GL3

Guideline on Anti-Money Laundering and Counter-Terrorist Financing

(For authorized insurers and reinsurers carrying on long term business, and licensed individual insurance agents, licensed insurance agencies and licensed insurance broker companies carrying on regulated activities in respect of long term business)

Insurance Authority

June 2023

Contents Page

Chapter 1 – OVERVIEW		
Introduction		
	1.1	This Guideline is published under section 7 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (AMLO) and section 133 of the Insurance Ordinance, Cap. 41 (IO), and shall take effect from 1 June 2023.
	1.2	Terms and abbreviations used in this Guideline should be interpreted by reference to the definitions set out in the Glossary part of this Guideline. Where applicable, interpretation of other words or phrases should follow those set out in the AMLO or the IO.
	1.3	This Guideline is issued by the Insurance Authority (IA) and sets out the relevant anti-money laundering and counter-financing of terrorism (AML/CFT) statutory and regulatory requirements, and the AML/CFT standards which authorized insurers and reinsurers carrying on long term business, and licensed individual insurance agents, licensed insurance agencies and licensed insurance broker companies carrying on regulated activities in respect of long term business (hereafter referred to as "insurance institutions" ("IIs")), should meet in order to comply with the statutory requirements under the AMLO and the IO. Compliance with this Guideline is enforced through the AMLO and the IO. IIs which fail to comply with this Guideline may be subject to disciplinary or other actions under the AMLO and/or the IO for non-compliance with the relevant requirements.
	1.4	This Guideline is intended for use by IIs and their officers and staff[1]. 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 IIs and their senior management in designing and implementing their own policies, procedures and controls in the relevant operational areas, taking into consideration their special circumstances, so as to meet the relevant AML/CFT statutory and regulatory requirements.
	1.5	The relevance and usefulness of this Guideline will be kept under review and it may be necessary to issue amendments from time to time.

[1] For the purpose of this Guideline, staff include licensed individual insurance agents and licensed technical representatives (agent)/(broker).

	1.6	For the avoidance of doubt, the use of the word "must" or "should" in relation to an action, consideration or measure referred to in this Guideline indicates that it is a mandatory requirement. Given the significant differences that exist in the organizational and legal structures of different IIs 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. IIs should therefore use this Guideline as a basis to develop measures appropriate to their structure and business activities.
s.7, AMLO	1.7	This Guideline also provides guidance in relation to the operation of the provisions of Schedule 2 to the AMLO (Schedule 2). This will assist IIs to meet their legal and regulatory obligations when tailored by IIs to their particular business risk profile. A failure by any person to comply with any provision of this Guideline does not by itself render the person liable to any judicial or other proceedings but, in any proceedings under the AMLO before any court, this Guideline is admissible in evidence; and if any provision set out in this Guideline appears to the court to be relevant to any question arising in the proceedings, the provision must be taken into account in determining that question. In considering whether a person has contravened a provision of Schedule 2, the IA must have regard to any relevant provision in this Guideline.
	1.8	A failure to comply with any provision of this Guideline by an authorized insurer or a reinsurer carrying on long term business may, for example, reflect adversely on the fitness and properness of its directors and controllers[2], and may result in disciplinary action being taken against the authorized insurer or reinsurer concerned. In addition, a failure to comply with any provision of this Guideline by a licensed individual insurance agent, a licensed insurance agency or a licensed insurance broker company carrying on regulated activities in respect of long term business may, for example, reflect adversely on the fitness and properness of the licensed individual insurance agent, and (in the case of a licensed insurance agency and a licensed insurance broker company) its controller(s), director(s) and responsible officer(s)[3], and may result in disciplinary action being taken against the regulated persons[4].

[2] For interpretations of the terms "director" and "controller", please refer to section 2 of the IO.

[3] "Controller", in relation to licensed insurance agencies and licensed insurance broker companies, has the meaning given to it by section 64F of the IO; and "director" and "responsible officer" are defined in section 2 of the IO.

