SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

# Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations)

November 2018

April 2012 first edition
July 2012 second edition
April 2015 third edition
March 2018 fourth edition
November 2018 fifth edition

Published by
**Securities and Futures Commission**
35th Floor
Cheung Kong Center
2 Queen's Road Central
Hong Kong

| | | |
|---|---|---|
| Tel | : | (852) 2231 1222 |
| Fax | : | (852) 2521 7836 |
| E-mail | : | enquiry@sfc.hk |
| SFC website | : | www.sfc.hk |

This Guideline supersedes all previous versions of this Guideline, which was formerly known as the Guideline on Anti-Money Laundering and Counter-Terrorist Financing.

# Content

# Chapter 1 – OVERVIEW

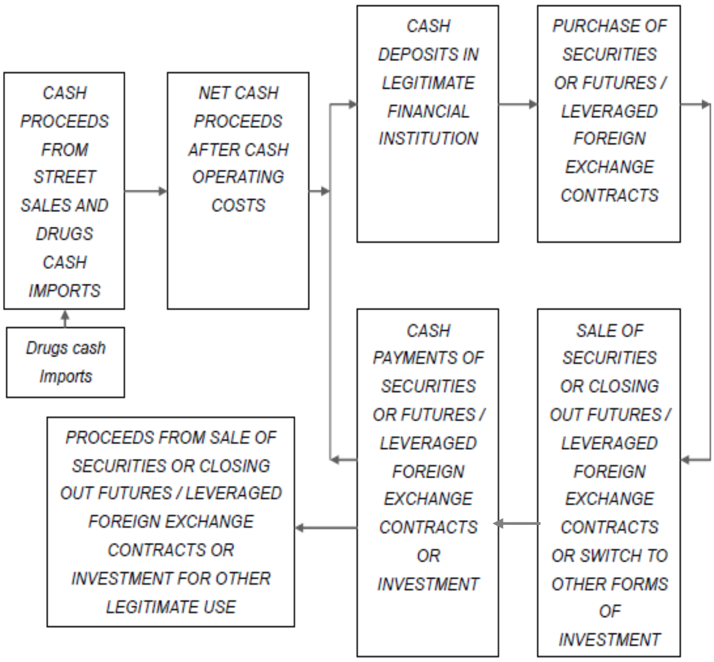
| Introduction | | |
|---|---|---|
| | 1.1 | This Guideline is published under section 7 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (the AMLO), and section 399 of the Securities and Futures Ordinance, Cap. 571 (the SFO). |
| | 1.2 | Terms and abbreviations used in this Guideline shall be interpreted by reference to the definitions set out in the Glossary part of this Guideline. |
| | 1.3 | Where applicable, interpretation of other words or phrases should follow those set out in the AMLO or the SFO. Unless the context otherwise requires, the term financial institutions (FIs) refers to licensed corporations (LCs). |
| | 1.4 | This Guideline is issued by the Securities and Futures Commission (SFC) and sets out the relevant anti-money laundering and counter-financing of terrorism (AML/CFT) statutory and regulatory requirements, and the AML/CFT standards which LCs should meet in order to comply with the statutory requirements under the AMLO and the SFO. Compliance with this Guideline is enforced through the AMLO and the SFO. LCs which fail to comply with this Guideline may be subject to disciplinary or other actions under the AMLO and/or the SFO for non-compliance with the relevant requirements. |
| | 1.5 | This Guideline is intended for use by FIs and their officers and staff. This Guideline also:<br><br>(a) provides a general background on the subjects of money laundering and terrorist financing (ML/TF), including a summary of the main provisions of the applicable AML/CFT legislation in Hong Kong; and<br>(b) provides practical guidance to assist FIs and their |

| | | |
|---|---|---|
| | | senior management in designing and implementing their own policies, procedures and controls in the relevant operational areas, taking into consideration their special circumstances so as to meet the relevant AML/CFT statutory and regulatory requirements. |
| | 1.6 | In addition to the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) issued by the Hong Kong Monetary Authority (HKMA) for use by authorized institutions, registered institutions (RIs) are required to have regard to paragraph 4.1.6 of this Guideline for the definition of “customer” for the securities, futures and leveraged foreign exchange businesses (hereinafter collectively referred to as “securities sector” or “securities businesses”), and paragraphs 7.13 and 7.14 of this Guideline in identifying securities sector specific suspicious transactions. |
| | 1.7 | The relevance and usefulness of this Guideline will be kept under review and it may be necessary to issue amendments from time to time. |
| | 1.8 | For the avoidance of doubt, the use of the word “must” or “should” in relation to an action, consideration or measure referred to in this Guideline indicates that it is a mandatory requirement. Given the significant differences that exist in the organisational and legal structures of different FIs as well as the nature and scope of the business activities conducted by them, there exists no single set of universally applicable implementation measures. The content of this Guideline is not intended to be an exhaustive list of the means of meeting the statutory and regulatory requirements. FIs therefore should use this Guideline as a basis to develop measures appropriate to their structure and business activities. |

| | | |
|---|---|---|
| | 1.9 | This Guideline also provides guidance in relation to the operation of the provisions of Schedule 2 to the AMLO (Schedule 2). |
| s.7, AMLO, s.399(6), SFO | 1.10 | A failure by any person to comply with any provision of this Guideline does not by itself render the person liable to any judicial or other proceedings but, in any proceedings under the AMLO or the SFO before any court, this Guideline is admissible in evidence; and if any provision set out in this Guideline appears to the court to be relevant to any question arising in the proceedings, the provision must be taken into account in determining that question. In considering whether a person has contravened a provision of Schedule 2, the SFC must have regard to any relevant provision in this Guideline. |
| s.193 & 194, SFO | 1.11 | In addition, a failure to comply with any of the requirements of this Guideline by LCs and (where applicable) licensed representatives may reflect adversely on their fitness and properness and may be considered to be misconduct. |
| s.193 & 196, SFO | 1.12 | Similarly, a failure to comply with any of the requirements of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) issued by the HKMA for use by authorized institutions or to have regard to paragraphs 4.1.6, 7.13 and 7.14 of this Guideline by RIs may reflect adversely on their fitness and properness and may be considered to be misconduct. |
| **The nature of money laundering and terrorist financing** | | |
| s.1, Sch. 1, AMLO | 1.13 | The term “money laundering” is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means an act intended to have the effect of making any property:<br><br>(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<br>(b) that in whole or in part, directly or indirectly, represents such proceeds,<br><br>not to appear to be or so represent such proceeds. |
| | 1.14 | There are three common stages in the laundering of money, and they frequently involve numerous transactions. An FI should be alert to any such sign for potential criminal activities. These stages are:<br><br>(a) <u>Placement</u> - the physical disposal of cash proceeds derived from illegal activities;<br>(b) <u>Layering</u> - 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<br>(c) <u>Integration</u> - 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. |
| <u>Potential uses of the securities sector in the money laundering process</u> | | |
| | 1.15 | Since the securities businesses are no longer predominantly cash based, they are less conducive to the initial placement of criminally derived funds than other financial industries, such as banking. Where, however, the payment underlying these transactions is in cash, the risk of these businesses being used as the placement facility cannot be ignored, and thus due diligence must be exercised. |

| | | |
|---|---|---|
| | 1.16 | The securities businesses are more likely to be used at the second stage of money laundering, i.e. the layering process. Unlike laundering via banking networks, these businesses provide a potential avenue which enables the launderer to dramatically alter the form of funds. Such alteration may not only allow conversion from cash in hand to cash on deposit, but also from money in whatever form to an entirely different asset or range of assets such as securities or futures contracts, and, given the liquidity of the markets in which these instruments are traded, with potentially great frequency. |
| | 1.17 | Investments that are cash equivalents, e.g. bearer bonds and similar investments in which ownership can be evidenced without reference to registration of identity, may be particularly attractive to the money launderer. |
| | 1.18 | As mentioned, transactions in the securities sector may prove attractive to money launderers due to the liquidity of the reference markets. The combination of the ability to readily liquidate investment portfolios procured with both licit and illicit proceeds, the ability to conceal the source of the illicit proceeds, the availability of a vast array of possible investment mediums, and the ease with which transfers can be effected between them, offers money launderers attractive ways to effectively integrate criminal proceeds into the general economy. |
| | 1.19 | The chart set out below illustrates the money laundering process relevant to the securities sector in detail. |

| | | |
|---|---|---|
| | | <br><br>Other examples of money laundering methods and characteristics of financial transactions that have been linked with terrorist financing can be found on the websites of the Joint Financial Intelligence Unit (JFIU) (www.jfiu.gov.hk) and the Financial Action Task Force (FATF) (www.fatf-gafi.org). |
| s.1,<br>Sch. 1,<br>AMLO | 1.20 | The term "terrorist financing" is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means:<br><br>(a) the provision or collection, by any means, directly or indirectly, of any property-<br>(i) with the intention that the property be used; or<br>(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<br>(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<br>(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. |
| | 1.21 | Terrorists or terrorist organisations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities. |
| **Legislation concerned with ML, TF, financing of proliferation of weapons of mass destruction (PF) and financial sanctions** | | |
| | 1.22 | The FATF is an inter-governmental body established in 1989. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating of ML, TF, PF, and other related threats to the integrity of the international financial system. The FATF has developed a series of Recommendations that are recognised as the international standards for combating of ML, TF and PF. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. In order to ensure full and effective implementation of its standards at the global level, the FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow-up after the evaluations, including identifying high risk and other monitored jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large. Many major economies have joined the FATF which has developed into a global network for international cooperation that facilitates exchanges between member jurisdictions. As a member of the FATF, Hong Kong is obliged to implement the AML/CFT |

| | | |
|---|---|---|
| | | requirements as promulgated by the FATF, which include the latest FATF Recommendations[1] and it is important that Hong Kong complies with the international AML/CFT standards in order to maintain its status as an international financial centre. |
| | 1.23 | The main pieces of legislation in Hong Kong that are concerned with ML, TF, PF and financial sanctions are the AMLO, the Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP), the Organized and Serious Crimes Ordinance (OSCO), the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO), the United Nations Sanctions Ordinance (UNSO) and the Weapons of Mass Destruction (Control of Provision of Services) Ordinance (WMD(CPS)O). It is very important that FIs and their officers and staff fully understand their respective responsibilities under the different legislation. |
| <u>AMLO</u> | | |
| s.23, Sch. 2 | 1.24 | The AMLO imposes requirements relating to customer due diligence (CDD) and record-keeping on FIs and provides relevant authorities (RAs) with the powers to supervise compliance with these requirements and other requirements under the AMLO. In addition, section 23 of Schedule 2 requires FIs to take all reasonable measures (a) to ensure that proper safeguards exist to prevent a contravention of any requirement under Parts 2 and 3 of Schedule 2; and (b) to mitigate ML/TF risks. |
| s.5, AMLO | 1.25 | The AMLO makes it a criminal offence if an FI (1) knowingly; or (2) with the intent to defraud any RA, contravenes a specified provision of the AMLO. The "specified provisions" are listed in section 5(11) of the AMLO. If the FI knowingly contravenes a specified provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If the FI contravenes a specified |

1 The FATF Recommendations can be found on the FATF's website (www.fatf-gafi.org).

| | | |
|---|---|---|
| | | provision with the intent to defraud any RA, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction. |
| s.5, AMLO | 1.26 | The AMLO also makes it a criminal offence if a person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI (1) knowingly; or (2) with the intent to defraud the FI or any RA, causes or permits the FI to contravene a specified provision in the AMLO. If the person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI knowingly contravenes a specified provision, he is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If that person does so with the intent to defraud the FI or any RA, he is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction. |
| s.21, AMLO | 1.27 | RAs may take disciplinary actions against FIs for any contravention of a specified provision in the AMLO. The disciplinary actions that can be taken include publicly reprimanding the FI; ordering the FI to take any action for the purpose of remedying the contravention; and ordering the FI to pay a pecuniary penalty not exceeding the greater of $10 million or 3 times the amount of profit gained, or costs avoided, by the FI as a result of the contravention. |
| <u>DTROP</u> | | |
| | 1.28 | The DTROP contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction. |
| <u>OSCO</u> | | |
| | 1.29 | The OSCO, among other things:<br><br>(a) gives officers of the Hong Kong Police Force and |

| | | |
|---|---|---|
| | | the Customs and Excise Department powers to investigate organised crime and triad activities;<br>(b) gives the Courts jurisdiction to confiscate the proceeds of organised and serious crimes, to issue restraint orders and charging orders in relation to the property of a defendant of an offence specified in the OSCO;<br>(c) creates an offence of ML in relation to the proceeds of indictable offences; and<br>(d) enables the Courts, under appropriate circumstances, to receive information about an offender and an offence in order to determine whether the imposition of a greater sentence is appropriate where the offence amounts to an organised crime/triad related offence or other serious offences. |
| UNATMO | | |
| | 1.30 | The UNATMO is principally directed towards implementing decisions contained in relevant United Nations Security Council Resolutions (UNSCRs) aimed at preventing the financing of terrorist acts and combating the threats posed by foreign terrorist fighters. Besides the mandatory elements of the relevant UNSCRs, the UNATMO also implements the more pressing elements of the FATF Recommendations specifically related to TF. |
| s.25, DTROP & OSCO | 1.31 | Under the DTROP and the OSCO, a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking or of an indictable offence respectively. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine of $5 million. |
| s.6, 7, 8, 8A, 13 & 14, UNATMO | 1.32 | The UNATMO, among other things, criminalises the provision or collection of property and making any property or financial (or related) services available to terrorists or terrorist associates. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine. The UNATMO also permits |

| | | |
|---|---|---|
| | | terrorist property to be frozen and subsequently forfeited. |
| s.25A, DTROP & OSCO, s.12 & 14, UNATMO | 1.33 | The DTROP, the OSCO and the UNATMO also make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly, represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property respectively. This offence carries a maximum term of imprisonment of 3 months and a fine of $50,000 upon conviction. |
| s.25A, DTROP & OSCO, s.12 & 14, UNATMO | 1.34 | "Tipping-off" is another offence under the DTROP, the OSCO and the UNATMO. A person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following that first-mentioned disclosure. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine. |
| <u>UNSO</u> | | |
| | 1.35 | The UNSO provides for the imposition of sanctions against persons and against places outside the People's Republic of China arising from Chapter 7 of the Charter of the United Nations. Most UNSCRs are implemented in Hong Kong under the UNSO. |
| <u>WMD(CPS)O</u> | | |
| s.4, WMD(CPS)O | 1.36 | The WMD(CPS)O controls the provision of services that will or may assist the development, production, acquisition or stockpiling of weapons capable of causing mass destruction or that will or may assist the means of delivery of such weapons. Section 4 of WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely |

| | | |
|---|---|---|
| | | defined and includes the lending of money or other provision of financial assistance. |

# Chapter 2 – AML/CFT SYSTEMS

| Introduction | | |
|---|---|---|
| s.23(a) & (b), Sch. 2 | 2.1 | FIs must take all reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML/TF and to prevent a contravention of any requirement under Part 2 or 3 of Schedule 2. To ensure compliance with this requirement, FIs should implement appropriate internal AML/CFT policies, procedures and controls (hereafter collectively referred to as "AML/CFT systems"). |
| <u>Risk factors</u> | | |
| | 2.2 | While no system will detect and prevent all ML/TF activities, FIs should establish and implement adequate and appropriate AML/CFT systems (including customer acceptance policies and procedures) taking into account factors including products and services offered, types of customers, geographical locations involved[2]. |
| *Product/service risk* | | |
| | 2.3 | An FI 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, an FI should identify and assess the ML/TF risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms (especially those that may lead to misuse of technological developments or facilitate anonymity in ML/TF schemes); and (b) the use of new or developing technologies for both new and pre-existing products, prior to the launch of the new products, new business practices or the use of new or developing technologies. FIs should take appropriate measures to mitigate and manage the risks identified. |

[2] Guidance on applying a risk-based approach to CDD and ongoing monitoring policies and procedures is provided in Chapters 3 and 5.

| | | |
|---|---|---|
| *Delivery/distribution channel risk* | | |
| | 2.4 | An FI should also consider its delivery/distribution channels and the extent to which these are vulnerable to ML/TF abuse. These may include sales through online, postal or telephone channels where a non-face-to-face account opening approach is used. Business sold through intermediaries may also increase risk as the business relationship between the customer and an FI may become indirect. |
| *Customer risk* | | |
| | 2.5 | When assessing the customer risk, FIs should consider who their customers are, what they do and any other information that may suggest the customer is of higher risk. |
| | 2.6 | An FI should be vigilant where the customer is of such a legal form that enables individuals to divest themselves of ownership of property whilst retaining an element of control over it or the business/industrial sector to which a customer has business connections is more vulnerable to corruption. Examples include:<br><br>(a) companies that can be incorporated without the identity of the ultimate underlying principals being disclosed;<br>(b) certain forms of trusts or foundations where knowledge of the identity of the true underlying principals or controllers cannot be guaranteed;<br>(c) the provision for nominee shareholders; and<br>(d) companies issuing bearer shares. |
| | 2.7 | An FI should also consider risks inherent in the nature of the activity of the customer and the possibility that the transaction may itself be a criminal transaction. For example, the arms trade and the financing of the arms trade is a type of activity that poses multiple ML and other risks, such as: |

| | | |
|---|---|---|
| | | (a) corruption risks arising from procurement contracts;<br>(b) risks in relation to politically exposed persons (PEPs); and<br>(c) terrorism and TF risks as shipments may be diverted. |
| *Country risk* | | |
| | 2.8 | An FI should pay particular attention to countries or geographical locations of operation with which its customers and intermediaries are connected where they are subject to high levels of organised crime, increased vulnerabilities to corruption and inadequate systems to prevent and detect ML/TF. When assessing which countries are more vulnerable to corruption, FIs may make reference to publicly available information or relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations (an example of which is Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption). |
| **AML/CFT systems** | | |
| | 2.9 | Having regard to the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses, an FI should implement adequate and appropriate AML/CFT systems which should include:<br>(a) compliance management arrangements;<br>(b) independent audit function;<br>(c) employee screening procedures; and<br>(d) an ongoing employee training programme (see Chapter 9). |
| *Compliance management arrangements* | | |
| | 2.10 | An FI should have appropriate compliance management arrangements that facilitate the FI to implement AML/CFT systems to comply with relevant legal and regulatory obligations as well as to manage ML/TF risks effectively. Compliance management |

| | | |
|---|---|---|
| | | arrangements should, at a minimum, include oversight by the FI's senior management, and appointment of a Compliance Officer (CO) and a Money Laundering Reporting Officer (MLRO)[3]. |
| *Senior management oversight* | | |
| | 2.11 | The senior management of an FI is responsible for implementing effective AML/CFT systems that can adequately manage the ML/TF risks identified. In particular, the senior management should:<br><br>(a) appoint a CO at the senior management level to have the overall responsibility for the establishment and maintenance of the FI's AML/CFT systems; and<br>(b) appoint a senior staff member as the MLRO to act as the central reference point for suspicious transaction reporting. |
| | 2.12 | In order that the CO and MLRO can discharge their responsibilities effectively, senior management should, as far as practicable, ensure that the CO and MLRO are:<br><br>(a) appropriately qualified with sufficient AML/CFT knowledge;<br>(b) subject to constraint of size of the FI, independent of all operational and business functions;<br>(c) normally based in Hong Kong;<br>(d) of a sufficient level of seniority and authority within the FI;<br>(e) 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 effective measures to protect itself against the |

[3] The role and functions of an MLRO are detailed in paragraphs 2.14, 7.9, 7.16-7.28. Depending on the size of an FI, the functions of the CO and the MLRO may be performed by the same staff member.

