Guideline on Anti-Money Laundering and Counter-Financing of Terrorism

(For Authorized Institutions)

~~Revised October 2018~~Consultation January 2023

CONTENTS

Page

Chapter 1 Overview 1

Chapter 2 Risk-based approach 8

Chapter 3 AML/CFT Systems 12

Chapter 4 Customer due diligence 17

Chapter 5 Ongoing monitoring 52

Chapter 6 Terrorist financing, financial sanctions and proliferation financing 55

Chapter 7 Suspicious transaction reports and law enforcement requests 60

Chapter 8 Record-keeping 67

Chapter 9 Staff training 70

Chapter 10 Wire transfers 73

Chapter 11 Correspondent banking and other similar relationships 78

Chapter 12 Private banking 84

Glossary of key terms and abbreviations 87

Chapter 1 – OVERVIEW		
Introduction		
	1.1	This Guideline is published under section 7 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) and section 7(3) of the Banking Ordinance (BO).
	1.2	Terms and abbreviations used in this Guideline should be interpreted by reference to the definitions set out in the Glossary part of this Guideline. Where applicable, interpretation of other words or phrases should follow those set out in the AMLO or the BO.
	1.3	This Guideline is issued by the Hong Kong Monetary Authority (HKMA) 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 Authorized Institutions (AIs), including Registered Institutions (RIs) [1], should meet in order to comply with the statutory requirements under the AMLO and the BO. Compliance with this Guideline is enforced through the AMLO and the BO. AIs which fail to comply with this Guideline may be subject to disciplinary or other actions under the AMLO and/or the BO for non-compliance with the relevant requirements.
	1.4	This Guideline is intended for use by AIs and their officers and staff. This Guideline also: (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 (b) provides practical guidance to assist AIs 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.
	1.5	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] In addition to ~~comply~~complying with this Guideline, RIs and associated entities that are AIs are required to have regard to ~~paragraph 4.1.6 of~~ the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations) issued by the Securities and Futures Commission ~~(SFC Guideline)~~ for ~~the definition of customer for~~requirements applicable to the securities, futures and leveraged foreign exchange businesses~~, as well as paragraphs 7.13 and 7.14 of the SFC Guideline in identifying~~ (e.g. definition of customer, provisions on cross-border correspondent relationships, illustrative indicators of suspicious transactions ~~for~~ and activities in the securities~~, futures and leveraged foreign exchange businesses.~~ sector, etc.)

	1.6	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 AIs 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. AIs should therefore use this Guideline as a basis to develop measures appropriate to their structure and business activities.
s.7, AMLO	1.7	This Guideline also provides guidance in relation to the operation of the provisions of Schedule 2 to the AMLO (Schedule 2). This will assist AIs to meet their legal and regulatory obligations when tailored by AIs to their particular business risk profile. 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 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 HKMA must have regard to any relevant provision in this Guideline.
	1.8	A failure to comply with any provision of this Guideline may reflect adversely on whether an AI continues to comply with the authorization criteria set out in the Seventh Schedule to the BO, particularly paragraph 10 of which requires an AI to maintain on and after authorization adequate accounting systems and systems of control. The HKMA is empowered to exercise various provisions under the BO in case of non-compliance with the requirements set out in this Guideline.
The nature of money laundering and terrorist financing		
s.1, Sch. 1, AMLO	1.9	The term "money laundering" (ML) 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: (a) that is the proceeds obtained from the commission of an indictable offence under the laws of Hong Kong, or of any conduct which if it had occurred in Hong Kong would constitute an indictable offence under the laws of Hong Kong; or (b) that in whole or in part, directly or indirectly, represents such proceeds,

		not to appear to be or so represent such proceeds.
	1.10	There are three common stages in the laundering of money, and they frequently involve numerous transactions. An AI should be alert to any such sign for potential criminal activities. These stages are: (a) Placement - the physical disposal of cash proceeds derived from illegal activities; (b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and (c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.
s.1, Sch. 1, AMLO	1.11	The term "terrorist financing" (TF) is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means: (a) the provision or collection, by any means, directly or indirectly, of any property – (i) with the intention that the property be used; or (ii) knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used); (b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or (c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.
	1.12	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		

	1.13	The Financial Action Task Force (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 latest FATF Recommendations[2] 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.
	1.14	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 AIs and their officers and staff fully understand their respective responsibilities under the different legislation.
AMLO		
s.23, Sch. 2	1.15	The AMLO imposes requirements relating to customer due diligence (CDD) and record-keeping on AIs and provides the HKMA with the powers to supervise compliance with these requirements and other requirements under the AMLO. In addition, section 23 of Schedule 2 requires AIs 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.

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

s.5, AMLO	1.16	The AMLO makes it a criminal offence if an AI (1) knowingly; or (2) with the intent to defraud the HKMA, contravenes a specified provision of the AMLO. The "specified provisions" are listed in section 5(11) of the AMLO. If the AI 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 AI contravenes a specified provision with the intent to defraud the HKMA, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.
s.5, AMLO	1.17	The AMLO also makes it a criminal offence if a person who is an employee of an AI or is employed to work for an AI or is concerned in the management of an AI (1) knowingly; or (2) with the intent to defraud the AI or the HKMA, causes or permits the AI to contravene a specified provision in the AMLO. If the person who is an employee of an AI or is employed to work for an AI or is concerned in the management of an AI 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 AI or the HKMA, he is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.
s.21, AMLO	1.18	The HKMA may take disciplinary actions against AIs for any contravention of a specified provision in the AMLO. The disciplinary actions that can be taken include publicly reprimanding the AI; ordering the AI to take any action for the purpose of remedying the contravention; and ordering the AI 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 AI as a result of the contravention.
<u>DTROP</u>		
	1.19	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>		
	1.20	The OSCO, among other things: (a) gives officers of the Hong Kong Police Force and the Customs and Excise Department powers to investigate organised crime and triad activities; (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;

		(c) creates an offence of ML in relation to the proceeds of indictable offences; and (d) enables the Courts, under appropriate circumstances, to receive information about an offender and an offence in order to determine whether the imposition of a greater sentence is appropriate where the offence amounts to an organised crime/triad related offence or other serious offences.
UNATMO		
	1.21	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	1.22	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	1.23	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	1.24	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	1.25	"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.
UNSO		

	1.26	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.
WMD(CPS)O		
s.4, WMD(CPS)O	1.27	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 – RISK-BASED APPROACH		
Introduction		
	2.1	The risk-based approach (RBA) is central to the effective implementation of an AML/CFT regime. An RBA to AML/CFT means that jurisdictions, competent authorities, and AIs are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate with those risks in order to manage and mitigate them effectively. RBA allows an AI to allocate its resources more effectively and apply preventive measures that are commensurate with the nature and level of risks, in order to focus its AML/CFT efforts in the most effective way. Therefore, an AI should adopt an RBA in the design and implementation of its AML/CFT policies, procedures and controls (hereafter collectively referred to as "AML/CFT Systems") with a view to managing and mitigating ML/TF risks.
Institutional ML/TF risk assessment		
	2.2	The institutional ML/TF risk assessment forms the basis of the RBA, enabling an AI to understand how and to what extent it is vulnerable to ML/TF. The AI should conduct an institutional ML/TF risk assessment to identify, assess and understand its ML/TF risks in relation to: (a) its customers; (b) the countries or jurisdictions its customers are from or in; (c) the countries or jurisdictions the AI has operations in; and (d) the products, services, transactions and delivery channels of the AI.
	2.3	The appropriate steps to conduct the institutional ML/TF risk assessment should include: (a) documenting the risk assessment process which includes the identification and assessment of relevant risks supported by qualitative and quantitative analysis, and information obtained from relevant internal and external sources; (b) considering all the relevant risk factors before determining what the level of overall risk is, and the appropriate level and type of mitigation to be applied; (c) obtaining the approval of senior management on the risk assessment results; (d) having a process by which the risk assessment is kept up-to-date; and (e) having appropriate mechanisms to provide the risk assessment to the HKMA when required to do so.

	2.4	In conducting the institutional ML/TF risk assessment, an AI should cover a range of factors, including: (a) customer risk factors, for example: (i) its target market and customer segments; (ii) the number and proportion of customers identified as high risk; (b) country risk factors, for example: (i) the countries or jurisdictions it is exposed to, either through its own activities or the activities of customers, especially countries or jurisdictions identified by credible sources, with relatively higher level of corruption or organised crime, and/or not having effective AML/CFT regimes; (c) product, service, transaction or delivery channel risk factors, for example: (i) the nature, scale, diversity and complexity of its business; (ii) the characteristics of products and services offered, and the extent to which they are vulnerable to ML/TF abuse; (iii) the volume and size of its transactions; (iv) the delivery channels, including the extent to which the AI deals directly with the customer, the extent to which the AI relies on (or is allowed to rely on) third party to conduct CDD, the extent to which the AI uses technology, and the extent to which these channels are vulnerable to ML/TF abuse; (d) other risk factors, for example: (i) the nature, scale and quality of available ML/TF risk management resources, including appropriately qualified staff with access to ongoing AML/CFT training and development; (ii) compliance and regulatory findings; (iii) results of internal or external audits.
	2.5	The scale and scope of the institutional ML/TF risk assessment should be commensurate with the nature, size and complexity of the AI's business.
	2.6	The institutional ML/TF risk assessment should consider any higher risks identified in other relevant risk assessments which may be issued from time to time, such as Hong Kong's jurisdiction-wide ML/TF risk assessment and any higher risks notified to the AIs by the HKMA.
	2.7	A locally-incorporated AI with branches or subsidiaries, including those located outside Hong Kong, should perform a group-wide ML/TF risk assessment.

	2.8	For the purpose of paragraphs 2.2 and 2.7, if an AI is a part of a financial group and a group-wide or regional ML/TF risk assessment has been conducted, it may make reference to or rely on those assessments provided that the assessments adequately reflect ML/TF risks posed to the AI in the local context.
	2.9	To keep the institutional ML/TF risk assessment up-to-date, an AI should conduct its assessment every two years and upon trigger events which are material to the AI's business and risk exposure.
New products, new business practices and use of new technologies		
	2.10	An AI 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; and (b) the use of new or developing technologies for both new and pre-existing products.
	2.11	An AI should undertake the risk assessment prior to the launch of the new products, new business practices, or the use of new or developing technologies, and should take appropriate measures to manage and mitigate the risks identified.
Customer risk assessment		
	2.12	An AI should assess the ML/TF risks associated with a proposed business relationship, which is usually referred to as a customer risk assessment. The assessment conducted at the initial stage of the CDD process would determine the extent of CDD measures to be applied[3]. This means that the amount and type of information obtained, and the extent to which this information is verified, should be increased where the ML/TF risks associated with the business relationship are higher. It may also be simplified where the ML/TF risks associated with the business relationship is lower. The risk assessment conducted will also assist the AI to differentiate between the risks of individual customers and business relationships, as well as apply appropriate and proportionate CDD and risk mitigating measures[4].
	2.13	Based on a holistic view of the information obtained in the context of the application of CDD measures, an AI should be able to finalise the customer risk assessment[5], which determines the level and type of ongoing monitoring (including ongoing CDD and

[3] For the avoidance of doubt, except for certain situations specified in Chapter 4, an AI should always apply all the CDD measures set out in paragraph 4.1.3 and conduct ongoing monitoring of its customers.

[4] An AI should adopt a balanced and common sense approach when conducting a customer risk assessment and applying CDD measures, which should not pose an unreasonable barrier to bona fide businesses and individuals accessing services offered by the AI.

[5] This is sometimes also called a "customer risk profile".

		transaction monitoring), and support the AI's decision whether to enter into, continue or terminate, the business relationship. As the customer risk profile will change over time, an AI should review and update the risk assessment of a customer from time to time, particularly during ongoing monitoring.
	2.14	Similar to other parts of the AML/CFT Systems, an AI should adopt an RBA in the design and implementation of its customer risk assessment framework, and the complexity of the framework should be commensurate with the nature and size of the AI's business, and should be designed based on the results of AI's institutional ML/TF risk assessment. In general, the customer risk assessment framework will include customer risk factors; country risk factors; and product, service, transaction or delivery channel risk factors[6].
s.20(1)(b)(ii), Sch. 2	2.15	An AI should keep records and relevant documents of its customer risk assessments so that it can demonstrate to the HKMA, among others: (a) how it assesses the customer's ML/TF risks; and (b) the extent of CDD measures and ongoing monitoring is appropriate based on that customer's ML/TF risks.

[6] Further guidance can be found in Chapter 4.

Chapter 3 – AML/CFT SYSTEMS		
AML/CFT Systems		
s.23, Sch. 2	3.1	An AI should 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, the AI should implement appropriate AML/CFT Systems following the RBA as stated in paragraph 2.1.
s.23(b), Sch. 2	3.2	An AI should: (a) have AML/CFT Systems, which are approved by senior management, to enable the AI to effectively manage and mitigate the risks that are relevant to the AI; (b) monitor the implementation of those AML/CFT Systems referred to in (a), and to enhance them if necessary; and (c) take enhanced measures to manage and mitigate the risks where higher risks are identified.
	3.3	The nature, scale and complexity of AML/CFT Systems may be simplified provided that: (a) an AI complies with the statutory requirements set out in the Schedule 2 of the AMLO and the requirements set out in paragraphs 2.2, 2.3 and 3.2; (b) the lower ML/TF risks which form the basis for doing so have been identified through an appropriate risk assessment (e.g. institutional ML/TF risk assessment); and (c) simplified AML/CFT Systems, which are approved by senior management, are subject to review from time to time. However, AML/CFT Systems are not permitted to be simplified whenever there is a suspicion of ML/TF.
	3.4	An AI should implement AML/CFT Systems having regard to the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses, and which should include: (a) compliance management arrangements; (b) an independent audit function; (c) employee screening procedures; and (d) an ongoing employee training programme (see Chapter 9).
<u>Compliance management arrangements</u>		
	3.5	An AI should have appropriate compliance management arrangements that facilitate the AI 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 AI's senior management, and appointment of a Compliance Officer (CO) and a Money Laundering Reporting Officer (MLRO)[7].
Senior management oversight		
	3.6	Effective ML/TF risk management requires adequate governance arrangements. The board of directors or its delegated committee (where applicable), and senior management of an AI should have a clear understanding of its ML/TF risks and ensure that the risks are adequately managed. Management information regarding ML/TF risks and the AML/CFT Systems should be communicated to them in a timely, complete, understandable and accurate manner so that they are equipped to make informed decisions.
	3.7	The senior management of an AI is responsible for implementing effective AML/CFT Systems that can adequately manage the ML/TF risks identified. In particular, the senior management should appoint a CO at the management level to have the overall responsibility for the establishment and maintenance of the AI's AML/CFT Systems; and a senior staff as the MLRO to act as the central reference point for suspicious transaction reporting.

