CHARTERED SECRETARIES
特許秘書

The Hong Kong Institute of Chartered Secretaries

Anti-Money Laundering and Counter-Terrorist Financing Guideline

May 2016

The Hong Kong Institute of Chartered Secretaries 香港特許秘書公會

(Incorporated in Hong Kong with limited liability by guarantee)

The Hong Kong Institute of Chartered Secretaries (HKICS) is an independent professional body dedicated to the promotion of its members' role in the formulation and effective implementation of good governance policies as well as the development of the profession of Chartered Secretary in Hong Kong and throughout Mainland China.

HKICS was first established in 1949 as an association of Hong Kong members of the Institute of Chartered Secretaries and Administrators (ICSA) of London. It became a branch of ICSA in 1990 before gaining local status in 1994.

HKICS is a founder member of Corporate Secretaries International Association (CSIA) which was established in March 2010 in Geneva, Switzerland to give a global voice to corporate secretaries and governance professionals.

HKICS has over 5,800 members and 3,200 students.

Contents

1

Overview

Chapter 1 - Overview

1. Introduction

1.1 The Hong Kong Institute of Chartered Secretaries (HKICS) is an independent professional institute representing Chartered Secretaries who are governance professionals in Hong Kong and Mainland China. HKICS is rooted with The Institute of Chartered Secretaries and Administrators (ICSA) in the United Kingdom with 9 divisions internationally and over 30,000 members and 10,000 students. It is also a Founder Member of the Corporate Secretaries International Association (CSIA), an international organisation comprising 16 national member organisations to promote good governance globally. This Guideline is issued by HKICS pursuant to the HKICS AML/CFT Charter (Charter) for self-regulation among HKICS AML/CFT Organisations as part of the obligations imposed under the Charter on HKICS AML/CFT Organisations and their related Responsible Persons (RPs).

1.2 Terms and abbreviations used in this Guideline shall be interpreted by reference to the definitions set out under the Charter, the explanatory memorandum (Explanatory Memorandum) thereto, and otherwise as set out in the glossary and other parts of this Guideline. HKICS retains the final interpretation on all matters pertaining to the Charter and its related obligations.

1.3 This Guideline follows the guidance provided to financial institutions (FIs) by relevant authorities (RAs), and is intended to ensure a high standard of AML/CFT measures for HKICS AML/CFT Organisations and their RPs within the CSP[1] sector.

1.4 The purposes of the Guideline are to:

(a) provide a general background on the subjects of money laundering and terrorist financing (ML/FT), 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 CSPs and their RPs, and other senior management in designing and implementing their own policies, procedures and controls in the relevant operational areas, taking into consideration their special circumstances so as to meet the relevant AML/CFT statutory and regulatory requirements, and for self-regulation among themselves.

1.5 The relevance and usefulness of the Guideline will be kept under review by HKICS and it may be necessary to issue amendments from time to time.

[1] Under the HKICS AML/CFT Charter and the Explanatory Memorandum thereto, a CSP is any organisation that provides any of the following services to third parties (1) acting as a formation agent of legal persons, (2) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons, (3) providing a registered office, business address or correspondence for a company, a partnership or any other legal person or arrangement, (4) acting as (or arranging for another person to act as) a nominee shareholder for another person, and (5) related business to these services (modified from FATF Recommendation 22).

1.6 Given the significant differences that exist in the organisational and legal structures of different CSPs as well as the nature and scope of the business activities conducted by them, there exists no single set of universally applicable implementation measures. It must also be emphasized that the contents of the Guideline is neither intended to, nor should be construed as, an exhaustive list of the means of meeting the statutory and regulatory requirements.

1.7 Departures from this Guidance, and the rationale for so doing, should be documented, and CSPs will have to stand prepared to justify departures to HKICS and the RAs, where appropriate.

The nature of money laundering and terrorist financing

1.8 There are three common stages in the laundering of money, and they frequently involve numerous transactions. A CSP should be alert to any such sign for potential criminal activities. These stages are:

(a) Placement - the physical disposal of cash proceeds derived from illegal activities;

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

(c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

1.9 Terrorists or terrorist organisations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

Legislation concerned with money laundering and terrorist financing

1.10 The Financial Action Task Force (the FATF) is an inter-governmental body formed in 1989 that sets the international AML standards. Its mandate was expanded in October 2001 to combat the financing of terrorism. In order to ensure full and effective implementation of its standards at the global level, the FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow-up after the evaluations, including identifying high-risk and uncooperative jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large. Many

major economies have joined the FATF which has developed into a global network for international cooperation that facilitates exchanges between member jurisdictions. As a member of the FATF, Hong Kong is obliged to implement the AML requirements as promulgated by the FATF, which are consolidated into 40 Recommendations (hereafter referred to 'FATF's Recommendations')[2] and it is important that Hong Kong complies with the international AML standards in order to maintain its status as an international financial centre.

1.11 The five main pieces of legislation in Hong Kong that are concerned with ML/FT are the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO), the Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP), the Organized and Serious Crimes Ordinance (OSCO), the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO) and the United Nations Sanctions Ordinance (UNSO). It is very important that CSPs, their RPs, officers and staff fully understand their respective responsibilities under the different legislation.

AMLO

1.12 The AMLO which is applicable to FIs, imposes requirements relating to customer due diligence (CDD) and record-keeping on FIs and provides RAs with the powers to supervise compliance with these requirements and other requirements under the AMLO[3]. 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/FT risks.

1.13 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[4]. The 'specified provisions' are listed in section 5(11) of the AMLO. If the FI knowingly contravenes a specified provision, it is liable to a maximum term of imprisonment of 2 years and a fine of HK$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 HK$1 million upon conviction.

1.14 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[5] (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 FI knowingly contravenes a specified provision he is liable to a maximum term of imprisonment of 2 years and a fine of HK$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 HK$1 million upon conviction.

[2] The FATF's Recommendations can be found on the FATF website www.fatf-gafi.org .
[3] S.23, Sch. 2 of AMLO
[4] S.5, AMLO
[5] S.5, AMLO

1.15 RAs may take disciplinary actions against FIs for any contravention of a specified provision in the AMLO[6]. The disciplinary actions that can be taken include publicly reprimanding the FI; ordering the FI to take any action for the purpose of remedying the contravention; and ordering the FI to pay a pecuniary penalty not exceeding the greater of HK$10 million or 3 times the amount of profit gained, or costs avoided, by the FI as a result of the contravention.

DTROP

1.16 The DTROP contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction.

OSCO

1.17 The OSCO, among other things:

(a) gives officers of the Hong Kong Police and the Customs and Excise Department powers to investigate organized crime and triad activities;

(b) gives the Courts jurisdiction to confiscate the proceeds of organized and serious crimes, to issue restraint orders and charging orders in relation to the property of a defendant of an offence specified in the OSCO;

(c) creates an offence of money laundering in relation to the proceeds of indictable offences; and

(d) enables the Courts, under appropriate circumstances, to receive information about an offender and an offence in order to determine whether the imposition of a greater sentence is appropriate where the offence amounts to an organized crime/triad related offence or other serious offences.

UNATMO

1.18 The UNATMO is principally directed towards implementing decisions contained in Resolution 1373 dated 28 September 2001 of the United Nations Security Council (UNSC) aimed at preventing the financing of terrorist acts. Besides the mandatory elements of the UNSC Resolution 1373, the UNATMO also implements the more pressing elements of the FATF's recommendations on terrorist financing.

1.19 Under the DTROP and the OSCO[7], a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking or of an indictable offence respectively. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine of HK$5 million.

[6] S.21, AMLO
[7] S.25,DTROP & OSCO

1.20 The UNATMO, among other things, criminalizes the provision or collection of property and making any property or financial (or related) services available to terrorists or terrorist associates. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine[8]. The UNATMO also permits terrorist property to be frozen and subsequently forfeited.

1.21 The DTROP, the OSCO and the UNATMO also make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly, represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property respectively[9]. This offence carries a maximum term of imprisonment of 3 months and a fine of HK$50,000 upon conviction.

1.22 'Tipping off' is another offence under the DTROP, the OSCO and the UNATMO. A person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following that first-mentioned disclosure[10]. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.

UNSO

1.23 The UNSO provides for the imposition of sanctions against places outside of the People's Republic of China arising from Chapter 7 of the Charter of the United Nations. It provides that the Chief Executive shall make regulations following the Ministry of Foreign Affairs of the People's Republic of China for sanctions. These could include partial economic and trade embargoes, arms embargoes, and other mandatory measures decided by the Security Council of the United Nations, implemented against a place outside the People's Republic of China, along with ceasing, modification or replacement of sanctions.

1.24 Any persons contravening sanctions compliance could on summary conviction be fined not exceeding HK$500,000 and imprisonment for a term not exceeding 2 years; and on conviction on indictment by an unlimited fine and imprisonment for a term not exceeding 7 years.

[8] S.6, 7, 8, 13 & 14, UNATMO
[9] S.25A, DTROP & OSCO, s.12 & 14, UNATMO
[10] S.25A, DTROP & OSCO, s.12 & 14, UNATMO

2

AML/CFT systems

Chapter 2 – AML/CFT systems

2. AML/CFT systems

2.1 CSPs should take all reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML/FT and to prevent a contravention of any requirement under applicable AML/CFT laws. To ensure compliance with this requirement, CSPs should implement appropriate internal AML/CFT policies, procedures and controls (hereafter collectively referred to as 'AML/CFT systems').

Risk factors

2.2 While no system will detect and prevent all ML/FT activities, CSPs should establish and implement adequate and appropriate AML/CFT systems (including customer acceptance policies and procedures) taking into account factors including products and services offered, types of customers, geographical locations involved.

- Product/service risk

2.3 A CSP should consider the characteristics of the products and services that it offers and the extent to which these are vulnerable to ML/FT abuse. In this connection, a CSP should assess the risks of any new products and services (especially those that may lead to misuse of technological developments or facilitate anonymity in ML/FT schemes) before they are introduced and ensure appropriate additional measures and controls are implemented to mitigate and manage the associated ML/FT risks.

- Delivery/distribution channel risk

2.4 A CSP should also consider its delivery/distribution channels and the extent to which these are vulnerable to ML/FT abuse. These may include sales through online, postal or telephone channels where a non-face-to-face approach is used. Business sold through intermediaries may also increase risk as the business relationship between the customer and a CSP may become indirect.

- Customer risk

2.5 When assessing the customer risk, CSPs should consider who their customers are, what they do and any other information that may suggest the customer is of higher risk.

2.6 A CSP should be vigilant where the customer is of such a legal form that enables individuals to divest themselves of ownership of property whilst retaining an element of control over it or the business/industrial sector to which a customer has business connections is more vulnerable to corruption.

Examples include:

(a) companies that can be incorporated without the identity of the ultimate underlying principals being disclosed;

(b) certain forms of trusts or foundations where knowledge of the identity of the true underlying principals or controllers cannot be guaranteed;

(c) the provision for nominee shareholders; and

(d) companies issuing bearer shares.

2.7 A CSP should also consider risks inherent in the nature of the activity of the customer and the possibility that the transaction may itself be a criminal transaction. For example, the arms trade and the financing of the arms trade is a type of activity that poses multiple ML and other risks, such as:

(a) corruption risks arising from procurement contracts;

(b) risks in relation to politically exposed persons (PEPs); and

(c) terrorism and TF risks as shipments may be diverted.

- Country risk

2.8 A CSP should pay particular attention to countries or geographical locations of operation with which its customers and intermediaries are connected where they are subject to high levels of organized crime, increased vulnerabilities to corruption and inadequate systems to prevent and detect ML/FT. When assessing which countries are more vulnerable to corruption, CSPs may make reference to publicly available information or relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations (an example of which is Transparency International's 'Corruption Perceptions Index', which ranks countries according to their perceived level of corruption).

Effective controls

2.9 To ensure proper implementation of such policies and procedures, CSPs should have effective controls covering:

(a) senior management oversight, and for the avoidance of doubts, partners in a partnership are regarded as part of senior management;

(b) appointment of a Compliance Officer (CO) and a Money Laundering Reporting Officer (MLRO)[11];

[11] For some CSPs, the functions of the CO and the MLRO may be performed by the same staff member, who could be the RP for the purposes of the HKICS AML/CFT Charter.

(c) compliance and audit function; and

(d) staff screening and training[12].

- Senior management oversight

2.10 The senior management of any CSP is responsible for managing its business effectively; in relation to AML/CFT this includes oversight of the functions described below.

2.11 Senior management should:

(a) be satisfied that the CSP's AML/CFT systems are capable of addressing the ML/FT risks identified;

(b) appoint a director or senior manager as a CO who has overall responsibility for the establishment and maintenance of the CSP's AML/CFT systems; and

(c) appoint a senior member of the CSP's staff as the MLRO who is the central reference point for suspicious transaction reporting.

2.12 In order that the CO and MLRO can discharge their responsibilities effectively, senior management should, as far as practicable, ensure that the CO and MLRO are:

(a) subject to constraint of size of the CSP, independent of all operational and business functions;

(b) normally based in Hong Kong;

(c) of a sufficient level of seniority and authority within the CSP;

(d) provided with regular contact with, and when required, direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and that the business is taking sufficiently robust measures to protect itself against the risks of ML/FT;

(e) fully conversant in the CSP's statutory and regulatory requirements and the ML/FT risks arising from the CSP's business;

(f) capable of accessing, on a timely basis, all available information (both from internal sources such as CDD records and external sources such as circulars from RAs); and

[12] For further guidance on staff training see Chapter 9.