| | | |
|---|---|---|
| | | risks of ML/TF;<br>(f) fully conversant with the FI's statutory and regulatory requirements and the ML/TF risks arising from the FI's business;<br>(g) capable of accessing, on a timely basis, all available information (both from internal sources such as CDD records and external sources such as circulars from RAs); and<br>(h) equipped with sufficient resources, including staff and appropriate cover for the absence of the CO and MLRO (i.e. an alternate or deputy CO and MLRO who should, where practicable, have the same status). |
| *Compliance officer and money laundering reporting officer* | | |
| | 2.13 | The principal function of the CO is to act as the focal point within an FI for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the senior management to ensure that ML/TF risks are adequately identified, understood and managed. In particular, the CO should assume responsibility for:<br><br>(a) developing and/or continuously reviewing the FI's AML/CFT systems, including (where applicable) any group-wide AML/CFT systems in the case of a Hong Kong-incorporated FI, to ensure they remain up-to-date, meet current statutory and regulatory requirements, and are effective in managing ML/TF risks arising from the FI's business;<br>(b) overseeing all aspects of the FI's AML/CFT systems which include monitoring effectiveness and enhancing the controls and procedures where necessary;<br>(c) communicating key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies; and<br>(d) ensuring AML/CFT staff training is adequate, appropriate and effective. |

| | | |
|---|---|---|
| | 2.14 | An FI should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the JFIU and law enforcement agencies. The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions of the MLRO should include having oversight of:<br><br>(a) review of internal disclosures and exception reports and, in light of all available relevant information, determination of whether or not it is necessary to make a report to the JFIU;<br>(b) maintenance of records related to such internal reviews; and<br>(c) provision of guidance on how to avoid tipping-off. |
| *Independent audit function* | | |
| | 2.15 | Where practicable, an FI should establish an independent audit function which should have a direct line of communication to the senior management of the FI. Subject to appropriate segregation of duties, the function should have sufficient expertise and resources to enable it to carry out an independent review of the FI's AML/CFT systems. |
| | 2.16 | The audit function should regularly review the AML/CFT systems to ensure effectiveness. This would include evaluating, among others:<br><br>(a) the adequacy of the FI's AML/CFT systems, ML/TF risk assessment framework and application of risk-based approach;<br>(b) the effectiveness of the system for recognising and reporting suspicious transactions;<br>(c) whether instances of non-compliance are reported to senior management on a timely basis; and<br>(d) the level of awareness of staff having AML/CFT responsibilities.<br><br>The frequency and extent of the review should be |

| | | |
|---|---|---|
| | | commensurate with the nature, size and complexity of the FI's businesses and the ML/TF risks arising from those businesses. Where appropriate, the FI should seek a review from external parties. |
| *Employee screening* | | |
| | 2.17 | FIs should have adequate and appropriate screening procedures in order to ensure high standards when hiring employees. |
| **Group-wide AML/CFT systems** | | |
| s.22(1), Sch. 2 | 2.18 | Subject to paragraphs 2.19 and 2.20, a Hong Kong-incorporated FI with overseas branches or subsidiary undertakings that carry on the same business as an FI as defined in the AMLO should implement group-wide AML/CFT systems[4] to apply the requirements set out in this Guideline to all of its overseas branches and subsidiary undertakings in its financial group, wherever the requirements in this Guideline are relevant and applicable to the overseas branches and subsidiary undertakings concerned.<br><br>In particular, a Hong Kong-incorporated FI should, through its group-wide AML/CFT systems, ensure that all of its overseas branches and subsidiary undertakings that carry on the same business as an FI as defined in the AMLO, have procedures in place to ensure compliance with the CDD and record-keeping requirements similar to those imposed under Parts 2 and 3 of Schedule 2, to the extent permitted by the laws and regulations of that place. |
| | 2.19 | If the AML/CFT requirements in the jurisdiction where the overseas branch or subsidiary undertaking of a Hong Kong-incorporated FI is located (host jurisdiction) differ from those relevant requirements referred to in paragraph 2.18, the FI should require that branch or subsidiary undertaking to apply the |

[4] For the avoidance of doubt, these include, but not limited to, the requirements set out in paragraph 2.9.

| | | |
|---|---|---|
| | | higher of the two sets of requirements, to the extent that the host jurisdiction's laws and regulations permit. |
| s.22(2), Sch. 2 | 2.20 | If the host jurisdiction's laws and regulations do not permit the branch or subsidiary undertaking of a Hong Kong-incorporated FI to apply the higher AML/CFT requirements, particularly the CDD and record-keeping requirements imposed under Parts 2 and 3 of Schedule 2, the FI should:<br><br>(a) inform the RA of such failure; and<br>(b) take additional measures to effectively mitigate ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the requirements. |
| | 2.21 | To the extent permitted by the laws and regulations of the jurisdictions involved and subject to adequate safeguards on the protection of confidentiality and use of information being shared, including safeguards to prevent tipping-off, a Hong Kong-incorporated FI should also implement, through its group-wide AML/CFT systems for:<br><br>(a) sharing information required for the purposes of CDD and ML/TF risk management; and<br>(b) provision to the FI's group-level compliance, audit and/or AML/CFT functions, of customer, account, and transaction information from its overseas branches and subsidiary undertakings that carry on the same business as an FI as defined in the AMLO, when necessary for AML/CFT purposes[5]. |

[5] This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include a suspicious transaction report, its underlying information, or the fact that a suspicious transaction report has been submitted. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management.

# Chapter 3 – RISK-BASED APPROACH

| **Introduction** | | |
|---|---|---|
| | 3.1 | Applying an AML/CFT risk-based approach (RBA) is recognised as an effective way to combat ML/TF. The use of an RBA has the advantage of allowing resources to be allocated in the most efficient way directed in accordance with priorities so that the greatest risks receive the highest attention.<br><br>In the context of CDD and ongoing monitoring, the general principle for applying an RBA is that where customers are assessed to be of higher ML/TF risks, an FI should take enhanced measures to manage and mitigate those risks, and that correspondingly where the risks are lower, simplified measures may be applied.<br><br>In other words, the degree, frequency or extent of CDD measures and ongoing monitoring conducted vary in accordance with the assessed ML/TF risks associated with individual customers or business relationships[6]. |
| **General requirement** | | |
| | 3.2 | FIs should determine the extent of CDD measures and ongoing monitoring, using an RBA depending upon the background of the customer and the product, transaction or service used by that customer, so that preventive or mitigating measures are commensurate to the risks identified.<br><br>The measures must however comply with the legal requirements of the AMLO. FIs should have regard, in particular, to section 4 of Schedule 2 which permits FIs not to identify and take reasonable measures to verify the identity of the beneficial owners of specific types of customers, or in relation to specific types of |

6 Illustrative examples of possible simplified and enhanced measures are set out in paragraphs 1 and 2 of Appendix A respectively.

| | | |
|---|---|---|
| | | products related to the transactions of the customers; and sections 8 to 15 of Schedule 2 which require FIs to comply with some special requirements in relation to specific types of customers, products, transactions or other high risk situations.<br><br>The RBA will enable FIs to subject customers to proportionate controls and oversight by determining:<br><br>(a) the extent of the due diligence to be performed on the direct customer; the extent of the measures to be undertaken to verify the identity of any beneficial owner and any person purporting to act on behalf of the customer;<br>(b) the level of ongoing monitoring to be applied to the business relationship; and<br>(c) measures to mitigate any risks identified.<br><br>For example, the RBA may require extensive CDD for high risk customers, such as an individual (or corporate entity) whose source of wealth and funds is unclear or who requires the setting up of complex structures.<br><br>FIs should be able to demonstrate to the RAs that the extent of CDD and ongoing monitoring is appropriate in view of the customer's ML/TF risks. |
| | 3.3 | There are no universally accepted methodologies that prescribe the nature and extent of an RBA. However, an effective RBA does involve identifying and categorising ML/TF risks at the customer level and establishing reasonable measures based on risks identified. An effective RBA will allow FIs to exercise reasonable business judgment with respect to their customers.<br><br>An RBA should not be designed to prohibit FIs from engaging in transactions with customers or establishing business relationships with potential customers, but rather it should assist FIs to effectively manage potential ML/TF risks. |

| Customer acceptance/risk assessment | | |
|---|---|---|
| | 3.4 | FIs may assess the ML/TF risks of individual customers by assigning a ML/TF risk rating to their customers. |
| | 3.5 | While there is no agreed upon set of risk factors and no one single methodology to apply these risk factors in determining the ML/TF risk rating of customers, relevant factors to be considered may include the following:<br><br><u>1. Country risk</u><br><br>Customers with residence in or connection with high risk jurisdictions[7] for example:<br><br>(a) those that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies;<br>(b) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations (UN);<br>(c) countries which are vulnerable to corruption; and<br>(d) those countries that are believed to have strong links to terrorist activities.<br><br>In assessing country risk associated with a customer, consideration may be given to local legislation (UNSO, UNATMO), data available from the UN, the International Monetary Fund, the World Bank, the FATF, etc. and the FI's own experience or the experience of other group entities (where the FI is part of a multi-national group) which may have indicated weaknesses in other jurisdictions.<br><br><u>2. Customer risk</u><br><br>The following are examples of customers who might be considered to carry lower ML/TF risks: |

[7] Guidance on jurisdictions posing higher risk is provided in paragraphs 4.13.

| | | |
|---|---|---|
| | | (a) customers who are employment-based or with a regular source of income from a known legitimate source which supports the activity being undertaken; and<br>(b) the reputation of the customer, e.g. a well-known, reputable private company, with a long history that is well documented by independent sources, including information regarding its ownership and control.<br><br>However, some customers, by their nature or behaviour might present a higher risk of ML/TF. Factors might include:<br><br>(a) the public profile of the customer indicating involvement with, or connection to, PEPs;<br>(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;<br>(c) a request to use numbered accounts or undue levels of secrecy with a transaction;<br>(d) involvement in cash-intensive businesses;<br>(e) nature, scope and location of business activities generating the funds/assets, having regard to sensitive or high risk activities; and<br>(f) where the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified.<br><br><u>3. Product/service risk</u><br><br>Factors presenting higher risk might include:<br><br>(a) services that inherently have provided more anonymity; and<br>(b) ability to pool underlying customers/funds.<br><br><u>4. Delivery/distribution channel risk</u><br><br>The distribution channel for products may alter the risk profile of a customer. This may include sales |

| | | |
|---|---|---|
| | | through online, postal or telephone channels where a non-face-to-face account opening approach is used. Business sold through intermediaries may also increase risk as the business relationship between the customer and an FI may become indirect. |
| **Ongoing review** | | |
| | 3.6 | The identification of higher risk customers, products and services, including delivery channels, and geographical locations are not static assessments. They will change over time, depending on how circumstances develop, and how threats evolve. In addition, while a risk assessment should always be performed at the inception of a customer relationship, for some customers, a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making monitoring of customer transactions and ongoing reviews a fundamental component of a reasonably designed RBA. An FI may therefore have to adjust its risk assessment of a particular customer from time to time or based upon information received from a competent authority, and review the extent of the CDD and ongoing monitoring to be applied to the customer. |
| | 3.7 | FIs should keep its policies and procedures under regular review and assess that its risk mitigation procedures and controls are working effectively. |
| **Documenting risk assessment** | | |
| | 3.8 | An FI should keep records and relevant documents of the risk assessment covered in this Chapter so that it can demonstrate to the RAs, among others:<br><br>(a) how it assesses the customer's ML/TF risks; and<br>(b) the extent of CDD measures and ongoing monitoring is appropriate based on that customer's ML/TF risks. |

# Chapter 4 - CUSTOMER DUE DILIGENCE

| | | |
|---|---|---|
| **4.1 What CDD measures are and when they must be carried out** | | |
| General | | |
| s.19(3), Sch. 2 | 4.1.1 | The AMLO defines what CDD measures are (see paragraph 4.1.4) and also prescribes the circumstances in which an FI must carry out CDD (see paragraph 4.1.9). This Chapter provides guidance in this regard. Wherever possible, this Guideline gives FIs a degree of discretion in how they comply with the AMLO and put in place procedures for this purpose. In addition, an FI should, in respect of each kind of customer, business relationship, product and transaction, establish and maintain effective AML/CFT systems for complying with the CDD requirements set out in this Chapter. |
| | 4.1.2 | FIs should also have regard to section 4 of Schedule 2 which permits FIs not to identify and take reasonable measures to verify the identity of the beneficial owners of specific types of customers, or in relation to specific types of products related to the transactions of the customers (see paragraphs 4.8); and sections 8 to 15 of Schedule 2 which require FIs to comply with some special requirements in relation to specific types of customers, products, transactions or other high risk situations (see paragraphs 4.9-4.14). |
| What CDD measures are | | |
| | 4.1.3 | CDD information is a vital tool for recognising whether there are grounds for knowledge or suspicion of ML/TF. |
| s.2(1), Sch. 2 | 4.1.4 | The following are CDD measures applicable to an FI:<br><br>(a) identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source (see paragraphs 4.2);<br>(b) where there is a beneficial owner in relation to |

| | | |
|---|---|---|
| | | the customer, identify and take reasonable measures to verify the beneficial owner's identity so that the FI is satisfied that it knows who the beneficial owner is, including, in the case of a legal person or trust, measures to enable the FI to understand the ownership and control structure of the legal person or trust (see paragraphs 4.3);<br>(c) obtain information on the purpose and intended nature of the business relationship (if any) established with the FI unless the purpose and intended nature are obvious (see paragraphs 4.6); and<br>(d) if a person purports to act on behalf of the customer:<br>(i) identify the person and take reasonable measures to verify the person's identity using documents, data or information provided by a reliable and independent source; and<br>(ii) verify the person's authority to act on behalf of the customer (see paragraphs 4.4). |
| | 4.1.5 | The term "customer" is defined in the AMLO to include a client. The meaning of "customer" and "client" should be inferred from its everyday meaning and in the context of the industry practice. |
| | 4.1.6 | Unless the context otherwise requires, for the securities sector, the term "customer" refers to a person who is a client of an LC and the term "client" is as defined in section 1 of Part 1 of Schedule 1 to the SFO and the phrase "potential customer" in the term "business relationship" is to be construed accordingly as meaning "potential client". |
| | 4.1.7 | In determining what constitutes reasonable measures to verify the identity of a beneficial owner and reasonable measures to understand the ownership and control structure of a legal person or trust, the FI should consider and give due regard to the ML/TF risks posed by a particular customer and a particular business relationship. Due consideration |

| | | |
|---|---|---|
| | | should also be given to the measures set out in Chapter 3. |
| | 4.1.8 | FIs should adopt a balanced and common sense approach with regard to customers connected with jurisdictions posing higher risk (see paragraphs 4.13). While extra care may well be justified in such cases, unless an RA has, through a "notice in writing", imposed a general or specific requirement (see paragraph 4.14.2), it is not a requirement that FIs should refuse to do any business with such customers or automatically classify them as high risk and subject them to the special requirements set out in section 15 of Schedule 2. Rather, FIs should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/TF. |
| <u>When CDD measures must be carried out</u> | | |
| s.3(1), Sch. 2 | 4.1.9 | An FI must carry out CDD measures in relation to a customer:<br><br>(a) at the outset of a business relationship;<br>(b) before performing any occasional transaction[8]:<br>(i) equal to or exceeding an aggregate value of \$120,000, whether carried out in a single operation or several operations that appear to the FI to be linked; or<br>(ii) a wire transfer equal to or exceeding an aggregate value of \$8,000, whether carried out in a single operation or several operations that appear to the FI to be linked;<br>(c) when the FI suspects that the customer or the customer's account is involved in ML/TF[9]; or<br>(d) when the FI doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the |

8 Occasional transactions may include for example, wire transfers, currency exchanges, purchase of cashier orders or gift cheques.

9 This criterion applies irrespective of the $120,000 or $8,000 threshold applicable to occasional transactions set out in paragraphs 4.1.9(b)(i) and 4.1.9(b)(ii) respectively.

| | | |
|---|---|---|
| | | purpose of verifying the customer's identity. |
| s.1, Sch. 2 | 4.1.10 | "Business relationship" between a person and an FI is defined in the AMLO as a business, professional or commercial relationship:<br><br>(a) that has an element of duration; or<br>(b) that the FI, at the time the person first contacts it in the person's capacity as a potential customer of the FI, expects to have an element of duration. |
| s.1, Sch. 2 | 4.1.11 | The term "occasional transaction" is defined in the AMLO as a transaction between an FI and a customer who does not have a business relationship with the FI[10]. |
| | 4.1.12 | FIs should be vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD thresholds of $8,000 for wire transfers and $120,000 for other types of transactions. Where FIs become aware that these thresholds are met or exceeded, CDD measures must be carried out. |
| | 4.1.13 | 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, where a customer regularly transfers funds to one or more destinations. In determining whether the transactions are in fact linked, FIs should consider these factors against the timeframe within which the transactions are conducted. |
| **4.2 Identification and verification of the customer's identity** | | |
| s.2(1)(a), Sch. 2 | 4.2.1 | The FI must identify the customer and verify the customer's identity by reference to documents, data or information provided by a reliable and independent source: |

[10] It should be noted that "occasional transactions" do not apply to the securities sector.

| | | |
|---|---|---|
| | | (a) a governmental body;<br>(b) the RA or any other RA;<br>(c) an authority in a place outside Hong Kong that performs functions similar to those of the RA or any other RA; or<br>(d) any other reliable and independent source that is recognised by the RA. |
| <u>Customer that is a natural person</u>[11] | | |
| s.2(1)(a), Sch. 2 | 4.2.2 | For a customer that is a natural person, FIs should identify the customer by obtaining at least the following identification information:<br><br>(a) full name;<br>(b) date of birth;<br>(c) nationality; and<br>(d) unique identification number (e.g. identity card number or passport number) and document type. |
| s.2(1)(a), Sch. 2 | 4.2.3 | In verifying the identity of a customer that is a natural person, an FI should verify the name, date of birth, unique identification number and document type of the customer. The FI should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include:<br><br>(a) Hong Kong identity card or other national identity card bearing the individual's photograph;<br>(b) valid travel document (e.g. unexpired passport); or<br>(c) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).<br><br>The FI should retain a copy of the individual's identification document or record. |

[11] For the purpose of this Guideline, the terms "natural person" and "individual" are used interchangeably.

| | | |
|---|---|---|
| | 4.2.4 | An FI should obtain the residential address information of a customer that is a natural person[12]. |
| <u>Customer that is a legal person</u>[13] | | |
| s.2(1)(a), Sch. 2 | 4.2.5 | For a customer that is a legal person, an FI should identify the customer by obtaining at least the following identification information:<br><br>(a) full name;<br>(b) date of incorporation, establishment or registration;<br>(c) place of incorporation, establishment or registration (including address of registered office);<br>(d) unique identification number (e.g. incorporation number or business registration number) and document type; and<br>(e) principal place of business (if different from the address of registered office). |
| s.2(1)(a), Sch. 2 | 4.2.6 | In verifying the identity of a customer that is a legal person, an FI should normally verify its name, legal form, current existence (at the time of verification), and powers that regulate and bind the legal person. The FI should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include[14]:<br><br>(a) certificate of incorporation;<br>(b) record of companies registry; |

12 For the avoidance of doubt, an FI may, under certain circumstances, further require proof of residential address from a customer for other purposes (e.g. group requirements, paragraph 5.4 of the current Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (a.k.a. Client Identity Rule), and other local or overseas legal and regulatory requirements). In such circumstances, the FI should communicate clearly to the customers the reasons why it requires proof of residential address.

13 Legal person refers to any entities other than natural person that can establish a permanent customer relationship with an FI or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, associations or other relevantly similar entities.

