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

Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers)

June 2023

April 2012 first edition
July 2012 second edition
April 2015 third edition
March 2018 fourth edition
November 2018 fifth edition
September 2021 sixth edition
June 2023 seventh edition

Published by
Securities and Futures Commission
54/F, One Island East
18 Westlands Road
Quarry Bay
Hong Kong
Tel : (852) 2231 1222
Fax : (852) 2521 7836
E-mail : enquiry@sfc.hk
SFC website : www.sfc.hk

Content

Chapter 1 – OVERVIEW

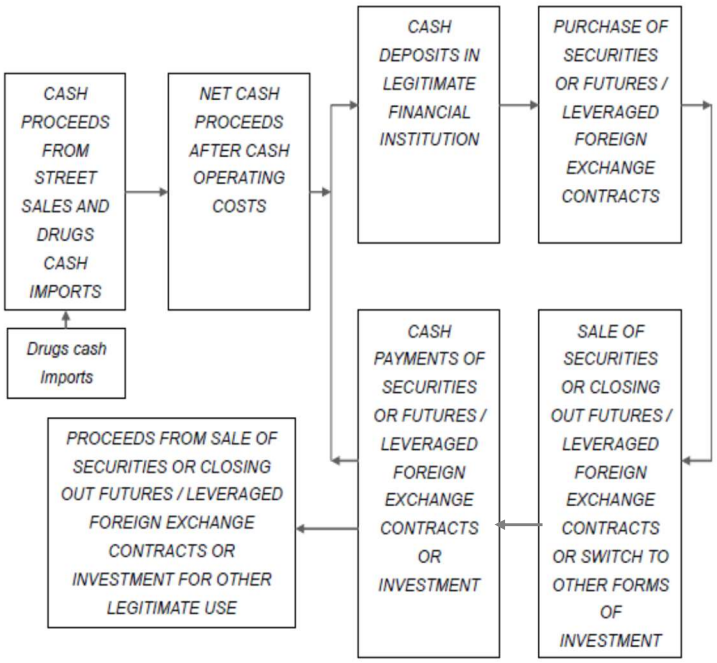
Introduction		
	1.1	This Guideline is published under sections 7 and 53ZTK of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (the AMLO), and section 399 of the Securities and Futures Ordinance, Cap. 571 (the SFO).
	1.2	Terms and abbreviations used in this Guideline shall be interpreted by reference to the definitions set out in the Glossary part of this Guideline.
	1.3	Where applicable, interpretation of other words or phrases should follow those set out in the AMLO or the SFO. Unless the context otherwise requires, the term financial institutions (FIs) refers to licensed corporations (LCs) and virtual asset service providers licensed by the Securities and Futures Commission (SFC) under the AMLO (SFC-licensed VAS Providers).
	1.4	This Guideline is issued by the SFC and sets out the relevant anti-money laundering and counter-financing of terrorism (AML/CFT) statutory and regulatory requirements, and the AML/CFT standards which LCs and SFC-licensed VAS Providers should meet in order to comply with the statutory requirements under the AMLO and the SFO. Compliance with this Guideline is enforced through the AMLO and the SFO. LCs and SFC-licensed VAS Providers which fail to comply with this Guideline may be subject to disciplinary or other actions under the AMLO and/or the SFO for non-compliance with the relevant requirements.
	1.5	This Guideline is intended for use by FIs and their officers and staff. This Guideline also: (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 FIs and their senior management in designing and implementing their own policies, procedures and controls in the relevant operational areas, taking into consideration their special circumstances so as to meet the relevant AML/CFT statutory and regulatory requirements.
	1.6	In addition to the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) issued by the Hong Kong Monetary Authority (HKMA) for use by authorized institutions, registered institutions (RIs) are required to have regard to paragraph 4.1.6 of this Guideline for the definition of "customer" for the securities, futures and leveraged foreign exchange businesses (hereafter collectively referred to as "securities sector" or "securities businesses"), paragraphs 4.20 of this Guideline for the provisions on cross-border correspondent relationships applicable to the securities sector, Chapter 12 of this Guideline for the provisions in relation to virtual assets, and Appendix B to this Guideline for illustrative indicators of suspicious transactions and activities in the securities sector.
	1.7	The relevance and usefulness of this Guideline will be kept under review and it may be necessary to issue amendments from time to time.
	1.8	For the avoidance of doubt, the use of the word "must" or "should" in relation to an action, consideration or measure referred to in this Guideline indicates that it is a mandatory requirement. Given the significant differences that exist in the organisational and legal structures of different FIs as well as the nature and scope of the business activities conducted by them, there exists no single

		set of universally applicable implementation measures. The content of this Guideline is not intended to be an exhaustive list of the means of meeting the statutory and regulatory requirements. FIs therefore should use this Guideline as a basis to develop measures appropriate to their structure and business activities.
	1.9	This Guideline also provides guidance in relation to the operation of the provisions of Schedule 2 to the AMLO (Schedule 2).
s.7 & s.53ZTK(5) & (6)(b), AMLO, s.399(6), SFO	1.10	A failure by any person to comply with any provision of this Guideline does not by itself render the person liable to any judicial or other proceedings but, in any proceedings under the AMLO or the SFO before any court, this Guideline is admissible in evidence; and if any provision set out in this Guideline appears to the court to be relevant to any question arising in the proceedings, the provision must be taken into account in determining that question. In considering whether a person has contravened a provision of Schedule 2, the SFC must have regard to any relevant provision in this Guideline.
s.193 & s.194, SFO, s.53ZTK (6)(a), AMLO	1.11	In addition, a failure to comply with any of the requirements of this Guideline by LCs or SFC-licensed VAS Providers and (where applicable) licensed representatives may reflect adversely on their fitness and properness and may be considered to be misconduct.
s.193 & s.196, SFO	1.12	Similarly, a failure to comply with any of the requirements of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) issued by the HKMA for use by authorized institutions or to have regard to paragraphs 4.1.6 and 4.20 of, Chapter 12 of, and Appendix B to this Guideline by RIs may reflect adversely on their fitness and properness and may be considered to be misconduct.

The nature of money laundering and terrorist financing		
s.1, Sch. 1, AMLO	1.13	The term "money laundering" is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means an act intended to have the effect of making any property: (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.
	1.14	There are three common stages in the laundering of money, and they frequently involve numerous transactions. An FI should be alert to any such sign for potential criminal activities. These stages are: (a) Placement - the disposal of cash proceeds derived from illegal activities into the financial system; (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.
Potential uses of the securities sector in the money laundering process		
	1.15	Since the securities businesses are no longer

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

		in detail.  Other examples of money laundering methods and characteristics of financial transactions that have been linked with terrorist financing can be found on the websites of the Joint Financial Intelligence Unit (JFIU) (www.jfiu.gov.hk) and the Financial Action Task Force (FATF) (www.fatf-gafi.org).
s.1, Sch. 1, AMLO	1.20	The term “terrorist financing” 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); or (b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or

		(c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.
	1.21	Terrorists or terrorist organisations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.
Legislation concerned with ML, TF, financing of proliferation of weapons of mass destruction (PF) and financial sanctions		
	1.22	The FATF is an inter-governmental body established in 1989. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating of ML, TF, PF, and other related threats to the integrity of the international financial system. The FATF has developed a series of Recommendations that are recognised as the international standards for combating of ML, TF and PF. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. In order to ensure full and effective implementation of its standards at the global level, the FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow-up after the evaluations, including identifying high risk and other monitored jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large. Many major economies have joined the FATF which has developed into a global network for international

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

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

		provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If the FI contravenes a specified provision with the intent to defraud any RA, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.
s.5, AMLO	1.26	The AMLO also makes it a criminal offence if a person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI (1) knowingly; or (2) with the intent to defraud the FI or any RA, causes or permits the FI to contravene a specified provision in the AMLO. If the person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI knowingly contravenes a specified provision, he is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If that person does so with the intent to defraud the FI or any RA, he is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.
s.21 & s.53ZSP, AMLO	1.27	RAs may take disciplinary actions against FIs for any contravention of a specified provision in the AMLO. The disciplinary actions that can be taken include publicly reprimanding the FI; ordering the FI to take any action for the purpose of remedying the contravention; and ordering the FI to pay a pecuniary penalty not exceeding the greater of $10 million or 3 times the amount of profit gained, or costs avoided, by the FI as a result of the contravention.
<u>DTROP</u>		
	1.28	The DTROP contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction.

OSCO		
	1.29	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		
	1.30	The UNATMO is principally directed towards implementing decisions contained in relevant United Nations Security Council Resolutions (UNSCRs) aimed at preventing the financing of terrorist acts and combating the threats posed by foreign terrorist fighters. Besides the mandatory elements of the relevant UNSCRs, the UNATMO also implements the more pressing elements of the FATF Recommendations specifically related to TF.
s.25, DTROP & OSCO	1.31	Under the DTROP and the OSCO, a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking or of an indictable offence respectively. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine of $5 million.
s.6, s.7, s.8, s.8A,	1.32	The UNATMO, among other things, criminalises the

s.13 & s.14, UNATMO		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 & s.14, UNATMO	1.33	The DTROP, the OSCO and the UNATMO also make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly, represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property respectively. This offence carries a maximum term of imprisonment of 3 months and a fine of $50,000 upon conviction.
s.25A, DTROP & OSCO, s.12 & s.14, UNATMO	1.34	"Tipping-off" is another offence under the DTROP, the OSCO and the UNATMO. A person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following that first-mentioned disclosure. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.
<u>UNSO</u>		
	1.35	The UNSO provides for the imposition of sanctions against persons and against places outside the People's Republic of China arising from Chapter 7 of the Charter of the United Nations. Most UNSCRs are implemented in Hong Kong under the UNSO.
<u>WMD(CPS)O</u>		
s.4, WMD(CPS)O	1.36	The WMD(CPS)O controls the provision of services that will or may assist the development, production, acquisition or stockpiling of weapons capable of causing mass destruction or that will or may assist

		the means of delivery of such weapons. Section 4 of WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

Chapter 2 – RISK-BASED APPROACH

Introduction		
	2.1	Applying an AML/CFT risk-based approach (RBA) is recognised as an effective way to combat ML/TF. The RBA to AML/CFT means that countries, competent authorities and FIs should identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures that are commensurate with those risks in order to mitigate them effectively. The use of an RBA allows an FI to allocate its resources in the most efficient way in accordance with priorities so that the greatest risks receive the highest attention. Therefore, FIs should have in place a process to identify, assess and understand the ML/TF risks to which they are exposed (hereafter referred to as "institutional risk assessment"), so as to facilitate the design and implementation of adequate and appropriate internal AML/CFT policies, procedures and controls (hereafter collectively referred to as "AML/CFT Systems"[2]) that are commensurate with the ML/TF risks identified in order to properly manage and mitigate them. FIs should also assess the ML/TF risks associated with a customer or proposed business relationship (hereafter referred to as "customer risk assessment") to determine the degree, frequency or extent of CDD measures and ongoing monitoring conducted which should vary in accordance with the assessed ML/TF risks associated with the customer or business relationship[3].

[2] Guidance on AML/CFT Systems is provided in Chapter 3.

[3] Illustrative examples of possible simplified and enhanced measures are set out in paragraphs 1 and 2 of Appendix C respectively.

Institutional risk assessment		
	2.2	An institutional risk assessment enables an FI to understand how, and to what extent, it is vulnerable to ML/TF.
	2.3	An FI should take appropriate steps to identify, assess, and understand its ML/TF risks which should include: (a) considering all relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigating measures to be applied (see paragraphs 2.6 to 2.8); (b) keeping the risk assessment up-to-date (see paragraph 2.9); (c) documenting the risk assessment (see paragraph 2.10); (d) obtaining the approval of senior management of the risk assessment results (see paragraph 2.11); and (e) having appropriate mechanisms to provide risk assessment information to RAs upon request.
	2.4	In conducting the institutional risk assessment, an FI should consider quantitative and qualitative information obtained from relevant internal and external sources to identify, manage and mitigate the risks. This may include consideration of relevant risk assessments and guidance issued by the FATF, inter-governmental organisations, governments and authorities from time to time, including Hong Kong's jurisdiction-wide ML/TF risk assessment and any higher risks notified to the FIs by the SFC.
	2.5	The nature and extent of institutional risk assessment procedures should be commensurate with the nature, size and complexity of the business of an FI. For FIs whose businesses are smaller in size or less complex in nature (for example, where the range of products and services offered by the FI are very

		limited or its customers have a homogeneous risk profile), a simpler risk assessment approach might suffice. Conversely, where the FI's products and services are more varied and complex, or the FI's customers have more diverse risk profiles, a more sophisticated risk assessment process will be required.
<u>Considering relevant risk factors</u>		
	2.6	An FI should holistically take into account relevant risk factors including country risk, customer risk, product/service/transaction risk, delivery/distribution channel risk and, where applicable, other risks that the FI is exposed to, depending on its specific circumstances. While there is no complete set of risk indicators, the list of illustrative risk indicators set out in Appendix A may help identify a higher or lower level of risk associated with the risk factors stated above that may be present in the business operations of an FI or its customer base and should be taken into account holistically whenever relevant in the institutional risk assessment.
	2.7	In determining the level of overall risk that the FI is exposed to, an FI should holistically consider a range of factors, including: (a) country risk, for example, the jurisdictions in which the FI is operating or otherwise exposed to, either through its own activities or the activities of customers, especially jurisdictions with greater vulnerability due to contextual and other risk factors such as: (i) the prevalence of crime, corruption, or financing of terrorism; (ii) the general level and quality of the jurisdiction's law enforcement efforts related to AML/CFT; (iii) the regulatory and supervisory regime and controls; and

		(iv) transparency of beneficial ownership[4]; (b) customer risk, for example, the proportion of customers identified as high risk; (c) product/service/transaction risk, for example, (i) the characteristics of the products and services that it offers and transactions it executes, and the extent to which these are vulnerable to ML/TF abuse; (ii) the nature, diversity and complexity of its business, products and target markets; and (iii) whether the volume and size of transactions are in line with the usual activity of the FI and the profile of its customers; (d) delivery/distribution channel risk, for example, the distribution channels through which the FI distributes its products, including: (i) the extent to which the FI deals directly with the customer, the extent to which it relies on third parties to conduct CDD or other AML/CFT obligations and the extent to which the delivery/distribution channels are vulnerable to ML/TF abuse; and (ii) the complexity of the transaction chain (e.g. layers of distribution and sub-distribution); and (e) other risks, for example, the review results of compliance, internal and external audits, as well as regulatory findings.
	2.8	An FI should also identify and assess the ML/TF risks that may arise in relation to: (a) the development of new products and new business practices, including new delivery mechanisms (especially those that may lead to misuse of technological developments or facilitate anonymity in ML/TF schemes); and (b) the use of new or developing technologies for

[4] For example, the availability of adequate, accurate and timely information on the beneficial ownership of legal persons and legal arrangements that can be obtained or accessed in a timely fashion by competent authorities in the country.

		both new and pre-existing products, prior to the launch of the new products, new business practices or the use of new or developing technologies. The FI should take appropriate measures to mitigate and manage the risks identified.
<u>Keeping risk assessment up-to-date</u>		
	2.9	An FI should review the institutional risk assessment at least every 2 years, or more frequently upon trigger events with material impact on the firm's business and risk exposure (e.g. a significant breach of the FI's AML/CFT Systems, the acquisition of new customer segments or delivery channels, the launch of new products and services by the FI, or a significant change of the FI's operational processes).
<u>Documenting risk assessment</u>		
	2.10	An FI should maintain records and relevant documents of the institutional risk assessment, including the risk factors identified and assessed, the information sources taken into account, and the evaluation made on the adequacy and appropriateness of the FI's AML/CFT Systems.
<u>Obtaining senior management approval</u>		
	2.11	The institutional risk assessment should be communicated to, reviewed and approved by the senior management of the FI.
<u>Other considerations</u>		
	2.12	A Hong Kong-incorporated FI with overseas branches and subsidiary undertakings that carry on the same business as an FI as defined in the AMLO should conduct a group-wide ML/TF risk assessment, to facilitate the FI to design and implement group-wide AML/CFT Systems as referred to in paragraph 3.13.

		If an FI 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 the ML/TF risks posed to the FI in the local context.
Customer risk assessment		
	2.13	An FI should assess the ML/TF risks associated with a customer or a proposed business relationship. The information obtained in the initial stages of the CDD process should enable an FI to conduct a customer risk assessment, which would determine the level of CDD measures[5] to be applied. The measures must however comply with the legal requirements of the AMLO[6]. The general principle is that the amount and type of information obtained, and the extent to which this information is verified, should be increased where the risk associated with the business relationship is higher, or may be decreased where the associated risk is lower.
	2.14	Based on a holistic view of the information obtained in the course of performing CDD measures, an FI should be able to finalise the customer risk assessment, which determines the level and type of ongoing monitoring (including keeping customer information up-to-date and transaction monitoring), and supports the decision of the FI whether to enter into, continue or terminate the business relationship. While a customer risk assessment should always be

[5] Illustrative examples of possible simplified and enhanced measures are set out in paragraphs 1 and 2 of Appendix C respectively.

[6] FIs should have regard, in particular, to section 4 of Schedule 2 which permits FIs not to identify and take reasonable measures to verify the identities of the beneficial owners of specific types of customers, or in relation to specific types of products related to the transactions of the customers; and sections 8 to 15 of Schedule 2 which require FIs to comply with some special requirements in relation to specific types of customers, products, transactions or other high risk situations. Further guidance is set out in Chapter 4.

		performed at the inception of a business relationship with a customer, a comprehensive risk profile for some customers may only become evident through time or based upon information received from a competent authority after establishing the business relationship. Therefore, an FI may have to periodically review and, where appropriate, update its risk assessment of a particular customer and adjust the extent of the CDD and ongoing monitoring to be applied to the customer.
	2.15	An FI should keep its policies and procedures under regular review and assess that its risk mitigation procedures and controls are working effectively.
<u>Conducting risk assessment</u>		
	2.16	An FI may assess the ML/TF risks of a customer by assigning a ML/TF risk rating to its customers.
	2.17	Similar to other parts of the AML/CFT Systems, an FI should adopt an RBA in the design and implementation of its customer risk assessment framework, and the framework should be designed taking into account the results of the institutional risk assessment of the FI and commensurate with the risk profile and complexity of its customer base. The customer risk assessment should holistically take into account relevant risk factors of a customer including the country risk, customer risk, product/service/transaction risk, and delivery/distribution channel risk. While there is no agreed upon set of indicators, the list of illustrative risk indicators set out in Appendix A may identify a higher or lower level of risk associated with the risk factors stated above and should be taken into account holistically whenever relevant in determining the ML/TF risk rating of a customer.

Documenting risk assessment		
s.20(1)(b)(ii), Sch. 2	2.18	An FI should keep records and relevant documents of the customer risk assessment so that it can demonstrate to the RAs, among others: (a) how it assesses its 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.

Chapter 3 – AML/CFT SYSTEMS

Introduction		
s.23(a) & (b), Sch. 2	3.1	An FI must take all reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML/TF and to prevent a contravention of any requirement under Part 2 or 3 of Schedule 2. To ensure compliance with this requirement, an FI should implement appropriate AML/CFT Systems that are commensurate with the risks identified in its risk assessments.
	3.2	An FI should: (a) have AML/CFT Systems, which are approved by senior management, to enable the FI to manage and mitigate the risks that have been identified; (b) monitor the implementation of the AML/CFT Systems and make enhancements if necessary; and (c) implement enhanced AML/CFT Systems to manage and mitigate the risks where higher risks are identified[7].
	3.3	An FI may implement simplified AML/CFT Systems to manage and mitigate the risks if lower risks are identified, provided that: (a) the FI complies with the statutory requirements set out in Schedule 2; (b) the lower ML/TF risk assessment is supported by an adequate analysis of risks having regard to the relevant risk factors and risk indicators; (c) the simplified AML/CFT Systems are commensurate with the lower ML/TF risks

[7] Depending on the assessed ML/TF risks, RBA may be applied on a specific customer segment, a specific line of business, or a specific product or service offered. For example, where a line of business is assessed to carry higher ML/TF risks, the FI should implement enhanced AML/CFT Systems with respect to the specific line of business (e.g. more frequent internal audit review or more frequent reporting to senior management).

		identified; and (d) the simplified AML/CFT Systems, which are approved by senior management, are subject to review from time to time. For the avoidance of doubt, an FI must not implement simplified AML/CFT Systems whenever there is any suspicion of ML/TF.
AML/CFT Systems		
	3.4	Having regard to the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses, an FI should implement adequate and appropriate AML/CFT Systems which should include: (a) compliance management arrangements; (b) independent audit function; (c) employee screening procedures; and (d) an ongoing employee training programme (see Chapter 9).
Compliance management arrangements		
	3.5	An FI should have appropriate compliance management arrangements that facilitate the FI to implement AML/CFT Systems to comply with relevant legal and regulatory obligations as well as to manage ML/TF risks effectively. Compliance management arrangements should, at a minimum, include oversight by the FI's senior management, and appointment of a Compliance Officer (CO) and a Money Laundering Reporting Officer (MLRO)[8].
Senior management oversight		
	3.6	The senior management of an FI is responsible for implementing effective AML/CFT Systems that can adequately manage the ML/TF risks identified. In

[8] The role and functions of an MLRO are detailed in paragraphs 3.9, 7.9, 7.13 to 7.25. Depending on the size of an FI, the functions of the CO and the MLRO may be performed by the same staff member. The Manager-In-Charge of Core Function responsible for managing the Anti-Money Laundering and Counter-Terrorist Financing function of the FI (i.e. MIC of AML/CFT) can be the CO provided that the requirements set out in paragraphs 3.7 and 3.8 are met.

		particular, the senior management should: (a) appoint a CO at the senior management level to have the overall responsibility for the establishment and maintenance of the FI's AML/CFT Systems; and (b) appoint a senior staff member as the MLRO to act as the central reference point for suspicious transaction reporting.
	3.7	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 FI, independent of all operational and business functions; (c) normally based in Hong Kong; (d) of a sufficient level of seniority and authority within the FI; (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 FI's statutory and regulatory requirements and the ML/TF risks arising from the FI'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 RAs); 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).

Compliance officer and money laundering reporting officer		
	3.8	The principal function of the CO is to act as the focal point within an FI for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the senior management to ensure that ML/TF risks are adequately identified, understood and managed. In particular, the CO should assume responsibility for: (a) developing and/or continuously reviewing the FI's AML/CFT Systems, including (where applicable) any group-wide AML/CFT Systems in the case of a Hong Kong-incorporated FI, to ensure they remain up-to-date, meet current statutory and regulatory requirements, and are effective in managing ML/TF risks arising from the FI's business; (b) overseeing all aspects of the FI'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.
	3.9	An FI should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the JFIU and law enforcement agencies. The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions of the MLRO should include having oversight of: (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 records related to such internal reviews; and

		(c) provision of guidance on how to avoid tipping-off.
Independent audit function		
	3.10	Where practicable, an FI should establish an independent audit function which should have a direct line of communication to the senior management of the FI. Subject to appropriate segregation of duties, the function should have sufficient expertise and resources to enable it to carry out an independent review of the FI's AML/CFT Systems.
	3.11	The audit function should regularly review the AML/CFT Systems to ensure effectiveness. This would include evaluating, among others: (a) the adequacy of the FI's AML/CFT Systems, ML/TF risk assessment framework and application of risk-based approach; (b) the effectiveness of the system for recognising and reporting suspicious transactions; (c) whether instances of non-compliance are reported to senior management on a timely basis; and (d) the level of awareness of staff having AML/CFT responsibilities. The frequency and extent of the review should be commensurate with the nature, size and complexity of the FI's businesses and the ML/TF risks arising from those businesses. Where appropriate, the FI should seek a review from external parties.
Employee screening		
	3.12	FIs should have adequate and appropriate screening procedures in order to ensure high standards when hiring employees.
Group-wide AML/CFT Systems		
s.22(1), Sch. 2	3.13	Subject to paragraphs 3.14 and 3.15, a Hong Kong-incorporated FI with overseas branches or subsidiary

		undertakings that carry on the same business as an FI as defined in the AMLO should implement group-wide AML/CFT Systems[9] to apply the requirements set out in this Guideline to all of its overseas branches and subsidiary undertakings in its financial group, wherever the requirements in this Guideline are relevant and applicable to the overseas branches and subsidiary undertakings concerned. In particular, a Hong Kong-incorporated FI should, through its group-wide AML/CFT Systems, ensure that all of its overseas branches and subsidiary undertakings that carry on the same business as an FI as defined in the AMLO, have procedures in place to ensure compliance with the CDD and record-keeping requirements similar to those imposed under Parts 2 and 3 of Schedule 2, to the extent permitted by the laws and regulations of that place.
	3.14	If the AML/CFT requirements in the jurisdiction where the overseas branch or subsidiary undertaking of a Hong Kong-incorporated FI is located (host jurisdiction) differ from those relevant requirements referred to in paragraph 3.13, the FI should require that branch or subsidiary undertaking to apply the higher of the two sets of requirements, to the extent that the host jurisdiction's laws and regulations permit.
s.22(2), Sch. 2	3.15	If the host jurisdiction's laws and regulations do not permit the branch or subsidiary undertaking of a Hong Kong-incorporated FI to apply the higher AML/CFT requirements, particularly the CDD and record-keeping requirements imposed under Parts 2 and 3 of Schedule 2, the FI should: (a) inform the RA of such failure; and (b) take additional measures to effectively mitigate

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

		ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the requirements.
	3.16	To the extent permitted by the laws and regulations of the jurisdictions involved and subject to adequate safeguards on the protection of confidentiality and use of information being shared, including safeguards to prevent tipping-off, a Hong Kong-incorporated FI should also implement 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 FI's group-level compliance, audit and/or AML/CFT functions, of customer, account, and transaction information from its overseas branches and subsidiary undertakings that carry on the same business as an FI as defined in the AMLO, when necessary for AML/CFT purposes[10].

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

Chapter 4 - CUSTOMER DUE DILIGENCE

4.1 What CDD measures are and when they must be carried out		
General		
s.19(3), Sch. 2	4.1.1	The AMLO defines what CDD measures are (see paragraph 4.1.4) and also prescribes the circumstances in which an FI must carry out CDD (see paragraph 4.1.9). This Chapter provides guidance in this regard. Wherever possible, this Guideline gives FIs a degree of discretion in how they comply with the AMLO and put in place procedures for this purpose. In addition, an FI should, in respect of each kind of customer, business relationship, product and transaction, establish and maintain effective AML/CFT Systems for complying with the CDD requirements set out in this Chapter.
	4.1.2	As stated in Chapter 2, FIs should determine the extent of CDD measures using an RBA, taking into account the higher or lower ML/TF risks identified in the customer risk assessment conducted by the FIs, so that preventive or mitigating measures are commensurate with the risks identified [11]. The measures must however comply with the legal requirements of the AMLO. FIs should also have regard to section 4 of Schedule 2 which permits FIs not to identify and take reasonable measures to verify the identities of the beneficial owners of specific types of customers, or in relation to specific types of products related to the transactions of the customers (see paragraphs 4.8); and sections 8 to 15 of Schedule 2 which require FIs to comply with some special requirements in relation to specific types of customers, products, transactions or other high risk situations (see paragraphs 4.9 to 4.14).

[11] Illustrative examples of possible simplified and enhanced measures are set out in paragraphs 1 and 2 of Appendix C respectively.

