公 司 註 冊 處

COMPANIES REGISTRY

Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for Licensed Money Lenders

June 2023

CONTENTS

Chapter 1

INTRODUCTION

1.1 **The Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for Licensed Money Lenders ("this Guideline") is issued by the Registrar of Money Lenders ("the Registrar") to provide guidance to money lenders who hold a licence granted or renewed under the Money Lenders Ordinance, Cap. 163, to carry on business as a money lender in Hong Kong ("the licensees") for the implementation of effective measures to mitigate the risks of money laundering and terrorist financing. This Guideline is promulgated by reference to the requirements set out in the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 ("the AMLO"). Any non-compliance with a provision in this Guideline may cast doubt on whether a licensee is fit and proper to carry on business as a money lender and whether its officers are fit and proper to be associated with the business of money-lending.**

1.2 Terms and abbreviations used in this Guideline shall be interpreted by reference to the definitions set out in the Glossary part of this Guideline. Interpretation of other words or phrases should follow those set out in the AMLO.

1.3 This Guideline is intended for use by licensees as well as their officers and staff. The purposes of this Guideline are to provide:

(a) a general background on the subjects of money laundering and/or terrorist financing ("ML/TF"); and

(b) practical guidance to assist licensees and their senior management in devising and implementing policies, procedures and controls in relevant operational areas, taking into consideration their own circumstances by reference to the anti-money laundering and counter-terrorist financing ("AML/CTF") requirements under Schedule 2 to the AMLO.

1.4 In case of doubt, you are advised to seek independent legal advice as you see fit.

1.5 If any provision set out in this Guideline appears to the court to be relevant to any question arising in any proceedings, the provision may be taken into account in determining that question.

1.6 Besides the AMLO, the Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 ("the DTROPO")[1], the Organized and Serious Crimes Ordinance, Cap. 455 ("the OSCO")[1], the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 ("the UNATMO")[2], the United Nations Sanctions Ordinance, Cap. 537 ("the UNSO")[3] and the Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526 ("the WMD(CPS)O")[4] are the other main pieces of legislation in Hong Kong that are concerned with money laundering, terrorist financing, financial sanctions and financing of proliferation of weapons of mass destruction ("PF"). Licensees are strongly advised to read the relevant provisions of these ordinances. Please refer to Chapters 7 and 8 of this Guideline for more information regarding the requirements for reporting suspicious transactions, financial sanctions, PF and terrorist financing.

[1] Please refer to Chapter 7 of this Guideline for more information as to the requirement for reporting suspicious transactions.

[2] Please refer to Chapter 7 of this Guideline for more information as to the requirement for reporting suspicious transactions and Chapter 8 of this Guideline regarding financial sanctions and terrorist financing.

[3] Please refer to Chapter 8 of this Guideline regarding financial sanctions.

[4] Please refer to Chapter 8 of this Guideline regarding financing of proliferation of weapons of mass destruction.

Chapter 2

WHAT ARE MONEY LAUNDERING AND TERRORIST FINANCING?

2.1 The term "money laundering" is defined in section 1 of Part 1 of Schedule 1 to the AMLO as an act intended to have the effect of making any property:

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

(b) that in whole or in part, directly or indirectly, represents such proceeds, not to appear to be or so represent such proceeds.

Three common stages in money laundering

(a) Placement - 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.

Numerous transactions are frequently involved in those stages. Licensees should be alert to any such sign for potential criminal activities.

2.2 The term "terrorist financing" is defined in section 1 of Part 1 of Schedule 1 to the AMLO as:

(a) the provision or collection, by any means, directly or indirectly, of any property-
  (i) with the intention that the property be used; or
  (ii) knowing that the property will be used,
  in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used); or

(b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or

(c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.

2.3 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. 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.

Chapter 3

AML/CTF OBLIGATIONS OF MONEY LENDERS

3.1 **In general, licensees are required to:**

(a) take all reasonable measures to mitigate the risk of ML/TF; and

(b) ensure that, among other things[5], the AML/CTF requirements under the AMLO are complied with.

3.2 To fulfil the above-mentioned obligations, licensees must assess the ML/TF risk of their businesses, develop and implement policies, procedures and controls (hereinafter collectively referred to as "AML/CTF systems") on:

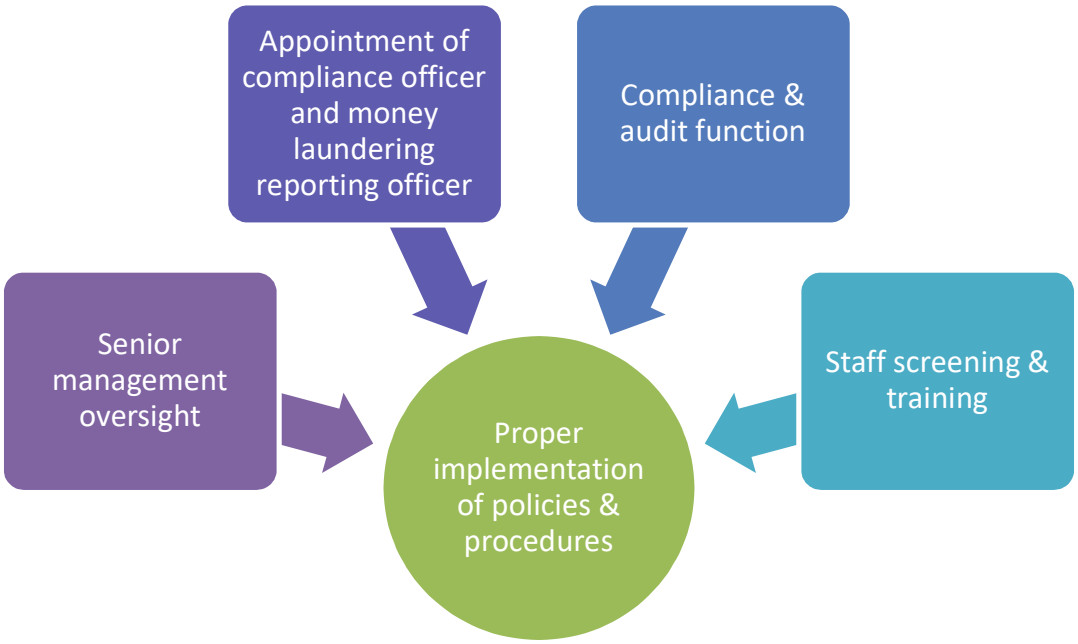
(a) risk assessment;
(b) customer due diligence ("CDD") measures;
(c) ongoing monitoring of customers;
(d) suspicious transactions reporting;
(e) record keeping;
(f) staff training; and
(g) independent audit function.

AML/CTF systems

3.3 **Licensees should establish and implement adequate and appropriate AML/CTF systems (including customer acceptance policies and procedures) taking into account factors including products and services offered, types of customers, geographical locations involved.**

[5] Other than the AMLO, licensees should also ensure that the AML/CTF requirements under the DTROPO, the OSCO, the UNATMO, the UNSO and the WMD(CPS)O are complied with.

Proper implementation of policies and procedures



3.4 The senior management of any licensee should:

(a) ensure that the licensee's AML/CTF systems are capable of addressing the ML/TF risks identified;

(b) appoint a director or senior manager as a compliance officer ("CO") who has overall responsibility for the establishment and maintenance of the licensee's AML/CTF systems; and

(c) appoint a senior member of the licensee's staff as the money laundering reporting officer ("MLRO") who is the central reference point for reporting suspicious transactions.

Major responsibilities of the CO and MLRO	
CO	**MLRO**
➢ Act as the focal point within the business or organisation of a licensee for the oversight of all activities relating to the prevention and detection of ML/TF. ➢ Provide support and guidance to the senior management to ensure that ML/TF risks are adequately managed. ➢ Develop and/or continuously review the licensee's AML/CTF systems to ensure they remain up-to-date and meet current statutory and regulatory requirements. ➢ Oversee all aspects of the licensee's AML/CTF systems which include monitoring effectiveness and enhancing the controls and procedures where necessary.	➢ Review all internal reports of suspicious transactions and exception reports and, in the light of all available information, determine whether or not it is necessary to file a suspicious transaction report ("STR") with the Joint Financial Intelligence Unit ("JFIU")[6]. ➢ Maintain all records relating to such internal reviews. ➢ Provide guidance to staff on how to avoid "tipping-off" if any STR is filed. ➢ Act as the main point of contact with the JFIU, law enforcement agencies, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.

3.5 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) normally based in Hong Kong;
(b) of a sufficient level of seniority and authority within the licensee's business;
(c) 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 ML/TF risks;
(d) subject to constraint of size of the licensee's business, independent of all operational and business functions[7];

[6] JFIU is jointly run by staff of the Hong Kong Police Force and the Customs and Excise Department. JFIU manages the STRs regime for Hong Kong and its role is to receive, analyse and store STRs and to disseminate them to the appropriate investigative unit. Please refer to its website at www.jfiu.gov.hk for further information.

[7] For example, where a licensee's money lending business is only managed by two persons, one of them may be appointed as the CO while the other may be appointed as the MLRO.

(e) fully conversant with the AML/CTF statutory and regulatory requirements on the licensee and the ML/TF risks arising from the licensee'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 issued by the Registrar and the relevant authorities specified in the AMLO). The Registrar and such relevant authorities are hereinafter collectively referred to as "RAs" and individually "RA"; and

(g) equipped with sufficient resources, including staff and appropriate cover for the absence of the CO and MLRO (for example, an alternate or deputy CO and MLRO).

3.6 Depending on the scale, operation, nature of business and risk profile of a licensee, the same person may be appointed as its CO and MLRO.

3.7 In order to effectively discharge those responsibilities, the CO should take into consideration different aspects of the licensee's AML/CTF systems, including:

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

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

(c) the number of internal reports of suspicious transactions and STRs filed with the JFIU;

(d) the mitigation of ML/TF risks arising from business relationships and transactions with persons (including both natural and legal persons) from jurisdictions identified by the Financial Action Task Force ("FATF")[8] as having strategic AML/CTF deficiencies;

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

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

(g) compliance with any requirements prescribed under Part 2 or 3 of Schedule 2 to the AMLO by branches and subsidiary undertakings outside Hong Kong and any guidance issued by RAs in this respect; and

(h) AML/CTF training for staff.

[8] FATF is an inter-governmental body established in 1989 that sets the international AML standards. The objectives of the FATF are to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Please refer to its website at www.fatf-gafi.org for further information.

Business conducted outside Hong Kong by a licensee which is incorporated in Hong Kong[9]

A. A licensee which is incorporated in Hong Kong but have branches or subsidiary undertakings outside Hong Kong should put in place a group AML/CTF policy to ensure that all branches and subsidiary undertakings that carry on the same business as the licensee in a place outside Hong Kong have policies and procedures in place to comply with the CDD and record-keeping requirements similar to those imposed under Parts 2 and 3 of Schedule 2 to the AMLO to the extent permitted by the law of that place. The licensee should communicate the group policy to its branches and subsidiary undertakings outside Hong Kong.

B. If a branch or subsidiary undertaking of a licensee outside Hong Kong is unable to comply with the requirements that are similar to those imposed under Parts 2 and 3 of Schedule 2 to the AMLO because this is not permitted by local laws, the licensee must:
   (a) inform the Registrar of such failure; and
   (b) take additional measures to effectively mitigate the ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the above requirements.