14 In some instances, an FI may need to obtain more than one document to meet this requirement. For example, a certificate of incorporation can only verify the name and legal form of the legal person in most circumstances but cannot act as a proof of current existence.

| | | |
|---|---|---|
| | | (c) certificate of incumbency;<br>(d) certificate of good standing;<br>(e) record of registration;<br>(f) partnership agreement or deed;<br>(g) constitutive document; or<br>(h) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).<br><br>Illustrative examples of possible measures to verify the name, legal form and current existence of a legal person are set out in paragraph 3 of Appendix A. |
| | 4.2.7 | For a customer that is a partnership or an unincorporated body, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to provide reliable and independent evidence of the identity of the customer as required in paragraph 4.2.6 provided that:<br><br>(a) the customer is a well-known, reputable organisation;<br>(b) the customer has a long history in its industry; and<br>(c) there is substantial public information about the customer, its partners and controllers. |
| | 4.2.8 | In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, an FI should satisfy itself as to the legitimate purpose of the organisation, e.g. by requesting sight of the constitutive document. |
| Customer that is a trust[15] or other similar legal arrangement[16] | | |
| s.2(1)(a), Sch. 2 | 4.2.9 | In respect of trusts, an FI should identify and verify the trust as a customer in accordance with the |

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

[16] Examples of legal arrangement include fiducie, treuhand and fideicomiso.

| | | |
|---|---|---|
| | | requirements set out in paragraphs 4.2.10 and 4.2.11. The FI should also regard the trustee as its customer if the trustee enters into a business relationship or carries out occasional transactions on behalf of the trust, which is generally the case if the trust does not possess a separate legal personality. In such a case, an FI should identify and verify the identity of the trustee in line with the identification and verification requirements for a customer that is a natural person or, where applicable, a legal person. |
| s.2(1)(a), Sch. 2 | 4.2.10 | For a customer that is a trust or other similar legal arrangement, FIs should identify the customer by obtaining at least the following identification information:<br><br>(a) the name of the trust or legal arrangement;<br>(b) date of establishment or settlement;<br>(c) the jurisdiction whose laws govern the trust or legal arrangement;<br>(d) unique identification number (if any) granted by any applicable official bodies and document type (e.g. tax identification number or registered charity or non-profit organisation number); and<br>(e) address of registered office (if applicable). |
| s.2(1)(a), Sch. 2 | 4.2.11 | In verifying the identity of a customer that is a trust or other similar legal arrangement, an FI should normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the trust or other similar legal arrangement. The FI should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include:<br><br>(a) trust deed or similar instrument[17]; |

[17] Under exceptional circumstance, the FI may choose to retain a redacted copy.

| | | |
|---|---|---|
| | | (b) record of an appropriate register[18] in the relevant country of establishment;<br>(c) written confirmation from a trustee acting in a professional capacity[19];<br>(d) written confirmation from a lawyer who has reviewed the relevant instrument; or<br>(e) written confirmation from a trust company which is within the same financial group as the FI, if the trust concerned is managed by that trust company. |
| <u>Connected parties</u> | | |
| | 4.2.12 | Where a customer is a legal person, a trust or other similar legal arrangement, an FI should identify the connected parties[20] of the customer by obtaining their names. |
| | 4.2.13 | A connected party of a customer that is a legal person, a trust or other similar legal arrangement:<br><br>(a) in relation to a corporation, means a director of the customer;<br>(b) in relation to a partnership, means a partner of the customer;<br>(c) in relation to a trust or other similar legal arrangement, means a trustee (or equivalent) of the customer; and<br>(d) in other cases not falling within subsection (a), (b) or (c), means a natural person holding a senior management position or having executive authority in the customer. |

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

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

[20] For the avoidance of doubt, if a connected party also satisfies the definition of a customer, a beneficial owner of the customer or a person purporting to act on behalf of the customer, the FI has to identify and verify the identity of that person with reference to relevant requirements set out in this Guideline.

| | | |
|---|---|---|
| <u>Other considerations</u> | | |
| | 4.2.14 | An FI may adopt an RBA in determining the documents, data or information to be obtained for verifying the identity of a customer that is a legal person, trust or other similar legal arrangement. Illustrative examples of relevant simplified and enhanced measures are set out in paragraph 4 of Appendix A. |
| **4.3 Identification and verification of a beneficial owner** | | |
| s.1 & s.2(1)(b), Sch. 2 | 4.3.1 | A beneficial owner is normally a natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. An FI must identify any beneficial owner in relation to a customer, and take reasonable measures to verify the beneficial owner's identity so that the FI is satisfied that it knows who the beneficial owner is. However, the verification requirements under the AMLO are different for a customer and a beneficial owner. |
| | 4.3.2 | Where a natural person is identified as a beneficial owner, the FI should endeavour to obtain the same identification information as at paragraph 4.2.2 as far as possible. |
| <u>Beneficial owner in relation to a natural person</u> | | |
| | 4.3.3 | In respect of a customer that is a natural person, there is no requirement on FIs to make proactive searches for beneficial owners of the customer in such a case, but they should make appropriate enquiries where there are indications that the customer is not acting on his own behalf. |
| <u>Beneficial owner in relation to a legal person</u> | | |
| s.1, Sch. 2 | 4.3.4 | The AMLO defines beneficial owner in relation to a corporation as:<br><br>(i) an individual who<br>(a) owns or controls, directly or indirectly, including through a trust or bearer share |

| | | |
|---|---|---|
| | | holding, more than 25% of the issued share capital of the corporation;<br>(b) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or<br>(c) exercises ultimate control over the management of the corporation; or<br>(ii) if the corporation is acting on behalf of another person, means the other person. |
| s.1, Sch. 2 | 4.3.5 | The AMLO defines beneficial owner, in relation to a partnership as:<br><br>(i) an individual who<br>(a) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership;<br>(b) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or<br>(c) exercises ultimate control over the management of the partnership; or<br>(ii) if the partnership is acting on behalf of another person, means the other person. |
| s.1, Sch. 2 | 4.3.6 | In relation to an unincorporated body other than a partnership, beneficial owner:<br><br>(i) means an individual who ultimately owns or controls the unincorporated body; or<br>(ii) if the unincorporated body is acting on behalf of another person, means the other person. |
| s.2(1)(b), Sch. 2 | 4.3.7 | For a customer that is a legal person, an FI should identify any natural person who ultimately has a controlling ownership interest (i.e. more than 25%) in the legal person and any natural person exercising control of the legal person or its management, and take reasonable measures to verify their identities. If there is no such natural person (i.e. no natural person falls within the definition of beneficial owners |

| | | |
|---|---|---|
| | | set out in paragraphs 4.3.4 to 4.3.6), the FI should identify the relevant natural persons who hold the position of senior managing official[21] in the legal person, and take reasonable measures to verify their identities. |
| | 4.3.8 | While an FI usually can identify who the beneficial owner of a customer is in the course of understanding the ownership and control structure of the customer, the FI may obtain an undertaking or declaration[22] from the customer on the identity of, and the information relating to, its beneficial owner. Nevertheless, in addition to the undertaking or declaration obtained, the FI should take reasonable measures to verify the identity of the beneficial owner (e.g. corroborating the undertaking or declaration with publicly available information). |
| | 4.3.9 | If the ownership structure of a customer involves different types of legal persons or legal arrangements, in determining who the beneficial owner is, an FI should pay attention to who has ultimate ownership or control over the customer, or who constitutes the controlling mind and management of the customer. |
| <u>Beneficial owner in relation to a trust or other similar legal arrangement</u> | | |
| s.1, Sch. 2 | 4.3.10 | The AMLO defines the beneficial owner, in relation to a trust as:<br><br>(i) an individual who is entitled to a vested interest in more than 25% of the capital of the trust property, whether the interest is in possession or |

[21] Examples of positions of senior managing official include chief executive officer, chief financial officer, managing or executive director, president, or natural person(s) who has significant authority over a legal person's financial relationships (including with FIs that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person.

[22] In some jurisdictions, corporations are required to maintain registers of their beneficial owners (e.g. the significant controllers registers maintained in accordance with the Companies Ordinance, Cap. 622). An FI may refer to those registers to assist in identifying the beneficial owners of its customers. Where a register of the beneficial owners is not made publicly available, the FI may obtain the record directly from its customers.

| | | |
|---|---|---|
| | | in remainder or reversion and whether it is defeasible or not;<br>(ii) the settlor of the trust;<br>(iii) a protector or enforcer of the trust; or<br>(iv) an individual who has ultimate control over the trust. |
| s.2(1)(b), Sch. 2 | 4.3.11 | For trusts, an FI should identify the settlor, the protector (if any), the enforcer (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate control over the trust (including through a chain of control or ownership), and take reasonable measures to verify their identities. For other similar legal arrangements, an FI should identify any natural person in equivalent or similar positions to beneficial owner of a trust as stated above and take reasonable measures to verify the identity of such person. If a trust or other similar legal arrangement is involved in a business relationship and an FI does not regard the trustee (or equivalent in the case of other similar legal arrangement) as its customer pursuant to paragraph 4.2.9 (e.g. when a trust appears as part of an intermediate layer referred to in paragraph 4.3.13), the FI should also identify the trustee (or equivalent) and take reasonable measures to verify the identity of the trustee (or equivalent) so that the FI is satisfied that it knows who that person is. |
| | 4.3.12 | For a beneficiary of a trust designated by characteristics or by class, an FI should obtain sufficient information[23] concerning the beneficiary to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights. |

[23] For example, an FI may ascertain and name the scope of the class of beneficiaries (e.g. children of a named individual).

| | | |
|---|---|---|
| Ownership and control structure | | |
| s.2(1)(b), Sch. 2 | 4.3.13 | Where a customer is not a natural person, an FI should understand its ownership and control structure, including identification of any intermediate layers (e.g. by reviewing an ownership chart of the customer)[24]. The objective is to follow the chain of ownerships to the beneficial owners of the customer.<br><br>Similar to a corporation, a trust or other similar legal arrangement can also be part of an intermediate layer in an ownership structure, and should be dealt with in similar manner to a corporate being part of an intermediate layer. |
| | 4.3.14 | Where a customer has a complex ownership or control structure, an FI should obtain sufficient information for the FI to satisfy itself that there is a legitimate reason behind the particular structure employed. |
| **4.4 Identification and verification of a person purporting to act on behalf of the customer** | | |
| | 4.4.1 | A person may be appointed to act on behalf of a customer to establish business relationships, or may be authorised to give instructions to an FI to conduct various activities through the account or the business relationship established. Whether the person is considered to be a person purporting to act on behalf of the customer (PPTA) should be determined based on the nature of that person's roles and the activities which the person is authorised to conduct[25], as well |

[24] Examples of information which may be collected to identify the intermediate layers of the corporate structure of a legal person with multiple layers in its ownership structure are set out in paragraph 5 of Appendix A.

[25] For example, those that carry out transactions on behalf of the customer may be considered as PPTAs. However, dealers and traders in an investment bank or asset manager who are authorised to act on behalf of the investment bank or asset manager would not ordinarily be considered PPTAs. For the avoidance of doubt, the person who is authorised to act on behalf of a customer to establish a business relationship with an FI should always be considered as a PPTA.

| | | |
|---|---|---|
| | | as the ML/TF risks associated with these roles and activities[26].<br><br>FIs should implement clear policies for determining who is considered to be a PPTA. |
| s.2(1)(d), Sch. 2 | 4.4.2 | If a person purports to act on behalf of the customer, FIs must:<br><br>(i) identify the person and take reasonable measures to verify the person's identity by reference to documents, data or information provided by a reliable and independent source:<br>(A) a governmental body;<br>(B) the RA or any other RA;<br>(C) an authority in a place outside Hong Kong that performs functions similar to those of the RA or any other RA; or<br>(D) any other reliable and independent source that is recognised by the RA; and<br>(ii) verify the person's authority to act on behalf of the customer. |
| | 4.4.3 | FI should identify a PPTA in line with the identification requirements for a customer that is a natural person or, where applicable, a legal person. In taking reasonable measures to verify the identity of the PPTA, FI should, as far as possible, follow the verification requirements for a customer that is a natural person or, where applicable, a legal person. |
| s.2(1)(d)(ii), Sch. 2 | 4.4.4 | FIs should verify the authority of each PPTA by appropriate documentary evidence (e.g. board resolution or similar written authorisation). |
| **4.5 Reliability of documents, data or information** | | |
| | 4.5.1 | In verifying the identity of a customer, an FI needs not establish accuracy of every piece of identification |

[26] Consideration should also be given to the ML/TF risk of products and services relevant to the transactions that the person is authorised to conduct, with reference to the guidance set out in paragraph 3.5.

| | | |
|---|---|---|
| | | information collected in paragraphs 4.2.2, 4.2.5 and 4.2.10. |
| | 4.5.2 | An FI should ensure that documents, data or information obtained for the purpose of verifying the identity of a customer as required in paragraphs 4.2.3, 4.2.6 and 4.2.11 is current at the time they are provided to or obtained by the FI. |
| | 4.5.3 | When using documents for verification, an FI should be aware that some types of documents are more easily forged than others, or can be reported as lost or stolen [27]. Therefore, the FI should consider applying anti-fraud procedures that are commensurate with the risk profile of the person being verified. |
| | 4.5.4 | If a natural person customer or a person representing a legal person, a trust or other similar legal arrangement to establish a business relationship with an FI is physically present during the CDD process, the FI should generally have sight of original identification document by its staff and retain a copy of the document. However, there are a number of occasions where an original identification document cannot be produced by the customers (e.g. the original document is in electronic form). In such an occasion, the FI should take appropriate measures to ensure the reliability of identification documents obtained. |
| | 4.5.5 | Where the documents, data or information being used for the purposes of identification are in a foreign language, appropriate steps should be taken by the FI to be reasonably satisfied that the documents in fact provide evidence of the customer's identity[28]. |

[27] Please refer to paragraph 6 of Appendix A for illustrative examples of procedures to establish whether the identification documents offered by customers are genuine, or have been reported as lost or stolen.

[28] For example, ensuring that staff assessing such documents are proficient in the language or obtaining a translation from a suitably qualified person.

| | | |
|---|---|---|
| **4.6 Purpose and intended nature of business relationship** | | |
| s.2(1)(c), Sch. 2 | 4.6.1 | An FI must understand the purpose and intended nature of the business relationship. In some instances, this will be self-evident, but in many cases, the FI may have to obtain information in this regard. |
| | 4.6.2 | Unless the purpose and intended nature of the business relationship are obvious, FIs should obtain satisfactory information from all new customers as to the intended purpose and reason for opening the account or establishing the business relationship, and record the information on the account opening documentation. The information obtained by the FIs should be commensurate with the risk profile of the customers and the nature of the business relationships. Information that might be relevant may include:<br><br>(a) nature and details of the customer's business/occupation/employment;<br>(b) the anticipated level and nature of the activity that is to be undertaken through the business relationship (e.g. what the typical transactions are likely to be);<br>(c) location of customer;<br>(d) the expected source and origin of the funds to be used in the business relationship; and<br>(e) initial and ongoing source(s) of wealth or income. |
| **4.7 Delayed identity verification during the establishment of a business relationship** | | |
| s.3(2) & (3), Sch. 2 | 4.7.1 | An FI should verify the identity of a customer and any beneficial owner of the customer before or during the course of establishing a business relationship or conducting transactions for occasional customers. However, FIs may, exceptionally, verify the identity of a customer and any beneficial owner of the customer after establishing the business relationship, provided that: |

| | | |
|---|---|---|
| | | (a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed;<br>(b) it is necessary not to interrupt the normal conduct of business with the customer; and<br>(c) verification is completed as soon as reasonably practicable. |
| | 4.7.2 | An example of a situation in the securities industry where it may be necessary not to interrupt the normal conduct of business is when companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed. |
| | 4.7.3 | If an FI allows verification of the identity of a customer and any beneficial owner of the customer after establishing the business relationship, it should adopt appropriate risk management policies and procedures concerning the conditions under which the customer may utilise the business relationship prior to verification. These policies and procedures should include:<br><br>(a) establishing a reasonable timeframe for the completion of the identity verification measures and the follow-up actions if exceeding the timeframe (e.g. to suspend or terminate the business relationship);<br>(b) placing appropriate limits on the number, types, and/or amount of transactions that can be performed;<br>(c) monitoring of large and complex transactions being carried out outside the expected norms for that type of relationship;<br>(d) keeping senior management periodically informed of any pending completion cases; and<br>(e) ensuring that funds are not paid out to any third party. Exceptions may be made to allow |

| | | |
|---|---|---|
| | | payments to third parties subject to the following conditions:<br>(i) there is no suspicion of ML/TF;<br>(ii) the risk of ML/TF is assessed to be low;<br>(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<br>(iv) the names of recipients do not match with watch lists such as those for terrorist suspects and PEPs. |
| | 4.7.4 | Verification of identity should be completed by an FI within a reasonable timeframe, which generally refers to the following:<br><br>(a) the FI completing such verification no later than 30 working days after the establishment of business relationship;<br>(b) the FI suspending business relationship with the customer and refraining from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if such verification remains uncompleted 30 working days after the establishment of business relationship; and<br>(c) the FI terminating business relationship with the customer if such verification remains uncompleted 120 working days after the establishment of business relationship. |
| s.3(4)(b), Sch. 2, s.25A, DTROP & OSCO, s.12, UNATMO | 4.7.5 | If verification cannot be completed within the reasonable timeframe set in the FI's risk management policies and procedures, the FI should terminate the business relationship as soon as reasonably practicable and refrain from carrying out further transactions (except to return funds or other assets in their original forms as far as possible). The FI should also assess whether this failure provides grounds for knowledge or suspicion of ML/TF and consider making a suspicious transaction report (STR) to the JFIU, particularly if the customer |

| | | |
|---|---|---|
| | | requests that funds or other assets be transferred to a third party or be "transformed" (e.g. from cash into a cashier order) without a justifiable reason. |
| **4.8 Simplified customer due diligence (SDD)** | | |
| <u>General</u> | | |
| s.4, Sch. 2 | 4.8.1 | Section 4 of Schedule 2 permits FIs not to identify and take reasonable measures to verify the identity of the beneficial owners [29] of specific types of customers, or in relation to specific types of products related to the transactions of the customers (referred to as "simplified customer due diligence" under section 4 of Schedule 2; and as "SDD" hereinafter). However, other aspects of CDD must be undertaken and it is still necessary to conduct ongoing monitoring of the business relationship. The use of SDD must be supported by robust assessment to ensure the conditions or circumstances of specific types of customers or products specified in section 4 of Schedule 2 are met. |
| s.3(1)(d) & (e), s.4(1), (3), (5) & (6), Sch. 2 | 4.8.2 | Nonetheless, SDD must not be or continue to be applied when the FI suspects that the customer, the customer's account or the transaction is involved in ML/TF, or when the FI doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity, notwithstanding when the customer, the product, and account type falls within paragraphs 4.8.3, 4.8.15 and 4.8.17 below. |
| s.4(3), Sch. 2 | 4.8.3 | An FI may apply SDD if the customer is -<br><br>(a) an FI as defined in the AMLO;<br>(b) an institution that-<br>(i) is incorporated or established in an equivalent jurisdiction (see paragraphs 4.19);<br>(ii) carries on a business similar to that carried |