What CDD measures are		
	4.1.3	CDD information is a vital tool for recognising whether there are grounds for knowledge or suspicion of ML/TF.
s.2(1), Sch. 2	4.1.4	The following are CDD measures applicable to an FI: (a) identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source (see paragraphs 4.2); (b) where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity so that the FI is satisfied that it knows who the beneficial owner is, including, in the case of a legal person or trust, measures to enable the FI to understand the ownership and control structure of the legal person or trust (see paragraphs 4.3); (c) obtain information on the purpose and intended nature of the business relationship (if any) established with the FI unless the purpose and intended nature are obvious (see paragraphs 4.6); and (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 paragraphs 4.4).
	4.1.5	The term "customer" is defined in the AMLO to include a client. The meaning of "customer" and "client" should be inferred from its everyday meaning and in the context of the industry practice.

	4.1.6	Unless the context otherwise requires, for the securities sector, the term "customer" refers to a person who is a client of an LC and the term "client" is as defined in section 1 of Part 1 of Schedule 1 to the SFO. For SFC-licensed VAS Providers, the term "customer" refers to a person to whom the SFC-licensed VAS Provider provides services in the course of providing a VA service as defined in section 53ZR of the AMLO. The phrase "potential customer" in the term "business relationship" is to be construed accordingly as meaning "potential client".
	4.1.7	In determining what constitutes reasonable measures to verify the identity of a beneficial owner and reasonable measures to understand the ownership and control structure of a legal person or trust, the FI should consider and give due regard to the ML/TF risks posed by a particular customer and a particular business relationship. Due consideration should also be given to the guidance in relation to customer risk assessment set out in Chapter 2.
	4.1.8	FIs should adopt a balanced and common sense approach with regard to customers connected with jurisdictions posing a higher risk (see paragraphs 4.13). While extra care may well be justified in such cases, unless an RA has, through a "notice in writing", imposed a general or specific requirement (see paragraph 4.14.2), it is not a requirement that FIs should refuse to do any business with such customers or automatically classify them as high risk and subject them to the special requirements set out in section 15 of Schedule 2. Rather, FIs should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/TF.

When CDD measures must be carried out		
s.3(1) & (1A), Sch. 2	4.1.9	An FI must carry out CDD measures in relation to a customer: (a) before establishing a business relationship with the customer; (b) before carrying out for the customer an occasional transaction[12]: (i) involving an amount equal to or above $120,000 or an equivalent amount in any other currency; or (ii) that is a wire transfer involving an amount equal to or above $8,000 or an equivalent amount in any other currency; whether the transaction is carried out in a single operation or in several operations that appear to the FI to be linked[13]; (c) when the FI suspects that the customer or the customer's account is involved in ML/TF[14]; or (d) when the FI doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.
s.1, Sch. 2	4.1.10	"Business relationship" between a person and an FI is defined in the AMLO as a business, professional or commercial relationship: (a) that has an element of duration; or (b) that the FI, at the time the person first contacts it in the person's capacity as a potential customer of the FI, expects to have an element of duration.
s.1, Sch. 2	4.1.11	The term "occasional transaction" is defined in the AMLO as a transaction between an FI and a

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

[13] FIs should also refer to the guidance provided in paragraphs 12.3 for occasional transactions in the context of virtual assets.

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

		customer who does not have a business relationship with the FI[15].
	4.1.12	FIs should be vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD thresholds of $8,000 for wire transfers and $120,000 for other types of transactions. Where FIs become aware that these thresholds are met or exceeded, CDD measures must be carried out.
	4.1.13	The factors linking occasional transactions are inherent in the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over a short period, where a customer regularly transfers funds to one or more destinations. In determining whether the transactions are in fact linked, FIs should consider these factors against the timeframe within which the transactions are conducted.
4.2 Identification and verification of the customer's identity		
s.2(1)(a), Sch. 2	4.2.1	The FI must identify the customer and verify the customer's identity by reference to documents, data or information provided by: (a) a governmental body; (b) the RA or any other RA; (c) an authority in a place outside Hong Kong that performs functions similar to those of the RA or any other RA; (d) a digital identification system that is a reliable and independent source that is recognised by the RA[16]; or (e) any other reliable and independent source that

[15] It should be noted that FIs that are LCs or SFC-licensed VAS Providers should not carry out "occasional transactions".

[16] The SFC recognises iAM Smart, developed and operated by the Hong Kong Government, as a digital identification system that can be used for identity verification of natural persons. The SFC may in future recognise other similar digital identification systems developed and operated by governments in other jurisdictions having regard to market developments and specific circumstances.

		is recognised by the RA.
Customer that is a natural person[17]		
s.2(1)(a), Sch. 2	4.2.2	For a customer that is a natural person, FIs should identify the customer by obtaining at least the following identification information: (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	4.2.3	In verifying the identity of a customer that is a natural person, an FI should verify the name, date of birth, unique identification number and document type of the customer. The FI should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include: (a) Hong Kong identity card or other national identity card bearing the individual's photograph; (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). The FI should retain a copy of the individual's identification document or record.

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

	4.2.4	An FI should obtain the residential address information of a customer that is a natural person[18].
Customer that is a legal person[19]		
s.2(1)(a), Sch. 2	4.2.5	For a customer that is a legal person, an FI should identify the customer by obtaining at least the following identification information: (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	4.2.6	In verifying the identity of a customer that is a legal person, an FI should normally verify its name, legal form, current existence (at the time of verification), and powers that regulate and bind the legal person. The FI should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include[20]: (a) certificate of incorporation; (b) record of companies registry;

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

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

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

		(c) certificate of incumbency; (d) certificate of good standing; (e) record of registration; (f) partnership agreement or deed; (g) constitutive document; or (h) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body). Illustrative examples of possible measures to verify the name, legal form and current existence of a legal person are set out in paragraph 3 of Appendix C.
	4.2.7	For a customer that is a partnership or an unincorporated body, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to provide reliable and independent evidence of the identity of the customer as required in paragraph 4.2.6 provided that: (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 partners and controllers.
	4.2.8	In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, an FI should satisfy itself as to the legitimate purpose of the organisation, e.g. by requesting sight of the constitutive document.

Customer that is a trust[21] or other similar legal arrangement[22]		
s.2(1)(a), Sch. 2	4.2.9	In respect of trusts, an FI should identify and verify the trust as a customer in accordance with the requirements set out in paragraphs 4.2.10 and 4.2.11. The FI should also regard the trustee[23] as its customer if the trustee enters into a business relationship or carries out occasional transactions on behalf of the trust, which is generally the case if the trust does not possess a separate legal personality. In such a case, an FI should identify and verify the identity of the trustee in line with the identification and verification requirements for a customer that is a natural person or, where applicable, a legal person.
s.2(1)(a), Sch. 2	4.2.10	For a customer that is a trust or other similar legal arrangement, FIs should identify the customer by obtaining at least the following identification information: (a) the 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).

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

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

[23] For the avoidance of doubt, the AMLO defines a beneficial owner in relation to a trust to include trustee (see paragraph 4.3.10). 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 person purporting to act on behalf of the customer), an FI should apply the higher of the relevant requirements set out in this Guideline for the purposes of identification and verification of the identity of the trustee.

s.2(1)(a), Sch. 2	4.2.11	In verifying the identity of a customer that is a trust or other similar legal arrangement, an FI should normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the trust or other similar legal arrangement. The FI should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include: (a) trust deed or similar instrument[24]; (b) record of an appropriate register [25] in the relevant country of establishment; (c) written confirmation from a trustee acting in a professional capacity[26]; (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 FI, if the trust concerned is managed by that trust company.
<u>Connected parties</u>		
	4.2.12	Where a customer is a legal person, a trust or other similar legal arrangement, an FI should identify the connected parties[27] of the customer by obtaining their names.
	4.2.13	A connected party of a customer that is a legal person, a trust or other similar legal arrangement:

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

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

[26] "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).

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

		(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.
<u>Other considerations</u>		
	4.2.14	An FI may adopt an RBA in determining the documents, data or information to be obtained for verifying the identity of a customer that is a legal person, trust or other similar legal arrangement. Illustrative examples of relevant simplified and enhanced measures are set out in paragraph 4 of Appendix C.
4.3 Identification and verification of a beneficial owner		
s.1 & s.2(1)(b), Sch. 2	4.3.1	Beneficial owner 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 FI must identify any beneficial owner in relation to a customer, and take reasonable measures to verify the beneficial owner's identity so that the FI is satisfied that it knows who the beneficial owner is.
	4.3.2	While an FI usually can identify who the beneficial owner of a customer is in the course of understanding the ownership and control structure of the customer, the FI may obtain an undertaking or declaration[28] from the customer on the identity of, and the information relating to, its beneficial owner. When identifying a beneficial owner, the FI should

[28] For example, an FI may obtain from a corporate customer its register of beneficial owners (i.e. the significant controllers register maintained in accordance with the Companies Ordinance, Cap. 622).

		endeavour to obtain the same identification information as at paragraph 4.2.2 as far as possible.
	4.3.3	The verification requirements under the AMLO are different for a customer and a beneficial owner. An FI may adopt an RBA to determine the extent of reasonable measures in relation to the verification of the identity of a beneficial owner of a customer, having regard to paragraph 4.1.7. The FI may consider whether it is appropriate to, for example, (i) make use of records of a beneficial owner available in the public domain[29]; (ii) request its customers to provide documents or information in relation to the identity of a beneficial owner that is obtained from a reliable and independent source; or (iii) where an undertaking or declaration is obtained from the customer (see paragraph 4.3.2), corroborate the customer's undertaking or declaration with publicly available information.
	4.3.4	If the ownership structure of a customer involves different types of legal persons or legal arrangements, in determining who the beneficial owner is, an FI should pay attention to who has ultimate ownership or control over the customer, or who constitutes the controlling mind and management of the customer.
<u>Beneficial owner in relation to a natural person</u>		
	4.3.5	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 FIs to make proactive searches for beneficial owners of the customer in such a case, but they should make appropriate enquiries where there are indications that the customer is not acting on his own behalf.

[29] For example, some jurisdictions maintain registers of beneficial owners which can be accessed by the public or FIs.

Beneficial owner in relation to a legal person		
s.1, Sch. 2	4.3.6	The AMLO defines beneficial owner in relation to a corporation as: (i) an individual who (a) owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation; (b) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or (c) exercises ultimate control over the management of the corporation; or (ii) if the corporation is acting on behalf of another person, means the other person.
s.1, Sch. 2	4.3.7	The AMLO defines beneficial owner, in relation to a partnership as: (i) an individual who (a) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership; (b) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or (c) exercises ultimate control over the management of the partnership; or (ii) if the partnership is acting on behalf of another person, means the other person.
s.1, Sch. 2	4.3.8	In relation to an unincorporated body other than a partnership, beneficial owner: (i) means an individual who ultimately owns or controls the unincorporated body; or (ii) if the unincorporated body is acting on behalf of another person, means the other person.

s.2(1)(b), Sch. 2	4.3.9	For a customer that is a legal person, an FI should identify any natural person who ultimately has a controlling ownership interest (i.e. more than 25%) in the legal person and any natural person exercising control of the legal person or its management, and take reasonable measures to verify their identities. If there is no such natural person (i.e. no natural person falls within the definition of beneficial owners set out in paragraphs 4.3.6 to 4.3.8), the FI should identify the relevant natural persons who hold the position of senior managing official[30] in the legal person, and take reasonable measures to verify their identities.
<u>Beneficial owner in relation to a trust or other similar legal arrangement</u>		
s.1, Sch. 2	4.3.10	The AMLO defines the beneficial owner, in relation to a trust as: (i) a beneficiary or a class of beneficiaries of the trust entitled to a vested interest in the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not; (ii) the settlor of the trust; (iii) the trustee of the trust; (iv) a protector or enforcer of the trust; or (v) an individual who has ultimate control over the trust.
s.2(1)(b), Sch. 2	4.3.11	For a customer that is a trust, an FI 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

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

		through a chain of control or ownership), and take reasonable measures[31] to verify their identities. For a customer that is an other similar legal arrangement, an FI should identify any natural person in equivalent or similar positions to beneficial owner of a trust as stated above and take reasonable measures to verify the identity of such person.
	4.3.12	For a beneficiary of a trust designated by characteristics or by class[32], an FI should obtain sufficient information[33] concerning the beneficiary to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights.
<u>Ownership and control structure</u>		
s.2(1)(b), Sch. 2	4.3.13	Where a customer is not a natural person, an FI should understand its ownership and control structure, including identification of any intermediate layers (e.g. by reviewing an ownership chart of the customer)[34]. The objective is to follow the chain of ownerships to the beneficial owners of the customer. Similar to a corporation, a trust or other similar legal

[31] An FI may adopt an RBA to determine the extent of reasonable measures in relation to the verification of the identities of the beneficiaries or class of beneficiaries of a customer that is a trust, which should be commensurate with the ML/TF risks associated with the customer or business relationship (see paragraph 4.3.3). For example, where the business relationship with a customer that is a trust is assessed to present a low ML/TF risk, it may be reasonable for the FI to verify the identities of the beneficiaries with reference to the information provided by the trustee that was also regarded as the customer by the FI and whose identity has been verified. Such information includes the identification information of the beneficiaries, and declaration that they are known to the trustee.

[32] For example, a trust may have no defined existing beneficiaries when it is set up but only a class of beneficiaries and objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, or following exercise of trustee discretion in the case of a discretionary trust.

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

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

		arrangement can also be part of an intermediate layer in an ownership structure, and should be dealt with in similar manner to a corporate being part of an intermediate layer.
	4.3.14	Where a customer has a complex ownership or control structure, an FI should obtain sufficient information for the FI to satisfy itself that there is a legitimate reason behind the particular structure employed.
4.4 Identification and verification of a person purporting to act on behalf of the customer		
	4.4.1	A person may be appointed to act on behalf of a customer to establish business relationships, or may be authorised to give instructions to an FI to conduct various activities through the account or the business relationship established. Whether the person is considered to be a person purporting to act on behalf of the customer (PPTA) should be determined based on the ML/TF risks associated with that person's roles and the activities which the person is authorised to conduct[35], as well as the ML/TF risks associated with the business relationship[36]. FIs should implement clear policies for determining who is considered to be a PPTA.
s.2(1)(d), Sch. 2	4.4.2	If a person purports to act on behalf of the customer, FIs must: (i) identify the person and take reasonable measures to verify the person's identity by

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

[36] A list of non-exhaustive illustrative risk indicators which may indicate higher or lower ML/TF risks as the case may be is provided in Appendix A.

		reference to documents, data or information provided by a reliable and independent source: (A) a governmental body; (B) the RA or any other RA; (C) an authority in a place outside Hong Kong that performs functions similar to those of the RA or any other RA; or (D) any other reliable and independent source that is recognised by the RA; and (ii) verify the person's authority to act on behalf of the customer.
	4.4.3	FI should identify a PPTA in line with the identification requirements for a customer that is a natural person or, where applicable, a legal person. In taking reasonable measures [37] to verify the identity of the PPTA, FI should, as far as possible, follow the verification requirements for a customer that is a natural person or, where applicable, a legal person.
s.2(1)(d)(ii), Sch. 2	4.4.4	FIs should verify the authority of each PPTA by appropriate documentary evidence (e.g. board resolution or similar written authorisation).
4.5 Reliability of documents, data or information		
	4.5.1	In verifying the identity of a customer, an FI needs not establish accuracy of every piece of identification information collected in paragraphs 4.2.2, 4.2.5 and 4.2.10.
	4.5.2	An FI should ensure that documents, data or information obtained for the purpose of verifying the identity of a customer as required in paragraphs

[37] An FI may adopt an RBA to determine the extent of reasonable measures in relation to the verification of the identity of the PPTA, which should be commensurate with the ML/TF risks associated with the business relationship. For example, where a business relationship with a legal person customer with many PPTAs is assessed to present low ML/TF risk, an FI could verify the identities of the PPTAs with reference to a list of PPTAs, whose identities and authority to act have been confirmed by a department or person within that legal person customer which is independent to the persons whose identities are being verified (for example, compliance, audit or human resources).

		4.2.3, 4.2.6 and 4.2.11 is current at the time they are provided to or obtained by the FI.
	4.5.3	When using documents for verification, an FI should be aware that some types of documents are more easily forged than others, or can be reported as lost or stolen[38]. Therefore, the FI should consider applying anti-fraud procedures that are commensurate with the risk profile of the person being verified.
	4.5.4	If a natural person customer or a person representing a legal person, a trust or other similar legal arrangement to establish a business relationship with an FI is physically present during the CDD process, the FI should generally have sight of original identification document by its staff and retain a copy of the document. However, there are a number of occasions where an original identification document cannot be produced by the customers (e.g. the original document is in electronic form). In such an occasion, the FI should take appropriate measures to ensure the reliability of identification documents obtained.
	4.5.5	Where the documents, data or information being used for the purposes of identification are in a foreign language, appropriate steps should be taken by the FI to be reasonably satisfied that the documents in fact provide evidence of the customer's identity[39].
4.6 Purpose and intended nature of business relationship		
s.2(1)(c), Sch. 2	4.6.1	An FI must understand the purpose and intended nature of the business relationship. In some

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

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

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

		owner's identity can be effectively managed[40]; (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	An example of a situation in the securities industry where it may be necessary not to interrupt the normal conduct of business is when companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
	4.7.3	If an FI allows verification of the identity of a customer and any beneficial owner of the customer after establishing the business relationship, it should adopt appropriate risk management policies and procedures concerning the conditions under which the customer may utilise the business relationship prior to verification. These policies and procedures should include: (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); (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

[40] For FIs that are SFC-licensed VAS Providers, it would be highly unlikely that the ML/TF risks arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed.

		(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 PEPs.
	4.7.4	Verification of identity should be completed by an FI within a reasonable timeframe, which generally refers to the following: (a) the FI completing such verification no later than 30 working days after the establishment of business relationship; (b) the FI suspending business relationship with the customer and refraining from carrying out further transactions (except to return funds to their sources, to the extent that this is possible) if such verification remains uncompleted 30 working days after the establishment of business relationship; and (c) the FI terminating business relationship with the customer if such verification remains uncompleted 120 working days after the establishment of business relationship.
s.3(4)(b), Sch. 2, s.25A, DTROP & OSCO, s.12, UNATMO	4.7.5	If verification cannot be completed within the reasonable timeframe set in the FI's risk management policies and procedures, the FI should terminate the business relationship as soon as reasonably practicable and refrain from carrying out further transactions (except to return funds or other assets in their original forms as far as possible). The FI should also assess whether this failure

		provides grounds for knowledge or suspicion of ML/TF and consider making a suspicious transaction report (STR) to the JFIU, particularly if the customer requests that funds or other assets be transferred to a third party or be "transformed" (e.g. from cash into a cashier order) without a justifiable reason.
4.8 Simplified customer due diligence (SDD)		
<u>General</u>		
s.4, Sch. 2	4.8.1	Section 4 of Schedule 2 permits FIs not to identify and take reasonable measures to verify the identities of the beneficial owners[41] of specific types of customers, or in relation to specific types of products related to the transactions of the customers (referred to as "simplified customer due diligence" under section 4 of Schedule 2; and as "SDD" hereafter). However, other aspects of CDD must be undertaken and it is still necessary to conduct ongoing monitoring of the business relationship. The use of SDD must be supported by robust assessment to ensure the conditions or circumstances of specific types of customers or products specified in section 4 of Schedule 2 are met.
s.3(1)(d) & (e), s.4(1), (3), (5) & (6), Sch. 2	4.8.2	Nonetheless, SDD must not be or continue to be applied when the FI suspects that the customer, the customer's account or the transaction is involved in ML/TF, or when the FI doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity, notwithstanding when the customer, the product, and account type falls within paragraphs 4.8.3, 4.8.15 and 4.8.17 below.
s.4(3), Sch. 2	4.8.3	An FI may apply SDD if the customer is -

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

		(a) an FI as defined in the AMLO; (b) an institution that- (i) is incorporated or established in an equivalent jurisdiction (see paragraphs 4.19); (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 ("listed company"); (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- i. has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and ii. 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	4.8.4	If a customer not falling within section 4(3) of Schedule 2 has in its ownership chain an entity that falls within that section, the FI is not required to identify or verify the beneficial owners of that entity in that chain when establishing a business relationship with or carrying out an occasional transaction for the customer. However, FIs should

		still identify and take reasonable measures to verify the identities of beneficial owners in the ownership chain that are not connected with that entity.
s.2(1)(a), (c) & (d), Sch. 2	4.8.5	For avoidance of doubt, the FI must still: (a) identify the customer and verify[42] the customer's identity; (b) if a business relationship is to be established and its purpose and intended nature are not obvious, obtain information on the purpose and intended nature of the business relationship with the FI; and (c) if a person purports to act on behalf of the customer, (i) identify the person and take reasonable measures to verify the person's identity; and (ii) verify the person's authority to act on behalf of the customer, in accordance with the relevant requirements stipulated in this Guideline.
<u>Local and foreign financial institution</u>		
s.4(3)(a) & (b), Sch. 2	4.8.6	FIs may apply SDD to a customer that is an FI as defined in the AMLO, or an institution that carries on a business similar to that carried on by an FI and meets the criteria set out in section 4(3)(b) of Schedule 2. If the customer does not meet the criteria, the FI must carry out all the CDD measures set out in section 2 of Schedule 2. FI may apply SDD to a customer that 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 second-mentioned FI or its underlying customers; or (b) in the name of an investment vehicle in the

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

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

Investment vehicle		
s.4(3)(d), Sch. 2	4.8.9	FIs may apply SDD to a customer that is an investment vehicle if the FI is able to ascertain that the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle falls within any of the categories of institutions set out in section 4(3)(d) of Schedule 2.
	4.8.10	An investment vehicle may be in the form of a legal person or trust, and may be a collective investment scheme or other investment entity.
	4.8.11	An investment vehicle whether or not responsible for carrying out CDD measures on the underlying investors under governing law of the jurisdiction in which the investment vehicle is established may, where permitted by law, appoint another institution ("appointed institution"), such as a manager, a trustee, an administrator, a transfer agent, a registrar or a custodian, to perform the CDD. Where the person responsible for carrying out the CDD measures (the investment vehicle[43] or the appointed institution) falls within any of the categories of institution set out in section 4(3)(d) of Schedule 2, an FI may apply SDD to that investment vehicle provided that it is satisfied that the investment vehicle has ensured that there are reliable systems and controls in place to conduct the CDD (including identification and verification of the identity) on the underlying investors in accordance with the requirements similar to those set out in the Schedule 2.
	4.8.12	If neither the investment vehicle nor appointed institution fall within any of the categories of

[43] 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 purposes 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.

		institution set out in section 4(3)(d) of Schedule 2, the FI must identify and take reasonable measures to verify the identity of any investor of the investment vehicle in accordance with the requirements for identification and verification of a beneficial owner of a specific type of customer (see paragraphs 4.3). The FI may consider whether it is appropriate to rely on a written representation from the investment vehicle or appointed institution (as the case may be) responsible for carrying out the CDD stating, to its actual knowledge, the identities of such investors or (where applicable) there is no such investor in the investment vehicle. This will depend on risk factors such as whether the investment vehicle is being operated for a small, specific group of persons. Where the FI accepts such a representation, this should be documented, retained, and subject to periodic review.
<u>Government and public body</u>		
s.4(3)(e) & (f), Sch. 2	4.8.13	FIs may apply SDD to a customer that is the Hong Kong Government, any public bodies in Hong Kong, the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.
s.1, Sch. 2	4.8.14	Public body includes: (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.
<u>SDD in relation to specific products</u>		
s.4(4) & (5), Sch. 2	4.8.15	FIs may apply SDD in relation to a customer if the FI has reasonable grounds to believe that the

		transaction conducted by the customer relates to any one of the following products: (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.
	4.8.16	For the purposes of item (a) of paragraph 4.8.15, FIs may generally treat the employer as the customer and apply SDD on the employer (i.e. choosing not to identify and take reasonable measures to verify the employees of the scheme). Where FIs have separate business relationships with the employees, it should apply CDD measures in accordance with relevant requirements set out in this Chapter.
<u>Solicitor's client accounts</u>		
s.4(6), Sch. 2	4.8.17	If a customer of an FI is a solicitor or a firm of solicitors, the FI may apply SDD to the client account opened by the customer, provided that the following criteria are satisfied: (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.
	4.8.18	When opening a client account for a solicitor or a firm of solicitors, FIs should establish the proposed use of the account, i.e. whether to hold co-mingled client funds or the funds of a specific client.
	4.8.19	If a client account is opened on behalf of a single client or there are sub-accounts for each individual client where funds are not co-mingled at the FI, the FI should establish the identity of the underlying client(s) in addition to that of the solicitor opening the account.
4.9 Special requirements in high risk situations[44]		
s.15, Sch.2	4.9.1	An FI must comply with the special requirements set out in section 15 of Schedule 2 in: (a) a situation that by its nature may present a high risk of ML/TF taking into account the list of non-exhaustive illustrative risk indicators which may indicate higher ML/TF risks set out in Appendix A; or (b) a situation specified by the RA in a notice in writing given to the FI.
s.15, Sch. 2	4.9.2	Section 15 of Schedule 2 specifies that an FI must, in any situation that by its nature presents a high risk of ML/TF, comply with the special requirements set out therein which include: (a) obtaining the approval of senior management to establish a business relationship, or continue an

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

		existing business relationship where the relationship subsequently presents a high risk of ML/TF; and (b) either: (i) taking reasonable measures to establish the relevant customer's or beneficial owner's source of wealth and the source of the funds that will be involved in the business relationship[45]; or (ii) taking additional measures to mitigate the risk of ML/TF.
	4.9.3	For illustration purposes, additional measures to mitigate the risk of ML/TF may include the examples of possible enhanced measures set out in paragraph 2 of Appendix C.
4.10 Customer not physically present for identification purposes		
	4.10.1	FIs must apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview[46]. Where a customer has not been physically present for identification purposes, FIs will generally not be able to determine that the documentary evidence of identity actually relates to the customer they are dealing with. Consequently, there are increased risks.
<u>Special requirements</u>		
s.5(3)(a), s.5(4) & s.9(1), Sch. 2	4.10.2	The AMLO permits FIs to establish business relationship through various channels, both face-to-face (e.g. branch) and non-face-to-face (e.g. internet). However, an FI should take additional measures to mitigate any risk (e.g. impersonation

[45] Guidance on source of wealth and source of funds are provided in paragraphs 4.11.13 and 4.11.14.

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

		risk) associated with customers not physically present for identification purposes. Except for the situation specified in paragraph 4.10.3, if a customer has not been physically present for identification purposes, the FI must carry out at least one of the following additional measures to mitigate the risks posed: (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 FI; or (c) ensuring that the payment or, if there is more than one payment, the first payment made in relation to the customer's account is carried out through an account opened in the customer's name with an authorized institution, or an institution that: (i) is incorporated or established in an equivalent jurisdiction; (ii) carries on a business similar to that carried on by an authorized institution; (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 authorities in that jurisdiction that perform functions similar to those of the HKMA.
s.9(2), Sch. 2	4.10.3	If an FI has verified the identity of the customer on the basis of data or information provided by a digital identification system that is a reliable and independent source that is recognised by the RA (see paragraph 4.2.1(d)), the FI is not required to carry out any of the additional measures set out in paragraph 4.10.2.