C. If a licensee knows or suspects that certain property in whole or in part directly or indirectly represents the proceeds of an indictable offence, it should normally report to the relevant authorities of the jurisdiction where the suspicion arises and where the records of the related transactions are held. However, in certain cases, e.g. where the account is held in Hong Kong, reporting to the JFIU may be required if section 25A of the OSCO or section 25A of the DTROPO applies.[10]

D. Section 25(4) of the OSCO stipulates that an indictable offence includes conduct outside Hong Kong which would constitute an indictable offence if the conduct had occurred in Hong Kong. Therefore, where a licensee in Hong Kong has information regarding money laundering, irrespective of the location, it should consider seeking clarification from the JFIU.

[9] Please refer to section 22 of Part 4 of Schedule 2 to the AMLO.

[10] Please refer to paragraph 7.1 of this Guideline and the text box under that paragraph for the requirements regarding reporting suspicious transactions.

3.8 Licensees must establish, implement and maintain appropriate procedures in order to be satisfied of the integrity of any new employees.

3.9 Licensees should establish an independent audit function which should have a direct line of communication to their senior management. The function should have sufficient expertise and resources to enable it to carry out its responsibilities, including independent reviews of the licensee's AML/CTF systems.

3.10 The audit function should regularly review the AML/CTF systems to ensure effectiveness. The review should include, but not limited to:

(a) adequacy of the licensee's AML/CTF systems, ML/TF risk assessment framework and application of risk-based approach;
(b) effectiveness of suspicious transaction reporting systems;
(c) effectiveness of the compliance function; and
(d) level of awareness of staff having AML/CTF responsibilities.

3.11 The frequency and extent of the review should be commensurate with the nature, size and complexity of the licensee's businesses and the ML/TF risks arising from those businesses. Where appropriate, the licensee should also seek a review from external parties.

Chapter 4

ASSESSING RISK AND APPLYING A RISK-BASED APPROACH

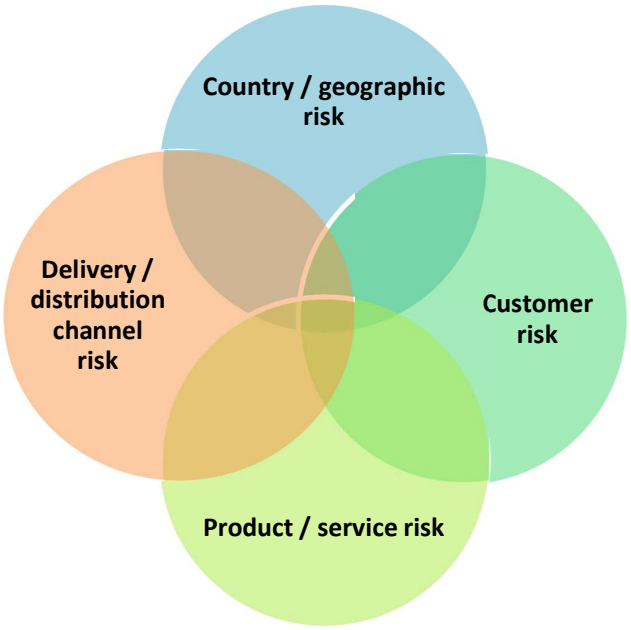
4.1 **Licensees are required to identify, assess and take effective action to mitigate their ML/TF risks. By adopting a risk-based approach, licensees can allocate resources in the most efficient way with proper priorities so that the greatest risk receives the highest attention.**

4.2 Licensees can apply appropriate control and oversight to new and existing customers by determining:

(a) the extent of CDD to be performed;
(b) the level of ongoing monitoring to be applied to the relationship with customers; and
(c) the measures to mitigate any ML/TF risks identified.

4.3 Licensees should be able to demonstrate to the Registrar that the extent of CDD and ongoing monitoring of customer relationship is appropriate in view of their customers' ML/TF risks.

4.4 Licensees may assess the ML/TF risks of an individual customer by assigning a ML/TF risk rating to their customers. While there is neither an agreed set of risk factors nor a single methodology to apply these risk factors in determining the ML/TF risk rating of customers, the following factors may be considered:



Country/geographic risk

A. Customers with residence in or connection with high-risk jurisdictions, for example:

(a) those that have been identified by the FATF as jurisdictions with strategic AML/CTF 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) countries that are believed to have strong links to terrorist activities.

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

Customer risk

Determining the potential ML/TF risks posed by a customer, or a category of customers, is critical to the development of an overall risk framework. Based on its own criteria, a licensee should determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment. Some customers, by their nature or behaviour, might present a higher risk of ML/TF. Factors might include:

(a) the public profile of the customer indicating involvement with, or connection to, politically exposed persons ("PEPs");
(b) 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;
(c) a request to use numbered accounts or undue levels of secrecy with a transaction;
(d) involvement in cash-intensive businesses;
(e) nature, scope and location of business activities generating the funds/assets, having regard to sensitive or high risk activities; and
(f) where the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified.

Product/service risk

A licensee should consider the characteristics of the products and services that it offers and the extent to which these are vulnerable to ML/TF abuse. In this connection, a licensee 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/TF schemes) before they are introduced and ensure appropriate additional measures and controls are implemented to mitigate and manage the associated ML/TF risks.

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 transactions through online, postal or telephone channels where a non-face-to-face approach is used for establishing business relationship. Business transaction made through intermediaries may also increase risk as the business relationship between the customer and a licensee may become indirect.

4.5 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 through an account, making monitoring of customer transactions and ongoing reviews a fundamental component of a reasonably designed risk-based approach. A licensee 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.

Documenting risk assessment

4.6 **Licensees should keep records and relevant documents of the risk assessment so that they can demonstrate to the Registrar, among others:**

(a) how the customer's ML/TF risks are assessed; and

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

Chapter 5

CUSTOMER DUE DILIGENCE ("CDD")

5.1 **CDD is intended to enable a licensee to form a reasonable belief that it knows the true identity of each customer and, with an appropriate degree of confidence, knows the type of business and transactions the customer is likely to undertake. Licensees should apply a risk-based approach when conducting CDD measures and the extent of CDD measures should be commensurate with the ML/TF risks associated with a business relationship. Schedule 2 to the AMLO contains the CDD requirements. Depending on specific circumstances, licensees may also need to conduct additional measures (referred to as enhanced customer due diligence ("EDD") hereinafter) or, alternatively, may conduct simplified customer due diligence ("SDD").**

APPLYING CDD

5.2 **Licensees are required to carry out the following CDD measures[11] :**

(a) **identifying the customer and verifying the customer's identity** using documents, data or information provided by reliable and independent source;

(b) where there is a beneficial owner in relation to the customer, **identifying and taking reasonable measures**[12] **to verify the beneficial owner's identity** so that the licensee is satisfied that it knows who the beneficial owner is, including in the case where the customer is a legal person or trust, measures to enable the licensee to understand the ownership and control structure of the legal person or trust;

(c) **obtaining information on the purpose and intended nature of the business relationship (if any) established with the licensee** unless the purpose and intended nature are obvious; and

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

  (i) **identifying the person and taking reasonable measures to verify the person's identity** using documents, data or information provided by reliable and independent source; and

  (ii) **verifying the person's authority to act on behalf of the customer**.

[11] Please refer to section 2 of Part 2 of Schedule 2 to the AMLO.

[12] Licensees may take reasonable measures to verify the identity of the beneficial owner by, for example, researching public information on the beneficial owner or arranging a face-to-face meeting with the beneficial owner, to corroborate the undertaking or declaration provided by the client.

5.3 Under section 1 of Part 2 of Schedule 1 to the AMLO, "customer" is defined to include a client. The meaning of "customer" and "client" should be inferred from its everyday meaning and in the context of industry practice. In this Guideline, "customer" includes "intending borrower" or "borrower", as the case may be.

5.4 Licensees must apply CDD[13]:

(a) before establishing a business relationship with the customer;
(b) before carrying out for the customer an occasional transaction that involves an amount equal to or above HK$120,000 or an equivalent amount in any other currency, whether carried out in a single operation or in several operations that appear to the licensee to be linked;
(c) when the licensee suspects that the customer or the customer's account is involved in ML/TF regardless of the levels of transaction of (b) above;
(d) when the licensee 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.

5.5 The definitions of "business relationship" and "occasional transaction" are set out in section 1 of Part 1 of Schedule 2 to the AMLO:

(a) "business relationship" means a business, professional or commercial relationship between a licensee and a person that has an element of duration, or at the time when the person first contacts the licensee in the person's capacity as a potential customer, the licensee expects the relationship to have an element of duration; and
(b) "occasional transaction" means a transaction between a licensee and a customer who does not have a business relationship with the licensee.

[13] Please refer to section 3(1) of Part 2 of Schedule 2 to the AMLO.

Handling occasional transactions

Insofar as occasional transactions are concerned, licensees should be vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD threshold of HK$120,000. Where licensees become aware that these thresholds are reached or exceeded, full CDD procedures must be applied. The factors linking occasional transactions are inherent in the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over a short period and where a customer regularly transfers funds to one or more destinations. In determining whether the transactions are in fact linked, licensees should consider these factors against the timeframe within which the transactions are conducted.

The purpose and intended nature of business relationship[14]

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

B. Unless the purpose and intended nature are obvious, licensees 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 account opening documentation. Depending on the licensee's risk assessment of the situation, information that might be relevant includes:

(a) nature and details of the business/occupation/employment of the customer;
(b) the anticipated level and nature of the activity that is to be undertaken through the relationship (e.g. what the typical transactions are likely to be);
(c) location of customer;
(d) the expected source and origin of the funds to be used in the relationship; and
(e) initial and ongoing source(s) of wealth or income.

[14] Please refer to section 2(1)(c) of Part 2 of Schedule 2 to the AMLO.

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

Can CDD be completed after the creation of a business relationship[15]?

5.6 **A licensee must complete the CDD process before establishing any business relationship or before carrying out a specified occasional transaction. Where the licensee 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/TF and filing an STR with the JFIU.**

5.7 Customer identification information (including information on beneficial owners of the customer, if any) and information about the purpose and intended nature of the business relationship should be obtained before the business relationship is entered into. However, licensees may, exceptionally, verify the identity of the customer and any beneficial owner after establishing the business relationship, provided that:

(a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed;
(b) this is necessary not to interrupt the normal conduct of business with regard to the customer;
(c) the verification is completed as soon as reasonably practicable; and
(d) the business relationship will be terminated if verification cannot be completed as soon as reasonably practicable.

5.8 The licensee must not apply the exception of paragraph 5.7 above where:

(a) the licensee has knowledge or a suspicion of ML/TF;
(b) the licensee becomes aware of anything which causes it to doubt the identity or intentions of the customer or beneficial owner; or
(c) the business relationship is assessed to pose a higher risk.

[15] Please refer to section 3 of Part 2 of Schedule 2 to the AMLO.

Establishing business relationship prior to identity verification – Policies and procedures

The policies and procedures to be adopted by licensees include:

(a) establishing timeframes for the completion of the identity verification measures;

(b) regular monitoring of such relationships pending completion of the identity verification, and keeping senior management periodically informed of any pending completion cases;

(c) obtaining all other necessary CDD information;

(d) ensuring verification of identity is carried out as soon as it is reasonably practicable;

(e) advising the customer of the licensee's obligation to terminate the relationship at any time on the basis of non-completion of the verification measures;

(f) placing appropriate limits on the number of transactions and type of transactions that can be undertaken pending verification; and

(g) ensuring that funds are not paid out to any third party. Exceptions may be made to allow payments to third parties subject to the following conditions:

  (i) there is no suspicion of ML/TF;

  (ii) the risk of ML/TF is assessed to be low;

  (iii) the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction; and

  (iv) the names of recipients do not match with watch lists such as those for terrorist suspects and PEPs.