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

| | | |
|---|---|---|
| | | on by an FI as defined in the AMLO;<br>(iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and<br>(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;<br>(c) a corporation listed on any stock exchange (“listed company”);<br>(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-<br>(i) an FI as defined in the AMLO;<br>(ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that-<br>i. has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and<br>ii. is supervised for compliance with those requirements.<br>(e) the Government or any public body in Hong Kong; or<br>(f) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body. |
| s.4(2), Sch. 2 | 4.8.4 | If a customer not falling within section 4(3) of Schedule 2 has in its ownership chain an entity that falls within that section, the FI is not required to identify or verify the beneficial owners of that entity in that chain when establishing a business relationship with or carrying out an occasional transaction for the customer. However, FIs 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. |
| s.2(1)(a), (c) & (d), Sch. 2 | 4.8.5 | For avoidance of doubt, the FI must still: |

| | | |
|---|---|---|
| | | (a) identify the customer and verify[30] the customer's identity;<br>(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 FI; and<br>(c) if a person purports to act on behalf of the customer,<br>(i) identify the person and take reasonable measures to verify the person's identity; and<br>(ii) verify the person's authority to act on behalf of the customer,<br><br>in accordance with the relevant requirements stipulated in this Guideline. |
| <u>Local and foreign financial institution</u> | | |
| s.4(3)(a) & (b), Sch. 2 | 4.8.6 | FIs may apply SDD to a customer that is an FI as defined in the AMLO, or an institution that carries on a business similar to that carried on by an FI and meets the criteria set out in section 4(3)(b) of Schedule 2. If the customer does not meet the criteria, the FI must carry out all the CDD measures set out in section 2 of Schedule 2.<br><br>FI may apply SDD to a customer that is an FI as defined in the AMLO that opens an account:<br><br>(a) in the name of a nominee company for holding fund units on behalf of the second-mentioned FI or its underlying customers; or<br>(b) in the name of an investment vehicle in the capacity of a service provider (such as manager or custodian) to the investment vehicle and the underlying investors have no control over the management of the investment vehicle's assets;<br><br>provided that the second-mentioned FI: |

[30] For FIs and listed companies, please refer to paragraphs 4.8.7 and 4.8.8 respectively.

| | | |
|---|---|---|
| | | (i) has conducted CDD:<br>(A) in the case where the nominee company holds fund units on behalf of the second-mentioned FI or the second-mentioned FI's underlying customers, on its underlying customers; or<br>(B) in the case where the second-mentioned FI acts in the capacity of a service provider (such as manager or custodian) to the investment vehicle, on the investment vehicle pursuant to the provisions of the AMLO; and<br>(ii) is authorised to operate the account as evidenced by contractual document or agreement. |
| | 4.8.7 | For ascertaining whether the institution meets the criteria set out in section 4(3)(a) & (b) of Schedule 2, it will generally be sufficient for an FI to verify that the institution is on the list of licensed (and supervised) FIs in the jurisdiction concerned. |
| <u>Listed company</u> | | |
| s.4(3)(c), Sch. 2 | 4.8.8 | An FI may apply SDD to a customer that is a company listed on a stock exchange. For this purpose, the FI should assess whether the stock exchange is subject to any disclosure requirements (either by stock exchange rules, or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership of the listed company. In such a case, it will be generally sufficient for an FI to obtain proof of the customer's listed status on that stock exchange. |
| <u>Investment vehicle</u> | | |
| s.4(3)(d), Sch. 2 | 4.8.9 | FIs may apply SDD to a customer that is an investment vehicle if the FI is able to 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 institutions set out in section |

| | | |
|---|---|---|
| | | 4(3)(d) of Schedule 2. |
| | 4.8.10 | An investment vehicle may be in the form of a legal person or trust, and may be a collective investment scheme or other investment entity. |
| | 4.8.11 | An investment vehicle whether or not responsible for carrying out CDD measures on the underlying investors under governing law of the jurisdiction in which the investment vehicle is established may, where permitted by law, appoint another institution ("appointed institution"), such as a manager, a trustee, an administrator, a transfer agent, a registrar or a custodian, to perform the CDD. Where the person responsible for carrying out the CDD measures (the investment vehicle[31] or the appointed institution) falls within any of the categories of institution set out in section 4(3)(d) of Schedule 2, an FI may apply SDD to that investment vehicle provided that it is satisfied that the investment vehicle has ensured that there are reliable systems and controls in place to conduct the CDD (including identification and verification of the identity) on the underlying investors in accordance with the requirements similar to those set out in the Schedule 2. |
| | 4.8.12 | If neither the investment vehicle nor appointed institution fall within any of the categories of institution set out in section 4(3)(d) of Schedule 2, the FI must identify any investor owning or controlling more than 25% interest of the investment vehicle. The FI may consider whether it is appropriate to rely on a written representation from the investment vehicle or appointed institution (as the case may be) responsible for carrying out the CDD stating, to its |

[31] If the governing law or enforceable regulatory requirements require the investment vehicle to implement CDD measures, the investment vehicle could be regarded as the responsible party for carrying out the CDD measures for the purpose of section 4(3)(d) of Schedule 2 where the investment vehicle meets the requirements, as permitted by law, by delegating or outsourcing to an appointed institution.

| | | |
|---|---|---|
| | | actual knowledge, the identities of such investors or (where applicable) there is no such investor in the investment vehicle. This will depend on risk factors such as whether the investment vehicle is being operated for a small, specific group of persons. Where the FI accepts such a representation, this should be documented, retained, and subject to periodic review. For the avoidance of doubt, the FI is still required to take reasonable measures to verify those investors owning or controlling more than 25% interest of the investment vehicle and (where applicable) other beneficial owners in accordance with paragraphs 4.3. |
| <u>Government and public body</u> | | |
| s.4(3)(e) & (f), Sch. 2 | 4.8.13 | FIs may apply SDD to a customer that is the Hong Kong government, any public bodies in Hong Kong, the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body. |
| s.1, Sch. 2 | 4.8.14 | Public body includes:<br><br>(a) any executive, legislative, municipal or urban council;<br>(b) any Government department or undertaking;<br>(c) any local or public authority or undertaking;<br>(d) any board, commission, committee or other body, whether paid or unpaid, appointed by the Chief Executive or the Government; and<br>(e) any board, commission, committee or other body that has power to act in a public capacity under or for the purposes of any enactment. |
| <u>SDD in relation to specific products</u> | | |
| s.4(4) & (5), Sch. 2 | 4.8.15 | FIs may apply SDD in relation to a customer if the FI has reasonable grounds to believe that the transaction conducted by the customer relates to any one of the following products:<br><br>(a) a provident, pension, retirement or |

| | | |
|---|---|---|
| | | superannuation scheme (however described) that provides retirement benefits to employees, where contributions to the scheme are made by way of deduction from income from employment and the scheme rules do not permit the assignment of a member's interest under the scheme;<br>(b) an insurance policy for the purposes of a provident, pension, retirement or superannuation scheme (however described) that does not contain a surrender clause and cannot be used as a collateral; or<br>(c) a life insurance policy in respect of which:<br>(i) an annual premium of no more than \$8,000 or an equivalent amount in any other currency is payable; or<br>(ii) a single premium of no more than \$20,000 or an equivalent amount in any other currency is payable. |
| | 4.8.16 | For the purpose of item (a) of paragraph 4.8.15, FIs may generally treat the employer as the customer and apply SDD on the employer (i.e. choosing not to identify and take reasonable measures to verify the employees of the scheme). Where FIs have separate business relationships with the employees, it should apply CDD measures in accordance with relevant requirements set out in this Chapter. |
| <u>Solicitor's client accounts</u> | | |
| s.4(6), Sch. 2 | 4.8.17 | If a customer of an FI is a solicitor or a firm of solicitors, the FI may apply SDD to the client account opened by the customer, provided that the following criteria are satisfied:<br><br>(a) the client account is kept in the name of the customer;<br>(b) moneys or securities of the customer's clients in the client account are mingled; and<br>(c) the client account is managed by the customer as those clients' agent. |

| | | |
|---|---|---|
| | 4.8.18 | When opening a client account for a solicitor or a firm of solicitors, FIs should establish the proposed use of the account, i.e. whether to hold co-mingled client funds or the funds of a specific client. |
| | 4.8.19 | If a client account is opened on behalf of a single client or there are sub-accounts for each individual client where funds are not co-mingled at the FI, the FI should establish the identity of the underlying client(s) in addition to that of the solicitor opening the account. |
| **4.9 Special requirements in high risk situations**[32] | | |
| s.15, Sch.2 | 4.9.1 | An FI must comply with the special requirements set out in section 15 of Schedule 2 in:<br><br>(a) a situation that by its nature may present a high risk of ML/TF; or<br>(b) a situation specified by the RA in a notice in writing given to the FI. |
| s.15, Sch. 2 | 4.9.2 | Section 15 of Schedule 2 specifies that an FI must, in any situation that by its nature presents a high risk of ML/TF, comply with the special requirements set out therein which include:<br><br>(a) obtaining the approval of senior management to commence or continue the relationship; and<br>(b) either:<br>(i) taking reasonable measures to establish the relevant customer's or beneficial owner's source of wealth and the source of the funds that will be involved in the business relationship; or<br>(ii) taking additional measures to mitigate the risk of ML/TF. |

[32] Guidance on the special requirements in a situation specified by the RA in a notice in writing given to the FI in relation to jurisdictions subject to a call by the FATF is provided in paragraphs 4.14. Guidance on the special requirements when a customer is not physically present for identification purposes as set out in section 9 of Schedule 2, and the special requirements when a customer is a PEP as set out in section 10 of Schedule 2, are provided in paragraphs 4.10 and 4.11 respectively.

| | | |
|---|---|---|
| | 4.9.3 | Examples of additional measures, for illustration purposes, may include:<br><br>(a) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.) and updating more regularly the identification data of customer and beneficial owner;<br>(b) obtaining additional information on the intended nature of the business relationship (e.g. anticipated account activity);<br>(c) obtaining information on the reasons for intended or performed transactions; or<br>(d) increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination. |
| **4.10 Customer not physically present for identification purposes** | | |
| | 4.10.1 | FIs must apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview[33]. Where a customer has not been physically present for identification purposes, FIs will generally not be able to determine that the documentary evidence of identity actually relates to the customer they are dealing with. Consequently, there are increased risks. |
| Special requirements | | |
| s.5(3)(a) & s.9, Sch. 2 | 4.10.2 | The AMLO permits FIs to establish business relationship through various channels, both face-to-face (e.g. branch) and non-face-to-face (e.g. internet). However, an FI should take additional measures to mitigate any risk (e.g. impersonation risk) associated with customers not physically present for identification purposes. If a customer has |

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

| | | |
|---|---|---|
| | | not been physically present for identification purposes, the FI must carry out at least one of the following additional measures to mitigate the risks posed:<br><br>(a) further verifying the customer's identity on the basis of documents, data or information referred to in section 2(1)(a) of Schedule 2 but not previously used for the purposes of verification of the customer's identity under that section;<br>(b) taking supplementary measures to verify information relating to the customer that has been obtained by the FI; or<br>(c) ensuring that the first payment made into the customer's account is received from an account in the customer's name with an authorized institution or a bank operating in an equivalent jurisdiction that has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 and is supervised for compliance with those requirements by a banking regulator in that jurisdiction. |
| | 4.10.3 | The extent of additional measures set out in paragraph 4.10.2 will depend on the nature and characteristics of the product or service requested and the assessed ML/TF risk presented by the customer. |
| | 4.10.4 | Paragraph 4.10.2(b) allows an FI to utilise different methods to mitigate the risk. These may include measures such as (i) use of an independent and appropriate person to certify identification documents[34]; (ii) checking relevant data against reliable databases or registries; or (iii) using appropriate technology, etc. Whether a particular measure or a combination of measures is acceptable should be assessed on a case-by-case basis. The FI should ensure and be able to demonstrate to the RA |

[34] Further guidance on the use of an independent and appropriate person to certify identification documents is set out in paragraph 7 of Appendix A.

| | | |
|---|---|---|
| | | that the supplementary measure(s) taken can adequately guard against impersonation risk. |
| | 4.10.5 | In taking additional measures to mitigate the risks posed by customers not physically present for identification purposes, reference should also be made by LCs to the relevant provisions (presently paragraph 5.1) in the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission concerning account opening procedures for customers who are not physically present for identification purposes. |
| Other considerations | | |
| | 4.10.6 | While the requirements to undertake additional measures generally apply to a customer that is a natural person, an FI should also mitigate any increased risk (e.g. applying additional due diligence measures set out in paragraph 4.10.2) if a customer that is not a natural person establishes a business relationship with an FI through a non-face-to-face channel. The increased risk may arise from circumstances where the natural person acting on behalf of the customer to establish the business relationship is not physically present for identification purposes. In addition, where an FI is provided with copies of documents for identifying and verifying a legal person customer's identity, an FI should also mitigate any increased risk (e.g. applying additional due diligence measures set out in paragraph 4.10.2). |
| **4.11 Politically exposed persons (PEPs)** | | |
| General | | |
| s.1 & s.10, Sch. 2 | 4.11.1 | Much international attention has been paid in recent years to the risk associated with providing financial and business services to those with a prominent political profile or holding senior public office. However, PEP status itself does not automatically mean that the individuals are corrupt or that they have been incriminated in any corruption. |

| | | |
|---|---|---|
| | 4.11.2 | However, their office and position may render PEPs vulnerable to corruption. The risks increase when the person concerned is from a foreign country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards. |
| | 4.11.3 | An FI should implement appropriate risk management systems to identify PEPs. Under-classification of PEPs poses a higher ML/TF risk to the FI whilst over-classification of PEPs leads to an unnecessary compliance burden to the FI and its customers. |
| s.15, Sch. 2 | 4.11.4 | While the statutory definition of PEPs in the AMLO (see paragraph 4.11.7 below) only includes individuals entrusted with prominent public function in a place outside the People's Republic of China[35], domestic PEPs and international organisation PEPs may also present, by virtue of the positions they hold, a higher ML/TF risk. FIs should therefore adopt an RBA to determine whether to apply the measures in paragraph 4.11.12 below in respect of domestic PEPs and international organisation PEPs. |
| s.1, s.15 & s.5(3)(c), Sch. 2 | 4.11.5 | The statutory definition does not automatically exclude sub-national political figures. Corruption by heads of regional governments, regional government ministers and large city mayors is no less serious as sub-national figures in some jurisdictions may have access to substantial funds. Where FIs identify a customer as a sub-national figure holding a prominent public function, they should apply appropriate measures set out in paragraph 4.11.12. This also applies to domestic sub-national figures assessed by the FI to pose a higher risk. |
| | 4.11.6 | The definitions of PEPs set out in paragraphs 4.11.7, |

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

| | | |
|---|---|---|
| | | 4.11.18 and 4.11.19 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 foreign or domestic government, or by an international organisation respectively. An FI should provide sufficient guidance and examples to its staff to enable them to identify all types of PEPs. In determining what constitutes a prominent (public) function, an FI 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. |
| <u>(Foreign) PEPs</u> | | |
| *Definition* | | |
| s.1, Sch. 2 | 4.11.7 | A (foreign) PEP is defined in the AMLO as:<br><br>(a) an individual who is or has been entrusted with a prominent public function in a place outside the People's Republic of China and<br>(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;<br>(ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);<br>(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<br>(c) a close associate of an individual falling within paragraph (a) (see paragraph 4.11.8). |
| s.1, Sch. 2 | 4.11.8 | The AMLO defines a close associate as:<br><br>(a) an individual who has close business relations |

| | | |
|---|---|---|
| | | with a person falling under paragraph 4.11.7(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph 4.11.7(a) is also a beneficial owner; or<br>(b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under paragraph 4.11.7(a) above. |
| *Identification of foreign PEPs* | | |
| s.19(1), Sch. 2 | 4.11.9 | An FI must establish and maintain effective procedures (e.g. by 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 foreign PEP. |
| | 4.11.10 | While an FI may refer to commercially available databases to identify foreign 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, an FI 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 foreign PEPs used by the database providers may or may not align with the definition of foreign PEPs applied by the FI; and any technical incapability of such databases that may hinder the FI's effectiveness of foreign PEP identification. An FI using such databases as a support tool should ensure that they are fit for the purpose. |
| | 4.11.11 | FIs may 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).<br><br>FIs should be vigilant where either the country to which the customer has business connections or the business/industrial sector is more vulnerable to corruption. |
| *Special requirements and additional measures for foreign PEPs* | | |
| s.5(3)(b) & s.10, Sch. 2 | 4.11.12 | When an FI knows that a customer or beneficial owner of a customer is a foreign PEP, it should, before (i) establishing a business relationship or (ii) continuing an existing business relationship where the customer or the beneficial owner is subsequently found to be a foreign PEP, apply all the following measures:<br><br>(a) obtaining approval from its senior management for establishing or continuing such business relationship[36];<br>(b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds; and<br>(c) conducting enhanced ongoing monitoring on that business relationship (see Chapter 5). |
| | 4.11.13 | Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets). This information will usually give an indication as to the size of wealth the customer would be expected to have, and a picture of how the individual acquired such wealth. Although an FI may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources. |
| | 4.11.14 | Source of funds refers to the origin of the particular |

[36] As a general rule, the approval seniority should be proportionate to the risks associated with the PEP and the related business relationship.

| | | |
|---|---|---|
| | | funds or other assets which are the subject of the business relationship between an individual and the FI (e.g. the amounts being invested, deposited, or wired as part of the business relationship). Source of funds information should not simply be limited to knowing from which the funds may have been transferred, but also the activity that generates the funds. The information obtained should be substantive and establish a provenance or reason for the funds having been acquired. |
| | 4.11.15 | It is for an FI to decide which measures it deems reasonable, in accordance with its assessment of the risks, to establish the source of funds and source of wealth. In practical terms, this will often amount to obtaining information from the foreign 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. FIs should however note that not all declarations are publicly available and that a foreign PEP customer may have legitimate reasons for not providing a copy. FIs 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. |
| | 4.11.16 | Although the measures set out in paragraph 4.11.12 also apply to family members and close associates of the foreign PEP, the risks associated with them may vary depending to some extent on the social-economic and cultural structure of the jurisdiction of the foreign PEP. |
| | 4.11.17 | Since not all foreign PEPs pose the same level of ML/TF risks, an FI should adopt an RBA in determining the extent of measures in paragraphs 4.11.12 taking into account relevant factors, such as:<br><br>(a) the prominent public functions that a foreign PEP |

| | | |
|---|---|---|
| | | holds;<br>(b) the geographical risk associated with the jurisdiction where a foreign PEP holds prominent public functions;<br>(c) the nature of the business relationship (e.g. the delivery/distribution channel used; or the product or service offered); or<br>(d) the level of influence that a foreign PEP may continue to exercise after stepping down from the prominent public function. |
| <u>Domestic PEPs and international organisation PEPs</u> | | |
| *Definition* | | |
| | 4.11.18 | For the purposes of this Guideline, a “domestic PEP” refers to:<br><br>(a) an individual who is or has been entrusted with a prominent public function in a place within the People’s Republic of China and<br>(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;<br>(ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);<br>(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<br>(c) a close associate of an individual falling within paragraph (a) (see paragraph 4.11.8). |
| | 4.11.19 | For the purposes of this Guideline, an “international organisation PEP” refers to:<br><br>(a) an individual who is or has been entrusted with a prominent function by an international organisation, and<br>(i) includes members of senior management, i.e. |

| | | |
|---|---|---|
| | | directors, deputy directors and members of the board or equivalent functions;<br>(ii) but does not include a middle-ranking or more junior official of the international organisation;<br>(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<br>(c) a close associate of an individual falling within paragraph (a) (see paragraph 4.11.8). |
| | 4.11.20 | International organisations referred to in paragraph 4.11.19 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 UN and affiliated international organisations such as the International Maritime Organization; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization; and economic organisations such as the World Trade Organization and the Association of Southeast Asian Nations; etc. |
| *Identification of and additional measures for domestic PEPs and international organisation PEPs* | | |
| | 4.11.21 | An FI should take reasonable measures to determine whether a customer or a beneficial owner of a customer is a domestic PEP or an international organisation PEP[37]. |
| | 4.11.22 | FIs should apply the measures specified in paragraph 4.11.12 with reference to the guidance |

[37] Reference should be made to paragraphs 4.11.9 and 4.11.10.

| | | |
|---|---|---|
| | | provided in paragraphs 4.11.13 to 4.11.17 in any of the following situations[38]:<br><br>(a) before establishing a high risk business relationship with a customer who is or whose beneficial owner is a domestic PEP or an international organisation PEP;<br>(b) when continuing an existing business relationship with a customer who is or whose beneficial owner is a domestic PEP or an international organisation PEP where the relationship subsequently becomes high risk; or<br>(c) when continuing an existing high risk business relationship where the FI subsequently knows that the customer or the beneficial owner of the customer is a domestic PEP or an international organisation PEP. |
| | 4.11.23 | If a domestic PEP or an international organisation PEP is no longer entrusted with a prominent (public) function, an FI may adopt an RBA[39] to determine whether to apply or continue to apply the measures set out in paragraph 4.11.12 in a high risk business relationship with a customer who is or whose beneficial owner is that domestic PEP or international organisation PEP, taking into account various risk factors, such as:<br><br>(a) the level of (informal) influence that the individual could still exercise;<br>(b) the seniority of the position that the individual held as a PEP; or<br>(c) whether the individual's previous and current function are linked in any way (e.g. formally by |

[38] For the avoidance of doubt, an FI should consider whether the application of special requirements in paragraph 4.11.12 could mitigate the ML/TF risk arising from the high risk business relationship with a domestic PEP or an international organisation PEP. Where applicable, an FI should also take additional measures to mitigate such risk in accordance with the guidance provided in paragraphs 4.9.2 and 4.9.3.