	4.10.4	The extent of additional measures set out in paragraph 4.10.2 will depend on the nature and characteristics of the product or service requested and the assessed ML/TF risk presented by the customer.
	4.10.5	Paragraph 4.10.2(b) allows an FI to utilise different methods to mitigate the risk. These may include measures such as (i) use of an independent and appropriate person to certify identification documents[47]; (ii) checking relevant data against reliable databases or registries; or (iii) using appropriate technology, etc. Whether a particular measure or a combination of measures is acceptable should be assessed on a case-by-case basis. The FI should ensure and be able to demonstrate to the RA that the supplementary measure(s) taken can adequately guard against impersonation risk.
	4.10.6	For the avoidance of doubt, LCs should also comply with the relevant provisions (presently paragraph 5.1) in the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission, having regard to the acceptable non-face-to-face account opening approaches as well as relevant circulars and frequently asked questions published by the SFC from time to time.
<u>Other considerations</u>		
	4.10.7	While the requirements to undertake additional measures generally apply to a customer that is a natural person, increased risk may arise if a customer that is not a natural person establishes a business relationship with an FI through a non-face-to-face channel, for example when the natural person acting on behalf of the customer to establish the business relationship is not physically present

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

		for identification purposes. In such a case, the FI should mitigate the increased risk (e.g. applying additional due diligence measures set out in paragraph 4.10.2 to such natural person, except where the FI has verified the identity of the natural person on the basis of data or information provided by a digital identification system (see paragraph 4.2.1(d))). In addition, where an FI is provided with copies of documents for identifying and verifying a legal person customer's identity, an FI should also mitigate any increased risk (e.g. applying additional due diligence measures set out in paragraph 4.10.2).
4.11 Politically exposed persons (PEPs)		
General		
s.1 & s.10, Sch. 2	4.11.1	Much international attention has been paid in recent years to the risk associated with providing financial and business services to those with a prominent political profile or holding senior public office. However, PEP status itself does not automatically mean that the individuals are corrupt or that they have been incriminated in any corruption.
	4.11.2	However, their office and position may render PEPs vulnerable to corruption. The risks increase when the person concerned is from a foreign country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards.
	4.11.3	An FI should implement appropriate risk management systems to identify PEPs. Under-classification of PEPs poses a higher ML/TF risk to the FI whilst over-classification of PEPs leads to an unnecessary compliance burden to the FI and its customers.
s.15, Sch. 2	4.11.4	While the statutory definition of PEPs in the AMLO (see paragraph 4.11.7 below) only includes

		individuals entrusted with prominent public function in a place outside Hong Kong, Hong Kong PEPs and international organisation PEPs may also present, by virtue of the positions they hold, a higher ML/TF risk. FIs should therefore adopt an RBA to determine whether to apply the measures in paragraph 4.11.12 below in respect of Hong Kong PEPs and international organisation PEPs.
s.1, s.5(3)(b) & (c), s.10 & s.15, Sch. 2	4.11.5	The statutory definition does not automatically exclude sub-national political figures. Corruption by heads of regional governments, regional government ministers and large city mayors is no less serious as sub-national figures in some jurisdictions may have access to substantial funds. Where FIs identify a customer as a sub-national figure holding a prominent public function, they should apply appropriate measures set out in paragraph 4.11.12.
	4.11.6	The definitions of PEPs set out in paragraphs 4.11.7, 4.11.20 and 4.11.21 provide some non-exhaustive examples of the types of prominent (public) functions that an individual may be or may have been entrusted with by a government, or by an international organisation respectively. An FI should provide sufficient guidance and examples to its staff to enable them to identify all types of PEPs. In determining what constitutes a prominent (public) function, an FI should consider on a case-by-case basis taking into account various factors, for example: the powers and responsibilities associated with particular public function; the organisational framework of the relevant government or international organisation; and any other specific concerns connected to the jurisdiction where the public function is/has been entrusted.
<u>Non-Hong Kong PEPs</u>		
Definition		
s.1, Sch. 2	4.11.7	A PEP (hereafter referred to as "non-Hong Kong PEP") is defined as:

		(a) an individual who is or has been entrusted with a prominent public function in a place outside Hong Kong and (i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official; (ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i); (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 4.11.8).
s.1, Sch. 2	4.11.8	A close associate is defined as: (a) an individual who has close business relations with a person falling under paragraph 4.11.7(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph 4.11.7(a) is also a beneficial owner; or (b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under paragraph 4.11.7(a) above.
Identification of non-Hong Kong PEPs		
s.19(1), Sch. 2	4.11.9	An FI must establish and maintain effective procedures (e.g. by making reference to publicly available information and/or screening against commercially available databases) for determining whether a customer or a beneficial owner of a customer is a non-Hong Kong PEP.

	4.11.10	While an FI may refer to commercially available databases to identify non-Hong Kong PEPs, the use of these databases should never replace traditional CDD processes (e.g. understanding the occupation and employer of a customer). When using commercially available databases, an FI should be aware of their limitations, for example, the databases are not necessarily comprehensive or reliable as they generally draw solely from information that is publicly available; the definition of non-Hong Kong PEPs used by the database providers may or may not align with the definition of non-Hong Kong PEPs applied by the FI; and any technical incapability of such databases that may hinder the FI's effectiveness of non-Hong Kong PEP identification. An FI using such databases as a support tool should ensure that they are fit for the purpose.
	4.11.11	FIs may use publicly available information or refer to relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations to assess which countries are most vulnerable to corruption (an example of which is Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption). FIs should be vigilant where either the country to which the customer has business connections or the business/industrial sector is more vulnerable to corruption.
Special requirements and additional measures for non-Hong Kong PEPs		
s.5(3)(b) & s.10(1) & (2), Sch. 2	4.11.12	When an FI knows that a customer or beneficial owner of a customer is a 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 non-Hong

		Kong PEP, apply all the following measures: (a) obtaining approval from its senior management for establishing or continuing such business relationship[48]; (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 on that business relationship (see Chapter 5).
	4.11.13	Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets). This information will usually give an indication as to the size of wealth the customer would be expected to have, and a picture of how the individual acquired such wealth. Although an FI may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources. Examples of information and documents which may be used to establish source of wealth include evidence of title, copies of trust deeds, audited financial statements, salary details, tax returns and bank statements.
	4.11.14	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 FI (e.g. the amounts being invested, deposited, or wired as part of the business relationship). Source of funds information should not simply be limited to knowing from where 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; e.g. salary payments and investment sale proceeds.

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

	4.11.15	It is for an FI to decide which measures it deems reasonable, in accordance with its assessment of the risks, to establish the source of funds and source of wealth. In practical terms, this will often amount to obtaining information from the non-Hong Kong PEP and verifying it against publicly available information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. FIs should however note that not all declarations are publicly available and that a non-Hong Kong PEP customer may have legitimate reasons for not providing a copy. FIs should also be aware that some jurisdictions impose restrictions on their PEP's ability to hold foreign bank accounts or to hold other office or paid employment.
	4.11.16	Although the measures set out in paragraph 4.11.12 also apply to family members and close associates of the non-Hong Kong PEP, the risks associated with them may vary depending to some extent on the social-economic and cultural structure of the jurisdiction of the non-Hong Kong PEP.
	4.11.17	Since not all non-Hong Kong PEPs pose the same level of ML/TF risks, an FI should adopt an RBA in determining the extent of measures in paragraph 4.11.12 taking into account relevant factors, such as: (a) the prominent public functions that a non-Hong Kong PEP holds; (b) the geographical risk associated with the jurisdiction where a non-Hong Kong PEP holds prominent public functions; (c) the nature of the business relationship (e.g. the delivery/distribution channel used; or the product or service offered); and (d) in relation to a former non-Hong Kong PEP, the

		risk factors specified in paragraph 4.11.19.
<u>Treatment of former non-Hong Kong PEPs</u>		
s.1, Sch. 2	4.11.18	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 4.11.8).
s.5(5) & s.10(3), Sch. 2	4.11.19	An FI should adopt an RBA[49] and may decide not to apply, or not to continue to apply, the measures set out in paragraph 4.11.12 to a former non-Hong Kong PEP who no longer presents a high risk of ML/TF after stepping down. To determine whether a former non-Hong Kong PEP no longer presents a high risk of ML/TF, the FI should conduct an appropriate assessment of the ML/TF risk associated with the previous 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 a non-Hong Kong PEP; and (c) whether the individual's previous and current functions are linked in any way (e.g. formally by appointment of the former non-Hong Kong PEP's successor, or informally by the fact that the former non-Hong Kong PEP continues to

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

		deal with the same substantive matters).
<u>Hong Kong PEPs and international organisation PEPs</u>		
Definition		
	4.11.20	For the purposes of this Guideline, a "Hong Kong PEP" refers to: (a) an individual who is or has been entrusted with a prominent public function in Hong Kong and (i) includes head of government, senior politician, senior government or judicial official, senior executive of a government-owned corporation and an important political party official; (ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i); (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 4.11.8).
	4.11.21	For the purposes of this Guideline, an "international organisation PEP" refers to: (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 (c) a close associate of an individual falling within

		paragraph (a) (see paragraph 4.11.8).
	4.11.22	International organisations referred to in paragraph 4.11.21 are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the UN and affiliated international organisations such as the International Maritime Organization; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization; and economic organisations such as the World Trade Organization and the Association of Southeast Asian Nations; etc.
Identification of and additional measures for Hong Kong PEPs and international organisation PEPs		
	4.11.23	An FI should take reasonable measures to determine whether a customer or a beneficial owner of a customer is a Hong Kong PEP or an international organisation PEP[50].
	4.11.24	FIs should apply the measures specified in paragraph 4.11.12 with reference to the guidance provided in paragraphs 4.11.13 to 4.11.17 in any of the following situations[51]:

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

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

		(a) before establishing a high risk business relationship[52] with a customer who is or whose beneficial owner is a Hong Kong PEP or an international organisation PEP; (b) when continuing an existing business relationship with a customer who is or whose beneficial owner is a Hong Kong PEP or an international organisation PEP where the relationship subsequently becomes high risk; or (c) when continuing an existing high risk business relationship where the FI subsequently knows that the customer or the beneficial owner of the customer is a Hong Kong PEP or an international organisation PEP.
Treatment of former Hong Kong PEPs or former international organisation PEPs		
	4.11.25	In the situations described in paragraph 4.11.24, an FI should adopt an RBA[53] and may decide not to apply, or not to continue to apply, the measures set out in paragraph 4.11.12 to a Hong Kong PEP or an international organisation PEP who has been but not currently entrusted with a prominent (public) function (hereafter referred to as "former Hong Kong PEP" or "former international organisation PEP")[54] and no longer presents a high risk of ML/TF after stepping down. To determine whether a former Hong Kong PEP or a former international organisation PEP no longer presents a high risk of ML/TF, the FI should conduct an appropriate assessment of the ML/TF risk associated with the previous PEP status taking into account various risk factors, including but not limited

[52] In determining whether a business relationship presents a high ML/TF risk, an FI should take into account all risk factors (including the list of illustrative risk indicators set out in Appendix A) that are relevant to the business relationship.

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

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

		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 Hong Kong PEP or an international organisation PEP; and (c) whether the individual's previous and current functions are linked in any way (e.g. formally by appointment of the successor of the former Hong Kong PEP or the former international organisation PEP, or informally by the fact that the former Hong Kong PEP or the former international organisation PEP continues to deal with the same substantive matters).
4.12 Bearer shares and nominee shareholders		
Bearer shares[55]		
s.15, Sch. 2	4.12.1	Bearer shares refer to negotiable instruments that accord ownership in a legal person to the person who possesses the 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 FI should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the FI is notified whenever there is a change of beneficial owner of such shares.
	4.12.2	Where bearer shares have been deposited with an authorised/registered custodian, FIs should seek independent evidence of this, for example confirmation from the registered agent that an authorised/registered custodian holds the bearer shares, together with the identities of the authorised/registered custodian and the person who

[55] For the avoidance of doubt, paragraphs 4.12.1 to 4.12.3 also apply to bearer share warrants, which refer to negotiable instruments that accord entitlement to ownership in a legal person to the person who possesses the physical bearer share warrant certificate, and any other similar warrants or instruments without traceability. In this regard, the reference to "bearer shares" or "shares" should also be read as "bearer share warrants" or "share warrants" respectively.

		has the right to those entitlements carried by the share. As part of the FI's ongoing periodic review, it should obtain evidence to confirm the authorised/registered custodian of the bearer shares.
	4.12.3	Where the shares are not deposited with an authorised/registered custodian, the FI should obtain declarations prior to account opening and annually thereafter from each beneficial owner of such shares. FIs should also require the customer to notify it immediately of any changes in the ownership of the shares.
Nominee shareholders		
	4.12.4	For a customer identified to have nominee shareholders in its ownership structure, an FI should obtain satisfactory evidence of the identities of the nominees, and the persons on whose behalf they are acting, as well as the details of arrangements in place, in order to determine who the beneficial owner is.
4.13 Jurisdictions posing a higher risk		
	4.13.1	FIs should give particular attention to, and exercise extra care in respect of: (a) business relationships and transactions with persons (including legal persons and other FIs) from or in jurisdictions identified by the FATF as having strategic AML/CFT deficiencies; and (b) transactions and business connected with jurisdictions assessed as higher risk. In such case, the special requirements of section 15 of Schedule 2 may apply (see paragraphs 4.9).
	4.13.2	In determining which jurisdictions are identified by the FATF as having strategic AML/CFT deficiencies, or may otherwise pose a higher risk, FIs should consider, among other things:

		(a) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems; (b) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity; (c) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the UN; or (d) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operation. "Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations.
4.14 Jurisdictions subject to a call by the FATF		
s.15, Sch. 2	4.14.1	An FI should apply additional measures, proportionate to the risks and in accordance with the guidance provided in paragraphs 4.9, to business relationships and transactions with natural and legal persons, and FIs, from jurisdictions for which this is called for by the FATF.

s.15, Sch. 2	4.14.2	Where mandatory enhanced measures or countermeasures[56] are called for by the FATF, or in other circumstances independent of any call by the FATF but also considered to be higher risk, RA may also, through a notice in writing: (a) impose a general obligation on FIs to comply with the special requirements set out in section 15 of Schedule 2; or (b) require FIs to undertake specific countermeasures identified or described in the notice. The type of measures in paragraphs (a) and (b) above would be proportionate to the nature of the risks and/or deficiencies.
4.15 Reliance on CDD performed by intermediaries		
General		
s.18, Sch. 2	4.15.1	An FI may rely upon an intermediary to perform any part of the CDD measures[57] specified in section 2 of Schedule 2, subject to the criteria set out in section 18 of Schedule 2. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the FI. In a third-party reliance scenario, the third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying FI, and would apply its own procedures to perform the CDD measures.
	4.15.2	For the avoidance of doubt, reliance on intermediaries does not apply to outsourcing or

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

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

		agency relationships, in which the outsourced entity or agent applies the CDD measures on behalf of the FI, in accordance with the FI's procedures, and subject to the FI's control of effective implementation of these procedures by the outsourced entity or agent.
s.18(1), Sch. 2	4.15.3	When relying on an intermediary, the FI must: (a) obtain written confirmation from the intermediary that the intermediary agrees to act as the FI's intermediary and perform which part of the CDD measures specified in section 2 of Schedule 2; and (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	4.15.4	An FI that carries out a CDD measure by means of an intermediary must immediately after the intermediary has carried out that measure, obtain from the intermediary the data or information that the intermediary has obtained in the course of carrying out that measure, but nothing in this paragraph requires the FI to obtain at the same time from the intermediary a copy of the document, or a record of the data or information, that is obtained by the intermediary in the course of carrying out that measure.
s.18(4)(b), Sch. 2	4.15.5	Where these documents and records are kept by the intermediary, the FI should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the FI's business relationship with the customer and for at least five years beginning on the date on which the business relationship of a customer with the FI ends or until such time as may be specified by the RA. The FI must ensure that the

		intermediary will, if requested by the FI within the period specified in the record-keeping requirements of AMLO, provide to the FI a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out that measure as soon as reasonably practicable after receiving the request. The FI should also obtain an undertaking from the intermediary to supply copies of all underlying CDD information in circumstances where the intermediary is about to cease trading or does not act as an intermediary for the FI anymore.
	4.15.6	An FI should conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay.
	4.15.7	Whenever an FI has doubts as to the reliability of the intermediary, it should take reasonable steps to review the intermediary's ability to perform its CDD duties. If the FI intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the FI has any doubts regarding the CDD measures carried out by the intermediary previously, the FI should perform the required CDD as soon as reasonably practicable.
<u>Domestic intermediaries</u>		
s.18(3)(a), (3)(b) & (7), Sch. 2	4.15.8	An FI may rely upon any one of the following domestic intermediaries, to perform any part of the CDD measures set out in section 2 of Schedule 2: (a) an FI that is an authorized institution, a licensed corporation, an authorized insurer, a licensed individual insurance agent, a licensed insurance agency or a licensed insurance broker company (intermediary FI); (b) an accounting professional meaning: (i) a certified public accountant as defined by section 2(1) of the Professional Accountants

		Ordinance (Cap. 50), or a certified public accountant (practising) as defined by section 2(1) of the Accounting and Financial Reporting Council Ordinance (Cap. 588); (ii) a corporate practice as defined by section 2(1) of the Accounting and Financial Reporting Council Ordinance (Cap. 588); or (iii) a CPA firm as defined by section 2(1) of the Accounting and Financial Reporting Council Ordinance (Cap. 588); (c) an estate agent meaning: (i) a licensed estate agent as defined by section 2(1) of the Estate Agents Ordinance (Cap. 511); or (ii) a licensed salesperson as defined by section 2(1) of the Estate Agents Ordinance (Cap. 511); (d) a legal professional meaning: (i) a solicitor as defined by section 2(1) of the Legal Practitioners Ordinance (Cap. 159); or (ii) a foreign lawyer as defined by section 2(1) of the Legal Practitioners Ordinance (Cap. 159); 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 FI is satisfied that the domestic intermediary has adequate procedures in place to prevent ML/TF and is required to comply

		with the relevant requirements set out in Schedule 2 with respect to the customer[58].
s.18(3)(a) & (3)(b), Sch. 2	4.15.9	An FI should take appropriate measures to ascertain if the domestic intermediary satisfies the criteria set out in paragraph 4.15.8, which may include: (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.
<u>Overseas intermediaries</u>		
s.18(3)(c), Sch. 2	4.15.10	An FI may rely upon an overseas intermediary[59] carrying on business or practising in an equivalent jurisdiction[60] 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; (ii) a lawyer or a notary public; (iii) an auditor, a professional accountant, or a tax advisor;

[58] 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.

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

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

		(iv) a trust or company service provider; (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).
	4.15.11	An FI should take appropriate measures to ascertain if the overseas intermediary satisfies the criteria set out in paragraph 4.15.10. Appropriate measures that should be taken to ascertain if the criterion set out in paragraph 4.15.10(c) is satisfied may include: (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	4.15.12	An FI may also rely upon a related foreign financial institution (related foreign FI) to perform any part of the CDD measures set out in section 2 of Schedule 2, if the related foreign FI: (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 FI; (ii) if the FI is incorporated in Hong Kong, it is a branch of the FI; (iii) if the FI is incorporated outside Hong Kong: (A) it is the head office of the FI; or (B) it is a branch of the head office of the FI; (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[61] that performs, in relation to the holding company or the head office of the FI, functions similar to those of an RA under the AMLO.
s.18(3A) & (4)(c), Sch. 2	4.15.13	The group policy set out in paragraph 4.15.12(b) refers to a policy of the group of companies to which the FI belongs and the policy applies to the FI and the related foreign FI. The group policy should include CDD and record-keeping requirements similar to the requirements imposed under Schedule 2 and group-wide AML/CFT Systems [62] (e.g. compliance and audit functions) to ensure compliance with those requirements. 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 FI should be satisfied that the related foreign FI is subject to regular and independent reviews over its ongoing compliance with the group policy conducted

[61] Guidance on jurisdictional equivalence is provided in paragraphs 4.19.
[62] Reference should be made to Chapter 3.

		by any group-level compliance, audit or other similar AML/CFT functions.
s.18(3A), Sch. 2	4.15.14	The FI should be able to demonstrate that the implementation of the group policy is supervised at a group level by either an RA or an authority in an equivalent jurisdiction that performs functions similar to those of an RA under the AMLO, which practises group-wide supervision which extends to the related foreign FI.
4.16 Pre-existing customers		
s.6, Sch. 2	4.16.1	FIs must perform the CDD measures prescribed in Schedule 2 and this Guideline in respect of pre-existing customers (with whom the business relationship was established before the AMLO came into effect on 1 April 2012), when: (a) a transaction takes place with regard to the customer, which is, by virtue of the amount or nature of the transaction, unusual or suspicious; or is not consistent with the FI's knowledge of the customer or the customer's business or risk profile, or with its knowledge of the source of the customer's funds; (b) a material change occurs in the way in which the customer's account is operated; (c) the FI suspects that the customer or the customer's account is involved in ML/TF; or (d) the FI doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.
	4.16.2	Trigger events may include the re-activation of a dormant account or a change in the beneficial ownership or control of the account but FIs will need to consider other trigger events specific to their own customers and business.
s.5, Sch. 2	4.16.3	FIs should note that requirements for ongoing

		monitoring under section 5 of Schedule 2 also apply to pre-existing customers (see Chapter 5).
4.17 Failure to satisfactorily complete CDD measures		
s.3(4), Sch. 2	4.17.1	Where an FI is unable to complete the CDD measures in accordance with paragraph 4.1.9 or 4.7.1, the FI: (a) must not establish a business relationship or carry out any occasional transaction with that customer; or (b) must terminate the business relationship as soon as reasonably practicable if the FI has already established a business relationship with the customer. The FI should also assess whether this failure provides grounds for knowledge or suspicion of ML/TF and where there is relevant knowledge or suspicion, should make an STR to the JFIU in relation to the customer.
4.18 Prohibition on anonymous accounts		
s.16, Sch. 2	4.18.1	FIs must not open, or maintain, any anonymous account or account in fictitious names for any customer. Besides, confidential numbered accounts [63] should not function as anonymous accounts, rather they should be subject to exactly the same CDD and control measures[64] as all other business relationships. While a numbered account can offer additional confidentiality for the customer, the identity of the customer should be verified by the FI 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's CDD

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

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

		record must be available to the RAs, other authorities, the CO, auditors, and other staff with appropriate authority.
4.19 Jurisdictional equivalence		
General		
s.4(3)(b)(i), s.4(3)(d)(iii), s.4(3)(f), s.9(1)(c)(ii) & s.18(3)(c), Sch. 2	4.19.1	Jurisdictional equivalence and the determination of equivalence is an important aspect in the application of CDD measures under the AMLO. Equivalent jurisdiction is defined in the AMLO as meaning: (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		
	4.19.2	An FI may therefore be required to evaluate and determine for itself which jurisdictions other than FATF members apply requirements similar to those imposed under Schedule 2 for jurisdictional equivalence purposes. The FI should document its assessment of the jurisdiction, and include consideration of the following factors: (a) whether the jurisdiction concerned is a member of FATF-style regional bodies and its recent mutual evaluation report published by the FATF-style regional bodies[65]; (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 circulars issued by RAs from time to time alerting FIs to such jurisdictions with poor AML/CFT controls; or (d) any other AML/CFT related publications that are published by specialised national, international,

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

		non-governmental or commercial organisations (for example, Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption).
	4.19.3	As the AML/CFT regime of a jurisdiction will change over time, an FI should review the jurisdictional equivalence assessment from time to time.
4.20 Cross-border correspondent relationships		
Introduction		
	4.20.1	For the purposes of this Guideline, "cross-border correspondent relationships" refers to the provision of services for dealing in securities, dealing in futures contracts, or leveraged foreign exchange trading[66], by an FI[67] (hereafter referred to as "correspondent institution") to another financial institution[68] located in a place outside Hong Kong (hereafter referred to as "respondent institution"), where transactions effected on a principal or agency basis under the business relationships are initiated by the respondent institution.
	4.20.2	An FI may establish cross-border correspondent relationships with respondent institutions around the world. An example of cross-border correspondent relationship is where a securities firm located in Hong Kong, as a correspondent institution, executes securities transactions on a stock exchange for a securities firm operating outside Hong Kong, which acts as a respondent institution for its underlying

[66] For the avoidance of doubt, paragraphs 4.20 may be applicable to an FI providing these services to a respondent institution even where the FI may rely on any incidental or other exemptions provided in the SFO to be exempt from the requirement of being licensed or registered for Type 1, 2 or 3 regulated activity. For example, paragraphs 4.20 are applicable to an FI dealing in fund shares or units for its customer that is a distributor located outside Hong Kong for funds under the FI's management.

[67] For the purposes of paragraphs 4.20, the term "FI" means a licensed corporation or a registered institution.

[68] Financial institution in this context refers to businesses falling within the definition of the term "financial institutions" under the FATF Recommendations and which are conducted for or on behalf of customers.

		local customers.
	4.20.3	Where a respondent institution conducts business for or on behalf of customers through a cross-border correspondent relationship with an FI, the FI normally has limited information regarding the underlying customers and the nature or purpose of the underlying transactions because it generally does not have direct relationships with the underlying customers of the respondent institution. This will expose the FI to risks stemming from the lack or incompleteness of information about the underlying customers and transactions.
s.19(3) & s.23(b), Sch. 2	4.20.4	An FI should establish and maintain effective procedures for mitigating the risks associated with cross-border correspondent relationships which may vary depending on a number of factors (see paragraph 4.20.6).
<u>Additional due diligence measures for cross-border correspondent relationships</u>		
	4.20.5	An FI must carry out CDD measures[69] in relation to a customer including a respondent institution. Although an FI is permitted not to identify and take reasonable measures to verify the identities of the beneficial owners[70] of a financial institution which meets the criteria set out in paragraph 4.8.3(b), the FI should apply the following additional due diligence measures when it establishes a cross-border correspondent relationship to mitigate the associated risks: (a) collect sufficient information about the respondent institution to enable it to understand fully the nature of the respondent institution's

[69] Please refer to paragraph 4.1.4.