(g) equipped with sufficient resources, including staff and appropriate cover for the absence of the CO and MLRO (i.e. an alternate or deputy CO and MLRO who should, where practicable, have the same status).

- Compliance officer and money laundering reporting officer

2.13 The principal function of the CO is to act as the focal point within a CSP for the oversight of all activities relating to the prevention and detection of ML/FT and providing support and guidance to the senior management to ensure that ML/FT risks are adequately managed. In particular, the CO should assume responsibility for:

(a) developing and/or continuously reviewing the CSP's AML/CFT systems to ensure they remain up-to date and meet current statutory and regulatory requirements; and

(b) the oversight of all aspects of the CSP's AML/CFT systems which include monitoring effectiveness and enhancing the controls and procedures where necessary.

2.14 In order to effectively discharge these responsibilities, a number of areas should be considered. These include:

(a) the means by which the AML/CFT systems are managed and tested;

(b) the identification and rectification of deficiencies in the AML/CFT systems;

(c) reporting numbers within the systems, both internally and disclosures to the Joint Financial Intelligence Unit (JFIU);

(d) the mitigation of ML/FT risks arising from business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations;

(e) the communication of key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies;

(f) changes made or proposed in respect of new legislation, regulatory requirements or guidance;

(g) compliance with any requirement under any guidance issued by RAs in this respect; and

(h) AML/CFT staff training.

2.15 The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions performed are expected to include:

(a) reviewing all internal disclosures and exception reports and, in light of all available relevant information, determining whether or not it is necessary to make a report to the JFIU;

(b) maintaining all records related to such internal reviews;

(c) providing guidance on how to avoid 'tipping off' if any disclosure is made; and

(d) acting as the main point of contact with the JFIU, law enforcement, and any other competent authorities in relation to ML/FT prevention and detection, investigation or compliance.

2.16 Where practicable, a CSP should establish an independent compliance and audit function which should have a direct line of communication to the senior management of the CSP.

2.17 The compliance and audit function of the CSP should regularly review the AML/CFT systems, e.g. sample testing, (in particular, the system for recognizing and reporting suspicious transactions) to ensure effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/FT and the size of the CSP's business. Where appropriate, the CSP should seek a review from external sources.

- Staff screening

2.18 CSPs must establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new employees.

Business conducted outside Hong Kong

2.19 A Hong Kong-incorporated CSP with overseas business activities should put in place a group AML/CFT policy to ensure that all branches and subsidiary undertakings that carry on the same business as a CSP in a place outside Hong Kong have procedures in place to comply with the CDD and record-keeping requirements similar to those under this Guideline. The CSP should communicate the group policy to its overseas branches and subsidiary undertakings.

2.20 When a branch or subsidiary undertaking of a CSP outside Hong Kong is unable to comply with requirements that are similar to those imposed under this Guideline because this is not permitted by local laws, the CSP must:

(a) inform HKICS and the RA of such failure, where appropriate; and

(b) take additional measures to effectively mitigate ML/FT risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the above requirements.

2.21 Suspicion that property in whole, or partly directly or indirectly represents the proceeds of an indictable offence, should normally be reported within the jurisdiction where the suspicion arises and where the records of the related transactions are held[13]. However, in certain cases reporting to the JFIU[14] may be required in such circumstances, but only if section 25A of OSCO/DTROP applies.

[13] S.25A, OSCO & DTROP

[14] S.25(4) of the OSCO stipulates that an indictable offence includes conduct outside Hong Kong which would constitute an indictable offence if it had occurred in Hong Kong. Therefore, where a CSP in Hong Kong has information regarding money laundering, irrespective of the location, it should consider seeking clarification with and making a report to the JFIU.

3

Risk based approach

Chapter 3 – Risk based approach

3. Introduction

3.1 The risk-based approach to CDD and ongoing monitoring (RBA) is recognized as an effective way to combat ML/FT. The general principle of a RBA is that where customers are assessed to be of higher ML/FT risks, CSPs should take enhanced measures to manage and mitigate those risks, and that correspondingly where the risks are lower, simplified measures may be applied. The use of a RBA has the advantage of allowing resources to be allocated in the most efficient way directed in accordance with priorities so that the greatest risks receive the highest attention.

General requirement

3.2 CSPs should determine the extent of CDD measures and ongoing monitoring, using a RBA depending upon the background of the customer and the product, transaction or service used by that customer, so that preventive or mitigating measures are commensurate to the risks identified. The measures must however comply with the legal requirements of the AMLO. A RBA will enable CSPs to subject customers to proportionate controls and oversight by determining:

(a) the extent of the due diligence to be performed on the direct customer; the extent of the measures to be undertaken to verify the identity of any beneficial owner and any person purporting to act on behalf of the customer;

(b) the level of ongoing monitoring to be applied to the relationship; and

(c) measures to mitigate any risks identified.

For example, a RBA may require extensive CDD for high risk customers, such as an individual (or corporate entity) whose source of wealth and funds is unclear or who requires the setting up of complex structures. CSPs should be able to demonstrate to the RAs that the extent of CDD and ongoing monitoring is appropriate in view of the customer's ML/FT risks.

3.3 There are no universally accepted methodologies that prescribe the nature and extent of a RBA. However, an effective RBA does involve identifying and categorizing ML/FT risks at the customer level and establishing reasonable measures based on risks identified. An effective RBA will allow CSPs to exercise reasonable business judgment with respect to their customers. A RBA should not be designed to prohibit CSPs from engaging in transactions with customers or establishing business relationships with potential customers, but rather it should assist CSPs to effectively manage potential ML/FT risks.

Customer acceptance/risk assessment

3.4 CSPs may assess the ML/FT risks of individual customers by assigning a ML/FT risk rating to their customers.

3.5 While there is no agreed upon set of risk factors and no one single methodology to apply these risk factors in determining the ML/FT risk rating of customers, relevant factors to be considered may include the following:

- Country risk

  Customers with residence in or connection with high risk jurisdictions[15] for example:

  (a) those that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies;

  (b) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;

  (c) countries which are vulnerable to corruption; and

  (d) those countries that are believed to have strong links to terrorist activities.

  In assessing country risk associated with a customer, consideration may be given to local legislation (like UNSO and UNATMO), data available from the United Nations, the International Monetary Fund, the World Bank, the FATF, etc. and the CSP's own experience or the experience of other group entities (where the CSP is part of a multi-national group) which may have indicated weaknesses in other jurisdictions.

- Customer risk

  The following are examples of customers who might be considered to carry lower ML/FT risks:

  (a) customers who are employment-based or with a regular source of income from a known legitimate source which supports the activity being undertaken; and

  (b) the reputation of the customer, e.g. a well-known, reputable private company, with a long history that is well documented by independent sources, including information regarding its ownership and control.

  However, some customers, by their nature or behaviour might present a higher risk of ML/FT. Factors might include:

[15] Guidance on jurisdictions that do not or insufficiently apply the FATF's Recommendations or otherwise pose a higher risk is provided at paragraph 4.15.

(i) the public profile of the customer indicating involvement with, or connection to, PEPs;

(ii) complexity of the relationship, including use of corporate structures, trusts and the use of nominee and bearer shares where there is no legitimate commercial rationale;

(iii) undue levels of secrecy with a transaction;

(iv) involvement in cash-intensive businesses;

(v) nature, scope and location of business activities generating the funds/assets, having regard to sensitive or high-risk activities; and

(vi) where the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified.

- Product/service risk

Factors presenting higher risk might include:

(a) services that inherently have provided more anonymity; and

(b) ability to pool underlying customers/funds.

- Delivery/distribution channel risk

The distribution channel for products may alter the risk profile of a customer. This may include sales through online, postal or telephone channels where a non-face-to-face approach is used. Business sold through intermediaries may also increase risk as the business relationship between the customer and a CSP may become indirect.

Ongoing review

3.6 The identification of higher risk customers, products and services, including delivery channels, and geographical locations are not static assessments. They will change over time, depending on how circumstances develop, and how threats evolve. In addition, while a risk assessment should always be performed at the inception of a customer relationship, for some customers, a comprehensive risk profile may only become evident once the customer has begun transacting, making monitoring of customer transactions and ongoing reviews a fundamental component of a reasonably designed RBA. A CSP may therefore have to adjust its risk assessment of a particular customer from time to time or based upon information received from a competent authority, and review the extent of the CDD and ongoing monitoring to be applied to the customer.

3.7 CSPs should keep its policies and procedures under regular review and assess that its risk mitigation procedures and controls are working effectively.

Documenting risk assessment

3.8 A CSP should keep records and relevant documents of the risk assessment covered in this Chapter so that it can demonstrate to HKICS and the RAs, where relevant, among others:

(a) how it assesses the customer's ML/FT risk; and

(b) the extent of CDD and ongoing monitoring is appropriate based on that customer's ML/FT risk.

4

Customer due diligence

Chapter 4 - Customer due diligence

4.1 Introduction to CDD

4.1.1 A CSP must carry out CDD. CSPs may also need to conduct additional measures (referred to as enhanced customer due diligence (EDD) hereafter) or could conduct simplified customer due diligence (SDD) depending on specific circumstances. This chapter sets out the expectations of in this regard and suggests ways that these expectations may be met. Wherever possible, this Guideline gives CSPs a degree of discretion in how they comply and put in place procedures for this purpose.

4.1.2 CDD information is a vital tool for recognising whether there are grounds for knowledge or suspicion of ML/FT.

The following are CDD measures applicable to a CSP:

(a) identify the customer and verify the customer's identity using reliable, independent source documents, data or information (see paragraphs 4.2);

(b) 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 CSP is satisfied that it knows who the beneficial owner is, including in the case of a legal person or trust[16], measures to enable the CSP to understand the ownership and control structure of the legal person or trust (see paragraph 4.3);

(c) obtain information on the purpose and intended nature of the business relationship (if any) established with the CSP unless the purpose and intended nature are obvious (see paragraph 4.6); and

(d) if a person purports to act on behalf of the customer:

(i) identify the person and take reasonable measures to verify the person's identity using reliable and independent source documents, data or information; and

(ii) verify the person's authority to act on behalf of the customer (see paragraph 4.4).

4.1.3 In determining what constitutes reasonable measures to verify the identity of a beneficial owner and reasonable measures to understand the ownership and control structure of a legal person or trust, the CSP should consider and give due regard to the ML/FT risks posed by a particular customer and a particular business relationship. Due consideration should also be given to the measures set out in Chapter 3.

[16] For the purpose of this Guideline, a trust means an express trust or any similar arrangement for which a legal-binding document (i.e. a trust deed or in any other forms) is in place.

4.1.4 CSPs should adopt a balanced and common sense approach with regard to customers connected with jurisdictions which do not or insufficiently apply the FATF. While extra care may well be justified in such cases, it is not a requirement that CSPs should refuse to do any business with such customers or automatically classify them as high risk and subject them to EDD process. Rather, CSPs should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/FT.

CDD requirements should apply:

(a) at the outset of a business relationship;

(b) when the CSP suspects that the customer is involved in ML/FT; or

(c) when the CSP doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

4.2 Identification and verification of the customer's identity

The CSP must identify the customer and verify the customer's identity by reference to documents, data or information provided by a reliable and independent source, and Appendix A contains a list of documents as independent and reliable sources for identity verification purposes.

4.3 Identification and verification of a beneficial owner

4.3.1 A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. In respect of a customer who is an individual not acting in an official capacity on behalf of a legal person or trust, the customer himself is normally the beneficial owner. There is no requirement on CSPs to make proactive searches for beneficial owners in such a case, but they should make appropriate enquiries where there are indications that the customer is not acting on his own behalf.

4.3.2 Where an individual is identified as a beneficial owner, the CSP should endeavour to obtain the same identification information as at paragraph 4.8.1.

4.3.3 The obligation to verify the identity of a beneficial owner is for the CSP to take reasonable measures based on its assessment of the ML/FT risks, so that it is satisfied that it knows who the beneficial owner is.

4.3.4 For beneficial owners, CSPs should obtain the residential address (and permanent address if different) and may adopt a RBA to determine the need to take reasonable measures to verify the 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 any business, contractual or family relationship.

4.4 Identification and verification of a person purporting to act on behalf of the customer

4.4.1 If a person purports to act on behalf of the customer, CSPs must:

(a) identify the person and take reasonable measures to verify the person's identity on the basis of documents, data or information provided by:

(i) a governmental body;

(ii) the relevant authority or any other relevant authority;

(iii) an authority in a place outside Hong Kong that performs functions similar to those of the relevant authority or any other relevant authority; or

(iv) any other reliable and independent source that is recognised by the relevant authority; and

(b) verify the person's authority to act on behalf of the customer.

4.4.2 The general requirement is to obtain the same identification information as set out in paragraph 4.8.1. In taking reasonable measures to verify the identity of persons purporting to act on behalf of customers (e.g. authorized signatories and attorneys), the CSP should refer to the documents and other means listed in Appendix A wherever possible. As a general rule CSPs should identify and verify the identity of those authorized to give instructions for the movement of funds or assets.

4.4.2 CSPs should obtain written authority[17] to verify that the individual purporting to represent the customer is authorized to do so.

4.5 Characteristics and evidence of identity

4.5.1 No form of identification can be fully guaranteed as genuine or representing correct identity and CSPs should recognise that some types of documents are more easily forged than others. If suspicions are raised in relation to any document offered, CSPs should take whatever practical and proportionate steps are available to establish whether the document offered is genuine, or has been reported as lost or stolen. This may include searching publicly available information, approaching relevant authorities (such as the Immigration Department through its hotline) or requesting corroboratory evidence from the customer. Where suspicion cannot be eliminated, the document should not be accepted and consideration should be given to making a report to the authorities.

