (LIMITED COMPANY)

NATURE OF MONEY SERVICE: MONEY CHANGING AND REMITTANCE SERVICE

NUMBER OF STAFF EMPLOYED: 26

CUSTOMER PROFILE:

CORPORATE CUSTOMERS

INDIVIDUAL CUSTOMERS

CUSTOMER OF SAME SECTOR

CUSTOMRS FROM PASSING TRADE

ID REQUIREMENT: ALL THE CUSTOMERS MUST PRESENT VALID PHOTO ID/TRAVEL DOCUMENT

PURPOSE AND SCOPE

CITY FOREIGN EXCHANGE LIMITED takes adequate measures to ensure that proper safeguards exist to mitigate the risks of Money Laundering and Terrorist Financing and to prevent a contravention of any requirement under the Anti-Money Laundering and Counter – Terrorist Financing (Financial Institutions) Ordinance, Chapter 615, Laws of Hong Kong (AMLO) and the related Guideline on AML and CTF.

CITY FOREIGN EXCHANGE LIMITED establishes and implements adequate and appropriate AML and CTF Policies, Procedures and Controls considering all factors like types of Customers, Products and Services offered and Geographical Locations involved.

RESPONSIBILITIES

The senior management of CITY FOREIGN EXCHANGE LIMITED undertakes the assessment of the risks faced and manages the Money Laundering and Terrorist Financing risks thereby ensuring that all relevant staff are trained and made aware of the law and obligations under the same.

We have appointed a Compliance Officer, Mr. Dheeraj BAJPAI to act as a focal point for over viewing all activities related to the prevention and detection of Money Laundering and Terrorist Financing and to provide support andguidance to the Senior Management to ensure that Money Laundering and Terrorist Financing Risks are adequately managed.

We have appointed a Money Laundering Reporting Officer (MLRO) Mr. Senthil DHARMARAJ as a central reference point for reporting of suspicious transactions to the Joint Financial Intelligence Unit of the Hong Kong Police Force. The MLRO receives complete cooperation and support from all staff and is an IT specialist with full access to all relevant documentation which enables him to perform his functions diligently.

Our Company also adopts appropriate measures through training and other communication methods, to let the frontline staff know the responsible areas to judge whether a transaction is suspicious and to report the same promptly to the Compliance Officer or the MLRO.

RISK IDENTIFICATION AND ASSESSMENT

CITY FOREIGN EXCHANGE LIMITEDapplies a risk based approach with regard to Types and Behavior Characteristics of Customers and their Profile, Products and Services offered and the related delivery channels and Customers' Business Organization and their locations involved as per **Annexure 1**

CUSTOMER DUE DILIGENCE, RECORD KEEPING AND ONGOING MONITORING

Our Company strives to carry out CDD and apply the CDD measures as per AML Guideline Chapter 4.1.9, 4.1.3 and Chapter 11.

Our Company also adopts appropriate controls to determine the extent of Due Diligence to be performed and the level of Ongoing Monitoring to be applied as per AML Guideline Chapter 3.2.

Our Company also monitors the business relationship with our customers under conditions stated in the AML Guideline Chapter 5.1.

CITY FOREIGN EXCHANGE LIMITED also in complying with the AML Guideline Chapter 8.3-8.6 keeps the documents obtained in the course of identifying and verifying the identity of the customer and maintains the documents obtained in connection with the transaction for a period of six years.

AML/CTF TRAINING TO STAFF

CITY FOREIGN EXCHANGE LIMITED provides training in AML/CTF to all relevant staff (including new staff) in order that they are made aware of the AMLO and are in a position to recognize suspicious transactions/activities.

This training is in the form of providing an updated AML Manual to every employee in the form of a soft copy on their respective computer terminals for their easy reference at any given point of time. Any new information is disseminated in the form of emails to the respective staff.

The Company also tied up with Thomson Reuters and provides the AML E-learning course for its employees ending with an evaluation. Our Company keeps the training records/records of relevant courses or seminars attended for inspection by the regulator.

SUSPICIOUS TRANSACTION REPORTING

Our Company gives on an ongoing basis sufficient guidance to all relevant staff to enable them to take appropriate actions when they detect any suspicious transaction or activity. These activities/transactions are escalated to the Compliance Officer/ MLRO and along with the ongoing monitoring process, STR s are reported to the JFIU, Hong Kong.

INTERNAL MONITORING SYSTEM AND PERIODICAL REVIEW

CITY FOREIGN EXCHANGE LIMITED undertakes regular assessments of the systems and controls in place to ensure that AML and CTF risks are mitigated and the company is compliant with the AMLO and the AML guideline.

The Company also reviews the AML and CTF policies and procedures regularly and assesses that risk mitigation procedures and controls are working effectively.

MONEY CHANGERS ORDINANCE

CITY FOREIGN EXCHANGE LIMITED operates the Money Changing Business according to the provisions of the Money Changers Ordinance, Chapter 34 Laws of Hong Kong

PERSONAL DATA (PRIVACY) ORDINANCE

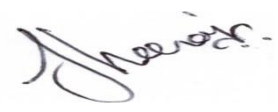
CITY FOREIGN EXCHANGE LIMITED protects the privacy of the customer/individual with respect to personal data collected and uses the personal data only for which the same was originally collected OR a directly related purpose UNLESS the subject of the data has given a prior consent. This is in accordance with the Personal Data (Privacy) Ordinance, Chapter 486 of the Laws of Hong Kong.

COOPERATION WITH REGULATOR AND LAW ENFORCEMENT AGENCIES

CITY FOREIGN EXCHANGE LIMITED has and will cooperate with the Customs and Excise Department with regard to their routine inspection or investigation. The Company also cooperates with other law enforcement agencies as and when required under the laws of Hong Kong.

CITY FOREIGN EXCHANGE LIMITED implements the above Policies, Procedures and Controls to mitigate the risks of Money Laundering and Terrorist Financing.

For CITY FOREIGN EXCHANGE LIMITED.



Name of signatory: DHEERAJ BAJPAI

Designation: MANAGER – Compliance and Operations

Date: January 13, 2016

1. Introduction

1.1 The Financial Action Task Force (FATF) is an inter-governmental body formed in 1989 that sets the international anti-money laundering and counter financing of terrorism (AML) standards. Its mandate was expanded in October 2001 to combat the financing of terrorism.

1.2 Hong Kong as a member of FATF is obliged to implement the AML requirements as promulgated by FATF from time to time. And since June 2003, remittance and money exchange providers have also been classified as "financial institutions" (FI) by FATF and now therefore subject to the same requirements in terms of AML measures as banks, deposit-taking companies and other traditionally regulated financial institutions.

1.3 As a result of the FATF review in 2008, Hong Kong has been subject to FATF's follow-up process and is required to report to FATF on actions taken or planned to address the deficiencies identified in the evaluation made by FATF. The FATF is scheduled to evaluate again in 2015-2016.

1.4 The new guideline is published under section 7 of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Cap. 615 (the AMLO).

1.5 This Guideline is issued by the Commissioner of Customs and Excise (CCE) for giving guidance to money service operators (MSOs).

The purpose of the Guidelines is to:

(a) provide a general background on the subjects of money laundering and terrorist financing (ML/TF), including a summary of the main provisions of the applicable anti-money laundering and counter-financing of terrorism (AML/CFT) legislation in Hong Kong; and

(b) provide practical guidance to assist FIs and their senior Management in designing and implementing their own policies,procedures and controls in the relevant operational areas, taking intoconsideration their special circumstances so as to meet the relevant AML/CFT statutory and regulatory requirements

1.6 The relevance and usefulness of the Guideline will be kept underreview and it may be necessary to issue amendments from time to time.

2. What is Money Laundering?

2.1 Money Laundering is a transaction or a series of transactions effected with the aim to conceal or change the identity of criminal proceeds, so that the money, after such processing, will appear to have originated from a legitimate source.

2.2 The act of money laundering therefore covers all procedure to change, obscure or conceals the ownership or audit trail of illegally obtained money or property.

2.3 The statutory definition of "money laundering activities" is as below:

"Activities intended to have the effect of making any property:

(a) Which is the proceeds obtained from the commission of an offence under the laws in Hong Kong, or of any conduct which if occurred in Hong Kong would constitute an offence under the laws of Hong Kong; or

(b) which in whole or in part, directly or indirectly, represents such proceeds,

not to appear to be or so represent such proceeds.