[7] Depending on the size of an AI, the functions of CO and MLRO may be performed by the same person.

	3.8	In order that the CO and MLRO can discharge their responsibilities effectively, senior management should, as far as practicable, ensure that the CO and MLRO are: (a) appropriately qualified with sufficient AML/CFT knowledge; (b) subject to constraint of size of the AI, independent of all operational and business functions; (c) normally based in Hong Kong; (d) of a sufficient level of seniority and authority within the AI; (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 risks of ML/TF; (f) fully conversant with the AI's statutory and regulatory requirements and the ML/TF risks arising from the AI's business; (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 the HKMA); and (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).
CO and MLRO		
	3.9	The principal function of the CO is to act as the focal point within an AI 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: (a) developing and/or continuously reviewing the AI's AML/CFT Systems, including any group-wide AML/CFT Systems in the case of a Hong Kong-incorporated AI, to ensure they remain up-to-date, meet current statutory and regulatory requirements, and are effective in managing ML/TF risks arising from the AI's business; (b) overseeing all aspects of the AI's AML/CFT Systems which include monitoring effectiveness and enhancing the controls and procedures where necessary; (c) communicating key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies; and (d) ensuring AML/CFT staff training is adequate, appropriate and effective.

	3.10	An AI should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the Joint Financial Intelligence Unit (JFIU) and law enforcement agencies. The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions of the MLRO should include having oversight of: (a) review of internal disclosures and exception reports and, in light of all available relevant information, determining whether or not it is necessary to make a report to the JFIU; (b) maintenance of all records related to such internal reviews; and (c) provision of guidance on how to avoid tipping off.
Independent Audit function		
	3.11	An AI should establish an independent audit function[8] which should have a direct line of communication to the senior management of the AI. The function should have sufficient expertise and resources to enable it to carry out its responsibilities, including independent reviews of the AI's AML/CFT Systems.
	3.12	The audit function should regularly review the AML/CFT Systems to ensure effectiveness. The review should include, but not be limited to: (a) adequacy of the AI's AML/CFT Systems, ML/TF risk assessment framework and application of RBA; (b) effectiveness of suspicious transaction reporting systems; (c) effectiveness of the compliance function; and (d) level of awareness of staff having AML/CFT responsibilities.
	3.13	The frequency and extent of the review should be commensurate with the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses. Where appropriate, the AI should also seek a review from external parties.
Employee screening		
	3.14	An AI should have adequate and appropriate screening procedures in order to ensure high standards when hiring employees[9].
Group-wide AML/CFT Systems		

[8] Reference should be made to relevant parts of the Supervisory Policy Manual published by the HKMA, particularly "IC-2 Internal Audit Function".

[9] Reference should be made to relevant parts of the Supervisory Policy Manual published by the HKMA, particularly "CG-6 Competence and ethical behavior".

	3.15	Subject to paragraphs 3.18 and 3.19, a Hong Kong-incorporated AI with overseas branches or subsidiary undertakings that carry on the same business as a financial institution (FI) as defined in the AMLO should implement group-wide AML/CFT Systems to apply the requirements set out in this Guideline[10] 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.
s.22(1), Sch. 2	3.16	In particular, a Hong Kong-incorporated AI 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.
	3.17	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 AI should also implement measures, through its group-wide AML/CFT Systems, for: (a) sharing information required for the purposes of CDD and ML/TF risk management; and (b) provision to the AI'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[11].
	3.18	If the AML/CFT requirements in the jurisdiction where the overseas branch or subsidiary undertaking of a Hong Kong-incorporated AI is located (host jurisdiction) differ from those relevant requirements referred to in paragraph 3.15, the AI should require that branch or subsidiary undertaking to apply the higher of the two sets of requirements, to the extent that host jurisdiction's laws and regulations permit.

[10] For the avoidance of doubt, these include, but not limited to, the requirements set out in paragraph 3.4.

[11] 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 subsidiary undertakings should receive such information from these group-level functions when relevant and appropriate to risk management.

s.22(2), Sch. 2	3.19	If the host jurisdiction's laws and regulations do not permit the branch or subsidiary undertaking of a Hong Kong-incorporated AI to apply the higher AML/CFT requirements, particularly the CDD and record-keeping requirements imposed under Parts 2 and 3 of Schedule 2, the AI should: (a) inform the HKMA of such failure; and (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.

Chapter 4 – CUSTOMER DUE DILIGENCE		
4.1 What CDD measures are		
s.19(3), Sch. 2	4.1.1	The AMLO defines what CDD measures are (see paragraph 4.1.3) and also prescribes the circumstances in which an AI should carry out CDD (see paragraph 4.2). This Chapter provides guidance in this regard. Wherever possible, this Guideline gives AIs a degree of discretion in how they comply with the AMLO and put in place procedures for this purpose. In addition, an AI 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	An AI should apply an RBA when conducting CDD measures and the extent of CDD measures should be commensurate with the ML/TF risks associated with a business relationship. Where the ML/TF risks are high, the AI should conduct enhanced due diligence (EDD) measures (see paragraph 4.9). In low risk situations, the AI may apply simplified due diligence (SDD) measures (see paragraph 4.8).
s.2(1), Sch. 2	4.1.3	The following are CDD measures applicable to an AI: (a) identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source (see paragraph 4.3); (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 AI is satisfied that it knows who the beneficial owner is, including, in the case of a legal person or trust [12], measures to enable the AI to understand the ownership and control structure of the legal person or trust (see paragraph 4.4); (c) obtain information on the purpose and intended nature of the business relationship (if any) established with the AI unless the purpose and intended nature are obvious (see paragraph 4.6); and (d) if a person purports to act on behalf of the customer: (i) identify the person and take reasonable measures to verify the person's identity using documents, data or information provided by a reliable and independent source; and (ii) verify the person's authority to act on behalf of the customer (see paragraph 4.5).

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

	4.1.4	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.
	4.1.5	In general, the term "customer" refers to the party, or parties, with whom a business relationship is established, or for whom a transaction is carried out by an AI. This generally excludes the third parties of a transaction. For example, an ordering AI in an outward wire transfer transaction does not regard the beneficiary (who has no other relationship with the AI) as its customer.
	4.1.6	Hong Kong is an international financial centre, and it is not uncommon for a customer relationship to be managed by an AI but the account of that customer to be booked outside Hong Kong. ~~Whether this~~ A major consideration in determining if a relationship ~~should be considered as~~is a business relationship as defined in the AMLO~~, a major consideration~~ is whether the relationship is managed in substance by the AI. If there is a business relationship, the AI should comply with relevant requirements set out in the AMLO and this Guideline in relation to that customer[13].
4.2 When CDD measures should be carried out		
s.3(1)&(1A), Sch. 2	4.2.1	An AI should carry out CDD measures in relation to a customer: (a) ~~at the outset of~~before establishing a business relationship with the customer; (b) before ~~performing any~~carrying out for the customer an occasional transaction[14]: (i) involving an amount equal to or ~~exceeding an aggregate value of~~above $120,000~~, whether carried out~~ or an equivalent amount in any other currency; ~~(i)~~ that is a ~~single operation or several operations that appear to the AI to be linked; or~~ (ii) ~~a~~ wire transfer involving an amount equal to or ~~exceeding an aggregate value of~~above $8,000~~,~~ or an equivalent amount in any other currency; or (iii) that is a virtual asset transfer[15] involving virtual assets that amount to no less than $8,000; whether the transaction is carried out in a single operation or in several operations that appear to the AI to be linked~~;~~. (c) when the AI suspects that the customer or the customer's account is involved in ML/TF[16]; or

[13] For the avoidance of doubt, a business relationship always exists whenever an account is booked in Hong Kong.

[14] Occasional transactions may include for example, wire transfers or virtual asset transfers, currency exchanges, purchase of cashier orders or gift cheques.

[15] Also see the requirements of section 13A of Schedule 2.

[16] This criterion applies irrespective of the $120,000 or $8,000 threshold applicable to occasional transactions set out in ~~paragraphs~~paragraph 4.2.1(b~~)(i) and 4.2.1(b)(ii) respectively.~~).

		(d) when the AI 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.
s.1, Sch. 2	4.2.2	"Business relationship" between a person and an AI is defined in the AMLO as a business, professional or commercial relationship: (a) that has an element of duration; or (b) that the AI, at the time the person first contacts it in the person's capacity as a potential customer of the AI, expects to have an element of duration.
s.1, Sch. 2	4.2.3	"Occasional transaction" is defined in the AMLO as a transaction between an AI and a customer who does not have a business relationship with the AI.
	4.2.4	An AI 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 or virtual asset transfers involving virtual assets) and $120,000 (for other types of transactions~~.~~). Where the AI become aware that these thresholds are met or exceeded, CDD measures should be carried out.
	4.2.5	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, an AI should consider these factors against the timeframe within which the transactions are conducted.
Third-party cash transactions		
	4.2.6	~~Where cash~~Cash transactions ~~are undertaken by an AI for non-account holders~~may be made by third parties other than the customer. Such transactions may represent an increased risk of ~~that AI, e.g.~~ML, especially when a large cash deposit that is ~~deposited into an existing account by a person whose name does not appear on the mandate of that account, care and vigilance are required. Where~~not consistent with the risk profile of the customer is made. When a cash transaction ~~involves~~involving an amount equal to or exceeding $120,000~~, or is otherwise unusual, the person~~ is undertaken by a person whose name does not appear on the mandate of an account, an AI should ~~be asked to produce positive evidence of~~ask for the person's identity~~,~~ document and retain a copy ~~should be retained on file~~to facilitate its ongoing monitoring.
4.3 Identification and verification of identity – customer		

s.2(1)(a), Sch. 2	4.3.1	An AI should identify the customer and verify the customer's identity by reference to documents, data or information provided by a reliable and independent source: (a) a governmental body; (b) the HKMA or any other relevant authority (RA); (c) an authority in a place outside Hong Kong that performs functions similar to those of the HKMA or any other RA; ~~or~~ (d) a digital identification system that is recognised by the HKMA (e.g. iAM Smart of Hong Kong); or ~~(d)~~(e) any other reliable and independent source that is recognised by the HKMA.
Customer that is a natural person[17]		
s.2(1)(a), Sch. 2	4.3.2	For a customer that is a natural person, an AI should identify the customer by obtaining at least the following identification information: (a) full name; (b) date of birth; (c) nationality; and (d) unique identification number (e.g. identity card number or passport number) and document type.
s.2(1)(a), Sch. 2	4.3.3	In verifying the identity of a customer that is a natural person, an AI should verify the name, date of birth, unique identification number and document type of the customer by reference to documents, data or information provided by a reliable and independent source, examples of which include: (a) Hong Kong identity card or other national identity card; (b) valid travel document (e.g. unexpired passport); or (c) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).
	4.3.4	The identification document obtained by an AI should contain a photograph of the customer. In exceptional circumstances where an AI is unable to obtain an identification document with a photograph, the AI may accept an identification document without a photograph if the associated risks have been properly assessed and mitigated.
	4.3.5	An AI should obtain the residential address information of a customer that is a natural person[18].

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

[18] For the avoidance of doubt, an AI may, under certain circumstances, require verification (on top of collection) of residential address from a customer for other purposes (e.g. group requirements, other local or overseas legal and

Customer that is a legal person[19]		
s.2(1)(a), Sch. 2	4.3.6	For a customer that is a legal person, an AI should identify the customer by obtaining at least the following identification information: (a) full name; (b) date of incorporation, establishment or registration; (c) place of incorporation, establishment or registration (including address of registered office); (d) unique identification number (e.g. incorporation number or business registration number) and document type; and (e) principal place of business (if different from the address of registered office).
s.2(1)(a), Sch. 2	4.3.7	In verifying the identity of a customer that is a legal person, an AI should normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the legal person by reference to documents, data or information provided by a reliable and independent source, examples of which include[20]: (a) certificate of incorporation; (b) record in an independent company registry; (c) certificate of incumbency; (d) certificate of good standing; (e) record of registration; (f) partnership agreement or deed; (g) constitutional document; or (h) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).
	4.3.8	For a customer that is a partnership or an unincorporated body, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to verify the identity of the customer as required in paragraph 4.3.7 provided that: (a) the customer is a well-known, reputable organisation; (b) the customer has a long history in its industry; and (c) there is substantial public information about the customer, its

regulatory requirements). In such circumstances, the AI should communicate clearly to the customer the reasons of requiring verification of address.