[4] For the definition of "regulated person", please refer to section 80 of the IO.

The nature of money laundering and terrorist financing		
s.1, Sch. 1, AMLO	1.9	The term "money laundering" (ML) is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means an act intended to have the effect of making any property: (a) that is the proceeds obtained from the commission of an indictable offence under the laws of Hong Kong, or of any conduct which if it had occurred in Hong Kong would constitute an indictable offence under the laws of Hong Kong; or (b) that in whole or in part, directly or indirectly, represents such proceeds, not to appear to be or so represent such proceeds.
	1.10	There are three common stages in the laundering of money, and they frequently involve numerous transactions. An II 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.
s.1, Sch. 1, AMLO	1.11	The term "terrorist financing" (TF) is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means: (a) the provision or collection, by any means, directly or indirectly, of any property – (i) with the intention that the property be used; or (ii) knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used); (b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or (c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.

	1.12	Terrorists or terrorist organizations 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.
Vulnerabilities in insurance industry		
	1.13	When a life insurance policy matures or is surrendered, funds become available to the policy holder or other beneficiaries (e.g. an assignee, where the policy has been assigned, or a trustee, where the policy has been placed in trust). The beneficiary to the contract may be changed before maturity or surrender, so that the payments are made by the insurer to a new beneficiary. A money launderer or terrorist financier may attempt to achieve their objective by nominating their conspirator as a beneficiary of a life insurance policy. Also, a life insurance policy might be used as collateral to purchase other financial instruments.
	1.14	[5] Examples of attributes which may tend to increase the ML/TF risk profile include: (a) Product/service/transaction-related risk: (i) acceptance of very high value or unlimited value payments or large volumes of lower value payments; (ii) acceptance of non-traceable payments such as cash, money orders, cashier cheques, or virtual assets; (iii) acceptance of frequent payments outside a normal premium or payment schedule; (iv) allowance of withdrawals at any time or early surrender, with limited charges or fees; (v) customer is not the payer or recipient of the funds; (vi) products with features that allow loans to be taken against the policy (particularly if frequent loans can be taken and/or repaid with cash); and (vii) significant, unexpected, or unexplained change in customer's pattern of payment, withdrawal, or surrender; (b) Geographic-related risk: (i) jurisdictions identified by credible sources as having weak governance, law enforcement and regulatory regimes, including jurisdictions identified by FATF statements as having weak AML/CFT regimes; and (ii) jurisdictions identified by credible sources as having

[5] Further examples of attributes are documented in the IAIS document "Application Paper on Combating Money Laundering and Terrorist Financing". The document can be downloaded at http://www.iaisweb.org. IIs are advised to browse the IAIS website regularly for the latest examples of attributes which may tend to increase the ML/TF risk profile.

		significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking, smuggling and illegal gambling; (c) Customer-related risk: (i) structure of a legal entity that is a customer, policy holder, or beneficiary obscures or makes it difficult to identify the ultimate beneficial owner or controlling interests; (ii) customer is reluctant to provide identification; exhibits difficulty producing identification; or provides identification documents of questionable authenticity; (iii) mismatch between wealth and income of the customer and proposed premium amounts, deposit amounts or policy limits; and (iv) customer is associated with negative news which may affiliate the customer with allegations of criminal behavior; or has ties to or is on a designated sanctions list; (d) Delivery/distribution channel-related risk: (i) payments via intermediary that may obscure the source of payment (e.g. long chain of intermediaries).
	1.15	Insurance intermediaries [6] are important for distribution, underwriting and claims settlement. They are often the direct link to the policy holder and therefore, intermediaries should play an important role in AML and CFT. The same principles that apply to authorized insurers should generally apply to insurance intermediaries. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of or does not conform to necessary procedures, or who fails to recognize or report information regarding possible cases of ML or TF. The intermediaries themselves could have been set up to channel illegitimate funds to insurers.
	1.16	An II should also give due consideration to the ML/TF threats and vulnerabilities in insurance industry identified in relevant risk assessments which may be issued from time to time, e.g. Hong Kong's jurisdiction-wide ML/TF risk assessment.
Legislation concerned with ML, TF, financing of proliferation of weapons of mass destruction (PF) and financial sanctions		
	1.17	The Financial Action Task Force (FATF) is an inter-governmental body established in 1989. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating of ML, TF, PF,