[17] For corporation, CSPs should obtain the board resolution or similar written authority.

Where documents are in a foreign language, appropriate steps should be taken by the CSP to be reasonably satisfied that the documents in fact provide evidence of the customer's identity (e.g. ensuring that staff assessing such documents are proficient in the language or obtaining a translation from a suitably qualified person).

4.6 Purpose and intended nature of business relationship

4.6.1 A CSP must understand the purpose and intended nature of the business relationship. In some instances, this will be self-evident, but in many cases, the CSP may have to obtain information in this regard.

4.6.2 Unless the purpose and intended nature are obvious, CSPs should obtain satisfactory information from all new customers as to the intended purpose and reason for establishing the business relationship, and record the information on the opening documentation.

4.6.3 This requirement also applies in the context of non-residents. While the vast majority of non-residents seek business relationships with CSPs in Hong Kong for perfectly legitimate reasons, some non-residents may represent a higher risk for ML/FT. A CSP should understand the rationale for a non-resident to seek to establish a business relationship in Hong Kong.

4.7 Timing of identification and verification of identity

- General requirement

4.7.1 Where the CSP is unable to complete the CDD process, it must not establish a business relationship or carry out any occasional transaction with that customer and should assess whether this failure provides grounds for knowledge or suspicion of ML/FT and a report to the JFIU is appropriate.

4.7.2 Further, customer information as to the purpose and intended nature of the business relationship should be obtained before the business relationship is implemented.

- Failure to complete verification of identity

4.7.3 Verification of identity should be concluded within a reasonable timeframe[18]. Where verification cannot be completed within such a period, the CSP should as soon as reasonably practicable suspend or terminate the business relationship unless there is a reasonable explanation for the delay. Examples of reasonable timeframe are:

(a) the CSP completing such verification no later than a number of 90working days after the initial approach for establishment of business relations;

[18] The same principle applies to the verification of address for a direct customer; an example of a reasonable timeframe being for say 120 working days.

(b) the CSP suspending business relations with the customer and refraining from carrying out further transactions (except to continue to follow up on outstanding verification documents to return funds to their sources, where relevant, to the extent that this is possible) if such verification remains uncompleted for 90 working days after the initial approach for establishment of business relations; and

(c) the CSP terminating business relations with the customer if such verification remains uncompleted for 120 working days after initial approach for the establishment of business relations.

4.7.4 The CSP should assess whether this failure provides grounds for knowledge or suspicion of ML/FT and a report to the JFIU is appropriate[19].

4.7.5 Wherever possible, when terminating a relationship where funds or other assets have been received, the CSP should return the funds or assets to the source from which they were received.

4.7.6 CSPs must guard against the risk of ML/FT since this is a possible means by which funds can be 'transformed'. Where the customer requests that money or other assets be transferred to third parties, the CSP should assess whether this provides grounds for knowledge or suspicion of ML/FT and a report to the JFIU is appropriate.

- Keeping customer information up-to-date

4.7.7 Once the identity of a customer has been satisfactorily verified, there is no obligation to reverify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification). However, a CSP should undertake periodic reviews of existing records of customers upon certain trigger events. These include:

(a) when a significant transaction[20] is to take place;

(b) when the CSP is aware that it lacks sufficient information about the customer concerned.

4.7.8 All high-risk customers should be subject to a minimum of an annual review, and more frequently if deemed necessary by the CSP, of their profile to ensure the CDD information retained remains up-to-date and relevant.

4.8 Natural persons

4.8.1 CSPs should collect the following identification information in respect of personal customers who need to be identified:

[19] s.25A, DTROP & OSCO, s.12, UNATMO

[20] The word 'significant' is not necessarily linked to monetary value. It may include transactions that are unusual or not in line with the CSP's knowledge of the customer.

(a) full name;

(b) date of birth;

(c) nationality; and

(d) identity document type and number.

- Verification (Hong Kong residents)

4.8.2 For Hong Kong permanent residents, CSPs should verify an individual's name, date of birth and identity card number by reference to their Hong Kong identity card. CSPs should retain a copy of the individual's identity card[21].

4.8.3 For non-permanent residents, CSPs should verify an individual's name, date of birth, nationality and travel document number and type by reference to a valid travel document (e.g. an unexpired international passport). In this respect the CSP should retain a copy of the 'biodata' page which contains the bearer's photograph and biographical details.

Alternatively, CSPs may verify the individual's name, date of birth, identity card number by reference to their Hong Kong identity card and the individual's nationality by reference to:

(a) a valid travel document;

(b) a relevant national (i.e. government or state-issued) identity card bearing the individual's photograph; or

(c) any government or state-issued document which certifies nationality.

CSPs should retain a copy of the above documents.

- Verification (non-residents)

4.8.4 For non-residents who are physically present in Hong Kong for verification purposes, CSPs should verify an individual's name, date of birth, nationality and travel document number and type by reference to a valid travel document (e.g. an unexpired international passport). In this respect the CSP should retain a copy of the 'biodata' page which contains the bearer's photograph and biographical details.

4.8.5 For non-residents who are not physically present in Hong Kong for verification purposes, CSPs should verify the individual's identity, including name, date of birth, nationality, identity or travel document number and type by reference to:

[21] Where a CSP is satisfied with the identity of a person, it is open to adopt the alternative of notation of information, instead of copy being obtained, out of privacy considerations, where appropriate.

(a) a valid travel document;

(b) a relevant national (i.e. government or state-issued) identity card bearing the individual's photograph;

(c) a valid national driving license bearing the individual's photograph; or

(d) any applicable alternatives mentioned in Appendix A.

Where a customer has not been physically present for identification purposes, a CSP must also carry out the measures provided at paragraphs 4.12.

- Address identification and verification

4.8.6 A CSP should obtain and verify the residential address (and permanent address if different) of a direct customer with whom it establishes a business relationship as this is useful for verifying an individual's identity and background.

4.8.7 For the avoidance of doubt, it is the trustee of the trust who will enter into a business relationship or carry out a transaction on behalf of the trust and who will be considered to be the customer. The address of the trustee in a direct customer relationship should therefore always be verified.

4.8.8 Methods for verifying residential addresses may include obtaining[22]:

(a) a recent utility bill issued within the last 3 months;

(b) recent correspondence from a Government department or agency (i.e. issued within the last 3 months);

(c) a statement, issued by an authorized institution, a licensed corporation or an authorized insurer within the last 3 months;

(d) a record of a visit to the residential address by the CSP;

(e) an acknowledgement of receipt duly signed by the customer in response to a letter sent by the CSP to the address provided by the customer;

(f) a letter from an immediate family member at which the individual resides confirming that the applicant lives at that address in Hong Kong, setting out the relationship between the applicant and the immediate family member, together with evidence that the immediate family member resides at the same address (for persons such as students and housewives who are unable to provide proof of address of their own name);

[22] The examples provided are not exhaustive.

(g) mobile phone or pay TV statement (sent to the address provided by the customer) issued within the last 3 months;

(h) a letter from a Hong Kong nursing or residential home for the elderly or disabled, which a CSP is satisfied that it can place reliance on, confirming the residence of the applicant;

(i) a letter from a Hong Kong university or college, which a CSP is satisfied that it can place reliance on, that confirms residence at a stated address;

(j) a Hong Kong tenancy agreement which has been duly stamped by the Inland Revenue Department;

(k) a current Hong Kong domestic helper employment contract stamped by an appropriate Consulate (the name of the employer should correspond with the applicant's visa endorsement in the passport);

(l) a letter from a Hong Kong employer together with proof of employment, which a CSP is satisfied that it can place reliance on and that confirms residence at a stated address in Hong Kong;

(m) a lawyer's confirmation of property purchase, or legal document recognising title to property; and

(n) for non-Hong Kong residents, a government issued photographic driving license or national identity card containing the current residential address or bank statements issued by a bank in an equivalent jurisdiction where the CSP is satisfied that the address has been verified.

4.8.9 It is conceivable that CSPs may not always be able to adopt any of the suggested methods in the paragraph above. Examples include countries without postal deliveries and virtually no street addresses, where residents rely upon post office boxes or their employers for the delivery of mail. Some customers may simply be unable to produce evidence of address to the standard outlined above. In such circumstances CSPs may, on a risk sensitive basis, adopt a common sense approach by adopting alternative methods such as obtaining a letter from a director or manager of a verified known overseas employer that confirms residence at a stated overseas address (or provides detailed directions to locate a place of residence).

There may also be circumstances where a customer's address is a temporary accommodation and where normal address verification documents are not available. For example, an expatriate on a short-term contract. CSPs should adopt flexible procedures to obtain verification by other means, e.g. copy of contract of employment, or bank's or employer's written confirmation. CSPs should exercise a degree of flexibility under special circumstances (e.g. where a customer is homeless). For the avoidance of doubt, a post office box address is not sufficient for persons residing in Hong Kong or corporate customers registered and/or operating in Hong Kong.

- Other considerations

4.8.10 The standard identification requirement is likely to be sufficient for most situations. If, however, the customer, or the product or service, is assessed to present a higher ML/FT risk because of the nature of the customer, his business, his location, or because of the product features, etc., the CSP should consider whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity.

4.8.11 Appendix A contains a list of documents as independent and reliable sources for identity verification purposes.

4.9 Legal persons and trusts

- General

4.9.1 For legal persons, the principal requirement is to look behind the customer to identify those who have ultimate control or ultimate beneficial ownership over the business and the customer's assets. CSPs would normally pay particular attention to persons who exercise ultimate control over the management of the customer.

4.9.2 In deciding who the beneficial owner is in relation to a legal person where the customer is not a natural person, the CSP's objective is to know who has ownership or control over the legal person which relates to the relationship, or who constitutes the controlling mind and management of any legal entity involved in the funds. Verifying the identity of the beneficial owner(s) should be carried out using reasonable measures based on a RBA, following the guidance in Chapter 3.

4.9.3 Where the owner is another legal person or trust, the objective is to undertake reasonable measures to look behind that legal person or trust and to verify the identity of beneficial owners. What constitutes control for this purpose will depend on the nature of the institution, and may vest in those who are mandated to manage funds, accounts or investments without requiring further authorisation.

4.9.4 For a customer other than a natural person, CSPs should ensure that they fully understand the customer's legal form, structure and ownership, and should additionally obtain information on the nature of its business, and the reasons for seeking the product or service unless the reasons are obvious.

4.9.5 CSPs should conduct reviews from time to time to ensure the customer information held is up-to-date and relevant; methods by which a review could be conducted include conducting company searches, seeking copies of resolutions appointing directors, noting the resignation of directors, or by other appropriate means.

4.9.6 Many entities operate internet websites, which contain information about the entity. CSPs should bear in mind that this information, although helpful in providing much of the materials that a CSP might need in relation to the customer, its management and business, may not be independently verified.

- Corporation Identification information

4.9.7 The information below should be obtained as a standard requirement; thereafter, on the basis of the ML/FT risk, a CSP should decide whether further verification of identity is required and if so the extent of that further verification. The CSP should also decide whether additional information in respect of the corporation, its operation and the individuals behind it should be obtained.

A CSP should obtain and verify the following information in relation to a customer which is a corporation:

(a) full name;

(b) date and place of incorporation;

(c) registration or incorporation number; and

(d) registered office address in the place of incorporation.

If the business address of the customer is different from the registered office address in (d) above, the CSP should obtain information on the business address and verify as far as practicable.

4.9.8 In the course of verifying the customer's information mentioned in paragraph 4.9.7, a CSP should also obtain the following information[23]:

(a) a copy of the certificate of incorporation and business registration (where applicable);

(b) a copy of the company's memorandum and articles of association which evidence the powers that regulate and bind the company; and

(c) details of the ownership and structure control of the company, e.g. an ownership chart.

4.9.9 A CSP should[24] record the names of all directors and verify the identity of directors on a RBA.

[23] Examples given are not exhaustive.

[24] The CSP may, of course, be already required to identify a particular director if the director acts as a beneficial owner or a person purporting to act on behalf of the customer (see paragraphs 4.3 and 4.4).

4.9.10 A CSP should:

(a) confirm the company is still registered and has not been dissolved, wound up, suspended or struck off;

(b) independently identify and verify the names of the directors and shareholders recorded in the company registry in the place of incorporation; and

(c) verify the company's registered office address in the place of incorporation.

4.9.11 The CSP should verify the information in paragraph 4.9.10 from:

for a locally incorporated company:

(a) a search of file at the Hong Kong Companies Registry and obtain a company report[25];

for a company incorporated overseas:

(b) a similar company search enquiry of the registry in the place of incorporation and obtain a company report;

(c) a certificate of incumbency[26] or equivalent issued by the company's registered agent in the place of incorporation; or

(d) a similar or comparable document to a company search report or a certificate of incumbency certified by a professional third party in the relevant jurisdiction verifying that the information at paragraph 4.9.10, contained in the said document, is correct and accurate.

4.9.12 If the CSP has obtained a company search report pursuant to paragraph 4.9.11 which contains information such as certificate of incorporation, company's memorandum and articles of association, etc, the CSP is not required to obtain the same information again from the customer pursuant to paragraph 4.9.8.

[25] Alternatively, the CSP may obtain from the customer a certified true copy of a company search report certified by a company registry or professional third party. The company search report should have been issued within the last 6 months. For the avoidance of doubt, it is not sufficient for the report to be self-certified by the customer.