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

[20] In some instances, an AI 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.

		partners and controllers.
	4.3.9	In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, an AI should satisfy itself as to the legitimate purpose of the organisation, e.g. by requesting sight of the constitution.
Customer that is a trust or other similar legal arrangement[21]		
s.2(1)(a), Sch. 2	4.3.10	In respect of trusts, an AI should identify and verify the trust as a customer in accordance with the requirements set out in paragraphs 4.3.11 and 4.3.12. The AI should also regard the trustee[22] 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, the AI 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 a legal person, where applicable.
s.2(1)(a), Sch. 2	4.3.11	For a customer that is a trust or other similar legal arrangement, an AI should identify the customer by obtaining at least the following identification information: (a) name of the trust or legal arrangement; (b) date of establishment or settlement; (c) the jurisdiction whose laws govern the trust or legal arrangement; (d) unique identification number (if any) granted by any applicable official bodies and document type (e.g. tax identification number or registered charity or non-profit organisation number); and (e) address of registered office (if applicable).
s.2(1)(a), Sch. 2	4.3.12	In verifying the identity of a customer that is a trust or other similar legal arrangement, an AI 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 by reference to documents, data or information provided by a reliable and independent source, examples of which include: (a) trust deed or similar instrument[23];

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

[22] For the avoidance of doubt, the AMLO defines a beneficial owner in relation to a trust to include trustee (see paragraph 4.4.10). Depending on the nature of the roles and activities which the trustee is authorised to conduct (e.g. if a trustee is also regarded as the customer or the PPTA), an AI should apply the higher of the relevant requirements set out in this Guideline for the purpose of identification and verification of the identity of the trustee.

[23] Under exceptional circumstance, the AI may choose to retain a redacted copy.

		(b) record of an appropriate register[24] in the relevant country of establishment; (c) written confirmation from a trustee acting in a professional capacity[25]; (d) written confirmation from a lawyer who has reviewed the relevant instrument; or (e) written confirmation from a trust company which is within the same financial group as the AI, if the trust concerned is managed by that trust company.
Reliability of documents, data or information		
	4.3.13	In verifying the identity of a customer, an AI needs not establish accuracy of every piece of identification information collected in paragraphs 4.3.2, 4.3.6 and 4.3.11.
	4.3.14	An AI should ensure that documents, data or information obtained for the purpose of verifying the identity of a customer as required in paragraphs 4.3.3, 4.3.7 and 4.3.12 is current at the time they are provided to or obtained by the AI.
	4.3.15	When using documents for verification, an AI should be aware that some types of documents are more easily forged than others, or can be reported as lost or stolen. Therefore, the AI should consider applying anti-fraud procedures that are commensurate with the risk profile of the person being verified.
	4.3.16	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 AI is physically present during the CDD process, the AI 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 AI should take appropriate measures to ensure the reliability of identification documents obtained.
	4.3.17	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 AI to be reasonably satisfied that the documents, data or information in fact provide evidence of the customer's identity.

[24] In determining whether a register is appropriate, the AI 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.

[25] "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).

Connected parties		
	4.3.18	Where a customer is a legal person, a trust or other similar legal arrangement, an AI should identify all the connected parties[26] of the customer by obtaining their names.
	4.3.19	A connected party of a customer that is a legal person, a trust or other similar legal arrangement: (a) in relation to a corporation, means a director of the customer; (b) in relation to a partnership, means a partner of the customer; (c) in relation to a trust or other similar legal arrangement, means a trustee (or equivalent) of the customer; and (d) in other cases not falling within subsection (a), (b) or (c), means a natural person holding a senior management position or having executive authority in the customer.
4.4 Identification and verification of identity – beneficial owner		
s.2(1)(b), Sch. 2	4.4.1	~~A beneficial~~Beneficial owner ~~is normally a~~refers to the natural person(s) who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. An AI should identify any beneficial owner in relation to a customer, and take reasonable measures to verify the beneficial owner's identity so that the AI is satisfied that it knows who the beneficial owner is.
	4.4.2	When identifying a beneficial owner, an AI should endeavour to obtain the same identification information as at paragraph 4.3.2 as far as possible.
	4.4.~~2~~3	The verification requirements for a customer and a beneficial owner are different under the AMLO. In determining what constitutes reasonable measures to verify the identity of a beneficial owner of a customer, an AI should consider and give due regard to the ML/TF risks posed by the customer and the business relationship. It is therefore up to the AI to consider whether it is appropriate to make use of the records of a beneficial owner available in the public domain[27], request its customer to provide documents or information in relation to the beneficial owner's identity obtained from a reliable and independent source, or corroborate the customer's undertaking or declaration with publicly available information. In exceptionally low ML/TF risk situation (e.g. charitable trust), it may be reasonable for the AI to

[26] 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 AI has to identify and verify the identity of that person with reference to relevant requirements set out in this Guideline.

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

		confirm the beneficial owner's identity based on the information provided by the customer (including trustee(s) whose identities have been verified). This could include information provided by the customer as to the beneficial owner's identity, and confirmation that they are known to the customer.
	4.4.~~3~~4	~~Where a natural person is identified as a beneficial owner, the AI should endeavour to obtain the same identification information as at paragraph 4.3.2 as far as possible.~~ If the ownership structure of a customer involves different types of legal persons or legal arrangements[28], in determining who the beneficial owner is, an AI should pay attention to who has ultimate ownership or control over the customer, or who constitutes the controlling mind and management of the customer.
Beneficial owner in relation to a natural person		
	4.4.~~4~~5	In respect of a customer that is a natural person, the customer is the beneficial owner, unless the characteristics of the transactions or other circumstances indicate otherwise. Therefore, there is no requirement on an AI to make proactive searches for beneficial owners of the customer in such a case, but the AI should make appropriate enquiries where there are indications that the customer is not acting on his own behalf.
Beneficial owner in relation to a legal person		
s.1, Sch. 2	4.4.~~5~~6	The AMLO defines beneficial owner in relation to a corporation as: (a) an individual who (i) owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation; (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or (iii) exercises ultimate control over the management of the corporation; or (b) if the corporation is acting on behalf of another person, means the other person.
s.1, Sch. 2	4.4.~~6~~7	The AMLO defines beneficial owner, in relation to a partnership as: (a) an individual who (i) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership; (ii) is, directly or indirectly, entitled to exercise or control the

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

		exercise of more than 25% of the voting rights in the partnership; or (iii) exercises ultimate control over the management of the partnership; or (b) if the partnership is acting on behalf of another person, means the other person.
s.1, Sch. 2	4.4.~~7~~8	In relation to an unincorporated body other than a partnership, beneficial owner: (a) means an individual who ultimately owns or controls the unincorporated body; or (b) if the unincorporated body is acting on behalf of another person, means the other person.
s.2(1)(b), Sch. 2	4.4.~~8~~9	For a customer that is a legal person, an AI 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 4.4.~~5~~6 to 4.4.~~7~~7),~~8~~8), the AI should identify the relevant natural persons who hold the position of senior managing official, and take reasonable measures to verify their identities.
	~~4.4.9~~	~~While an AI 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 AI may obtain an undertaking or declaration[29] 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 AI should take reasonable measures to verify the identity of the beneficial owner (e.g. corroborating the undertaking or declaration with publicly available information).~~
	~~4.4.10~~	~~If the ownership structure of a customer involves different types of legal persons or legal arrangements, in determining who the beneficial owner is, an AI should pay attention to who has ultimate ownership or control over the customer, or who constitutes the controlling mind and management of the customer.~~
Beneficial owner in relation to a trust or other similar legal arrangement		
s.1, Sch. 2	4.4.~~11~~10	The AMLO defines the beneficial owner, in relation to a trust as:

~~[29] 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 of Hong Kong). An AI 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 AI may obtain the record directly from its customers.~~

		(a) ~~an individual who is~~a beneficiary or a class of beneficiaries of the trust entitled to a vested interest in~~ more than 25% of the capital of~~ the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not; (b) the settlor of the trust; (c) the trustee of the trust; ~~(c)~~(d) a protector or enforcer of the trust; or ~~(d)~~(e) an individual who has ultimate control over the trust.
s.2(1)(b), Sch. 2	4.4.~~12~~11	~~Similar to~~For a ~~corporation,~~customer that is a trust~~ or other similar legal arrangement can also be part of an intermediate layer in an ownership structure, and should be dealt with in similar manner to a corporation being part of an intermediate layer. For trusts~~, an AI should identify the settlor, the trustee, 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~~a customer that is another similar legal ~~arrangements~~arrangement, an AI should identify any natural person in equivalent or similar positions to a beneficial owner of a trust as stated above and take reasonable measures to verify the identity of such person.~~ If a trust or other similar legal arrangement is involved in a business relationship and an AI does not regard the trustee (or equivalent in other similar legal arrangement) as its customer pursuant to paragraph 4.3.10 (e.g. when a trust appears as part of an intermediate layer), the AI should also identify the trustee and take reasonable measures to verify the identity of the trustee so that the AI is satisfied that it knows who the trustee is.~~
	4.4.~~13~~12	For a beneficiary of a trust designated by characteristics or by class, an AI should obtain sufficient information [30] concerning the beneficiary to satisfy the AI that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights.
Ownership and control structure		
s.2(1)(b), Sch. 2	4.4.~~14~~13	Where a customer is not a natural person, an AI should understand its ownership and control structure, including identification of any intermediate layers (e.g. by reviewing an ownership chart of the customer). The objective is to follow the chain of ownerships to the beneficial owners of the customer.
	4.4.~~15~~14	Where a customer has a complex ownership or control structure, an AI should obtain sufficient information for the AI to satisfy itself

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

		that there is a legitimate reason behind the particular structure employed.
Bearer shares[31]		
	4.4.~~16~~15	Bearer shares refer to negotiable instruments that accord ownership in a legal person to the person who possesses the physical bearer share certificate, and any other similar instruments without traceability. Therefore it is more difficult to establish the beneficial ownership of a company with bearer shares. An AI should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the AI is notified whenever there is a change of beneficial owner of such shares.
	4.4.~~17~~16	Where bearer shares have been deposited with an authorised/registered custodian, an AI 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 AI's ongoing periodic review, it should obtain evidence to confirm the authorised/registered custodian of the bearer shares.
	4.4.~~18~~17	Where the shares are not deposited with an authorised/registered custodian, an AI should obtain declarations prior to account opening and annually thereafter from each beneficial owner of such shares. The AI should also require the customer to notify it immediately of any changes in the ownership of the shares.
Nominee shareholders		
	4.4.~~19~~18	For a customer identified to have nominee shareholders in its ownership structure, an AI 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.
4.5 Identification and verification of identity – person purporting to act on behalf of the customer		
	4.5.1	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 AI 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

[31] The same controls should be applied to bearer share warrants, which refer to negotiable instruments that accord entitlement to ownership in a legal person who possesses the physical bearer share warrant certificate, and any other similar warrants or instruments without traceability.

		to conduct, as well as the ML/TF risks associated with these roles and activities. An AI should implement clear policies and procedures for determining who is considered to be a PPTA.
s.2(1)(d), Sch. 2	4.5.2	If a person is a PPTA, an AI should: (a) identify the person and take reasonable measures to verify the person's identity on the basis of documents, data or information provided by- (i) a governmental body; (ii) the HKMA or any other RA; (iii) an authority in a place outside Hong Kong that performs functions similar to those of the HKMA or any other RA; or (iv) any other reliable and independent source that is recognised by the HKMA; and (b) verify the person's authority to act on behalf of the customer.
s.2(1)(d)(i), Sch. 2	4.5.3	An AI should identify and verify the identity of the PPTA in line with the identification and verification requirements for a customer that is a natural person or a legal person, where applicable.
s.2(1)(d)(ii), Sch. 2	4.5.4	An AI should verify the authority of each PPTA by appropriate documentary evidence (e.g. board resolution or similar written authorisation).
4.6 Purpose and intended nature of business relationship		
s.2(1)(c), Sch. 2	4.6.1	An AI should understand the purpose and intended nature of the business relationship. In some instances, this will be self-evident, but in many cases, the AI may have to obtain information in this regard. The information obtained by the AI to understand the purpose and intended nature should be commensurate with the risk profile of the customer and the nature of the business relationship. In addition, where a customer is not a natural person, an AI should also understand the nature of the customer's business.
4.7 Timing of verification		
s.3(2) & (3), Sch. 2	4.7.1	An AI 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, an AI 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; (b) it is necessary not to interrupt the normal conduct of business with the customer; and

		(c) verification is completed as soon as reasonably practicable.
	4.7.2	Examples of situations where it may be necessary not to interrupt the normal conduct of business include: (a) securities transactions – in the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed; and (b) life insurance business – in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policy holder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.
	4.7.3	If an AI 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: (a) establishing a reasonable timeframe for the completion of the identity verification measures and the follow-up actions if exceeding the timeframe (e.g. to suspend or terminate the business relationship concerned); (b) placing appropriate limits on the number, types and/or amount of transactions that can be performed; (c) monitoring of large and complex transactions being carried out outside the expected norms for that type of relationship; (d) keeping senior management periodically informed of any pending completion cases; and (e) ensuring that funds are not paid out to any third party. Exceptions may be made to allow payments to third parties subject to the following conditions: (i) there is no suspicion of ML/TF; (ii) the risk of ML/TF is assessed to be low; (iii) the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction; and (iv) the names of recipients do not match with watch lists such as those for terrorist suspects and politically exposed persons (PEPs).

s.3(3) & (4)(b), Sch. 2	4.7.4	Verification of identity should be completed by an AI within a reasonable timeframe, which generally refers to the following: (a) the AI completing such verification no later than 30 working days after the establishment of business relationship; (b) the AI 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 (c) the AI 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 AI's risk management policies and procedures, the AI 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 AI 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 due diligence (SDD)		
General		
	4.8.1	In general, an AI should carry out all four CDD measures set out in paragraph 4.1.3 before establishing any business relationship, before carrying out a specified occasional transaction, and continuously monitor its business relationship (i.e. ongoing CDD and transaction monitoring). As stated in Chapter 2, the extent of four CDD measures and ongoing monitoring should be determined using an RBA.
	4.8.2	An AI may apply SDD measures in relation to a business relationship or transaction if it determines that, taking into account its risk assessment, the business relationship or transaction presents a low ML/TF risk.
	4.8.3	SDD measures should not be applied or continue to be applied, where: (a) the AI's risk assessment changes and it no longer considers that there is a low degree of ML/TF risk; (b) where the AI suspects ML or TF; or (c) where there are doubts about the veracity or accuracy of documents or information previously obtained for the purposes

		of identification or verification.
	4.8.4	The assessment of low risks should be supported by an adequate analysis of ML/TF risks by the AI.
	4.8.5	The SDD measures applied should be commensurate with the nature and level of ML/TF risk, based on the lower ML/TF risk factors identified by the AI.
s.5(1), Sch. 2	4.8.6	When an AI applies SDD measures, it is still required to continuously monitor its business relationship (i.e. ongoing CDD and transaction monitoring) in accordance with section 5 of Schedule 2 and Chapter 5.
	4.8.7	Examples of potentially lower risk factors[32] include: (a) customer risk factors: (i) a government entity or a public body[33] in Hong Kong or in an equivalent jurisdiction; (ii) a corporation listed on a stock exchange and subject to disclosure requirements (e.g. either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership; (iii) an FI as defined in the AMLO, or other FI incorporated or established in an equivalent jurisdiction and is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; or (iv) a collective investment scheme authorised for offering to the public in Hong Kong or in an equivalent jurisdiction. (b) product, service, transaction or delivery channel risk factors: (i) 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; (ii) 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

[32] In assessing ML/TF risk of a business relationship, an AI should consider a range of factors in a holistic approach.