2.4 Proceeds of many crimes are often generated in the form of cash. Cash is the commons medium of exchange in the world of drug trafficking and organized crime. However, not all criminal offencesinvolve cash. There are just as many criminal offences that do not involve cash, such as fraud, false accounting and tax evasion.

2.5 The key stage for the detection of money laundering operations is where the cash first enters the financial system. There are 3 common stages of money laundering during which or any one of which there may be numerous transactions that could be a hint to criminal activity. Although it is important to remember that the 3 stages may help to explain the process, in the real world, all 3 stages could take place at the same time.

2.6 The 3 common stages of money laundering:

(a) **Placement** – the disposal of criminal proceeds derived from illegal activity into financial system;

(b) **Layering** – separating the criminal proceeds from their original source by creating complex layers of financial transactions in order to disguise the audit trail and obscure the origin of the funds and provide anonymity;

(c) **Integration** – if the layering process has succeeded, the criminal proceeds will go back to the financial system as legitimate funds and assets.

2.7 In any event, no matter what the criminal may do, the criminal may want to achieve 3 things:

(i) **Conceal** the true ownership of the money and where it came from;

(ii) **Keep control** of the money, and

(iii) **Change** its form

2.8 Criminals therefore can make use of the services provided by anotherCompany in order to:

- Convert money from one currency to another, and/or
- Transfer money from one country to another,

in the hope that this will make it difficult for investigators to trace.

3. What is Terrorist Financing?

3.1 Terrorist financing generally covers the carrying out of any transaction that involve funds owned by terrorists, or that have been, or are intended to be, used to facilitate the commission of terrorist acts.

3.2 Similar to money laundering, terrorist financing also aims at disguising the origins of funds, but its focus is on the directing of fund, whether legitimate or not, to terrorists. In terrorist financing, the key fact is on the destination or use of funds, which may have been derived from legitimate sources.

3.3 Although terrorist groups earn money from crimes, they may also receive money in the form of apparently legitimate donations, and this is further complicated because people donating the money might not know they are giving money to a terrorist group, they might think they are donating to a charity.

3.4 Likewise, this money may be sent overseas by using the services of a similar Company. We should be able to identify and report transactions with terrorist suspects.

3.5 We should ensure that we maintain a database of names and particulars of terrorist suspect (which may include lists of terrorists, terrorist organizations, their agents and terrorist property) that have been made known to us. Alternatively, we may arrange to secure access to such a database maintained by reliable third party service providers.

3.6 The aforesaid database should include the lists published in the Gazette (The list of designated terrorists is published in the Gazette regularly) and those designated under the US Executive Order of 23rd of the September 2001. The said database should be subject to timely updates regularly whenever there are changes, and should be easily accessible by staff to check the names of both existing and new customers against the names in the database.

4. Legislation on Money Laundering and Terrorist Financing

Legislation on Money Laundering;

4.1 Hong Kong, China as a member of the FATFis required to be fully compliant to the 40 Recommendations and 9 Special Recommendations of FATF. Local legislation in Hong Kong as result has been developed to address the problems associated with laundering of proceeds from drug trafficking, serious crimes and terrorist financing.

4.2 Since June 2003, remittance and money exchange providers have been classified by the FATF as "financial institutions" and now therefore all Money Service Operators are subject to the same requirements in terms of anti-money laundering and counter terrorist financing measures as banks, deposit-taking companies and the other traditionally regulated financial institutions.

4.3 Hong Kong has given effect to FATF Recommendations by way of 4 statutes. These 4 main Ordinances form the Hong Kong law relating to money laundering and terrorism. They are:

1. The Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Cap. 615 (the AMLO)
2. The Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) (DTRPO);
3. The Organized and Serious Crimes Ordinance (Cap. 455) (OSCO); and

4. The United Nations (Anti-Terrorism) Measures Ordinance (Cap. 625) (UNATMO)

4.4 The AMLO imposes requirements relating to customer due diligence (CDD) and record-keeping on FIs and provides the Relevant Authorities(RA's) with the powers to supervise compliance with these requirements and other requirements under the AMLO. In addition, section 23 of Schedule 2 requires FIs to take all reasonable measures (a) to ensure that proper safeguards exist to prevent a contravention of any requirement under Parts 2 and 3 of Schedule 2; and (b) to mitigate ML/TF risks

(a) The AMLO makes it a criminal offence if an FI (1) knowingly; or (2) with the intent to defraud any RA, contravenes a specified provision of the AMLO. The"specified provisions" are listed in section 5(11) of the AMLO. If the FI knowingly contravenes aspecified provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million.If the FI contravenes a specified provision with the intent to defraud any RA, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.

(b) The AMLO also makes it a criminal offence if a person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI (1) knowingly; or (2) with the intent to defraud the FI or any RA, causes or permits the FI to contravene a specified provision in the AMLO. If the person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FIknowingly contravenes a specified provision he is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If that

person does so with the intent to defraud the FI or any RA he is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.

(c) RAs may take disciplinary actions against FIs for any contravention ofa specifiedprovision in the AMLO. The disciplinary actions that can betaken include publicly reprimanding the FI; ordering the FI to take anyaction for the purpose of remedying the contravention; and ordering the FI to pay a pecuniary penalty not exceeding the greater of $10 million or three times the amount of profit gained, or costs avoided, by the FI result of the contravention.

4.5 Section 25(1) of DTRPO and OSCO sets out the principal offence of money laundering. DTRPO came into force in September 1989. It provides for the tracing, freezing and confiscation of the proceeds of drugs trafficking and creates the criminal offence of money laundering in relation to such proceeds.

4.6 OSCO which was modeled on the DTRPO was brought into operation in December 1994. It extends the money laundering offence to cover the proceeds of all "indictable offences" listed out in Schedules 1 &2 of the Ordinance.

4.7 The same section numbers in DTRPO and OSCO refer to the same offences. For practical purposes, it is sufficient to remember and to concentrate on OSCO which covers all serious crimes there is no need to remember that there are 2 ordinances as they are mirror images of each other and the only difference is that DTRPO focuses attention on drug trafficking.

4.8 There are 2 aspects of the law relating on money laundering that you must know:

(a) **Dealing Offence** – it is a criminal offence to deal with money or other property that is the proceeds of a predicate crime;

(b) **Reporting Obligation** – there is an obligation to make a report if you know or suspect that any property is the proceeds of a predicate crime

4.9 Section 25(1) of DTRPO and OSCO creates the offence of **dealing with any property**, knowing or **having reasonable grounds to believe** it in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence respectively. These offences carry a maximum sentence of 14 years' imprisonment and a maximum fine of HK$5 million.

4.10 "**Dealing**" is defined under Section 2 of DTRPO and OSCO to include:-

(a) Receiving or acquiring the property;

(b) Concealing or disguising the property (whether by concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect of it or otherwise);

(c) Disposing of or converting the property;

(d) Bringing into or removing from Hong Kong the property;

(e) Using the property to borrow money, or as security (whether by way of charge, mortgage or pledge or otherwise)

4.11 This covers such a wide range of activities and it is not necessary for you to know that the money or other property is actually the proceeds of a crime, it is sufficient if you have "reasonable grounds to believe".

4.12 The definition of "**indictable offence**" includes something that might have taken place outside Hong Kong, and even if the principal crime is not committed in Hong Kong provided that it would constitute an indictable offence if it had occurred in Hong Kong.

For example, if someone committed a fraud in China and the money was transferred in Hong Kong, dealing with that money in Hong Kong would

be money laundering. There is no need to check the laws in mainland China to find out if that is or is not an offence there. It is sufficient that it would have been an offence if it had taken place in Hong Kong.

4.13 It also covers, for example, the situation where a money remittance business in Hong Kong might accept funds from a local customer to be paid to somebody abroad, and the money was actually going to be used for a criminal purpose – e.g. paying a bribe to a foreign government official. Likewise, it is not necessary for you to be concerned about whether or not a payment of bribe is technically a criminal offence in that country. Suffice to say that, if such act had taken place in Hong Kong, it would be an indictable offence.

4.14 **The Reporting Obligation-**It is the statutory duty of a person, who **knows** or **suspects** that any property in whole or part directly or indirectly represents the proceeds of drug trafficking, or of an indictable offence respectively or was or is intended to be used in that connection with, to make a disclosure to an authorized officer.

4.15 **It is also a criminal offence not to make a report** under section 25A (1) when you should do so. These offences carry a maximum sentence of 3 months' imprisonment and a maximum fine of HK$50,000.

4.16 None of the ingredients necessary for the offence, namely "Knowing", "Belief" and "Suspicion" is defined in the DTRPO and OSCO. We therefore need to turn to case law.