[70] It includes the individuals who ultimately own or control the customer and the person(s) on whose behalf the customer is acting (e.g. underlying customer(s) of a customer that is an FI). For the avoidance of doubt, the provisions of paragraphs 4.20 do not require an FI to conduct CDD on the underlying customers of a respondent institution.

		business (see paragraph 4.20.7); (b) determine from publicly available information the reputation of the respondent institution and the quality of regulatory supervision over the respondent institution by authorities in the jurisdictions in which it operates and/or is incorporated which perform functions similar to those of the RAs (see paragraph 4.20.8); (c) assess the AML/CFT controls of the respondent institution and be satisfied that the AML/CFT controls of the respondent institution are adequate and effective (see paragraph 4.20.9); (d) obtain approval from its senior management (see paragraph 4.20.10); and (e) understand clearly the respective AML/CFT responsibilities of the FI and the respondent institution within the cross-border correspondent relationship (see paragraph 4.20.11).
	4.20.6	Given that not all cross-border correspondent relationships pose the same level of ML/TF risks, the FI should adopt an RBA in applying the additional due diligence measures stated above, taking into account relevant factors such as: (a) the purpose of the cross-border correspondent relationship, the nature and expected volume and value of transactions; (b) how the respondent institution will provide services to its underlying customers through the account maintained by the FI for the respondent institution (hereafter referred to as "correspondent account"), including the potential use of the account by other respondent institutions through a "nested" correspondent relationship[71] and the purpose, and the direct respondent institution's control framework with respect to the "nested" correspondent

[71] Nested correspondent relationship refers to the use of a correspondent account by a number of respondent institutions through their relationships with the FI's direct respondent institution, to conduct transactions and obtain access to other financial services.

		relationship; (c) the types of underlying customers to whom the respondent institution intends to serve through the correspondent account, and the extent to which any of these underlying customers and their transactions are assessed as high risk by the respondent institution; and (d) the quality and effectiveness of the AML/CFT regulation as well as supervision by authorities in the jurisdictions in which the respondent institution operates and/or is incorporated[72].
	4.20.7	An FI should determine on a risk-sensitive basis the amount of information to collect about the respondent institution to enable it to understand the nature of the respondent institution's business including the respondent institution's management and ownership, the financial group to which the respondent institution belongs, major business activities, target markets, customer base and locations of customers. The FI may make reference to publicly available information to understand the respondent institution's business (e.g. where applicable, its corporate website, annual reports filed with stock exchanges, reputable newspapers and journals).
	4.20.8	When determining from publicly available information (e.g. public databases of regulatory and enforcement actions, news media sources or other types of open source information) the reputation of the respondent institution and the quality of regulatory supervision over the respondent institution, consideration should be given to whether and when the respondent institution has been subject to any targeted financial sanction, ML/TF

[72] Consideration may be given to country assessment reports and other relevant information published by international bodies (including the FATF, FATF-style regional bodies, the International Monetary Fund and the World Bank) which measure AML/CFT compliance and address ML/TF risks, lists issued by the FATF in the context of its International Cooperation Review Group process, ML/TF risk assessments and other relevant public information from national authorities.

		investigation or regulatory action.
	4.20.9	When assessing the AML/CFT controls of the respondent institution and ascertaining whether these controls are adequate and effective, the FI should have regard to the AML/CFT measures of the jurisdictions in which the respondent institution operates and/or is incorporated, and whether the AML/CFT controls of the respondent institution are subject to an independent audit. Information for assessing the AML/CFT controls may first be obtained from the respondent institution, for example, by way of a due diligence questionnaire, to facilitate the information collection and risk assessment processes. A more in-depth review of the respondent institution's AML/CFT controls should be conducted for any cross-border correspondent relationship that presents higher risks, possibly by interviewing compliance officers, conducting an on-site visit or reviewing the findings reported by internal or external auditors.
	4.20.10	An FI should obtain approval from its senior management before establishing a cross-border correspondent relationship. In this regard, the level of seniority of the member of an FI's senior management in making such approval should be commensurate with the assessed ML/TF risk.
	4.20.11	An FI should clearly understand the respective AML/CFT responsibilities of the FI and the respondent institution within the cross-border correspondent relationship, including the type and nature of services to be provided under the cross-border correspondent relationship, the respondent institution's responsibilities concerning compliance with AML/CFT requirements, and the conditions regarding the provision of documents, data or

		information on particular transactions and (where applicable) the underlying customers which should be provided by the respondent institution upon the FI's request. The level of detail may vary having regard to the nature of the cross-border correspondent relationship and the associated ML/TF risks. For example, an FI may also consider to impose potential restrictions on the use of the correspondent account by the respondent institution (e.g. limiting transaction types, volumes, etc.) in accordance with its terms of business when the ML/TF risks become higher.
<u>Direct access to the correspondent account by the underlying customers of a respondent institution</u>		
	4.20.12	Where a respondent institution meets the criteria set out in paragraph 4.8.3(b) and its underlying customers not being the customers of the FI (having regard to the definition of "customer" in paragraph 4.1.6) are allowed to directly access and operate the correspondent account[73], the FI should take further steps [74] and be satisfied that the respondent institution: (a) has conducted CDD on the underlying customers having direct access to the correspondent account, including verifying their identities and continuously monitoring its business relationships with them, in accordance with requirements similar to those imposed under the AMLO; and (b) will, upon the FI's request, provide documents, data or information obtained by the respondent

[73] For example, where an FI provides its electronic trading system for a respondent institution under a white label arrangement which permits the underlying customers of the respondent institution to submit orders directly to the FI for execution, and the identities of those underlying customers are not known to the FI. For the avoidance of doubt, where a respondent institution does not meet the criteria set out in paragraph 4.8.3(b), the FI should identify and take reasonable measures to verify the identities of the underlying customers of the respondent institution, whether or not the underlying customers have direct access to the correspondent account.

[74] In this regard, the FI may also consider conducting sample tests from time to time.

		institution in relation to those customers in accordance with requirements similar to those imposed under the AMLO.
<u>Ongoing monitoring</u>		
s.5(1)(a), Sch. 2	4.20.13	An FI should monitor the cross-border correspondent relationship in accordance with the guidance set out in Chapter 5, including: (a) on a regular basis and/or upon trigger events, reviewing the information obtained by the FI from applying the additional due diligence measures under paragraph 4.20.5 in the course of establishing the cross-border correspondent relationship with the respondent institution[75], together with other existing CDD records of the respondent institution, to ensure that the documents, data and information of the respondent institution obtained are up-to-date and relevant; and (b) monitoring transactions of the respondent institution with a view to detecting any unexpected or unusual activities or transactions, and any changes in the risk profile of the respondent institution for compliance with AML/CFT measures and applicable targeted financial sanctions. Where unusual activities or transactions are detected, the FI should follow up with the respondent institution by making a request for information on any particular transactions, and where applicable, more information on the

[75] If these additional due diligence measures have not previously been performed by the FI, the FI should do so during the review.

		underlying customers of the respondent institution on a risk-sensitive basis[76].
<u>Cross-border correspondent relationships with related foreign financial institutions</u>		
	4.20.14	Where a cross-border correspondent relationship is established with a related foreign financial institution, an FI may adopt a streamlined approach to applying additional due diligence measures and other risk mitigating measures for the cross-border correspondent relationship. The FI may rely on its group AML/CFT programme for this purpose. It may be sufficient for the FI to demonstrate its compliance with the requirements set out in paragraphs 4.20.5 to 4.20.13 by performing a documented assessment and satisfying itself that: (a) the group policy which applies to the respondent institution includes: (i) CDD, continuous monitoring of business relationships and record-keeping requirements similar to the requirements imposed under Schedule 2; (ii) the AML/CFT responsibilities of the respondent institution within the cross-border correspondent relationship; and (iii) group-wide AML/CFT Systems (including the compliance and audit functions, the provision of customer, account and transaction information to the FI's group-level compliance, audit or AML/CFT functions and the sharing of such

[76] Where the FI cannot obtain the requested information of the transactions and underlying customers in question, it may conclude that there are grounds for suspicion, leading to STR filing by the FI to the JFIU in accordance with paragraph 5.15, and triggering the need to conduct an appropriate review (including reassessing the risk of the respondent institution) of the cross-border correspondent relationship and apply appropriate measures to mitigate the risks identified. For the avoidance of doubt, where the level of ML/TF risks associated with the cross-border correspondent relationship becomes higher in the course of any review, the FI should take reasonable measures (e.g. performing enhanced measures by limiting the services provided or restricting individual transactions) to mitigate the risks.

		information for the purposes of CDD and ML/TF risk management[77]) which monitor and regularly review the effective implementation of CDD, continuous monitoring of business relationships and record-keeping requirements by the respondent institution and support effective group-wide ML/TF risk management; (b) the group policy is able to adequately mitigate any higher risk factors including country risk, customer risk, product/service/transaction risk, and delivery/distribution channel risk to which the respondent institution is exposed throughout the business relationship; and (c) the effective implementation of the group policy and group-wide AML/CFT Systems is supervised at the group level by a competent authority. The aforesaid assessment should be approved by an MIC of AML/CFT, MIC of Compliance or other appropriate senior management personnel.
<u>Cross-border correspondent relationships involving shell financial institutions</u>		
	4.20.15	An FI must not establish or continue a cross-border correspondent relationship with a shell financial institution. The FI should also take appropriate measures to satisfy itself that its respondent institutions do not permit their correspondent accounts to be used by shell financial institutions[78].

[77] This should include information and analysis of transactions or activities which appear unusual and could include an STR, its underlying information or the fact that an STR has been submitted. If the laws and regulations of the place where the respondent institution operates or is incorporated do not permit such sharing of information for group-wide ML/TF risk management, the FI should take appropriate measures to comply with the requirements in paragraphs 4.20.12 and 4.20.13.

[78] This includes a nested correspondent relationship under which the respondent institution uses the correspondent account to provide services to a shell financial institution with which it has a business relationship.

	4.20.16	For the purposes of this Guideline, a shell financial institution is a corporation that: (a) is incorporated in a place outside Hong Kong; (b) is authorised to carry on financial services businesses[79] in that place; (c) does not have a physical presence in that place (see paragraph 4.20.17); and (d) is not an affiliate[80] of a regulated financial group that is subject to effective group-wide supervision.
	4.20.17	A corporation is considered to have a physical presence[81] in a place or jurisdiction if: (a) the corporation carries on financial services businesses at any premises in that place or jurisdiction; and (b) at least one full-time employee of the corporation performs duties related to financial services businesses at those premises.
<u>Other group-wide considerations</u>		
	4.20.18	If an FI relies on a financial institution within the same group of companies (related FI) to establish a cross-border correspondent relationship and perform the additional due diligence and other risk mitigating measures set out in paragraphs 4.20.5 to 4.20.12 and 4.20.15, the FI should ensure that its related FI has taken into account the FI's own specific circumstances and business arrangements, and its particular cross-border correspondent relationship with the respondent institution. The

[79] In this context, this refers to businesses falling within the definition of the term "financial institutions" under the FATF Recommendations and which are conducted for or on behalf of customers.

[80] In this context, a corporation is an affiliate of another corporation if (a) the corporation is a subsidiary of the other corporation; or (b) at least one individual who is a controller of the corporation is at the same time a controller of the other corporation.

[81] In general, physical presence means meaningful mind and management located within a jurisdiction. The mere existence of a local agent or junior staff does not constitute physical presence.

		ultimate responsibility for ensuring that the additional due diligence and other relevant requirements are met remains with the FI.
	4.20.19	If an FI has cross-border correspondent relationships with several respondent institutions in different jurisdictions that belong to the same financial group, the FI whilst assessing each of the cross-border correspondent relationships independently should also take into account that these respondent institutions belong to the same group.

Chapter 5 - ONGOING MONITORING

General		
s.5(1), Sch. 2	5.1	Ongoing monitoring is an essential component of effective AML/CFT Systems. An FI must continuously monitor its business relationship with a customer by: (a) reviewing from time to time documents, data and information relating to the customer that have been obtained by the FI for the purpose of complying with the requirements imposed under Part 2 of Schedule 2 to ensure that they are up-to-date and relevant; (b) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the FI's knowledge of the customer, the customer's business, risk profile and source of funds; and (c) 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.
Keeping customer information up-to-date		
s.5(1)(a), Sch. 2	5.2	To ensure documents, data and information of a customer obtained are up-to-date and relevant[82], an FI should undertake reviews of existing CDD records of customers on a regular basis and/or upon trigger events[83]. Clear policies and procedures should be

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

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

		developed, especially on the frequency of periodic review or what constitutes a trigger event[84].
	5.3	All customers that present high ML/TF risks should be subject to a minimum of an annual review, or more frequent reviews if deemed necessary by the FI, to ensure the CDD information retained remains up-to-date and relevant.
Transaction monitoring systems and processes		
s.19(3), Sch.2	5.4	An FI should establish and maintain adequate systems and processes (e.g. the use of large transactions exception reports which help an FI to stay apprised of operational activities) to monitor transactions. The design, degree of automation and sophistication of transaction monitoring systems and processes should be developed appropriately having regard to the following factors: (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 FI should ensure that the transaction monitoring systems and processes can provide all relevant staff who are tasked with conducting transaction monitoring and investigation with timely and sufficient information required to identify, analyse and effectively monitor customers' transactions.
	5.6	An FI should ensure that the transaction monitoring systems and processes can support the ongoing monitoring of a business relationship in a holistic approach, which may include monitoring activities of

[84] Examples of trigger events are set out in paragraph 8 of Appendix C.

		a customer's multiple accounts within or across lines of business, and related customers' accounts within or across lines of business. This means preferably the FI adopts a relationship-based approach rather than on a transaction-by-transaction basis.
	5.7	In designing transaction monitoring systems and processes, including (where applicable) setting of parameters and thresholds, an FI should take into account the transaction characteristics, which may include: (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 FI should regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including (where applicable) parameters and thresholds adopted. The parameters and thresholds should be properly documented and independently validated to ensure that they are appropriate to its operations and context.
Risk-based approach to monitoring		
s.5(4) & (5), Sch. 2	5.9	FIs should conduct ongoing monitoring in relation to all business relationships following the RBA. The extent of monitoring (e.g. frequency and intensity of monitoring) should be commensurate with the ML/TF risk profile of the customer. Where the ML/TF risks are higher, the FI should conduct enhanced monitoring. In lower risk situations, the FI may reduce the extent of monitoring.

s.5(3), Sch. 2	5.10	FIs must take additional measures to compensate for any risk of ML/TF in monitoring business relationships involving (a) a customer not having been physically present for identification purposes; (b) a customer or a beneficial owner of a customer being a non-Hong Kong PEP; and (c) a customer or a beneficial owner of a customer being involved in a situation referred to in section 15 of Schedule 2.
	5.11	FIs should be vigilant for changes of the basis of the business relationship with the customer over time. These may include where: (a) new products or services that pose higher risk are entered into; (b) new corporate or trust structures are created; (c) the stated activity or turnover of a customer changes or increases; or (d) the nature of transactions changes or their volume or size increases, etc.
	5.12	Where the basis of the business relationship changes significantly, FIs should carry out further CDD procedures to ensure that the ML/TF risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures must take account of the above changes.
<u>Review of transactions</u>		
s.5(1)(b) & (c), Sch. 2	5.13	An FI should take appropriate steps (e.g. examining the background and purposes of the transactions; making appropriate enquiries to or obtaining additional CDD information from a customer) to identify if there are any grounds for suspicion, when: (a) the customer's transactions are not consistent with the FI's knowledge of the customer, the customer's business, risk profile or source of funds; (b) the FI identifies transactions that (i) are complex, unusually large in amount or of an unusual

		pattern, and (ii) have no apparent economic or lawful purpose[85].
	5.14	Where the FI conducts enquiries and obtains what it considers to be a satisfactory explanation of the activity or transaction, it may conclude that there are no grounds for suspicion, and therefore take no further action. Even if no suspicion is identified, the FI should consider updating the customer risk profile based on any relevant information obtained.
	5.15	However, where the FI cannot obtain a satisfactory explanation of the transaction or activity, it may conclude that there are grounds for suspicion. In any event where there is any suspicion identified during transaction monitoring, an STR should be made to the JFIU.
	5.16	An FI should be aware that making enquiries to customers, when conducted properly and in good faith, will not constitute tipping-off. However, if the FI reasonably believes that performing the CDD process will tip off the customer, it may stop pursuing the process. The FI should document the basis for its assessment and file an STR to the JFIU.
	5.17	The findings and outcomes of steps taken by the FI in paragraph 5.13, as well as the rationale of any decision made after taking these steps, should be properly documented in writing and be available to RAs, other competent authorities and auditors.
	5.18	Where cash transactions (including deposits and withdrawals) and third-party deposits and payments are being proposed by customers, and such requests are not in accordance with the customer's profile and normal commercial practices, FIs must approach

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

		such situations with caution and make relevant further enquiries[86].
	5.19	Ongoing monitoring of a customer's account involving cash, third-party deposits and payments should be enhanced. An FI should be alert to the red flags relating to cash and third-party transactions, having regard to the list of illustrative indicators of suspicious transactions and activities set out in Appendix B.
	5.20	Where the FI has been unable to satisfy itself that any cash transaction or third-party deposit or payment is reasonable, and therefore considers it suspicious, it should make an STR to the JFIU.

[86] Guidance on third-party deposits and payments is provided in Chapter 11.

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 [87] 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 FIs, and are listed below. (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

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

		occurs); or the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs as a result of the training).
s.6(1), 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 FI seeking such a licence should write to the Security Bureau.
Financial sanctions & proliferation financing		
s.3(1), UNSO	6.7	UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the UNSC, including targeted financial sanctions [88] against certain persons and entities designated by the UNSC or its Committees. Designated persons and entities are specified by notice published in the Gazette or on the website of the Commerce and Economic Department Bureau. Except under the authority of a licence granted by the Chief Executive, it is an offence: (a) to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of, (i) designated persons or entities, (ii) persons or entities acting on behalf or at the direction of the designated persons or entities mentioned in (i), or (iii) entities owned or controlled by any persons or entities mentioned in (i) or (ii); or (b) to deal with, directly or indirectly, any funds or other financial assets or economic resources belonging to, or owned or controlled by, persons

[88] 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 persons and entities falling within paragraph 6.7(a).

		and entities falling within paragraph (a) above.
Applicable UNSO Regulation	6.8	The Chief Executive may grant a licence for making available any funds or other financial assets or economic resources to; or dealing with any funds or other financial assets or economic resources belonging to, or owned or controlled by, persons or entities falling within paragraph 6.7(a) under specified circumstances in accordance with the provisions of the relevant regulation made under the UNSO. An FI seeking such a licence should write to the Commerce and Economic Development Bureau.
	6.9	To combat PF, the UNSC adopts a two-tiered approach through resolutions made under Chapter VII of the UN Charter imposing mandatory obligations on UN member states: (a) global approach under UNSCR 1540 (2004) and its successor resolutions; and (b) country-specific approach under UNSCR 1718 (2006) against the Democratic People's Republic of Korea (DPRK) and UNSCR 2231 (2015) against the Islamic Republic of Iran (Iran) and their successor resolutions.
s.4, WMD(CPS)O	6.10	The counter 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.
<u>Sanctions imposed by other jurisdictions</u>		
	6.11	While FIs do not normally have any obligation under Hong Kong laws to have regard to unilateral sanctions imposed by other organisations or authorities in other jurisdictions, an FI operating internationally will need to be aware of the scope and focus of relevant sanctions regimes in those jurisdictions. Where these sanctions regimes may

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

		UNSCRs and sanctions lists are included in the database as soon as practicable after they are promulgated by the UNSC and regardless of whether the relevant sanctions have been implemented by legislation in Hong Kong.
	6.15	An FI should include in its database (i) the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau; and (ii) the lists that RAs draw to the attention of FIs from time to time. The database should be subject to timely update whenever there are changes, and should be made easily accessible by relevant staff.
	6.16	To avoid establishing business relationship or conducting transactions with any terrorist suspects and possible persons or entities falling within paragraph 6.7(a), an FI should implement an effective screening mechanism [89], which should include: (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 other connected parties as defined in paragraph 4.2.13 and PPTAs of a customer using an RBA.
	6.18	When possible name matches are identified during screening, an FI should conduct enhanced checks to

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

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

Chapter 7 – SUSPICIOUS TRANSACTION REPORTS AND LAW ENFORCEMENT REQUESTS

General issues		
s.25A(1) & (7), DTROP & OSCO, s.12(1) & 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 FI is concerned, when a transaction or a series of transactions of a customer is not consistent with the FI's knowledge of the customer, or is unusual (e.g. in a pattern that has no apparent economic or lawful purpose), the FI should take appropriate steps to further examine the transactions and identify if there is any suspicion (see paragraphs 5.13 to 5.20).

	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 FI should file an STR even where no transaction has been conducted by or through the FI[90]; and (b) the STR must 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 FI, but has not yet been reported to the JFIU.
AML/CFT Systems in relation to suspicious transaction reporting		
	7.7	An FI should implement appropriate AML/CFT Systems in order to fulfil its statutory reporting obligation, and properly manage and mitigate the risks associated with any customer or transaction involved in an STR. The AML/CFT Systems should include: (a) appointment of an MLRO (see Chapter 3); (b) implementing clear policies and procedures over

[90] 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.

		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	The FI should have measures in place to check, on an ongoing basis, that its AML/CFT Systems in relation to suspicious transaction reporting comply with relevant legal and regulatory requirements and operate effectively. The type and extent of the measures to be taken should be appropriate having regard to the risk of ML/TF as well as the nature and size of the business.
<u>Money laundering reporting officer</u>		
	7.9	An FI should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the JFIU and law enforcement agencies. The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions of the MLRO should include having oversight of: (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. To fulfil these functions, all FIs must ensure that the MLRO receives full co-operation from all staff and full access to all relevant documentation so that he is in a position to decide whether attempted or actual ML/TF is suspected or known.
<u>Identifying suspicious transactions</u>		
	7.10	An FI should provide sufficient guidance to its staff to enable them to form suspicion or to recognise the signs when ML/TF is taking place. The guidance

		should take into account the nature of the transactions and customer instructions that staff is likely to encounter, the type of product or service and the means of delivery.
	7.11	An FI may adopt, where applicable, the "SAFE" approach promoted by the JFIU, which includes: (a) screening the account for suspicious indicators; (b) asking the customers appropriate questions; (c) finding out the customer's records; and (d) evaluating all the above information. Details of the "SAFE" approach are available at JFIU's website (www.jfiu.gov.hk).
	7.12	An FI should have reasonable policies and procedures to identify and analyse relevant red flags of suspicious activities for its customer accounts. A list of non-exhaustive illustrative indicators of suspicious transactions and activities is provided in Appendix B to assist an FI in determining what types of red flags are relevant to its businesses, taking into account the nature of customer transactions, risk profile of the customers and business relationships. The list is intended solely to provide an aid to FIs, and must not be applied by FIs as a routine instrument without analysis or context. The detection of any relevant red flag by an FI however should prompt further investigations and be a catalyst towards making at least initial enquiries about the source of funds. FIs should also be aware of elements of individual transactions and situations that might give rise to suspicion of TF in certain circumstances. The FATF publishes studies of methods and trends of TF from time to time, and FIs may refer to the FATF website for additional information and guidance.
<u>Internal reporting</u>		
	7.13	An FI 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 must reach the MLRO without undue delay.
	7.14	While FIs may wish to set up internal systems that allow staff to consult with supervisors or managers before sending a report to the MLRO, under no circumstances should reports raised by staff be filtered out by supervisors or managers who have no responsibility for the money laundering reporting/compliance function. The legal obligation is to report as soon as it is reasonable to do so, so reporting lines should be as short as possible with the minimum number of people between the staff with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO.
s.25A(4), DTROP & OSCO, s.12(4), UNATMO	7.15	Once a staff member of an FI has reported suspicion to the MLRO in accordance with the policies and procedures established by the FI for the making of such reports, the statutory obligation of the staff member has been fully satisfied.
	7.16	The internal report should include sufficient details of the customer concerned and the information giving rise to the suspicion.
	7.17	The MLRO should acknowledge receipt of an internal report and provide a reminder of the obligation regarding tipping-off to the reporting staff member upon internal reporting.
	7.18	When evaluating an internal report, the MLRO must take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the FI concerning the customers to which the report relates. This may include: (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[91].
	7.19	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>		
	7.20	If after completing the review of the internal report, the MLRO decides that there are grounds for knowledge or suspicion, he should disclose the information to the JFIU as soon as it is reasonable to do so after his evaluation is complete together with the information on which that knowledge or suspicion is based. Dependent on when knowledge or suspicion arises, an STR may be made either before a suspicious transaction or activity occurs (whether the intended transaction ultimately takes place or not), or after a transaction or activity has been completed.
	7.21	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

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

		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.
	7.22	In the event that an urgent reporting is required (e.g. where a customer has instructed the FI to move funds or other property, close the account, make cash available for collection, or carry out significant changes to the business relationship, etc.), particularly when the account is part of an ongoing law enforcement investigation, an FI should indicate this in the STR. Where exceptional circumstances exist in relation to an urgent reporting, an initial notification by telephone should be considered.
	7.23	An FI is recommended to indicate any intention to terminate a business relationship in its initial disclosure to the JFIU.
	7.24	An FI should ensure STRs filed with the JFIU are of high quality taking into account feedback and guidance provided by the JFIU and RAs from time to time.
	7.25	The JFIU recognises the importance of having effective feedback procedures in place and therefore, provides feedback both in its quarterly report [92] and other appropriate platform when needed.
<u>Post reporting matters</u>		
s.25A(2)(a), DTROP & OSCO, s.12(2B)(a), UNATMO	7.26	The JFIU will acknowledge receipt of an STR made by an FI under section 25A of both the DTROP and the OSCO, and section 12 of the UNATMO. If there is no need for imminent action, e.g. the issue of a restraint order on an account, consent will usually be

[92] 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. FIs 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.

		given for the institution to operate the account under the provisions of section 25A(2) of both the DTROP and the OSCO, and section 12(2B)(a) of the UNATMO. The JFIU may, on occasion, seek additional information or clarification with an FI of any matter on which the knowledge or suspicion is based. Otherwise, the FI should take appropriate action and seek legal advice where necessary.
s.25A(2), DTROP & OSCO, s.12(2), UNATMO	7.27	Filing a report to the JFIU provides FIs with a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report, provided: (a) the report is made before the FI undertakes the disclosed acts and the acts (transaction(s)) are undertaken with the consent of the JFIU; or (b) the report is made after the FI has performed the disclosed acts (transaction(s)) and the report is made on the FI's own initiative and as soon as it is reasonable for the FI to do so.
	7.28	However, the statutory defence stated in paragraph 7.27 does not absolve an FI from the legal, reputational or regulatory risks associated with the account's continued operation. An FI should also be aware that a "consent" response from the JFIU to a pre-transaction report should not be construed as a "clean bill of health" for the continued operation of the account or an indication that the account does not pose a risk to the FI.
	7.29	An FI should conduct an appropriate review of a business relationship upon the filing of an STR to the JFIU, irrespective of any subsequent feedback provided by the JFIU, and apply appropriate risk mitigating measures. Filing a report with the JFIU and continuing to operate the relationship without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified is not acceptable. If necessary, the issue should be escalated to the FI's senior management to determine how to handle the

		relationship concerned to mitigate any potential legal or reputational risks posed by the relationship in line with the FI's business objectives, and its capacity to mitigate the risks identified.
	7.30	An FI should be aware that the reporting of a suspicion in respect of a transaction or event does not remove the need to report further suspicious transactions or events in respect of the same customer. Further suspicious transactions or events, whether of the same nature or different to the previous suspicion, must continue to be reported to the MLRO who should make further reports to the JFIU if appropriate.
Record-keeping		
	7.31	An FI must establish and maintain a record of all ML/TF reports made to the MLRO. The record should include details of the date the report was made, the staff members subsequently handling the report, the results of the assessment, whether the internal report resulted in an STR to the JFIU, and information to allow the papers relevant to the report to be located.
	7.32	An FI must establish and maintain a record of all STRs made to the JFIU. The record should include details of the date of the STR, the person who made the STR, and information to allow the papers relevant to the STR to be located. This register may be combined with the register of internal reports, if considered appropriate.
Requests from law enforcement agencies		
	7.33	An FI may receive various requests from law enforcement agencies, e.g. search warrants, production orders, restraint orders or confiscation orders, pursuant to relevant legislation in Hong Kong. These requests are crucial to aid law enforcement agencies, to carry out investigations as well as restrain and confiscate illicit proceeds. Therefore, an FI should establish clear policies and

		procedures to handle these requests in an effective and timely manner, including allocation of sufficient resources. An FI should appoint a staff member as the main point of contact with law enforcement agencies.
	7.34	An FI should respond to any search warrant and production order within the required time limit by providing all information or materials that fall within the scope of the request. Where an FI encounters difficulty in complying with the timeframes stipulated, the FI should at the earliest opportunity contact the officer-in-charge of the investigation for further guidance.
s.10 & s.11, DTROP, s.15 & s.16, OSCO, s.6, UNATMO	7.35	During a law enforcement investigation, an FI may be served with a restraint order which prohibits the dealing with particular funds or property pending the outcome of an investigation. An FI must ensure that it is able to 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 FIs should consider what, if any, funds or property may be utilised subject to the laws of Hong Kong.
s.3, DTROP, s.8, OSCO, s.13, UNATMO	7.36	Upon the conviction of a defendant, a court may order the confiscation of his criminal proceeds and an FI may be served with a confiscation order in the event that it holds funds or other property belonging to that defendant that are deemed by the Courts to represent his benefit from the crime. A court may also order the forfeiture of property where it is satisfied that the property is terrorist property.
	7.37	When an FI receives a request from a law enforcement agency, e.g. search warrant or production order, in relation to a particular customer or business relationship, the FI should timely assess the risk involved and the need to conduct an appropriate review on the customer or the business relationship to determine whether there is any

		suspicion, and should also be aware that the customer subject to the request can be a victim of crime.