[39] The handling of a domestic PEP or an international organisation PEP who is no longer entrusted with a prominent (public) function should be based on an assessment of risk and not merely on prescribed time limits.

| | | |
|---|---|---|
| | | appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).<br><br>The FI should obtain approval from its senior management for such a decision. |
| **4.12 Bearer shares and nominee shareholders** | | |
| <u>Bearer shares</u> | | |
| s.15, Sch. 2 | 4.12.1 | Bearer shares refer to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate. Therefore it is more difficult to establish the beneficial ownership of a company with bearer shares. An FI should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the FI is notified whenever there is a change of beneficial owner of such shares. |
| | 4.12.2 | Where bearer shares have been deposited with an authorised/registered custodian, FIs should seek independent evidence of this, for example confirmation from the registered agent that an authorised/registered custodian holds the bearer shares, together with the identities of the authorised/registered custodian and the person who has the right to those entitlements carried by the share. As part of the FI's ongoing periodic review, it should obtain evidence to confirm the authorised/registered custodian of the bearer shares. |
| | 4.12.3 | Where the shares are not deposited with an authorised/registered custodian, the FI should obtain declarations prior to account opening and annually thereafter from each beneficial owner of such shares. FIs should also require the customer to notify it immediately of any changes in the ownership of the shares. |

| | | |
|---|---|---|
| Nominee shareholders | | |
| | 4.12.4 | For a customer identified to have nominee shareholders in its ownership structure, an FI should obtain satisfactory evidence of the identities of the nominees, and the persons on whose behalf they are acting, as well as the details of arrangements in place, in order to determine who the beneficial owner is. |
| **4.13 Jurisdictions posing higher risk** | | |
| | 4.13.1 | FIs should give particular attention to, and exercise extra care in respect of:<br><br>(a) business relationships and transactions with persons (including legal persons and other FIs) from or in jurisdictions that do not or insufficiently apply the FATF Recommendations; and<br>(b) transactions and business connected with jurisdictions assessed as higher risk.<br><br>In such case, the special requirements of section 15 of Schedule 2 may apply (see paragraphs 4.9). |
| | 4.13.2 | In determining which jurisdictions do not apply, or insufficiently apply the FATF Recommendations, or may otherwise pose a higher risk, FIs should consider, among other things:<br><br>(a) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT systems;<br>(b) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;<br>(c) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the UN; or<br>(d) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations |

| | | |
|---|---|---|
| | | operation.<br><br>"Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, 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. |
| **4.14 Jurisdictions subject to a call by the FATF** | | |
| s.15, Sch. 2 | 4.14.1 | An FI should apply additional measures, proportionate to the risks and in accordance with the guidance provided in paragraphs 4.9, to business relationships and transactions with natural and legal persons, and FIs, from jurisdictions for which this is called for by the FATF. |
| s.15, Sch. 2 | 4.14.2 | Where mandatory enhanced measures or countermeasures[40] are called for by the FATF, or in other circumstances independent of any call by the FATF but also considered to be higher risk, RA may also, through a notice in writing:<br><br>(a) impose a general obligation on FIs to comply with the special requirements set out in section 15 of Schedule 2; or<br>(b) require FIs to undertake specific countermeasures identified or described in the notice.<br><br>The type of measures in paragraphs (a) and (b) above would be proportionate to the nature of the risks and/or deficiencies. |

[40] 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 countermeasures.

| 4.15 Reliance on CDD performed by intermediaries | | |
|---|---|---|
| General | | |
| s.18, Sch. 2 | 4.15.1 | An FI may rely upon an intermediary to perform any part of the CDD measures[41] specified in section 2 of Schedule 2, subject to the criteria set out in section 18 of Schedule 2. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the FI.<br><br>In a third-party reliance scenario, the third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying FI, and would apply its own procedures to perform the CDD measures. |
| | 4.15.2 | For the avoidance of doubt, reliance on intermediaries does not apply to outsourcing or agency relationships, in which the outsourced entity or agent applies the CDD measures on behalf of the FI, in accordance with the FI's procedures, and subject to the FI's control of effective implementation of these procedures by the outsourced entity or agent. |
| s.18(1), Sch. 2 | 4.15.3 | When relying on an intermediary, the FI must:<br><br>(a) obtain written confirmation from the intermediary that the intermediary agrees to act as the FI's intermediary and perform which part of the CDD measures specified in section 2 of Schedule 2; and<br>(b) be satisfied that the intermediary will on request provide a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out the CDD measures without delay. |

[41] For the avoidance of doubt, an FI cannot rely on an intermediary to continuously monitor its business relationship with a customer for the purpose of complying with the requirements in section 5 of Schedule 2.

| | | |
|---|---|---|
| s.18(4)(a), Sch. 2 | 4.15.4 | An FI 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 FI to obtain at the same time from the intermediary a copy of the document, or a record of the data or information, that is obtained by the intermediary in the course of carrying out that measure. |
| s.18(4)(b), Sch. 2 | 4.15.5 | Where these documents and records are kept by the intermediary, the FI should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the FI's business relationship with the customer and for at least five years beginning on the date on which the business relationship of a customer with the FI ends or until such time as may be specified by the RA. The FI must ensure that the intermediary will, if requested by the FI within the period specified in the record-keeping requirements of AMLO, provide to the FI a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out that measure as soon as reasonably practicable after receiving the request. The FI 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 FI anymore. |
| | 4.15.6 | An FI should conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay. |
| | 4.15.7 | Whenever an FI 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 FI intends to terminate its relationship |

| | | |
|---|---|---|
| | | with the intermediary, it should immediately obtain all CDD information from the intermediary. If the FI has any doubts regarding the CDD measures carried out by the intermediary previously, the FI should perform the required CDD as soon as reasonably practicable. |
| <u>Domestic intermediaries</u> | | |
| s.18(3)(a), (3)(b) & (7), Sch. 2 | 4.15.8 | An FI may rely upon any one of the following domestic intermediaries, to perform any part of the CDD measures set out in section 2 of Schedule 2:<br><br>(a) an FI that is an authorized institution, a licensed corporation, an authorized insurer, an appointed insurance agent or an authorized insurance broker (intermediary FI);<br>(b) an accounting professional meaning:<br>(i) a certified public accountant or a certified public accountant (practising), as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50);<br>(ii) a corporate practice as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50); or<br>(iii) a firm of certified public accountants (practising) registered under Part IV of the Professional Accountants Ordinance (Cap. 50);<br>(c) an estate agent meaning:<br>(i) a licensed estate agent as defined by section 2(1) of the Estate Agents Ordinance (Cap. 511); or<br>(ii) a licensed salesperson as defined by section 2(1) of the Estate Agents Ordinance (Cap. 511);<br>(d) a legal professional meaning:<br>(i) a solicitor as defined by section 2(1) of the Legal Practitioners Ordinance (Cap. 159); or<br>(ii) a foreign lawyer as defined by section 2(1) of the Legal Practitioners Ordinance (Cap. 159); or<br>(e) a trust or company service provider (TCSP) licensee meaning: |

| | | |
|---|---|---|
| | | (i) a person who holds a licence granted under section 53G or renewed under section 53K of the AMLO; or<br>(ii) a deemed licensee as defined by section 53ZQ(5) of the AMLO,<br><br>provided that in the case of an accounting professional, an estate agent, a legal professional or a TCSP licensee, the FI is satisfied that the domestic intermediary has adequate procedures in place to prevent ML/TF and is required to comply with the relevant requirements set out in Schedule 2 with respect to the customer[42]. |
| s.18(3)(a) & (3)(b), Sch. 2 | 4.15.9 | An FI should take appropriate measures to ascertain if the domestic intermediary satisfies the criteria set out in paragraph 4.15.8, which may include:<br><br>(a) where the domestic intermediary is an accounting professional, an estate agent, a legal professional or a TCSP licensee, ascertaining whether the domestic intermediary is required to comply with the relevant requirements set out in Schedule 2 with respect to the customer;<br>(b) making enquiries concerning the domestic intermediary's stature or the extent to which any group AML/CFT standards are applied and audited; or<br>(c) reviewing the AML/CFT policies and procedures of the domestic intermediary. |
| <u>Overseas intermediaries</u> | | |
| s.18(3)(c), Sch. 2 | 4.15.10 | An FI may rely upon an overseas intermediary[43] carrying on business or practising in an equivalent jurisdiction[44] to perform any part of the CDD |

[42] CDD requirements set out in Schedule 2 apply to an accounting professional, an estate agent, a legal professional or a TCSP licensee with respect to a customer only when it, by way of business, prepares for or carries out for the customer a transaction specified under section 5A of the AMLO.

[43] The overseas intermediary and the FI could be unrelated or within the same group of companies to which the FI belongs.

[44] Guidance on jurisdictional equivalence is provided in paragraphs 4.19.

| | | |
|---|---|---|
| | | measures set out in section 2 of Schedule 2, where the intermediary:<br><br>(a) falls into one of the following categories of businesses or professions:<br>(i) an institution that carries on a business similar to that carried on by an intermediary FI;<br>(ii) a lawyer or a notary public;<br>(iii) an auditor, a professional accountant, or a tax advisor;<br>(iv) a trust or company service provider;<br>(v) a trust company carrying on trust business; and<br>(vi) a person who carries on a business similar to that carried on by an estate agent;<br>(b) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction;<br>(c) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and<br>(d) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs or the regulatory bodies (as may be applicable). |
| | 4.15.11 | An FI should take appropriate measures to ascertain if the overseas intermediary satisfies the criteria set out in paragraph 4.15.10. Appropriate measures that should be taken to ascertain if the criterion set out in paragraph 4.15.10(c) is satisfied may include:<br><br>(a) making enquiries concerning the overseas intermediary's stature or the extent to which any group's AML/CFT standards are applied and audited; or<br>(b) reviewing the AML/CFT policies and procedures of the overseas intermediary. |

| Related foreign financial institutions as intermediaries | | |
|---|---|---|
| s.18(3)(d), (3A) & (7), Sch. 2 | 4.15.12 | An FI may also rely upon a related foreign financial institution (related foreign FI) to perform any part of the CDD measures set out in section 2 of Schedule 2, if the related foreign FI:<br><br>(a) carries on, in a place outside Hong Kong, a business similar to that carried on by an intermediary FI; and falls within any of the following descriptions:<br>(i) it is within the same group of companies as the FI;<br>(ii) if the FI is incorporated in Hong Kong, it is a branch of the FI;<br>(iii) if the FI is incorporated outside Hong Kong:<br>(A) it is the head office of the FI; or<br>(B) it is a branch of the head office of the FI;<br>(b) is required under group policy:<br>(i) to have measures in place to ensure compliance with requirements similar to the requirements imposed under Schedule 2; and<br>(ii) to implement programmes against ML/TF; and<br>(c) is supervised for compliance with the requirements mentioned in paragraph (b) at a group level:<br>(i) by an RA; or<br>(ii) by an authority in an equivalent jurisdiction[45] that performs, in relation to the holding company or the head office of the FI, functions similar to those of an RA under the AMLO. |
| s.18(3A) & (4)(c), Sch. 2 | 4.15.13 | The group policy set out in paragraph 4.15.12(b) refers to a policy of the group of companies to which the FI belongs and the policy applies to the FI and the related foreign FI. The group policy should include CDD and record-keeping requirements similar to the requirements imposed under Schedule 2 and a group-wide AML/CFT system[46] (e.g. compliance and audit functions). The group policy |

[45] Guidance on jurisdictional equivalence is provided in paragraphs 4.19.
[46] Reference should be made to Chapter 2.

| | | |
|---|---|---|
| | | should also be able to mitigate adequately any higher country risk in relation to the jurisdiction where the related foreign FI is located. The FI should be satisfied that the related foreign FI is subject to regular and independent reviews over its ongoing compliance with the group policy conducted by any group-level compliance, audit or other similar AML/CFT functions. |
| s.18(3A), Sch. 2 | 4.15.14 | The FI should be able to demonstrate that the implementation of the group policy is supervised at a group level by either an RA or an authority in an equivalent jurisdiction that performs functions similar to those of an RA under the AMLO, which practises group-wide supervision which extends to the related foreign FI. |
| **4.16 Pre-existing customers** | | |
| s.6, Sch. 2 | 4.16.1 | FIs must perform the CDD measures prescribed in Schedule 2 and this Guideline in respect of pre-existing customers (with whom the business relationship was established before the AMLO came into effect on 1 April 2012), when:<br><br>(a) a transaction takes place with regard to the customer, which is, by virtue of the amount or nature of the transaction, unusual or suspicious; or is not consistent with the FI'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;<br>(b) a material change occurs in the way in which the customer's account is operated;<br>(c) the FI suspects that the customer or the customer's account is involved in ML/TF; or<br>(d) the FI doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity. |
| | 4.16.2 | Trigger events may include the re-activation of a dormant account or a change in the beneficial |

| | | |
|---|---|---|
| | | ownership or control of the account but FIs will need to consider other trigger events specific to their own customers and business. |
| s.5, Sch. 2 | 4.16.3 | FIs should note that requirements for ongoing monitoring under section 5 of Schedule 2 also apply to pre-existing customers (see Chapter 5). |
| **4.17 Failure to satisfactorily complete CDD measures** | | |
| s.3(4), Sch. 2 | 4.17.1 | Where an FI is unable to complete the CDD measures in accordance with paragraph 4.1.9 or 4.7.1, the FI:<br><br>(a) must not establish a business relationship or carry out any occasional transaction with that customer; or<br>(b) must terminate the business relationship as soon as reasonably practicable if the FI has already established a business relationship with the customer.<br><br>The FI should also assess whether this failure provides grounds for knowledge or suspicion of ML/TF and where there is relevant knowledge or suspicion, should make an STR to the JFIU in relation to the customer. |
| **4.18 Prohibition on anonymous accounts** | | |
| s.16, Sch. 2 | 4.18.1 | FIs must not maintain anonymous accounts or accounts in fictitious names for any new or existing customer. Where numbered accounts exist, FIs must maintain them in such a way that full compliance can be achieved with the AMLO. FIs 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 available to the RAs, other authorities, the CO, auditors, and other staff with appropriate authority. |

| 4.19 Jurisdictional equivalence | | |
|---|---|---|
| General | | |
| s.4(3)(b)(i), s.4(3)(d)(iii), s.4(3)(f), s.9(c)(ii) & s.18(3)(c), Sch. 2 | 4.19.1 | Jurisdictional equivalence and the determination of equivalence is an important aspect in the application of CDD measures under the AMLO. Equivalent jurisdiction is defined in the AMLO as meaning:<br><br>(a) a jurisdiction that is a member of the FATF, other than Hong Kong; or<br>(b) a jurisdiction that imposes requirements similar to those imposed under Schedule 2. |
| Determination of jurisdictional equivalence | | |
| | 4.19.2 | An FI may therefore be required to evaluate and determine for itself which jurisdictions other than FATF members apply requirements similar to those imposed under Schedule 2 for jurisdictional equivalence purposes. The FI should document its assessment of the jurisdiction, and include consideration of the following factors:<br><br>(a) whether the jurisdiction concerned is a member of FATF-style regional bodies and its recent mutual evaluation report published by the FATF-style regional bodies[47];<br>(b) whether the jurisdiction concerned is identified by the FATF as having strategic AML/CFT deficiencies and the recent progress of improving its AML/CFT regime;<br>(c) any advisory circulars issued by RAs from time to time alerting FIs to such jurisdictions with poor AML/CFT controls; or<br>(d) any other AML/CFT related publications that are published by specialised national, international, non-governmental or commercial organisations (for example, Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption). |

[47] FIs should bear in mind that mutual evaluation reports are at a "point in time", and should be interpreted as such.

| | | |
|---|---|---|
| | 4.19.3 | As the AML/CFT regime of a jurisdiction will change over time, an FI should review the jurisdictional equivalence assessment from time to time. |

# Chapter 5 - ONGOING MONITORING

| General | | |
|---|---|---|
| s.5(1), Sch. 2 | 5.1 | Ongoing monitoring is an essential component of effective AML/CFT systems.<br><br>An FI must continuously monitor its business relationship with a customer by:<br><br>(a) reviewing from time to time documents, data and information relating to the customer that have been obtained by the FI for the purpose of complying with the requirements imposed under Part 2 of Schedule 2 to ensure that they are up-to-date and relevant;<br>(b) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the FI's knowledge of the customer, the customer's business, risk profile and source of funds; and<br>(c) identifying transactions that<br>(i) are complex, unusually large in amount or of an unusual pattern; and<br>(ii) have no apparent economic or lawful purpose,<br>and examining the background and purposes of those transactions and setting out the findings in writing. |
| **Keeping customer information up-to-date** | | |
| s.5(1)(a), Sch. 2 | 5.2 | To ensure documents, data and information of a customer obtained are up-to-date and relevant[48], an FI should undertake reviews of existing CDD records of customers on a regular basis and/or upon trigger events[49]. Clear policies and procedures should be |

[48] Keeping the CDD information up-to-date and relevant does not mean that an FI has to re-verify identities that have been verified (unless doubts arise as to veracity or adequacy of the evidence previously obtained for the purposes of customer identification).