4.17 "Knowing" in Section 25(1) of DTRPO and OSCO, will mean the alleged offenders' knowledge that the property he is dealing with represents the proceeds of drug trafficking or an indictable offence.

4.18 The objective element is the existence of grounds that a common-sense, right-thinking member of the community would consider are sufficient to establish a belief. The subjective aspect is that the alleged offender knew of those grounds.

4.19 Applying this view, a person would commit Section 25(1) offence if he deals with property in respect of which there are grounds, which he knows of and which any common-sense, right-thinking member of the community would say are sufficient to form the belief that the property concerned represents the proceeds of an indictable crime. It is not necessary that he should actually believe that the property represents theproceeds of a crime.

4.20 The prosecution needs to prove only that the alleged offender had reasonable grounds to believe that the property represented criminal proceeds. For example, the offender may believe it was money from drug trafficking but in fact it was money from tax evasion in Mainland China.

4.21 A suspicion that something exists is more than a mere idle wondering whether it exists or not; it is a positive feeling of actual apprehension or mistrust, amounting to a "slight opinion, **but without sufficient evidence**".

4.22 So "suspicion" is something more than speculation. There must be some degree of satisfaction (not necessarily amounting to belief), that an event has occurred. Knowledge or suspicion of the exact nature of the underlying criminal activity is not required. Therefore, it is important to remember the word "suspects" – there is no need to have a sufficient proof or evidence before making a report- Mere suspicion which is subjective is sufficient to make a report. So the test for "suspicion" would be subjective, i.e. whether the person concerned had the suspicion.

4.23 As a result, if any person knows (or just suspects) that a particular transaction is connected to a serious offence and he/she does not report it, he/she have committed an offence just by staying silent.

4.24 Section 25A(3) of DTRPO and OSCO provides that disclosures made under Section 25A (1) shall not be treated as a breach of contract or of any enactment restricting disclosure of information, and shall not render the person making the disclosure liable in damages for any loss arising out of

disclosure. Therefore, neither your company nor any individual member of staff can be sued by an unhappy customer because a report was made about the customer, and we need not be afraid that by making a report under the Ordinances, it will breach the duty of confidentiality owed to customers.

4.25 However, we are reminded not to tip off the person/customer under investigation after a report was made under the Ordinances. A "tipping-off" offence is created under Section 25A(5) of DTRPO and OSCO, under which a person commits an offence if knowing or suspecting that a disclosure has been made, he/she discloses to any other person any matter which is likely to prejudice an investigation into money laundering activities.

4.26 For this reason, it is vital and important that once any member of staff becomes suspicious about any customer or any transaction, they report the matter to the Compliance Officer in the Company, and **do not** discuss the matter with anyone else. They should not tell anyone else inside the Company, if anyone else needs to know, it is up to the Compliance Officer of the Company to inform them. When talking to a customer, a staff must never give them any reason to think that they might have been reported.

4.27 The maximum penalty for "tipping off" is 3 years imprisonment and a fine of HK$500,000.00.

4.28 Section 24 of DTRPO and Section 7 of OSCO make it an offence if any person, who knows or suspects that an investigation by the authorities is taking place or about to take place, prejudices the investigation by disclosing it.

4.29 There are, however, some differences in the ingredients that constitute the offence, and also in the punishment provisions. Under Section 24 of DTRPO, it is disclosure which is **likely to prejudice** the investigation but under Section 7 of OSCO, the person making the disclosure should do so with the **intention to prejudice** the investigation.

4.30 Section 24 of DTRPO does not require any intention for making the disclosure. So long as it can be shown that the disclosure could prejudice the investigation, the offence will be made out. Whereas, for making out the offence under Section 7 of OSCO, the offender should make the disclosure with the purpose of thwarting the investigation.

Legislation on Terrorist Financing:

4.31 The United Nations Security Council (UNSC) has passed various resolutions to require sanctions against designated terrorists and terrorist organizations. In Hong Kong, regulations issued under the United Nations (Sanctions) Ordinance give effect to these UNSC resolutions.

4.32 The United Nations (Anti-Terrorism Measures) Ordinance ("UNATMO") was enacted on 12th July 2002. This Ordinance adds to the legislation on Terrorist Financing in 2 significant ways:

- It makes it **illegal to supply of funds** to any terrorist organization; and
- It requires a person **to make a report** if the person knows or suspects that any account, any transaction or any property is connected to **terrorism** in any way.

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

4.34 Lists of known terrorist entities and individuals are disseminated by the United Nations and this is incorporated into the local law in Hong Kong. A list of terrorist names will be published in the Gazette from time to time. A more comprehensive list is maintained by the US Treasury Office of Foreign Assets Control (OFAC) black list.

5. The Requirement to be a Money Service Operator

5.1 The Commissioner of Customs and Excise (CCE) is the relevant authority for regulating the money service operators (MSO) with effect from 1 April 2012. Relevant powers are provided under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Chapter 615 (AMLO).

5.2 Any person operating a money service is required to be licensed with the Commissioner of Customs and Excise (CCE). It is an offence to operate a money service in Hong Kong without a license.

The responsible officer and departmentare;

The Customs and Excise Department (C&ED),
Money Service Supervision Bureau,Customs and Excise Department,
13/F, Customs Headquarters Building,
222 Java Road, North Point,Hong Kong

5.3 Under section 30(3) of the AMLO, the CCE may grant or renew a licenses to an applicant to operate a money service only if the CCE is satisfied that

(a) where the applicant is an individual, the individual and each ultimate owner is a fit and proper person to operate a money service;

(b) where the applicant is a partnership, each partner and each ultimate owner in the partnership is a fit and proper person to operate a money service;

(c) where the applicant is a corporation, each director and each ultimate owner of the corporation is a fit and proper person to be associated with the business of operating a money service;

5.4 The application form can be obtained from or downloaded from C&ED's website atwww.customs.gov.hk

6. Basic Policies and Principles required of Money Service Operators.

To ensure compliance, theCompany should have in place the following policies, procedures and controls:

(a) TheCompany should fully commit to establish appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and fully comply to existing regulatory requirements; Such policies and procedures should be communicated and applicable to all levels of staff within the Company and reviewed regularly for the purpose of ensuring its up-to-date and effectiveness;

(b) TheCompany should have office manuals setting out procedures for:

- Accounting opening;
- Client Identification;
- Record Keeping; and
- Reporting of Suspicious Transactions

(c) TheCompany should appoint a primary contact person (usually a compliance officer) within the organization and such person should have sufficient seniority and experience to which staff are instructed to report suspected money laundering or terrorist financing transactions to him/her;

(j) TheCompany should closely cooperate with law enforcement agency whenever possible;

(k) TheCompany should undertake to ensure that all staff are familiar with and maintain sufficient level of awareness of local regulations and requirements for the prevention of money laundering and terrorist financing by providing training both as part of their induction procedures and at regular future intervals.

(l) TheCompany should instruct their internal audit to check regularly the compliance of the Company's policies and procedures for the prevention of money laundering and terrorist financing, and where circumstances permit, instruct outside consulting firm to conduct an independent annual review to evaluate the effectiveness of the compliance officer, the adequacy of management monitoring of unusual transactions, the quality of reporting of suspicious transactions, and the level of awareness of front line staff of their responsibilities.

6.01 Customer DueDiligence:

(a) The AMLO defines what CDD measures are as mentioned in B below and alsoprescribes the circumstances in which an FI must carry out CDD. As indicated in the AMLO, FIs may also need to conduct additional measures (referred to as Enhanced Due Diligence (EDD) hereafter) or could conduct Simplified Due Diligence(SDD)dependingonspecific circumstances.This chaptersets out the expectations of RAs in this regard and suggests ways thattheseexpectations may be met.Whereverpossible, the guideline gives FIs adegree of discretion in how they comply with the AMLO and put in place procedures for this purpose. CDD information is a vital tool for recognizing whether there are grounds for knowledge or suspicion of ML/TF.