[26] CSPs may accept a certified true copy of a certificate of incumbency certified by a professional third party. The certificate of incumbency should have been issued within the last 6 months. For the avoidance of doubt, it is not sufficient for the certificate to be self-certified by the customer.

- Beneficial owners

4.9.13 Under this Guideline, beneficial owner in relation to a corporation is defined as:

(a) an individual who:

(i) owns or controls, directly or indirectly, including through a trust or bearer share holding, not less than 10% of the issued share capital of the corporation;

(ii) is, directly or indirectly, entitled to exercise or control the exercise of not less than 10% of the voting rights at general meetings of the corporation; or

(iii) exercises ultimate control over the management of the corporation; or

(iv) if the corporation is acting on behalf of another person, means the other person.

4.9.14 A CSP should identify and record the identity of all beneficial owners, and take reasonable measures to verify the identity of:

(a) all shareholders holding 25% (for normal risk circumstances)/10% (for high risk circumstances) or more of the voting rights or share capital;

(b) any individual who exercises ultimate control over the management of the corporation; and

(c) any person on whose behalf the customer is acting.

4.9.15 For companies with multiple layers in their ownership structures, a CSP should ensure that it has an understanding of the ownership and control structure of the company. The intermediate layers of the company should be fully identified. The manner in which this information is collected should be determined by the CSP, for example by obtaining a director's declaration incorporating or annexing an ownership chart describing the intermediate layers (the information to be included should be determined on a risk sensitive basis but at a minimum should include company name and place of incorporation, and where applicable, the rationale behind the particular structure employed). The objective should always be to follow the chain of ownership to the individuals who are the ultimate beneficial owners of the direct customer of the CSP and verify the identity of those individuals.

4.9.16 CSPs need not, as a matter of routine, verify the details of the intermediate companies in the ownership structure of a company. Complex ownership structures (e.g. structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to ensure that the CSP is satisfied on reasonable grounds as to the identity of the beneficial owners.

4.9.17 The need to verify the intermediate corporate layers of the ownership structure of a company will therefore depend upon the CSP's overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for the CSP to consider if it has taken adequate measures to identify the beneficial owners.

4.9.18 Where the ownership is dispersed, the CSP should concentrate on identifying and taking reasonable measures to verify the identity of those who exercise ultimate control over the management of the company.

- Partnerships and unincorporated bodies

4.9.19 Partnerships and unincorporated bodies, although principally operated by individuals or groups of individuals, are different from individuals, in that there is an underlying business. This business is likely to have a different ML/FT risk profile from that of an individual.

4.9.20 Under this Guideline, beneficial owner, in relation to a partnership is defined as:

(a) an individual who:

(i) is entitled to or controls, directly or indirectly, not less than a 10% share of the capital or profits of the partnership;

(ii) is, directly or indirectly, entitled to exercise or control the exercise of not less than 10% of the voting rights in the partnership; or

(iii) exercises ultimate control over the management of the partnership; or

(b) if the partnership is acting on behalf of another person, means the other person.

4.9.21 Under this Guideline, in relation to an unincorporated body other than a partnership, beneficial owner:

(a) means an individual who ultimately owns or controls the unincorporated body; or

(b) if the unincorporated body is acting on behalf of another person, means the other person.

4.9.22 The CSP should obtain the following information in relation to the partnership or unincorporated body:

(a) the full name;

(b) the business address; and

(c) the names of all partners and individuals who exercise control over the management of the partnership or unincorporated body, and names of individuals who own or control not less than 10% of its capital or profits, or of its voting rights.

In cases where a partnership arrangement exists, a mandate from the partnership authorizing the establishing of a relationship and conferring authority on those who will deal with it should be obtained.

4.9.23 The CSP's obligation is to verify the identity of the customer using evidence from a reliable and independent source. Where partnerships or unincorporated bodies are well-known, reputable organisations, with long histories in their industries, and with substantial public information about them, their partners and controllers, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to provide such reliable and independent evidence of the identity of the customer. This does not remove the need to take reasonable measures to verify the identity of the beneficial owners of the partnerships or unincorporated bodies.

4.9.24 Other partnerships and unincorporated bodies have a lower profile, and generally comprise a much smaller number of partners and controllers. In verifying the identity of such customers, CSPs should primarily have regard to the number of partners and controllers. Where these are relatively few, the customer should be treated as a collection of individuals; where numbers are larger, the CSP should decide whether it should continue to regard the customer as a collection of individuals, or whether it can be satisfied with evidence of membership of a relevant professional or trade association. In either case, CSPs should obtain the partnership deed (or other evidence in the case of sole traders or other unincorporated bodies), to satisfy themselves that the entity exists, unless an entry in an appropriate national register may be checked.

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

- Trusts

4.9.26 A trust does not possess a separate legal personality. It cannot form business relationships or carry out occasional transactions itself. It is the trustee who enters into a business relationship or carries out occasional transactions on behalf of the trust and who is considered to be the customer (i.e. the trustee is acting on behalf of a third party – the trust and the individuals concerned with the trust).

4.9.27 Under this Guideline, the beneficial owner, in relation to a trust is defined as:

(a) an individual who is entitled to a vested interest in not less than 10% of the capital of the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not;

(b) the settlor of the trust;

(c) a protector or enforcer of the trust; or

(d) an individual who has ultimate control over the trust.

4.9.28 CSPs should collect the following identification information in respect of a trust on whose behalf the trustee (i.e. the customer) is acting:

(a) the name of the trust;

(b) date of establishment/settlement;

(c) the jurisdiction whose laws govern the arrangement, as set out in the trust instrument;

(d) the identification number (if any) granted by any applicable official bodies (e.g. tax identification number or registered charity or non-profit organisation number);

(e) identification information of trustee(s) - in line with guidance for individuals or corporations;

(f) identification information of settlor(s) and any protector(s) or enforcers in line with the guidance for individuals/corporations; and

(g) identification information of known beneficiaries[27]. Known beneficiaries mean those persons or that class of persons who can, from the terms of the trust instrument, be identified as having a reasonable expectation of benefiting from the trust capital or income.

[27] With reference to paragraph 4.9.27(a)

- Verifying the trust

4.9.29 A CSP must verify the name and date of establishment of a trust and should obtain appropriate evidence to verify the existence, legal form and parties to it, i.e. trustee, settlor, protector, beneficiary, etc. The beneficiaries should be identified as far as possible where defined. If the beneficiaries are yet to be determined, the CSP should concentrate on the identification of the settlor and/or the class of persons in whose interest the trust is set up. The most direct method of satisfying this requirement is to review the appropriate parts of the trust deed.

Reasonable measures to verify the existence, legal form and parties to a trust, having regard to the ML/FT risk, may include:

(a) reviewing a copy of the trust instrument and retaining a redacted copy;

(b) by reference to an appropriate register [28] in the relevant country of establishment;

(c) a written confirmation from a trustee acting in a professional capacity[29];

(d) a written confirmation from a lawyer who has reviewed the relevant instrument; or

(e) for trusts that are managed by the trust companies which are subsidiaries (or affiliate companies) of a CSP, that CSP may rely on a written confirmation from its trust subsidiaries (or trust affiliate companies).

For the avoidance of doubt, reasonable measures are still required to be taken to verify[30] the actual identity of the individual parties (i.e. trustee, settlor, protector, beneficiary, etc.).

4.9.30 Where only a class of beneficiaries is available for identification, the CSP should ascertain and name the scope of the class (e.g. children of a named individual).

4.9.31 Particular care should be taken in relation to trusts created in jurisdictions where there is no money laundering legislation similar to Hong Kong.

- Other considerations

4.9.32 Appendix A contains a list of documents recognised by the RAs as independent and reliable sources for identity verification purposes.

---

[28] In determining whether a register is appropriate, regard should be had to adequate transparency (e.g. a system of central registration where a national registry records details on trusts and other legal arrangements registered in that country). Changes in ownership and control information would need to be kept up-to-date.

[29] 'Trustees acting in their professional capacity' in this context means that they act in the course of a profession or business which consists of or includes the provision of services in connection with the administration or management of trusts (or a particular aspect of the administration or management of trusts).

[30] Reference should be made to paragraph 4.9.27.

4.10 Simplified customer due diligence (SDD)

- General

4.10.1 SDD means that application of full CDD measures is not required. In practice, this means that CSPs are not required to identify and verify the beneficial owner[31]. However, other aspects of CDD must be undertaken and it is still necessary to conduct ongoing monitoring of the business relationship. CSPs must have reasonable grounds to support the use of SDD and may have to demonstrate these grounds to the relevant RA.

4.10.2 Nonetheless, SDD must not be applied when the CSP suspects that the customer, or the transaction is involved in ML/FT, or when the CSP doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity.

- Listed company

4.10.3 CSPs may perform SDD in respect of a corporate customer listed on a stock exchange[32]. This means CSPs need not identify the beneficial owners of the listed company. In such cases, it will be generally sufficient for a CSP to obtain proof of listed status on a stock exchange. In all other cases, CSPs should follow the CDD requirements for a legal person set out in paragraphs 4.9 of this Guideline.

- Investment vehicle

4.10.4 CSPs may apply SDD to a customer that is an investment vehicle if the CSP is able to ascertain that the person responsible for carrying out measures that are similar to the CDD measures that would have been applied by the CSP in relation to all the investors of the investment vehicle falls.

4.10.5 An investment vehicle may be in the form of a legal person or trust, and may be a collective investment scheme or other investment entity.

4.10.6 An investment vehicle whether or not responsible for carrying out CDD measures on the underlying investors under governing law of the jurisdiction in which the investment vehicle is established may, where permitted by law, appoint another institution ('appointed institution'), such as a manager, a trustee, an administrator, a transfer agent, a registrar or a custodian, to perform the CDD. Where the person responsible for carrying out the CDD measures (the investment vehicle[33] or the appointed institution) and CSP may apply SDD to that investment vehicle where similar CDD measures as those of the CSP would have been applied provided that it is satisfied that the investment vehicle has ensured that there are reliable

[31] It includes the individuals who ultimately own or control the customer and the person(s) on whose behalf the customer is acting (e.g. underlying customer(s) of a customer that is a CSP).

[32] Reference should be made to paragraph 4.15.

[33] If the governing law or enforceable regulatory requirements require the investment vehicle to implement CDD measures, the investment vehicle could be regarded as the responsible party for carrying out the CDD measures where the investment vehicle meets the requirements, as permitted by law, by delegating or outsourcing to an appointed institution.

systems and controls in place to conduct the CDD (including identification and verification of the identity) on the underlying investors in accordance with the requirements similar to those set out in this Guideline.

4.10.7 The CSP may adopt a RBA in determining if it is appropriate to rely on a written representation from the investment vehicle or appointed institution (as the case may be) responsible for carrying out the CDD stating, to its actual knowledge, the identities of such investors or (where applicable) there is no such investor in the investment vehicle. In making the risk-based determination, the CSP should take into consideration whether the investment vehicle is being operated for a small, specific group of persons. Where the CSP accepts such a representation, this should be documented, retained, and subject to periodic review. Where investors owning or controlling more than 25% interest are identified, the CSP must take reasonable measures to verify their identity itself.

- Government and public body

4.10.8 CSPs may apply SDD to a customer that is the Hong Kong government, any public bodies in Hong Kong, the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.

4.10.9 Public body includes:

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

(b) any Government department or undertaking;

(c) any local or public authority or undertaking;

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

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

4.11 High-risk situations

4.11.1 A CSP must, in any situation that by its nature presents a higher risk of ML/FT, take additional measures to mitigate the risk of ML/FT.

Additional measures[34] or EDD should be taken to mitigate the ML/FT risk involved, which for illustration purposes, may include:

(a) obtaining additional information on the customer (e.g. connected parties or relationships) and updating more regularly the customer profile including the identification data;

[34] Additional measures should be documented in the CSP's policies and procedures.

(b) obtaining additional information on the intended nature of the business relationship (e.g. anticipated activity), the source of wealth and source of funds;

(c) obtaining the approval of senior management to commence or continue the relationship; and

(d) conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.

For the avoidance of doubt, all high-risk customers should be subject to a minimum annual review with reference to paragraph 4.7.8.

4.12 Customer not physically present for identification purposes

4.12.1 CSPs must apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview[35]. Where a customer has not been physically present for identification purposes, CSPs will generally not be able to determine that the documentary evidence of identity actually relates to the customer they are dealing with. Consequently, there are increased risks.

4.12.2 A CSP is required to take additional measures to compensate for any risk associated with customers not physically present for identification purposes. If a customer has not been physically present for identification purposes, the CSP must taking supplementary measures to verify all the information provided by the customer. Consideration should be given on the basis of the ML/FT risk to obtaining copies of documents that have been certified by a suitable certifier.

- Suitable certifiers and the certification procedure

4.12.3 Use of an independent suitable certifier guards against the risk that documentation provided does not correspond to the customer whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation.

4.12.4 Suitable persons to certify verification of identity documents may include:

(a) a specified intermediary in section 18(3) of Schedule 2 AMLO, including an HKICS member;

(b) a member of the judiciary in an equivalent jurisdiction;

[35] For the avoidance of doubt, this is not restricted to being physically present in Hong Kong; the face-to-face meeting could take place outside Hong Kong.

(c) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; and

(d) a Justice of the Peace.