[33] Public body, as defined in Schedule 2, includes: (a) any executive, legislative, municipal or urban council; (b) any Government department or undertaking; (c) any local or public authority or undertaking; (d) any board, commission, committee or other body, whether paid or unpaid, appointed by the Chief Executive or the Government; and (e) any board, commission, committee or other body that has power to act in a public capacity under or for the purposes of any enactment.

		(iii) a life insurance policy in respect of which: (A) an annual premium of no more than $8,000 or an equivalent amount in any other currency is payable; or (B) a single premium of no more than $20,000 or an equivalent amount in any other currency is payable. (c) country risk factors: (i) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems; or (ii) countries or jurisdictions identified by credible sources as having a lower level of corruption or other criminal activity.
	4.8.8	Examples of possible SDD measures include: (a) accepting other documents, data or information (e.g. proof of FI's license, listed status or authorization status etc.), other than examples provided in paragraphs 4.3.7 and 4.3.12, for a customer falling within any category specified in paragraph 4.8.7(a); (b) adopting simplified customer due diligence in relation to beneficial owners as specified in paragraph 4.8.9 to 4.8.20; (c) reducing the frequency of updates of customer identification information; (d) reducing the degree of ongoing monitoring and scrutiny of transactions based on a reasonable monetary threshold; or (e) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and intended nature from the type of transactions or business relationship established.
<u>Simplified customer due diligence in relation to beneficial owners</u>		
General		
s.4, Sch. 2	4.8.9	An AI may choose not to identify and take reasonable measures to verify the beneficial owner in relation to: (a) a customer that is listed in paragraph 4.8.10; (b) a transaction conducted to a customer relates to a product listed in paragraph 4.8.17; or (c) a customer who is a solicitor or a firm of solicitor, and meeting the criteria set out in paragraph 4.8.19.
Specific customers		
s.4(3), Sch. 2	4.8.10	An AI may choose not to identify and take reasonable measures to verify the beneficial owner of a customer, if the customer is –

		(a) an FI as defined in the AMLO; (b) an institution that- (i) is incorporated or established in an equivalent jurisdiction; (ii) carries on a business similar to that carried on by an FI as defined in the AMLO; (iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and (iv) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs; (c) a corporation listed on any stock exchange; (d) an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is- (i) an FI as defined in the AMLO; (ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that- (A) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and (B) is supervised for compliance with those requirements. (e) the Government or any public body in Hong Kong; or (f) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.
s.4(2), Sch. 2	4.8.11	If a customer not falling within paragraph 4.8.10 has in its ownership chain an entity that falls within that paragraph, the AI is not required to identify or verify the beneficial owners of that entity in that chain when establishing a business relationship with or carrying out an occasional transaction for the customer. However, the AI 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.4(3)(c), Sch. 2	4.8.12	Where a customer is a corporation listed on any stock exchange, an AI may choose not to identify and take reasonable measures to verify its beneficial owners. For this purpose, the AI should assess whether the customer is subject to any disclosure requirements (either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership of the customer.
s.4(3)(a) & (b), Sch. 2	4.8.13	An AI may choose not to identify and take reasonable measures to verify the beneficial owner of a customer, if a customer is an FI as defined in the AMLO that opens an account:

		(a) in the name of a nominee company for holding fund units on behalf of the FI or its underlying customers; or (b) in the name of an investment vehicle in the capacity of a service provider (such as manager or custodian) to the investment vehicle and the underlying investors have no control over the management of the investment vehicle's assets; provided that the FI: (i) has conducted CDD: (A) in the case where the nominee company holds fund units on behalf of the FI or the FI's underlying customers, on its underlying customers; or (B) in the case where the FI acts in the capacity of a service provider (such as manager or custodian) to the investment vehicle, on the investment vehicle pursuant to the provisions of the AMLO; and (ii) is authorised to operate the account as evidenced by contractual document or agreement.
s.4(3)(d), Sch. 2	4.8.14	Where a customer is an investment vehicle[34], an AI may choose not to identify and take reasonable measures to verify its beneficial owners (i.e. the investors), provided that the AI 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.
	4.8.15	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[35] or the appointed institution) falls within any of the categories of institution set out in section 4(3)(d) of Schedule 2, an AI may choose not to identify and take reasonable measures to verify the beneficial owners of the 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

[34] 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.

[35] 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.

		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.
	4.8.16	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, an AI should identify any investor owning or controlling more than 25% interest of the investment vehicle. The AI 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 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 AI accepts such a representation, this should be documented, retained, and subject to periodic review. For the avoidance of doubt, the AI 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 paragraph 4.4.
Specific products		
s.4(4) & (5), Sch. 2	4.8.17	An AI may choose not to identify and take reasonable measures to verify the beneficial owners in relation to a customer if the AI has reasonable grounds to believe that the transaction conducted by the customer relates to any one of the following products: (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; (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 (c) a life insurance policy in respect of which: (i) an annual premium of no more than $8,000 or an equivalent amount in any other currency is payable; or (ii) a single premium of no more than $20,000 or an equivalent amount in any other currency is payable.
	4.8.18	For the purpose of item (a) of paragraph 4.8.17, an AI may generally treat the employer as the customer and may choose not to identify and take reasonable measures to verify the beneficial owners of the scheme (i.e. the employees). Where the AI have a separate business relationship with the employees, it should apply

		CDD measures in accordance with relevant requirements set out in this Chapter.
Solicitors' client accounts		
s.4(6), Sch. 2	4.8.19	If a customer of an AI is a solicitor or a firm of solicitors, the AI may choose not to identify and take reasonable measures to verify the beneficial owners of the client account opened by the customer, provided that the following criteria are satisfied: (a) the client account is kept in the name of the customer; (b) moneys or securities of the customer's clients in the client account are mingled; and (c) the client account is managed by the customer as those clients' agent.
	4.8.20	When opening a client account for a solicitor or a firm of solicitors, an AI should establish the proposed use of the account, i.e. whether to hold co-mingled client funds or the funds of a specific client. If a client account is opened on behalf of a single client or there are sub-accounts for each individual client where funds are not co-mingled at the AI, the AI should establish the identity of the underlying client(s) in addition to that of the solicitor opening the account.
4.9 Enhanced due diligence (EDD)		
General		
s.10&15, Sch. 2	4.9.1	An AI should apply EDD measures in relation to a business relationship or transaction to mitigate and manage the high ML/TF risks in: (a) a situation that by its nature may present a high ML/TF risk taking into account the potentially higher risk factors set out in paragraph 4.9.5; or (b) a situation specified by the HKMA in a notice in writing given to the AI.
s.10&15, Sch. 2	4.9.2	The EDD measures applied should be commensurate with the nature and level of ML/TF risks, based on the higher ML/TF risk factors identified by the AI. The extent of EDD measures should be proportionate, appropriate and discriminating, and be able to be justified to the HKMA. Where the applicable EDD measures cannot fully mitigate the ML/TF risks identified, the AI should take other measures to mitigate the residual risks (e.g. placing transaction limits or restricting account functionalities).
s.15, Sch. 2	4.9.3	An AI should obtain approval from its senior management to establish ~~or continue~~ a business relationship that presents a high ML/TF risk, or continue an existing business relationship where the relationship is subsequently assessed to present a high ML/TF risk.

s.5(3)(c), Sch. 2	4.9.4	An AI should conduct enhanced ongoing monitoring of a business relationship that presents a high ML/TF risk, for example, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination. Reference should be made to Chapter 5.
	4.9.5	Examples of potentially higher risk factors[36] include: (a) customer risk factor: (i) business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic difference between the AI and the customer); (ii) legal persons or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose; (iii) companies that have nominee shareholders ~~or shares in~~, nominee directors, bearer ~~form~~shares or bearer share warrants; (iv) cash intensive business; (v) the ownership structure of the legal person or legal arrangement appears unusual or excessively complex given the nature of the legal person's or legal arrangement's business; or (vi) the customer or the beneficial owner of the customer is a ~~foreign~~ politically exposed person. (b) product, service, transaction or delivery channel risk factors: (i) anonymous transactions (which may involve cash); or (ii) frequent payments received from unknown or un-associated third parties. (c) country risk factors: (i) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems; (ii) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity; (iii) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or (iv) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operation.

[36] In assessing ML/TF risk of a business relationship, an AI should consider a range of factors in a holistic approach.

	4.9.6	Examples of possible EDD measures[37] include: (a) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner; (b) obtaining additional information on the intended nature of the business relationship; (c) obtaining information on the source of funds or source of wealth of the customer (see paragraphs 4.9.~~22~~24 and 4.9.~~23);~~25); (d) obtaining information on the reasons for intended or performed transactions; or (e) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.
Politically exposed persons (PEPs)		
~~Foreign~~Non-Hong Kong PEPs		
Definition		
s.1, Sch. 2	4.9.7	A ~~(foreign)~~non-Hong Kong PEP is defined ~~in the AMLO~~ as: (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~~Hong Kong and (i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official; (ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i); (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or (c) a close associate of an individual falling within paragraph (a) (see paragraph 4.9.8).
s.1, Sch. 2	4.9.8	~~The AMLO defines a~~A close associate is defined as: (a) an individual who has close business relations with a person falling under paragraph 4.9.7(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph 4.9.7(a) is also a beneficial

[37] For the avoidance of doubt, there is no expectation for an AI to conduct all the examples of possible EDD measures for each business relationship that presents a high ML/TF risk. AIs are reminded of the requirements set out in paragraph 4.9.2.

		owner; or (b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under paragraph 4.9.7(a) above.
Identification of ~~foreign~~and EDD measures for non-Hong Kong PEPs		
s.19(1), Sch. 2	4.9.9	An AI should 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~~non-Hong Kong PEP.
~~EDD measures for foreign PEPs~~		
s.5(3)(b) & s.10~~,~~(1)&(2), Sch. 2	4.9.10	When an AI knows that a customer or a beneficial owner of a customer is a ~~foreign~~non-Hong Kong 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~~non-Hong Kong PEP, apply all the following EDD measures: (a) obtaining approval from its senior management for establishing or continuing such business relationship; (b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds; and (c) conducting enhanced ongoing monitoring of that business relationship (see Chapter 5).
Treatment of former non-Hong Kong PEPs		
s.1, Sch. 2	4.9.11	A former non-Hong Kong PEP is defined as: (a) an individual who, being a non-Hong Kong PEP, has been but is not currently entrusted with a prominent public function in a place outside Hong Kong; (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or (c) a close associate of an individual falling within paragraph (a) (see paragraph 4.9.8).
s.10(3), Sch. 2	4.9.12	Following an RBA, an AI may decide not to apply or continue to apply the EDD measures set out in paragraph 4.9.10 to a customer who is or whose beneficial owner is a former non-Hong Kong PEP. Such decision can only be made with the approval of the AI's senior management and on the basis that the PEP no longer presents a high risk of ML/TF. To determine whether a former non-Hong Kong PEP no longer presents a high risk of ML/TF, the AI should

		conduct an appropriate assessment[38] on the ML/TF risk associated with the PEP status taking into account various risk factors, including but not limited to: (a) the level of (informal) influence that the individual could still exercise; (b) the seniority of the position that the individual held as the PEP; and (c) whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the PEP's successor, or informally by the fact that the PEP continues to deal with the same substantive matters).
~~Domestic~~Hong Kong PEPs & international organisation PEPs		
Definition		
	4.9.~~11~~13	A ~~domestic~~Hong Kong PEP is defined as: (a) an individual who is or has been entrusted with a prominent public function in ~~a place within the People's Republic of China~~Hong Kong and (i) includes ~~a head of state,~~ head of government, senior politician, senior government~~,~~ or judicial ~~or military~~ official, senior executive of a ~~state~~government-owned corporation and an important political party official; (ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i); (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or (c) a close associate of an individual falling within paragraph (a) (see paragraph 4.9.8).
	4.9.~~12~~14	An international organisation PEP is defined as: (a) an individual who is or has been entrusted with a prominent function by an international organisation, and (i) includes members of senior management, i.e. directors, deputy directors and members of the board or ~~-~~equivalent functions; (ii) but does not include a middle-ranking or more junior official of the international organisation; (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

[38] For the avoidance of doubt, if an AI does not apply EDD measures to a former non-Hong Kong PEP but without conducting an appropriate risk assessment, the AI will be considered by the HKMA as contravening section 10(1) or 10(2) of Schedule 2, where appropriate. Hence, records of the relevant risk assessment should be retained by the AI as proof of compliance with section 10(3) of Schedule 2.