(b) Thefollowing are CDD measures applicable to an FI:

1. Identify the customer and verify the customer's identity usingreliable, independent source documents, data or information (see Point 6.2 (A));

2. where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity so that the FI is satisfied that it knows who the beneficial owner is, including in the case of a legal person or trust, measures to enable the FI to understand the ownership and control structure of the legal person or trust (see Point 6.2(B));
3. obtain informationon the purposeandintended natureofthebusinessrelationship (if any) established with the FI unless the purpose and intended nature are obvious; and
4. if a person purports to act on behalf of the customer;identify the person and take reasonable measures verify the person's identityusing reliableandindependentsource documents,data orinformation; andverify the person's authority to acton behalf of the customer

(c) CDD requirements should apply;at the outset of a business Relationshipbeforeperforming anyoccasional transaction equalto orexceedingan aggregate value of$120,000,

1. whether carried out in a single operation or several operations that appear to the FI to be linked; or
2. 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 FI to be linked;
3. When the FI suspects that the customer or the customer's account is involvedinML/TF; or
4. when the FI doubts the veracity or adequacy of anyinformation previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

(d) FIsshouldbevigilanttothepossibilitythataseriesoflinkedoccasionaltransactions couldmeetorexceedtheCDDthresholdsof$8,000forwiretransfers&$120,000/-for other types oftransactions.Where FIsbecomeaware that these thresholds are met or exceeded,full CDD procedures must be applied.Aftera business relationship is set up, the Company should conduct regular checks and reviews of the existing records of the customer to ensure that they remain up-to-date and relevant.

6.02 Customer Identification & Verification

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

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

(i) 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 traveldocuments for the purpose of identity verification:

(a) Permanent Resident Identity Card of Macau SAR;

(b) Mainland Travel Permit for Taiwan Residents;

(c) Seaman's Identity Document (issued under and in accordance with theILOConvention/Seafarers Identity

DocumentConvention 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 OfficialPurposes; and

(g)Exit-entry Permit for Travelling to and from Hong Kong

and Macau

(ii) 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 aminor, the identity of the minor's parent or guardianrepresenting or accompanying the minor should also berecorded and verified in accordance with the aboverequirements.

(iii) Take down the name, date of birth, nationality, current residential address (supported by documentary proof e.g. recent utility bill or bank statement), telephone, facsimile number (if any), e-mail address;

(a) Obtain original identification documents like identity card OR passport as mentioned above (insist on documents with photograph);

(b) Make copies of the original of the documents and make a note in the copies that they are copies of the originals, the date the copies were made and name of the person who made the copies;

(c) Look out for discrepancies and clarify them.

(iv) It is appreciated that no form of identification can be fully guaranteed as genuine or representing correct identity. The Company is expected to demonstrate a reasonable level of diligence in this respect. If there is any doubt as to validity of an identity card, assistance should be sought through the Hotline run by The Immigration Department (Tel: 2824 1551).

(v) A Hong Kong resident should always carry a Hong Kong Identity Card and should not use a Foreign Passport as a means of identification. Unwillingness of the customer, for no good reason, to provide the information requested and to cooperate with the customer due diligence process, may itself be a factor that should trigger suspicion. **If a customer refuses to provide identification document for verification, the transaction should be refused**

B. Identification and verification of a beneficial owner:

(i) Abeneficialownerisnormallyanindividualwhoultimatelyownsor controlsthe customeroronwhosebehalfatransactionoractivityis beingconducted. Inrespect ofacustomerwhoisanindividualnot actinginanofficialcapacityonbehalfofa legalpersonortrust,the customerhimselfisnormallythebeneficialowner. Thereis no requirementonFIstomakeproactivesearchesforbeneficialownersin sucha case,buttheyshouldmakeappropriateenquirieswherethereare indicationsthatthe customer isnot acting on his own behalf

(ii) FIs should identify all beneficial owners of a customer. In relation to verification of beneficial owners' identities, except where a situation of

High Risk referred to in section 15 of Schedule 2 exists, the AMLO requires FIs to take reasonable measures to verify the identity of any beneficial owner owning or controlling 25% or more of the voting rights or shares, etc. of a corporation, partnership or trust. In high risk situations, the threshold for the requirement is 10%.

(iii) For beneficial owners, FIs should obtain the residential address (and permanent address if different) and may adopt a risk- basedroach to determine the need to take reasonablemeasures to verifythe address, taking account of the number of beneficial owners, the nature and distribution of the interests in the entity and the nature and extent of anybusiness,contractual or family relationship.

C. Identification and verification of a person purporting to act on behalf of theCustomer:

(i) Ifa person purports to act on behalf of the customer, FIs must:

(a) identifythepersonandtakereasonable measurestoverifytheperson'sidentity on the basis of documents, data or information provided by-

1. a governmental body;
2. the relevant authority or any other relevant authority;
3. an authority in a place outside Hong Kong that performs functions similar to those of the relevant authority or any other relevant authority; or
4. any other reliable and independent source that is recognized by the relevant authority; and
5. verify the person's authority to act on behalf of the customer

(ii) FIsshould obtain writtenauthoritytoverify thattheindividual purporting to representthe customer is authorized to do so.

(iii) FIs may on occasion encounter difficulties in identifying and verifying signatoriesofcustomersthat may have long lists ofaccountsignatories particularly if such customers are based outside HongKong.Insuch cases,FIs may adopt a risk-based approach in determining the appropriatemeasurestocomplywith theserequirements; For example in respect of verification of accountsignatories related to a customer,such as an FI ora listedcompany,FIscould adopt a more streamlined approach.The provision of asignatory list,recording the names of the account signatories, whose identities andauthority to act have been confirmed by a department orperson within that customer which is independent to the persons whose identities are beingverified (e.g. compliance, audit or human resources),maybesufficient todemonstrate compliance with these requirements.

D. Timing of identificationand verification of identity:

(i) AnFImustcompletetheCDDprocessbeforeestablishinganybusiness relationship, orbeforecarryingoutaspecifiedoccasionaltransaction.

(ii) However, FIs may, exceptionally, verify the identity of the customer andanybeneficialowner after establishing the business relationship, provided that:

1. anyriskofML/TFarisingfromthedelayedverificationofthecustomer's or beneficial owner's identity can be effectively managed;
2. it is necessary not to interrupt the normalcourse of business with the customer;

(iii) WheretheFIisunabletocompletetheCDDprocessinaccordancewithparagraph (i) ,itmustnot establisha businessrelationship orcarry out anyoccasional

transactionwith that customer and should assess whether this failure provides grounds for knowledge or suspicion of ML/TF and a report to the JFIU is appropriate

(iv) Verification of identity should be concluded within a reasonable timeframe.Where verification cannot be completed within such a period, the FI shouldas soon as reasonably practicable suspend or terminate the business relationship unless there is a reasonable explanation for the delay. Examples ofreasonable timeframe are:

(a) the FI completing such verification no later than 30 working days after the establishment of business relations;

(b) the FI suspending business relations with the customerandrefraining from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if such verification remains uncompleted 30 working days afterthe establishment of business relations; and

(c) the FI terminating business relations with the customer if such verification remains incomplete 120 working days after the establishmentof businessrelations.

(v) Wherever possible, when terminating a relationship where funds or other assets havebeen received, the FI should return the funds or assets to the source from which they were received. In general, this means that the funds or assets should be returned to the customer/account holder but this may not always be possible.

(vi) FIs must guard against the risk of ML/TF since this is a possible means bywhich funds can be "transformed", e.g. from cash into a cashier order.Wherethe customer requests that money or other assets be transferred to third parties, the FI should assess whether this provides

grounds for knowledge or suspicion of ML/TF and a report to the JFIU is appropriate.

E. CORPORATE CUSTOMERS:

The following documents or information should be obtained in respect of corporate customers who are registered in Hong Kong (comparable documents certified by qualified persons such as lawyers or accountants in the country of registration should be obtained for those customerswhoare not registered in Hong Kong):

(a) Certificateof Incorporation & Business Registration Certificate;
(b) Memorandum and Articles of Association;
(c) Resolution of the Board of Directors to open an account and confer authority on those who will operate the account and do business with theCompany;
(d) Copy of the last and up-to-date Annual Return (or other documents) showing the identity of the principal shareholders and all the directors;
(e) Satisfactory evidence of the identity of all authorized signatories as well as the evidence of the nature of the business of the customer; and
(f) A search of the file at the Company Registry

F.Where a customer concerned is:

(i) A company which is listed on The Stock Exchange of Hong Kong or is a subsidiary of such a listed company;
(ii) A company which is listed on the stock market of a country which is a member of FATF and which is a stock market recognized by the Securities and Futures Commission for the purposes of Section 65A(2)(a) of the Securities Ordinance;

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

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

(v) A state-owned enterprise;

a. The customer itself can be regarded as the person whose identity is to be verified. It will therefore generally be sufficient for theCompany to obtain the documents specified above without the need to make further enquiries about the identity of the principal shareholders, individual directors or account signatories. Nevertheless, it is still vital to obtain the documentary evidence to prove that any individual representing the customer has the necessary authority to do business with the Company.

b. For other companies, in addition to obtaining the documents specified abovetheCompany should obtain satisfactory evidence of the identity of the principal shareholders, all the directors and the authorized signatories in line with the requirements for individual customer.