[49] While it is not necessary to regularly review the existing CDD records of a dormant customer, an FI should conduct a review upon reactivation of the relationship. The FI should define clearly what constitutes a dormant customer in its policies and procedures.

| | | |
|---|---|---|
| | | developed, especially on the frequency of periodic review or what constitutes a trigger event[50]. |
| | 5.3 | All customers that present high ML/TF risks should be subject to a minimum of an annual review, or more frequent reviews if deemed necessary by the FI, to ensure the CDD information retained remains up-to-date and relevant. |
| **Transaction monitoring systems and processes** | | |
| s.19(3), Sch.2 | 5.4 | An FI should establish and maintain adequate systems and processes (e.g. the use of large transactions exception reports which help an FI to stay apprised of operational activities) to monitor transactions. The design, degree of automation and sophistication of transaction monitoring systems and processes should be developed appropriately having regard to the following factors:<br><br>(a) the size and complexity of its business;<br>(b) the ML/TF risks arising from its business;<br>(c) the nature of its systems and controls;<br>(d) the monitoring procedures that already exist to satisfy other business needs; and<br>(e) the nature of the products and services provided (which includes the means of delivery or communication). |
| | 5.5 | An FI should ensure that the transaction monitoring systems and processes can provide all relevant staff who are tasked with conducting transaction monitoring and investigation with timely and sufficient information required to identify, analyse and effectively monitor customers' transactions. |
| | 5.6 | An FI should ensure that the transaction monitoring systems and processes can support the ongoing monitoring of a business relationship in a holistic approach, which may include monitoring activities of |

[50] Examples of trigger events are set out in paragraph 8 of Appendix A.

| | | |
|---|---|---|
| | | a customer's multiple accounts within or across lines of business, and related customers' accounts within or across lines of business. This means preferably the FI adopts a relationship-based approach rather than on a transaction-by-transaction basis. |
| | 5.7 | In designing transaction monitoring systems and processes, including (where applicable) setting of parameters and thresholds, an FI should take into account the transaction characteristics, which may include:<br><br>(a) the nature and type of transactions (e.g. abnormal size or frequency);<br>(b) the nature of a series of transactions (e.g. structuring a single transaction into a number of cash deposits);<br>(c) the counterparties of transactions;<br>(d) the geographical origin/destination of a payment or receipt; and<br>(e) the customer's normal account activity or turnover. |
| | 5.8 | An FI should regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including (where applicable) parameters and thresholds adopted. The parameters and thresholds should be properly documented and independently validated to ensure that they are appropriate to its operations and context. |
| **Risk-based approach to monitoring** | | |
| | 5.9 | FIs should conduct ongoing monitoring in relation to all business relationships following the RBA. The extent of monitoring (e.g. frequency and intensity of monitoring) should be commensurate with the ML/TF risk profile of the customer. Where the ML/TF risks are higher, the FI should conduct enhanced monitoring. In lower risk situations, the FI may reduce the extent of monitoring. |

| | | |
|---|---|---|
| s.5(3), Sch. 2 | 5.10 | FIs must take additional measures to compensate for any risk of ML/TF in monitoring business relationships involving (a) a customer not having been physically present for identification purposes; (b) a customer or a beneficial owner of a customer being a foreign PEP; and (c) a customer or a beneficial owner of a customer being involved in a situation referred to in section 15 of Schedule 2. |
| | 5.11 | FIs should be vigilant for changes of the basis of the business relationship with the customer over time. These may include where:<br><br>(a) new products or services that pose higher risk are entered into;<br>(b) new corporate or trust structures are created;<br>(c) the stated activity or turnover of a customer changes or increases; or<br>(d) the nature of transactions changes or their volume or size increases, etc. |
| | 5.12 | Where the basis of the business relationship changes significantly, FIs should carry out further CDD procedures to ensure that the ML/TF risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures must take account of the above changes. |
| <u>Review of transactions</u> | | |
| s.5(1)(b) & (c), Sch. 2 | 5.13 | An FI should take appropriate steps (e.g. examining the background and purposes of the transactions; making appropriate enquiries to or obtaining additional CDD information from a customer) to identify if there are any grounds for suspicion, when:<br><br>(a) the customer's transactions are not consistent with the FI's knowledge of the customer, the customer's business, risk profile or source of funds;<br>(b) the FI identifies transactions that (i) are complex, unusually large in amount or of an unusual pattern, and (ii) have no apparent economic or |

| | | |
|---|---|---|
| | | lawful purpose[51]. |
| | 5.14 | Where the FI conducts enquiries and obtains what it considers to be a satisfactory explanation of the activity or transaction, it may conclude that there are no grounds for suspicion, and therefore take no further action. Even if no suspicion is identified, the FI should consider updating the customer risk profile based on any relevant information obtained. |
| | 5.15 | However, where the FI cannot obtain a satisfactory explanation of the transaction or activity, it may conclude that there are grounds for suspicion. In any event where there is any suspicion identified during transaction monitoring, an STR should be made to the JFIU. |
| | 5.16 | An FI should be aware that making enquiries to customers, when conducted properly and in good faith, will not constitute tipping-off. However, if the FI reasonably believes that performing the CDD process will tip off the customer, it may stop pursuing the process. The FI should document the basis for its assessment and file an STR to the JFIU. |
| | 5.17 | The findings and outcomes of steps taken by the FI in paragraph 5.13, as well as the rationale of any decision made after taking these steps, should be properly documented in writing and be available to RAs, other competent authorities and auditors. |
| | 5.18 | Where cash transactions (including deposits and withdrawals) and transfers to third parties are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, FIs must approach such situations with caution and make relevant further enquiries. Where the FI has been unable to satisfy itself that any cash transaction or third party transfer is reasonable, and |

[51] An FI should examine the background and purposes of the transactions and set out its findings in writing.

| | | |
|---|---|---|
| | | therefore considers it suspicious, it should make an STR to the JFIU. |

# Chapter 6 – TERRORIST FINANCING, FINANCIAL SANCTIONS AND PROLIFERATION FINANCING

| Terrorist financing | | |
|---|---|---|
| | 6.1 | TF is the financing of terrorist acts, and of terrorists and terrorist organisations. It generally refers to the carrying out of transactions involving property owned by terrorists or terrorist organisations, or that has been, or is intended to be, used to assist the commission of terrorist acts. Different from ML, the focus of which is on the handling of criminal proceeds (i.e. the source of property is what matters), the focus of TF is on the destination or use of property, which may have derived from legitimate sources. |
| UNSCR 1267 (1999), 1373 (2001), 1988 (2011), 1989 (2011), 2253 (2015), and 2368 (2017) | 6.2 | The United Nations Security Council (UNSC) has passed UNSCR 1373 (2001), which calls on all member states to act to prevent and suppress the financing of terrorist acts. The UN has also published the names of individuals and organisations in relation to involvement with Al-Qa'ida, ISIL (Da'esh) and the Taliban under relevant UNSCRs (e.g. UNSCR 1267 (1999), 1988 (2011), 1989 (2011), 2253 (2015), 2368 (2017) and their successor resolutions). All UN member states are required to freeze any funds, or other financial assets, or economic resources of any person(s) named in these lists and to report any suspected name matches to the relevant authorities. |
| | 6.3 | UNATMO is an ordinance to further implement a decision under UNSCR 1373 (2001) relating to measures for prevention of terrorist acts and a decision under UNSCR 2178 (2014) relating to the prevention of travel for the purpose of terrorist acts or terrorist training; as well as to implement certain terrorism-related multilateral conventions and certain FATF Recommendations. |

| | | |
|---|---|---|
| s.4 & 5, UNATMO | 6.4 | Where a person or property is designated by a Committee of the UNSC established pursuant to the relevant UNSCRs as stated in paragraph 6.2 as a terrorist/terrorist associate or terrorist property [52] respectively, the Chief Executive may publish a notice in the Gazette specifying the name of the person or the property under section 4 of the UNATMO. Besides, section 5 of the UNATMO 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 respectively, and if the order is made, it will also be published in the Gazette. |
| s.6, 7, 8, 8A & 11L, UNATMO | 6.5 | A number of provisions in the UNATMO are of particular relevance to FIs, and are listed below.<br><br>(a) section 6 empowers the Secretary for Security (S for S) to freeze suspected terrorist property;<br>(b) section 7 prohibits the provision or collection of property for use to commit terrorist acts;<br>(c) section 8 prohibits any person from making available or collecting or soliciting property or financial (or related) services for terrorists and terrorist associates;<br>(d) section 8A prohibits any person from dealing with any property knowing that, or being reckless as to whether, the property is specified terrorist property or property of a specified terrorist or terrorist associate; and<br>(e) section 11L prohibits any person from providing or collecting any property to finance the travel of a person between states with the intention or knowing that the travel will be for a specified purpose, i.e. the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually |

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

| | | |
|---|---|---|
| | | occurs); or the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs as a result of the training). |
| s.6(1), 8 & 8A(1), UNATMO | 6.6 | The S for S can licence exceptions to the prohibitions to enable frozen property to be unfrozen and to allow payments to be made to or for the benefit of a designated party under the UNATMO (e.g. reasonable living/legal expenses and payments liable to be made under the Employment Ordinance). An FI seeking such a licence should write to the Security Bureau. |
| **Financial sanctions & proliferation financing** | | |
| s.3(1), UNSO | 6.7 | UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the UNSC, including targeted financial sanctions [53] against individuals and entities designated by the UNSC or its Committees. Designated persons and entities are specified by notice published in the Gazette or on the website of the Commerce and Economic Department Bureau.<br><br>It is an offence to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of, a designated person or entity, as well as those acting on their behalf, at their direction, or owned or controlled by them; or to deal with any funds, other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities, except under the authority of a licence granted by the Chief Executive. |

[53] Targeted financial sanctions refer to both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

| | | |
|---|---|---|
| Applicable UNSO Regulation | 6.8 | The Chief Executive may grant licence for making available or dealing with any funds, or other financial assets, and economic resources to or belonging to a designated person or entity under specified circumstances in accordance with the provisions of the relevant regulation made under the UNSO. An FI seeking such a licence should write to the Commerce and Economic Development Bureau. |
| | 6.9 | To combat PF, the UNSC adopts a two-tiered approach through resolutions made under Chapter VII of the UN Charter imposing mandatory obligations on UN member states: (a) global approach under UNSCR 1540 (2004) and its successor resolutions; and (b) country-specific approach under UNSCR 1718 (2006) against the Democratic People's Republic of Korea (DPRK) and UNSCR 2231 (2015) against the Islamic Republic of Iran (Iran) and their successor resolutions. |
| s.4, WMD(CPS)O | 6.10 | The counter proliferation financing regime in Hong Kong is implemented through legislation, including the regulations made under the UNSO which are specific to DPRK and Iran, and the WMD(CPS)O. Section 4 of WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely defined and includes the lending of money or other provision of financial assistance. |
| <u>Sanctions imposed by other jurisdictions</u> | | |
| | 6.11 | While FIs do not normally have any obligation under Hong Kong laws to have regard to unilateral sanctions imposed by other organisations or authorities in other jurisdictions, an FI operating internationally will need to be aware of the scope and focus of relevant sanctions regimes in those jurisdictions. Where these sanctions regimes may affect their operations, FIs should consider what implications exist and take appropriate measures, such as including relevant overseas designations in |

| | | |
|---|---|---|
| | | its database for screening purpose, where applicable. |
| **Database maintenance, screening and enhanced checking** | | |
| | 6.12 | An FI should establish and maintain effective policies, procedures and controls to ensure compliance with the relevant regulations and legislation on TF, financial sanctions and PF. The legal and regulatory obligations of FIs and those of their staff should be well understood and adequate guidance and training should be provided to the latter. |
| | 6.13 | It is particularly vital that an FI should be able to identify terrorist suspects and possible designated parties, and detect prohibited transactions. To this end, an FI should ensure that it maintains a database of names and particulars of terrorists and designated parties which consolidates the various lists that have been made known to the FI. Alternatively, an FI may make arrangements to access to such a database maintained by third party service providers and take appropriate measures (e.g. conduct sample testing periodically) to ensure the completeness and accuracy of the database. |
| | 6.14 | Whether or not a UNSCR or sanctions list has been implemented through Hong Kong legislation, there are offences under existing legislation relating to ML, TF and PF that are relevant. Inclusion of a country, individual, entity or activity in the UNSCR or sanctions list may constitute grounds for knowledge or suspicion for the purposes of relevant ML, TF and PF laws, thereby triggering statutory (including reporting) obligations as well as offence provisions. RAs draw to the attention to FIs from time to time whenever there are any updates to the UNSCRs or sanctions lists relating to terrorism, TF and PF promulgated by the UNSC. The FI should ensure that countries, individuals and entities included in |

| | | |
|---|---|---|
| | | UNSCRs and sanctions lists are included in the database as soon as practicable after they are promulgated by the UNSC and regardless of whether the relevant sanctions have been implemented by legislation in Hong Kong. |
| | 6.15 | An FI should include in its database (i) the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau; (ii) the lists that RAs draw to the attention of FIs from time to time; and (iii) any relevant designations by overseas authorities which may affect its operations. The database should be subject to timely update whenever there are changes, and should be made easily accessible by relevant staff. |
| | 6.16 | To avoid establishing business relationship or conducting transactions with any terrorist suspects and possible designated parties, an FI should implement an effective screening mechanism [54], which should include:<br><br>(a) screening its customers and any beneficial owners of the customers against current database at the establishment of the relationship;<br>(b) screening its customers and any beneficial owners of the customers against all new and any updated designations to the database as soon as practicable; and<br>(c) screening all relevant parties in a cross-border wire transfer against current database before executing the transfer. |
| | 6.17 | The screening requirements set out in paragraph 6.16 (a) and (b) should extend to other connected parties as defined in paragraph 4.2.13 and PPTAs of a customer using an RBA. |

[54] Screening should be carried out carried out irrespective of the risk profile attributed to the customer.

| | | |
|---|---|---|
| | 6.18 | When possible name matches are identified during screening, an FI should conduct enhanced checks to determine whether the possible matches are genuine hits. In case of any suspicions of TF, PF or sanction violations, the FI should make a report to the JFIU. Records of enhanced checking results, together with all screening records, should be documented, or recorded electronically. |
| | 6.19 | An FI may rely on its overseas office to maintain the database or to undertake the screening process. However, the FI is reminded that the ultimate responsibility for ensuring compliance with the relevant regulations and legislation on TF, financial sanctions and PF remains with the FI. |

# Chapter 7 – SUSPICIOUS TRANSACTION REPORTS AND LAW ENFORCEMENT REQUESTS

| | | |
|---|---|---|
| **General issues** | | |
| s.25A(1) & (7), DTROP & OSCO, s.12(1) & 14(5), UNATMO | 7.1 | It is a statutory obligation under sections 25A(1) of the DTROP and the OSCO, as well as section 12(1) of the UNATMO, that where a person knows or suspects that any property: (a) in whole or in part directly or indirectly represents any person's proceeds of, (b) was used in connection with, or (c) is intended to be used in connection with, drug trafficking or an indictable offence; or that any property is terrorist property, the person shall as soon as it is reasonable for him to do so, file an STR with the JFIU. The STR should be made together with any matter on which the knowledge or suspicion is based. Under the DTROP, the OSCO and the UNATMO, failure to report knowledge or suspicion carries a maximum penalty of imprisonment for three months and a fine of $50,000. |
| **Knowledge vs. suspicion** | | |
| | 7.2 | Generally speaking, knowledge is likely to include:<br><br>(a) actual knowledge;<br>(b) knowledge of circumstances which would indicate facts to a reasonable person; and<br>(c) knowledge of circumstances which would put a reasonable person on inquiry. |
| | 7.3 | Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence. As far as an FI is concerned, when a transaction or a series of transactions of a customer is not consistent with the FI's knowledge of the customer, or is unusual (e.g. in a pattern that has no apparent economic or lawful purpose), the FI should take appropriate steps to further examine the transactions and identify if there is any suspicion |

| | | |
|---|---|---|
| | | (see paragraphs 5.13 to 5.18). |
| | 7.4 | For a person to have knowledge or suspicion, he does not need to know the nature of the criminal activity underlying the ML, or that the funds themselves definitely arose from the criminal offence. Similarly, the same principle applies to TF. |
| | 7.5 | Once knowledge or suspicion has been formed,<br><br>(a) an FI should file an STR even where no transaction has been conducted by or through the FI[55]; and<br>(b) the STR must be made as soon as is reasonably practical after the suspicion was first identified. |
| Tipping-off | | |
| s.25A(5), DTROP & OSCO, s.12(5), UNATMO | 7.6 | It is an offence ("tipping-off") to reveal to any person any information which might prejudice an investigation; if a customer is told that a report has been made, this would prejudice the investigation and an offence would be committed.<br><br>The tipping-off provision includes circumstances where a suspicion has been raised internally within an FI, but has not yet been reported to the JFIU. |
| **AML/CFT systems in relation to suspicious transaction reporting** | | |
| | 7.7 | An FI should implement appropriate AML/CFT systems in order to fulfil its statutory reporting obligation, and properly manage and mitigate the risks associated with any customer or transaction involved in an STR. The AML/CFT systems should include: |

55 The reporting obligations require a person to report suspicions of ML/TF, irrespective of the amount involved. The reporting obligations of section 25A(1) DTROP and OSCO and section 12(1) UNATMO apply to "any property". These provisions establish a reporting obligation whenever a suspicion arises, without reference to transactions *per se.* Thus, the obligation to report applies whether or not a transaction was actually conducted and also covers attempted transactions.

| | | |
|---|---|---|
| | | (a) appointment of an MLRO (see Chapter 2);<br>(b) implementing clear policies and procedures over internal reporting, reporting to the JFIU, post-reporting risk mitigation and prevention of tipping-off; and<br>(c) keeping proper records of internal reports and STRs. |
| | 7.8 | The FI should have measures in place to check, on an ongoing basis, that its AML/CFT systems in relation to suspicious transaction reporting comply with relevant legal and regulatory requirements and operate effectively. The type and extent of the measures to be taken should be appropriate having regard to the risk of ML/TF as well as the nature and size of the business. |
| <u>Money laundering reporting officer</u> | | |
| | 7.9 | An FI should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the JFIU and law enforcement agencies. The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions of the MLRO should include having oversight of:<br><br>(a) review of internal disclosures and exception reports and, in light of all available relevant information, determination of whether or not it is necessary to make a report to the JFIU;<br>(b) maintenance of all records related to such internal reviews; and<br>(c) provision of guidance on how to avoid tipping-off.<br><br>To fulfil these functions, all FIs must ensure that the MLRO receives full co-operation from all staff and full access to all relevant documentation so that he is in a position to decide whether attempted or actual ML/TF is suspected or known. |

| Identifying suspicious transactions | | |
|---|---|---|
| | 7.10 | An FI should provide sufficient guidance to its 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. |
| | 7.11 | An FI may adopt, where applicable, the "SAFE" approach promoted by the JFIU, which includes: (a) screening the account for suspicious indicators; (b) asking the customers appropriate questions; (c) finding out the customer's records; and (d) evaluating all the above information. Details of the "SAFE" approach are available at JFIU's website (www.jfiu.gov.hk). |
| | 7.12 | The following is a (non-exhaustive) list of general examples of situations that might give rise to suspicion in certain circumstances:<br><br>(a) transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;<br>(b) transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business;<br>(c) where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular customer;<br>(d) where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged;<br>(e) where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing |

| | | |
|---|---|---|
| | | monitoring process;<br>(f) where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;<br>(g) the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services;<br>(h) transfers to and from high risk jurisdictions[56] without reasonable explanation, which are not consistent with the customer's declared business dealings or interests; and<br>(i) unnecessary routing of funds or other property from/to third parties or through third party accounts. |
| | 7.13 | Sector-specific examples of situations that might give rise to suspicion of ML using transactions involving securities, future contracts or leveraged foreign exchange contracts in certain circumstances include:<br><br>**Customer-related**<br><br>(a) A customer introduced by an overseas bank, affiliate or other investor both of which are based in jurisdictions that do not or insufficiently apply the FATF recommendations or otherwise pose higher risk.<br><br>(b) A customer located in a place outside Hong Kong who uses local accounts to trade on stock or futures exchanges located in that place.<br><br>(c) Requests by customers for investment management services (as regards securities, futures contracts or leveraged foreign exchange contracts) where the source of the funds is unclear or not consistent with the customers' |

[56] Guidance on determining high risk jurisdictions is provided at paragraphs 4.13.