Chapter 8 – RECORD-KEEPING

General		
	8.1	Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps the investigating authorities to establish a financial profile of a suspect, trace the criminal or terrorist property or funds and assists the Court to examine all relevant past transactions to assess whether the property or funds are the proceeds of or relate to criminal or terrorist offences. Record-keeping also enables an FI to demonstrate compliance with the requirements set out in the AMLO, this Guideline and other relevant guidance promulgated by the RAs from time to time.
	8.2	An FI should maintain CDD information, transaction records and other records that are necessary and sufficient to meet the statutory and regulatory requirements, that are appropriate to the nature, size and complexity of its businesses. The FI should ensure that: (a) the audit trail for funds moving through the FI that relate to any customer and, where appropriate, the beneficial owner of the customer, account or transaction is clear and complete; (b) all CDD information and transaction records are available swiftly to RAs, 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 RAs.

Retention of records relating to CDD and transactions		
	8.3	An FI should keep:
s.20(1)(b)(i), Sch. 2		(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, situations where special requirements are required, additional due diligence measures and other requirements for cross-border correspondent relationships, and when taking simplified and enhanced measures[93];
s.2(1)(c), Sch. 2		(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;
s.20(1)(b)(ii), Sch. 2		(d) the original or a copy of the records and documents relating to the customer's account (e.g. account opening form; risk assessment form[94]) and business correspondence[95] 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

[93] For SDD, please refer to paragraphs 4.8; for situations where special requirements are required, please refer to paragraphs 4.9 to 4.14; for additional due diligence measures and other requirements for cross-border correspondent relationships, please refer to paragraphs 4.20; for simplified and enhanced measures, please refer to paragraph 4.1.2.

[94] This refers to a document which FIs may use to document the assessment of ML/TF risk levels associated with customers or business relationships. For example, the ML/TF risk rating of a customer (see paragraph 2.16), the assessment of ML/TF risk associated with the previous PEP status of the former non-Hong Kong PEPs, the former Hong Kong PEPs or the former international organisation PEPs (see paragraphs 4.11.19 and 4.11.25), etc.

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

		(e) the results of any analysis undertaken (e.g. inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose).
s.20(2), (3) & (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 thresholds (i.e. $8,000 for wire transfers and $120,000 for other types of transactions[96]), an FI should keep all documents and records mentioned in paragraph 8.3 for a period of at least five years after the date of the occasional transaction.
s.20(1)(a), Sch. 2	8.5	FIs should maintain the original or a copy of the documents, and a record of the data and information, obtained in connection with each transaction the FI carries out, both domestic and international, which should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.
s.20(2), Sch. 2	8.6	All documents and records mentioned in paragraph 8.5 should be kept for a period of at least five years after the completion of a transaction, regardless of whether the business relationship ends during the period.
s.21, Sch. 2	8.7	If the record consists of a document, either the original of the document should be retained or a copy of the document should be kept on microfilm or in the database of a computer. If the record consists of data or information, such record should

[96] For the avoidance of doubt, FIs that are LCs or SFC-licensed VAS Providers should not carry out occasional transactions. FIs should also refer to the guidance provided in paragraph 12.9.1 for occasional transaction that is a virtual asset transfer.

		be kept either on microfilm or in the database of a computer.
s.20(4), Sch. 2	8.8	An RA may, by notice in writing to an FI, require it to keep the records relating to a specified transaction or customer for a period specified by the RA that is longer than those referred to in paragraphs 8.4 and 8.6, where the records are relevant to an ongoing criminal or other investigation carried out by the RA, or to any other purposes as specified in the notice.
Part 3, Sch. 2	8.9	Irrespective of where CDD and transaction records are held, an FI is required to comply with all legal and regulatory requirements in Hong Kong, especially Part 3 of Schedule 2.
Records kept by intermediaries		
s.18(4)(b), Sch. 2	8.10	Where customer identification and verification documents are held by an intermediary on which the FI is relying to carry out CDD measures, an FI concerned remains responsible for compliance with all record-keeping requirements. The FI should ensure that the intermediary being relied on has systems in place to comply with all the record-keeping requirements under the AMLO and this Guideline (including the requirements of paragraphs 8.3 to 8.9), and that documents and records will be provided by the intermediary as soon as reasonably practicable after the intermediary receives the request from the FI.
s.18(4)(a), Sch. 2	8.11	For the avoidance of doubt, an FI that relies on an intermediary for carrying out a CDD measure should immediately obtain the data or information that the intermediary has obtained in the course of carrying out that measure.
	8.12	An FI should ensure that an intermediary will pass the documents and records to the FI, upon termination of the services provided by the intermediary.

Chapter 9 – STAFF TRAINING

	9.1	Ongoing staff training is an important element of an effective system to prevent and detect ML/TF activities. The effective implementation of even a well-designed internal control system can be compromised if staff using the system is not adequately trained.
	9.2	It is an FI's responsibility to provide adequate training for its staff so that they are adequately trained to implement its AML/CFT Systems. The scope and frequency of training should be tailored to the specific risks faced by the FI and pitched according to the job functions, responsibilities and experience of the staff. New staff should be required to attend initial training as soon as possible after being hired or appointed. Apart from the initial training, an FI should also provide refresher training regularly to ensure that its staff are reminded of their responsibilities and are kept informed of new developments related to ML/TF.
	9.3	An FI should implement a clear and well articulated policy for ensuring that relevant staff receive adequate AML/CFT training.
	9.4	Staff should be made aware of: (a) their FI's and their own personal statutory obligations and the possible consequences for failure to comply with CDD and record-keeping requirements under the AMLO; (b) their FI's and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROP, the OSCO and the UNATMO; (c) any other statutory and regulatory obligations that concern their FIs 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 FI'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 FI 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 FI; and (ii) the need for identifying and reporting of any suspicious transactions to the MLRO, and the offence of tipping-off; (b) front-line personnel who are dealing directly with the public: (i) the importance of their roles in the FI's ML/TF strategy, as the first point of contact with potential money launderers; (ii) the FI'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 FI'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 FI is encouraged to consider using a mix of training techniques and tools in delivering training, depending on the available resources and learning needs of their staff. These techniques and tools may include on-line learning systems, focused classroom training, relevant videos as well as paper- or intranet-based procedures manuals. An FI may consider including available FATF papers and typologies as part of the training materials. The FI should be able to demonstrate to the RA that all materials should be up-to-date and in line with current requirements and standards.
	9.7	No matter which training approach is adopted, an FI should maintain records of who have been trained, when the staff received the training and the type of the training provided. Records should be maintained for a minimum of 3 years.
	9.8	An FI should monitor the effectiveness of the training. This may be achieved by: (a) testing staff's understanding of the FI's policies and procedures to combat ML/TF, the

		understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions; (b) monitoring the compliance of staff with the FI's AML/CFT Systems as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken; and (c) monitoring attendance and following up with staff who miss such training without reasonable cause.

Chapter 10 – WIRE TRANSFERS

General		
	10.1	This Chapter primarily applies to authorized institutions and money service operators. Other FIs should also comply with section 12 of Schedule 2 and the guidance provided in this Chapter if they act as an ordering institution, an intermediary institution or a beneficiary institution as defined under the AMLO. Where an FI is the originator or recipient of a wire transfer, it is not acting as an ordering institution, an intermediary institution or a beneficiary institution and thus is not required to comply with the requirements under section 12 of Schedule 2 or this Chapter in respect of that transaction.
s.1(4) & s.12(11), Sch. 2	10.2	A wire transfer is a transaction carried out by an institution (the ordering institution) on behalf of a person (the originator) by electronic means with a view to making an amount of money available to that person or another person (the recipient) at an institution (the beneficiary institution), which may be the ordering institution [97] or another institution, whether or not one or more other institutions (intermediary institutions) participate in completion of the transfer of the money. An FI should follow the relevant requirements set out in this Chapter with regard to its role in a wire transfer.
	10.3	The requirements set out in section 12 of Schedule 2 and this Chapter are also applicable to wire transfers using cover payment mechanism (e.g. MT202COV payments)[98].
s.12(2), Sch. 2	10.4	Section 12 of Schedule 2 and this Chapter do not apply to the following wire transfers:

[97] For example, a wire transfer conducted between branches of the same FI.

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

		(a) a wire transfer between two FIs as defined in the AMLO if each of them acts on its own behalf; (b) a wire transfer between an FI as defined in the AMLO and a foreign institution[99] 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, 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 card, debit card or prepaid card); (ii) the card is not used as a payment system to effect a person-to-person transfer; and (iii) the number (or equivalent unique identifier) of the credit card, debit card 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 must ensure that a wire transfer of amount equal to or above $8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information: (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;

[99] For the purposes 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.

		(c) the originator's address or, the originator's customer identification number [100] 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 must ensure that a wire transfer of amount below $8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information: (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.
	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.

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

	10.8	For a wire transfer of amount equal to or above $8,000 (or an equivalent amount in any other currency), an ordering institution must ensure that the required originator information accompanying the wire transfer is accurate.
s.3(1)(d) & (1A), Sch. 2	10.9	For an occasional wire transfer involving an amount equal to or above $8,000 (or an equivalent amount in any other currency), an ordering institution must verify the identity of the originator. For an occasional wire transfer below $8,000 (or an equivalent amount in any other currency), the ordering institution is in general not required to verify the originator's identity, except when several transactions are carried out which appear to the ordering institution to be linked and are equal to or above $8,000 (or an equivalent amount in any other currency), or when there is a suspicion of ML/TF.
s.12(7), Sch. 2	10.10	An ordering institution may bundle a number of wire transfers from a single originator into a batch file for transmission to a recipient or recipients in a place outside Hong Kong. In such cases, the ordering institution may only include the originator's account number or, in the absence of such an account, a unique reference number in the wire transfer but the batch file should contain required and accurate originator information, and required recipient information, that is fully traceable within the recipient country.
s.12(6), Sch. 2	10.11	For a domestic wire transfer [101], 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

[101] 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.

		traceability of the wire transfer.
s.12(6), Sch. 2	10.12	If an ordering institution chooses not to include complete required originator information as stated in paragraph 10.11, it must, on the request of the institution to which it passes on the transfer instruction or the RA, provide complete required originator information within 3 business days after the request is received. In addition, such information should be made available to law enforcement agencies immediately upon request.
s.19(2), Sch. 2	10.13	An ordering institution should establish and maintain effective procedures to ensure that proper safeguards exist to prevent 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	10.14	An intermediary institution must ensure that all originator and recipient information which accompanies the wire transfer is retained with the transfer and is transmitted to the institution to which it passes on the transfer instruction.
	10.15	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	10.16	An intermediary institution must establish and maintain effective procedures for identifying and handling incoming wire transfers that do not comply with the relevant originator or recipient information requirements, which include: (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	10.17	In respect of the risk-based policies and procedures referred to in paragraph 10.16, if a cross-border wire transfer is not accompanied by the required originator information or required recipient information, the intermediary institution must as soon as reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, the intermediary institution should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved.

s.12(10)(b), Sch. 2	10.18	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 must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
Beneficiary institutions		
s.19(2), Sch. 2	10.19	A beneficiary institution must establish and maintain effective procedures for identifying and handling incoming wire transfers that do not comply with the relevant originator or recipient information requirements, which include: (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	10.20	In respect of the risk-based policies and procedures referred to in paragraph 10.19, if a domestic or cross-border wire transfer is not accompanied by the required originator information or required recipient information, the beneficiary institution must as soon as reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, the beneficiary institution should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved.
s.12(9)(b) & s.12(10)(b), Sch.2	10.21	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 must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
s.3(1) & (1A), Sch. 2	10.22	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 – THIRD-PARTY DEPOSITS AND PAYMENTS

General		
	11.1	When a customer uses a third party[102] to pay for or receive the proceeds of investment, there is a risk that the arrangement may be used to disguise the true beneficial owner or the source of funds. There are increased risks that these investment transactions are linked to predicate offences in securities markets (such as insider dealing and market manipulation) or used to launder illicit proceeds obtained elsewhere.
s.23(b), Sch. 2	11.2	An FI must take all reasonable measures to mitigate the ML/TF risks associated with transactions involving third-party deposits and payments, having regard to the provisions in this Guideline as well as relevant circulars and frequently asked questions published by the SFC from time to time.
Policies and procedures		
	11.3	Third-party deposits or payments should be accepted only under exceptional and legitimate circumstances and when they are reasonably in line with the customer's profile and normal commercial practices. Before an FI accepts any third-party deposit or payment arrangement, it should ensure that adequate policies and procedures are put in place to mitigate the inherently high risk and meet all applicable legal and regulatory requirements. These policies and procedures should be approved by senior management and address, among others:

[102] For the purposes of Chapter 11, "third party" means any person other than the customer.

		(a) the exceptional and legitimate circumstances under which third-party deposits or payments[103] may be accepted and their evaluation criteria; (b) the monitoring systems and controls for identifying transactions involving third-party deposits in the form of funds (i.e. fiat currency)[104]; (c) if applicable, the due diligence process for assessing whether third-party deposits or payments meet the evaluation criteria for acceptance; (d) if an FI allows the due diligence on the source of a deposit or the evaluation of a third-party deposit to be completed after settling transactions with the deposited funds (please refer to paragraphs 11.9 to 11.11) in exceptional situations, the identification of those exceptional situations and the risk management policies and procedures concerning the conditions under which such delayed due diligence or evaluation may be allowed[105]; (e) the enhanced monitoring of client accounts involving third-party deposits or payments[106], and the reporting of any ML/TF suspicions identified to the JFIU; and (f) the respective designated managers or staff members responsible for carrying out these policies and procedures. An MIC of AML/CFT, MIC of Compliance or other appropriate senior management personnel should

[103] Given that the need for third-party payments should be rare and normal commercial practices may differ, circumstances which may be considered to be exceptional and legitimate for third-party payments may not be the same as or similar to those for third-party deposits.

[104] For example, an FI may require the client to confirm whether a cheque deposit made for the account of the client has originated from the bank account of client or a third party, and provide an image of the cheque showing the name of its drawer.

[105] For the avoidance of doubt, delayed due diligence on the source of a deposit or evaluation of a third-party deposit should be allowed only when there is no suspicion of ML/TF.

[106] The extent of enhanced monitoring should be commensurate with the ML/TF risks posed by the third parties. For example, closer monitoring should be applied to deposits from third parties who are not immediate family members (e.g. a spouse, parent or child), beneficial owners or affiliated companies of the clients, regulated custodians or lending institutions.

		be designated to oversee the proper design and implementation of these policies and procedures.
	11.4	To facilitate the prompt identification of the sources of deposits in the form of funds, FIs are strongly encouraged to require their clients to designate bank accounts held in their own names or the names of any acceptable third parties for the making of all deposits. This will make it easier for FIs to ascertain whether deposits have originated from their clients or any acceptable third parties[107].
Due diligence process for assessing third-party deposits and payments		
	11.5	Due diligence process for assessing third-party deposits and payments should include: (a) critically evaluating the reasons and the need for third-party deposits or payments; (b) taking reasonable measures on a risk-sensitive basis to: (i) verify the identities of the third parties; and (ii) ascertain the relationship between the third parties and the customers; (c) obtaining the approval of the MIC of AML/CFT, another member of senior management with a relevant role at the FI with respect to AML/CFT, or MLRO (hereafter referred to as "third-party deposit or payment approvers") for the acceptance for a third-party deposit or payment; and (d) documenting the findings of inquiries made and corroborative evidence obtained during the due diligence process as well as the approval of a third-party deposit or payment.

[107] Likewise, if applicable, the use of designated bank accounts held in the names of any acceptable third parties for the making of fund withdrawals will make it easier for FIs to complete the necessary due diligence to determine the acceptability of a third-party payee before effecting a third-party fund payment.

	11.6	While a standing approval may be given by third-party deposit or payment approvers for accepting deposits or payments from or to a particular third party after assessing the risks and reasonableness of the third-party arrangement, the standing approval should be subject to review periodically or upon trigger events to ensure that it remains appropriate.
	11.7	Given that not all third-party payors and payees pose the same level of ML/TF risk[108], an FI should apply enhanced scrutiny to those third parties which might pose higher risks, and require the dual approval of deposits or payments from or to such third parties by the third-party deposit or payment approvers for enhanced control.
	11.8	An FI should exercise extra caution when the relationship between the customer and the third party is hard to verify, the customer is unable to provide details of the identity of the third-party payor for verification before the deposit is made, or one third party is making or receiving payments for or from several seemingly unrelated customers.
Delayed due diligence on the source of a deposit or evaluation of a third-party deposit in the form of funds		
	11.9	An FI should perform due diligence on the source of a deposit and evaluation of any third-party deposit (hereafter referred to as "third-party deposit due diligence") before settling transactions with the deposited funds. However, FIs may, in exceptional situations, complete the third-party deposit due diligence after settling transactions with the deposited funds, provided that: (a) any risk of ML/TF arising from the delay in

[108] Examples of third parties that are generally considered to pose relatively low risks include immediate family members (e.g. a spouse, parent or child), beneficial owners or affiliated companies of the customers, or regulated custodians or lending institutions. Other third parties might pose higher risks.

		completing the third-party deposit due diligence can be effectively managed; (b) it is necessary to avoid interruption of the normal conduct of business with the customer[109]; and (c) the third-party deposit due diligence is completed as soon as possible after settling transactions with the deposited funds.
	11.10	If an FI allows third-party deposit due diligence to be delayed in exceptional situations, it should adopt appropriate risk management policies and procedures setting out the conditions under which the customer may utilise the deposited funds prior to the completion of the third-party deposit due diligence. These policies and procedures should include: (a) establishing a reasonable timeframe[110] for the completion of the third-party deposit due diligence, and the follow-up actions if the stipulated timeframe is exceeded (e.g. to suspend or terminate the business relationship); (b) placing appropriate limits on the number, types, and/or amount of transactions that can be performed[111]; (c) performing enhanced monitoring of transactions carried out by or for the customer; and (d) ensuring senior management is periodically informed of all cases involving delay in completing third-party deposit due diligence.

[109] An example of a situation where it may be necessary not to interrupt the normal conduct of business is when FIs are required to meet settlement obligations on behalf of its customers (e.g. to meet a margin call deadline) using funds the customer has deposited shortly before.

[110] In determining the reasonable timeframe for completing third-party deposit due diligence, an FI should take into account the ML/TF risks associated with the business relationship with a customer, e.g. a stricter timeframe is imposed on deposits for high risk customers.

[111] For example, prior to the completion of third-party deposit due diligence on the deposited funds, an FI may restrict a customer from withdrawing the subsequent sales proceeds arising from the disposal of investments purchased with the deposited funds (except to return funds to the payment source). In this regard, the FI should ensure that a standing authority or written direction is obtained from the client to return the funds to the third party's payment source (see sections 4 to 8 of the Securities and Futures (Client Money) Rules).

	11.11	If the third-party deposit due diligence cannot be completed within the reasonable timeframe set out in the FI's risk management policies and procedures, the FI should refrain from carrying out further transactions for the customer. The FI should assess whether there are grounds for knowledge or suspicion of ML/TF and filing an STR to the JFIU, particularly where the customer refuses without reasonable explanation to provide information or document requested by the FI, or otherwise refuses to cooperate with the third-party deposit due diligence process.

Chapter 12 – VIRTUAL ASSETS

12.1 Introduction		
	12.1.1	This Chapter provides guidance on the ML/TF risks in relation to virtual assets and the AML/CFT regulatory requirements and standards for addressing such risks. These include factors that should be taken into consideration when conducting risk assessments under an RBA, virtual asset-specific requirements in conducting CDD and ongoing monitoring, and requirements in relation to virtual asset transfers and third-party deposits and payments in the form of virtual assets. It also provides elaborations and explanations of existing requirements in this Guideline with respect to their application to virtual asset transactions and activities, and sets out non-exhaustive illustrative risk indicators for assessing ML/TF risks and indicators of suspicious transactions and activities in relation to virtual assets.
	12.1.2	This Chapter is applicable to FIs that are SFC-licensed VAS Providers, and LCs when carrying out businesses associated with virtual assets or businesses which give rise to ML/TF risks in relation to virtual assets[112].
	12.1.3	For the purposes of this Chapter, the term "virtual assets" means (i) any "virtual asset" as defined in section 53ZRA of the AMLO; and (ii) any security token. The term "security token" means a cryptographically secured digital representation of value which constitutes "securities" as defined in section 1 of Part 1 of Schedule 1 to the SFO.

[112] For example, when an LC offers products, services or transactions involving virtual assets, or when an LC's customer derives its funds or wealth substantially from virtual assets or carries out virtual asset businesses.

s.23(a) & (b), Sch. 2	12.1.4	An FI must take all reasonable measures to ensure that proper safeguards exist to prevent a contravention of any requirement under Part 2 or 3 of Schedule 2 and to mitigate the ML/TF risks in relation to virtual assets, having regard to the guidance and requirements set out in this Chapter as well as (where applicable) relevant circulars and frequently asked questions published by the SFC from time to time.
Potential uses of the virtual asset sector in the money laundering process		
	12.1.5	Virtual asset transactions are, in general, pseudonymous or anonymity-enhanced by nature. Illicit actors or money launderers could take advantage of the borderless nature and near-instantaneous transaction speed that virtual assets provide. In addition, virtual asset transactions could be exploited by illicit actors or money launderers as they can be conducted on peer-to-peer basis without any involvement of intermediaries to carry out AML/CFT measures such as CDD and transaction monitoring.
	12.1.6	There are three common stages in the laundering of money, and they frequently involve numerous transactions. An FI should be alert to any such sign for potential criminal activities. These stages are: (a) Placement - the disposal of cash proceeds or disposal of virtual assets derived from illegal activities; (b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions, or utilising technologies (e.g. anonymity-enhancing technologies or mechanisms), designed to disguise the source of the funds or virtual assets, 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.
	12.1.7	Transactions facilitated by virtual asset businesses may be cash based, and hence may be used as the initial placement of criminally derived cash proceeds. Further, virtual asset businesses may be used as the placement facility for disposing or depositing virtual assets derived from illicit activities or linked to predicate offences (such as online scams, ransomware and other cybercrimes).
	12.1.8	Virtual asset businesses are also likely to be used at the second stage of money laundering, i.e. the layering process. These businesses provide a potential avenue which enables the illicit actors or money launderers to dramatically alter the form of funds (i.e. fiat currency) or virtual assets. This not only allows conversion from cash in hand or other funds to virtual assets as well as conversion from one type of virtual asset to another, it also allows conversion from virtual assets derived from illicit activities or associated with illicit sources to cash in hand or other funds after conducting transactions for no other purposes but to further obfuscate the fund flows and the identity of the holder or beneficial owner of the virtual assets. To obfuscate the sources of virtual assets derived from illicit activities, illicit actors or money launderers may move assets across multiple wallet addresses, service providers, types of virtual assets or blockchains. They may exploit virtual asset-specific layering techniques such as peel chains[113] and chain-hopping[114].

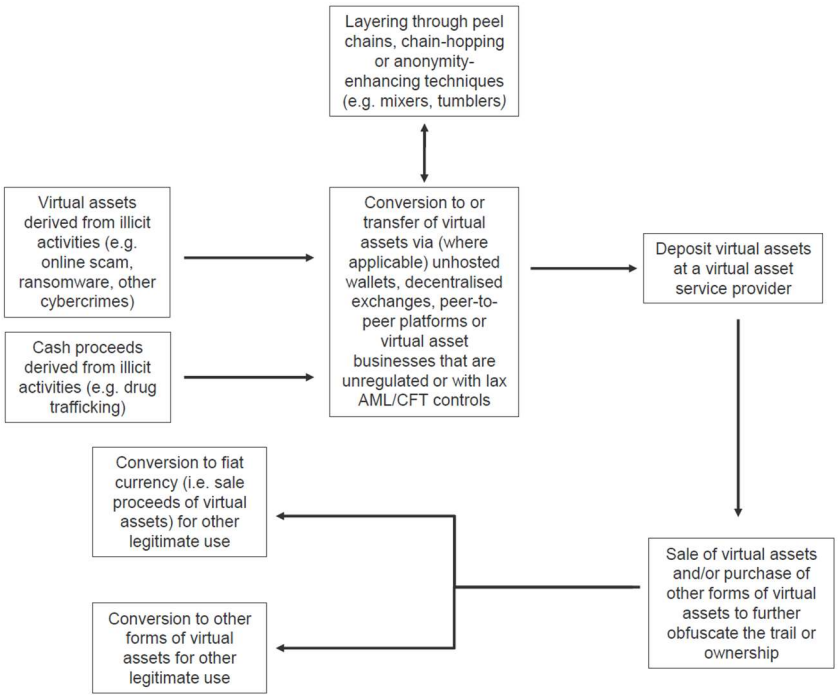
[113] Peel chains mean moving a large amount of virtual assets through a series of transactions in which a slightly smaller amount of virtual assets is transferred to a new address each time.

[114] Chain-hopping means moving virtual assets on a blockchain to another blockchain, often in rapid succession and with the aim of evading attempts to track these movements.

		Virtual assets are sometimes laundered through anonymity-enhancing services such as mixers or tumblers [115] and the use of other anonymity-enhancing technologies or mechanisms (e.g. anonymity-enhanced virtual asset or privacy coin, privacy wallet, etc.).
	12.1.9	Unhosted wallets [116], decentralised virtual asset exchanges, peer-to-peer platforms or virtual asset businesses that are unregulated or with lax AML/CFT controls are particularly attractive to illicit actors or money launderers.
	12.1.10	The combination of the ability to readily convert virtual assets procured with both licit and illicit proceeds, the ability to conceal the source of the illicit proceeds, the availability of a vast array of virtual assets, and the ease and near-instantaneous transaction speed with which virtual asset transactions can be effected, offers illicit actors or money launderers attractive ways to effectively integrate criminal proceeds into the general economy.
	12.1.11	In addition to the examples of money laundering methods and characteristics of financial transactions that have been linked with terrorist financing provided in paragraph 1.19, the chart set out below illustrates the money laundering process relevant to the virtual asset sector in detail.

[115] Mixers or tumblers are services which mix virtual assets from different users and subsequently return the assets to a new wallet address designated by the users, with an aim to break the connection between a sending and receiving address and obscure the trail to the original source while simultaneously improving the anonymity of transactions.

[116] An unhosted wallet refers to software or hardware that enables a person to store and transfer virtual assets on his own behalf, and in relation to which the private key is controlled or held by that person.



12.2 RBA - Institutional risk assessment and customer risk assessment

Considering relevant risk factors

	12.2.1	In addition to the factors set out in paragraph 2.7 which an FI should holistically consider in determining the level of overall risk that the FI is exposed to, an FI should consider: (a) in relation to country risk, the regulatory and supervisory regime and controls of the jurisdictions in which the FI is operating or otherwise exposed to – for example, the regulatory treatment of virtual assets in the jurisdiction; and the AML/CFT laws and regulations of the jurisdiction, including (where applicable) those in relation to virtual asset service providers (VASPs) (referred to in paragraph 12.6.1); and (b) in relation to product/service/transaction risk: (i) the characteristics of the products and services that it offers and transactions it executes, and the extent to which these are vulnerable to ML/TF abuse, for example,

		(A) the market capitalisation, value and price volatility, trading volume or liquidity, and (where applicable) market share of a virtual asset that it offers; (B) whether a product is or a service involves an anonymity-enhanced virtual asset or other virtual asset that has characteristics that promote anonymity, obfuscate the trail of transactions or impede the FI in identifying the counterparties of the transactions; (C) whether the virtual asset transactions are effected under an open (e.g. public blockchain) or closed-loop system (e.g. private blockchain); and (D) (where applicable) the reputation and AML/CFT controls of the issuer and/or the central entity governing the arrangement in relation to the virtual asset; and (ii) the proportion of virtual asset transactions conducted for its customers that are identified as being associated with illicit or suspicious activities/sources[117].
	12.2.2	Pursuant to paragraph 2.8, in identifying and assessing the ML/TF risks that may arise in relation to the development of new products and new business practices and the use of new or developing technologies for both new and pre-existing products, an FI should also identify and assess the ML/TF risks that may arise from conducting virtual asset transactions involving the use of anonymity-enhancing technologies or mechanisms, including but not limited to anonymity-enhanced virtual assets, mixers, tumblers, privacy wallets and other technologies that obfuscate the identity of the originator, recipient, holder or beneficial owner of a virtual asset.