G. Foreign Corporate:

Any corporate that is not incorporated in Hong Kong is, by definition, a foreign company, e.g. a BVI company, even though all the directors and shareholders, and the place of business, are all in Hong Kong.

E. If the customer is a foreign company, it is necessary to obtain the equivalent documents to those that would be required in the case of a Hong Kong registered company. Copies of the

equivalent documents will be required to be certified by the qualified persons such as Notary Public, lawyers or bank official in the country of the registration of the company. If these documents are not in English or Chinese, a certified translation will be required.

H. Clubs, Societies and Charities

In the case of transactions purportedly on behalf of clubs, societies and charities, if such organizations are incorporated as a Company Limited by Guarantee, theCompany should deal with such organization in line with the way specified in paragraph (d) above.

F. If, however, the organization is not incorporated, and is just registered under the Societies Ordinance, the Company should satisfy itself:

- The legitimate purpose of the constitution by examining and keep a copy of the constitution or By-Laws of the organization;
- By obtaining a copy of the Registration under the Societies and Ordinance or a copy of the Registration under the Charities Ordinance (in the case of a Charity);
- By recording and verifying the identity of the individual who performs the transaction in accordance with paragraph 6.2 above;
- By obtaining the Resolution of the Board or Committee of the organization to do business and confer authority on those individuals who will transact business on a face-to-face basis; and
- The reason why the transaction is being carried out

I. Partnerships or Unincorporated Businesses

In the case of a partnership or other unincorporated customer, satisfactory evidence should be obtained of the identity of all the partners.

These should be verified in the same way as for individual as specified above.

In case where a formal partnership arrangement exists, theCompany should obtain a mandate from the partnership authorizing relationship and conferring authority on the individual who performs the transaction with the Company.

6.03 Record Keeping (Customer Record Keeping Requirements)

a. Section24(C) of OSCO creates a statutory obligation for recordkeeping, and it requires that for all remittance transactions for**HK$8,000.00 or more** or its foreign currency equivalent AND foreign currency transactions for **HKD120,000.00 or more**or its foreign currency equivalent, businesses must record and retain the following information for **six years after the date of the transaction**.

b. Failure to record and keep the same is subject to a maximum fine of HK$100,000.00 and 3 months imprisonment.

6.04 Outward remittance to a place outside Hong Kong

i. Transaction reference number

ii. Transaction type, currency, amount and value date of remittance

iii. Date of remitter's instructions

iv. Instruction details including

- **Name and address of the beneficiary**
- **Name and address of the beneficiary's bank and their account number**
- **Remitter's message (if any) to beneficiary**

v. Name, identity card number (or any other document of identity or travel document number with place of issue) of remitter or his

representative. The identification document must be physically verified if the remitter or his representative appears in person

vi. Telephone number and address of remitter

6.05 Inward remittance from a place outside Hong Kong

i. Transaction reference number

ii. Transaction type, currency, amount and value date of remittance

iii. Date of remitter's instructions

iv. Instruction details including

- **Name and address of the beneficiary**
- **Name and address of the beneficiary's bank and their account number**
- **Remitter's message (if any) to beneficiary**

v. Name, identity card number (or any other document of identity or travel document number with place of issue) of remitter or his representative. The identification document must be physically verified if the remitter or his representative appears in person.

vi. Telephone number and address of remitter

6.06 Money exchange transactions

(i) Transaction reference number

(ii) Date and time of transaction

(iii) Currencies and amount exchanged

(iv) Exchange rate

(v) Name, identity card number (or any other document of identity or travel document number with place of issue) of customer. The identification document must be physically verified

(vi) Telephone number and address of customer

(vii) If the customer refuses to provide address and telephone number, thetransaction should not be carried out.

6.07 TheCompany must be able to retrieve all relevant information about a past transaction without delay. Retention of the record may be by way of original document, stored on microfilm or on computer.

6.08 Where records relate to on-going investigations or transactions that have been the subject of a suspicious transaction report, they should be kept until the Customs and Excise Department confirms in writing that the case has been closed or for six years whichever is later.

6.09 Originator Information Accompanying Remittance Transactions

An ordering business (i.e. originator) should for all remittance transactions of HK$8,000.00 or more or its foreign currency equivalent always include in the remittance message:

- The name of the originating customer
- The customer's account number or a designated transaction reference number
- The address of the originating customer or, alternatively, the customer's Hong Kong identity card or passport number, or date and place of birth

6.10 Only in the case of a remittance of less than HK$8,000.00 or its foreign currency equivalent, may the above information in the remittance message not be included.

6.11 An ordering business should adopt a risk-based approach to check whether certain remittances may be suspicious. Consideration should be taken to factors like the identity of the beneficiary, the destination and amount of the remittance. If a remittance carries the name of a third party as the ordering person or otherwise does not appear to be consistent with the usual business/activity of the customer, the customer

should be asked to provide further explanation of the nature of the remittance.

6.12 If theCompany is acting as an intermediary in a chain of remittances, it should make sure that the information in paragraph 6.9 remains with the remittance message throughout the payment chain.

6.13 If theCompany handles incoming remittance for a beneficiary, it should check the remittance messages to make sure that they contain complete originator information if the transaction is valued at HK$8,000.00 or more or its foreign currency equivalent.

6.14 The Company should consider to terminate and/or assessing whether a suspicious transaction report be made in the situation when the absence of complete originator information occurs in the remittance message for transaction valued at HK$8,000.00 or more or its foreign currency equivalent.

7. Risk Identification and Assessment

7.1 The following factors are relevant in determining the risk profile of a particular customer or type of customer that theCompany should pay attention to:

- Geographical Risks
- Nature of Business & Client
- Non face-to-face customers
- Politically Exposed Persons (PEP)
- Watch Lists

Geographical Risks

7.2 Some countries may pose higher risk to the Company and it should apply heightened scrutiny to customers and beneficial owners resident in and funds sourced from countries identified by credible sources as having inadequate anti-money laundering standards or representing high-risk for crime and corruption, e.g.the customer is connected with certain

jurisdiction known to theCompany to be lack of proper standards in the prevention of money laundering or customer due diligence process.

7.3 Therefore, theCompany should be cautious to the origin of the customer, e.g. place of birth, place of residence, nationality, etc., the place where the customer's business is carrying out, the location of the counterparties with whom the customer conducts transaction and business.

7.4 Some countries require certain "Large Value Transactions" to be reported, e.g. daily cash transactions, daily inter-bank transfers between companies, daily inter-bank transfers between the accounts of individuals and daily cross-border transactions. Transactions which appear to be deliberately "structured" in order to avoid these limits should be considered potentially suspicious.

Nature of Business & Client

7.5 Certain business of the customer may be subject to higher risk and susceptible to money laundering risk. TheCompany should apply heightened scrutiny to customers and beneficial owners whose source of wealth emanated from activities known to be susceptible to money laundering e.g. casinos or corporate customer using unduly complex structure of ownership for no good reason.

7.6 It is important to know your customer's business so that theCompany could spot out any unusual features of the transaction requested by the customer and to ensure that the transactions being conducted are consistent with the businesses' knowledge of the customer and the customer's activity. This also requires theCompany to have a good understanding of what is normal and reasonable activity for particular types of customers, taking into account the nature of the individual customer's business.

7.7 It is also crucial to note that proper and sufficient consideration should be paid to any other information theCompany obtained in the due diligence

process that may suggest the customer is of higher risk e.g. knowledge that the customer has been refused a banking relationship by another institution.

7.8 TheCompany should also pay attention to certain type of customers and set up clear policy and make known to all the staff that transaction involving such customer should be denied and consider to make suspicious report (if necessary) e.g.

- Minors – without their legal guardian being present;
- Persons who are known to have criminal backgrounds;
- Persons who are clearly mentally incapacitated and unable to fully comprehend what they are doing;
- Persons carrying forged documentation/instruments;
- Persons who cannot produce any acceptable form of identification;
- Persons who do not know why they are sending or receiving funds and/or from whom or to whom they are dealing with.

Non face-to-face customers

7.9 Given the nature of the remittance and money exchange business, the Company should avoid non face-to-face transactions.

7.10 To avoid non face-to-face customers, it is highly recommended that all corporate customers and individual customers who transact on a regular basis must open and maintain an account with the Company.