Failure to complete verification of identity[16]

5.9 **Verification of identity should be concluded within a reasonable timeframe. Where verification cannot be completed within such a period, the licensee should, as soon as reasonably practicable, suspend or terminate the business relationship unless there is a reasonable explanation for the delay.** In this regard:

(a) if a licensee cannot complete identity verification within 60 working days after the establishment of a business relationship with a customer, the licensee should suspend the business relationship and refrain from carrying out further transactions (except to return funds to their sources, to the extent that this is possible); and

(b) if a licensee cannot complete identity verification within 120 working days after the establishment of the business relationship, the licensee should terminate the business relationship with the customer.

5.10 The licensee should assess whether the aforesaid failures provide grounds for knowledge or suspicion of ML/TF and a report to the JFIU is appropriate. The licensee must not, knowing or suspecting that a disclosure has been made to the JFIU, disclose to any other person any matter which is likely to prejudice any investigation. Doing so would constitute "tipping-off", which is an offence prohibited by section 25A(5) of the DTROPO/OSCO and section 12(5) of the UNATMO. For more information, please refer to paragraph 7.3 of this Guideline.

5.11 Wherever possible, when terminating a relationship where funds or other assets have been received, the licensee should return the funds or assets to the source from which they were received. In general, this means that the funds or assets should be returned to the customer/account holder. However, it may not be applicable where the licensee is served a restraint order or confiscation order. Please refer to paragraph 7.20 of this Guideline.

5.12 Licensees must guard against the risk of ML/TF since this is a possible means by which funds can be "transformed", e.g. from cash into a cashier order. Where the customer requests that money or other assets be transferred to third parties, the licensee should assess whether this provides grounds for knowledge or suspicion of ML/TF and a report to the JFIU is appropriate.

[16] Please refer to section 3(4) of Part 2 of Schedule 2 to the AMLO.

Keeping customer information up-to-date[17]

5.13 **Licensees should take steps from time to time to ensure that customers' information obtained for the purposes of complying with the requirements of sections 2 and 3 of Part 2 of Schedule 2 to the AMLO is up-to-date and relevant.**

5.14 Licensees should undertake periodic reviews of existing records of customers and conduct review under circumstances of certain triggering events, including:

(a) when a significant transaction (i.e. in terms of monetary value or where the transaction is unusual or not in line with the licensee's knowledge of the customer) is to take place;
(b) when a material change occurs in the way the customer's account is operated;
(c) when the licensee's customer documentation standards change substantially; or
(d) when the licensee is aware that it lacks sufficient information about the customer concerned.

5.15 In all cases, the factors determining the period of review or what constitutes a triggering event should be clearly defined in the licensees' policies and procedures.

5.16 All high-risk customers (excluding dormant accounts) should be subject to a minimum of an annual review, and more frequently if deemed necessary by the licensee, of their profile to ensure the CDD information retained remains up-to-date and relevant. The licensees should however clearly define what constitutes a dormant account in their policies and procedures.

Identifying and verifying customer's identity[18]

5.17 **Licensees must identify the customer and verify the customer's identity by reference to documents, data or information provided by:**

(a) a governmental body;
(b) the Registrar or any other RA;
(c) an authority in a place outside Hong Kong that performs functions similar to those of the Registrar or any other RA;
(d) a digital identification system that is a reliable and independent source that is recognized by the Registrar; or

[17] Please refer to section 5(1)(a) of Part 2 of Schedule 2 to the AMLO.
[18] Please refer to section 2(1)(a) of Part 2 of Schedule 2 to the AMLO.

(e) any other reliable and independent source that is recognized by the Registrar.

5.18 Guidance for the identification and verification of different types of customers (including their beneficial owners) are set out in the appendices of this Guideline:

Customer type	Appendix
Individual	**A**
Corporation	**B**
Partnership or unincorporated body	**C**
Trust	**D**

5.19 Licensees should recognise that some types of documents are more easily forged than others. If there is suspicion in relation to any documents provided by customers, licensees should take steps to establish whether the document provided 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) or requesting corroboratory evidence from the customer. Where suspicion remains, the document in question should not be accepted and consideration should be given to making a report to the authorities.

Identifying and verifying customer's beneficial owner[19]

A. As a general rule, a beneficial owner of a customer is an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. Please refer to Appendices B, C and D of this Guideline for the definitions of the beneficial owner in relation to a corporation, partnership, unincorporated body or trust respectively.

B. A licensee must identify any beneficial owner in relation to a customer, and, based on its assessment of the ML/TF risks, take reasonable measures to verify the beneficial owner's identity so that the licensee is satisfied that it knows who the beneficial owner is.

[19] Please refer to section 2(1)(b) of Part 2 of Schedule 2 to the AMLO.

Identifying and verifying a person purporting to act on behalf of a customer[20]

A. If a person purports to act on behalf of the customer, licensees 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 Registrar or any other RA;
  (iii) an authority in a place outside Hong Kong that performs functions similar to those of the Registrar or any other RA; or
  (iv) any other reliable and independent source that is recognized by the Registrar; and

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

B. The general requirement is to obtain the identification information as set out in paragraph 1 of Appendix A of this Guideline from the person. In taking measures to verify the identity of the person purporting to act on behalf of a customer (e.g. authorised signatories and attorneys), the licensee should refer to the documents and other means listed in Appendix A of this Guideline wherever possible. As a general rule, licensees should identify and verify the identity of those authorised to give instructions for the movement of funds or assets.

C. Licensees should obtain written authority (including board resolution or similar written authority for corporations) to verify that the individual purporting to represent the customer is authorised to do so.

[20] Please refer to section 2(1)(d) of Part 2 of Schedule 2 to the AMLO.

Verification of documents in a language other than Chinese or English

For documents in a language other than Chinese or English, appropriate steps should be taken by the licensee to be satisfied that the documents in fact provide evidence of the customer's identity (e.g. ensuring that staff assessing such documents is proficient in the language or obtaining a translation from a suitably qualified person).

APPLYING SDD

Application of SDD[21]

5.20 **Where SDD applies (see paragraph 5.22 below), the licensee is not required to identify and verify the beneficial owner. However, other aspects of CDD must be undertaken and it is still necessary to conduct ongoing monitoring of the business relationship. Licensees must have solid grounds to support the use of SDD and may have to demonstrate these grounds to the Registrar.**

5.21 Nonetheless, SDD must not be applied when the licensee suspects that the customer, the customer's account or the transaction is involved in ML/TF, or when the licensee doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity, notwithstanding that the type of customers falls within paragraph 5.22 below (see section 3(1)(d) and (e) of Part 2 of Schedule 2 to the AMLO).

To whom may SDD be applied?

5.22 Customers to whom SDD may be applied are[22]:

(a) a financial institution;
(b) an institution that-
  (i) is incorporated or established in an equivalent jurisdiction[23];
  (ii) carries on a business similar to that carried on by a financial institution;

[21] Please refer to section 4 of Part 2 of Schedule 2 to the AMLO.
[22] Please refer to section 4(3) of Part 2 of Schedule 2 to the AMLO.
[23] "Equivalent jurisdiction" referred to in this Guideline means a jurisdiction that is a member of the FATF, other than Hong Kong, or a jurisdiction that imposes requirements similar to those imposed under Schedule 2 to the AMLO.

(iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 to the AMLO; and

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

(c) a corporation listed on any stock exchange;

(d) an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is-

(i) a financial institution; or

(ii) an institution that-

- is incorporated or established in Hong Kong or in an equivalent jurisdiction;
- has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 to the AMLO; and
- is supervised for compliance with those requirements;

(e) the Government or any public body in Hong Kong; or

(f) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.

Checking of customer's identity to ascertain whether SDD is applicable

A. To ascertain whether a customer is within categories (a) to (d) of paragraph 5.22 above, it will be generally sufficient for licensees to:

(a) verify that the customer is a financial institution or institution on the list of authorised (or supervised) financial institutions in the jurisdiction concerned;
(b) obtain proof of listed status on a stock exchange; or
(c) ascertain that the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle falls within any of the categories of institution set out in section 4(3)(d) of Part 2 of Schedule 2 to the AMLO.

B. If a customer not falling within section 4(3) of Part 2 of Schedule 2 to the AMLO has in its ownership chain an entity that falls within that section, licensees are not required to identify or verify the beneficial owners of that entity in that chain when establishing a business relationship with or carrying out an occasional transaction for the customer. However, licensees should still identify and take reasonable measures to verify the identity of beneficial owners in the ownership chain that are not connected with that entity.

What customer information should be collected under SDD[24]?

5.23 Licensees should:

(a) identify the customer and verify the customer's identity;
(b) if a business relationship is to be established and its purpose and intended nature are not obvious, obtain information on the purpose and intended nature of the business relationship with the licensee; and
(c) 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; and
  (ii) verify the person's authority to act on behalf of the customer.

[24] Please refer to section 4(1) of Part 2 of Schedule 2 to the AMLO.

APPLYING EDD

Situations where special requirements on CDD is required

5.24 By reference to section 15 of Part 2 of Schedule 2 to the AMLO, a licensee must take additional measures or EDD to mitigate the risk of ML/TF in any situation that by its nature presents a higher risk of ML/TF.

5.25 **Guidance for the application of additional measures or EDD in respect of the following situations are set out in paragraphs 5.27 to 5.50 below:**

(a) customer not physically present for identification purposes;
(b) customer or its beneficial owner being a PEP;
(c) corporate customer which has issued bearer shares;
(d) customer from or transaction connected with a jurisdiction identified by the FATF as having strategic AML/CTF deficiencies; and
(e) any situation specified by the Registrar in a notice given to the licensee.

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

Customer not physically present for identification purposes[25]

5.27 Where a customer is not physically present for identification purposes, licensees will generally not be able to determine that the documentary evidence of identity actually relates to the customer they are dealing with. Consequently, the risk in respect of the customer increases.

5.28 In order to mitigate the risk, a licensee is required to take additional measures by reference to sections 5(3)(a)[26] and 9 of Part 2 of Schedule 2 to the AMLO. Except for the situation specified in paragraph 5.29 below, if a customer has not been physically present for identification purposes, the licensee must carry out at least one of the following measures to mitigate the risk posed:

(a) further verifying the customer's identity on the basis of documents, data or

[25] Please refer to section 9 of Part 2 of Schedule 2 to the AMLO.
[26] Section 5(3)(a) of Part 2 of Schedule 2 to the AMLO is subject to section 5(4) of Part 2 of Schedule 2 to the AMLO.

information referred to in paragraph 5.17 above but not previously used for the purposes of verification of the customer's identity;

(b) taking supplementary measures to verify information relating to the customer that has been obtained by the licensee;

(c) ensuring that the first payment made in relation to the customer's account is carried out through an account opened in the customer's name with an authorized institution, or a bank operating in an equivalent jurisdiction that has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 to the AMLO and is supervised for compliance with those requirements by a banking regulator in that jurisdiction.

5.29 If a licensee has verified the identity of the customer on the basis of data or information provided by a digital identification system that is a reliable and independent source that is recognized by the Registrar (see paragraph 5.17 above), the licensee is not required to carry out any additional measures set out in paragraph 5.28 above [27].

5.30 Consideration should be given by licensees to mitigate ML/TF risk by obtaining copies of documents that have been certified by a suitable certifier. 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.

[27] Please refer to section 9(2) of Part 2 of Schedule 2 to the AMLO.

Certifying the verification of identity documents

A. Suitable persons for certifying verification of identity documents may include:

(a) an intermediary specified in section 18(3) of Part 2 of Schedule 2 to the AMLO, including an accounting professional, an estate agent, a legal professional and a TCSP licensee;
(b) a member of the judiciary in an equivalent jurisdiction;
(c) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity;
(d) a Justice of the Peace; and
(e) other professional person[28] such as certified public accountant, lawyer, notary public and professional company secretary[29].