[117] Examples of illicit or suspicious activities/sources are provided in paragraph 12.7.3.

		In taking appropriate measures to mitigate and manage the risks identified, the FI should refrain from conducting such virtual asset transactions if the identified risks cannot be mitigated and managed.
Conducting risk assessment		
	12.2.3	When conducting institutional risk assessment and customer risk assessment, in addition to the list of illustrative risk indicators set out in Appendix A, an FI should also refer to paragraphs 12.15 for the list of non-exhaustive illustrative risk indicators in relation to virtual assets, which may help identify a higher or lower level of risk associated with the risk factors stated in paragraphs 2.6 and 2.17 and should be taken into account holistically whenever relevant.
12.3 CDD – What CDD measures are and when they must be carried out		
When CDD measures must be carried out		
s.3(1A), Sch.2	12.3.1	In addition to the circumstances set out in paragraph 4.1.9 pursuant to which an FI must carry out CDD measures in relation to a customer, an FI must carry out CDD measures in relation to a customer before carrying out for the customer an occasional transaction that is a virtual asset transfer 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 FI to be linked.
	12.3.2	In the context of virtual assets, "occasional transactions" [118] may also include, for example, virtual asset transfers and virtual asset conversions.

[118] It should be noted that FIs that are LCs or SFC-licensed VAS Providers should not carry out "occasional transactions".

	12.3.3	The criterion in paragraph 4.1.9(c) also applies irrespective of the $8,000 threshold applicable to occasional transactions set out in paragraph 12.3.1.
	12.3.4	An FI should be vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD threshold of $8,000 for occasional transactions set out in paragraph 12.3.1. Where FIs become aware that this threshold is met or exceeded, CDD measures must be carried out.
	12.3.5	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 or virtual assets to one or more destinations. In determining whether the transactions are in fact linked, FIs should consider these factors against the timeframe within which the transactions are conducted.
12.4 CDD – Identification and verification of the customer's identity		
Other considerations		
	12.4.1	In addition to the identification information in paragraphs 4.2.2, 4.2.5 and 4.2.10, (where applicable) an FI should obtain additional customer information that enables it to identify, manage and mitigate the ML/TF risks associated with the channels [119] through which the FI establishes business relationship with its customers and/or through which its customers conduct virtual asset transactions. Such additional customer information could include:

[119] For example, virtual asset transactions are typically conducted by customers of an FI through non-face-to-face channels (e.g. web-based platforms and mobile applications).

		(a) IP address(es) with an associated time stamp; (b) geo-location data; and (c) device identifier(s).
12.5 CDD – Pre-existing customers		
	12.5.1	For SFC-licensed VAS Providers that were not licensed by the SFC under the SFO before 1 June 2023, the reference to "the AMLO came into effect on 1 April 2012" in paragraph 4.16.1 should be read as "1 June 2023".
12.6 CDD – Cross-border correspondent relationships		
Introduction		
	12.6.1	In the context of virtual assets, "cross-border correspondent relationships" set out in paragraph 4.20.1 also refers to, for the purposes of this Guideline, the provision of services by an FI in the course of providing a VA service as defined in section 53ZR of the AMLO (hereafter referred to as "correspondent institution") to a VASP [120] or financial institution [121] located in a place outside Hong Kong (hereafter referred to as "respondent institution"), where transactions effected on a principal or agency basis under the business relationships are initiated by the respondent institution.
	12.6.2	An example of a cross-border correspondent relationship in the context of virtual assets is where an FI located in Hong Kong, as a correspondent institution, executes virtual asset trading transactions for a VASP or a financial institution operating outside Hong Kong, which acts as a respondent institution for its underlying local customers.

[120] For the purposes of this Guideline, VASP refers to businesses falling within the definition of the term "virtual asset service providers" under the FATF Recommendations and which are conducted for or on behalf of customers.

[121] For the purposes of this Chapter, financial institution refers to businesses falling within the definition of the term "financial institutions" under the FATF Recommendations and which are conducted for or on behalf of customers.

Additional due diligence measures for cross-border correspondent relationships		
	12.6.3	In determining on a risk-sensitive basis pursuant to paragraph 4.20.7 the amount of information to collect about a respondent institution to enable it to understand the nature of the respondent institution's business, an FI should understand whether the respondent institution engages in activities or transactions involving virtual assets that provide higher anonymity such as anonymity-enhanced virtual assets; and the extent to which any of these activities or transactions are conducted for non-resident customers of the respondent institution.
	12.6.4	When assessing the AML/CFT controls of a respondent institution pursuant to paragraph 4.20.9, where the respondent institution handles virtual asset transactions, an FI should assess and ascertain whether the AML/CFT controls implemented by the respondent institution in relation to, among other things, virtual asset transfers, and screening of virtual asset transactions and the associated wallet addresses are adequate and effective.
Ongoing monitoring		
	12.6.5	In monitoring transactions of the respondent institution under paragraph 4.20.13(b), an FI should also take into account the requirements for ongoing monitoring of virtual asset transactions and the associated wallet addresses in paragraphs 12.7.2 to 12.7.4 and 12.7.6.
Cross-border correspondent relationships involving shell VASPs		
	12.6.6	In addition to the prohibition to establish or continue a cross-border correspondent relationship with a shell financial institution under paragraph 4.20.15, an FI must not establish or continue a cross-border correspondent relationship with a shell VASP.

		The FI should also take appropriate measures to satisfy itself that its respondent institutions do not permit their correspondent accounts to be used by shell VASPs[122].
	12.6.7	For the purposes of this Guideline, a shell VASP is a corporation that: (a) is incorporated in a place outside Hong Kong; (b) is authorised to carry on virtual asset businesses[123] in that place; (c) does not have a physical presence in that place (see paragraph 4.20.17); and (d) is not an affiliate[124] of a regulated financial group that is subject to effective group-wide supervision.
<u>Other considerations</u>		
	12.6.8	Where an FI establishes similar business relationships with VASPs or financial institutions operating in Hong Kong ("correspondent relationships")[125], the FI will also be exposed to risks similar to cross-border correspondent relationships (i.e. lack or incompleteness of information about the underlying customers and transactions). In particular, the FI will be exposed to higher risks for correspondent relationships with VASPs that are not licensed or regulated but operating in Hong Kong.

[122] This includes a nested correspondent relationship under which the respondent institution uses the correspondent account to provide services to a shell VASP with which it has a business relationship.

[123] In this context, this refers to businesses falling within the definition of the term "virtual asset service providers" under the FATF Recommendations and which are conducted for or on behalf of customers.

[124] In this context, a corporation is an affiliate of another corporation if (a) the corporation is a subsidiary of the other corporation; or (b) at least one individual who is a controller of the corporation is at the same time a controller of the other corporation.

[125] This refers to where an FI provides services in the course of providing a VA service as defined in section 53ZR of the AMLO to VASPs or financial institutions operating in Hong Kong, where transactions effected on a principal or agency basis under the business relationships are initiated by the VASPs or financial institutions.

		Where applicable, the FI should adopt an RBA in applying the additional due diligence and other risk mitigating measures set out in paragraphs 4.20.5 to 4.20.13 and 12.6.3 to 12.6.4 for the correspondent relationships with VASPs or financial institutions operating in Hong Kong.
12.7 Ongoing monitoring in relation to virtual asset transactions and activities		
	12.7.1	Given the pseudonymous nature and transaction speed of virtual assets, illicit actors and designated parties may easily obfuscate the fund flows and further complicate the trail by utilising multiple wallets to conduct numerous or structured virtual asset transactions, thereby concealing the origin and destination of their virtual assets to avoid the detection of their ML/TF or other illicit activities.
	12.7.2	An FI[126] should therefore implement effective risk-based transaction monitoring procedures to detect the origin and destination of the virtual assets transferred from or to its customers or other parties in relation to virtual asset transactions conducted for its customers[127], particularly those from or to a VA transfer counterparty that presents a higher ML/TF risk (see paragraph 12.13.11) or an unhosted wallet (see paragraph 12.14.3), and to identify and report suspicious transactions as well as take appropriate follow-up actions.
	12.7.3	In this connection, the FI should establish and maintain adequate and effective systems and controls to conduct screening of virtual asset

[126] For the avoidance of doubt, paragraphs 12.7.2 to 12.7.4 and 12.7.6, Chapter 11 and paragraphs 12.10 are applicable to an FI that is an LC when it manages or distributes virtual asset funds that accept subscriptions or redemptions made by the fund investors in the form of virtual assets. Where such subscriptions or redemptions are handled by an appointed institution such as an administrator or a transfer agent, the LC should ensure that the appointed institution has appropriate measures in place to ensure compliance with the requirements similar to those imposed in paragraphs 12.7.2 to 12.7.4 and 12.7.6, Chapter 11 and paragraphs 12.10, so as to ensure that proper safeguards exist to mitigate the associated ML/TF risks.

[127] These include virtual asset transfers referred to in paragraphs 12.11.5 to 12.11.24 and 12.14.

		transactions and the associated wallet addresses. In particular, the FI should[128]: (a) track the transaction history of virtual assets to more accurately identify the source and destination of these virtual assets; and (b) identify transactions involving wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources[129], or designated parties. The FI should adopt appropriate technological solutions (e.g. blockchain analytic tools[130]) that enable the tracking of virtual assets and the associated wallet addresses and identification of potentially suspicious transactions.
	12.7.4	Where an FI employs a technological solution provided by an external party to conduct screening of virtual asset transactions and the associated wallet addresses, the FI remains responsible for discharging its AML/CFT obligations. The FI should conduct due diligence on the solution before deploying it, taking into account relevant factors such as: (a) the quality and effectiveness of the tracking

[128] For the avoidance of doubt, the FI should conduct screening of virtual asset transactions and/or the associated wallet addresses before conducting a virtual asset transfer or making the transferred virtual assets available to the customer, and after conducting a virtual asset transfer on a risk-sensitive basis, so as to more timely and accurately identify the source and destination of these virtual assets and involvement or subsequent involvement of wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources, or designated parties.

[129] Illicit activities include, for example, ransomware, fraud, identity theft, phishing, and other cybercrimes; and suspicious activities/sources include, for example, darknet marketplaces, online gambling services, peel chains and use of anonymity-enhancing technologies or mechanisms (e.g. mixers, tumblers, privacy wallets). In addition, any wallet addresses owned or controlled by customer(s) with which the FI has decided not to establish or continue business relationships due to suspicion of ML/TF should be included as those associated with suspicious sources. Please refer to the meaning of peel chains and mixers and tumblers set out in paragraph 12.1.8.

[130] Blockchain analytic tools typically enable their users to trace the on-chain history of specific virtual assets. These tools support a number of common virtual assets and compare transaction histories against a database of wallet addresses connected to illicit or suspicious activities/sources, and flag identified transactions.

		and detection tools; (b) the coverage, accuracy and reliability of the information maintained in the database that supports its screening capability (e.g. whether the list of wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources, or designated parties, is subject to timely review and update); and (c) any limitations (e.g. limited reach of the blockchain analytical tools; or inability to deal with virtual assets or wallet addresses involving the use of anonymity-enhancing technologies or mechanisms such as anonymity-enhanced virtual assets, mixers or tumblers).
	12.7.5	An FI should (where applicable) monitor the additional customer information (i.e. IP addresses with associated time stamps, geo-location data, and device identifiers) referred to in paragraph 12.4.1 obtained by the FI on an ongoing basis[131] to identify suspicious transactions and activities as well as take appropriate follow-up actions.
	12.7.6	The FI should also put in place policies and procedures to identify and analyse any additional red flags of suspicious transactions and activities in connection with the screening of virtual asset transactions and the associated wallet addresses as well as the ongoing monitoring of additional customer information, having regard to the list of illustrative indicators of suspicious transactions and activities set out in paragraphs 12.16 and Appendix B, which should prompt further investigations (see paragraph 7.12); and take appropriate steps such as making appropriate enquiries with customers to

[131] For example, an FI may adopt technological solution(s) that enables it to track and monitor the additional customer information on an ongoing basis.

		identify if there are any grounds for suspicion (see paragraphs 5.13 to 5.17)[132]. Furthermore, where the FI becomes aware of any heightened ML/TF risks from the screening of virtual asset transactions and the associated wallet addresses or the ongoing monitoring of additional customer information, the FI should apply enhanced customer due diligence and ongoing monitoring, and take other additional preventive or mitigating actions as necessary to mitigate the ML/TF risks involved[133].
12.8 Terrorist financing, financial sanctions and proliferation financing – Database maintenance, screening and enhanced checking		
	12.8.1	In implementing an effective screening mechanism pursuant to paragraph 6.16, an FI's screening mechanism should also include screening all relevant parties in a virtual asset transfer (referred to in paragraphs 12.11.5 to 12.11.24 and 12.14), including: (a) the recipient if the FI acts as the ordering institution or the virtual asset is transferred to an unhosted wallet; (b) the originator if the FI acts as the beneficiary institution or the virtual asset is transferred from an unhosted wallet; or (c) both the originator and recipient if the FI acts as the intermediary institution, against current database before executing the virtual asset transfer.

[132] When an FI evaluates a potentially suspicious transaction identified from the screening of virtual asset transactions and the associated wallet addresses, it may take into account the required originator and recipient information, as well as other customer information, transaction history, and any additional information that the FI obtained from the customer.

[133] For example, where a customer enters the FI's platform from and/or initiates transactions with a masked IP address, the FI may request the customer to unmask the IP address and, where necessary, the FI may decline to provide services to that customer if the IP address remains masked.

	12.8.2	For the screening requirement set out in paragraph 12.8.1, an FI should screen the required originator and recipient information[134] referred to in: (a) paragraph 12.11.5 or 12.11.6 in relation to a virtual asset transfer (including information which may be held separately to the virtual asset transfer itself); or (b) paragraph 12.14.2 in relation to a virtual asset transfer to or from an unhosted wallet.
	12.8.3	Where an incoming virtual asset transfer is conducted without the said screening or when any of the required originator and recipient information in relation to an incoming virtual asset transfer is missing (which renders the FI unable to conduct screening), the FI should take appropriate risk mitigating measures, having regard to its business practices[135]. The risk mitigating measures taken by the FI should be documented.
12.9 Record-keeping – Retention of records relating to CDD and transactions		
s.20(3A), Sch. 2	12.9.1	In addition to the documents and records required to be kept and the period of time such documents and records are required to be kept pursuant to paragraphs 8.3 and 8.4, for an occasional transaction that is a virtual asset transfer involving virtual assets that amount to no less than $8,000, an FI should keep all documents and records

[134] An FI should include the names of relevant parties in the screening, and should take into consideration the address, identification document number or date and place of birth of the originator (where applicable) in the screening. In addition, the FI should observe the requirements for ongoing monitoring of virtual asset transactions and the associated wallet addresses in paragraphs 12.7.2 to 12.7.4 and 12.7.6 when carrying out virtual asset transfers on behalf of its customers.

[135] These may include implementing controls to prevent the relevant virtual assets from being made available to the recipient, or putting the receiving wallet on hold, until the screening is completed and confirmed that no concern is raised. Please also refer to risk mitigating measures in paragraph 12.11.22.

		mentioned in paragraph 8.3 for a period of at least five years beginning on the date on which the occasional transaction is completed.
s.20(1)(a), Sch. 2	12.9.2	In addition to the documents and records required to be kept and the period of time such documents and records are required to be kept pursuant to paragraphs 8.5 and 8.6, an FI should keep the required originator and recipient information set out in paragraphs 12.11.5 and 12.11.6 obtained or received by the FI in relation to a virtual asset transfer referred to in paragraphs 12.11.5 to 12.11.24, and/or the required originator and recipient information set out in paragraph 12.14.2 obtained by the FI in relation to a virtual asset transfer to or from an unhosted wallet referred to in paragraphs 12.14, for a period of at least five years after the completion of the transfer, regardless of whether the business relationship ends during the period.
12.10 Third-party deposits and payments		
General		
	12.10.1	For the purposes of Chapter 11, paragraphs 5.18 to 5.20 and 12.10, unless otherwise specified, when an FI handles deposits and payments in the form of virtual assets on behalf of its customer, the term “third-party deposits or payments” covers both third-party deposits or payments in the form of funds (i.e. fiat currency) and virtual assets.
	12.10.2	Where a customer uses a third party to make or receive payments in the form of virtual assets to or from an FI, there is a risk that the arrangement may be used to disguise the true beneficial owner or the source of funds. There are increased risks that these transactions are linked to predicate offences (such as online scams, ransomware and other cybercrimes, insider dealing and market manipulation), or used to launder illicit proceeds obtained elsewhere.

Policies and procedures		
	12.10.3	In relation to the policies and procedures for the acceptance of third-party deposits and payments as required under paragraph 11.3, the policies and procedures of an FI should also address the monitoring systems and controls for identifying transactions involving third-party deposits or payments in the form of virtual assets[136] (please refer to paragraph 12.10.6).
	12.10.4	In relation to the guidance in paragraph 11.3(d) requiring FIs to have policies and procedures for the exceptional situations under which delayed due diligence or evaluation may be allowed, it should be noted that delayed due diligence on the source of a deposit or evaluation of a third-party deposit does not apply to a deposit in the form of virtual assets considering the nature and ML/TF risks associated with virtual assets.
	12.10.5	To facilitate the prompt identification of the sources of deposits in the form of virtual assets, FIs are strongly encouraged to whitelist accounts (or wallet addresses as appropriate[137]) owned or controlled by their clients or any acceptable third parties for the making of all such deposits. This will make it easier for FIs to ascertain whether the deposits have originated from their clients or any acceptable third parties[138].

[136] Unlike payments in the form of funds which are usually made to bank accounts designated in the name of a payee which can be easily identified by an FI before making payments, payments in the form of virtual assets are usually made to wallet addresses which are not designated in the name of a payee. Hence, an FI should put in place monitoring systems and controls for identifying transactions involving a third party for both deposits and payments in the form of virtual assets (e.g. by ascertaining the ownership or control of the account or wallet address).

[137] When whitelisting accounts (or wallet addresses as appropriate) owned or controlled by its clients or any acceptable third parties, an FI should only accept wallet addresses that the FI has assessed to be reliable and have regard to the relevant requirements set out in paragraphs 12.10.6, 12.10.7 and 12.14.3(b).

[138] Likewise, if applicable, the use of whitelisted accounts (or wallet addresses as appropriate) owned or controlled by any acceptable third parties for the making of withdrawals will make it easier for FIs to complete the necessary due diligence to determine the acceptability of a third-party payee before effecting a third-party payment.

	12.10.6	For deposits and payments in the form of virtual assets, the nature and extent of monitoring systems and controls set out in paragraph 12.10.3 should be commensurate with the channel of deposits or payments (i.e. whether the deposits or payments were made via a VA transfer counterparty (referred to in paragraphs 12.13) or an unhosted wallet (referred to in paragraphs 12.14)), having regard to the associated ML/TF risks[139]. For a virtual asset deposit or payment made via an ordering or beneficiary institution that presents low ML/TF risk, the required originator or recipient information verified by the ordering or beneficiary institution may be sufficient for an FI to ascertain whether the transaction involves a third party[140]. Conversely, where a virtual asset deposit or payment is made via an ordering or beneficiary institution that presents higher ML/TF risk or an unhosted wallet, the FI should ascertain the customer's ownership or control of the account (or wallet address as appropriate) maintained with the ordering or beneficiary institution, or the unhosted wallet, by taking appropriate measures, for example: (a) using appropriate confirmation methods[141]; and (b) obtaining evidence from the customer such as statement of account issued by the VA transfer counterparty.
<u>Due diligence process for assessing third-party deposits and payments</u>		
	12.10.7	In addition to the due diligence process set out in paragraphs 11.5 to 11.8, an FI should take

[139] Where applicable, an FI should have regard to the results of the counterparty due diligence as set out in paragraphs 12.13.

[140] In other words, this means that whether the originator and the recipient are the same person.

[141] Examples of confirmation methods may include requesting the customer to perform the micropayment test (i.e. by effecting a virtual asset transfer with an (typically small) amount specified by the FI) or message signing test (i.e. by signing a message specified by the FI which is then verified by the FI).

		reasonable measures on a risk-sensitive basis to ascertain the third party's ownership of the account (or wallet address as appropriate). For a virtual asset deposit or payment made via an ordering or beneficiary institution that presents low ML/TF risk, it may be sufficient for an FI to rely on the required originator or recipient information verified by the ordering or beneficiary institution for ascertaining the third party's ownership of the account. Conversely, where a virtual asset deposit or payment is made via an ordering or beneficiary institution that presents higher ML/TF risk or an unhosted wallet, the FI should use its best endeavours to ascertain the third party's ownership or control of the account (or wallet address as appropriate) maintained with the ordering or beneficiary institution, or the unhosted wallet, by taking appropriate measures which may include the examples mentioned in paragraph 12.10.6.
12.11 Virtual asset transfers		
General		
	12.11.1	An FI should comply with section 13A of Schedule 2, the guidance and requirements set out in paragraphs 12.11 to 12.14 as well as (where applicable) relevant circulars and frequently asked questions published by the SFC from time to time when acting as an ordering institution, an intermediary institution or a beneficiary institution as defined in paragraph 12.11.4 in a virtual asset transfer, and/or when conducting virtual asset transfers to or from an unhosted wallet[142]. For the avoidance of doubt, where an FI is the originator or recipient of a virtual asset transfer, it is not acting as an ordering institution, an intermediary institution or a beneficiary institution and is thus not required to comply with the requirements under section 13A of Schedule 2 and

[142] Refer to paragraph 12.1.9 for the meaning of "unhosted wallets".

		paragraphs 12.11.5 to 12.11.24, 12.12 and 12.13 in respect of that transaction.
	12.11.2	To prevent criminals and terrorists from having unfettered opportunities to move their assets through virtual asset transfers and to detect such misuse when it occurs, an FI must take all reasonable measures to ensure that proper safeguards exist to mitigate the ML/TF risks associated with virtual asset transfers. In particular, an FI should establish and maintain effective procedures to ensure compliance with: (a) the virtual asset transfers requirements under paragraphs 12.11.5 to 12.11.24 (a.k.a. travel rule[143]); and (b) other relevant requirements under paragraphs 12.12 to 12.14, to enable it to carry out sanctions screening and transaction monitoring procedures on all relevant parties involved in a virtual asset transfer in an effective manner.
<u>Virtual asset transfers to or from an institution</u>		
	12.11.3	Paragraphs 12.11.5 to 12.11.24, 12.12 and 12.13 apply to virtual asset transfers to or from an institution, including an institution that is a VASP or financial institution (referred to in paragraph 12.6.1) located in a place within or outside Hong Kong. Requirements that apply to virtual asset transfers to or from unhosted wallets are set out in paragraphs 12.14.

[143] The travel rule refers to the application of the wire transfer requirements set out in FATF Recommendation 16 in a modified form in the context of virtual asset transfers (in particular, the requirements to obtain, hold, and submit required and accurate originator and required recipient information immediately and securely when conducting virtual asset transfers), recognising the unique technological properties of virtual assets.

s.13A(1) & (8), Sch. 2	12.11.4	Section 13A of Schedule 2, paragraphs 12.11.5 to 12.11.24, 12.12 and 12.13 apply to a virtual asset transfer that is a transaction carried out: (a) by an institution (the ordering institution) on behalf of a person (the originator) by transferring any virtual assets; and (b) with a view to making the virtual assets available: (i) to that person or another person (the recipient); and (ii) at an institution (the beneficiary institution), which may be the ordering institution or another institution, whether or not one or more other institutions (intermediary institutions) participate in completion of the transfer of the virtual assets. An FI should comply with the corresponding requirements set out in paragraphs 12.11.5 to 12.11.24 when acting as an ordering institution, an intermediary institution or a beneficiary institution (as the case may be) in a virtual asset transfer.
<u>Ordering institutions</u>		
s.13A(2), Sch.2	12.11.5	Before carrying out a virtual asset transfer involving virtual assets that amount to not less than $8,000, an ordering institution must obtain and record the following originator and recipient information[144]: (a) the originator's name; (b) the number of the originator's account maintained with the ordering institution and from which the virtual assets are transferred (i.e. the account used to process the

[144] For the avoidance of doubt, in relation to virtual asset transfers carried out for a customer, an FI is not required to obtain the originator information from a customer that is the originator before carrying out every individual virtual asset transfer (unless doubts arise as to veracity or adequacy of the information previously obtained for the purposes of customer identification and verification).

		transaction) or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the ordering institution; (c) the originator's address [145], the originator's customer identification number [146] 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 virtual assets are transferred (i.e. the account used to process the transaction) or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the beneficiary institution.
s.13A(2) & (3), Sch.2	12.11.6	Before carrying out a virtual asset transfer involving virtual assets that amount to less than $8,000, an ordering institution must obtain and record 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 virtual assets are transferred or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the ordering institution; (c) the recipient's name; and (d) the number of the recipient's account maintained with the beneficiary institution and

[145] The originator's address refers to the geographical address of the originator (i.e. residential address of the originator that is a natural person; or the address of registered office (or principal place of business if different from the registered office) of the originator that is a legal person, a trust or other similar legal arrangement).

[146] Customer identification number means a number which uniquely identifies the originator to the ordering institution and is a different number from the unique transaction reference number referred to in paragraph 12.11.8. The customer identification number must refer to a record held by the ordering institution which contains at least one of the following: the customer's address, identification document number, or date and place of birth.

		to which the virtual assets are transferred or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the beneficiary institution.
	12.11.7	Where applicable, the number of the account maintained with the ordering institution or beneficiary institution from or to which the virtual assets are transferred referred to in paragraphs 12.11.5 and 12.11.6 could mean the wallet address of the originator or recipient maintained with the ordering institution or beneficiary institution and used to process the transaction.
	12.11.8	The unique reference number assigned to the virtual asset transfer by the ordering institution or beneficiary institution referred to in paragraphs 12.11.5 and 12.11.6 should permit traceability of the virtual asset transfer.
s.13A(4), Sch.2	12.11.9	An ordering institution must submit the required originator and recipient information obtained and held under paragraphs 12.11.5 and 12.11.6 (hereafter referred to as "required information") to the beneficiary institution securely (see paragraph 12.11.12).
s.13A(4), Sch.2	12.11.10	In addition, the ordering institution must submit the required information to the beneficiary institution immediately (see paragraph 12.11.13).
	12.11.11	For the avoidance of doubt, the required information may be submitted either directly or indirectly to the beneficiary institution provided that it is submitted in accordance with the requirements set out in paragraphs 12.11.9 and 12.11.10. This means that it is not necessary for the required information to be attached directly to, or be included in, the virtual asset transfer itself.
	12.11.12	“Securely” referred to in paragraph 12.11.9 means that the ordering institution should store and submit the required information in a secure manner to

		protect the integrity and availability of the required information for facilitating record-keeping and the use of such information by the beneficiary institution and, where applicable, the intermediary institution, in fulfilling its AML/CFT obligations[147]; and protect the information from unauthorised access or disclosure. To ensure that the required information is submitted in a secure manner, an ordering institution should[148]: (a) undertake the VA transfer counterparty due diligence measures as set out in paragraphs 12.13 to determine whether the beneficiary institution and, where applicable, the intermediary institution can reasonably be expected to adequately protect the confidentiality and integrity of the information submitted to it; and (b) take other appropriate measures and controls, for example: (i) entering into a bilateral data sharing agreement with the beneficiary institution and, where applicable, the intermediary institution and/or (where applicable) a service-level agreement with the technological solution provider for travel rule compliance (see paragraphs 12.12) which specifies the responsibilities of the institutions involved and/or of the provider to ensure the protection of the confidentiality and integrity of the information submitted; (ii) using, or ensuring the technological solution adopted for travel rule compliance (where applicable) uses, a strong encryption algorithm to encrypt the

[147] AML/CFT obligations include, among others, identifying and reporting suspicious virtual asset transfers, taking freezing actions and prohibiting virtual asset transfers with designated persons and entities.