7.11 Each regular corporate customer and individual customer after going through the customer identification, verification and due diligence process should be given a pre-determined transaction limit after making enquiry to their business nature and activities and potential turn over and frequency of such activities.

7.12 The pre-determined transaction limit should include Daily Limits and Transaction Limits. The Daily Limits are the maximum amount each customer can conduct with theCompany per day, and the Transaction

Limits are the maximum amount that can be sent per money transfer/transaction. This is helpful to the Company to spot out any existence of unusual features.

7.13 If a proposed transaction exceeds the Daily Limits and/or Transaction Limits, procedures to request a temporary and/or permanent Daily/Transaction Limits should be taken promptly by the customer or theCompany by its own motion, and theCompany should review the profile of the customer and conduct due diligence process again.

7.14 Where anyone undertakes a remittance transaction on behalf of a third party for an amount of HK$8,000.00 or more of its foreign currency equivalent who is not an existing customer of the Company, it is necessary to record and verify the identity of that third party. To reduce the risk posed by such non face-to-face third party customer, certification of identification documents presented by suitable and qualified certifiers are necessary.

Politically Exposed Persons (PEP)

7.15 In addition, to performing normal due diligence measures, it is highly recommended that additional measures be taken in respect of senior or prominent public figures, as they can be the vehicle for money laundering or terrorist financing, or they themselves can be directly involved in those prohibited activities or other indictable offences.

7.16 PEPs are defined as individuals being, or who have been, entrusted with prominent public functions, such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of public organizations and senior political party officials. The concern is that there is widespread potential risk, that such PEPs may abuse their public powers and position for their own illicit enrichment through corrupt activities.

7.17 Enhanced due diligence in respect of such PEPs is vital, such measures should also extend to cover business relationship with those persons or companies clearly related to PEPs (i.e. family members, close associates, etc.)

7.18 Again a risk-based approach is helpful and should be adopted for identifying PEPs and particular attention should be placed on those persons from countries that have a higher prevalence of crime, e.g. drug trafficking, corruption or politically unstable (reference could be made to e.g. to publicly available information such as the Corruption Perceptions Index – http://www.transparency.org/)

7.19 It is highly recommended that the decision of accepting any transaction involving PEPs should only be taken at a senior management level.

7.20 TheCompany should consider and assess the following risk factors when dealing with a business relationship (or potential relationship) with or involving PEPs:

- Any particular concern over the country where the PEP is from, taking into account his position;
- Any unexplained or unreasonable sources of wealth or income (i.e. value of assets owned not in line with the PEP's income level);
- Expected receipts of large sums from government bodies or state owned entities;
- Source of wealth described as commission earned on government contracts;
- Request by the PEP to associate any form of secrecy with a transaction; and
- Use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

Watch Lists

7.21 The Hong Kong JFIU and the OFAC maintain lists of known individuals, religious and charitable organizations that are known money launderers or are fronts for unscrupulous individuals or movements.

7.22 TheCompany should obtain updated copies of such lists and made easily accessible and available to all staff and particularly front/desk staff and the staff who deal with transaction.

7.23 In addition to the said lists referred to in paragraph 7.21 above, theCompany should set up their own Watch Lists in a data based form in the computer for monitoring purposes.

8. On-Going Monitoring

8.1 Where theCompany has an on-going business relationship with a regular customer, it is necessary to conduct on-going due diligence and scrutiny of their trading activities.

8.2 This means that theCompany should conduct review of the customer transaction periodically throughout the course of the relationship to ensure that the transaction they are carrying out is consistent with what is known about the customer, the customer's business activities and risk profile. Steps should also be taken to ensure that the records of existing customers remain up-to-date and relevant.

8.3 To achieve this process, theCompany, apart from setting a particular time for conducting such review, should also undertake such review when the following triggering points exist:

- When a significant or unusual transaction is to take place;
- When there's a material change in the way the account is operated;
- When the businesses' customer documentation standards change substantially;
- When the business is aware that it lacks sufficient information about the customer; or

- When the pre-determined limits for the customers in question exceeds the pre-determined limits

8.4 In order to carry out the aforesaid review, it is recommended that theCompany should have systems in place to enable it to identify and report the aforesaid triggering points. It is not sufficient to solely rely on the initiative of front-line staff to make ad hoc reports when the triggering points occur.

8.5 It is advisable for theCompany to have management information systems (MIS) to provide senior management and compliance officers with timely information on a regular basis to enable them to detect patterns of unusual or suspicious activity.

8.6 MIS reports used for monitoring purposes should be capable of identifying transactions that are unusual either in terms of amount, type of transaction or other relevant risk factors or pre-set factors.

9. Risk Management

9.1 The risk of inadvertently becoming involved in a money laundering or terrorist financing situation is extremely serious, and could lead to criminal prosecution as well as the loss of reputation and business.

9.2 TheCompany must be fully committed to having appropriate Policies & Procedures in place and take all reasonable steps to prevent their businesses – and indeed the whole industry – against the risk of money laundering and terrorist financing.

9.3 It is highly recommended that theCompany should appoint a compliance officer as a central reference point for reporting suspicious transactions, and the compliance officer is of sufficient status within the organization, and has adequate resources and knowledge, to enable him to play an active role in the identification and reporting of suspicious transactions.

9.4 TheCompany must appreciate that if the compliance officer decides that a Suspicious Transaction report should be made, that decision should not be over-ruled by senior management.

9.5 When faced with an unusual or potentially suspicious transaction, the compliance officer has to consider whether or not it is suspicious, and

- If it is, it must be formally reported to the JFIU as a Suspicious Transaction Report (STR), or
- If not, the action taken must still be documented and retained on file.

9.6 Obligation ofthe Compliance Officer

The following are recommended obligations that a compliance officer may take:

- Investigate all reports of suspicious transactions reported to him by his staff;
- Report suspicious transactions to the JFIU and upon notification by the Police to deal with money transferred in such manner as the Police may require;
- Liaise with the Hong Kong Police and appropriate bodies on new and updated procedures and implement their own company's own policies according in line with them;
- Ensure all watch lists have been entered in the database of the Company Computer system and ensuring the information is up-to-date;
- Ensure compliance by all staff members of all their obligations set out in the Company manual related to prevention of anti-money laundering and terrorist financing measures and hand out disciplinary action when necessary;
- Arranging and/or providing training to all staff in their anti money laundering and terrorist financing obligations;

- Set a transaction limit based upon the expected transaction information provided by the customer when setting their relationship with theCompany;
- Review each customer transaction position to consider based on the actual needs of their business, if their transaction limits need to be adjusted;
- Recommend and implement procedures from time to time in relation to both anti-money laundering and terrorist financing in line with the local regulations and international standards;

The aforesaid suggested obligations are not to be treated as definitive and exhaustive.

9.7 The appointment of a compliance officer to undertake the aforesaid role and obligations is important within the organization of the Company together with a clear system and procedures established for the employees to follow when a suspicious transaction spotted and needed to report.

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

New Staff and Staff Training

9.9 TheCompany is recommended that for all new staff before they are put in a position to deal with transactions for funds of the company a background check is conducted.

9.10 TheCompany should ensure that all staff is adequately trained in their anti-money laundering and terrorist financing obligations.

9.11 TheCompany should educate their staff that even if they do not know precisely what the underlying criminal activity is or whether illegal activities have occurred, they should still report suspicious transaction to the authorities or their compliance officer (if any).

9.12 All new employees irrespective of the level of seniority should have general appreciation of the background of money laundering and terrorist financing, their legal obligation to identify suspicious transactions and report such transactions, and the offence of "tipping off".

9.13 All members of staff who are dealing directly with the public and/or in a position to deal with account opening, or to process applications for business and/or transactions obligations under the local regulations and international standards in relation to anti-money laundering and terrorist financing measures.

9.14 A higher level of training covering all aspects of money laundering and terrorist financing procedures should be provided to those with the responsibility for supervising or managing staff.

9.15 It will be important to make arrangements for on-going training to the aforesaid staff regularly.

Independent Review

9.16 TheCompany is recommended to conduct a periodic independent review of its anti-money laundering and terrorist financing compliance program to ensure the said programs continued to be effective and efficient.

9.17 The aforesaid review should be conducted by a person other than the compliance officer within our organization (internal audit) or by someone knowledgeable about anti-money laundering and terrorist financing measures and practices preferable to be carried out by an outside

consulting firm (independent audit) e.g. accountant or lawyer on an annual basis.