[6] "Insurance intermediaries" refer to all licensed insurance intermediaries carrying on regulated activities in respect of long term business.

		and other related threats to the integrity of the international financial system. The FATF has developed a series of Recommendations that are recognized as the international standards for combating of ML, TF and PF. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. In order to ensure full and effective implementation of its standards at the global level, the FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow-up after the evaluations, including identifying high-risk and other monitored jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large. Many major economies have joined the FATF which has developed into a global network for international cooperation that facilitates exchanges between member jurisdictions. As a member of the FATF, Hong Kong is obliged to implement the latest FATF Recommendations[7] 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.
	1.18	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 IIs and their officers and staff fully understand their respective responsibilities under the different legislation.
<u>AMLO</u>		
s.23, Sch. 2	1.19	The AMLO imposes requirements relating to customer due diligence (CDD) and record-keeping on IIs and provides the IA with the powers to supervise compliance with these requirements and other requirements under the AMLO. In addition, section 23 of Schedule 2 requires IIs 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	1.20	The AMLO makes it a criminal offence if an II (1) knowingly; or (2) with the intent to defraud the IA, contravenes a specified provision of the AMLO. The "specified provisions" are listed in section 5(11) of the AMLO. If the II knowingly contravenes a specified provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If the II

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

		contravenes a specified provision with the intent to defraud the IA, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.
s.5, AMLO	1.21	The AMLO also makes it a criminal offence if a person who is an employee of an II or is employed to work for an II or is concerned in the management of an II (1) knowingly; or (2) with the intent to defraud the II or the IA, causes or permits the II to contravene a specified provision in the AMLO. If the person who is an employee of an II or is employed to work for an II or is concerned in the management of an II 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 II or the IA, he is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.
s.21, AMLO	1.22	The IA may take disciplinary actions against IIs for any contravention of a specified provision in the AMLO. The disciplinary actions that can be taken include publicly reprimanding the II; ordering the II to take any action for the purpose of remedying the contravention; and ordering the II 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 II as a result of the contravention.
DTROP		
	1.23	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		
	1.24	The OSCO, among other things: (a) gives officers of the Hong Kong Police Force and the Customs and Excise Department powers to investigate organized crime and triad activities; (b) gives the Courts jurisdiction to confiscate the proceeds of organized and serious crimes, to issue restraint orders and charging orders in relation to the property of a defendant of an offence specified in the OSCO; (c) creates an offence of 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 organized crime/triad related offence or other serious offences.

UNATMO		
	1.25	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	1.26	Under the DTROP and the OSCO, a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking or of an indictable offence respectively. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine of $5 million.
s.6, 7, 8, 8A, 13 & 14, UNATMO	1.27	The UNATMO, among other things, criminalizes the provision or collection of property and making any property or financial (or related) services available to terrorists or terrorist associates. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine. The UNATMO also permits terrorist property to be frozen and subsequently forfeited.
s.25A, DTROP & OSCO, s.12 & 14, UNATMO	1.28	The DTROP, the OSCO and the UNATMO also make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly, represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property respectively. This offence carries a maximum term of imprisonment of 3 months and a fine of $50,000 upon conviction.
s.25A, DTROP & OSCO, s.12 & 14, UNATMO	1.29	"Tipping off" is another offence under the DTROP, the OSCO and the UNATMO. A person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following that first-mentioned disclosure. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.
UNSO		
	1.30	The UNSO provides for the imposition of sanctions against persons and against places outside the People's Republic of China arising from Chapter 7 of the Charter of the United Nations. Most UNSCRs are implemented in Hong Kong under the UNSO.
WMD(CPS)O		
s.4, WMD(CPS)O	1.31	The WMD(CPS)O controls the provision of services that will or may assist the development, production, acquisition or stockpiling