B. The certifier must sign and date the copy document (printing his/her name clearly in capitals underneath) and indicate clearly 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).

C. Licensees 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 licensee is unsure of the authenticity of certified documents, or that the documents relate to the customer, the licensee should take additional measures to mitigate the ML/TF risk.

[28] A licensee may accept other appropriate professional person as certifier. The licensee should have due consideration to paragraph C of this text box under paragraph 5.30 in similar manner to other types of appropriate certifiers being used.

[29] Please refer to the meaning of "professional company secretaries" set out in the Companies Registry External Circular No. 7/2022 on "Translation and Certification of Documents" (or the latest version of a superseding Circular) at Companies Registry's website (www.cr.gov.hk).

Customer or its beneficial owner being a PEP

5.31 The definitions of different types of PEPs are set out as follows:

Definitions of different types of PEPs

A. A ***non-Hong Kong PEP***[30] is defined as:

(a) an individual who is or has been entrusted with a prominent public function in a place outside Hong Kong 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) above;

(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) above (see paragraph C below).

B. A ***former non-Hong Kong PEP***[31] is defined as:

(a) an individual who, being a non-Hong Kong PEP, has been but is not currently entrusted with a prominent public function in a place outside Hong Kong;

(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) above (see paragraph C below).

C. A **close associate**[32] is defined as:

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

(e) 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 A(a).

[30] Please refer to section 1 of Part 1 of Schedule 2 to the AMLO for the definition of "politically exposed person".

[31] Please refer to section 1 of Part 1 of Schedule 2 to the AMLO for the definition of "former politically exposed person".

[32] Please refer to section 1(3) of Part 1 of Schedule 2 to the AMLO.

D. A ***Hong Kong PEP*** means:

(a) an individual who is or has been entrusted with a prominent public function in Hong Kong and

(i) includes head of government, senior politician, senior government or judicial official, senior executive of a government-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) above;

(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) above (see paragraph C above).

E. An ***international organisation PEP*** means:

(a) an individual who is or has been entrusted with a prominent function by an international organisation, and

(i) includes members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions;

(ii) but does not include a middle-ranking or more junior official of the international organisation;

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a), 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) above (see paragraph C above).

F. International organisations referred to in paragraph E above are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organisation for Security and Co-operation in Europe and the Organisation of American States; military international organisations such as the North Atlantic Treaty Organisation, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.

EDD measures for non-Hong Kong PEPs

Use of publicly available information for assessment of non-Hong Kong PEP

A. Licensees 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 non-Hong Kong PEP[33].

B. Licensees may also use publicly available information or refer to relevant reports and databases on corruption risk published by specialised national, international, non-governmental 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). Licensees should be vigilant where either the country to which the customer has business connections or the business/industrial sector is more vulnerable to corruption.

5.32 When licensees know that a particular customer or beneficial owner is a non-Hong Kong PEP, they should, before establishing a business relationship or continuing an existing business relationship where the customer or the beneficial owner is subsequently found to be a non-Hong Kong PEP, apply all the following EDD measures[34]:

(a) obtaining approval from its senior management; and
(b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds.

5.33 Licensees should conduct enhanced ongoing monitoring[35] of a business relationship with a customer if the customer or the beneficial owner of the customer is a non-Hong Kong PEP. Reference should be made to Chapter 6 of this Guideline.

[33] Please refer to section 19(1) of Part 2 of Schedule 2 to the AMLO.
[34] Please refer to section 10 of Part 2 of Schedule 2 to the AMLO.
[35] Please refer to section 5(3)(b) of Part 2 of Schedule 2 to the AMLO.

EDD measures for Hong Kong PEPs and international organisation PEPs

5.34 Licensees should take reasonable measures to determine whether a customer or a beneficial owner of a customer is a Hong Kong PEP or an international organisation PEP.

5.35 Licensees should apply the measures set out in paragraphs 5.32 and 5.33 above in any of the following situations[36]:

(a) before establishing a high risk business relationship[37] with a customer who is or whose beneficial owner is a Hong Kong PEP or an international organisation PEP;
(b) when continuing an existing business relationship with a customer who is or whose beneficial owner is a Hong Kong PEP or an international organisation PEP where the relationship subsequently becomes high risk; or
(c) when continuing an existing high risk business relationship where the licensee subsequently knows that the customer or the beneficial owner of the customer is a Hong Kong PEP or an international organisation PEP.

Treatment of former non-Hong Kong PEPs

5.36 Following a risk-based approach[38], a licensee may decide not to apply or continue to apply the measures set out in paragraphs 5.32 and 5.33 above to a customer who is or whose beneficial owner is a former non-Hong Kong PEP[39]. Such decision can only be made with the approval of the licensee's senior management and on the basis that the PEP does not present a high risk of ML/TF. To determine whether a former non-Hong Kong PEP does not present a high risk of ML/TF, the licensee should conduct an appropriate assessment on the ML/TF risk associated with the PEP status taking into account various risk factors, including but not limited to:

(a) the level of (informal) influence that the individual could still exercise;
(b) the seniority of the position that the individual held as the PEP; and

[36] For the avoidance of doubt, licensees should consider whether the application of measures in paragraphs 5.32 and 5.33 of this Guideline could mitigate the ML/TF risk arising from the high risk business relationship with a Hong Kong PEP or an international organisation PEP. Where applicable, licensees must also apply measures to mitigate such risk in accordance with the guidance provided in paragraphs 5.24 and 5.26.

[37] In determining whether a business relationship presents a high ML/TF risk, licensees should take into account all risk factors that are relevant to the business relationship.

[38] The handling of a former non-Hong Kong PEP should be based on an assessment of risk and not merely on prescribed time limits.

[39] Please refer to sections 5(5) and 10(3) of Part 2 of Schedule 2 to the AMLO.

(c) whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the PEP's successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

Treatment of former Hong Kong PEPs and former international organisation PEPs

5.37 Following a risk-based approach[40], for a Hong Kong PEP or an international organisation PEP who has been but is not currently entrusted with a prominent (public) function, a licensee may decide not to apply or continue to apply the measures set out in paragraphs 5.32 and 5.33 above in a high risk business relationship with a customer who is or whose beneficial owner is a former Hong Kong PEP or former international organisation PEP[41]. Such decision can only be made on the basis that the PEP dose not present a high risk of ML/TF. To determine whether a former Hong Kong PEP or former international organisation PEP does not present a high risk of ML/TF, the licensee should conduct an appropriate assessment on the ML/TF risk associated with the PEP status taking into account various risk factors, including but not limited to:

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

Further guidance applied to all types of PEPs

5.38 Licensees should implement appropriate risk management systems to identify PEPs. The definitions of PEPs set out above provide some non-exhaustive examples of the types of prominent (public) functions that an individual may be or may have been entrusted with by a government, or by an international organisation. Licensees should provide sufficient guidance and examples to their staff to enable them to identify all types of PEPs. In determining what constitutes a prominent (public) function, the licensee should consider on a case-by-case basis taking into account various factors, for example: the powers and responsibilities associated with particular public function; the organisational framework of the relevant government or international organisation; and any other specific concerns connected to the jurisdiction where the public function is/has been entrusted.

[40] The handling of a former Hong Kong PEP or former international organization PEP should be based on an assessment of risk and not merely on prescribed time limits.

[41] For the avoidance of doubt, such decision may also apply to a spouse, a partner, a child or a parent, or a spouse or a partner of a child, or a close associate of the former Hong Kong PEP or former international organization PEP.

5.39 While a licensee may refer to commercially available databases to identify PEPs, the use of these databases should never replace traditional CDD processes (e.g. understanding the occupation and employer of a customer). When using commercially available databases, the licensee should be aware of their limitations, for example, the databases are not necessarily comprehensive or reliable as they generally draw solely from information that is publicly available; the definition of PEPs used by the database providers may or may not align with the definition of PEPs applied by the licensee; and any technical incapability of such databases that may hinder the licensee's effectiveness of PEP identification. Therefore, the licensee should only use such databases as a support tool and ensure they are fit for purpose.

5.40 Since not all PEPs pose the same level of ML risks, a licensee should adopt a risk-based approach in determining the extent of EDD measures in paragraph 5.32 and enhanced ongoing monitoring in paragraph 5.33 above taking into account relevant factors, such as:

(a) the nature of the prominent (public) functions that a PEP holds;
(b) the geographical risk associated with the jurisdiction where a PEP holds prominent (public) functions;
(c) the nature of the business relationship (e.g. the delivery/distribution channel used; or the product or service offered); and
(d) if the PEP becomes a former PEP, the risk factors specified in paragraphs 5.36 and 5.37 above.

5.41 Each licensee should adopt reasonable measures, in accordance with its assessment of the risk, for establishing 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. Licensees should however note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. Licensees should also be aware that some jurisdictions impose restrictions on their PEP's ability to hold foreign bank accounts or to hold other office or paid employment.

5.42 The approval person of the licensee should take into account the advice of the CO. The more potentially sensitive the PEP is, the more senior the approving person should be. Licensees should retain a copy of the assessment for inspection by the Companies Registry ("the CR"), other authorities and auditors and should review the assessment whenever concerns as to the activities of the individual arise.

Corporate customer which has issued bearer shares

5.43 Bearer shares are equity securities wholly owned by whoever holds the physical share certificate. The issuing corporation does not register the owner of the shares or track transfers of ownership. Transferring the ownership of the shares involves only delivering the physical share certificate. Bearer shares therefore lack the regulation and control of common shares because ownership is never recorded. Owing to the higher ML/TF risk associated with bearer shares, the FATF recommends member countries that have legal persons able to issue bearer shares should take appropriate measures to ensure that they are not misused for ML/TF.

5.44 To reduce the opportunity for bearer shares to be used to obscure information on beneficial ownership, licensees must take additional measures as required by section 15 of Part 2 of Schedule 2 to the AMLO in the case of corporate customer with capital in the form of bearer shares, as it is often difficult to identify the beneficial owner(s) in such situation. Licensees 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.

5.45 Where bearer shares have been deposited with an authorised/registered custodian, licensees should seek independent evidence of such arrangement, e.g. confirmation from the registered agent that an authorised/registered custodian holds the bearer shares, the identity of the authorised/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 licensee's ongoing periodic review, it should obtain evidence to confirm the identity of authorised/registered custodian of the bearer shares.

5.46 Where the bearer shares are not deposited with an authorised/registered custodian, licensees should obtain declarations prior to account opening and annually thereafter from each beneficial owner holding more than 25% of the share capital. Given the higher ML/TF risk associated with bearer shares, licensees may wish to adopt higher levels of risk mitigation than prescribed in the AMLO. Licensees should also require customers to notify them immediately of any changes in the ownership of the shares.

Customer from or transaction connected with a jurisdiction identified by the FATF as having strategic AML/CTF deficiencies

5.47 Licensees should give particular attention to, and exercise extra care in respect of:

(a) business relationships and transactions with persons (including natural persons and legal persons) from or in jurisdictions identified by the FATF as having strategic AML/CTF deficiencies; and
(b) transactions and business connected with jurisdictions assessed as higher risk.

5.48 Based on the licensee's assessment of the risk in either case, EDD may apply. In addition to ascertaining and documenting the business rationale for establishing a relationship, a licensee should take reasonable measures to establish the source of funds of such customers.