| | | |
|---|---|---|
| | | apparent standing.<br><br>(d) A customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.<br><br>**Trading-related**<br><br>(a) Buying and selling of securities or futures with no discernible purpose or where the nature, size or frequency of the transactions appears unusual. For example, where a customer frequently purchases securities at a high price and subsequently sells them at a considerable loss to the same party. This may indicate transferring value from one party to another.<br><br>(b) A number of transactions by the same customer in small amounts relating to the same investment, each purchased for cash and then sold in one transaction, the proceeds being paid to a person other than that customer.<br><br>(c) A customer engages in prearranged or other non-competitive trading in particular securities, futures contracts or leveraged foreign exchange contracts.<br><br>(d) The entry of matching buys and sells in particular securities or futures or leveraged foreign exchange contracts ("wash trading"), creating the illusion of trading. Such wash trading does not result in a bona fide market position, and might provide "cover" for a money launderer.<br><br>(e) Wash trading through multiple accounts might be used to transfer funds between accounts by generating offsetting losses and profits in different accounts. Transfers of positions between accounts that do not appear to be |

| | | |
|---|---|---|
| | | commonly controlled also could be a warning sign. (It should be noted that wash trading is also an indication of market manipulation and LCs are expected to take appropriate steps to ensure that proper safeguards exist to prevent the firm from acting in a way which would result in the firm perpetrating any conduct which constitutes market misconduct under section 274, 275 or 278 of the SFO, or any criminal offence under section 295, 296 or 299 of the SFO).<br><br>(f) Securities transactions occur across many jurisdictions, and in particular jurisdictions that do not or insufficiently apply the FATF recommendations or otherwise pose higher risk.<br><br>**Settlement/custody/transfers-related**<br><br>(a) Large or unusual settlements of transactions in cash or bearer form or where a customer only deals with a LC in cash or cash equivalent.<br><br>(b) A customer uses a LC to make payments or to hold funds and/or other property that are rarely used or are not being used to trade in securities, futures contracts or leveraged foreign exchange contracts i.e. account appears to be used as a depositary account or a conduit for transfers.<br><br>(c) Non-resident account with very large account movements and subsequent fund transfers to offshore financial centres.<br><br>(d) Transfers of positions, funds or other property between securities accounts of parties that do not appear to be commonly controlled or have an apparent relationship.<br><br>(e) Frequent funds or other property transfers or cheque payments to or from third parties that |

| | | |
|---|---|---|
| | | are unrelated, unverified or difficult to verify.<br><br>(f) Incoming payments made by cheques with multiple endorsements.<br><br>(g) A customer allocates incoming third party deposits among numerous accounts.<br><br>(h) The involvement of offshore companies on whose accounts multiple transfers are made, especially when they are destined for a tax haven, and to accounts in the name of offshore companies of which the customer may be a shareholder.<br><br>(i) The customer's explanation regarding the method of acquiring the physical securities deposited at the LC does not make sense or changes. |
| | 7.14 | Sector-specific examples of situations which might give rise to suspicion of ML involving employees of LCs in certain circumstances include:<br><br>(a) Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays without reasonable cause.<br><br>(b) Unusual or unexpected increase in the sales performance of an employee.<br><br>(c) The employee's supporting documentation for customers' accounts or orders is incomplete or missing.<br><br>(d) The use of an address which is not the customer's home or office address, e.g. utilization of an employee's address for the dispatch of customer documentation or correspondence. |

| | | |
|---|---|---|
| | 7.15 | The examples set out in paragraphs 7.12 to 7.14 are non-exhaustive and only provide examples of the most basic ways in which money may be laundered. However, identification of any of the types of transactions listed above should prompt further investigations and be a catalyst towards making at least initial enquiries about the source of funds.<br><br>FIs should also be aware of elements of individual transactions and situations that might give rise to suspicion of TF in certain circumstances. The FATF publishes studies of methods and trends of TF from time to time, and FIs may refer to the FATF website for additional information and guidance. |
| Internal reporting | | |
| | 7.16 | An FI should establish and maintain clear policies and procedures to ensure that:<br><br>(a) all staff are made aware of the identity of the MLRO and of the procedures to follow when making an internal report; and<br>(b) all internal reports must reach the MLRO without undue delay. |
| | 7.17 | While FIs may wish to set up internal systems that allow staff to consult with supervisors or managers before sending a report to the MLRO, under no circumstances should reports raised by staff be filtered out by supervisors or managers who have no responsibility for the money laundering reporting/compliance function. The legal obligation is to report as soon as it is reasonable to do so, so reporting lines should be as short as possible with the minimum number of people between the staff with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO. |
| s.25A(4), DTROP & OSCO, s.12(4), | 7.18 | Once a staff member of an FI has reported suspicion to the MLRO in accordance with the policies and procedures established by the FI for |

| | | |
|---|---|---|
| UNATMO | | the making of such reports, the statutory obligation of the staff member has been fully satisfied. |
| | 7.19 | The internal report should include sufficient details of the customer concerned and the information giving rise to the suspicion. |
| | 7.20 | The MLRO should acknowledge receipt of an internal report and provide a reminder of the obligation regarding tipping-off to the reporting staff member upon internal reporting. |
| | 7.21 | When evaluating an internal report, the MLRO must take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the FI concerning the customers to which the report relates. This may include:<br><br>(a) making a review of other transaction patterns and volumes through connected accounts, preferably adopting a relationship-based approach rather than on a transaction-by-transaction basis;<br>(b) making reference to any previous patterns of instructions, the length of the business relationship and CDD and ongoing monitoring information and documentation; and<br>(c) appropriate questioning of the customer per the systematic approach to identify suspicious transactions recommended by the JFIU[57]. |
| | 7.22 | The need to search for information concerning connected accounts or relationships should strike an appropriate balance between the statutory requirement to make a timely STR to the JFIU and any delays that might arise in searching for more relevant information concerning connected accounts or relationships. The review process should be |

[57] For details, please see JFIU's website (www.jfiu.gov.hk).

| | | |
|---|---|---|
| | | documented, together with any conclusions drawn. |
| <u>Reporting to the JFIU</u> | | |
| | 7.23 | If after completing the review of the internal report, the MLRO decides that there are grounds for knowledge or suspicion, he should disclose the information to the JFIU as soon as it is reasonable to do so after his evaluation is complete together with the information on which that knowledge or suspicion is based.<br><br>Dependent on when knowledge or suspicion arises, an STR may be made either before a suspicious transaction or activity occurs (whether the intended transaction ultimately takes place or not), or after a transaction or activity has been completed. |
| | 7.24 | Providing an MLRO acts in good faith in deciding not to file an STR with the JFIU, it is unlikely that there will be any criminal liability for failing to report if the MLRO concludes that there is no suspicion after taking into account all available information. It is however vital for the MLRO to keep proper records of the deliberations and actions taken to demonstrate he has acted in reasonable manner. |
| | 7.25 | In the event that an urgent reporting is required (e.g. where a customer has instructed the FI to move funds or other property, close the account, make cash available for collection, or carry out significant changes to the business relationship, etc.), particularly when the account is part of an ongoing law enforcement investigation, an FI should indicate this in the STR. Where exceptional circumstances exist in relation to an urgent reporting, an initial notification by telephone should be considered. |
| | 7.26 | An FI is recommended to indicate any intention to terminate a business relationship in its initial disclosure to the JFIU, thereby allowing the JFIU to comment, at an early stage, on such a course of action. |

| | | |
|---|---|---|
| | 7.27 | An FI should ensure STRs filed with the JFIU are of high quality taking into account feedback and guidance provided by the JFIU and RAs from time to time. |
| | 7.28 | The JFIU recognises the importance of having effective feedback procedures in place and therefore, provides feedback both in its quarterly report [58] and other appropriate platform when needed. |
| Post reporting matters | | |
| s.25A (2)(a), DTROP & OSCO, s.12(2B)(a), UNATMO | 7.29 | The JFIU will acknowledge receipt of an STR made by an FI under section 25A of both the DTROP and the OSCO, and section 12 of the UNATMO. If there is no need for imminent action e.g. the issue of a restraint order on an account, consent will usually be given for the institution to operate the account under the provisions of section 25A(2) of both the DTROP and the OSCO, and section 12(2B)(a) of the UNATMO. An example of such a letter is given at Appendix B to this Guideline. For disclosures submitted via e-channel "STREAMS", e-receipt will be issued via the same channel. The JFIU may, on occasion, seek additional information or clarification with an FI of any matter on which the knowledge or suspicion is based. If a no-consent letter is issued by the JFIU, the FI should act according to the content of the letter and seek legal advice where necessary. |
| s.25A(2), DTROP & OSCO, s.12(2), UNATMO | 7.30 | Filing a report to the JFIU provides FIs with a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report, provided:<br><br>(a) the report is made before the FI undertakes the disclosed acts and the acts (transaction(s)) are |

[58] The purpose of the quarterly report, which is relevant to all financial sectors, is to raise AML/CFT awareness. It consists of two parts, (i) analysis of STRs and (ii) matters of interest and feedback. The report is available at a secure area of the JFIU's website at www.jfiu.gov.hk. LCs can apply for a login name and password by completing the registration form available on the JFIU's website or by contacting the JFIU directly.

| | | |
|---|---|---|
| | | undertaken with the consent of the JFIU; or<br>(b) the report is made after the FI has performed the disclosed acts (transaction(s)) and the report is made on the FI’s own initiative and as soon as it is reasonable for the FI to do so. |
| | 7.31 | However, the statutory defence stated in paragraph 7.30 does not absolve an FI from the legal, reputational or regulatory risks associated with the account’s continued operation. An FI should also be aware that a “consent” response from the JFIU to a pre-transaction report should not be construed as a “clean bill of health” for the continued operation of the account or an indication that the account does not pose a risk to the FI. |
| | 7.32 | An FI should conduct an appropriate review of a business relationship upon the filing of an STR to the JFIU, irrespective of any subsequent feedback provided by the JFIU, and apply appropriate risk mitigating measures. Filing a report with the JFIU and continuing to operate the relationship without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified is not acceptable. If necessary, the issue should be escalated to the FI’s senior management to determine how to handle the relationship concerned to mitigate any potential legal or reputational risks posed by the relationship in line with the FI’s business objectives, and its capacity to mitigate the risks identified. |
| | 7.33 | An FI should be aware that the reporting of a suspicion in respect of a transaction or event does not remove the need to report further suspicious transactions or events in respect of the same customer. Further suspicious transactions or events, whether of the same nature or different to the previous suspicion, must continue to be reported to the MLRO who should make further reports to the JFIU if appropriate. |

| | | |
|---|---|---|
| <u>Record-keeping</u> | | |
| | 7.34 | An FI 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 assessment, whether the internal report resulted in an STR to the JFIU, and information to allow the papers relevant to the report to be located. |
| | 7.35 | An FI must establish and maintain a record of all STRs made to the JFIU. The record should include details of the date of the STR, the person who made the STR, and information to allow the papers relevant to the STR to be located. This register may be combined with the register of internal reports, if considered appropriate. |
| **Requests from law enforcement agencies** | | |
| | 7.36 | An FI may receive various requests from law enforcement agencies, e.g. search warrants, production orders, restraint orders or confiscation orders, pursuant to relevant legislation in Hong Kong. These requests are crucial to aid law enforcement agencies, to carry out investigations as well as restrain and confiscate illicit proceeds. Therefore, an FI should establish clear policies and procedures to handle these requests in an effective and timely manner, including allocation of sufficient resources. An FI should appoint a staff member as the main point of contact with law enforcement agencies. |
| | 7.37 | An FI should respond to any search warrant and production order within the required time limit by providing all information or materials that fall within the scope of the request. Where an FI encounters difficulty in complying with the timeframes stipulated, the FI should at the earliest opportunity contact the officer-in-charge of the investigation for further guidance. |

| | | |
|---|---|---|
| s.10 & 11, DTROP, s.15 & 16, OSCO, s.6, UNATMO | 7.38 | During a law enforcement investigation, an FI may be served with a restraint order which prohibits the dealing with particular funds or property pending the outcome of an investigation. An FI must ensure that it is able to freeze the relevant property that is the subject of the order. It should be noted that the restraint order may not apply to all funds or property involved within a particular business relationship and FIs should consider what, if any, funds or property may be utilised subject to the laws of Hong Kong. |
| s.3, DTROP, s.8, OSCO, s13, UNATMO | 7.39 | Upon the conviction of a defendant, a court may order the confiscation of his criminal proceeds and an FI may be served with a confiscation order in the event that it holds funds or other property belonging to that defendant that are deemed by the Courts to represent his benefit from the crime. A court may also order the forfeiture of property where it is satisfied that the property is terrorist property. |
| | 7.40 | When an FI receives a request from a law enforcement agency, e.g. search warrant or production order, in relation to a particular customer or business relationship, the FI should assess the risk involved and the need to conduct an appropriate review on the customer or the business relationship to determine whether there is any suspicion, and should also be aware that the customer subject to the request can be a victim of crime. |

# Chapter 8 – RECORD-KEEPING

| General | | |
|---|---|---|
| | 8.1 | Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps the investigating authorities to establish a financial profile of a suspect, trace the criminal or terrorist property or funds and assists the Court to examine all relevant past transactions to assess whether the property or funds are the proceeds of or relate to criminal or terrorist offences. |
| | 8.2 | An FI should maintain CDD information, transaction records and other records that are necessary and sufficient to meet the record-keeping requirements under the AMLO, this Guideline and other regulatory requirements, that are appropriate to the nature, size and complexity of its businesses. The FI should ensure that:<br><br>(a) the audit trail for funds moving through the FI that relate to any customer and, where appropriate, the beneficial owner of the customer, account or transaction is clear and complete;<br>(b) all CDD information and transaction records are available swiftly to RAs, other authorities and auditors upon appropriate authority; and<br>(c) it can demonstrate compliance with any relevant requirements specified in other sections of this Guideline and other guidelines issued by the RAs. |

| Retention of records relating to CDD and transactions | | |
|---|---|---|
| s.20(1)(b)(i), Sch. 2<br><br>s.2(1)(c), Sch. 2<br><br>s.20(1)(b)(ii), Sch. 2 | 8.3 | An FI should keep:<br><br>(a) the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and where applicable, verifying the identity of the customer and/or beneficial owner of the customer and/or beneficiary and/or persons who purport to act on behalf of the customer and/or other connected parties to the customer;<br>(b) other documents and records obtained throughout the CDD and ongoing monitoring process, including SDD, situations where special requirements are required, and when taking simplified and enhanced measures[59];<br>(c) where applicable, the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship;<br>(d) the original or a copy of the records and documents relating to the customer's account (e.g. account opening form; risk assessment form[60]) and business correspondence[61] with the customer and any beneficial owner of the customer (which at a minimum should include business correspondence material to CDD measures or significant changes to the operation of the account); and |

[59] For SDD, please refer to paragraphs 4.8; for situations where special requirements are required, please refer to paragraphs 4.9 to 4.14; for simplified and enhanced measures, please refer to paragraphs 3.1 and 3.2.

[60] This refers to a document which FIs may use to document the assessment of ML/TF risk levels associated with customers or business relationships. For example, the ML/TF risk rating of a customer (refer to paragraph 3.4), the risk assessment of business relationships with domestic PEPs or international organisation PEPs who are no longer entrusted with a prominent (public) function (refer to paragraph 4.11.23), etc.

[61] An FI is not expected to keep each and every correspondence, such as a series of emails with the customer; the expectation is that sufficient correspondence is kept to demonstrate compliance with the AMLO.

| | | |
|---|---|---|
| | | (e) the results of any analysis undertaken (e.g. inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose). |
| s.20(2) & (3), Sch. 2 | 8.4 | All documents and records mentioned in paragraph 8.3 should be kept throughout the continuance of the business relationship with the customer and for a period of at least five years after the end of the business relationship. Similarly, for occasional transaction equal to or exceeding the CDD thresholds (i.e. $8,000 for wire transfers and $120,000 for other types of transactions), an FI should keep all documents and records mentioned in paragraph 8.3 for a period of at least five years after the date of the occasional transaction. |
| s.20(1)(a), Sch. 2 | 8.5 | FIs should maintain the original or a copy of the documents, and a record of the data and information, obtained in connection with each transaction the FI carries out, both domestic and international, which should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. |
| s.20(2), Sch. 2 | 8.6 | All documents and records mentioned in paragraph 8.5 should be kept for a period of at least five years after the completion of a transaction, regardless of whether the business relationship ends during the period. |
| s.21, Sch. 2 | 8.7 | 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. |
| s.20(4), Sch. 2 | 8.8 | An RA may, by notice in writing to an FI, require it to keep the records relating to a specified transaction or |

| | | |
|---|---|---|
| | | customer for a period specified by the RA that is longer than those referred to in paragraphs 8.4 and 8.6, where the records are relevant to an ongoing criminal or other investigation, or to any other purposes as specified in the notice. |
| Part 3, Sch. 2 | 8.9 | Irrespective of where CDD and transaction records are held, an FI is required to comply with all legal and regulatory requirements in Hong Kong, especially Part 3 of Schedule 2. |
| **Records kept by intermediaries** | | |
| s.18(4)(b), Sch. 2 | 8.10 | Where customer identification and verification documents are held by an intermediary on which the FI is relying to carry out CDD measures, an FI concerned remains responsible for compliance with all record-keeping requirements. The FI should ensure that the intermediary being relied on has systems in place to comply with all the record-keeping requirements under the AMLO and this Guideline (including the requirements of paragraphs 8.3 to 8.9), and that documents and records will be provided by the intermediary as soon as reasonably practicable after the intermediary receives the request from the FI. |
| s.18(4)(a), Sch. 2 | 8.11 | For the avoidance of doubt, an FI that relies on an intermediary for carrying out a CDD measure should immediately obtain the data or information that the intermediary has obtained in the course of carrying out that measure. |
| | 8.12 | An FI should ensure that an intermediary will pass the documents and records to the FI, upon termination of the services provided by the intermediary. |

# Chapter 9 – STAFF TRAINING

| | | |
|---|---|---|
| | 9.1 | Ongoing staff training is an important element of an effective system to prevent and detect ML/TF activities. The effective implementation of even a well-designed internal control system can be compromised if staff using the system is not adequately trained. |
| | 9.2 | It is an FI's responsibility to provide adequate training for its staff so that they are adequately trained to implement its AML/CFT systems. The scope and frequency of training should be tailored to the specific risks faced by the FI and pitched according to the job functions, responsibilities and experience of the staff. New staff should be required to attend initial training as soon as possible after being hired or appointed.<br><br>Apart from the initial training, an FI should also provide refresher training regularly to ensure that its staff are reminded of their responsibilities and are kept informed of new developments related to ML/TF. |
| | 9.3 | An FI should implement a clear and well articulated policy for ensuring that relevant staff receive adequate AML/CFT training. |
| | 9.4 | Staff should be made aware of:<br><br>(a) their FI's and their own personal statutory obligations and the possible consequences for failure to comply with CDD and record-keeping requirements under the AMLO;<br>(b) their FI's and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROP, the OSCO and the UNATMO;<br>(c) any other statutory and regulatory obligations that concern their FIs and themselves under the DTROP, the OSCO, the UNATMO, the UNSO |

| | | |
|---|---|---|
| | | and the AMLO, and the possible consequences of breaches of these obligations;<br>(d) the FI's policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting; and<br>(e) 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 particular roles in the FI with respect to AML/CFT. |
| | 9.5 | In addition, the following areas of training may be appropriate for certain groups of staff:<br><br>(a) all new staff, irrespective of seniority:<br>(i) an introduction to the background to ML/TF and the importance placed on ML/TF by the FI; and<br>(ii) the need for identifying and reporting of any suspicious transactions to the MLRO, and the offence of tipping-off;<br>(b) front-line personnel who are dealing directly with the public:<br>(i) the importance of their roles in the FI's ML/TF strategy, as the first point of contact with potential money launderers;<br>(ii) the FI's policies and procedures in relation to CDD and record-keeping requirements that are relevant to their job responsibilities; and<br>(iii) training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required;<br>(c) back-office staff, depending on their roles:<br>(i) appropriate training on customer verification and relevant processing procedures; and<br>(ii) how to recognise unusual activities including abnormal settlements, payments or delivery instructions;<br>(d) managerial staff including internal audit officers and COs: |

| | | |
|---|---|---|
| | | (i) higher level training covering all aspects of the FI's AML/CFT regime; and<br>(ii) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as reporting of suspicious transactions to the JFIU; and<br>(e) MLROs:<br>(i) specific training in relation to their responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the JFIU; and<br>(ii) training to keep abreast of AML/CFT requirements/developments generally. |
| | 9.6 | An FI is encouraged to consider using a mix of training techniques and tools in delivering training, depending on the available resources and learning needs of their staff. These techniques and tools may include on-line learning systems, focused classroom training, relevant videos as well as paper- or intranet-based procedures manuals. An FI may consider including available FATF papers and typologies as part of the training materials. The FI should be able to demonstrate to the RA that all materials should be up-to-date and in line with current requirements and standards. |
| | 9.7 | No matter which training approach is adopted, an FI should maintain records of who have been trained, when the staff received the training and the type of the training provided. Records should be maintained for a minimum of 3 years. |
| | 9.8 | An FI should monitor the effectiveness of the training. This may be achieved by:<br><br>(a) testing staff's understanding of the FI's policies and procedures to combat ML/TF, the understanding of their statutory and regulatory obligations, and also their ability to recognise |

| | | |
|---|---|---|
| | | suspicious transactions;<br>(b) monitoring the compliance of staff with the FI's AML/CFT systems as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken; and<br>(c) monitoring attendance and following up with staff who miss such training without reasonable cause. |