		(c) a close associate of an individual falling within paragraph (a) (see paragraph 4.9.8).
	4.9.~~13~~15	International organisations referred to in paragraph 4.9.~~12~~14 are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime 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 or the Association of Southeast Asian Nations, etc.
Identification of and EDD measures for ~~domestic~~Hong Kong PEPs & international organisation PEPs		
	4.9.~~14~~16	An AI should take reasonable measures to determine whether a customer or a beneficial owner of a customer is a ~~domestic~~Hong Kong PEP or an international organisation PEP.
s.15, Sch. 2	4.9.~~15~~17	An AI should apply the EDD measures set out in paragraph 4.9.10 in any of the following situations[39]: (a) before establishing a high risk business relationship[40] with a customer who is or whose beneficial owner is a ~~domestic~~Hong Kong PEP or an international organisation PEP; (b) when continuing an existing business relationship with a customer who is or whose beneficial owner is a ~~domestic~~Hong Kong PEP or an international organisation PEP where the relationship subsequently becomes high risk; or (c) when continuing an existing high risk business relationship where the AI subsequently knows that the customer or the beneficial owner of the customer is a ~~domestic~~Hong Kong PEP or an international organisation PEP.
Treatment of former Hong Kong or international organisation PEPs		

[39] For the avoidance of doubt, an AI should consider whether the application of EDD measures in paragraph 4.9.10 could mitigate the ML/TF risk arising from the high risk business relationship with a ~~domestic~~Hong Kong PEP or an international organisation PEP. Where applicable, an AI should also apply EDD measures to mitigate such risk in accordance with the guidance provided in paragraphs 4.9.1 to 4.9.6.

[40] In determining whether a business relationship presents a high ML/TF risk, an AI should take into account all risk factors (including those in paragraph 4.9.5) that are relevant to the business relationship.

	4.9.~~16~~18	~~If a domestic~~Following an RBA[41], if a Hong Kong PEP or an international organisation PEP is no longer entrusted with a prominent (public) function, an AI may ~~adopt an RBA[42] to determine whether~~decide not to apply or continue to apply the EDD measures set out in paragraph 4.9.10 in a high risk business relationship with a customer who is or whose beneficial owner is ~~that domestic PEP~~a former Hong Kong or international organisation PEP~~,~~. Such decision can only be made with the approval of the AI's senior management and on the basis that the PEP no longer presents a high risk of ML/TF. To determine whether a former Hong Kong or international organisation PEP no longer presents a high risk of ML/TF, the AI should conduct an appropriate assessment[43] on the ML/TF risk associated with the PEP status taking into account various risk factors, ~~such as~~including but not limited to: (a) the level of (informal) influence that the individual could still exercise; (b) the seniority of the position that the individual held as ~~a~~the PEP; ~~or~~and (c) whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the ~~PEPs~~PEP's successor, or informally by the fact that the PEP continues to deal with the same substantive matters). ~~The AI should obtain approval from its senior management for such a decision.~~
Further guidance applied to all types of PEPs		
Scope of PEPs		
	4.9.~~17~~19	An AI should implement appropriate risk management systems to identify PEPs. Under-classification of PEPs poses a higher ML risk to the AI whilst over-classification of PEPs leads to an unnecessary compliance burden to the AI and its customers.
	4.9.~~18~~20	The definitions of PEPs set out above provide some non-exhaustive examples of the types of prominent (public) functions that an individual may be or may have been entrusted with by a ~~foreign or domestic~~ government~~,~~ or by an international organisation. An AI should provide sufficient guidance and examples to its staff to enable them to identify all types of PEPs. In determining what

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

[42] ~~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.~~

[43] For the avoidance of doubt, if an AI does not apply EDD measures to a former Hong Kong or international organisation PEP but without conducting an appropriate risk assessment, the AI will be considered by the HKMA as contravening section 15(a) or 15(b) of Schedule 2, where appropriate. Hence, records of the relevant risk assessment should be retained by the AI as proof of compliance with section 15(a) or 15(b) of Schedule 2.

		constitutes a prominent (public) function, the AI 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.
	4.9.~~19~~21	While an AI may refer to commercially available databases to identify PEPs, the use of these databases should never replace traditional CDD processes (e.g. understanding the occupation and employer of a customer). When using commercially available databases, the AI should be aware of their limitations, for example, the databases are not necessarily comprehensive or reliable as they generally draw solely from information that is publicly available; the definition of PEPs used by the database providers may or may not align with the definition of PEPs applied by the AI; and any technical incapability of such databases that may hinder the AI's effectiveness of PEP identification. Therefore, the AI should only use such databases as a support tool and ensure they are fit for purpose.
	4.9.~~20~~22	Although the EDD requirements also apply to family members and close associates of the PEP, the risks associated with them may vary depending to some extent on the social-economic and cultural structure of the jurisdiction of the PEP.
EDD measures for PEPs		
	4.9.~~21~~23	Since not all PEPs pose the same level of ML risks, an AI should adopt an RBA in determining the extent of EDD measures in paragraph 4.9.10 taking into account relevant factors, such as: (a) the nature of the prominent (public) functions that a PEP holds; (b) the geographical risk associated with the jurisdiction where a PEP holds prominent (public) functions; (c) the nature of the business relationship (e.g. the delivery/distribution channel used; or the product or service offered); ~~or~~and ~~(d) the level of influence that a PEP may continue to exercise after stepping down from the prominent (public) function.~~ (d) if the PEP is a former PEP, the risk factors specified in paragraphs 4.9.12 and 4.9.18.
	4.9.~~22~~24	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 AI 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.
	4.9.~~23~~25	Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and the AI (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.
	4.9.~~24~~26	It is for an AI to decide which measures it deems appropriate, in accordance with its assessment of the risks, to establish the source of funds and source of wealth. In practical terms, this will often amount to obtaining information from the PEP and verifying it against publicly available information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. The AI should however note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. The AI 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.
4.10 Customer not physically present for identification purposes		
s.9~~,~~(1), Sch. 2	4.10.1	The AMLO permits AIs to establish business relationships through various channels, both face-to-face (e.g. branch) and non-face-to-face (e.g. internet). However, an AI should take additional measures to mitigate the risk (e.g. impersonation risk) associated with customers not physically present for identification purposes. ~~If~~Except for the situation specified in paragraph 4.10.2, if a customer has not been physically present for identification purposes, the AI should carry out at least one of the following additional measures to mitigate the risks posed: (a) further verifying the customer's identity on the basis of documents, data or information 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; (b) taking supplementary measures to verify information relating to the customer that has been obtained by the AI; or (c) ensuring that the payment or, if there is more than one payment, the first payment made ~~into~~in relation to the customer's account is ~~received from~~carried out through an account opened in the customer's name with an AI or ~~a bank operating~~an institution that:

		(i) is incorporated or established in an equivalent jurisdiction ~~that~~ ; (ii) carries on a business similar to that carried on by an AI; ~~(i)~~(iii) 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.~~; and (iv) is supervised for compliance with those requirements by authorities in that jurisdiction that perform functions similar to those of the HKMA.
s.9(2), Sch. 2	4.10.2	If an AI has verified the identity of the customer on the basis of data or information provided by a digital identification system that is a reliable and independent source recognised by the HKMA, the AI is not required to carry out any additional measures set out in paragraph 4.10.1.
	4.10.~~2~~3	The extent of additional measures set out in paragraph 4.10.1 will depend on the nature and characteristics of the product or service requested and the assessed ML/TF risks presented by the customer.
	4.10.~~3~~4	Paragraph 4.10.1(b) allows an AI 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; (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 AI should ensure and be able to demonstrate to the HKMA that the supplementary measure(s) taken can adequately guard against impersonation risk.
	4.10.~~4~~5	While the requirements to undertake additional measures generally apply to a customer that is a natural person, an AI should also mitigate any increased risk (e.g. applying additional due diligence measures set out in paragraph 4.10.1) if a customer that is not a natural person establishes a business relationship with an AI 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 AI is provided with copies of documents for identifying and verifying a legal person customer's identity, an AI should also mitigate any increased risk (e.g. applying additional due diligence measures set out in paragraph 4.10.1).
4.11 Reliance on CDD performed by intermediaries		
General		

s.18, Sch. 2	4.11.1	An AI may rely upon an intermediary to perform any part of the CDD measures[44] 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 AI. 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 AI, and would apply its own procedures to perform the CDD measures.
	4.11.2	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 AI, in accordance with the AI's procedures, and subject to the AI's control of effective implementation of these procedures by the outsourced entity or agent.
s.18(1), Sch. 2	4.11.3	When relying on an intermediary, an AI should: (a) obtain written confirmation from the intermediary that the intermediary agrees to act as the AI's intermediary and perform which part of the CDD measures specified in section 2 of Schedule 2; and (b) be satisfied that the intermediary will on request provide a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out the CDD measures without delay.
s.18(4)(a), Sch. 2	4.11.4	An AI that carries out a CDD measure by means of an intermediary should 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 AI 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	4.11.5	Where these documents and records are kept by the intermediary, an AI should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the AI'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 AI ends or until such time as may be specified by the HKMA. The AI should ensure that the intermediary will, if

[44] For the avoidance of doubt, an AI 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.

		requested by the AI within the period specified in the record-keeping requirements of the AMLO, provide to the AI 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 AI 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 AI anymore.
	4.11.6	An AI 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.
	4.11.7	Whenever an AI 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 AI intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the AI has any doubts regarding the CDD measures carried out by the intermediary previously, the AI should perform the required CDD as soon as reasonably practicable.
Domestic intermediaries		
s.18(3)(a), (3)(b) & (7), Sch. 2	4.11.8	An AI 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: (a) an FI that is an AI, a licensed corporation, an authorized insurer, ~~an appointed~~a licensed individual insurance agent, licensed insurance agency or ~~an authorized~~licensed insurance broker company (intermediary FI); (b) an accounting professional meaning: (i) a certified public accountant ~~or a certified public accountant (practising),~~ as defined by section 2(1) of the Professional Accountants Ordinance~~;~~, or a certified public accountant (practising) as defined by section 2(1) of the Accounting and Financial Reporting Council Ordinance; (ii) a corporate practice as defined by section 2(1) of the ~~Professional Accountants~~Accounting and Financial Reporting Council Ordinance; or (iii) a CPA firm ~~of certified public accountants (practising) registered under Part IV~~as defined by section 2(1) of the ~~Professional Accountants~~Accounting and Financial Reporting Council Ordinance; (c) an estate agent meaning: (i) a licensed estate agent as defined by section 2(1) of the Estate Agents Ordinance; or

		(ii) a licensed salesperson as defined by section 2(1) of the Estate Agents Ordinance; (d) a legal professional meaning: (i) a solicitor as defined by section 2(1) of the Legal Practitioners Ordinance; or (ii) a foreign lawyer as defined by section 2(1) of the Legal Practitioners Ordinance; or (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 (ii) a deemed licensee as defined by section 53ZQ(5) of the AMLO, provided that in the case of an accounting professional, an estate agent, a legal professional or a TCSP licensee, the AI 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[45].
s.18(3)(a) & (3)(b), Sch. 2	4.11.9	An AI should take appropriate measures to ascertain if the domestic intermediary satisfies the criteria set out in paragraph 4.11.8, which may include: (a) where the domestic intermediary is an accounting professional, an estate agent, a legal professional or a TCSP licensee, ascertaining whether the domestic intermediary is required to comply with the relevant requirements set out in Schedule 2 with respect to the customer; (b) making enquiries concerning the domestic intermediary's stature or the extent to which any group AML/CFT standards are applied and audited; or (c) reviewing the AML/CFT policies and procedures of the domestic intermediary.
Overseas intermediaries		
s.18(3)(c), Sch. 2	4.11.10	An AI may rely upon an overseas intermediary[46] carrying on business or practising in an equivalent jurisdiction[47] to perform any part of the CDD measures set out in section 2 of Schedule 2, where the intermediary: (a) falls into one of the following categories of businesses or professions: (i) an institution that carries on a business similar to that carried on by an intermediary FI;

[45] 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.

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

[47] Guidance on jurisdictional equivalence is provided in paragraph 4.16.

		(ii) a lawyer or a notary public; (iii) an auditor, a professional accountant, or a tax advisor; (iv) a TCSP; (v) a trust company carrying on trust business; and (vi) a person who carries on a business similar to that carried on by an estate agent; (b) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction; (c) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and (d) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs or the regulatory bodies (as may be applicable).
	4.11.11	An AI should take appropriate measures to ascertain if the overseas intermediary satisfies the criteria set out in paragraph 4.11.10. Appropriate measures that should be taken to ascertain if the criterion set out in paragraph 4.11.10(c) is satisfied may include: (a) making enquiries concerning the overseas intermediary's stature or the extent to which any group's AML/CFT standards are applied and audited; or (b) reviewing the AML/CFT policies and procedures of the overseas intermediary.
<u>Related foreign financial institutions as intermediaries</u>		
s.18(3)(d), (3A) & (7), Sch. 2	4.11.12	An AI 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: (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: (i) it is within the same group of companies as the AI; (ii) if the AI is incorporated in Hong Kong, it is a branch of the AI; (iii) if the AI is incorporated outside Hong Kong: (A) it is the head office of the AI; or (B) it is a branch of the head office of the AI; (b) is required under group policy: (i) to have measures in place to ensure compliance with requirements similar to the requirements imposed under Schedule 2; and (ii) to implement programmes against ML/TF; and (c) is supervised for compliance with the requirements mentioned in paragraph (b) at a group level: (i) by an RA; or

		(ii) by an authority in an equivalent jurisdiction that performs, in relation to the holding company or the head office of the AI, functions similar to those of an RA under the AMLO.
s.18(3A) & (4)(c), Sch. 2	4.11.13	The group policy set out in paragraph 4.11.12(b) refers to a policy of the group of companies to which the AI belongs and the policy applies to the AI and the related foreign FI. The group policy should include CDD and record-keeping requirements similar to the requirements imposed under Schedule 2 and the group-wide AML/CFT Systems[48] (e.g. compliance and audit functions). The group policy should also be able to mitigate adequately any higher country risk in relation to the jurisdiction where the related foreign FI is located. The AI 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	4.11.14	The AI 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.
4.12 Pre-existing customers		
s.6, Sch. 2	4.12.1	An AI should 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: (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 AI's knowledge of the customer or the customer's business or risk profile, or with its knowledge of the source of the customer's funds; (b) a material change occurs in the way in which the customer's account is operated; (c) the AI suspects that the customer or the customer's account is involved in ML/TF; or (d) the AI 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.
	4.12.2	Trigger events may include the re-activation of a dormant ~~account~~relationship or a change in the beneficial ownership or control of the account but the AI will need to consider other trigger events specific to its own customers and business.