Higher risk jurisdictions

Factors which licensees may take into consideration

A. In determining which jurisdictions are identified by the FATF as having strategic AML/CTF deficiencies, or may otherwise pose a higher risk, licensees should consider, among other things:

(a) any relevant notification issued to licensees by the Registrar;

(b) whether the jurisdiction is subject to sanctions, embargoes or similar measures issued by, for example, the United Nations. In addition, in some circumstances where a jurisdiction is subject to sanctions or measures similar to those issued by bodies such as the United Nations, but which may not be universally recognised, the sanctions or measures may still be given credence by a licensee 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/CTF 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.

B. "Credible sources" refers to well-known bodies that generally are regarded as reputable and that make information produced by them publicly and widely available. In addition to the FATF and similar regional bodies, such sources may include, but are not limited to, supra-national 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 a jurisdiction is of higher risk.

High-risk situation specified in a Notice given by the Registrar[42]

5.49 Licensees must apply additional measures, proportionate to the risks and in accordance with the guidance provided in relation to EDD in this Chapter 5, to business relationships and transactions with natural and legal persons from jurisdictions for which this is called for by the FATF.

5.50 Where the requirement is called for by the FATF (which may include mandatory enhanced measures or counter-measures[43] called for by the FATF) or in other circumstances which are considered to be higher risk, the Registrar may issue a notice to the licensee in respect of the situation specified in the notice to:

(a) impose an obligation on licensees to undertake EDD measures; or
(b) require licensees to undertake specific counter-measures identified or described in the notice.

Prohibition on anonymous accounts[44]

Licensees must not open or maintain anonymous accounts or accounts in fictitious names for any new or existing customer. Where numbered accounts exist, licensees must maintain them in such a way that full compliance can be achieved with the AMLO. Licensees must properly identify and verify the identity of the customer in accordance with this Guideline. In all cases, whether the relationship involves numbered accounts or not, the customer identification and verification records must be made available to the CO, the Registrar, other RAs, other authorities, auditors, and other staff with appropriate authority.

[42] Please refer to section 15 of Part 2 of Schedule 2 to the AMLO.
[43] For jurisdictions with serious deficiencies in applying the FATF Recommendations and where inadequate progress has been made to improve their position, the FATF may recommend the application of counter-measures.
[44] Please refer to section 16 of Part 2 of Schedule 2 to the AMLO.

Application of AMLO to pre-existing customers[45]

A Licensees must perform the CDD measures prescribed in Schedule 2 to the AMLO and this Guideline in respect of pre-existing customers (with whom the business relationship was established before the initial publication of this Guideline on 21 September 2018), when:

(a) a transaction takes place with regard to the customer which, by virtue of the amount or nature of the transaction, is unusual or suspicious; or is not consistent with the licensee'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's business or account is operated;

(c) the licensee suspects that the customer or the customer's business or account is involved in ML/TF; or

(d) the licensee 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.

B. Trigger events may include the re-activation of a dormant account of the customer or a change in the beneficial ownership or control of the account but licensees will need to consider other trigger events specific to their own customers and businesses.

C. If a licensee is unable to comply with the above requirements, it must terminate its business relationship with the customer as soon as reasonably practicable.

D. Licensees should note that requirements for ongoing monitoring under section 5 of Part 2 of Schedule 2 to the AMLO also apply to pre-existing customers.

[45] Please refer to section 6 of Part 2 of Schedule 2 to the AMLO.

CARRYING OUT CDD BY MEANS OF INTERMEDIARIES[46]

5.51 **A licensee may carry out any CDD measure by means of an intermediary if:**

(a) the intermediary consents in writing to be the licensee's intermediary; and

(b) the licensee is satisfied that the intermediary will on request provide a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out the CDD measures without delay.[47]

However, the ultimate responsibility for ensuring that CDD requirements are met remains with the licensee and the licensee remains liable for a failure to carry out CDD measures[48].

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

5.53 **The licensee must ensure that the intermediary will, if requested by the licensee within the period specified in the record-keeping requirements of the AMLO, provide to the licensee a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out CDD measures as soon as reasonably practicable after receiving the request.**

5.54 **A licensee 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 licensee to obtain at the same time from the intermediary a copy of any document, or a record of any data or information, that is obtained by the intermediary in the course of carrying out that measure.**

5.55 Where these documents and records are kept by the intermediary, the licensee should obtain an undertaking from the intermediary to keep all underlying CDD information

---

[46] Please refer to section 18 of Part 2 of Schedule 2 to the AMLO.

[47] Please refer to section 18(1) of Part 2 of Schedule 2 to the AMLO. The purpose of obtaining the underlying documentation is to ensure that it is immediately available on file for reference purposes by the CR and other relevant authorities such as the JFIU, and for on-going monitoring of the customer. It will also enable the licensee to verify that the intermediary is doing its job properly.

[48] Please refer to section 18(2) of Part 2 of Schedule 2 to the AMLO.

throughout the continuance of the licensee's business relationship with the customer and for at least 5 years beginning on the date on which the business relationship of a customer with the licensee ends or until such time as may be specified by the Registrar. Licensees 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 licensee anymore.

5.56 Licensees should conduct sample checks from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay. Whenever a licensee 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 licensee intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the licensee has any doubts regarding the CDD measures carried out by the intermediary previously, the licensee should perform the required CDD as soon as reasonably practicable.**

5.57 Licensees may carry out any CDD measure by means of intermediaries in Hong Kong or in an equivalent jurisdiction. To ensure the compliance of the requirements set out in paragraphs 5.51 to 5.56 above, licensees should:

(a) review the intermediaries' AML/CTF policies and procedures to ensure that they have adequate policies and procedures in place to prevent money laundering and terrorist financing; or

(b) make enquiries concerning the intermediaries' statures and regulatory track records and the extent to which any of their AML/CTF standards are applied and audited.

Intermediaries in Hong Kong

A. Licensees may carry out any CDD measure by means of a financial institution that is an authorized institution, a licensed corporation, an authorized insurer, a licensed individual insurance agent, a licensed insurance agency or a licensed insurance broker company ("intermediary FI")[49].

B. Licensees may also carry out any CDD measure by means of the following categories of intermediaries[50] in Hong Kong, provided that such intermediaries are able to satisfy the licensee that they have adequate procedures in place to prevent ML/TF and are required to comply with the requirements set out in Schedule 2 to the AMLO with respect to customers:

(a) an accounting professional;
(b) an estate agent;
(c) a legal professional; and
(d) a TCSP licensee.

[49] The relevant terms are as defined in section 1 of Part 2 of Schedule 1 to the AMLO.
[50] The relevant categories are as defined in section 1 of Part 2 of Schedule 1 to the AMLO.

Intermediaries in an equivalent jurisdiction[51]

Licensees may carry out any part of the CDD measure by means of an intermediary in an equivalent jurisdiction where:

(a) the intermediary is:
  (i) a lawyer, a notary public, an auditor, a professional accountant, a trust or company service provider or a tax advisor practising in the jurisdiction;
  (ii) a trust company carrying on trust business in the jurisdiction;
  (iii) a person who carries on in the jurisdiction a business similar to that carried on by an estate agent; or
  (iv) an institution that carries on in the jurisdiction a business similar to that carried on by a financial institution that is an authorized institution, a licensed corporation, an authorized insurer, a licensed individual insurance agent, a licensed insurance agency or a licensed insurance broker company;

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

(c) the intermediary has measures in place to ensure compliance with similar CDD and record-keeping requirements as those imposed under Schedule 2 to the AMLO; and

(d) the intermediary is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs or the regulatory bodies (as may be applicable).

[51] Please refer to section 18(3)(c) of Part 2 of Schedule 2 to the AMLO.

Related foreign financial institutions as intermediaries

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

(a) carries on, in a place outside Hong Kong, a business similar to that carried on by an intermediary FI[52]; and falls within any of the following descriptions:
  (i) it is within the same group of companies[53] as the licensee;
  (ii) if the licensee is incorporated in Hong Kong, it is a branch of the licensee;
  (iii) if the licensee is incorporated outside Hong Kong:
    (A) it is the head office of the licensee; or
    (B) it is a branch of the head office of the licensee;

(b) is required under group policy:
  (i) to have measures in place to ensure compliance with requirements similar to the requirements imposed under Schedule 2 to the AMLO; and
  (ii) to implement programmes against ML/TF; and

(c) is supervised for compliance with the requirements mentioned in paragraph (b) above at a group level:
  (i) by an RA; or
  (ii) by an authority in an equivalent jurisdiction that performs, in relation to the holding company or the head office of the licensee, functions similar to those of an RA.

The group policy set out in paragraph (b) above refers to a policy of the group of companies to which the licensee belongs and the policy applies to the licensee and the related foreign FI. The group policy should be able to mitigate adequately any higher country risk in relation to the jurisdiction where the related foreign FI is located. The licensee should be satisfied that the related foreign FI is subject to regular and independent reviews over its ongoing compliance with the group policy conducted by any group-level compliance, audit or other similar AML/CTF functions.

[52] Please see the definition of "intermediary financial institution" in section 18(7) of Part 2 of Schedule 2 to the AMLO.
[53] "group of companies" has the meaning given by section 2(1) of the Companies Ordinance, Cap. 622.

Chapter 6

ONGOING MONITORING OF BUSINESS RELATIONSHIP WITH CUSTOMERS

Requirements on ongoing monitoring

6.1 Effective ongoing monitoring is vital for understanding customers' activities and an integral part of effective AML/CTF systems. It helps licensees to update their knowledge of their customers and detect unusual or suspicious activities. Failure to conduct ongoing monitoring could expose a licensee to potential abuse by criminals, and may call into question the adequacy of systems and controls.

6.2 **A licensee must continuously monitor the business relationship with a customer by[54]:**

(a) reviewing from time to time documents, data and information relating to the customer that have been obtained for the purpose of complying with CDD requirements to ensure that they are up-to-date and relevant;

(b) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the licensee's knowledge of the customer and the customers' business, risk profile and source of funds; and

(c) identifying transactions that are complex, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose and which may indicate ML/TF.

Aspects for licensees to identify unusual customer transactions

To identify unusual customer transactions, the aspects which licensees should consider include:

(a) the nature and type of individual transactions;
(b) the nature of a series of transactions;
(c) the amount of the transactions, paying special attention to particularly substantial transactions;
(d) the geographical origin/destination of a payment or receipt; and
(e) the customer's usual pattern of activities or turnover.

[54] Please refer to section 5 of Part 2 of Schedule 2 to the AMLO.

6.3 Where the basis of the business relationship changes significantly, licensees should carry out further CDD procedures to ensure that the ML/TF risks involved and basis of the relationship are fully understood.

Changes of business relationship with customers

Licensees should be vigilant for changes in the basis of the business relationship with customers over time. Such changes may include:

(a) setting up new corporate or trust structures (including frequent change of directorship);
(b) buying new products or services that pose higher risk;
(c) unusual changes or increase of the activities or turnover of a customer; or
(d) unusual changes in the nature of transactions of a customer.

6.4 Licensees 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 licensees to assess appropriate levels of ongoing review and monitoring.

Risk-based approach to ongoing monitoring[55]

6.5 The extent of monitoring should be commensurate with the risk profile of the customer compiled through the risk assessment. For effective monitoring, resources should be targeted towards business relationships presenting a higher risk of ML/TF.

6.6 Licensees must take additional measures when monitoring business relationships which pose a higher risk (please see paragraphs 5.24 to 5.50 of this Guideline). High-risk business relationships will require more frequent and intensive monitoring. When monitoring high-risk situations, the 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, relationship managers and insurance agents) with timely information (i.e. the result of EDD or other additional measures undertaken, any information on any connected accounts or relationships, etc.); and
(b) how the sources of funds, wealth and income for higher risk customers will be monitored and how any changes in circumstances will be recorded.