# Chapter 10 – WIRE TRANSFERS

| **General** | | |
|---|---|---|
| | 10.1 | This Chapter primarily applies to authorized institutions and money service operators. Other FIs should also comply with section 12 of Schedule 2 and the guidance provided in this Chapter if they act as an ordering institution, an intermediary institution or a beneficiary institution as defined under the AMLO. Where an FI is the originator or recipient of a wire transfer, it is not acting as an ordering institution, an intermediary institution or a beneficiary institution and thus is not required to comply with the requirements under section 12 of Schedule 2 or this Chapter in respect of that transaction. |
| s.1(4) & s.12(11), Sch. 2 | 10.2 | A wire transfer is a transaction carried out by an institution (the ordering institution) on behalf of a person (the originator) by electronic means with a view to making an amount of money available to that person or another person (the recipient) at an institution (the beneficiary institution), which may be the ordering institution or another institution, whether or not one or more other institutions (intermediary institutions) participate in completion of the transfer of the money. An FI should follow the relevant requirements set out in this Chapter with regard to its role in a wire transfer. |
| | 10.3 | The requirements set out in section 12 of Schedule 2 and this Chapter are also applicable to wire transfers using cover payment mechanism (e.g. MT202COV payments)[62]. |
| s.12(2), Sch. 2 | 10.4 | Section 12 of Schedule 2 and this Chapter do not apply to the following wire transfers: |

[62] Reference should be made to the paper "Due diligence and transparency regarding cover payment messages related to cross-border wire transfer" published by the Basel Committee on Banking Supervision in May 2009 and the "Guidance Paper on Cover Payment Messages Related to Cross-border Wire Transfers" issued by the HKMA in February 2010.

| | | |
|---|---|---|
| | | (a) a wire transfer between two FIs as defined in the AMLO if each of them acts on its own behalf;<br>(b) a wire transfer between an FI as defined in the AMLO and a foreign institution[63] if each of them acts on its own behalf;<br>(c) a wire transfer if:<br>(i) it arises from a transaction that is carried out using a credit card or debit card (such as withdrawing money from a bank account through an automated teller machine with a debit card, obtaining a cash advance on a credit card, or paying for goods or services with a credit or debit card), except when the card is used to effect a transfer of money; and<br>(ii) the credit card or debit card number is included in the message or payment form accompanying the transfer. |
| **Ordering institutions** | | |
| s.12(3) & (5), Sch. 2 | 10.5 | An ordering institution must ensure that a wire transfer of amount equal to or above $8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information:<br><br>(a) the originator's name;<br>(b) the number of the originator's account maintained with the ordering institution and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned by the ordering institution;<br>(c) the originator's address or, the originator's customer identification number[64] or identification |

[63] For the purpose of section 12 of Schedule 2 and this Chapter, "foreign institution" means an institution that is located in a place outside Hong Kong and that carries on a business similar to that carried on by an FI as defined in the AMLO.

[64] Customer identification number refers to a number which uniquely identifies the originator to the originating institution and is a different number from the unique transaction reference number referred to in paragraph 10.7. The customer identification number must refer to a record held by the originating institution which contains at least one of the following: the customer address, the identification document number, or the date and place of birth.

| | | |
|---|---|---|
| | | document number or, if the originator is an individual, the originator's date and place of birth;<br>(d) the recipient's name; and<br>(e) the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution. |
| s.12(3), (3A) & (5), Sch. 2 | 10.6 | An ordering institution must ensure that a wire transfer of amount below $8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information:<br><br>(a) the originator's name;<br>(b) the number of the originator's account maintained with the ordering institution and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned by the ordering institution;<br>(c) the recipient's name; and<br>(d) the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution. |
| | 10.7 | The unique reference number assigned by the ordering institution or beneficiary institution referred to in paragraphs 10.5 and 10.6 should permit traceability of the wire transfer. |
| | 10.8 | For a wire transfer of amount equal to or above $8,000 (or an equivalent amount in any other currency), an ordering institution must ensure that the required originator information accompanying the wire transfer is accurate. |

| | | |
|---|---|---|
| s.3(1)(c) & (d), Sch. 2 | 10.9 | For an occasional wire transfer involving an amount equal to or above $8,000 (or an equivalent amount in any other currency), an ordering institution must verify the identity of the originator. For an occasional wire transfer below $8,000 (or an equivalent amount in any other currency), the ordering institution is in general not required to verify the originator's identity, except when several transactions are carried out which appear to the ordering institution to be linked and are equal to or above $8,000 (or an equivalent amount in any other currency), or when there is a suspicion of ML/TF. |
| s.12(7), Sch. 2 | 10.10 | An ordering institution may bundle a number of wire transfers from a single originator into a batch file for transmission to a recipient or recipients in a place outside Hong Kong. In such cases, the ordering institution may only include the originator's account number or, in the absence of such an account, a unique reference number in the wire transfer but the batch file should contain required and accurate originator information, and required recipient information, that is fully traceable within the recipient country. |
| s.12(6), Sch. 2 | 10.11 | For a domestic wire transfer[65], an ordering institution may choose not to include the complete required originator information in the wire transfer but only include the originator's account number or, in the absence of an account, a unique reference number, provided that the number permits traceability of the wire transfer. |
| s.12(6), Sch. 2 | 10.12 | If an ordering institution chooses not to include complete required originator information as stated in paragraph 10.11, it must, on the request of the institution to which it passes on the transfer |

[65] Domestic wire transfer means a wire transfer in which the ordering institution and the beneficiary institution and, if one or more intermediary institutions are involved in the transfer, the intermediary institution or all the intermediary institutions are FIs (as defined in the AMLO) located in Hong Kong.

| | | |
|---|---|---|
| | | instruction or the RA, provide complete required originator information within 3 business days after the request is received. In addition, such information should be made available to law enforcement agencies immediately upon request. |
| **Intermediary institutions** | | |
| s.12(8), Sch. 2 | 10.13 | An intermediary institution must ensure that all originator and recipient information which accompanies the wire transfer is retained with the transfer and is transmitted to the institution to which it passes on the transfer instruction. |
| | 10.14 | Where technical limitations prevent the required originator or recipient information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary institution should keep a record, for at least five years, of all the information received from the ordering institution or another intermediary institution. The above requirement also applies to a situation where technical limitations prevent the required originator or recipient information accompanying a domestic wire transfer from remaining with a related cross-border wire transfer. |
| s.19(2), Sch. 2 | 10.15 | An intermediary institution must establish and maintain effective procedures for identifying and handling incoming wire transfers that do not comply with the relevant originator or recipient information requirements, which include:<br><br>(a) taking reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required recipient information; and<br>(b) having risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator information or required recipient |

| | | |
|---|---|---|
| | | information; and (ii) the appropriate follow-up action. |
| s.12(10)(a), Sch. 2 | 10.16 | In respect of the risk-based policies and procedures referred to in paragraph 10.15, if a cross-border wire transfer is not accompanied by the required originator information or required recipient information, the intermediary institution must as soon as reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, the intermediary institution should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved. |
| s.12(10)(b), Sch. 2 | 10.17 | If the intermediary institution is aware that the accompanying information that purports to be the required originator information or required recipient information is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved. |
| **Beneficiary institutions** | | |
| s.19(2), Sch. 2 | 10.18 | A beneficiary institution must establish and maintain effective procedures for identifying and handling incoming wire transfers that do not comply with the relevant originator or recipient information requirements, which include:<br><br>(a) taking reasonable measures (e.g. post-event monitoring) to identify domestic or cross-border wire transfers that lack required originator information or required recipient information; and<br>(b) having risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator information or required recipient information; and (ii) the appropriate follow-up action. |

| | | |
|---|---|---|
| s.12(9)(a) & s.12(10)(a), Sch.2 | 10.19 | In respect of the risk-based policies and procedures referred to in paragraph 10.18, if a domestic or cross-border wire transfer is not accompanied by the required originator information or required recipient information, the beneficiary institution must as soon as reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, the beneficiary institution should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved. |
| s.12(9)(b) & s.12(10)(b), Sch.2 | 10.20 | If the beneficiary institution is aware that the accompanying information that purports to be the required originator information or required recipient information is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved. |
| s.3(1)(c), Sch. 2 | 10.21 | For a wire transfer of amount equal to or above $8,000 (or an equivalent amount in any other currency), a beneficiary institution should verify the identity of the recipient, if the identity has not been previously verified. |

# APPENDIX A

| Illustrative examples and further guidance | | |
|---|---|---|
| 3.1 | 1 | **Examples of possible simplified measures in relation to RBA** |
| | | Examples include:<br><br>(a) reducing the frequency of updates of customer identification information;<br>(b) reducing the degree of ongoing monitoring and scrutiny of transactions based on a reasonable monetary threshold; or<br>(c) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and intended nature from the type of transactions or business relationship established. |
| 3.1 | 2 | **Examples of possible enhanced measures in relation to RBA** |
| | | Examples include:<br><br>(a) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.) and updating more regularly the identification data of customer and beneficial owner;<br>(b) obtaining additional information on the intended nature of the business relationship (e.g. anticipated account activity);<br>(c) obtaining information on the reasons for intended or performed transactions; or<br>(d) increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination. |

| | | |
|---|---|---|
| 4.2.6 | 3 | **Examples of possible measures in relation to the verification of the name, legal form and current existence of a customer that is a legal person** |
| | | Examples of possible measures to verify the name, legal form and current existence of a legal person:<br><br>for a locally incorporated company:<br><br>(a) performing a search of file at the Hong Kong Company Registry to obtain a company report (or obtaining from the customer a certified true copy of a company search report issued and certified by a company registry or professional person);<br><br>for a company incorporated overseas:<br><br>(b) performing a similar company search enquiry of the registry in the place of incorporation to obtain a company report;<br>(c) obtaining a certificate of incumbency or equivalent issued by the company's registered agent in the place of incorporation (or accepting a certified true copy of a certificate of incumbency certified by a professional person); or<br>(d) obtaining a similar or comparable document to a company search report or a certificate of incumbency certified by a professional person in the relevant jurisdiction. |
| 4.2.14 | 4 | **Examples of simplified and enhanced measures in verifying the identity of a customer that is a legal person, trust or other similar legal arrangement** |
| | | <u>Simplified measures</u><br><br>Where the assessed ML/TF risks are lower, an FI may consider to accept documents, data or information other than the examples provided in paragraphs 4.2.6 and 4.2.11, when verifying the |

| | | |
|---|---|---|
| | | name, legal form and current existence of the customer, or powers that regulate and bind the customer. Examples of such other documents, data or information include:<br><br>(a) where the customer is<br>(i) an FI as defined in the AMLO; or<br>(ii) other FI that is incorporated or established in an equivalent jurisdiction, carry on a business similar to that carried out by an FI as defined in the AMLO, and subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF;<br>a proof that the customer is a licensed (and supervised) FI in the jurisdiction concerned;<br>(b) where the customer is a listed company, a proof of its listed status;<br>(c) where the customer is the government or a public body in Hong Kong or in an equivalent jurisdiction, a proof that the customer is the government or a public body; and<br>(d) where the customer is a collective investment scheme authorised for offering to the public in Hong Kong or in an equivalent jurisdiction, a proof of its authorisation status.<br><br><u>Enhanced measures</u><br><br>Where the assessed ML/TF risks are higher, in addition to verifying the name, legal form and current existence of the customer, and powers that regulate and bind the customer in accordance with paragraphs 4.2.6 and 4.2.11, an FI should decide whether additional information in respect of the customer, its operation and the individuals behind it should be obtained and the extent of further verification that is required. |

| | | |
|---|---|---|
| 4.3.13 | 5 | **Examples of information which may be collected to identify the intermediate layers of the corporate structure of a legal person with multiple layers in its ownership structure** |
| | | If the customer's ownership structure consists of multiple layers of companies, an FI should determine on a risk sensitive basis the amount of information in relation to the intermediate layers to be collected, which may include 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).<br><br>FIs need not, as a matter of routine, verify the details of the intermediate companies in the ownership structure of a company. Complex ownership structures (e.g. structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to ensure that the FI is satisfied on reasonable grounds as to the identity of the beneficial owners.<br><br>The need to verify the intermediate corporate layers of the ownership structure of a company will therefore depend upon the FI's overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for the FI to consider if it has taken adequate measures to identify the beneficial owners.<br><br>Where the ownership is dispersed, the FI may concentrate on identifying and taking reasonable measures to verify the identity of those who exercise ultimate control over the management of the company. |

| | | |
|---|---|---|
| 4.5.3 | 6 | **Examples of procedures to establish whether the identification documents offered by customers are genuine, or have been reported as lost or stolen** |
| | | If suspicions are raised in relation to any identification document offered by customers, FIs should take whatever practical and proportionate steps that are available to establish whether the document offered is genuine, or has been reported as lost or stolen. This may include:<br><br>(a) searching publicly available information,<br>(b) approaching relevant authorities (such as the Immigration Department through its hotline); or<br>(c) requesting corroboratory evidence from the customer. Where suspicion cannot be eliminated, the document should not be accepted and consideration should be given to making a report to the authorities. |
| 4.10.4 | 7 | **Use of an independent and appropriate person to certify identification documents** |
| | 7.1 | Use of an independent[66] and appropriate person to certify verification of identification documents 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. |
| | 7.2 | The following is a list of non-exhaustive examples of appropriate persons to certify verification of identification documents:<br><br>(a) an intermediary specified in section 18(3) of Schedule 2; |

[66] In general, it is not sufficient for the copy documents to be self-certified by the customer. However, an FI may accept the copy documents certified by a professional person within a legal person customer if that professional person is subject to the professional conduct requirements of a relevant professional body, and has certified the copy documents in his or her professional capacity.

| | | |
|---|---|---|
| | | (b) a member of the judiciary in an equivalent jurisdiction;<br>(c) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity;<br>(d) a Justice of the Peace; and<br>(e) other professional person[67] such as certified public accountant, lawyer, notary public and chartered secretary[68]. |
| | 7.3 | The certifier should sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it. The certifier should state that it is a true copy of the original (or words to similar effect). |
| | 7.4 | FIs remain liable for failure to carry out prescribed CDD and therefore should 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.<br><br>In any circumstances where an FI is unsure of the authenticity of certified documents, or that the documents relate to the customer, FIs should take additional measures to mitigate the ML/TF risk. |
| 5.2 | 8 | **Examples of trigger events upon which existing records of customers should be reviewed** |
| | | Examples of trigger events include:<br><br>(a) when a significant transaction[69] is to take place; |

67 An FI may accept other appropriate professional person as certifier. The FI should have due consideration to paragraph 7.4 of Appendix A in similar manner to other types of appropriate certifiers being used.

68 A chartered secretary refers to a person who is a current full member of the Institute of Chartered Secretaries and Administrators or its designated divisions.

69 The word “significant” is not necessarily linked to monetary value. It may include transactions that are unusual or not in line with the FI’s knowledge of the customer.

| | | |
|---|---|---|
| | | (b) when a material change occurs in the way the customer's account is operated[70];<br>(c) when the FI's customer documentation standards change substantially; or<br>(d) when the FI is aware that it lacks sufficient information about the customer concerned. |

70 Reference should also be made to section 6 of Schedule 2 "Provisions relating to Pre-Existing Customers".

# APPENDIX B

CONFIDENTIAL 機密

Joint Financial Intelligence Unit

G.P.O. Box No. 6555, General Post Office,
Hong Kong

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

**Date: 2012-XX-XX**

Money Laundering Reporting Officer,
XXXXXXX.

**Fax No. : XXXX XXXX**

Dear Sir/Madam,

**Suspicious Transaction Report ("STR")**

| **JFIU No.** | **Your Reference** | **Date Received** |
|---|---|---|
| XX | XX | XX |

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

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

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

Yours faithfully,

(XXXXX)
*for* Head, Joint Financial Intelligence Unit

**PERSONAL DATA**

Joint Financial Intelligence Unit

G.P.O. Box No. 6555, General Post Office,
Hong Kong
**Tel : 2866 3366   Fax : 2529 4013**
**Email : jfiu@police.gov.hk**

Our Ref. :
Your Ref :

2012-XX-XX

Money Laundering Reporting Officer,
XXXXXX
Fax No. : XXXX XXXX

Dear Sir/Madam,

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

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

| JFIU No. | Your Reference | Dated |
|---|---|---|
| XX | XX | XX |

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

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

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

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

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

Yours faithfully,

( XXXXXXX )
Superintendent of Police
Head, Joint Financial Intelligence Unit

c.c. OC Case

**Annex A**

| S/N | Account holder | Account Number |
| --- | --- | --- |
| 1. | | |

# GLOSSARY OF KEY TERMS AND ABBREVIATIONS

| Terms / abbreviations | Meaning |
|---|---|
| AMLO | Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) |
| AML/CFT | Anti-money laundering and counter financing of terrorism |
| CDD | Customer due diligence |
| CO | Compliance officer |
| DTROP | Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) |
| FATF | Financial Action Task Force |
| FI(s) | Financial institution(s) |
| JFIU | Joint Financial Intelligence Unit |
| MLRO | Money laundering reporting officer |
| ML/TF | Money laundering and terrorist financing |
| OSCO | Organized and Serious Crimes Ordinance (Cap. 455) |
| PEP(s) | Politically exposed person(s) |
| Proliferation financing or PF | Financing of proliferation of weapons of mass destruction |
| RA(s) | Relevant authority (authorities) |
| RBA | Risk-based approach |
| Schedule 2 | Schedule 2 to the AMLO |

| | |
|---|---|
| Senior management | Senior management means directors (or board) and senior managers (or equivalent) of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business. This may include a firm's Chief Executive Officer, Managing Director, Responsible Officer, Manager-In-Charge of Core Function(s) or other senior operating management personnel (as the case may be). |
| SFO | Securities and Futures Ordinance (Cap. 571) |
| STR(s) | Suspicious transaction report(s); also referred to as reports or disclosures |
| 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) |