9.18 The purpose of this annual review is to independently evaluate, the company's anti-money laundering and terrorist financing procedures, and it should check:

- The effectiveness of the compliance officer function;
- The adequacy of management monitoring of unusual transactions;
- The quality of reporting of suspicious transactions; and
- The level of awareness and knowledge of front line staff and other staff of their legal obligations to the anti-money laundering and terrorist financing responsibilities.

10. Suspicious Transactions & Reporting

10.1 The types of transactions that may be used by a money launderer or terrorist are almost unlimited. It is very difficult to define a suspicious transaction. Nevertheless, a suspicious transaction will often be one that is inconsistent with a customer's known legitimate business or personal activities. As a result of the aforesaid, the key to identify a suspicious transaction is to have sufficient knowledge about the customer's business so as to appreciate that a transaction, or a series of transactions, is unusual.

10.2 Examples of what might consider as a suspicious transaction is given in Annexure 1. They are not intended to be conclusive and exhaustive and only provide a guideline to the most common and basic ways in which money may be laundered. If theCompany encounters the situation mentioned in Annexure 1, at least further enquiries about the source of funds is required.

10.3 TheCompany may encounter a suspicious transaction in one of the following scenarios:

a. Something about the customer's behavior (whether that customer is a walk-in customer or an existing customer) during the interaction with a member of staff makes them think there is something suspicious going on;

b. The name of any one (or more) of the parties involved in the transaction is flagged by the name screening software. If that happens, it is most likely that the person is, or has the same name as, someone:

- known to be involved in terrorism, drug trafficking or some other serious crime; or
- who is a Politically Exposed Person

c. In the case of an Existing Customer, the transaction is so different from what is expected from that customer (considered in the context of what is known about their business) that it appears to be suspicious.

10.4 In any of the aforesaid case, the steps the Company or compliance officer of theCompany should take are the same, and such steps can be remembered by the word: **SAFE**

1st S = **Screen** the account for "Indicators of Suspicious Activity"

2nd A = **Ask** the customer appropriate questions

3rd F = **Check** the customer's File

4th E = **Evaluate** all the above information

10.5 S:Screen the account for "Indicators of SuspiciousActivity"

Recognizing one or more known indicators of suspicious activity commonly associated with money laundering or terrorist financing is the first step.

10.6 Suspicious activity based on a transaction pattern that is not trade-based. This could, for example, include:

- "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

valued based transaction reporting requirements, e.g. frequent remittances of just below AUD$10,000.00 from Australia, or US$10,000.00 from USA.

- One particular customer whose business activity appears to be significantly different from other firms in the same line of business.
- Transactions indicative of "U-turn" transactions, i.e. money passes from one person or company to another, and then back to the original person or company.
- Customers whose transactions show an increased level of activity on the first banking day after Hong Kong horse racing, normally Mondays and Thursdays, indicating illegal bookmaking.

10.7 Involvement of one or more of the following entities that have, in the past, commonly been involved in, or associated with, money laundering or terrorist financing:

- "Shelf" or "Shell" companies
- Companies registered in a known "Tax haven" or "Off-shore financial centre" such as Bermuda, the Cayman Islands or the British Virgin Islands
- Company Formation Agents, or Secretarial Companies acting as the authorized signatory of bank accounts
- Remittance Agents or Money Changers who are NOT AMSOHK members and whose anti-money laundering and terrorist financing Policies & Procedures are therefore unknown
- Casinos or any other business related to the gaming industry, such as junket tour or operators

10.8 The involvement of a "High Risk" factor

This could mean the unexplained (or insufficiently explained) involvement of one or more:

- Currencies,
- Countries or

- National of countries

Commonly associated with

- Terrorism, or
- International crime such as drug trafficking or corruption, or

Have been publicly criticized by the Financial Action Task Force ("FATF") or another international body for failing to implement the FATF Recommendations or take other measures necessary to prevent money laundering or terrorist financing.

10.9 Any refusal to provide information

- Any attempt by a customer to withhold information that you reasonable require, or any attempt by a customer to provide information which is considered incorrect or misleading must be considered as suspicious.
- In the case of walk-in customer (someone attempting to carry out a transaction of less than HK$8,000.00 or its foreign currency equivalent in Remittances OR HK$120,000.00 or its foreign currency equivalent in Exchange transaction) if someone acts in a suspicious manner and refuses to provide identification or answer any questions asked of them – even though there is no legal obligation to demand identification from them – you should decline to carry out the transaction (Filing a Suspicious Transaction Report is of little practical value if you cannot identify the person involved. However, you should still keep a file note of the incident.).

10.10 Activity that is not what you expected from the customer

- This obviously depends on the Company's knowledge on the customer and their previous financial activity
- It could, in any case, be based on whatever is known about the customer, such as their age, occupation, residential address, general appearance, type and level of previous financial activity, or for company accounts, the sort of business they have in the past.

10.11 The involvement of a Politically Exposed Person (PEP)does not automatically mean the transaction should be reported, only that the person holds, by definition, a position that could be abused for personal gain. For that reason, the possibility of corruption or other wrongdoing has to be considered, particularly in the case of a foreign PEP, from a country where corruption and abuse of public funds is more common.

10.12 A: Ask the customer appropriate questions

If staff are carrying out a transaction for a customer and they recognize one or more "suspicious activity indicators" they should try to ask the customer about the reason for the transaction.

10.13 Specifically, it is important to try and identify the **source** of the money, and in the case of a remittance transaction, also the **ultimate beneficiary** of the money being transacted. TheCompany should consider whether the customer's story amounts to a reasonable and legitimate explanation of what they have observed. If not, then the customer's activity should be regarded as suspicious and this should be reported.

10.14 F: Check the customer's file

The third stage in the systemic S-A-F-E approach to suspicious activity identification is to refer back to the information already known about the customer and their previous transactions. This may help decide if the apparently suspicious activity is different from what you would expect from that customer.

10.15 In dealing with existing customers on a regular basis, the Company will come to build up various pieces of information about them, and that can

be very useful when considering if the particular transaction is to be expected or is unusual.

10.16 Walk-in customers, on the other hand, present a more difficult problem – but some special features may cause more concerns to theCompany:

- The customer occupation. If customer's occupation indicate that they are a low wage earner, it would be unusual for such a person to be dealing in large sums of money.
- The customer residential address. If a residential address in an area indicate that the customer may be a low wage earner, again it would be unusual for such a person to be dealing in large sums of money.
- The customer's age. If very young or very old persons involved in a frequent high value transactions which a usual young or old person would not be expected to carry out.

10.17E: Evaluate all the above information

The final step in the suspicious activity identification system is the decision whether or not to make a Suspicious Transaction Report.

10.18 Such decision should be made when all the relevant circumstances are known to, and considered by, the decision maker, i.e. when all three of the preceding steps in the suspicious transaction identification system have been completed and are considered.

10.19 Reporting Procedure

(a) STREAMS-The Company is registered with the JFIU as user of the STREAMS (system for electronic filing of STR)

(b) Paper Reporting- Reports should be sent by the following means:

By mail: Joint Financial Intelligence Unit

GPO Box 6555, Hong Kong

Tel: 2866 3366 or 2860 3414Fax: 2529 4013

Email: jfiu@police.gov.hk

Reports should be made by fax or otherwise delivered as advised by the JFIU. Verbal reports can be made by telephone only if urgent (and during office hours) and in any event, information must be followed up in writing. The JFIU will always send an acknowledgment letter. The compliance officer of theCompany should make a file note of all material steps taken in respect of a Suspicious Transaction Report, and keep management advised of all developments.

Annexure 1

Examples of Suspicious Transactions Indicators and Risk Areas

The following is a list of transactions which may give rise to suspicion of money laundering or terrorist financing.

The list of examples shall not be treated as exhaustive and only gives an indication of what may be regarded as suspicious. The Company does not have to devise systems to detect the following types of transaction.

The Companyis only required to recognize suspicious transactions. What is actually regarded as suspicious is up to the Company to decide using a combination of the principles of "Know Your Customer" (KYC) and "Know Your Business" (KYB).

Where the KYC and KYB principles diverge in relation to a particular customer or transaction, the matter requires closer examination. Depending on your knowledge of the customer, the following examples may not be suspicious at all. Whether or not they are suspicious depends on the circumstances. You must report all suspicions. The Golden Rule is "If in doubt, report".