[55] Please refer to section 5 of Part 2 of Schedule 2 to the AMLO.

6.7 There are various methods by which those objectives can be met including exception reports (e.g. large transactions exception report) and transaction monitoring systems. Exception reports will help licensees to monitor their operational activities.

6.8 Where transactions are complex, unusually large in amount or of an unusual pattern, or have no apparent economic or lawful purpose, licensees should examine the background and purposes, including where appropriate the circumstances, of the transactions. The findings and outcomes of these examinations should be properly documented in writing and be available for the inspection by the CR, other competent authorities and auditors. Proper records of the decisions made and the reasons of the decisions will help a licensee demonstrate that its handling of unusual or suspicious activities are appropriate.

Examination of the background and purposes of transactions

Examinations or enquiries may include asking the customer appropriate questions. Such enquiries, when conducted properly and in good faith, will not constitute tipping-off. The results of the enquiries should be properly documented and be available for inspection by the CR, other authorities and auditors. Where there is any suspicion, an STR must be made to the JFIU (please refer to Chapter 7 of this Guideline for details).

Cash transactions and transfers to third parties

In case where cash transactions or transfers to third parties are being proposed by a customer and such requests are not in accordance with the customer's known pattern of practice, the licensee must be cautious and make relevant further enquiries. Where the licensee, having made the necessary enquiries, does not consider the cash transaction or third party transfer reasonable, it should make an STR to the JFIU (please refer to Chapter 7 of this Guideline for details).

6.9 Licensees should be aware that making enquiries to customers, when conducted properly and in good faith, will not constitute tipping-off. However, if the licensee reasonably believes that performing the CDD process will tip off the customer, it may stop pursuing the process. The licensee should document the basis for its assessment and file an STR to the JFIU.

Chapter 7

REPORTING SUSPICIOUS TRANSACTIONS

The requirements

7.1 **CDD and ongoing monitoring of business relationship with customers provide the basis for identifying unusual and suspicious transactions and events. Once a licensee identifies or suspects that a transaction is related to ML/TF activity, the licensee must report the transaction to JFIU.**

Statutory requirements for reporting suspicious transactions

Section 25A of the DTROPO and section 25A of the OSCO make it an offence if a person fails to disclose to an authorized officer (i.e. JFIU) where the person knows or suspects that property represents the proceeds of drug trafficking or of an indictable offence. Likewise, section 12 of the UNATMO makes it an offence to fail to disclose knowledge or suspicion of terrorist property. Under the DTROPO, the OSCO and the UNATMO, failure to report the knowledge or suspicion carries a maximum penalty of three months' imprisonment and a fine of HK$50,000.

7.2 The filing of a report to the JFIU provides the licensee a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report, provided that:

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

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

7.3 **Licensees must note that it is an offence for a person, knowing or suspecting that a disclosure has been made to the JFIU, if he/she discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following the disclosure (commonly referred to as "tipping-off").** The customer's awareness of a possible STR or investigation could prejudice future efforts to investigate the suspected ML/TF operation. Therefore, if licensees form a suspicion that transactions relate to ML/TF, they should take into account the risk of tipping-off when performing the

CDD process. Licensees should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

7.4 **Licensees must ensure sufficient guidance is given to staff to enable them to form suspicion or to recognise the signs when ML/TF is taking place.** The guidance should take into account the nature of the transactions and customer 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.

The "SAFE" approach

A. An effective systemic approach to identify suspicious transactions may safeguard licensees from the risk of being involved with ML/TF. Licensees may adopt, where applicable, the "SAFE" approach promoted by JFIU.

B. Four steps are involved in the SAFE approach:

(a) **S**creen the account for suspicious indicators;
(b) **A**sk the customers appropriate questions;
(c) **F**ind out the customer's records; and
(d) **E**valuate all the above information.

C. Licensees are strongly advised to familiarise themselves with the SAFE approach. Details of the SAFE approach are available at JFIU's website (www.jfiu.gov.hk).

When and how to report suspicious transactions to JFIU?

7.5 **When a licensee knows or suspects that any property represents the proceeds of crime or is terrorist property, a disclosure must be made to the JFIU as soon as it is reasonable to do so.** The use of STR proforma or the e-reporting system named Suspicious Transaction Report And Management System ("STREAMS") to report suspicious transactions is strongly encouraged. Please visit JFIU's website at www.jfiu.gov.hk for full details of reporting methods and advice. In the event that the subject in the disclosure is related to any ongoing investigation, it should be indicated in the STR with the provision of relevant details (i.e. case reference number, name of the investigative unit and the

officer-in-charge etc.), if any. Under exceptional circumstances, an initial notification by telephone may be considered for an urgent disclosure.

7.6 STRs shall be made to the JFIU before a licensee deals with a suspicious transaction or activity (whether the intended transaction ultimately takes place or not) for its customer, or, where the relevant knowledge or suspicion arises only after the transaction or activity has been completed, be made to the JFIU as soon as reasonably practicable and on the licensee's own initiative after the transaction or activity has been completed.

7.7 The law requires the STR be made together with any information or other matter on which the knowledge or suspicion is based. The need for prompt reporting is particularly important where a customer has instructed the licensee to move funds or other property, carry out significant changes to the business relationship, etc. In such circumstances, licensees should consider contacting the JFIU urgently.

Internal reporting of licensees

7.8 Licensees should have measures in place to check, on an ongoing basis, that it has proper policies and procedures to test and ensure compliance with legal and regulatory requirements. The type and extent of the measures to be taken in this respect should be appropriate having regard to the risk of ML/TF and the size of their respective business.

7.9 Licensee's MLRO should act as a central reference point for reporting suspicious transactions. The licensee should ensure that the MLRO is of sufficient status within the organisation, and has adequate resources, to enable the MLRO to perform his/her functions (please refer to paragraph 3.4 of this Guideline for the major responsibilities of the MLRO).

7.10 **A key responsibility of the MLRO is to diligently consider all vital information and report the suspicious transaction or activity or suspicious attempted transaction or activity to the JFIU in accordance with statutory requirements.**

7.11 Licensees should set up and maintain procedures to ensure that:

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

No filtering of reports to MLRO

While licensees may wish to set up internal systems that allow staff to consult their 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**. Since the legal obligation is to report the suspicious transaction as soon as it is reasonable to do so, the 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 the speediness, confidentiality and accessibility of the systems.

7.12 **All suspicious activities reported to the MLRO must be documented. The report must include the full details of the customer and a full statement on the information giving rise to the suspicion. In urgent cases, suspicious activities may be reported verbally, e.g. over the telephone, to be followed by documentation.**

7.13 The MLRO must acknowledge receipt of the report and, at the same time, issue a reminder to the reporting staff of the obligation regarding tipping-off. The tipping-off provision also applies to circumstances where a suspicion has been raised internally, but has not yet been reported to the JFIU.

Reporting further suspicious transactions of the same customer

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

7.14 When evaluating an internal report of suspicious transaction, the MLRO must take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within the organisation concerning the entities to which the report relates.

Steps to be taken by the MLRO include:

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

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

(c) appropriate questioning of the customer using the systematic approach to identifying suspicious transactions as recommended by the JFIU.

7.15 As part of the review, other connected business relationships may need to be examined. Regarding the need to search for information concerning connected business relationships, a balance should be struck between making a timely disclosure to the JFIU as required by law and any delays in making the disclosure that might arise from searching more relevant information. The evaluation process and the conclusion drawn should be documented.

7.16 If after completing the evaluation, a MLRO decides that there are grounds for knowledge or suspicion of transactions related to ML/TF activity, he/she should file an STR to the JFIU as soon as reasonable together with the information or matters on which that knowledge or suspicion is based. If the MLRO decides not to file an STR with the JFIU, provided that the MLRO acts in good faith and reasonable manner and concludes that there is no suspicion after taking into account all available information, it is unlikely that there will be any criminal liability for failing to report. The MLRO should keep proper records of the deliberations and actions taken to demonstrate he/she has acted in reasonable manner.

Keeping of records

7.17 **Licensees must establish and maintain a record of all ML/TF 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 evaluation, whether the report eventually resulted in an STR filed with the JFIU, and information to allow the documentation relevant to the report to be located.

7.18 **Licensees must establish and maintain a record of all STRs 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 STRs to be located. This register may be combined with the register of internal reports, if considered appropriate.

Post-reporting matters

7.19 The JFIU will acknowledge receipt of an STR made by a licensee under section 25A of the DTROPO, section 25A of the OSCO, or section 12 of the UNATMO. The JFIU may, on occasion, seek additional information or clarification with the licensee of any matter on which the knowledge or suspicion is based.

7.20 In some cases, the licensee may also be served the orders below for compliance:

Type of Order	**Production Order**	**Restraint Order**	**Confiscation Order**
Issuing Authority	The Court	The Court	The Court
Purpose or effect of the order	➢ To order the licensee to provide all the information or materials which fall within the scope of the order within the required time limit	➢ To freeze particular funds or property of a person pending the outcome of an investigation	➢ To confiscate, upon the conviction of a defendant, the defendant's criminal proceeds in the event that the licensee holds funds or other property belonging to that defendant
Remarks	➢ The licensee should comply with the order and provide the relevant information and materials within the timeframe stipulated in the order	➢ The licensee must ensure that it is able to freeze the relevant funds or property that is the subject of the order	➢ If the order applies to only part of the funds or property involved within a particular business relationship, the licensee should consider what, if any, funds or property may be utilised subject to the content of the order

Chapter 8

FINANCIAL SANCTIONS, PROLIFERATION FINANCING AND TERRORIST FINANCING

Financial sanctions and proliferation financing

8.1 The Chief Executive makes regulations under the UNSO to implement sanctions, including targeted financial sanctions against certain persons and entities, such as those designated by the Security Council of the United Nations ("Security Council").

8.2 The Chief Executive or the Secretary for Commerce and Economic Development may, by notice published in the Gazette or on the website of the Commerce and Economic Development Bureau ("CEDB") (https://www.cedb.gov.hk/en/policies/united-nations-security-council-sanctions.html), specify persons or entities designated by the Security Council or its Sanctions Committees for the purpose of financial sanctions. Except under the authority of a licence granted by the Chief Executive, it is an offence:

(a) to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of,
  (i) a designated person or entity;
  (ii) those persons or entities acting on behalf of or at the direction of designated persons or entities; or
  (iii) entities owned or controlled by the aforementioned; or
(b) to deal with, directly or indirectly, any funds, other financial assets, or economic resources belonging to, or owned or controlled by, such persons or entities.

A licensee seeking such a licence should write to the CEDB. Offenders will be subject to a maximum sentence of 7 years' imprisonment and a fine.

8.3 The prohibitions imposed by the regulations made under the UNSO apply to all persons including money lenders. All persons are required to report any asset frozen or actions taken in compliance with the financial sanctions requirements by way of filing an STR to the JFIU. Lists of persons and entities subject to financial sanctions under the UNSO are available on CR's website (www.cr.gov.hk).

8.4 The counter PF regime in Hong Kong is implemented through legislation, including the regulations made under the UNSO which are specific to the Democratic People's Republic of Korea and the Islamic Republic of Iran, and the WMD(CPS)O. Section 4 of the

WMD(CPS)O prohibits a person from providing any services where he/she believes or suspects, on reasonable grounds, that those services may be connected to weapon of mass destruction proliferation. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

Sanctions imposed by other jurisdictions

Licensees do not normally have any obligation under Hong Kong laws to have regard to unilateral sanctions imposed by other authorities in other jurisdictions. However, a licensee with international operations will need to be aware of the sanctions regimes in those jurisdictions. Where these sanctions may affect their operations, licensees should consider the implications and take appropriate measures where necessary.