[148] An ordering institution should give due regard to the laws and regulations on privacy and data protection of the jurisdictions in which the ordering institution operates and/or is incorporated.

		information during the data submission; and (iii) implementing adequate information security controls to prevent unauthorised access, disclosure or alteration. For the avoidance of doubt, an ordering institution should not execute a virtual asset transfer when it could not ensure that the required information could be submitted to a beneficiary institution, and where applicable, an intermediary institution, in a secure manner having regard to the above guidance and the VA transfer counterparty due diligence results.
	12.11.13	"Immediately" referred to in paragraph 12.11.10 means that the ordering institution should submit the required information prior to, or simultaneously or concurrently with, the virtual asset transfer (i.e. the submission must occur before or when the virtual asset transfer is conducted)[149].
	12.11.14	An ordering institution should keep records and relevant documents so that it can demonstrate to the relevant authority whether and how the required information is submitted to a beneficiary institution in accordance with the requirements set out in paragraphs 12.11.9 and 12.11.10[150].
	12.11.15	For a virtual asset transfer involving virtual assets that amount to not less than $8,000, an ordering institution must ensure that the required originator

[149] Where an intermediary institution is involved in a virtual asset transfer, an ordering institution should undertake the VA transfer counterparty due diligence measures as set out in paragraphs 12.13 to determine if the intermediary institution can submit the required information immediately to the beneficiary institution, or where applicable, another intermediary institution and should not execute the virtual asset transfer if the intermediary institution is unable to do so.

[150] For the avoidance of doubt, where technological solution is adopted for travel rule compliance, the ordering institution should keep any records or relevant documents of its due diligence on the technological solution. Please also refer to the guidance provided in paragraphs 12.12. In addition, where an intermediary institution is involved in a virtual asset transfer, the ordering institution should keep records and relevant documents that demonstrate whether and how the required information is submitted to the beneficiary institution through the intermediary institution in accordance with the requirements set out in paragraphs 12.11.9 and 12.11.10.

		information submitted with the virtual asset transfer is accurate[151].
s.3(1)(d) & (1A), Sch.2	12.11.16	For an occasional virtual asset transfer[152] involving virtual assets that amount to not less than $8,000, an ordering institution must verify the identity of the originator[153]. For an occasional virtual asset transfer involving virtual assets that amount to less than $8,000, 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 amount to not less than $8,000, or when there is a suspicion of ML/TF.
	12.11.17	The ordering institution should not execute a virtual asset transfer unless it has ensured compliance with the requirements in paragraphs 12.11.5 to 12.11.16.
<u>Intermediary institutions</u>		
s.13A(6), Sch.2	12.11.18	An intermediary institution must ensure that all originator and recipient information as set out in paragraphs 12.11.5 and 12.11.6 which the intermediary institution receives in connection with the virtual asset transfer is retained with the required information submission, and is transmitted to the institution to which it passes on the transfer instruction[154].

[151] "Accurate" in this context means information that has been verified for accuracy as part of its CDD process. For example, if the originator's address is part of the required information to be submitted by the ordering institution as set out in paragraphs 12.11.9 and 12.11.10, the ordering institution should ensure that the originator's address is accurate having regard to the CDD information obtained pursuant to paragraph 4.2.4, 4.2.5 or 4.2.10 as appropriate.

[152] It should be noted that FIs that are LCs or SFC-licensed VAS Providers should not carry out occasional virtual asset transfers.

[153] For the avoidance of doubt, where the originator is a customer of an FI, the FI does not need to re-verify the identity of the customer that has been verified (unless doubts arise as to veracity or adequacy of the information previously obtained for the purposes of customer identification and verification).

[154] An intermediary institution should undertake the VA transfer counterparty due diligence measures on the ordering institution and, where applicable, another intermediary institution(s), as set out in paragraphs 12.13.

	12.11.19	As with the submission of required information by an ordering institution, an intermediary institution should transmit the aforesaid information to another intermediary institution or the beneficiary institution in accordance with the manner set out in paragraphs 12.11.12 to 12.11.13 and the requirement set out in paragraph 12.11.14[155].
<u>Beneficiary institutions</u>		
s.13A(5), Sch.2	12.11.20	A beneficiary institution must obtain and record the required information submitted to it by the institution from which it receives the transfer instruction[156].
s.3(1A), Sch. 2	12.11.21	For a virtual asset transfer involving virtual assets that amount to not less than $8,000, a beneficiary institution should verify the identity of the recipient if the identity has not been previously verified as part of its CDD process. The beneficiary institution should also confirm whether the recipient's name and account number obtained from the institution from which it receives the transfer instruction match with the recipient information verified by it, and take reasonable measures as set out in paragraph 12.11.24 where such information does not match.
<u>Identification and handling of incoming virtual asset transfers lacking the required information</u>		
s.19(2A), Sch.2	12.11.22	A beneficiary institution or an intermediary institution (hereafter referred to as "instructed institution") must establish and maintain effective procedures for identifying and handling incoming virtual asset transfers that do not comply with the relevant requirements on required originator or

[155] For the purpose of paragraph 12.11.19, any reference to "ordering institution" and "the intermediary institution" in paragraphs 12.11.12 to 12.11.14 refers to "intermediary institution" and "another intermediary institution" respectively.

[156] A beneficiary institution should undertake the VA transfer counterparty due diligence measures on the ordering institution and, where applicable, the intermediary institution(s), as set out in paragraphs 12.13.

		recipient information, which include: (a) taking reasonable measures (e.g. real-time or post-event monitoring) to identify virtual asset transfers that lack the required information; and (b) having risk-based policies and procedures for determining: (i) whether and when to execute, suspend (i.e. prevent the relevant virtual assets from being made available to the recipient) a virtual asset transfer lacking the required information or, where appropriate, return the relevant virtual assets to the account of the ordering institution or another intermediary institution (hereafter referred to as "instructing institution") from which the instructed institution receives the transfer instruction[157]; and (ii) the appropriate follow-up action.
s.13A(7)(a), Sch.2	12.11.23	In respect of the risk-based policies and procedures referred to in paragraph 12.11.22, if an instructing institution does not submit all of the required information in connection with the virtual asset transferred to the instructed institution, the instructed institution must as soon as reasonably practicable obtain the missing information from the instructing institution. If the missing information cannot be obtained, the instructed institution should either consider restricting or terminating its business relationship with the instructing institution in relation to virtual asset transfers, or take reasonable measures to mitigate the risk of ML/TF involved.
s.13A(7)(b), Sch.2	12.11.24	If the instructed institution is aware that any of the information submitted to it that purports to be the

[157] An instructed institution should consider preventing the relevant virtual assets from being made available to the recipient until the missing information is obtained or, where appropriate, returning the relevant virtual assets to the account of the instructing institution when there is no suspicion of ML/TF, taking into account the results of the VA transfer counterparty due diligence (see paragraphs 12.13) and screening of the virtual asset transactions and the associated wallet addresses in relation to the virtual asset transfers (see paragraphs 12.7.2 to 12.7.4 and 12.7.6). Please also refer to risk mitigating measures in paragraph 12.8.3.

		required information is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved having regard to the procedures set out in paragraph 12.11.22(b).
12.12 Virtual asset transfers – Technological solutions for travel rule compliance		
	12.12.1	An FI may adopt any technological solution to submit and/or obtain the required information for a virtual asset transfer provided that the solution enables the FI to comply with the travel rule as set out in paragraphs 12.11.5 to 12.11.24, when it acts as an ordering institution, an intermediary institution or a beneficiary institution.
	12.12.2	Where an FI chooses to use a technological solution to ensure travel rule compliance, it remains responsible for discharging its AML/CFT obligations in relation to travel rule compliance. The FI should conduct due diligence to satisfy itself that the solution enables it to comply with the travel rule in an effective and efficient manner. In particular, the FI should consider whether the solution enables it to: (a) identify VA transfer counterparties (see paragraphs 12.13); and (b) submit the required information immediately (see paragraph 12.11.13) and securely (see paragraph 12.11.12) (i.e. whether the solution could protect the submitted information from unauthorised access, disclosure or alteration), and obtain the required information[158].
	12.12.3	In addition, an FI should consider a range of

[158] In considering whether the solution enables the FI to obtain the required information, the FI should take into account whether it could identify situations where the required information provided by ordering institutions is incomplete or missing, which may result from slight differences in travel rule requirements across the laws, rules and regulations of other jurisdictions, before conducting virtual asset transfers.

		factors as appropriate when conducting due diligence on the technological solution for travel rule compliance, such as: (a) the interoperability of the solution with other similar solution(s) adopted by the VA transfer counterparties that the FI may deal with; (b) whether the solution allows the required information for a large volume of virtual asset transfers to be submitted immediately and securely to and/or obtained from multiple VA transfer counterparties in a stable manner; (c) whether the solution enables the FI to implement measures or controls for the effective scrutiny of virtual asset transfers to identify and report suspicious transactions (as set out in paragraphs 12.7.2 to 12.7.4 and 12.7.6), and screening of virtual asset transfers to meet the sanctions obligations (i.e. taking freezing actions and prohibiting virtual asset transfers with designated persons and entities) (as set out in paragraphs 12.8.1 to 12.8.3); (d) whether the solution facilitates the FI in conducting VA transfer counterparty due diligence (see paragraphs 12.13) and requesting additional information from the VA transfer counterparty as and when necessary; and (e) whether the solution facilitates the FI in keeping the required information (see paragraph 12.9.2).
12.13 VA transfer counterparty due diligence and additional measures		
<u>Introduction</u>		
	12.13.1	When an FI conducts a virtual asset transfer referred to in paragraphs 12.11.5 to 12.11.24, the FI will be exposed to ML/TF risks associated with the institution which may be the ordering institution, intermediary institution or beneficiary institution involved in the virtual asset transfer (hereafter

		collectively referred to as "VA transfer counterparty"), which may vary depending on a number of factors, including: (a) the types of products and services offered by the VA transfer counterparty; (b) the types of customers to which the VA transfer counterparty provides services; (c) geographical exposures of the VA transfer counterparty and its customers; (d) the AML/CFT regime in the jurisdictions in which the VA transfer counterparty operates and/or is incorporated; and (e) the adequacy and effectiveness of the AML/CFT controls of the VA transfer counterparty.
	12.13.2	To avoid sending or receiving virtual assets to or from illicit actors or designated parties that had not been subject to the appropriate CDD and screening measures undertaken by a VA transfer counterparty and to ensure compliance with the travel rule, an FI should conduct due diligence on the VA transfer counterparty to identify and assess the ML/TF risks associated with the virtual asset transfers to or from the VA transfer counterparty and apply appropriate risk-based AML/CFT measures.
<u>VA transfer counterparty due diligence measures</u>		
	12.13.3	An FI should conduct due diligence measures on a VA transfer counterparty before conducting a virtual asset transfer or making the transferred virtual assets available to the recipient. If an FI conducts virtual asset transfers with several VA transfer counterparties located in different jurisdictions but belonging to the same group, the FI, whilst conducting due diligence on each of the VA transfer counterparties independently, should also take into account that these counterparties belong to the same group in order to holistically

		assess the ML/TF risks posed by the counterparties.
	12.13.4	An FI does not need to undertake the VA transfer counterparty due diligence process for every individual virtual asset transfer when dealing with VA transfer counterparties that it has previously conducted counterparty due diligence on, unless when there is a suspicion of ML/TF or when the FI is aware of any heightened ML/TF risks from its ongoing monitoring of virtual asset transfers with VA transfer counterparties (see paragraph 12.13.10).
	12.13.5	VA transfer counterparty due diligence typically involves the following procedures: (a) determining whether the virtual asset transfer is or will be with a VA transfer counterparty or an unhosted wallet; (b) where applicable, identifying the VA transfer counterparty (e.g. by making reference to lists of licensed or registered VASPs or financial institutions in different jurisdictions); and (c) assessing whether the VA transfer counterparty is an eligible counterparty to deal with and to send the required information to (see paragraphs 12.13.6 to 12.13.9).
	12.13.6	An FI should adopt an RBA in applying the following due diligence measures on a VA transfer counterparty, taking into account relevant factors such as those set out in paragraph 12.13.1: (a) collect sufficient information about the VA transfer counterparty to enable it to understand

		fully the nature of the VA transfer counterparty's business[159]; (b) understand the nature[160] and expected volume and value of virtual asset transfers with the VA transfer counterparty; (c) determine from publicly available information the reputation of the VA transfer counterparty and the quality and effectiveness of the AML/CFT regulation and supervision over the VA transfer counterparty by authorities in the jurisdictions in which it operates and/or is incorporated which perform functions similar to those of the RAs; (d) assess the AML/CFT controls of the VA transfer counterparty and be satisfied that the AML/CFT controls of the VA transfer counterparty are adequate and effective; and (e) obtain approval from its senior management.
	12.13.7	While a relationship with a VA transfer counterparty is different from a cross-border correspondent relationship referred to in paragraph 12.6.1, there are similarities in the due diligence approach which can be of assistance to an FI. By virtue of this, the FI should conduct the due diligence measures in paragraph 12.13.6, with reference to the requirements set out in paragraphs 4.20.7 to 4.20.10 and 12.6.3 to 12.6.4[161].
	12.13.8	As part of the VA transfer counterparty due

[159] While an FI should determine on a risk-sensitive basis the amount of information to collect about the VA transfer counterparty to enable it to understand the nature of the VA transfer counterparty's business, the FI should, among other things, endeavour to identify and verify the identity of the VA transfer counterparty using documents, data or information provided by a reliable and independent source; and take reasonable measures to understand the ownership and control structure of the VA transfer counterparty, with the objective to follow the chain of ownerships to its beneficial owners.

[160] For example, the extent to which any of the virtual asset transfers and relevant underlying customers (who may be the originator or recipient of a virtual asset transfer) are assessed as high risk by the VA transfer counterparty.

[161] For the purposes of paragraph 12.13.7, any reference to "cross-border correspondent relationship" and "respondent institution" in paragraphs 4.20.7 to 4.20.10 and 12.6.3 to 12.6.4 refers to "VA transfer counterparty relationship" and "VA transfer counterparty" respectively.

		diligence measures in relation to its AML/CFT controls, an FI should assess whether the VA transfer counterparty can comply with the travel rule, taking into account relevant factors such as: (a) whether the VA transfer counterparty is subject to requirements similar to the travel rule imposed under section 13A of Schedule 2 and this Chapter in the jurisdictions in which the VA transfer counterparty operates and/or is incorporated; and (b) the adequacy and effectiveness of the AML/CFT controls that the VA transfer counterparty has put in place for ensuring compliance with the travel rule. In addition, the FI should assess whether the VA transfer counterparty can protect the confidentiality and integrity of personal data (e.g. the required originator and recipient information), taking into account the adequacy and robustness of data privacy and security controls of the VA transfer counterparty[162].
	12.13.9	When assessing the ML/TF risks posed by a VA transfer counterparty, an FI should take into account relevant factors that may indicate a higher ML/TF risk, for example, a VA transfer counterparty that: (a) operates or is incorporated in a jurisdiction posing a higher risk or with a weak AML/CFT regime; (b) is not (or is yet to be) licensed or registered and supervised for AML/CFT purposes in the jurisdictions in which it operates and/or is incorporated by authorities which perform functions similar to those of the RAs; (c) does not have in place adequate and effective

[162] This is to ensure that, among other things, the required information is submitted in a secure manner as mentioned in paragraph 12.11.12.

		AML/CFT Systems, including measures for ensuring compliance with the travel rule; (d) does not implement adequate measures or safeguards for protecting the confidentiality and integrity of personal data; or (e) is associated with ML/TF or other illicit activities.
<u>Ongoing monitoring</u>		
	12.13.10	An FI should monitor the VA transfer counterparties on an ongoing basis, including: (a) adopting an RBA in monitoring virtual asset transfers with VA transfer counterparties with a view to detecting any unexpected or unusual activities or transactions and any changes in the risk profiles of the VA transfer counterparties, taking into account the transaction monitoring requirements in Chapter 5 and paragraphs 12.7.2 to 12.7.4 and 12.7.6; and (b) reviewing the information obtained by the FI from applying the VA transfer counterparty due diligence measures under paragraph 12.13.6 on a regular basis and/or upon trigger events (e.g. when the FI is aware of any heightened ML/TF risks from its ongoing monitoring of virtual asset transfers with VA transfer counterparties or other information such as negative news from credible media or public information that the counterparty has been subject to any targeted financial sanction, ML/TF investigation or regulatory action) and, where appropriate, updating its risk assessment of a VA transfer counterparty. Based on the VA transfer counterparty due diligence results, the FI should determine if it should continue to conduct virtual asset transfers with, and submit the required information to, a VA transfer counterparty, and the extent of AML/CFT measures that it should apply in relation to virtual

		asset transfers with the VA transfer counterparty on a risk-sensitive basis[163].
<u>Other risk mitigating measures</u>		
	12.13.11	An FI should assess how the ML/TF risks identified from the VA transfer counterparty due diligence may affect it, and take reasonable measures on a risk-sensitive basis to mitigate and manage the ML/TF risks posed by a VA transfer counterparty[164], which include: (a) perform enhanced and/or more frequent due diligence reviews; (b) conduct enhanced monitoring of virtual asset transfers with the VA transfer counterparty; and (c) (where appropriate) impose transaction limits, when dealing with a VA transfer counterparty that presents a higher ML/TF risk.
	12.13.12	An FI should also determine on a risk-sensitive basis whether to restrict or continue to deal with, or refrain from executing or facilitating any virtual asset transfers to or from, a VA transfer counterparty that presents higher ML/TF risks. If the FI cannot mitigate and manage the ML/TF risks posed by a VA transfer counterparty, it should refrain from executing or facilitating such virtual asset transfers.
	12.13.13	An FI must not conduct virtual asset transfers with a VA transfer counterparty that is a shell VASP or shell financial institution[165].

[163] Further guidance on risk mitigating measures is set out in paragraphs 12.13.11 to 12.13.13.

[164] In particular, the FI should implement appropriate measures to mitigate and manage the risks posed by virtual asset transfers from or to originators or recipients that are third parties and ensure compliance with the requirements set out in Chapter 11 and paragraphs 12.10.

[165] An FI may refer to the guidance set out in paragraphs 4.20.16 and 12.6.7 to determine if the counterparty is a shell VASP or shell financial institution.

12.14 Virtual asset transfers to or from unhosted wallets		
	12.14.1	Peer-to-peer transactions associated with unhosted wallets[166] may be attractive to illicit actors given the anonymity and mobility of virtual assets and that there is typically no intermediary involved in the peer-to-peer transactions to carry out AML/CFT measures such as CDD and transaction monitoring. An FI should comply with the requirements set out in paragraphs 12.14.2 and 12.14.3 when conducting virtual asset transfers to or from unhosted wallets so as to mitigate the associated ML/TF risks.
	12.14.2	Before an FI sends or receives virtual assets to or from an unhosted wallet on behalf of its customer (i.e. the originator or the recipient, as the case may be), the FI should obtain the following originator and recipient information from the customer[167] and record: (a) in relation to a virtual asset transfer to an unhosted wallet, (i) the originator's name; (ii) the number of the originator's account maintained with the FI and from which the virtual assets are transferred or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the FI; (iii) the originator's address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth;

[166] Refer to paragraph 12.1.9 for the meaning of "unhosted wallets".

[167] For the avoidance of doubt, an FI is not required to obtain the originator information (for a virtual asset transfer to an unhosted wallet) or the recipient information (for a virtual asset transfer from an unhosted wallet) from a customer that is the originator or recipient respectively for every individual virtual asset transfer to or from an unhosted wallet (unless doubts arise as to veracity or adequacy of the information previously obtained for the purposes of customer identification and verification). For the purposes of paragraph 12.14.2, an FI is not required to obtain the information in (a)(iii) and (b)(iii) set out therein for a virtual asset transfer to or from an unhosted wallet involving virtual assets that amount to less than $8,000.

		(iv) the recipient's name; and (v) the recipient's wallet address; (b) in relation to a virtual asset transfer from an unhosted wallet, (i) the originator's name; (ii) the originator's wallet address; (iii) the originator's address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth; (iv) the recipient's name; and (v) the number of the recipient's account maintained with the FI and to which the virtual assets are transferred or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the FI.
	12.14.3	An FI should also assess the ML/TF risks associated with virtual asset transfers to or from unhosted wallets and take reasonable measures on a risk-sensitive basis to mitigate and manage the ML/TF risks associated with the transfers[168], which include: (a) conduct enhanced monitoring of virtual asset transfers with unhosted wallets; (b) accept virtual asset transfers only to or from unhosted wallets that the FI has assessed to be reliable[169], having regard to the screening results of the virtual asset transactions and the associated wallet addresses (see paragraphs 12.7.2 to 12.7.4 and 12.7.6) and the

[168] In particular, the FI should implement appropriate measures to mitigate and manage the risks posed by virtual asset transfers to or from third parties and ensure compliance with the requirements in Chapter 11 and paragraphs 12.10.

[169] For example, an FI may implement controls to prevent the relevant virtual assets from an unhosted wallet being made available to its customer, or putting the transfer to an unhosted wallet on hold, unless the FI is satisfied that the relevant unhosted wallet is reliable.

		assessment results of the ownership or control of the unhosted wallet [170] (see paragraphs 12.10.6 and 12.10.7); and (c) (where appropriate) impose transaction limits[171].
12.15 Illustrative risk indicators for assessing ML/TF risks		
	12.15.1	In addition to the non-exhaustive illustrative risk indicators for institutional risk assessment and customer risk assessment set out in Appendix A, paragraphs 12.15 set out non-exhaustive illustrative risk indicators in relation to virtual assets.
<u>Customer risk</u>		
	12.15.2	Examples of customers[172] that may present higher ML/TF risk include: (a) where the origin of wealth is substantially derived from activities that may present higher risks, e.g. initial coin offerings which are known to associate with predicate offences for ML/TF or financial crimes; virtual asset activities conducted via VASPs that are unregulated or with lax AML/CFT controls; (b) a customer who appears to operate as an unregulated VASP on peer-to-peer platforms, particularly when the customer handles or conducts frequent and/or large virtual asset transfers or transactions on behalf of its underlying customer(s), and charges higher

[170] Where virtual assets are transferred to or from an unhosted wallet that has been whitelisted in accordance with the requirements in paragraph 12.10.5, an FI should ascertain the ownership or control of the unhosted wallet on a periodic and risk-sensitive basis, in particular, where the FI becomes aware of any heightened ML/TF risks from the ongoing monitoring of virtual asset transactions and the associated wallet addresses or additional customer information (see paragraphs 12.7.2 to 12.7.6).

[171] For example, an FI may place appropriate limits on the amount of virtual asset transfers with unhosted wallets.

[172] These customer risk indicators are also relevant to FIs that are not SFC-licensed VAS Providers when, for example, the FI's customer is a VASP or derives its funds or wealth substantially from virtual assets.

		service fees compared to other VASPs; (c) a customer's wallet(s) used for deposit and withdrawal exhibit(s) patterns of virtual asset transactions associated with the use of anonymity-enhancing technologies or mechanisms (e.g. mixers, tumblers) or peer-to-peer platforms; and (d) a customer who is a VASP sets up offices in, or moves offices to, jurisdictions for no apparent business reason or posing a higher risk (especially those that neither prohibit nor regulate virtual asset-related activities or services).
<u>Product/service/transaction risk</u>		
	12.15.3	Examples of products, services or transactions[173] that may present higher ML/TF risk include: (a) products or services that may inherently favour anonymity or obscure information about underlying customer transactions, especially those involving the use of anonymity-enhancing technologies or mechanisms, or that are not supported by any technological solutions adopted for screening of virtual asset transactions and the associated wallet addresses[174]; (b) deposits from or payments to unknown or unrelated third parties in the form of virtual assets; (c) virtual assets that have been associated with fraud, market abuse or other illicit activities; (d) the purchase of virtual assets using physical cash; and (e) virtual asset-related products or services funded by payments from or instructions given by unexpected third parties, particularly from

[173] These product, service and transaction risk indicators are also relevant to FIs that are not SFC-licensed VAS Providers when, for example, an FI offers products, services or transactions involving virtual assets.

[174] Guidance on technological solutions adopted for screening of virtual asset transactions and the associated wallet addresses is provided in paragraphs 12.7.3 and 12.7.4.

		jurisdictions posing a higher risk.
12.16 Illustrative indicators of suspicious transactions and activities		
	12.16.1	In addition to the non-exhaustive illustrative indicators of suspicious transactions and activities set out in Appendix B, paragraphs 12.16 set out non-exhaustive illustrative indicators of suspicious transactions and activities in relation to virtual assets.
<u>Customer-related</u>		
	12.16.2	(a) A customer who has no discernible reason for using the FI's services (e.g. a customer has opened an account for virtual asset trading services but only deposits fiat currency or virtual assets and subsequently withdraws the entire balance or a substantial portion of the deposited assets without other activity; or a customer located in a place outside Hong Kong who opens an account with the FI to trade virtual assets that are also available from VASPs located in that place[175]); (b) Requests by customers for virtual asset trading services or virtual asset transfers where the source of the funds is unclear or not consistent with the customers' profile and apparent standing; (c) A customer who enters an FI's platform and/or initiates transactions from an IP address that may present higher risks, for example: (i) from jurisdictions posing a higher risk; (ii) not in line with the customer's profile (e.g. IP address from a jurisdiction which is not the customer's place of residence or principal business); (iii) previously identified as suspicious by the FI; or

[175] This may, for example, include situations where an FI acts as a respondent institution and provides trading services for virtual assets through a cross-border correspondent relationship with a correspondent institution (see paragraphs 4.20.1 and 12.6.1).