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

Chapter 2 – RISK-BASED APPROACH		
Introduction		
	2.1	The risk-based approach (RBA) is central to the effective implementation of an AML/CFT regime. An RBA to AML/CFT means that jurisdictions, competent authorities, and IIs are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate with those risks in order to manage and mitigate them effectively. RBA allows an II to allocate its resources more effectively and apply preventive measures that are commensurate with the nature and level of risks, in order to focus its AML/CFT efforts in the most effective way. Therefore, an II should adopt an RBA in the design and implementation of its AML/CFT policies, procedures and controls (hereafter collectively referred to as "AML/CFT Systems") with a view to managing and mitigating ML/TF risks.
Institutional ML/TF risk assessment		
	2.2	The institutional ML/TF risk assessment forms the basis of the RBA, enabling an II to understand how and to what extent it is vulnerable to ML/TF. The II should conduct an institutional ML/TF risk assessment to identify, assess and understand its ML/TF risks in relation to: (a) its customers; (b) the countries or jurisdictions its customers are from or in; (c) the countries or jurisdictions the II has operations in; (d) the products/services/transactions of the II; and (e) delivery/distribution channels of the II.
	2.3	The appropriate steps to conduct the institutional ML/TF risk assessment should include: (a) documenting the risk assessment process which includes the identification and assessment of relevant risks supported by qualitative and quantitative analysis, and information obtained from relevant internal and external sources; (b) considering all the relevant risk factors before determining what the level of overall risk is, and the appropriate level and type of mitigation to be applied; (c) obtaining the approval of senior management on the risk assessment results; (d) having a process by which the risk assessment is kept up-to-date; and (e) having appropriate mechanisms to provide the risk assessment to the IA when required to do so.

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

	2.8	For the purpose of paragraphs 2.2 and 2.7, if an II is a part of a financial group and a group-wide or regional ML/TF risk assessment has been conducted, it may make reference to or rely on those assessments provided that the assessments adequately reflect ML/TF risks posed to the II in the local context.
	2.9	To keep the institutional ML/TF risk assessment up-to-date, an II should conduct its assessment every two years and upon trigger events[8] which are material to the II's business and risk exposure.
New products, new business practices and use of new technologies		
	2.10	An II should identify and assess the ML/TF risks that may arise in relation to: (a) the development of new products and new business practices, including new delivery/distribution mechanisms; and (b) the use of new or developing technologies for both new and pre-existing products.
	2.11	An II should undertake the risk assessment prior to the launch of new products, new business practices, or the use of new or developing technologies, and should take appropriate measures to manage and mitigate the risks identified.
Customer risk assessment		
	2.12	An II should assess the ML/TF risks associated with a proposed business relationship, which is usually referred to as a customer risk assessment. The assessment conducted at the initial stage of the CDD process would determine the extent of CDD measures to be applied[9]. This means that the amount and type of information obtained, and the extent to which this information is verified, should be increased where the ML/TF risks associated with the business relationship are higher. It may also be simplified where the ML/TF risks associated with the business relationship is lower. The risk assessment conducted will also assist the II to differentiate between the risks of individual customers and business relationships, as well as apply appropriate and proportionate CDD and risk mitigating measures[10].
	2.13	Based on a holistic view of the information obtained in the context of the application of CDD measures, an II should be able to finalise

[8] Examples include acquisition of new customer segments, or the launch of new products, services and delivery/distribution channels by the II.