Terrorist Financing

8.5 According to the FATF's definition, terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organisations. Section 7 of the UNATMO prohibits the provision or collection of property for use to commit terrorist acts. Section 8 of the UNATMO prohibits any person from making available or collecting/soliciting property or financial (or related) services for terrorists and terrorist associates.

Background of the UNATMO

A. The United Nations Security Council Resolution ("UNSCR") 1373 calls on all member states to act to prevent and suppress the financing of terrorist acts.

B. The United Nations has also published the names of individuals and organisations subject to United Nations financial sanctions in relation to involvement with Al-Qa'ida, ISIL (Da'esh) and the Taliban. All United Nations member states are required to freeze the funds and other financial assets or economic resources of any person(s) named in the lists and to report any suspected name matches to the relevant authorities. The obligation is extended to the prohibition of making available such funds and other financial assets or economic resources for the benefit of such persons.

C. In Hong Kong, the UNATMO was enacted in 2002 and amended in 2004 and 2012 to implement UNSCR 1373, some terrorism-related multilateral conventions, and certain recommendations of the FATF. The UNATMO was further amended in 2018 having regard to UNSCR 2178 which affirmed the need to combat threats by foreign terrorist fighters, as well as FATF's recommendation on enhancing the freezing mechanism of terrorist property.

8.6 Where a person or property is designated by a Committee of the Security Council established pursuant to the Resolutions 1267 (1999), 1989 (2011) and 2253 (2015) and the Resolution 1988 (2011) as a terrorist / terrorist associate or terrorist property, and the details are specified and published under section 4 of the UNATMO in the Government Gazette, such specifications will also be available at the CR's website (www.cr.gov.hk).

8.7 Section 5 of the UNATMO also provides that the Chief Executive may make an application to the Court of First Instance for an order to specify a person or property as a terrorist / terrorist associate or terrorist property[56]. The Court will only make the order if it is satisfied that the person or property is a terrorist / terrorist associate or terrorist property.

8.8 According to section 6 of the UNATMO, 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 granted by S for S.

[56] According to section 2 of UNATMO, terrorist property means the property of a terrorist or a terrorist associates, or any other property that is intended to be used or was used to finance or assist the commission of terrorist acts.

Contraventions are subject to a maximum penalty of 7 years' imprisonment and a fine. Section 8A of the UNATMO also provides that a person shall not deal with any property, knowing that, or being reckless as to whether, the property is (a) specified terrorist property, (b) owned or controlled by a specified terrorist or terrorist associate, or (c) held on behalf of, or at the direction of, a specified terrorist or terrorist associate. Contraventions are subject to a maximum penalty of 14 years' imprisonment and a fine.

8.9 S for S can grant licence to enable the property mentioned at paragraph 8.8 above be dealt with. A licensee seeking such a licence should write to the Security Bureau.

8.10 It is an offence under section 8 of the UNATMO for any person to make any property or financial (or related) 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. 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 a fine.

Sections 8 and 8A of the UNATMO

Section 8 of the UNATMO prohibits a person from:

(a) making available, by any means, directly or indirectly, any property or financial (or related) services to or for the benefit of a person knowing that, or being reckless as to whether, such person is a terrorist or terrorist associate, except under the authority of a licence granted by S for S; and

(b) collecting property or soliciting financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, such person is a terrorist or terrorist associate.

Section 8A of the UNATMO prohibits a person from dealing with any property, knowing that, or being reckless as to whether, the property is:

(a) specified terrorist property;

(b) owned or controlled by a specified terrorist or terrorist associate; or

(c) held on behalf of, or at the direction of, a specified terrorist or terrorist associate.

8.11 Section 11L of the UNATMO prohibits any person from providing or collecting property with the intention or knowing that the property will be used, in whole or in part, to finance the travel of a person between states for the purpose of the perpetration, planning or preparation of, or participation in, terrorist acts, or the provision or receiving of terrorist training (whether or not the property is actually so used). Contraventions are subject to a maximum penalty of 7 years' imprisonment and a fine.

8.12 Licensees may also draw reference from different sources including relevant designation by overseas authorities, such as the designations made by the US Government under relevant Executive Orders.

8.13 All licensees will therefore need to ensure that they should have an appropriate system to conduct name checks against the relevant list(s) for screening purposes and that the list(s) is/are up-to-date.

Database maintenance and screening (customers and payments)

8.14 Licensees should take measures to ensure compliance with the relevant regulations and legislation on terrorist financing. The legal obligations of licensees and those of its staff should be well understood and adequate guidance and training should be provided to the staff. Licensees 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.

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

Screening of Customer

A. Licensees should ensure that the relevant designations are included in their database. Such database should, in particular, include (i) the lists published in the Gazette or on the website of the CEDB; and (ii) the lists that the Registrar draws to the attention of licensees from time to time. The database should be subject to timely update whenever there are changes, and should be made easily accessible by relevant staff.

B. Comprehensive ongoing screening of a licensee'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 lists of terrorist and sanction designations at the establishment of the relationship; and
   (b) thereafter, as soon as practicable after the new lists of terrorist and sanction designations are published, screening their entire client base against the new lists.

Screening of payment transactions

A. Licensees need to have some means of screening payment instructions to ensure that proposed payments to designated parties are not made.

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

8.16 In order to demonstrate compliance with the requirements for screening of customers and payment instructions, the screening records and any results should be documented, or recorded electronically.

8.17 **In case of any suspicions of TF, PF or sanctions violations, the licensee 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.

Chapter 9

RECORD-KEEPING

The requirements[57]

9.1 Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps investigating authorities to establish the financial profile of a suspect, trace the criminal's or terrorist's 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 offences or terrorist activities.

9.2 **Licensees should maintain all relevant records of customers, transactions, etc. that are necessary and sufficient to meet the record-keeping requirements under the AMLO, this Guideline and other relevant regulatory requirements.** This is to ensure that:

(a) the audit trail for funds moving through a licensee that relate to any customer and, where appropriate, the beneficial owner of the customer, account 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/transaction records and information are available on a timely basis to the CR, other authorities and auditors with appropriate authority; and

(d) licensees are able to comply with any relevant requirements specified in other sections of this Guideline and other requirements imposed by the Registrar, including, among others, records of customer risk assessment (see paragraph 4.6 of this Guideline), records in relation to suspicious transaction reports (see paragraphs 7.17 and 7.18 of this Guideline) and training records (see paragraph 10.5 of this Guideline).

[57] Please refer to sections 20 and 21 of Part 3 of Schedule 2 to the AMLO.

9.3 The record-keeping requirements in respect of each customer and each transaction are illustrated in the following table:

	Record-keeping requirements in respect of	
	each customer	***each transaction***
For how long should records be kept ?	Throughout the continuance of the business relationship with the customer and for a period of **at least 5 years** after the end of the business relationship Similarly, for occasional transaction involving an amount equal to or above HK$120,000 (or an equivalent amount in any other currency), **at least 5 years** beginning on the date on which the occasional transaction is completed.	**At least 5 years** after the completion of a transaction regardless of whether the business relationship ends during the period
What records should be kept ?	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; • beneficial owner of the customer; • the person who purports to act on behalf of the customer; and • other connected parties[58] to the customer. *(Note: The information should include the additional information obtained for the purposes of EDD or ongoing monitoring.)* ➢ the documents, and a record of the data and information, on the purpose and intended nature of the business	The original or a copy of the documents, and a record of the data and information obtained in connection with the transaction, including the following types of information: ➢ the identity of the parties to the transaction; ➢ the nature and date of the transaction; ➢ the type and amount of currency involved; ➢ the origin of the funds (if known); ➢ the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc; ➢ the destination of the funds; ➢ the form of instruction and authority; and ➢ the type and identifying number of any

[58] For the purpose of this paragraph, "connected parties" to a customer include the beneficial owner and any individual having the power to direct the activities of the customer (e.g. any director, shareholder, beneficial owner, signatory, trustee, settlor, protector, or defined beneficiary of a legal arrangement).

	relationship; and ➢ the files relating to the customer's business relationship and business correspondence with the customer and any beneficial owner of the customer.	account involved in the transaction (where applicable).

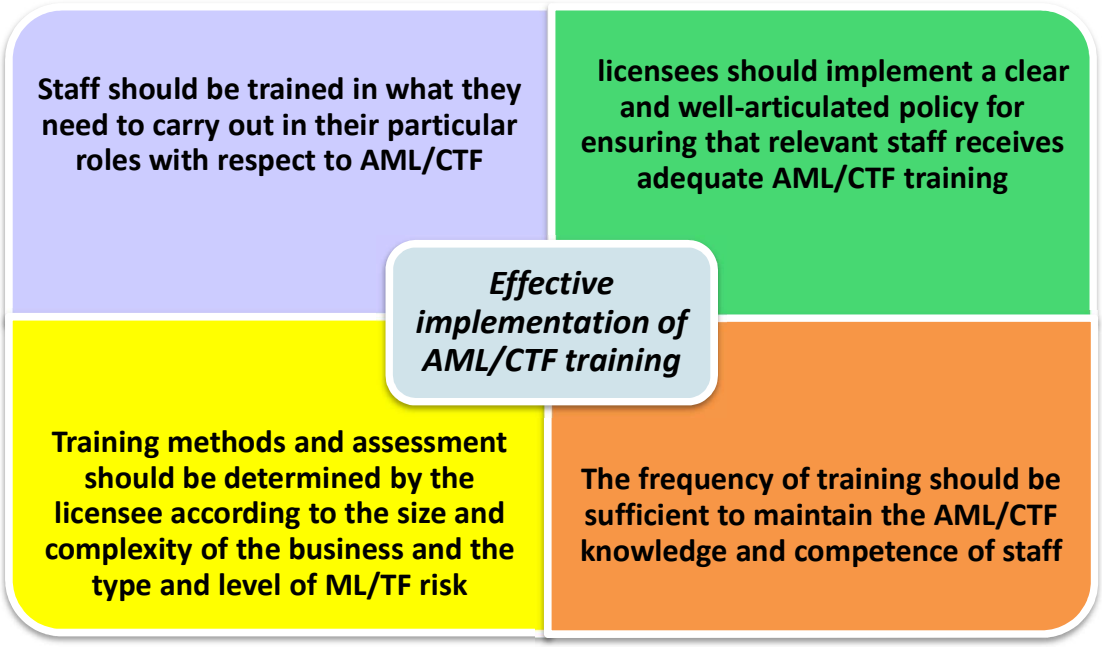
9.4 If the record consists of a document, either the original of the document should be retained or a copy of the document should be kept on microfilm or in the database of a computer. If the record consists of data or information, such record should be kept either on microfilm or in the database of a computer.

9.5 The Registrar may, by notice in writing to a licensee, require it to keep the records relating to a specified transaction or customer for a specified period that is longer than those referred to in paragraph 9.3 above, where the records are relevant to an ongoing criminal or other investigation, or any other purposes as specified in the notice.

Chapter 10

STAFF TRAINING

10.1 **Staff training is an important element of an effective system to prevent and detect ML/TF activities.** The effective implementation of even well-designed AML/CTF systems can be compromised if staff using the systems is not adequately trained.



10.2 Staff should be made aware of:

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

(b) any other statutory and regulatory obligations that concern the licensee and themselves under the AMLO, the DTROPO, the OSCO, the UNATMO, the UNSO and the WMD(CPS)O and the possible consequences of breaches of these obligations;

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

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

10.3 Focused training for appropriate staff or groups of staff will enable licensees to implement their AML/CTF systems effectively. The following diagram and tables illustrate the areas of training which may be provided to appropriate staff or groups of staff:

All new staff (irrespective of seniority)

Areas to be covered in training should include, among others:

(a) an introduction to the background of ML/TF and the importance of AML/CTF to the licensee; and

(b) the need and obligation to identify and report suspicious transactions to the MLRO, and the offence of "tipping-off".