[48] Reference should be made to Chapter 3.

s.5, Sch. 2	4.12.3	An AI should note that requirements for ongoing monitoring under section 5 of Schedule 2 also apply to pre-existing customers (see Chapter 5).
4.13 Failure to satisfactorily complete CDD		
s.3(1) & (4), Sch. 2	4.13.1	Where the AI is unable to comply with relevant CDD requirements set out in this Chapter and the ongoing due diligence requirements set out in Chapter 5, it should not establish a business relationship or carry out any occasional transaction with that customer, or should terminate business relationship as soon as reasonably practicable (where applicable), and where there is relevant knowledge or suspicion, should make an STR to the JFIU.
4.14 Prohibition on anonymous accounts		
s.16, Sch. 2	4.14.1	An AI should not open, or maintain any anonymous ~~accounts~~account or ~~accounts~~account in a fictitious ~~names~~name for any ~~new or existing~~ customer. ~~Where~~Confidential numbered accounts ~~exist, the AI~~[49] should ~~maintain them in such a way that full compliance with the AMLO can be achieved. The AI~~not function as anonymous accounts, rather they should ~~properly identify~~be subject to exactly the same CDD and ~~verify~~control measures[50] as all other business relationships. While a numbered account can offer additional confidentiality for the customer, the identity of the ~~customer in accordance with this Guideline.~~latter must be verified by the AI and known to a sufficient number of staff to facilitate effective CDD and ongoing monitoring. In all cases, whether the relationship involves numbered accounts or not, the ~~customer identification and verification records~~customer's CDD record should be available to the HKMA, other competent authorities, the CO, auditors, and other staff with appropriate authority.
4.15 Jurisdictions subject to a call by the FATF		
s.15, Sch. 2	4.15.1	An AI should apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons~~, and~~ (including FIs~~,~~) from jurisdictions for which this is called for by the FATF in accordance with the guidance provided in paragraph 4.9.
s.15, Sch. 2	4.15.2	Where mandatory EDD or countermeasures[51] are called for by the FATF, or in other circumstances independent of any call by the FATF but also considered to be higher risk, the HKMA may also, through a notice in writing:

[49] In respect of a numbered account, the name of the customer (and/or the beneficial owner) is known to the AI but is substituted by an account number or code name in subsequent documentation.

[50] For example, wire transfers from numbered accounts must reflect the real name of the account holder.

[51] For jurisdictions with serious deficiencies in applying the FATF Recommendations and where inadequate progress has been made to improve their positions, the FATF may recommend the application of countermeasures.

		(a) impose a general obligation on AIs to comply with the requirements set out in section 15 of Schedule 2; or (b) require AIs to undertake specific countermeasures described in the notice. The type of measures in paragraph (a) and (b) would be proportionate to the nature of the risks and/or deficiencies.
4.16 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	4.16.1	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: (a) a jurisdiction that is a member of the FATF, other than Hong Kong; or (b) a jurisdiction that imposes requirements similar to those imposed under Schedule 2.
Determination of jurisdictional equivalence		
	4.16.2	An AI 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 AI should document its assessment of the jurisdiction, and may include consideration of the following factors: (a) whether the jurisdiction concerned is a member of FATF-style regional bodies and recent mutual evaluation report published by the FATF-style regional bodies; (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; (c) any advisory circular issued by the HKMA from time to time alerting AIs to jurisdictions with poor AML/CFT controls; (d) any other AML/CFT-related publications published by specialised national, international, non-governmental or commercial organisations.
	4.16.3	As the AML/CFT regime of a jurisdiction will change over time, an AI should review the jurisdictional equivalence assessment on a regular basis and/or upon trigger events.

Chapter 5 – ONGOING MONITORING		
General		
s.5(1), Sch. 2	5.1	Ongoing monitoring is an essential component of effective AML/CFT Systems. An AI should continuously monitor its business relationship with a customer in two aspects: (a) **ongoing CDD**: reviewing from time to time documents, data and information relating to the customer that have been obtained by the AI 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; and (b) **transaction monitoring**: (i) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the AI's knowledge of the customer, the customer's business, risk profile and source of funds; and (ii) identifying transactions that (i) are complex, unusually large in amount or of an unusual pattern; and (ii) have no apparent economic or lawful purpose, and examining the background and purposes of those transactions and setting out the findings in writing.
Ongoing CDD		
s.5(1)(a), Sch. 2	5.2	To ensure documents, data and information of a customer obtained are up-to-date and relevant[52], an AI should undertake reviews of existing CDD records of customers on a regular basis and/or upon trigger events [53]. Clear policies and procedures should be developed, especially on the frequency of periodic review or what constitutes a trigger event.
s.5(1)(a), Sch. 2	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 AI, to ensure the CDD information retained remains up-to-date and relevant.
Transaction monitoring		
Transaction monitoring systems and processes		
s.19(3), Sch. 2	5.4	An AI should establish and maintain adequate systems and processes 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:

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

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

		(a) the size and complexity of its business; (b) the ML/TF risks arising from its business; (c) the nature of its systems and controls; (d) the monitoring procedures that already exist to satisfy other business needs; and (e) the nature of the products and services provided (which includes the means of delivery or communication).
	5.5	An AI 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 AI 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 a customer's multiple accounts within or across lines of businesses, and related customers' accounts within or across lines of businesses. This means preferably the AI adopts a relationship-based approach rather than on a transaction-by-transaction basis.
	5.7	In designing transaction monitoring systems and processes, including setting of parameters and thresholds, an AI should take into account the transaction characteristics, which may include: (a) the nature and type of transactions (e.g. abnormal size or frequency); (b) the nature of a series of transactions (e.g. structuring a single transaction into a number of cash deposits); (c) the counterparties of transactions; (d) the geographical origin/destination of a payment or receipt; and (e) the customer's normal account activity or turnover.
	5.8	An AI should regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including 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.
RBA to transaction monitoring and review of transactions		
s.5(3), (4)&(5), Sch. 2	5.9	An AI should conduct transaction 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 a customer. Where

		the ML/TF risks are high[54], the AI should conduct enhanced transaction monitoring. In low risk situations, the AI may reduce the extent of monitoring.
s.5(1)(b) & (c), Sch. 2	5.10	An AI 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: (a) the customer's transactions are not consistent with the AI's knowledge of the customer, the customer's business, risk profile or source of funds; or (b) the AI identifies transactions that (i) are complex, unusually large in amount or of an unusual pattern, and (ii) have no apparent economic or lawful purpose[55].
	5.11	Where an AI conducts enquiries and obtains what it considers to be a satisfactory explanation of the transaction or activity, it may conclude that there are no grounds for suspicion, and therefore take no further action. Even if no suspicion is identified, the AI should consider updating the customer risk profile based on any relevant information obtained.
	5.12	However, where the AI 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.
	5.13	An AI should be aware that making enquiries to customers, when conducted properly and in good faith, will not constitute tipping off. However, if the AI reasonably believes that performing the CDD process will tip off the customer, it may stop pursuing the process. The AI should document the basis for its assessment and file an STR to the JFIU.
s.5(1)(a), Sch. 2	5.14	The findings and outcomes of steps taken by the AI in paragraph 5.10, as well as the rationale of any decision made after taking these steps, should be properly documented in writing and be available to the HKMA, other competent authorities and auditors.

[54] Examples of high ML/TF risk situations that require enhancing transaction monitoring include: (a) a customer or a beneficial owner of a customer being a ~~foreign~~non-Hong Kong PEP; and (b) a business relationship presenting a high risk of ML/TF under section 15 of Schedule 2.

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

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 & s.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[56] 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, s.7, s.8, s.8A & s.11L, UNATMO	6.5	A number of provisions in the UNATMO are of particular relevance to AIs, and are listed below:

[56] 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.

		(a) section 6 empowers the Secretary for Security (S for S) to freeze suspected terrorist property; (b) section 7 prohibits the provision or collection of property for use to commit terrorist acts; (c) section 8 prohibits any person from making available or collecting or soliciting property or financial (or related) services for terrorists and terrorist associates; (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 (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 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), s.8 & s.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 AI seeking such a licence should write to the Security Bureau.
Financial sanctions & proliferation financing		
	6.7	The UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the UNSC, including targeted financial sanctions [57] against ~~individuals~~certain persons and entities, such as those 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 Development Bureau. ~~It~~Except under the authority of a licence granted by the Chief Executive, it is an offence~~:~~ (a) to make available, directly or indirectly, any funds~~,~~ or other financial assets~~,~~ or economic resources~~,~~ to, or for the benefit of, ~~a~~(i) designated ~~person~~persons or ~~entity, as well as~~entities, (ii) those acting on their behalf, at their direction, or owned or controlled by them~~;~~, or (iii) entities owned by the aforementioned; or ~~(a)~~(b) to deal with, directly or indirectly, any funds~~,~~ or other

[57] 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.

		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~~.
Applicable UNSO Regulation	6.8	The Chief Executive may grant a licence for making available ~~or dealing with~~ any funds~~,~~ or other financial assets~~, and~~ or economic resources to ~~or~~; or dealing with any funds or other financial assets or economic resources belonging to ~~a designated person or entity~~, or owned or controlled by, certain persons or entities under specified circumstances in accordance with the provisions of the relevant regulation made under the UNSO. An AI 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~~PF 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.
Sanctions imposed by other jurisdictions		
	6.11	While AIs 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 AI 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 its operations, the AI should consider what implications exist ~~for its procedures~~ 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 AI 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 AIs 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 AI should be able to identify terrorist suspects and possible designated parties, and detect prohibited transactions. To this end, an AI 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 AI. Alternatively, an AI may subscribe to such a database maintained by a third party service provider 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. The HKMA draws to the attention to AIs from time to time whenever there are any updates to UNSCRs or sanctions lists relating to terrorism, TF and PF promulgated by the UNSC. AIs 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 AI should include in its database: (i) the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau; and (ii) the lists that the HKMA draws to the attention of AIs from time to time~~; and (iii) any relevant designations by overseas authorities which may affect its operations~~. The database should also 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~~sanctioned parties, an AI should implement an effective screening mechanism[58], which should include:

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

		(a) screening its customers and any beneficial owners of the customers against current database at the establishment of the relationship; (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 (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 connected parties as defined in paragraph 4.3.19 and PPTAs of a customer using an RBA.
	6.18	When possible name matches are identified during screening, an AI should conduct enhanced checks to determine whether the possible matches are genuine hits. In case of any suspicions of TF, PF or sanctions violations, the AI 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 AI may rely on its overseas office to maintain the database or to undertake the screening process. However, the AI is reminded that the ultimate responsibility for ensuring compliance with the relevant regulations and legislation on TF, financial sanctions and PF remains with the AI.

Chapter 7 – SUSPICIOUS TRANSACTION REPORTS AND LAW ENFORCEMENT REQUESTS		
Suspicious transaction reporting regime in Hong Kong		
General issues		
s.25A(1) & (7), DTROP & OSCO, s.12(1) & s.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: (a) actual knowledge; (b) knowledge of circumstances which would indicate facts to a reasonable person; and (c) knowledge of circumstances which would put a reasonable person on inquiry.
	7.3	Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence. As far as an AI is concerned, when a transaction or a series of transactions of a customer is not consistent with the AI's knowledge of the customer, or is unusual (e.g. in a pattern that has no apparent economic or lawful purpose), the AI should take appropriate steps to further examine the transactions and identify if there is any suspicion (see paragraphs 5.10 to 5.14).
	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, (a) an AI should file an STR even where no transaction has been

		conducted by or through the AI[59]; and (b) the STR should be made as soon as 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. The tipping off provision includes circumstances where a suspicion has been raised internally within an AI, but has not yet been reported to the JFIU.
AML/CFT Systems in relation to suspicious transaction reporting		
	7.7	An AI should implement appropriate AML/CFT Systems in order to fulfil its statutory reporting obligations, and properly manage and mitigate the risks associated with any customer or transaction involved in an STR. The AML/CFT Systems should include: (a) appointment of an MLRO (see Chapter 3); (b) implementing clear policies and procedures over internal reporting, reporting to the JFIU, post-reporting risk mitigation and prevention of tipping off; and (c) keeping proper records of internal reports and STRs.
	7.8	An AI 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 its business.
MLRO		

[59] 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.

	7.9	An AI 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: (a) review of internal disclosures and exception reports and, in light of all available relevant information, determination of whether or not it is necessary to make a report to the JFIU; (b) maintenance of all records related to such internal reviews; and (c) provision of guidance on how to avoid tipping off.
<u>Identifying suspicious transactions and internal reporting</u>		
	7.10	An AI 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 AI 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	An AI should establish and maintain clear policies and procedures to ensure that: (a) all staff are made aware of the identity of the MLRO and of the procedures to follow when making an internal report; and (b) all internal reports should reach the MLRO without undue delay.
	7.13	While an AI 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), UNATMO	7.14	Once a staff of an AI has reported suspicion to the MLRO in accordance with the policies and procedures established by the AI

		for the making of such reports, the statutory obligation of the staff has been fully satisfied.
	7.15	The internal report should include sufficient details of the customer concerned and the information giving rise to the suspicion.
	7.16	The MLRO should acknowledge receipt of an internal report and provide a reminder of the obligation regarding tipping off to the reporting staff upon internal reporting.
	7.17	When evaluating an internal report, an MLRO should take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the AI concerning the customer to which the report relates. This may include: (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; (b) making reference to any previous patterns of instructions, the length of the business relationship, and CDD and ongoing monitoring information and documentation; and (c) appropriate questioning of the customer per the systematic approach to identify suspicious transactions recommended by the JFIU[60].
	7.18	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 documented, together with any conclusions drawn.
<u>Reporting to the JFIU</u>		
	7.19	If after completing the review of the internal report, an 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. 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.