Generic Suspicious Transaction Indicators

- Unusually large cash transactions made by an individual or company whose apparent business activities would normally be conducted through cheques and other financial instruments.
- Substantial increases in transactions of an individual or business without apparent cause, especially if such transactions involve transfers within a short period out of the account and/or to a destination not normally associated with the customer.
- Customers who exchange or remit cash by means of numerous smaller transactions so that each transaction is unremarkable, but the total of all transactions will exceed the threshold.
- Customers who seek to exchange large quantities of low denomination notes for those of higher denominations.
- Reluctance to provide normal information when conducting transactions, providing minimal or apparently fictitious information.
- Customers who appear to conduct transactions with several different businesses within the same locality.
- Large number of customers transferring funds to the same beneficiary without an adequate explanation.
- Structured transfers – transfers broken up into series of smaller transfers to avoid record keeping and customer identification requirements.
- Transactions in the name of an offshore company with structured movement of funds.
- Transactions inconsistent with the customer's usual business or apparent means without good explanation.
- Customers who make regular and large payments that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs.

- Frequent exchange of traveler's cheques, foreign currency drafts by the same customer.
- Customers' receipt of numerous transfers but each transfer is below the reporting/identification requirement in the remitting country.
- Customers sending and receiving transfers to/from tax havens, particularly if there are no apparent business reasons for such transfers or such transfers are not consistent with the customer's business or apparent background.

Possible Terrorist Financing Indicators

Remittance Transactions

- Remittance transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.
- Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and the funnel funds immediately or after a short time to a small number of foreign beneficiaries.
- Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.

Customer Characteristics

- Funds generated by a business owned by individuals of the same ethnic group/origin or involvement of multiple individuals of the same ethnic origin/group from countries of specific concern (e.g. countries designated by United Nations, national authorities, etc.) acting on behalf of similar business types.
- Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).
- Customer's stated occupation is not commensurate with the level or type of activity (e.g. a student or an unemployed individual who received or sends large number of wire transfers, or who make daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Regarding non-profit or charitable organizations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- Unexplained inconsistencies arising from the process of identifying or verifying the customer (e.g. regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

Transactions linked to locations of concern

- Foreign currency exchange transactions that are followed within a short period of time by wire transfers to locations of specific concern (e.g. countries designated by United Nations, national authorities, etc).

- A large number of incoming or outgoing remittance transfers for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern to a specific individual or groups of individuals.
- A customer remits funds to a smaller number of foreign beneficiaries, both individuals and businesses, particularly when
- These are in locations of specific concern.

Annexure 2 - Suspicious Transaction Report Form

Suspicious Transaction Report Form

For Use by Remittance Agents & Money Changers

For Reports Made Under S. 25A of the DTRPO & OSCO and S.12 of the UNATMO

1.	Source Name of person/company making report: Address of person/company making report: …… Tel No…… Fax No…….. Date of Report:……Reporting Company Ref No……
2.	Details of the Suspicious Activity (Provide details of the transaction(s) and the reason(s) why you consider it/them to be suspicious)
3.	Suspicious Activity Indicators Observed
4.	Explanation given by the Subject of the Report (What was the subject's explanation for carrying out the suspicious transaction?)

5.	Details of the Subject Name: M/F: DOB: HKID or other identification doc. & type: Address: …… Tel No.: Fax No.: Bank Account (No. & Name of Bank): Occupation:……Company:…… Company Address:
6.	Details of Other Entities involved in the Suspicious Activity

_____

Signature

Annexure 3 - Checklist for Independent Review

Name of Company:

Business nature of the Company:

(a) Money Changer ( ); (b) Remittance Agent ( ); or (c) Both ( )

Any Compliance Officer responsible for the Company Anti-Money Laundering Program?

Yes ( ) Name of Compliance Officer:
No ( ) (If no, please provide explanation) _____

Please complete all of the questions below:

Item #	Anti-Money Laundering Inspection Checklist	Yes	No	Comment
I. GENERAL POLICIES				
1	Has the company issued a clear statement of policies in relation to money laundering?			
2	Has this statement been communicated in writing to all management and relevant staff and reviewed on a regular basis?			
3	Does the company review these policies on regular basis?			
4	Has the company issued relevant Instruction Manuals			

	setting out procedures for: Account Opening Customer Identification Record Keeping			
5	Does the company have a compliance officer who is responsible for day-to-day compliance with the company's prevention of money laundering policies? Are all suspicious transactions required to be reported to him? Does he report all suspicious transactions to the JFIU?			
6	Do the policies of the company include that the manager responsible for anti-money affairs "AML compliance officer" (or any outside independent party) shall conduct independent testing to determine the level of the effectiveness of these policies?			
7	Does the company have written guidelines on what constitutes a suspicious transaction? Do these guidelines comply with the requirement of the law, and/or executive regulations? How does the company ensure that staff is aware of the guidelines referred to above?			
8	Does the company provide training courses to assist staff in their execution of 7 above? Do these courses meet the suggested criteria for staff education packages set out by the JFIU's Money Laundering guidance notes?			
9	Does the company keep a copy of the staff training materials, the names of the trainees and their managerial levels?			
10	Have policies on money laundering been communicated to overseas branches and subsidiaries?			
11	Does the company apply same procedure on the employees' accounts?			
II. VERIFICATION OF IDENTITY Has the company established appropriate identification procedures for all persons and entities conducting business with it? These should include:				
12	Ensuring that the company's new account opening form and customer financial profile form designed properly to include all required information			
13	Ensuring completion of all account opening forms signed by branch manager/responsible person			
14	Obtaining the following information in respect of personal customers: • True name • Correct Permanent Address • Date of Birth and Nationality • Risk Tolerance			

	• Nature of Activity			
15	Ensuring that it attempts to establish the "true" identity of the customer by reference to reputable sources such as: <u>Personal customers</u> • Reliable personal introductions/and or personal interviews • Checking against original and official identification documents of applicants seeking to open accounts (e.g. identification card, passport, etc.) • Obtaining details of customer's nature of activity • Obtaining official documents authorizing persons that the customer entrusts to deal in his or her accounts <u>Corporate customers</u> • Certificate of Incorporated or certificate to Trade • Official documents authorizing natural persons to deal in the accounts and their personal information • Where the company is registered abroad attention should be paid to the place of origin documents and the background against which they are produced			
16	Ensuring that the name and permanent address of the customer is properly verified through a secondary source to establish the "true" identity of the customer (e.g. by reference to recent utility or charge bills, confirmation of identity from other financial institutions, as appropriate)			
17	Ensuring that the company did not open accounts or deal with prohibited persons or entities pursuant to applicable legal rules and regulations in line with what is received from competent authorities in this respect			
18	Ensuring that the company did not open accounts for clients who deal with unknown money, or under unreal or false names			
III. RECORD KEEPING				
19	Has the company established appropriate record keeping and retention of records policies and procedures in respect to relevant information on any of its customer accounts, to cover as a minimum: • Beneficial ownership of the account (where intermediaries are involved) • Volume and nature of the transactions in the account • Origin and destination of funds • Identify the persons involved in a transaction			
20	Does the company retain according to the following periods? • Account opening records 6 years after ending the deal with a client or after closing an account, as the case may be			

	• Account ledger records 6 years after ending the deal with a client or after closing an account, as the case may be • STR's records 6 years or until the final ruling is issued, whichever longer • AML annual reports 6 years • Other supporting records 6 years after ending dealing with a client or after closing an account, as the case may be			
21	Does the manager responsible for Anti-Money Laundering affairs (AML compliance officer) keep the related files in a private and safe place? Does he also separate it from other files that are not related to AML activities?			
IV. RECOGNITION OF SUSPICIOUS TRANSACTIONS				
22	Does the company routinely produce reports to highlight accounts, which may be used for the laundering of money and other suspicious activity? This reports would include: • Account activity reports, which highlight those with "excessive" activity • "Large" transactions or "cash in and out" reports which are able to identify large (more than $100,000) or unusual in and out remittance, selling or buying, particularly those involving cash • Unusual destination reports to highlight unusual sources and destination of funds			
23	Does the company have policies and procedures to ensure that accounts identified in IV-22 above are properly followed up?			
V. CONCLUSION				
24	Are you satisfied with the adequacy of policies and procedures related to anti-money laundering? Do these policies and procedures comply with the requirements of the law and its executive regulations?			
25	According to your level of satisfactions, do you recommend that the company should be re-inspected again? If yes, will it be within (1 week, 2 weeks, one month, other _____)			

Disclaimer

Notwithstanding the recommendations made in this Guideline, they are not intended to provide legal advice and do not have the force of law and should not be interpreted as such. The Guideline is intended to self-regulate the Staff members within the Company. Staff members are required to form their own opinions on each individual case to comply with the laws of Hong Kong.