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

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

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

4.13 Politically exposed persons (PEPs)

4.13.1 Much international attention has been paid in recent years to the risk associated with providing financial and business services to those with a prominent political profile or holding senior public office. However, PEP status itself does not automatically mean that the individuals are corrupt or that they have been incriminated in any corruption.

4.13.2 However, their office and position may render PEPs vulnerable to corruption. The risks increase when the person concerned is from a foreign country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards.

4.13.3 Following AMLO's definition PEPs include individuals entrusted with prominent public function in a place outside the People's Republic of China [36], and domestically by virtue of the positions they hold. PEPs are a high risk situation and EDD should be applied. CSPs should therefore adopt a RBA to determining whether to apply the measures in paragraph 4.13.11 below in respect of domestic PEPs.

4.13.4 The reference to PEPs does not automatically exclude sub-national political figures. Corruption by heads of regional governments, regional government ministers and large city mayors is no less serious as sub-national figures in some jurisdictions may have access to substantial funds. Where CSPs identify a customer as a sub-national figure holding a prominent public function, they should apply appropriate EDD. This also applies to domestic sub-national figures assessed by the CSP to

[36] Reference should be made to the definition of the People's Republic of China in the Interpretation and General Clauses Ordinance (Cap. 1).

pose a higher risk. In determining what constitutes a prominent public function, CSPs should consider factors such as persons with significant influence in general, significant influence over or control of public procurement or state owned enterprises, etc.

- Foreign Politically exposed person

4.13.5 Under this Guideline, in respect to a foreign PEP, this is defined to include:

(a) an individual who is or has been entrusted with a prominent public function in a place outside the People's Republic of China and

(i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a stateowned corporation and an important political party official;

(ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual falling within paragraph (a) (see paragraph 4.13.6).

4.13.6 Under this Guideline, close associate is defined to include:

(a) an individual who has close business relations with a person falling under paragraph 4.13.5(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph 4.13.5(a) is also a beneficial owner; or

(b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under paragraph 4.13.5(a) above.

4.13.7 CSPs that handle the proceeds of corruption, or handle illegally diverted government, supranational or aid funds, face reputational and legal risks, including the possibility of criminal charges for having assisted in laundering the proceeds of crime.

4.13.8 CSPs can reduce risk by conducting EDD at the outset of the business relationship and ongoing monitoring where they know or suspect that the business relationship is with a PEP.

4.13.9 CSPs must establish and maintain effective procedures (for example making reference to publicly available information and/or screening against commercially available databases) for determining whether a customer or a beneficial owner of a customer is a PEP. These procedures should extend to the connected parties of the customer using a RBA.

4.13.10 CSPs may use publicly available information or refer to relevant reports and databases on corruption risk published by specialised national, international, nongovernmental and commercial organisations to assess which countries are most vulnerable to corruption (an example of which is Transparency International's 'Corruption Perceptions Index', which ranks countries according to their perceived level of corruption).

CSPs should be vigilant where either the country to which the customer has business connections or the business/industrial sector is more vulnerable to corruption.

4.13.11 When CSPs know that a particular customer or beneficial owner is a PEP, it should, before (i) establishing a business relationship or (ii) continuing an existing business relationship where the customer or the beneficial owner is subsequently found to be a PEP, apply all the following EDD measures:

(a) obtaining approval from its senior management;

(b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds; and

(c) applying enhanced monitoring to the relationship in accordance with the assessed risks.

4.13.12 It is for a CSP to decide which measures it deems reasonable, in accordance with its assessment of the risks, to establish the source of funds and source of wealth. In practical terms, this will often amount to obtaining information from the PEP and verifying it against publicly available information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. CSPs should however note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. CSPs should also be aware that some jurisdictions impose restrictions on their PEP's ability to hold foreign assets or bank accounts or to hold other office or paid employment.

- Senior management approval

4.13.13 The CSP's approval for the establishment or continuation of the relationship should take into account the advice of the CSP's CO. The more potentially sensitive the PEP, the higher the approval process should be escalated.

- Domestic politically exposed persons

4.13.14 For the purposes of this Guideline, a domestic PEP is defined as:

(a) an individual who is or has been entrusted with a prominent public function in a place within the People's Republic of China and

(i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;

(ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual falling within paragraph (a) (see paragraph 4.13.6).

4.13.15 CSPs should take reasonable measures to determine whether an individual is a domestic PEP.

4.13.16 If an individual is known to be a domestic PEP, the CSP should perform a risk assessment to determine whether the individual poses a higher risk of ML/FT. Domestic PEPs status in itself does not automatically confer higher risk. In any situation that the CSP assesses to present a higher risk of ML/FT, it should apply the EDD and monitoring specified in paragraph 4.11.1.

4.13.17 CSPs should retain a copy of the assessment for RAs, other authorities and auditors and should review the assessment whenever concerns as to the activities of the individual arise.

- Periodic reviews

4.13.18 For foreign PEPs and domestic PEPs assessed to present a higher risk, they should be subject to a minimum annual review. CSPs should review CDD information to ensure that it remains up-to-date and relevant.

4.14 Bearer shares

4.14.1 Bearer shares are an equity security that is wholly owned by whoever holds the physical stock certificate. The issuing corporate does not register the owner of the stock or track transfers of ownership. Transferring the ownership of the stock involves only delivering the physical document. Bearer shares therefore lack the regulation and control of common shares because ownership is never recorded.

Due to the higher ML/FT risks associated with bearer shares the FATF requires countries that have legal persons able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering.

4.14.2 To reduce the opportunity for bearer shares to be used to obscure information on beneficial ownership, CSPs must take additional measures in the case of companies with capital in the form of bearer shares, as it is often difficult to identify the beneficial owner(s). CSPs should adopt procedures to establish the identities of the holders and beneficial owners of such shares and ensure that they are notified whenever there is a change of holder or beneficial owner.

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

4.14.4 Where the shares are not deposited with an authorized/registered custodian, the CSP should obtain declarations prior to account opening and annually thereafter from each beneficial owner holding 10% or more of the share capital. Given the higher ML/ TF risks associated with bearer shares, CSPs may wish to adopt higher levels of risk mitigation and obtain such declarations from each beneficial owner holding 5% or more of the share capital. CSPs should also require the customer to notify it immediately of any changes in the ownership of the shares.

4.15 Jurisdictions that do not or insufficiently apply the FATF recommendations or otherwise posing higher risk

4.15.1 CSPs should give particular attention to, and exercise extra care in respect of:

(a) business relationships and transactions with persons (including legal persons and other CSPs) from or in jurisdictions that do not or insufficiently apply the FATF Recommendations; and

(b) transactions and business connected with jurisdictions assessed as higher risk.

In addition to ascertaining and documenting the business rationale for establishing a relationship, a CSP should take reasonable measures to establish the source of funds of such customers.

4.15.2 In determining which jurisdictions do not apply, or insufficiently apply the FATF Recommendations, or may otherwise pose a higher risk, CSPs should consider, among other things:

(a) circulars issued to CSPs by RAs;

(b) whether the jurisdiction is subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances where a jurisdiction is subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, the sanctions or measures may still be given credence by a CSP because of the standing of the issuer and the nature of the measures;

(c) whether the jurisdiction is identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures;

(d) whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organisations operating within it; and

(e) whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.

(i) 'Credible sources' refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supranational or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

(ii) A CSP should be aware of the potential reputation risk of conducting business in jurisdictions which do not or insufficiently apply the FATF Recommendations or other jurisdictions known to apply inferior standards for the prevention of ML/FT.

(iii) If a CSP incorporated in Hong Kong has operating units in such jurisdictions, care should be taken to ensure that effective controls on prevention of ML/FT are implemented in these units. In particular, the CSP should ensure that the policies and procedures adopted in such overseas units are similar to those adopted in Hong Kong. There should also be compliance and internal audit checks by staff from the head office in Hong Kong.

4.16 Notice in writing from HKICS and/or RA

4.16.1 Where the requirement is called for by the FATF (which may include mandatory EDD or the application of countermeasures[37]) or in other circumstances independent of the FATF but also considered to be higher risk, HKICS and/or RA may, through a notice in writing:

(a) impose a general obligation on CSPs to undertake EDD measures; or

(b) require CSPs to undertake specific countermeasures identified or described in the notice.

The type of EDD/countermeasures would be proportionate to the nature of the risks and/or deficiencies.

4.17 Reliance on CDD performed by intermediaries

- General

4.17.1 CSPs may rely upon an intermediary to perform any part of the CDD measures specified in this Guideline. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the CSP.

For the avoidance of doubt, reliance on intermediaries does not apply to:

(a) outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the CSP to carry out its CDD function. In such a situation the outsource or agent is to be regarded as synonymous with the CSP (i.e. the processes and documentation are those of the CSP itself); and

(b) business relationships or transactions between CSPs for their clients.

In practice, this reliance on third parties often occurs through introductions made by another member of the same group, or in some jurisdictions from another CSP or third party.

4.17.2 The CSP must obtain written confirmation from the intermediary that:

(a) it agrees to perform the role; and

(b) it will provide without delay a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of the CSP upon request.

[37] For jurisdictions with serious deficiencies in applying the FATF's Recommendations and where inadequate progress has been made to improve their position, the FATF may recommend the application of counter-measures.

The CSP must ensure that the intermediary will, if requested by the CSP within the period specified in the record-keeping requirements under this Guideline, provide to the CSP a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out that measure as soon as reasonably practicable after receiving the request.

4.17.3 CSPs should obtain satisfactory evidence to confirm the status and eligibility of the intermediary. Such evidence may comprise corroboration from the intermediary's regulatory authority, or evidence from the intermediary of its status, regulation, policies and procedures.

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

4.17.5 Where these documents and records are kept by the intermediary, the CSP should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the CSP's business relationship with the customer and for at least seven years beginning on the date on which the business relationship of a customer with the CSP ends or until such time as may be specified by the RA. CSPs should also obtain an undertaking from the intermediary to supply copies of all underlying CDD information in circumstances where the intermediary is about to cease trading or does not act as an intermediary for the CSP anymore.

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

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

- Domestic intermediaries

4.17.8 CSPs may also rely upon the following categories of domestic intermediaries:

(a) a solicitor practising in Hong Kong;

(b) a certified public accountant practising in Hong Kong;

(c) a current member of The Hong Kong Institute of Chartered Secretaries practising in Hong Kong; and

(d) a trust company registered under Part VIII of the Trustees Ordinance carrying on trust business in Hong Kong,

provided that the intermediary is able to satisfy the CSP that they have adequate procedures in place to prevent ML/FT.

- Overseas intermediaries

4.17.10 CSPs may only rely upon an overseas intermediary carrying on business or practising in an equivalent jurisdiction where the intermediary:

(a) falls into one of the following categories of businesses or professions:

(i) a lawyer or a notary public;

(ii) an auditor, a professional accountant, or a tax advisor;

(iii) a trust or company service provider; and

(iv) a trust company carrying on trust business;

(b) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction;

(c) has measures in place to ensure compliance with requirements similar to those imposed under this Guideline; and

(d) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs.

4.17.11 Compliance with the requirements set out above for both domestic or overseas intermediaries may entail the CSP:

(a) reviewing the intermediary's AML/CFT policies and procedures; or

(b) making enquiries concerning the intermediary's stature and regulatory track record and the extent to which any group's AML/CFT standards are applied and audited.

4.18 Pre-existing customers

4.18.1 CSPs must perform the CDD measures prescribed this Guideline in respect of pre-existing customers (with whom the business relationship was established before this Guideline), when:

(a) a transaction takes place with regard to the customer, which is, by virtue of the amount or nature of the transaction, unusual or suspicious; or is not consistent with the CSP's knowledge of the customer or the customer's business or risk profile, or with its knowledge of the source of the customer's funds;

(b) a material change occurs in the way in which the customer operates;

(c) the CSP suspects that the customer or the customer's account is involved in ML/FT; or

(d) the CSP doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

4.18.2 Trigger events may include a change in the beneficial ownership or control but CSPs will need to consider other trigger events specific to their own customers and business.

4.18.3 CSPs should note that requirements for ongoing monitoring under this Guideline also apply to pre-existing customers (see Chapter 5).

4.19 Prohibition on anonymous relations

4.19.1 CSPs must properly identify and verify the identity of the customer in accordance with the Guideline. In all cases, the customer identification and verification records must be available to the CO, other appropriate staff, RAs, other authorities and auditors upon appropriate authority.

5

Ongoing monitoring

Chapter 5 – Ongoing monitoring

General

5.1 Effective ongoing monitoring is vital for understanding of customers' activities and an integral part of effective AML/CFT systems. It helps CSPs to know their customers and to detect unusual or suspicious activities.

A CSP must continuously monitor its business relationship with a customer by:

(a) reviewing from time to time documents, data and information relating to the customer to ensure that they are up-to-date and relevant;

(b) monitoring the activities (including cash and noncash transactions) of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds. An unusual transaction may be in the form of activity that is inconsistent with the expected pattern for that customer, or with the normal business activities for the type of product or service that is being delivered; and

(c) identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/FT.

5.2 Failure to conduct ongoing monitoring could expose a CSP to potential abuse by criminals, and may call into question the adequacy of systems and controls, or the prudence and integrity or fitness and properness of the CSP's management.

5.3 Possible characteristics CSPs should consider monitoring include:

(a) the nature and type of transactions (e.g. abnormal size or frequency);

(b) the nature of a series of transactions;

(c) the amount of any transactions, paying particular attention to particularly substantial transactions;

(d) the geographical origin/destination of a payment or receipt; and

(e) the customer's normal activity or turnover.