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

	7.20	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.
	7.21	In the event that an urgent reporting is required (e.g. where a customer has instructed the AI 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 investigation by law enforcement agency, an AI should indicate this in the STR. Where exceptional circumstances exist in relation to an urgent reporting, an initial notification by telephone to the JFIU should be considered.
	7.22	An AI is recommended to indicate any intention to terminate a business relationship in its initial STR to the JFIU~~, thereby allowing the JFIU to comment, at an early stage, on such a course of action~~.
	7.23	An AI should ensure STRs filed to the JFIU are of high quality taking into account feedback and guidance provided by the JFIU in its quarterly report[61] and the HKMA from time to time.
Post STR reporting		
s.25A(2)(a), DTROP & OSCO, s.12(2B)(a), UNATMO	7.24	The JFIU will acknowledge receipt of an STR made by an AI 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 AI to operate the account under the provisions of section 25A(2)(a) of both the DTROP and the OSCO, and section 12(2B)(a) of the UNATMO. ~~If a no consent letter is issued~~Otherwise, the AI should ~~act according to the contents of the letter~~take appropriate action and seek legal advice where necessary.
s.25A(2), DTROP & OSCO, s.12(2), UNATMO	7.25	Filing an STR to the JFIU provides an AI with a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report, provided: (a) the report is made before the AI undertakes the disclosed acts and the acts (transaction(s)) are undertaken with the consent of the JFIU; or

[61] 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. AIs 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.

		(b) the report is made after the AI has performed the disclosed acts (transaction(s)) and the report is made on the AI's own initiative and as soon as it is reasonable for the AI to do so.
	7.26	However, the statutory defence stated in paragraph 7.25 does not absolve an AI from the legal, reputational or regulatory risks associated with the account's continued operation. An AI 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 AI.
	7.27	An AI 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 AI'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 AI's business objectives, and its capacity to mitigate the risks identified.
	7.28	An AI 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, should continue to be reported to the MLRO who should make further reports to the JFIU if appropriate.
Record-keeping		
	7.29	An AI should 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.
	7.30	An AI should 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 and crime-related intelligence		

	7.31	An AI may receive various requests from law enforcement agencies, e.g. search warrants, production orders, restraint orders or confiscation orders, pursuant to relevant legislations in Hong Kong. These requests are crucial to aid law enforcement agencies to carry out investigations as well as restrain and confiscate illicit proceeds. Therefore, an AI should establish clear policies and procedures to handle these requests in an effective and timely manner, including provision of accurate information, allocation of sufficient resources and appointing a staff as the main point of contact with law enforcement agencies.
	7.32	An AI 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 AI encounters difficulty in complying with the timeframes stipulated, the AI 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	7.33	During a law enforcement investigation, an AI may be served with a restraint order which prohibits the dealing with particular funds or property pending the outcome of an investigation. The AI should ensure that it is able to ~~freeze~~withhold the relevant property that is the subject of the order. It should be noted that the restraint order may not apply to all funds or property involved within a particular business relationship and the AI should consider what, if any, funds or property may be utilised subject to the laws of Hong Kong.
s.3, DTROP, s.8, OSCO, s.13, UNATMO	7.34	Upon the conviction of a defendant, a court may order the confiscation of his criminal proceeds and an AI may be served with a confiscation order in the event that it holds funds or other property belonging to that defendant that are deemed by the court to represent his benefit from the crime. A court may also order the forfeiture of property where it is satisfied that the property is terrorist property.
	7.35	When an AI receives a ~~request from a law enforcement agency,~~ requirement (e.g. search warrant or production order~~,~~) or other types of crime-related intelligence requests including those from a law enforcement agency (e.g. notification letter) in relation to a particular customer or business relationship, the AI should timely assess the risks involved and the need to conduct an appropriate review on the customer or the business relationship to determine whether there is any suspicion and should also be aware that the customer subject to the request can be a victim of crime.

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. Record-keeping also enables an AI to demonstrate compliance with the requirements set out in the AMLO, this Guideline and other relevant guidance promulgated by the HKMA from time to time.
	8.2	An AI 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~~statutory and ~~other~~ regulatory requirements~~,~~ that are appropriate to the nature, size and complexity of its businesses. The AI should ensure that: (a) the audit trail for funds moving through the AI that relate to any customer and, where appropriate, the beneficial owner of the customer, account or transaction is clear and complete; (b) all CDD information and transaction records are available swiftly to the HKMA, other authorities and auditors upon appropriate authority; and (c) it can demonstrate compliance with any relevant requirements specified in other sections of this Guideline and other guidelines issued by the HKMA.
Retention of records relating to CDD and transactions		
s.20(1)(b)(i), Sch. 2 s.20(1)(b)(ii), Sch. 2	8.3	An AI should keep: (a) the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and, where applicable, verifying the identity of the customer and/or beneficial owner of the customer and/or beneficiary and/or persons who purport to act on behalf of the customer and/or other connected parties to the customer; (b) other documents and records obtained throughout the CDD and ongoing monitoring process, including SDD and EDD; (c) where applicable, the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship; (d) the original or a copy of the records and documents relating to the customer's account (e.g. account opening form or risk

		assessment form) and business correspondence[62] with the customer and any beneficial owner of the customer (which at a minimum should include business correspondence material to CDD measures or significant changes to the operation of the account); and (e) the results of any analysis undertaken (e.g. inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose).
s.20(2)~~)&(~~), (3)&(3A), 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 threshold (i.e. $8,000 for wire transfers and virtual asset transfers involving virtual assets, and $120,000 for other types of transactions), an AI 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	An AI should maintain the original or a copy of the documents, and a record of the data and information, obtained or generated in connection with each transaction the AI 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	The HKMA may, by notice in writing to an AI, require it to keep the records relating to a specified transaction or customer for a period specified by the HKMA 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 carried out by the HKMA, or to any other purposes as specified in the notice.

[62] An AI 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.

Part 3, Sch. 2	8.9	Irrespective of where CDD and transaction records are held, an AI 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)(a) & (b), Sch. 2	8.10	Where customer identification and verification documents are held by an intermediary on which an AI is relying to carry out CDD measures, the AI concerned remains responsible for compliance with all record-keeping requirements. The AI 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 AI.
s.18(4)(a), Sch. 2	8.11	For the avoidance of doubt, an AI 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 AI should ensure that an intermediary will pass the documents and records to the AI, 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 AI'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 AI 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. Apart from the initial training, an AI 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 AI 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: (a) their AI's and their own personal statutory obligations and the possible consequences for failure to comply with CDD and record-keeping requirements under the AMLO; (b) their AI'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; (c) any other statutory and regulatory obligations that concern their AIs and themselves under the DTROP, the OSCO, the UNATMO, the UNSO, the WMD(CPS)O and the AMLO, and the possible consequences of breaches of these obligations; (d) the AI's policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting; and (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 AI with respect to AML/CFT.
	9.5	In addition, the following areas of training may be appropriate for certain groups of staff: (a) all new staff, irrespective of seniority: (i) an introduction to the background to ML/TF and the importance placed on ML/TF by the AI; and (ii) the need for identifying and reporting of any suspicious

		transactions to the MLRO, and the offence of tipping off; (b) members of staff who are dealing directly with the public (e.g. front-line personnel): (i) the importance of their roles in the AI's ML/TF strategy, as the first point of contact with potential money launderers; (ii) the AI's policies and procedures in relation to CDD and record-keeping requirements that are relevant to their job responsibilities; and (iii) training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required; (c) back-office staff, depending on their roles: (i) appropriate training on customer verification and relevant processing procedures; and (ii) how to recognise unusual activities including abnormal settlements, payments or delivery instructions; (d) managerial staff including internal audit officers and COs: (i) higher level training covering all aspects of the AI's AML/CFT regime; and (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 (e) MLROs: (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 (ii) training to keep abreast of AML/CFT requirements/developments generally.
	9.6	An AI 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 AI may consider including available FATF papers and typologies as part of the training materials. The AI should be able to demonstrate to the HKMA that all materials are up-to-date and in line with current requirements and standards.
	9.7	No matter which training approach is adopted, an AI 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 AI should monitor the effectiveness of the training. This may be achieved by:

		(a) testing staff's understanding of the AI's policies and procedures to combat ML/TF, the understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions; (b) monitoring the compliance of staff with the AI'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 (c) monitoring attendance and following up with staff who miss such training without reasonable cause.

Chapter 10 – WIRE TRANSFERS		
General		
s.1(4) & s.12(11), Sch. 2	10.1	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[63] or another institution, whether or not one or more other institutions (intermediary institutions) participate in completion of the transfer of the money. An AI should follow the relevant requirements set out in this Chapter with regard to its role in a wire transfer.
	10.2	Where an AI 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.
	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)[64].
s.12(2), Sch. 2	10.4	Section 12 of Schedule 2 and this Chapter do not apply to the following wire transfers: (a) a wire transfer between an AI and an FI as defined in the AMLO if each of them acts on its own behalf; (b) a wire transfer between an AI and a foreign institution[65] if each of them acts on its own behalf; (c) a wire transfer if: (i) it arises from a transaction that is carried out using a credit card ~~or~~, debit card or prepaid 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~~card, debit card~~), except when the card is used to effect a transfer of money; and~~ or prepaid card); (ii) the card is not used as a payment system to effect a person-to-person transfer; and ~~(ii)~~(iii) the number (or equivalent unique identifier) of the

[63] For example, a wire transfer conducted between branches of the same banking institution.

[64] 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.

[65] 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.

		credit card ~~or~~, debit card ~~number~~or prepaid card is included in the message or payment form accompanying the transfer.
Ordering institutions		
s.12(3) & (5), Sch. 2	10.5	An ordering institution should 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: (a) the originator's name; (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; (c) the originator's address or, the originator's customer identification number[66] or identification document number or, if the originator is an individual, the originator's date and place of birth; (d) the recipient's name; and (e) the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution.
s.12(3), (3A) & (5), Sch. 2	10.6	An ordering institution should 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 : (a) the originator's name; (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; (c) the recipient's name; and (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.

[66] 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 should 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.

	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 should 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 should 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[67], 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 should, on the request of the institution to which it passes on the transfer instruction or the HKMA, 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.
s.19(2), Sch. 2	10.13	An ordering institution should establish and maintain effective procedures to ensure that proper safeguards exist to prevent

[67] 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.

		carrying out outgoing wire transfers that do not comply with the relevant originator or recipient information requirements, which include: (a) taking reasonable measures (e.g. regular review or testing by internal control or audit function to assess system capabilities) to identify whether domestic or cross-border wire transfers lack required originator information or required recipient information; and (b) having risk-based policies and procedures for handling wire transfers lacking required originator information or required recipient information, and timely rectifying any control deficiencies identified.
Intermediary institutions		
s.12(8), Sch. 2	10.~~13~~14	An intermediary institution should 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~~15	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~~16	An intermediary institution should 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: (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 (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~~17	In respect of the risk-based policies and procedures referred to in paragraph 10.~~15,~~16, if a cross-border wire transfer is not accompanied by the required originator information or required recipient information, the intermediary institution should 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~~18	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 should 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~~19	A beneficiary institution should 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: (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 (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~~20	In respect of the risk-based policies and procedures referred to in paragraph 10.~~18,~~19, if a domestic or cross-border wire transfer is not accompanied by the required originator information or required recipient information, the beneficiary institution should 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~~21	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 should as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
s.3(1)(c), Sch. 2	10.~~21~~22	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.

Chapter 11 – CORRESPONDENT BANKING AND OTHER SIMILAR RELATIONSHIPS		
General		
s.1~~(1),~~ Sch. 2	11.1	In the AMLO, correspondent banking is defined as the provision of banking services by an AI (the correspondent bank) to another institution (the respondent bank) to enable the latter to provide services and products to its own customers.
	11.2	A correspondent banking relationship is also a type of business relationship, so it does not include occasional transactions or the mere exchange of SWIFT Relationship Management Application (RMA) keys in the context of non-customer relationships, but rather is characterized by its on-going, repetitive nature.
	11.3	An AI may act as a correspondent for thousands of other banks around the world. The respondent bank may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), cross-border wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
	11.4	Correspondent banking services do not all carry the same level of ML/TF risks. Therefore, in assessing the ML/TF risks of a respondent bank[68], an AI should take into account all the relevant risk factors and any applicable risk mitigation measures in order to form an accurate and comprehensive picture of the risks.
	11.5	An AI is only required to conduct appropriate due diligence on the respondent bank, which is its customer, but is not required to do so on the respondent bank's customers.
Cross-border correspondent banking relationships[69]		
Additional measures		
s.14(1), s.14(2)(a), (b) & (c), Sch. 2	11.6	In addition to the CDD measures set out in Chapter 4, an AI should carry out the following additional measures when it establishes a correspondent banking relationship with a respondent bank: (a) collecting sufficient information about the respondent bank to enable it to understand fully the nature of the respondent bank's business; (b) determining from publicly available information the reputation of the respondent bank and the quality of its supervision by

[68] In assessing the ML/TF risks associated with correspondent banking relationships, an AI should refer to Annex II – Correspondent banking in the Basel Committee on Banking Supervision's Guidelines on "Sound management of risks related to money laundering and financing of terrorism" issued in June 2017.