Front-line staff (i.e. staff dealing with customers directly)

Areas to be covered in training should include, among others:

(a) the importance of their roles in the licensee's AML/CTF strategy being the first point of contact with potential money launderers and persons involved in terrorist financing;

(b) the licensee's policies and procedures in relation to CDD and record-keeping requirements relevant to their job responsibilities;

(c) guidance or tips for identifying unusual activities in different circumstances that may give rise to suspicion; and

(d) the relevant policies and procedures for reporting unusual activities, including the line of reporting and the circumstances where extra vigilance might be required.

Back-office staff (i.e. staff not dealing with customers directly but involved in the processing of customer information or customer transactions)

Areas to be covered in training should include, among others:

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

(b) ways to recognise unusual activities including abnormal settlements, payments or delivery instructions.

Managerial staff (including internal audit staff and CO)

Areas to be covered in training should include, among others:

(a) higher level training covering all aspects of Hong Kong's AML/CTF regime;

(b) specific training in the AML/CTF requirements applicable to licensees; and

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

MLRO

Areas to be covered in training should include, among others:

(a) specific training in relation to the MLRO's responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the JFIU; and

(b) training to keep abreast of AML/CTF requirements/developments generally.

10.4 Depending on the learning needs of their staff, licensees are encouraged to consider using a mix of training techniques and tools in delivering training. These techniques and tools may include on-line learning systems, focused classroom training, relevant videos as well as procedural manuals. Licensees may consider including available FATF publications and typologies as part of the training materials. All materials should be up-to-date and in line with current requirements and standards.

10.5 No matter which training approach is adopted, licensees should maintain staff's training records, including the date and type of training received by each staff. Training records of staff should be maintained for a minimum of 3 years and be made available to the CR on demand.

10.6 Licensees should monitor the effectiveness of the training. This may be achieved by:

(a) testing staff's understanding of the licensee's policies and procedures to combat ML/TF, their understanding of relevant statutory and regulatory obligations, and also their ability to identify suspicious transactions; and

(b) monitoring the compliance of staff with the licensee's AML/CTF 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.

Appendix A

Identification and verification of customer who is an individual

1. Information of customer to be collected include:

   (a) Full name;
   (b) Date of birth;
   (c) Nationality;
   (d) Identity document type and number; and
   (e) Residential address.

2. Licensees should obtain the following documents for verification of the information as stated in paragraphs (1)(a) to (d) above and retain a copy of the documents for record keeping:

   (a) Hong Kong residents:
   - Hong Kong identity card for permanent residents;
   - Birth certificate of a minor *(i.e. a person who has not attained the age of 18 years)* not in possession of a valid travel document or Hong Kong identity card (the identity of the minor's parent or guardian representing or accompanying the minor should also be recorded and verified); or
   - Travel document *(a copy of the "biodata" page should be retained).*

   (b) Non-residents:
   - A valid travel document;
   - A relevant national identity card (issued by government) bearing the person's photograph;
   - A valid national driving licence (issued by government) bearing the person's photograph; or
   - Where customers do not have a travel document or a national identity card or driving licence with a photograph, licensees may, exceptionally and applying a risk-based approach, accept other documents as evidence of identity. Wherever possible such documents should have a photograph of the individual.

Travel Documents

Travel document includes a passport or some other document which contains 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:

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

3. 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/TF risk because of the nature of the customer, his business, his location, or because of the product features, etc., the licensee should consider whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity.

Appendix B

Identification and verification of customer which is a corporation

1. Information of customer to be collected include:

   (a) Full name of the corporation;
   (b) Date and place of incorporation;
   (c) Registration or incorporation number; and
   (d) Address of registered office in the place of incorporation and business address (where applicable) *(post office box address is not acceptable)*.

2. The above-mentioned information should be obtained as a standard requirement. On the basis of the ML/TF risk, a licensee should decide whether further verification of identity is required and if so the extent of that further verification. The licensee should also decide whether additional information in respect of the corporation, its operation and the individuals behind it should be obtained.

3. Licensees should obtain the following documents for verification of the information as stated in paragraphs 1(a) to (c) above and retain a copy of the documents for record keeping:

   (a) a copy of the certificate of incorporation and a copy of the business registration certificate (where applicable);
   (b) a copy of the company's articles of association which evidence the powers that regulate and bind the company;
   (c) details of the ownership and control structure of the company, e.g. an ownership chart; and
   (d) a list showing all directors of the corporation.

4. Licensees should:

   (a) confirm that the corporation is still registered and has not been dissolved, wound up, suspended or struck off; and
   (b) independently identify and verify the names of the directors and shareholders recorded in the companies registry in the place of incorporation.

5. For a corporation incorporated in Hong Kong, i.e. a company incorporated under the Companies Ordinance, Cap. 622, the information of the company can be verified against the information in the Companies Register maintained by the CR, by obtaining, for example, a company particulars report and image records of documents showing the shareholders of the company.

6. For a corporation incorporated outside Hong Kong, the information of the corporation can be verified against:

   (a) a similar company search enquiry of the registry in the place of incorporation and obtain a company particulars report;
   (b) a certificate of incumbency or equivalent issued by the company's registered agent in the place of incorporation; or
   (c) 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 stated in paragraph 4 above, which is contained in the said document, is correct and accurate.

7. A licensee should identify and record the identity of all beneficial owners and take reasonable measures to verify the identity of the beneficial owners. For companies with multiple layers in their ownership structures, a licensee 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 licensee, 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 licensee and verify the identity of those individuals.

Definition of "beneficial owner" in relation to a corporation

Section 1 of Part 1 of Schedule 2 to the AMLO defines a beneficial owner in relation to a corporation as:

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

8. Licensees 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 be taken so that the licensee is satisfied on reasonable grounds as to the identity of the beneficial owners.

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

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

Appendix C

Identification and verification of customer which is a partnership or an unincorporated body

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

2. Information of customer to be collected include:

   (a) Full name of the partnership or the unincorporated body;
   (b) The names of all partners of the partnership or all members of the unincorporated body and the beneficial owners or office bearers of the partnership or the unincorporated body; and
   (c) The business address *(post office box address is not acceptable)*.

3. The licensee's obligation is to verify the information as stated in paragraphs 2(a) and (b) above using evidence obtained from a reliable and independent source. Where partnerships or unincorporated bodies are well-known or 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. Most 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, licensees 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 the number is larger, the licensee 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, licensees should obtain the partnership deed (or other evidence in the case of other unincorporated bodies), to satisfy themselves that the partnership or unincorporated body exists, unless an appropriate national register is available for public inspection.

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

Definition of "beneficial owner" in relation to a partnership

Section 1 of Part 1 of Schedule 2 to the AMLO defines a beneficial owner in relation to a partnership as:

(a) an individual who
  (i) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership;
  (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% 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.

Definition of "beneficial owner" in relation to an unincorporated body

Under section 1 of Part 1 of Schedule 2 to the AMLO, the beneficial owner in relation to an unincorporated body is defined as:

(a) 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.

Appendix D

Identification and verification of customer which is a trust

1. A trust does not possess a separate legal personality. It cannot form business relationships or carry out transactions itself. It is the trustee who enters into a business relationship or carries out 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).

2. Information of customer to be collected include:

   (a) the name of the trust, if any;
   (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 the verification of the identity for individuals or corporations (please refer to Appendix A or B of this Guideline);
   (f) identification information of settlor(s) and any protector(s) or enforcers in verification of the identity for individuals or corporations (please refer to Appendix A or B of this Guideline); and
   (g) identification information of known beneficiaries[59] (in line with the verification of the identity for individuals (please refer to Appendix A of this Guideline)). 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.

3. Licensees 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 licensee 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.

[59] With reference to paragraph (a) in the text box under paragraph 3 of this Appendix D.

Definition of "beneficial owner" in relation to a trust

Section 1 of Part 1 of Schedule 2 to the AMLO defines a beneficial owner in relation to a trust as:

(a) a beneficiary or a class of beneficiaries of the trust entitled to a vested interest in 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) the trustee of the trust;
(d) a protector or enforcer of the trust; or
(e) an individual who has ultimate control over the trust.

4. Reasonable measures to verify the existence, legal form and parties to a trust, having regard to the ML/TF risks, may include:

(a) reviewing and retaining a copy of the trust instrument;
(b) by reference to an appropriate register in the relevant country of establishment;
(c) a written confirmation from a trustee acting in a professional capacity[60]; or
(d) a written confirmation from a lawyer who has reviewed the relevant instrument.

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

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

[60] "A trustee acting in a professional capacity" means a trustee who acts 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 a trust (or a particular aspect of the administration or management of a trust).

GLOSSARY OF KEY TERMS AND ABBREVIATIONS	
Terms / abbreviations	**Meaning**
AMLO	Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615
AML/CTF	Anti-money laundering and counter-terrorist financing
AML/CTF systems	The policies, procedures and controls developed and implemented by a licensee for AML/CTF purposes.
CDD	Customer due diligence
CO	Compliance officer
Corporation	A company as defined by section 2(1) of the Companies Ordinance, Cap. 622 or other body corporate incorporated either in Hong Kong or elsewhere[61].
CR	Companies Registry
DTROPO	Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405
EDD	Enhanced customer due diligence
FATF	Financial Action Task Force
Individual	Individual means a natural person, other than a deceased natural person.
JFIU	Joint Financial Intelligence Unit
licensee	Holder of a valid licence granted or renewed by the licensing court for carrying on business as a money lender in Hong Kong.
MLRO	Money laundering reporting officer
ML/TF	Money laundering and/or terrorist financing
OSCO	Organized and Serious Crimes Ordinance, Cap. 455
PEP(s)	Politically exposed person(s)
PF	Financing of proliferation of weapons of mass destruction
RA(s)	The Registrar and the relevant authorities specified in the AMLO, and: (a) in relation to an authorized institution or stored value facility licensee, means the Monetary Authority; (b) in relation to a licensed corporation, means the Securities and Futures Commission; (c) in relation to an authorized insurer, a licensed individual insurance agent, a licensed insurance agency or a licensed

[61] Please refer to section 1 of Part 2 of Schedule 1 to the AMLO.

GLOSSARY OF KEY TERMS AND ABBREVIATIONS	
Terms / abbreviations	**Meaning**
	insurance broker company, means the Insurance Authority; (d) in relation to a licensed money service operator or the Postmaster General of Hong Kong, means the Commissioner of Customs and Excise and a delegate of the Commissioner; (e) in relation to a TCSP licensee, means the Registrar of Companies; and (f) in relation to a licensee, means the Registrar of Money Lenders.
Registrar	Registrar of Money Lenders
Registrar of Companies	The Registrar of Companies or a delegate of the Registrar of Companies.
SDD	Simplified customer due diligence
Senior management	For a corporation, senior management means directors (or board) and senior managers (or equivalent) of the corporation, who are responsible, either individually or collectively, for management and supervision of the corporation's business. This may include a company's Chief Executive Officer, Managing Director, or other senior operating management personnel (as the case may be).
STR(s)	Suspicious transaction report(s), also referred to as reports or disclosures.
TCSP licensee	Holder of a valid licence granted or renewed by the Registrar of Companies for carrying on a trust or company service business in Hong Kong.
Trust	For the purposes 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 any other document) is in place.
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575
UNSO	United Nations Sanctions Ordinance, Cap. 537
WMD(CPS)O	Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526