5.4 CSPs should be vigilant for changes on the basis of the business relationship with the customer over time. These may include where:

(a) new products or services that pose higher risk are entered into;

(b) new corporate or trust structures are created;

(c) the stated activity or turnover of a customer changes or increases; or

(d) the nature of transactions changes or their volume or size increases etc.

5.5 Where the basis of the business relationship changes significantly, CSPs should carry out further CDD procedures to ensure that the ML/FT risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures must take account of the above changes.

5.6 CSPs should conduct an appropriate review of a business relationship upon the filing of a report to the JFIU and should update the CDD information where appropriate; this will enable CSPs to assess appropriate levels of ongoing review and monitoring.

Risk-based approach to monitoring

5.7 The extent of monitoring should be linked to the risk profile of the customer which has been determined through the risk assessment required in Chapter 3. To be most effective, resources should be targeted towards business relationships presenting a higher risk of ML/FT.

5.8 CSPs must take additional measures when monitoring business relationships that pose a higher risk. High risk relationships, for example those involving PEPs, will require more frequent and intensive monitoring. In monitoring high-risk situations, relevant considerations may include:

(a) whether adequate procedures or management information systems are in place to provide relevant staff (e.g. CO, MLRO, front line staff, and relationship managers) with timely information that might include, as a result of EDD or other additional measures undertaken, any information on any connected relationships; and

(b) how to monitor the sources of funds, wealth and income for higher risk customers and how any changes in circumstances will be recorded.

Methods and procedures

5.9 When considering how best to monitor customer transactions and activities, a CSP should take into account the following factors:

(a) the size and complexity of its business;

(b) its assessment of the ML/FT risks arising from its business;

(c) the nature of its systems and controls;

(d) the monitoring procedures that already exist to satisfy other business needs; and

(e) the nature of the products and services (which includes the means of delivery or communication).

There are various methods by which these objectives can be met including exception reports (e.g. large transactions exception report) and transaction monitoring systems. Exception reports will help CSP's stay apprised of operational activities.

5.10 Where transactions that are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose are noted, CSPs should examine the background and purpose, including where appropriate the circumstances, of the transactions. The findings and outcomes of these examinations should be properly documented in writing and be available to assist the RAs, other competent authorities and auditors. Proper records of decisions made, by whom, and the rationale for them will help a CSP demonstrate that it is handling unusual or suspicious activities appropriately.

5.11 Such examinations may include asking the customer questions, based on common sense that a reasonable person would ask in the circumstances[38]. Such enquiries, when conducted properly and in good faith, do not constitute tipping off. These enquiries are directly linked to the CDD requirements, and reflect the importance of 'knowing your customer' in detecting unusual or suspicious activities. Such enquiries and their results should be properly documented and be available to assist the RAs, other authorities and auditors. Where there is any suspicion, a report must be made to the JFIU.

5.12 Where cash transactions (including deposits and withdrawals) and transfers to third parties are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, CSPs must approach such situations with caution and make relevant further enquiries. Where the CSP has been unable to satisfy itself that any cash transaction or third party transfer is reasonable, and therefore considers it suspicious, it should make a suspicious transaction report (STR) to the JFIU.

[38] S. 25A(5), DTROP & OSCO, s.12(5), UNATMO

6

Financial sanctions and terrorist financing

Chapter 6 – Financial sanctions and terrorist financing

Financial sanctions & proliferation financing

6.1 The obligations under the Hong Kong's financial sanctions regime apply to all persons, and not just CSPs.

6.2 The United Nations Sanctions Ordinance, Cap. 537 (UNSO) gives the Chief Executive the authority to make regulations to implement sanctions decided by the Security Council of the United Nations and to specify or designate relevant persons and entities[39].

6.3 These sanctions normally prohibit making available or dealing with, directly or indirectly, any funds or economic resources for the benefit of or belonging to a designated party.

6.4 RAs circulate to all CSPs designations published in the government Gazette under the UNSO.

6.5 While CSPs will not normally have any obligation under Hong Kong law to have regard to lists issued by other organisations or authorities in other jurisdictions, a CSP operating internationally will need to be aware of the scope and focus of relevant financial/trade sanctions regimes in those jurisdictions. Where these sanctions may affect their operations, CSPs should consider what implications exist for their procedures, such as the consideration to monitor the parties concerned with a view to ensuring that there are no payments to or from a person on a sanctions list issued by an overseas jurisdiction.

6.6 The Chief Executive can licence exceptions to the prohibitions on making funds and economic resources available to a designated party under the UNSO. A CSP seeking such a licence should write to the Commerce and Economic Development Bureau.

Terrorist financing

6.7 Terrorist financing generally refers to the carrying out of transactions involving property that are owned by terrorists, or that have been, or are intended to be, used to assist the commission of terrorist acts. This has not previously been explicitly covered under the money laundering regime where the focus is on the handling of criminal proceeds, i.e. the source of property is what matters. In terrorist financing, the focus is on the destination or use of property, which may have derived from legitimate sources.

[39] S.3(1), UNSO

6.8 The UN Security Council has passed United Nations Security Council Resolution (UNSCR) 1373 (2001), which calls on all member states to act to prevent and suppress the financing of terrorist acts[40].

6.9 The UN has also published the names of individuals and organisations subject to UN financial sanctions in relation to involvement with Usama bin Laden, AlQa'ida, and the Taliban under relevant UNSCRs (e.g. UNSCR 1267 (1999), 1390 (2002) and 1617 (2005)). All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities.

6.10 The United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 (UNATMO) was enacted in 2002 to give effect to the mandatory elements of UNSCR 1373 and the Special Recommendations of the FATF.

6.11 The Secretary for Security (S for S) has the power to freeze suspected terrorist property and may direct that a person shall not deal with the frozen property except under the authority of a licence. Contraventions are subject to a maximum penalty of 7 years imprisonment and an unspecified fine[41].

6.12 Section 6 of the UNATMO essentially confers the S for S an administrative power to freeze suspected terrorist property for a period of up to two years, during which time the authorities may apply to the court for an order to forfeit the property. This administrative freezing mechanism will enable the S for S to take freezing action upon receiving intelligence of suspected terrorist property in Hong Kong.

6.13 It is an offence for any person to make any property or financial services available, by any means, directly or indirectly, to or for the benefit of a terrorist or terrorist associate except under the authority of a licence granted by S for S[42]. It is also an offence for any person to collect property or solicit financial (or related) services, by any means, directly or indirectly, for the benefit of a terrorist or terrorist associate. Contraventions are subject to a maximum sentence of 14 years imprisonment and an unspecified fine.

6.14 Section 8 of the UNATMO does not affect a freeze per se; it prohibits a person from (i) making available, by any means, directly or indirectly, any property or financial services to or for the benefit of a person he knows or has reasonable grounds to suspect is a terrorist or terrorist associate, in the absence of a licence granted by S for S; and (ii) collecting property or soliciting financial (or related) services, by any means, directly or indirectly, for the benefit of a person he knows or has reasonable grounds to suspect is a terrorist or terrorist associate.

[40] UNSCR 1373 (2001)
[41] S.6, UNATMO
[42] S.8 & 14, UNATMO

6.15 The S for S can licence exceptions to the prohibitions to enable frozen property and economic resources to be unfrozen and to allow payments to be made to or for the benefit of a designated party under the UNATMO[43]. A CSP seeking such a licence should write to the Security Bureau.

6.16 Where a person is designated by a Committee of the United Nations Security Council as a terrorist and his details are subsequently published in a notice under section 4 of the UNATMO in the Government gazette, RAs will circulate the designations to all CSPs[44].

6.17 It is an offence under section 4 of the Weapons of Mass Destruction (Control of Provision of Services) Ordinance (WMD(CPS)O), Cap. 526, for a person to provide any services where he believes or suspects, on reasonable grounds, that those services may be connected to WMD proliferation[45]. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

6.18 CSPs may draw reference from a number of sources including relevant designation by overseas authorities, such as the designations made by the US Government under relevant Executive Orders. The RA may draw the CSP's attention to such designations from time to time.

All CSPs will therefore need to ensure that they should have appropriate system to conduct checks against the relevant list for screening purposes and that this list is up-to-date.

Database maintenance and screening

6.19 CSPs should take measures to ensure compliance with the relevant regulations and legislation on terrorist financing. The legal obligations of CSPs and those of its staff should be well understood and adequate guidance and training should be provided to the latter. CSPs are required to establish policies and procedures for combating terrorist financing. The systems and mechanisms for identification of suspicious transactions should cover terrorist financing as well as money laundering.

6.20 It is particularly vital that a CSP should be able to identify and report transactions with terrorist suspects and designated parties. To this end, the CSP should ensure that it maintains a database of names and particulars of terrorist suspects and designated parties which consolidates the various lists that have been made known to it. Alternatively, a CSP may make arrangements to access to such a database maintained by third party service providers.

[43] S.6(1), UNATMO
[44] S.4(1), UNATMO
[45] S.4, WMD(CPS)O

6.21 CSPs should ensure that the relevant designations are included in the database. Such database should, in particular, include the lists published in the Gazette and those designated under the US Executive Order 13224. The database should also be subject to timely update whenever there are changes, and should be made easily accessible by staff for the purpose of identifying suspicious transactions.

6.22 Comprehensive ongoing screening of a CSP's complete customer base is a fundamental internal control to prevent terrorist financing and sanction violations, and should be achieved by:

(a) screening customers against current terrorist and sanction designations at the establishment of the relationship; and

(b) thereafter, as soon as practicable after new terrorist and sanction designations are published by the RAs that these new designations, screening against their entire client base.

6.23 CSPs need to have some means of screening payment instructions to ensure that proposed payments to designated parties are not made. CSPs should be particularly alert for suspicious wire transfers.

6.24 Enhanced checks should be conducted before establishing a business relationship or processing a transaction, where possible, if there are circumstances giving rise to suspicion.

6.25 In order to demonstrate compliance with the provisions of paragraphs 6.22 to 6.24 above, the screening and any results should be documented, or recorded electronically.

6.26 If a CSP suspects that a transaction is terrorist-related, it should make a report to the JFIU. Even if there is no evidence of a direct terrorist connection, the transaction should still be reported to the JFIU if it looks suspicious for other reasons, as it may emerge subsequently that there is a terrorist link.

7

Suspicious transaction reports

Chapter 7 – Suspicious transaction reports

General issues

7.1 Sections 25A of the DTROP and the OSCO make it an offence to fail to disclose where a person knows or suspects that property represents the proceeds of drug trafficking or of an indictable offence respectively. Likewise, section 12 of the UNATMO makes it an offence to fail to disclose knowledge or suspicion of terrorist property. Under the DTROP and the OSCO, failure to report knowledge or suspicion carries a maximum penalty of three months imprisonment and a fine of HK$50,000.

7.2 Filing a report to the JFIU provides CSPs with a statutory defence to the offence of ML/FT in respect of the acts disclosed in the report[46], provided:

(a) the report is made before the CSP undertakes the disclosed acts and the acts (transaction(s)) are undertaken with the consent of the JFIU; or

(b) the report is made after the CSP has performed the disclosed acts (transaction(s)) and the report is made on the CSP's own initiative and as soon as it is reasonable for the CSP to do so.

7.3 Once an employee has reported his suspicion to the appropriate person in accordance with the procedure established by his employer for the making of such disclosures, he has fully satisfied the statutory obligation[47].

7.4 It is an offence ('tipping off') to reveal to any person any information which might prejudice an investigation[48]; if a client is told that a report has been made, this would prejudice the investigation and an offence would be committed.

7.5 Once knowledge or suspicion has been formed the following general principles should be applied:

(a) in the event of suspicion of ML/FT, a disclosure should be made even where no transaction has been conducted by or through the CSP[49];

(b) disclosures must be made as soon as is reasonably practical after the suspicion was first identified; and

[46] S.25A(2), DTROP & OSCO, s.12(2), UNATMO
[47] S.25A(4), DTROP & OSCO, s.12(4), UNATMO
[48] S.25A(5), DTROP & OSCO, s.12(5), UNATMO
[49] The reporting obligations require a person to report suspicions of ML/TF, irrespective of the amount involved. The reporting obligations of section 25A(1) DTROP and OSCO and section 12(1) UNATMO apply to 'any property'. These provisions establish a reporting obligation whenever a suspicion arises, without reference to transactions per se. Thus, the obligation to report applies whether or not a transaction was actually conducted and also covers attempted transactions.

(c) CSPs must ensure that they put in place internal controls and systems to prevent any directors, officers and employees committing the offence of tipping off the customer or any other person who is the subject of the disclosure. CSPs should also take care that their line of enquiry with customers is such that tipping off cannot be construed to have taken place.

7.6 CDD and ongoing monitoring provide the basis for recognising unusual and suspicious transactions and events. An effective way of recognising suspicious activity is knowing enough about customers, their circumstances and their normal expected activities to recognise when a transaction or instruction, or a series of transactions or instructions, is unusual.

7.7 CSPs must ensure sufficient guidance is given to staff to enable them to form suspicion or to recognise when ML/FT is taking place, taking account of the nature of the transactions and instructions that staff is likely to encounter, the type of product or service and the means of delivery, i.e. whether face to face or remote. This will also enable staff to identify and assess the information that is relevant for judging whether a transaction or instruction is suspicious in the circumstances.

Knowledge vs. suspicion

7.8 CSPs have an obligation to report where there is knowledge or suspicion of ML/FT. Generally speaking, knowledge is likely to include:

(a) actual knowledge;

(b) knowledge of circumstances which would indicate facts to a reasonable person; and

(c) knowledge of circumstances which would put a reasonable person on inquiry.