[69] For the purposes of this section, correspondent banking relationships refer to cross-border correspondent banking relationships unless otherwise specified. However, an AI may consider applying the same measures in relation to correspondent banking relationships with other AIs.

		authorities in that place that perform functions similar to those of the HKMA; (c) assessing the AML/CFT controls of the respondent bank; (d) being satisfied that the AML/CFT controls of the respondent bank are adequate and effective; (e) obtaining approval from its senior management; and (f) understanding and documenting clearly its responsibilities and the responsibilities of the respondent bank, including AML/CFT responsibilities.
s.15, Sch. 2	11.7	The extent of additional measures set out in paragraph 11.6 will depend on the nature and characteristics of the correspondent banking services provided and the assessed ML/TF risks presented by the respondent bank. For the avoidance of doubt, an AI should also apply appropriate EDD measures if the correspondent banking relationship with a respondent bank is assessed to be of high ML/TF risk in accordance with the guidance provided in paragraph 4.9.
	11.8	Other factors that an AI should consider in determining the extent of additional measures set out in paragraph 11.6 include, but are not limited to: (a) the respondent bank's major business activities, target markets, customer base and their locations; (b) the ownership and management structures of the respondent bank; (c) the business group to which the respondent bank belongs; (d) the jurisdictions in which the respondent bank, and where applicable, the parent company, subsidiaries and branches of the respondent bank, are located; (e) the quality and effectiveness of AML/CFT and banking regulation as well as supervision in the jurisdictions[70] of the respondent bank; (f) the nature of the services provided to the respondent bank; (g) how the respondent bank will offer services through the correspondent relationship to its customers, including the nature, expected activity level, volume and value of the transactions; and (h) the potential use of the account by other respondent banks in a "nested" correspondent banking relationship[71], including the purpose of the nested relationship and the respondent bank's

[70] In assessing levels of regulation and supervision, consideration may be given to country assessment reports or other information published by international bodies which measures compliance and addresses ML/TF risks (including the FATF, FSRBs, BCBS, IMF and World Bank), lists issued by the FATF in the context of its International Cooperation Review Group process, national risk assessments, public information from national authorities and any restrictive measures imposed on a country, particularly prohibitions on providing correspondent banking services.

[71] Nested correspondent banking relationship refers to the use of an AI's correspondent relationship by a number of respondent banks through their relationships with the AI's direct respondent bank to conduct transactions and obtain access to other financial services.

		control framework with respect to the relationship.
s.7 & s.14, Sch. 2	11.9	Unless an AI has carried out the measures set out in paragraph 11.6 and, if applicable, paragraph 11.13, the AI should not establish a correspondent banking relationship with any institution, or if a correspondent banking relationship has been established, the AI should terminate the relationship with the respondent bank.
	11.10	An AI may collect, and subsequently update, the respondent bank's information by using third-party databases that contain relevant information (i.e. KYC utilities). However, the ultimate responsibility for ensuring that CDD requirements are met remains with the AI.
	11.11	An AI may use an industry questionnaire as a starting point to facilitate the information collection and risk assessment processes.
Payable-through accounts		
	11.12	Particular care should be exercised where the respondent bank allows direct use of the correspondent account by its customers to transact business on their own behalf (i.e. payable-through account). An AI should therefore ascertain whether the correspondent banking services will be used, via payable-through account, by the respondent bank's customers.
s.14(2)(d), Sch. 2	11.13	If a respondent bank allows its customers to directly operate the correspondent accounts maintained with an AI, the AI should be satisfied that the respondent bank: (a) will perform CDD on the customers, including verifying the identities of, and continuously monitoring its business relationships with those customers, in accordance with requirements similar to those imposed under the AMLO; and (b) will be able to provide to the AI, on request, the documents, data or information obtained by the respondent bank in relation to those customers in accordance with requirements similar to those imposed under the AMLO.
Correspondent banking relationships with shell banks		
s.17, Sch.2	11.14	An AI should not establish or continue a correspondent banking relationship with a shell bank. The AI should also take appropriate measures to satisfy itself that its respondent banks do not permit their accounts to be used by shell banks.
s. 17(1), Sch. 2	11.15	A shell bank is a corporation that (a) is incorporated in a place outside Hong Kong; (b) is authorised to carry on banking business in that place; (c) does not have a physical presence in that place; and

		(d) is not affiliated with a regulated financial services group which is subject to effective consolidated supervision.
s. 17(2), Sch. 2	11.16	A corporation has a physical presence[72] in a place or jurisdiction if (a) the corporation carries on banking business at any premises in that place or jurisdiction; and (b) at least one full-time employee of the corporation performs banking-related duties at those premises.
Ongoing monitoring		
s.5(1)(a), Sch.2	11.17	Following paragraph 5.2, an AI should conduct ongoing CDD of its correspondent banking relationships to ensure that the documents, data and information obtained in relation to the respondent banks are up-to-date and relevant. The AI should undertake reviews of the existing records of the respondent banks on a regular basis and upon trigger events. The frequency of periodic review should be determined using an RBA. If the correspondent banking relationship presents high ML/TF risks, it should be subject to a minimum of annual review.
	11.18	An AI should conduct transaction monitoring of its correspondent banking relationships for compliance with targeted financial sanctions and to detect changes in the respondent bank's transaction pattern or any unusual activities[73]. The level and nature of transaction monitoring should be commensurate with the risks and the nature of the correspondent banking services being provided. An AI may refer to Chapter 5 for details.
	11.19	Where, in the course of any review, a respondent bank refuses to provide the required due diligence or transaction information or where the level of risks become higher, an AI should take reasonable measures (e.g. performing more enhanced measures by limiting the services provided, or restricting individual products/transactions, and/or filing a suspicious transaction report) to mitigate the ML/TF risks before considering to terminate the relationship. The AI should consider communicating ~~their~~its concerns to senior management of the respondent bank.
Group-wide considerations		

[72] In general, physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

[73] Where any unusual activities or transactions on the respondent bank are detected, the AI will follow up with the respondent bank by making a request for information, possibly leading to more information being required on a specific customer or customers of the respondent bank. However, there is no expectation, intention or requirement for the AI to conduct CDD on its respondent bank's customers.

	11.20	If an AI relies on its parent bank, head office or foreign branch in establishing a correspondent banking relationship, and the parent bank, head office or foreign branch perform the due diligence and assume responsibilities to conduct assessments and reviews on the correspondent banking relationship, the AI should ensure that the assessments and reviews adopted take into account its own specific circumstances and business arrangements, and the particular correspondent banking relationship in Hong Kong. The AI should still ensure that it complies with the requirements set out in this Guideline and the ultimate responsibility for implementing AML/CFT measures remains with it.
	11.21	If an AI is the head office of a financial group, it should ensure that the ML/TF risk assessments conducted by different group entities are consistent with its group AML/CFT policy. The AI should also coordinate among different group entities the monitoring of the correspondent banking relationships with the same respondent bank, particularly in the case of a high-risk relationship, and ensure that adequate information-sharing mechanism is in place within the group.
	11.22	If an AI has correspondent banking relationships with several respondent banks in different jurisdictions but belonging to the same financial group, the AI should take into account that these respondent banks belong to the same financial group in its ML/TF risk assessment. Nevertheless, the AI should also independently assess each correspondent banking relationship.
Other similar relationships		
	11.23	While the AMLO only requires an AI to conduct additional measures set out in ~~paragraph~~paragraphs 11.6 and 11.13 (if applicable) when it establishes a cross-border correspondent banking relationship with a respondent bank, the AI should also conduct these additional measures when it provides services that are similar to correspondent banking (correspondent services) to other FIs (e.g. money or value transfer service (MVTS) providers) and virtual asset service providers (VASPs)[74] located outside Hong Kong.
	11.24	Where a customer is an FI or a VASP located outside Hong Kong, an AI should ascertain whether the FI or the VASP intends to use the account maintained with the AI for its own corporate or settlement purposes, or whether it intends to use the account to provide correspondent services to its own customers. Where the FI or the VASP offers correspondent services for its own customers through its account, the AI should carry out additional measures ~~on~~

[74] For the purpose of this Chapter, the term "virtual asset service provider" has the same definition as set out in the FATF Recommendations.

		~~the FI~~ set out in ~~paragraph~~paragraphs 11.6 and 11.13 on the FI or the VASP (where applicable).
	11.25	To facilitate effective monitoring of these two types of activities which present different levels of ML/TF risks, an AI could consider encouraging or requiring a customer that is an FI or a VASP located outside Hong Kong to open one account for conducting its own corporate or settlement activities, and another separate account for providing correspondent ~~banking~~ services for its customers.
Non-customer SWIFT RMA relationships		
	11.26	While the mere exchange of SWIFT RMA keys in the context of non-customer relationships is not a correspondent banking relationship, an AI should have appropriate policies and procedures to manage its non-customer SWIFT RMA relationships on an ongoing basis.

Chapter 12 – PRIVATE BANKING		
General		
	12.1	The characteristics of private banking relationships can represent an increased risk of ML/TF. On the whole, private banking is more complex and provides a more personalised service than retail banking. A unique characteristic of private banking is the close relationship between customer and relationship manager (RM) and the "all inclusive" money management services provided.
	12.2	An AI should therefore ensure that it understands and manages the risks accordingly and make special provisions for private banking customers in its customer acceptance, CDD procedures and in its ongoing monitoring programmes.
CDD process for private banking		
	12.3	Generally, given the potentially higher ML/TF risks presented by private banking relationships, the level of due diligence carried out for a private banking relationship will be higher than that needed for normal retail banking purposes. Therefore, in addition to the CDD measures set out in Chapter 4, an AI should carry out the following additional measures when it establishes a private banking relationship with a customer: (a) obtain additional customer profile information, including: (i) business or employment background; (ii) source of wealth (see paragraph 4.9.~~22);~~24); (iii) source of funds (see paragraph 4.9.~~23);~~25); (iv) family background, e.g. information on spouse, and where appropriate (e.g. in the case of inherited wealth), parents; and (v) anticipated account activity (e.g. products and services to be utilised by the customer; nature and level of business to be expected); and ~~(vi) references, where appropriate (e.g. introduced by whom and when and the length of relationship) or other sources to corroborate reputation information where available; and~~ (b) obtaining approval from the AI's senior management.
	12.4	The extent of additional measures as set out in paragraph 12.3 will depend on the nature and characteristics of the private banking services provided and the assessed ML/TF risk presented by the customer[75]. For the avoidance of doubt, an AI should also apply appropriate EDD measures if the private banking relationship with

[75] For example, an AI should determine whether walk-in customers require a higher degree of due diligence prior to account opening.

		a customer is assessed to be of high ML/TF risk in accordance with the guidance provided in paragraph 4.9.
	12.5	For private banking, an AI should take reasonable steps on a risk-based approach to verify or corroborate information collected on source of wealth and source of funds. This means that, in the case of source of wealth, the steps taken should be sufficient to form a reasonable belief of how the wealth, or the majority of the wealth was acquired by the customer. The reasonable steps taken will therefore vary depending on the ML/TF risks.
	12.6	An AI should perform adverse news screening on a potential customer, and any other persons known by the AI to be associated with the customer as far as practicable, before establishing the private banking relationship. The screening helps identify potentially questionable relationships for further examination and evaluation.
	12.7	Complex corporate structure and vehicles often exist in private banking (e.g. use of offshore trust or shell companies; structure involving different jurisdictions). While using these structures may have a genuine and legitimate purpose, an AI should have appropriate policies and procedures in place to understand the reason and purpose for these structures, including any additional CDD measures required.
	12.8	Meeting the customer is an important part of the overall CDD process and will assist in constructing a more comprehensive customer risk profile. In general, given the potentially higher ML/TF risks presented by private banking relationships, an AI should meet the customer before establishing a private banking relationship as far as possible. Meetings can take place in or out of Hong Kong. The AI can use technology to facilitate the meeting providing adequate safeguards are in place.
Ongoing monitoring		
	12.9	Following paragraph 5.2, an AI should conduct ongoing CDD of its private banking relationships to ensure that the documents, data and information obtained in relation to the customers are up-to-date and relevant. The AI should undertake a review of the existing records of its private banking customers on a regular basis and upon trigger events. The frequency of periodic review should be determined using an RBA. If the private banking relationship presents high ML/TF risks, it should be subject to a minimum of annual review.
	12.10	An AI should meet their private banking customers on a regular basis as far as possible.

	12.11	An AI should conduct transaction monitoring of its private banking relationships. The level and nature of transaction monitoring should be commensurate with the risks and the nature of the private banking services being provided. The AI may refer to Chapter 5 for details.
Dedicated relationship management		
	12.12	As close relationships often develop between RMs and their customers, in order to mitigate the risk of ML/TF, the activities of RMs should be subject to frequent reporting to and review by their supervisors. An AI should also ensure that the account opening, including CDD documentation, adequacy of CDD and ongoing monitoring are subject to reviews conducted by staff independent of the RMs to demonstrate that any risks of abuse and/or conflict of interest are effectively mitigated.

GLOSSARY OF KEY TERMS AND ABBREVIATIONS	
Terms / abbreviations	**Meaning**
AI(s)	Authorized Institution(s)
AMLO	Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)
AML/CFT	Anti-money laundering and counter-financing of terrorism
AML/CFT Systems	AML/CFT policies, procedures and controls
BO	Banking Ordinance (Cap.155)
CDD	Customer due diligence
CO	Compliance officer
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
EDD	Enhanced due diligence
FATF	Financial Action Task Force
FI(s)	Financial institution(s) (Note: unless specified otherwise (e.g. an FI as defined in the AMLO), the term "financial institutions (FIs)" has the same definition as set out in the FATF Recommendations.)
HKMA	Hong Kong Monetary Authority
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
RI(s)	Registered Institution(s), which is an Authorized Institution

	registered under the Securities and Futures Ordinance to conduct securities intermediary activities.
Schedule 2	Schedule 2 to the AMLO
SDD	Simplified due diligence
STR(s)	Suspicious transaction report(s)
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)