		(iv) associated with a darknet market or software that increases anonymity or allows anonymous communications (e.g. proxies, unverifiable IP geographical location, virtual private networks, The Onion Router (Tor)); (d) A customer and other apparently unrelated customer(s) entering the FI's platform from the same IP or MAC address; (e) A customer who frequently changes contact information, e.g. email address, phone number, especially when those are disposable or temporary[176]; and (f) A customer who frequently or over a short period of time, e.g. within a few hours, changes the IP address or device used to enter the FI's platform and/or conduct transactions.
<u>Trading-related</u>		
	12.16.3	(a) Buying and selling of virtual assets with no discernible purpose or where the nature, size or frequency of the transactions appears unusual. For example, where a customer repeatedly conducts virtual asset transactions with a particular person or group of persons at a significant profit or considerable loss, which may indicate that the transactions are used to transfer value or obfuscate funds flow as part of a ML/TF scheme, or a potential account takeover; (b) Mirror trades or transactions involving virtual assets used for currency conversion for illegitimate or no apparent business purposes; (c) Converting virtual assets to fiat currency at a potential loss with no apparent commercial rationale regardless of, for example, the price fluctuations or high commission fees; and (d) Conversion of a large amount of fiat currency

[176] This may also indicate a potential account takeover against a customer (i.e. a fraudster poses as a genuine customer, gains control of an account and then conducts unauthorised transactions).

		or virtual assets into other or multiple types of virtual assets with no logical or apparent reason which obscures the flow of funds.
<u>Market abuse activities-related</u>		
	12.16.4	(a) Placing of buy and sell orders in close chronological sequence for accounts with the same beneficial owner or of connected persons in the same virtual assets which are thinly-traded; (b) Multiple new customers are referred by the same individual to open accounts for trading in the same virtual asset within a short period of time; (c) A customer engages in prearranged or other non-competitive trading in particular virtual assets; (d) The entry of matching buy and sell orders in specific virtual assets ("wash trading"), creating the illusion of active trading with no change in the beneficial ownership of the virtual assets. Such wash trading does not result in a bona fide market position, which might also provide "cover" for a money launderer; (e) Accumulation of a virtual asset with small increments in price to gradually increase the price of the virtual asset over a period of time; (f) A customer makes large purchases of a virtual asset, particularly a virtual asset which is thinly-traded, within a short period of time, and the size of the transactions is incommensurate with the customer's profile; and (g) A group of customers sharing the same trading patterns (e.g. purchasing the same virtual asset at the same or similar time or price), particularly in relation to a virtual asset which is thinly-traded, authorise the same person or third party to operate their accounts and/or transfer fiat currency or virtual assets amongst their accounts.

Related to movement of funds and virtual assets		
	12.16.5	(a) A customer uses an FI to make payments or to hold funds or other property that are rarely used or are not being used to trade in virtual assets, i.e. the account appears to be used as a depositary account or a conduit for transfers; (b) Transfers of positions, funds, virtual assets or other property between accounts of parties that do not appear to be commonly controlled or have an apparent relationship; (c) Frequent funds, virtual assets or other property transfers or cheque payments to or from third parties that are unrelated or difficult to verify; (d) Transfers of funds or virtual assets to and from financial institutions or VASPs located in jurisdictions posing a higher risk[177], or, which are not consistent with the customer's declared place of residence, business dealings or interests, without reasonable explanation; (e) Transfers of funds or virtual assets to the same person from different parties, or to different persons from the same party without reasonable explanation; (f) Frequent changes of bank account or wallet address details or information for receiving funds or virtual assets; (g) Multiple transactions involving a high value of virtual assets where the nature, frequency or pattern of the transactions appears unusual, e.g. the transactions are conducted in short succession such as within a 24-hour period, or in a staggered and regular pattern followed by a long period of inactivity; transfer of virtual assets to another wallet, particularly a new wallet or wallet that has been inactive for a period of time, which may indicate possibility of ransomware attack or other cybercrimes; (h) Virtual assets are transferred from wallet

[177] For example, a VASP located in a jurisdiction that neither prohibits nor regulates virtual asset-related activities or services. Please also refer to guidance on jurisdictions posing a higher risk provided in paragraphs 4.13 for details.

		addresses which are known to hold stolen virtual assets, or are known to associate with holders of stolen virtual assets; (i) Deposits of virtual assets, including those from new customers, are immediately followed by transactions with no apparent legitimate purpose or commercial rationale which incur additional or unnecessary cost or fees (e.g. converting the deposited virtual assets to other or multiple types of virtual assets which obfuscates the trail of transactions, and/or withdrawing all or part of the deposited virtual assets to unhosted wallets immediately); (j) Transfers of virtual assets from multiple wallets in small amounts, in particular, those that are held by third parties, with subsequent transfer to another wallet or conversion of the entire amount to fiat currency; (k) Transactions involving virtual assets that provide higher anonymity such as anonymity-enhanced virtual assets (e.g. depositing a virtual asset that operates on a public blockchain and immediately converting it into a virtual asset that provides higher anonymity); (l) A customer uses an FI to convert an unusual amount (in terms of volume or number) of virtual assets from peer-to-peer platforms (e.g. a peer-to-peer platform with lax AML/CFT controls) into fiat currency for no logical or apparent reason; (m) Transfers of virtual assets to or from wallet addresses presenting higher risks, for example, wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources or designated parties[178];

[178] Guidance on identifying transactions involving wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities/sources or designated parties is provided in paragraph 12.7.3.

		(n) Transfers of virtual assets that have been associated with chain-hopping[179]; (o) Frequent and/or large transactions involving virtual assets from virtual asset automatic teller machines or kiosks, especially those located in jurisdictions posing a higher risk; (p) Information or message transmitted with a virtual asset transfer indicates that the transaction may be used to finance or assist illicit activities; (q) A customer who is a financially vulnerable person and/or has no prior knowledge of virtual assets engages in frequent and/or large transactions (in particular, deposits and withdrawals of funds and/or virtual assets) through an FI, which may be signs indicating money mule or scam victim; (r) Deposits of large amounts of virtual assets followed by conversion to fiat currencies, where the source of the funds is unclear and the size of transactions is not in line with the background of the customer, which may suggest that the deposited virtual assets are stolen assets; (s) A customer's funds or virtual assets originate from, or are sent to, a financial institution or VASP that (i) is not registered or licensed in the jurisdiction that it operates from (or where the customer to whom it offers products and/or services resides or is located), or (ii) operates from (or the customer to whom it offers products and/or services resides or is located in) a jurisdiction that neither prohibits nor regulates virtual asset-related activities or services; (t) The required information in a virtual asset transfer is inaccurate or incomplete, for example, in the case of an ordering institution, discrepancies were noted between the

[179] Refer to paragraph 12.1.8 for the meaning of "chain-hopping".

		recipient's information provided by its customer and the information maintained by the beneficiary institution which may have resulted in a rejection of the virtual asset transfer request or return of the relevant virtual assets by the beneficiary institution, or the information noted from the screening of the recipient's wallet address associated with the virtual asset transfer (see paragraphs 12.7.2 to 12.7.4 and 12.7.6); (u) A customer with limited or no other assets at the FI receives a transfer of large amounts of thinly-traded virtual assets; and (v) A customer deposits virtual assets and requests to credit them to multiple accounts that do not appear to be related, and to sell or otherwise transfer ownership of the virtual assets.
12.17 Miscellaneous illustrative examples and further guidance		
<u>Examples of possible enhanced measures in relation to RBA</u>		
	12.17.1	In addition to the examples of possible enhanced measures in relation to RBA set out in paragraph 2 of Appendix C, paragraph 12.17.2 sets out other examples relevant to virtual assets.
Para. 2.1, 2.13, 4.1.2 & 4.9.3 of this Guideline	12.17.2	Examples of possible enhanced measures relevant to virtual assets include: (a) where the customer is a financial institution or VASP [180] , obtaining additional or more particular information about the financial institution or VASP's underlying customer base and its AML/CFT controls; and (b) evaluating the information provided by the customer with regard to destination of funds or

[180] For the avoidance of doubt, where the provision of services by an FI to a customer that is a financial institution or VASP located in a place outside Hong Kong constitutes a cross-border correspondent relationship having regard to paragraphs 4.20.1 and 12.6.1 of this Guideline, the FI should also comply with the relevant provisions in paragraphs 4.20 and 12.6.

		virtual assets involved in the transaction and the reason for the transaction to better assess the risk of ML/TF.

APPENDIX A Illustrative risk indicators for assessing ML/TF risks

The following is a list of non-exhaustive illustrative risk indicators for institutional risk assessment and customer risk assessment. These examples of indicators associated with each risk factor mentioned in paragraphs 2.6 and 2.17 may indicate higher or lower ML/TF risks as the case may be.

1	**Country risk**
	Examples of countries or jurisdictions[181] that may present higher ML/TF risk include: (a) countries or jurisdictions that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies; (b) countries or jurisdictions subject to sanctions, embargos or similar measures issued by, for example, the UN; (c) countries or jurisdictions which are more vulnerable to corruption[182]; and (d) countries or jurisdictions that are believed to have strong links to terrorist activities. Examples of countries or jurisdictions that may be considered to carry lower ML/TF risk include: (a) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems; and (b) countries or jurisdictions identified by credible sources as having a low level of corruption or other criminal activity.

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

[182] When assessing which countries are more vulnerable to corruption, FIs may make reference to publicly available information or relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations (an example of which is Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption).

2	**Customer risk**
	Examples of customers that may present higher ML/TF risk include: (a) the business relationships established in unusual circumstances (e.g. a customer instructs an FI to set up a discretionary management agreement for an investment vehicle owned by the customer but requests the FI to buy and sell particular securities for the investment vehicle only according to the customer's instructions); (b) non-resident customers who have no discernible reasons for opening an account with FIs in Hong Kong; (c) the use of legal persons or arrangements as personal asset-holding vehicles without any commercial or other valid reasons; (d) companies that have nominee shareholders, nominee directors, bearer shares or bearer share warrants; (e) customers that engage in, or derive wealth or revenues from, cash-intensive businesses; (f) the ownership structure of a company appears unusual or excessively complex having considered the nature of the company's business; (g) the customer or the family member or close associate of a customer is a PEP (including where a beneficial owner of a customer is a PEP); (h) customers that have been mentioned in negative news reports from credible media, particularly those related to predicate offences for ML/TF or financial crimes; (i) nature, scope and location of business activities generating the funds[183] may be related to high risk activities or jurisdictions posing a higher risk; (j) customers that have sanction exposure; (k) where the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified; and (l) a customer introduced by an overseas financial institution, affiliate or other investor, both of which are based in jurisdictions posing a higher risk[184].

[183] Consideration should be given to the risks inherent in the nature of the activity of the customer and the possibility that the transaction may itself be a criminal transaction.
[184] Guidance on jurisdictions posing a higher risk is provided in paragraphs 4.13.

	Examples of customers that may be considered to carry lower ML/TF risk include: (a) specific types of customers that may be eligible for SDD as specified in paragraph 4.8.3 or simplified measures as specified in paragraph 4 of Appendix C; (b) customers who are employment-based or with a regular source of income from a known legitimate source which supports the activity being undertaken; and (c) the reputation of the customer, e.g. a well-known, reputable private company, with a long history that is well documented by independent sources, including information regarding its ownership and control.
3	**Product/service/transaction risk**
	Examples of products, services or transactions that may present higher ML/TF risk include: (a) products or services that may inherently favour anonymity or obscure information about underlying customer transactions; (b) products that have the ability to pool underlying customers/funds; (c) deposits from or payments to unknown or unrelated third parties; (d) the products or services offered to customers associated with jurisdictions posing a higher risk (e.g. where a customer resides in a jurisdiction posing a higher risk or where the customer's source of funds or source of wealth is mainly derived from jurisdictions posing a higher risk); (e) products with unusual complexity or structure and with no obvious economic purpose; (f) products or services that permit the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly from jurisdictions posing a higher risk; (g) use of new technologies or payment methods not used in the normal course of business by the FI; (h) products that have been particularly subject to fraud and market abuse, such as low-priced/small-cap and

	thinly-traded stocks; (i) the purchase of securities using physical cash; and (j) securities-related products or services funded by payments from or instructions given by unexpected third parties, particularly from jurisdictions posing a higher risk. Examples of products, services or transactions that may be considered to carry lower ML/TF risk include: (a) specific types of products that may be eligible for SDD as set out in paragraph 4.8.15.
4	**Delivery/distribution channel risk**
	Examples of delivery/distribution channels that may present higher ML/TF risk include: (a) business relationships established using a non-face-to-face approach or transactions conducted by customer through non-face-to-face channels, where increased risks (e.g. impersonation or identity fraud) could not be adequately mitigated and/or are more susceptible to risk situations such as unauthorised trading and related ML/TF abuse; and (b) products or services distributed or sold through intermediaries (i.e. business relationship between an FI and the end customer may become indirect), especially if the intermediaries are: (i) suspected of criminal activities, particularly financial crimes or association with criminal associates; (ii) located in a higher risk country or in a country with a weak AML/CFT regime; (iii) serving high risk customers without appropriate risk mitigating measures; or (iv) with a history of non-compliance with laws or regulation or that have been the subject of relevant negative attention from credible media or law enforcement. Examples of delivery/distribution channels that may be considered to carry lower ML/TF risk include:

	(a) business relationships established or transactions conducted by customers through channels that are less susceptible to risk situations such as unauthorised trading and related ML/TF abuse; and (b) products or services distributed or sold directly to the customer.

APPENDIX B Illustrative indicators of suspicious transactions and activities

The following is a list of non-exhaustive illustrative indicators of suspicious transactions and activities that may help assess whether or not transactions and activities might give rise to grounds of ML/TF suspicion.

1	**Customer-related**
	(a) A customer who has no discernible reason for using the FI's services (e.g. a customer has opened an account for discretionary management services but directs the FI to carry out his own investment decisions or a customer located in a place outside Hong Kong who uses local accounts to trade on stock or futures exchanges located in that place); (b) A customer who has requested, without reasonable explanation, transactions that are out of the ordinary range of services normally requested, or are outside the experience of the financial services business in relation to the particular customer; (c) Extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services; (d) A legal person customer with bearer shares constituting a large part of its issued capital; (e) A customer who has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason; (f) A customer's legal or mailing address is associated with other apparently unrelated accounts; or does not seem connected to the customer; (g) Requests by customers for dealing or investment management services (with regard to securities, futures contracts or leveraged foreign exchange contracts) where the source of the funds is unclear or not consistent with the customers' profile and apparent standing; (h) A customer who refuses to provide the information

	requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process; (i) A customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation; (j) A customer who exhibits unusual concern with the FI's AML/CFT Systems including policies, controls, monitoring or reporting thresholds; (k) A customer who does not exhibit any concern with the cost of transactions or fees; and (l) A customer who is known to have criminal, civil or regulatory proceedings against it for corruption, misuse of public funds, other financial crimes or regulatory non-compliance, or is known to associate with such persons.
2	**Trading-related**
	(a) Transactions or instructions which have no apparent legitimate purpose or commercial rationale or involve apparently unnecessary complexity; (b) The size or pattern of transactions is not in line with the background of the customer or its past transaction volume/pattern; (c) Buying and selling of securities, futures or leveraged foreign exchange contracts with no discernible purpose or where the nature, size or frequency of the transactions appears unusual. For example, where a customer frequently purchases securities at a high price and subsequently sells them at a considerable loss to the same party. This may indicate transferring value from one party to another; (d) A number of transactions by the same customer in small amounts relating to the same investment, each purchased for cash and then sold in one transaction, the proceeds being paid to a person other than that customer; (e) Mirror trades or transactions involving securities used for currency conversion for illegitimate or no apparent business purposes; (f) Securities, futures or leveraged foreign exchange

	contracts transactions occur across many jurisdictions, and in particular jurisdictions posing a higher risk; (g) Securities intended to be held-to-maturity are unwound before maturity in the absence of volatile market conditions or other logical or apparent reason; and (h) Suspected front-running of other pending customer orders.
3	**Selected indicators of market manipulation[185] and insider dealing**
	(a) Making a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security, which may be suggestive of potential insider trading or market manipulation; (b) A request to execute or clear a buy order and sell order in close chronological sequence for accounts with the same beneficial owner or of connected persons in the same securities which are thinly-traded; (c) Multiple new customers are referred by the same individual to open accounts for trading in the same security within a short period of time; (d) A customer engages in prearranged or other non-competitive trading in particular securities or futures contracts; (e) The entry of matching buy and sell orders in particular securities or futures contracts ("wash trading"), creating the illusion of active trading. Such wash trading does not result in a bona fide market position, which might also provide "cover" for a money launderer; (f) Transfers of positions between accounts that do not appear to be commonly controlled; (g) Accumulation of a security with small increments in price throughout the trading day to increase the price of the security; (h) Executing purchase or sale orders for one or more accounts in a security regularly at or near the close of

[185] FIs are expected to take appropriate steps to ensure that proper safeguards exist to prevent the firm from acting in a way which would result in the firm perpetrating any conduct which constitutes market misconduct under section 274, 275 or 278 of the SFO, or any criminal offence under section 295, 296 or 299 of the SFO.

	market trading hours that alter the closing price of the security; and (i) Placing multiple buy or sell orders and cancelling some or all of them before execution regularly.
4	**Related to deposits of securities**
	(a) The customer's explanation regarding the method of acquiring the physical share certificates deposited at the FI does not make sense or changes; (b) A customer has a pattern of depositing physical share certificates or receiving incoming share transfers, forthwith selling the shares and transferring out the proceeds; (c) A customer with limited or no other assets at the FI receives a transfer of large amounts of thinly-traded securities; and (d) A customer deposits securities and requests to credit them to multiple accounts that do not appear to be related, and to sell or otherwise transfer ownership of the securities.
5	**Related to settlement and movement of funds and securities**
	(a) Large or unusual settlements of transactions in cash or bearer form or where a customer only deals with an FI in cash; (b) A customer uses an FI to make payments or to hold funds or other property that are rarely used or are not being used to trade in securities, futures contracts or leveraged foreign exchange contracts, i.e. account appears to be used as a depositary account or a conduit for transfers; (c) Non-resident customer's account with very large account movements and subsequent fund transfers to offshore financial centres; (d) Transfers of positions, funds or other property between securities accounts of parties that do not appear to be commonly controlled or have an apparent relationship; (e) Frequent funds or other property transfers or cheque payments to or from third parties that are unrelated or difficult to verify;

	(f) Transfers to and from jurisdictions posing a higher risk without reasonable explanation, which are not consistent with the customer's declared business dealings or interests; (g) The involvement of offshore companies on whose accounts multiple transfers are made, especially when they are destined for a tax haven, and to accounts in the name of offshore companies of which the customer may be a shareholder; (h) Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring threshold; (i) Transfers of funds or securities to the same person from different parties, or to different persons from the same party without reasonable explanation; (j) Funds are transferred to other FIs in different jurisdictions from the FI where the funds were initially received; and (k) Frequent changes of bank account details or information for receiving investment sale proceeds.
6	**Employee-related**
	(a) Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays without reasonable cause; (b) Unusual or unexpected increase in the sales performance of an employee; (c) The employee's supporting documentation for customers' accounts or orders is incomplete or missing; and (d) The use of an address which is not the customer's home or office address, e.g. utilisation of an employee's address for the dispatch of customer documentation or correspondence.

APPENDIX C Miscellaneous illustrative examples and further guidance

	1	**Examples of possible simplified measures in relation to RBA**
Para. 2.1, 2.13 & 4.1.2 of this Guideline		Examples include: (a) limiting the type or extent of CDD measures, such as altering the type or range of documents, data or information used for verifying the identity of a customer; (b) reducing the frequency of review of the existing CDD records; (c) reducing the degree of ongoing monitoring and scrutiny of transactions based on a reasonable monetary threshold; or (d) 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.
	2	**Examples of possible enhanced measures in relation to RBA**
Para. 2.1, 2.13, 4.1.2 & 4.9.3 of this Guideline		Examples include: (a) obtaining additional information from a wide variety of sources [186] on the customer and (where appropriate) the beneficial owner of the customer before the establishment of the business relationship, and for performing ongoing customer risk assessment; (b) increasing the frequency of review of the existing CDD records; (c) obtaining additional information and corroborating it with other available sources on

[186] Examples of additional information include occupation, volume of assets, reputation and background of the customer and (where appropriate) the beneficial owner. Examples of sources include the internet and publicly or commercially available databases.

		the purpose and intended nature of the business relationship or transaction; (d) obtaining additional information and corroborating it with other available sources on the customer's source of wealth or source of funds involved in the transaction or business relationship[187]; (e) increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination; (f) where the customer is a financial institution[188], obtaining additional or more particular information about the financial institution's underlying customer base and its AML/CFT controls; (g) evaluating the information provided by the customer with regard to destination of funds involved in the transaction and the reason for the transaction to better assess the risk of ML/TF; (h) requiring that investment sale proceeds are paid to the customer's bank account from which the funds for investment were originally transferred; or (i) where an FI is being appointed by a customer that is an asset management company located in a place outside Hong Kong (the "delegating asset management company") to provide discretionary asset management services in relation to an investment vehicle and does not have a business relationship with the investment vehicle, where appropriate, obtaining additional customer information such as a general understanding of the delegating asset management company's customer base (e.g.

[187] Guidance on source of wealth and source of funds are provided in paragraphs 4.11.13 and 4.11.14. For the avoidance of doubt, for a customer or beneficial owner of a customer that is a non-Hong Kong PEP, a Hong Kong PEP or an international organisation PEP, and in any situation that by its nature presents a higher risk of ML/TF, the respective special requirements set out in paragraphs 4.11 and 4.9 apply.

[188] For the avoidance of doubt, where the provision of services by an FI to a customer that is a financial institution located in a place outside Hong Kong constitutes a cross-border correspondent relationship having regard to paragraph 4.20.1 of this Guideline, the FI should also comply with the relevant provisions in paragraphs 4.20.

		the types of funds it transacts for; these funds' investor bases in their entirety; and the jurisdictions where these funds are offered), the reputation of the delegating asset management company (e.g. whether it has or had been subject to any targeted sanctions, ML/TF investigations or regulatory actions) and its AML/CFT controls; obtaining senior management approval and understanding respective AML/CFT responsibilities clearly.
	3	**Examples of possible measures in relation to the verification of the name, legal form and current existence of a customer that is a legal person**
Para. 4.2.6 of this Guideline		Examples of possible measures to verify the name, legal form and current existence of a legal person: for a locally incorporated company: (a) performing a search of file at the Hong Kong Company Registry to obtain a company report (or obtaining from the customer a certified true copy of a company search report issued and certified by a company registry or professional person); for a company incorporated overseas: (b) performing a similar company search enquiry of the registry in the place of incorporation to obtain a company report; (c) obtaining a certificate of incumbency or equivalent issued by the company's registered agent in the place of incorporation (or accepting a certified true copy of a certificate of incumbency certified by a professional person); or (d) obtaining a similar or comparable document to a company search report or a certificate of incumbency certified by a professional person in the relevant jurisdiction.

	4	**Examples of simplified and enhanced measures in verifying the identity of a customer that is a legal person, trust or other similar legal arrangement**
Para. 4.2.14 of this Guideline		<u>Simplified measures</u> Where the assessed ML/TF risks are lower, an FI may consider to accept documents, data or information other than the examples provided in paragraphs 4.2.6 and 4.2.11, when verifying the name, legal form and current existence of the customer, or powers that regulate and bind the customer. Examples of such other documents, data or information include: (a) where the customer is (i) an FI as defined in the AMLO; or (ii) other FI that is incorporated or established in an equivalent jurisdiction, carry on a business similar to that carried out by an FI as defined in the AMLO, and subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, a proof that the customer is a licensed (and supervised) FI in the jurisdiction concerned; (b) where the customer is a listed company, a proof of its listed status; (c) where the customer is the government or a public body in Hong Kong or in an equivalent jurisdiction, a proof that the customer is the government or a public body; and (d) where the customer is a collective investment scheme authorised for offering to the public in Hong Kong or in an equivalent jurisdiction, a proof of its authorisation status. <u>Enhanced measures</u> Where the assessed ML/TF risks are higher, in addition to verifying the name, legal form and current existence of the customer, and powers that

		regulate and bind the customer in accordance with paragraphs 4.2.6 and 4.2.11, an FI should decide whether additional information in respect of the customer, its operation and the individuals behind it should be obtained and the extent of further verification that is required.
	5	**Examples of information which may be collected to identify the intermediate layers of the corporate structure of a legal person with multiple layers in its ownership structure**
Para. 4.3.13 of this Guideline		If the customer's ownership structure consists of multiple layers of companies, an FI should determine on a risk-sensitive basis the amount of information in relation to the intermediate layers to be collected, which may include obtaining a director's declaration incorporating or annexing an ownership chart describing the intermediate layers (the information to be included should be determined on a risk-sensitive basis but at a minimum should include company name and place of incorporation, and where applicable, the rationale behind the particular structure employed). FIs need not, as a matter of routine, verify the details of the intermediate companies in the ownership structure of a company. Complex ownership structures (e.g. structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to ensure that the FI is satisfied on reasonable grounds as to the identities of the beneficial owners. The need to verify the intermediate corporate layers of the ownership structure of a company will therefore depend upon the FI's overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for the FI to consider if it has taken adequate measures to identify the beneficial owners.

		Where the ownership is dispersed, the FI may concentrate on identifying and taking reasonable measures to verify the identities of those who exercise ultimate control over the management of the company.
	6	**Examples of procedures to establish whether the identification documents offered by customers are genuine, or have been reported as lost or stolen**
Para. 4.5.3 of this Guideline		If suspicions are raised in relation to any identification document offered by customers, FIs should take whatever practical and proportionate steps that are available to establish whether the document offered is genuine, or has been reported as lost or stolen. This may include: (a) searching publicly available information; (b) approaching relevant authorities (such as the Immigration Department through its hotline); or (c) requesting corroboratory evidence from the customer. Where suspicion cannot be eliminated, the document should not be accepted and consideration should be given to making a report to the authorities.

	7	**Use of an independent and appropriate person to certify identification documents**
Para. 4.10.5 of this Guideline	7.1	Use of an independent[189] and appropriate person to certify verification of identification documents guards against the risk that documentation provided does not correspond to the customer whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation.
	7.2	The following is a list of non-exhaustive examples of appropriate persons to certify verification of identification documents: (a) an intermediary specified in section 18(3) of Schedule 2; (b) a member of the judiciary in an equivalent jurisdiction; (c) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; (d) a Justice of the Peace; and (e) other professional person[190] such as certified public accountant, lawyer, notary public and chartered secretary[191].
	7.3	The certifier should sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it. The certifier should state that it is a true copy of the original (or words to similar effect).

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

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

[191] A chartered secretary refers to a current member of The Chartered Governance Institute (formerly The Institute of Chartered Secretaries and Administrators) who has attained the chartered status.

	7.4	FIs remain liable for failure to carry out prescribed CDD and therefore should exercise caution when considering accepting certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. In any circumstances where an FI is unsure of the authenticity of certified documents, or that the documents relate to the customer, FIs should take additional measures to mitigate the ML/TF risk.
	8	**Examples of trigger events upon which existing records of customers should be reviewed**
Para. 5.2 of this Guideline		Examples of trigger events include: (a) when a significant transaction[192] is to take place; (b) when a material change occurs in the way the customer's account is operated[193]; (c) when the FI's customer documentation standards change substantially; or (d) when the FI is aware that it lacks sufficient information about the customer concerned.

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

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

GLOSSARY OF KEY TERMS AND ABBREVIATIONS

Terms / abbreviations	Meaning
AMLO	Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)
AML/CFT	Anti-money laundering and counter-financing of terrorism
AML/CFT Systems	AML/CFT policies, procedures and controls
CDD	Customer due diligence
CO	Compliance officer
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
FATF	Financial Action Task Force
FI(s)	Financial institution(s)
JFIU	Joint Financial Intelligence Unit
MLRO	Money laundering reporting officer
ML/TF	Money laundering and terrorist financing
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)
PEP(s)	Politically exposed person(s)
PPTA	Person purporting to act on behalf of the customer
Proliferation financing or PF	Financing of proliferation of weapons of mass destruction

RA(s)	Relevant authority (authorities)
RBA	Risk-based approach
Schedule 2	Schedule 2 to the AMLO
Senior management	Senior management means directors (or board) and senior managers (or equivalent) of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business. This may include a firm's Chief Executive Officer, Managing Director, Responsible Officer, Manager-In-Charge of Core Function(s) or other senior operating management personnel (as the case may be).
SFO	Securities and Futures Ordinance (Cap. 571)
STR(s)	Suspicious transaction report(s); also referred to as reports or disclosures
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
UNSO	United Nations Sanctions Ordinance (Cap. 537)
VASP(s)	Virtual asset service provider(s)
WMD(CPS)O	Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526)