7.9 Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence.

7.10 As the types of transactions which may be used for criminal activity are almost unlimited, it is difficult to determine what will constitute a suspicious transaction.

7.11 The key is knowing enough about the customer's business to recognise that a transaction, or a series of transactions, is unusual and, from an examination of the unusual, whether there is a suspicion of ML/FT. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, etc., the transaction should be considered as unusual and the CSP should be put on alert.

7.12 Where the CSP conducts enquiries and obtains what it considers to be a satisfactory explanation of the activity or transaction, it may conclude that there are no grounds for suspicion, and therefore take no further action. However, where the CSP's enquiries do not provide a satisfactory explanation of the activity or transaction, it may conclude that there are grounds for suspicion, and must make a disclosure.

7.13 For a person to have knowledge or suspicion, he does not need to know the nature of the criminal activity underlying the money laundering, or that the funds themselves definitely arose from the criminal offence.

7.14 The following is a (non-exhaustive) list of examples of situations that might give rise to suspicion in certain circumstances:

(a) transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;

(b) transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business;

(c) where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular customer;

(d) where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged;

(e) where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process;

(f) where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;

(g) the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services;

(h) transfers to and from high risk jurisdictions[50] without reasonable explanation, which are not consistent with the customer's declared business dealings or interests; and

(i) unnecessary routing of funds or other property from/to third parties or through third party.

[50] Guidance on determining high risk jurisdictions is provided at paragraph 4.15.

7.15 The OSCO, DTROP and UNATMO prohibit disclosure by the CSP or its staff that a suspicious transaction report (STR) has been made which is likely to prejudice any investigation that might be conducted following that disclosure. A risk exists that customers could be unintentionally tipped off when the CSP is seeking to perform its CDD obligations during the establishment or course of the business relationship, or when conducting occasional transactions.

The customer's awareness of a possible STR or investigation could prejudice future efforts to investigate the suspected ML/FT operation. Therefore, if CSPs form a suspicion that transactions relate to ML/FT, they should take into account the risk of tipping off when performing the CDD process. CSPs should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

Timing and manner of reports

7.16 When a CSP knows or suspects that property represents the proceeds of crime or terrorist property, a disclosure must be made to the JFIU as soon as it is reasonable to do so[51]. The use of a standard form or the use of the e-channel 'STREAMS'[52] by registered users is strongly encouraged. Further details of reporting methods and advice may be found at JFIU's website. In the event that an urgent disclosure is required, particularly when the proceeds is part of an ongoing investigation, it should be indicated in the disclosure. Where exceptional circumstances exist in relation to an urgent disclosure, an initial notification by telephone may be considered.

7.17 Dependent on when knowledge or suspicion arises, disclosures may be made either before a suspicious transaction or activity occurs (whether the intended transaction ultimately takes place or not), or after a transaction or activity has been completed.

7.18 The law requires the disclosure to be made together with any matter on which the knowledge or suspicion is based[53]. The need for prompt disclosures is especially important where a customer has instructed the CSP to move funds or other property, close its account, make cash available for collection, or carry out significant changes to the business relationship. In such circumstances, consideration may be given to contact the JFIU urgently.

Internal reporting

7.19 A CSP should appoint a Money Laundering Reporting Officer (MLRO) as a central reference point for reporting suspicious transactions. The CSP should have measures in place to check, on an ongoing basis that it has policies and procedures to ensure compliance with legal and regulatory requirements and of testing such

[51] The purpose of disclosure is to fulfil the legal obligations set out in paragraph 7.1. Where CSPs want to make a crime report, a report should be made directly to the Hong Kong Police.

[52] STREAMS (Suspicion Transaction Report and Management System) is a web-based platform to assist in the receipt, analysis and dissemination of STRs. Use of STREAMS is recommended, especially for CSPs who make frequent reports. Further details may be obtained from the JFIU.

[53] S.25A(1), DTROP & OSCO, s.12(1), UNATMO

compliance. The type and extent of the measures to be taken in this respect should be appropriate having regard to the risk of ML/FT and the size of the business.

7.20 The CSP should ensure that the MLRO is of sufficient status within the organisation, and has adequate resources, to enable him to perform his functions.

7.21 It is the responsibility of the MLRO to consider all internal disclosures he receives in the light of full access to all relevant documentation and other parties[54]. However, the MLRO should not simply be that of a passive recipient of ad hoc reports of suspicious transactions. Rather, the MLRO should play an active role in the identification and reporting of suspicious transactions. This may also involve regular review of exception reports or large or irregular transaction reports as well as ad hoc reports made by staff. To fulfil these functions all CSPs must ensure that the MLRO receives full co-operation from all staff and full access to all relevant documentation so that he is in a position to decide whether attempted or actual ML/FT is suspected or known.

7.22 Failure by the MLRO to diligently consider all relevant material may lead to vital information being overlooked and the suspicious transaction or activity or suspicious attempted transaction or activity not being disclosed to the JFIU in accordance with the requirements of the legislation. Alternatively, it may also lead to vital information being overlooked which may have made it clear that a disclosure would have been unnecessary.

7.23 CSPs should establish and maintain procedures to ensure that:

(a) all staff are made aware of the identity of the MLRO and of the procedures to follow when making an internal disclosure report; and

(b) all disclosure reports must reach the MLRO without undue delay.

7.24 While CSPs may wish to set up internal systems that allow staff to consult with supervisors or managers before sending a report to the MLRO, under no circumstances should reports raised by staff be filtered out by supervisors or managers who have no responsibility for the money laundering reporting/compliance function. The legal obligation is to report as soon as it is reasonable to do so, so reporting lines should be as short as possible with the minimum number of people between the staff with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO.

7.25 All suspicious activity reported to the MLRO must be documented (in urgent cases this may follow an initial discussion by telephone). The report must include the full details of the customer and as full a statement as possible of the information giving rise to the suspicion.

[54] S.25A(4), DTROP & OSCO, s12(4), UNATMO

7.26 The MLRO must acknowledge receipt of the report and at the same time provide a reminder of the obligation regarding tipping off[55]. The tipping-off provision includes circumstances where a suspicion has been raised internally, but has not yet been reported to the JFIU.

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

7.28 When evaluating an internal disclosure, the MLRO must take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the CSP concerning the entities to which the report relates. This may include:

(a) making a review of other transaction patterns and volumes through connected parties;

(b) any previous patterns of instructions, the length of the business relationship and reference to CDD and ongoing monitoring information and documentation; and

(c) appropriate questioning of the customer per the systematic approach to identifying suspicious transactions recommended by the JFIU[56].

7.29 As part of the review, other connected parties or relationships may need to be examined. The need to search for information concerning connected relationships should strike an appropriate balance between the statutory requirement to make a timely disclosure to the JFIU and any delays that might arise in searching for more relevant information concerning connected relationships. The evaluation process should be documented, together with any conclusions drawn.

7.30 If after completing the evaluation, the MLRO decides that there are grounds for knowledge or suspicion, the MLRO should disclose the information to the JFIU as soon as it is reasonable to do so after his evaluation is complete together with the information on which that knowledge or suspicion is based. Providing they act in good faith in deciding not to file an STR with the JFIU, it is unlikely that there will be any criminal liability for failing to report if a MLRO concludes that there is no suspicion after taking into account all available information. It is however vital for MLROs to keep proper records of their deliberations and actions taken to demonstrate they have acted in reasonable manner.

[55] S.25A(5), DTROP & OSCO, s.12(5), UNATMO

[56] For details, please see www.jfiu.gov.hk.

- Recording internal reports

7.31 CSPs must establish and maintain a record of all ML/FT reports made to the MLRO. The record should include details of the date the report was made, the staff members subsequently handling the report, the results of the assessment, whether the report resulted in a disclosure to the JFIU, and information to allow the papers relevant to the report to be located.

- Records of reports to the JFIU

7.32 CSPs must establish and maintain a record of all disclosures made to the JFIU. The record must include details of the date of the disclosure, the person who made the disclosure, and information to allow the papers relevant to the disclosure to be located. This register may be combined with the register of internal reports, if considered appropriate.

- Post reporting matters

7.33 CSPs should note that:

(a) filing a report to the JFIU only provides a statutory defence to ML/FT in relation to the acts disclosed in that particular report. It does not absolve a CSP from the legal, reputational or regulatory risks associated with the account's continued operation;

(b) a 'consent' response from the JFIU to a pre-transaction report should not be construed as a 'clean bill of health' for the continued operation of the account or an indication that the account does not pose a risk to the CSP;

(c) CSPs should conduct an appropriate review of a business relationship upon the filing of a report to the JFIU, irrespective of any subsequent feedback provided by the JFIU;

(d) once a CSP has concerns over the operation of a customer's or a particular business relationship, it should take appropriate action to mitigate the risks. Filing a report with the JFIU and continuing to operate the relationship without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified is not acceptable;

(e) relationships reported to the JFIU should be subject to an appropriate review by the MLRO and if necessary the issue should be escalated to the CSP's senior management to determine how to handle the relationship to mitigate any potential legal or reputational risks posed by the relationship in line with the CSP's business objectives, and its capacity to mitigate the risks identified; and

(f) CSPs are not obliged to continue business relationships with customers if such action would place them at risk. It is recommended that CSPs indicate any intention to terminate a relationship in the initial disclosure to the JFIU, thereby allowing the JFIU to comment, at an early stage, on such a course of action.

7.34 The JFIU will acknowledge receipt of a disclosure made by a CSP under section 25A of both the DTROP and the OSCO, and section 12 of the UNATMO[57]. If there is no need for imminent action e-consent will usually be given under the provisions of section 25A(2) of both the DTROP and the OSCO. An example of such a letter is given at Appendix B to this Guideline. For disclosures submitted via echannel 'STREAM', e-receipt will be issued via the same channel. The JFIU may, on occasion, seek additional information or clarification with a CSP of any matter on which the knowledge or suspicion is based.

7.35 Whilst there are no statutory requirements to provide feedback arising from investigations, the Hong Kong Police and Customs and Excise Department recognise the importance of having effective feedback procedures in place. The JFIU provides feedback upon request, to a disclosing CSP in relation to the current status of an investigation.

7.36 After initial analysis by the JFIU, reports that are to be developed are allocated to financial investigation officers for further investigation. CSPs must ensure that they respond to all production orders within the required time limit and provide all of the information or material that falls within the scope of such orders. Where a CSP encounters difficulty in complying with the timeframes stipulated, the MLRO should at the earliest opportunity contact the officer-in-charge of the investigation for further guidance.

7.37 During a law-enforcement investigation, a CSP may be served with a Restraint Order, designed to freeze particular funds or property pending the outcome of an investigation[58]. A CSP must ensure that it is able to freeze the relevant property that is the subject of the order. It should be noted that the Restraint Order may not apply to all funds or property involved within a particular business relationship and CSPs should consider what, if any, funds or property may be utilised subject to having obtained the appropriate consent from the JFIU.

7.38 Upon the conviction of a defendant, a court may order the confiscation of his criminal proceeds and a CSP may be served with a Confiscation Order in the event that it holds funds or other property belonging to that defendant that are deemed by the Courts to represent his benefit from the crime[59]. A court may also order the forfeiture of property where it is satisfied that the property is terrorist property.

[57] S.25A(1)(c) & (2)(a), DTROP & OSCO, s.1 & 12(2)(a), UNATMO
[58] S.10 & 11, DTROP, s.15 & 16, OSCO, s.6, UNATMO
[59] S.3, DTROP, s.8, OSCO, s13, UNATMO

8

Record keeping

Chapter 8 – Record keeping

General legal and regulatory requirements

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

8.2 CSPs should maintain customer, transaction and other records that are necessary and sufficient to meet the record-keeping requirements under this Guideline and other regulatory requirements, that are appropriate to the scale, nature and complexity of their businesses. This is to ensure that:

(a) the audit trail for funds moving through a CSP that relate to any customer and, where appropriate, the beneficial owner of the customer or transaction is clear and complete;

(b) any customer and, where appropriate, the beneficial owner of the customer can be properly identified and verified;

(c) all customer and transaction records and information are available on a timely basis to RAs, other authorities and auditors upon appropriate authority; and

(d) CSPs are able to comply with any relevant requirements specified in other sections of this Guideline and other guidelines issued by the RAs, including, among others, records of customer risk assessment (see paragraph 3.8), registers of suspicious transaction reports (see paragraph 7.32) and training records (see paragraph 9.9).

Retention of records relating to customer identity and transactions

8.3 CSPs should keep:

(a) the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and verifying the identity of the customer and/or beneficial owner of the customer and/or beneficiary and/or persons who purport to act on behalf of the customer and/or other connected parties to the customer;

(b) any additional information in respect of a customer and/or beneficial owner of the customer that may be obtained for the purposes of EDD or ongoing monitoring;

(c) where applicable, the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship;

(d) the original or a copy of the records and documents relating to the customer's relationship (e.g. opening form; and risk assessment form) and business correspondence[60] with the customer and any beneficial owner of the customer (which at a minimum should include business correspondence material to CDD measures or significant changes to the operation of the relationship).

8.4 All documents and records mentioned in paragraph 8.3 should be kept throughout the business relationship with the customer and for a period of seven years after the end of the business relationship.

Records kept by intermediaries

8.5 Where customer identification and verification documents are held by an intermediary on which the CSP is relying to carry out CDD measures, the CSP concerned remains responsible for compliance with all record-keeping requirements. CSPs should ensure that the intermediaries being relied on have systems in place to comply with all the record-keeping requirements under this Guideline (including the requirements of paragraphs 8.3 to 8.4), and that documents and records will be provided by the intermediaries as soon as reasonably practicable after the intermediaries receive the request from the CSPs.

8.6 For the avoidance of doubt, CSPs that rely on intermediaries for carrying out a CDD measure should immediately obtain the information that the intermediary has obtained in the course of carrying out that measure, for example, name and address.

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

8.8 Irrespective of where identification and transaction records are held, CSPs are required to comply with all legal and regulatory requirements in Hong Kong.

[60] CSPs are not expected to keep each and every correspondence, such as a series of emails with the customer; the expectation is that sufficient correspondence is kept to demonstrate compliance with this Guideline.

9

Staff training

Chapter 9 – Staff training

9.1 Staff training is an important element of an effective system to prevent and detect ML/FT activities. The effective implementation of even a well-designed internal control system can be compromised if staff using the system is not adequately trained.

9.2 Staff should be trained in what they need to do to carry out their particular roles in the CSP with respect to AML/CFT. This is particularly important before new staff commence work.

9.3 CSPs should implement a clear and well-articulated policy for ensuring that relevant staff receive adequate AML/CFT training.

9.4 The timing and content of training packages for different groups of staff will need to be adapted by individual CSPs for their own needs, with due consideration given to the size and complexity of their business and the type and level of ML/FT risk.

9.5 CSPs should provide appropriate AML/CFT training to their staff. The frequency of training should be sufficient to maintain the AML/CFT knowledge and competence of the staff.

9.6 Staff should be made aware of:

(a) their CSP's and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROP, the OSCO and the UNATMO;

(b) any other statutory and regulatory obligations that concern their CSPs and themselves under the DTROP, the OSCO, the UNATMO, the UNSO and the AMLO, and the possible consequences of breaches of these obligations;

(c) the CSP's policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting; and

(d) any new and emerging techniques, methods and trends in ML/FT to the extent that such information is needed by the staff to carry out their particular roles in the CSP with respect to AML/CFT.

9.7 In addition, the following areas of training may be appropriate for certain groups of staff:

(a) all new staff, irrespective of seniority:

(i) an introduction to the background to ML/FT and the importance placed on ML/FT by the CSP; and

(ii) the need for identifying and reporting of any suspicious transactions to the MLRO, and the offence of 'tipping-off';

(b) members of staff who are dealing directly with the public:

(i) the importance of their role in the CSP's ML/FT strategy, as the first point of contact with potential money launderers;

(ii) the CSP's policies and procedures in relation to CDD and record-keeping requirements that are relevant to their job responsibilities; and

(iii) training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required;

(c) back-office staff, depending on their roles:

(i) appropriate training on customer verification and relevant processing procedures; and

(ii) how to recognise unusual activities including abnormal settlements, payments or delivery instructions;

(d) managerial staff including internal audit officers and COs:

(e) higher level training covering all aspects of the CSP's AML/CFT regime; and

(f) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as reporting of suspicious transactions to the JFIU; and

(g) MLROs:

(h) specific training in relation to their responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the JFIU; and

(i) training to keep abreast of AML/CFT requirements/ developments generally.

9.8 CSPs are encouraged to consider using a mix of training techniques and tools in delivering training, depending on the available resources and learning needs of their staff. These techniques and tools may include on-line learning systems, focused classroom training, relevant videos as well as paper- or intranet-based procedures manuals. CSPs may consider including available FATF papers and typologies as part of the training materials. All materials should be up-to-date and in line with current requirements and standards.

9.9 No matter which training approach is adopted, CSPs should monitor and maintain records of who have been trained, when the staff received the training and the type of the training provided. Records should be maintained for a minimum of 3 years.

9.10 CSPs should monitor the effectiveness of the training. This may be achieved by:

(a) testing staff's understanding of the CSP's policies and procedures to combat ML/FT, the understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions; and

(b) monitoring the compliance of staff with the CSP's AML/CFT systems as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken.

10

Guidance for whistleblowing and ethics

Chapter 10 – Guidance for whistleblowing and ethics

10.1 In accordance with Article 19 of the Charter, CSPs should establish adequate and effective whistleblowing policies subject to and otherwise in accordance with applicable laws and regulations as an important element of its AML/CFT compliance programme. In this connection, HKICS AML/CFT Organisations are expected to adopt standards to at least those commensurate with the HKICS Whistleblowing Toolkit[61] relating to their internal controls as part of risk management as part of the Charter and its related obligations.

10.2 As guidance to the conduct and ethics of RPs, senior management and staff, HKICS AML/CFT Organisations are expected to adhere to HKICS's The Essential Company Secretary[62] for HKICS members and to set the tone at the top consistent thereto.

[61] Please see https://www.hkics.org.hk/hkicsFckEditor/file/guidance%20notes/GN11_Whistleblowing.pdf.

[62] Please see https://www.hkics.org.hk/media/publication/attachment/PUBLICATION_A_2357_The%20Essential%20Company%20Secretary.pdf

Apendix A

Examples of reliable and independent sources for customer identification purposes

Appendix A – Examples of reliable and independent sources for customer identification purposes

1. The identity of an individual physically present in Hong Kong should be verified by reference to their Hong Kong identify card or travel document. CSPs 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.

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

   (a) a valid international passport or other travel document; or

   (b) a current national (i.e. Government or State issued) identity card bearing the photograph of the individual; or

   (c) current valid national (i.e. Government or State issued) driving license[63] incorporating photographic evidence of the identity of the applicant, issued by a competent national or state authority.

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

   (a) Permanent Resident Identity Card of Macau Special Administrative Region;

   (b) Mainland Travel Permit for Taiwan Residents;

   (c) Seaman's Identity Document (issued under and in accordance with the International Labour Organisation Convention/Seafarers Identity Document Convention 1958);

   (d) Taiwan Travel Permit for Mainland Residents;

   (e) Permit for residents of Macau issued by Director of Immigration;

   (f) Exit-entry Permit for Travelling to and from Hong Kong and Macau for Official Purposes; and

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

[63] For the avoidance of doubt, international drivers permits and licences are not acceptable for this purpose.

4. For minors born in Hong Kong who are not in possession of a valid travel document or Hong Kong identity card[64], their identity should be verified by reference to the minor's Hong Kong birth certificate. Whenever establishing relations with a minor, the identity of the minor's parent or guardian representing or accompanying the minor should also be recorded and verified in accordance with the above requirements.

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

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

[64] All residents of Hong Kong who are aged 11 and above are required to register for an identity card. Hong Kong permanent residents will have a Hong Kong Permanent Identity Card. The identity card of a permanent resident (i.e. a Hong Kong Permanent Identity Card) will have on the front of the card a capital letter 'A' underneath the individual's date of birth.

Appendix B

JFIU e-consent

Appendix B – JFIU e-consent

CONFIDENTIAL 機密
Joint Financial Intelligence Unit
G.P.O. Box No. 6555, General Post Office, Hong Kong

Tel: 2866 3366 Fax: 2529 4013 Email: jfiu@police.gov.hk

Date: 2012-XX-XX

Money Laundering Reporting Officer, XXXXXXX

Fax No. : XXXX XXXX

Dear Sir/Madam,

Suspicious Transaction Report ('STR')

JFIU No.	Your Reference	Date Received
XX XX	XX	

I acknowledge receipt of the above mentioned STR made in accordance with the provisions of section 25A(1) of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap 405) / Organized and Serious Crimes Ordinance (Cap 455) and section 12(1) of the United Nations (Anti-Terrorism Measures) Ordinance (Cap 575).

Based upon the information currently in hand, consent is given in accordance with the provisions of section 25A(2) of the Drug Trafficking (Recovery of Proceeds) Ordinance and Organized / Serious Crimes Ordinance, and section 12(2) of United Nations (Anti-Terrorism Measures) Ordinance.

Should you have any queries, please feel free to contact Senior Inspector Mr. XXXXX on (852) 2860 XXXX.

Yours faithfully,

(XXXXX)

for Head, Joint Financial Intelligence Unit

PERSONAL DATA
Joint Financial Intelligence Unit
G.P.O. Box No. 6555, General Post Office,
Hong Kong

Tel: 2866 3366 Fax: 2529 4013 Email: jfiu@police.gov.hk

Our Ref.: Your Ref.:

2012-XX-XX

Money Laundering Reporting Officer, XXXXXX

Fax No.: XXXX XXXX

Dear Sir/Madam,

Drug Trafficking (Recovery of Proceeds) Ordinance/
Organized and Serious Crimes Ordinance

I refer to your disclosure made to JFIU under the following reference:

JFIU No.	Your Reference	Dated
XX	XX	XX

Your disclosure is related to an investigation of 'XXXXX' by officers of XXXXX under reference XXXXX.

In my capacity as an Authorized Officer under the provisions of section 25A(2) of the Organized and Serious Crimes Ordinance, Cap. 455 ('OSCO'), I wish to inform you that you do NOT have my consent to further deal with the [subject matter]] listed in Annex A since the funds in the account are believed to be crime proceeds.

As you should know, dealing with money known or reasonably believed to represent the proceeds of an indictable offence is an offence under section 25 of OSCO. This information should be treated in strict confidence and disclosure of the contents of this letter to any unauthorized person, including the subject under investigation which is likely to prejudice the police investigation, may be an offence under section 25A(5) OSCO. Neither the accounts holder nor any other person should be notified about this correspondence.

If any person approaches your institution and attempts to make a transaction involving the account, please ask your staff to immediately contact the officer-in-charge of the case, and decline the transaction. Should the account holder or a third party question the bank as to why he cannot access the funds in the accounts he should be directed to the officer-in-charge of the case, without any further information being revealed.

Please contact the officer-in-charge, Inspector XXXXX on XXXX XXXX or the undersigned should you have any other query or seek clarification of the contents of this letter.

Yours faithfully,

(XXXXX)

Superintendent of Police
Head, Joint Financial Intelligence Unit

c.c. OC Case

Annex A

S/N		
1.		

Glossary

Glossary

AMLO	Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615)
CDD	Customer due diligence
CO	Compliance officer
Connected parties	Connected parties to a customer include the beneficial owner and any natural person having the power to direct the activities of the customer. For the avoidance of doubt the term connected party will include any director, shareholder, beneficial owner, signatory, trustee, settlor/grantor/founder, protector(s), or defined beneficiary of a legal arrangement
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
EDD	Enhanced customer due diligence
HKICS	The Hong Kong Institute of Chartered Secretaries
HKICS AML/CFT Charter	The agreement between HKICS and the CSPs as founding subscribers for self-regulation of the HKICS AML/CFT Organisations open for subscription by other CSPs qualified and willing to comply with the terms and provisions thereof
Individual	Individual means a natural person, other than a deceased natural person
JFIU	Joint Financial Intelligence Unit
Minor	Minor means a person who has not attained the age of 18 years (Interpretation and General Clauses Ordinance (Cap. 1), section 3)
MLRO	Money laundering reporting officer
ML/FT	Money laundering and/or terrorist financing
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)
PEP(s)	Politically exposed person(s)
RA(s)	Relevant authority (authorities)
RBA	Risk-based approach to CDD and ongoing monitoring
SDD	Simplified customer due diligence

Senior management	Senior management means directors (or board) and senior managers (or equivalent) of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business. This may include a firm's Chief Executive Officer, Managing Director, or other senior operating management personnel (as the case may be)
SFO	Securities and Futures Ordinance (Cap. 571)
STR(s)	Suspicious transaction report(s); also referred to as reports or disclosures
Trust	For the purposes of the guideline, a trust means an express trust or any similar arrangement for which a legal-binding document (i.e. a trust deed or in any other form) is in place
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
UNSO	United Nations Sanctions Ordinance (Cap. 537)

Acknowledgement

This Guideline is based on the Securities and Futures Commission's Guideline on Anti-Money Laundering and Counter-Terrorist Financing (July 2012) with modifications.

Disclaimer and Copyright

Notwithstanding the recommendations herein, this Guideline is not intended to constitute legal advice or to derogate from the responsibility of HKICS members or any persons to comply with the relevant rules and regulations. Members and readers should be aware that this Guideline is for reference only and they should form their own opinions on each individual case. In case of doubt, they should consult their own legal or professional advisers, as they deem appropriate. The views expressed herein do not necessarily represent those of HKICS. It is also not intended to be exhaustive in nature, but to provide guidance in understanding the topic involved. The Institute shall not be responsible to any person or organisation by reason of reliance upon any information or viewpoint set forth under this Guideline, including any losses or adverse consequences consequent therefrom.

Chartered Secretaries. More than meets the eye.
特許秘書. 潛能. 超越所見.

The Hong Kong Institute of Chartered Secretaries 香港特許秘書公會
(Incorporated in Hong Kong with limited liability by guarantee)

Hong Kong Office
3/F Hong Kong Diamond Exchange Building, 8 Duddell Street, Central, Hong Kong
Tel: (852) 2881 6177 **Fax:** (852) 2881 5050
E-mail: ask@hkics.org.hk **Website:** www.hkics.org.hk

Beijing Representative Office
Room. 15A04, 15A/F, Dacheng Tower, No.127 Xuanwumen West Street, Xicheng District, Beijing, China PRC 100031
Tel: (8610) 6641 9368 **Fax:** (8610) 6641 9078
E-mail: bro@hkics.org.hk **Website:** www.hkics.org.cn