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

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

		the customer risk assessment[11], which determines the level and type of ongoing monitoring (including ongoing CDD and transaction monitoring), and support the II's decision whether to enter into the business relationship. As the customer risk profile will change over time, an II should review and update the risk assessment of a customer from time to time, particularly during ongoing monitoring.
	2.14	Similar to other parts of the AML/CFT Systems, an II should adopt an RBA in the design and implementation of its customer risk assessment framework, and the complexity of the framework should be commensurate with the nature and size of the II's business, and should be designed based on the results of II's institutional ML/TF risk assessment. In general, the customer risk assessment framework will include customer risk factors; country risk factors; product/service/transaction risk factors and delivery/distribution channel risk factors[12].
s.20(1)(b)(ii), Sch. 2	2.15	An II should keep records and relevant documents of its customer risk assessments so that it can demonstrate to the IA, among others: (a) how it assesses the customer's ML/TF risks; and (b) the extent of CDD measures and ongoing monitoring is appropriate based on that customer's ML/TF risks.

[11] This is sometimes also called a "customer risk profile".
[12] Further guidance can be found in Chapter 4.

Chapter 3 – AML/CFT SYSTEMS		
AML/CFT Systems		
s.23, Sch. 2	3.1	An II should take all reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML/TF and to prevent a contravention of any requirement under Part 2 or 3 of Schedule 2. To ensure compliance with this requirement, the II should implement appropriate AML/CFT Systems following the RBA as stated in paragraph 2.1.
s.23(b), Sch. 2	3.2	An II should: (a) have AML/CFT Systems, which are approved by senior management, to enable the II to effectively manage and mitigate the risks that are relevant to the II; (b) monitor the implementation of those AML/CFT Systems referred to in (a), and to enhance them if necessary; and (c) take enhanced measures to manage and mitigate the risks where higher risks are identified.
	3.3	The nature, scale and complexity of AML/CFT Systems may be simplified provided that: (a) an II complies with the statutory requirements set out in the Schedule 2 to the AMLO and the requirements set out in paragraphs 2.2, 2.3 and 3.2; (b) the lower ML/TF risks which form the basis for doing so have been identified through an appropriate risk assessment (e.g. institutional ML/TF risk assessment); and (c) simplified AML/CFT Systems, which are approved by senior management, are subject to review from time to time. However, AML/CFT Systems are not permitted to be simplified whenever there is a suspicion of ML/TF.
	3.4	An II should implement AML/CFT Systems having regard to the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses, and which should include: (a) compliance management arrangements; (b) an independent audit function; (c) employee screening procedures; and (d) an ongoing employee training programme (see Chapter 9).
Compliance management arrangements		
	3.5	An II should have appropriate compliance management arrangements that facilitate the II 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 II's senior management, and appointment of a Compliance Officer (CO) and a Money Laundering Reporting Officer (MLRO) [13].
Senior management oversight		
	3.6	Effective ML/TF risk management requires adequate governance arrangements. The senior management of an II should have a clear understanding of its ML/TF risks and ensure that the risks are adequately managed. Management information regarding ML/TF risks and the AML/CFT Systems should be communicated to them in a timely, complete, understandable and accurate manner so that they are equipped to make informed decisions.
	3.7	The senior management of an II is responsible for implementing effective AML/CFT Systems that can adequately manage the ML/TF risks identified. In particular, the senior management should appoint a CO at the management level to have the overall responsibility for the establishment and maintenance of the II's AML/CFT Systems; and a senior staff as the MLRO to act as the central reference point for suspicious transaction reporting.
	3.8	In order that the CO and MLRO can discharge their responsibilities effectively, senior management should, as far as practicable, ensure that the CO and MLRO are: (a) appropriately qualified with sufficient AML/CFT knowledge; (b) subject to constraint of size of the II, independent of all operational and business functions; (c) normally based in Hong Kong; (d) of a sufficient level of seniority and authority within the II; (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 II's statutory and regulatory requirements and the ML/TF risks arising from the II's business; (g) capable of accessing, on a timely basis, all available information (both from internal sources such as CDD records and external sources such as circulars from the IA); 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).

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

Compliance officer and money laundering reporting officer		
	3.9	The principal function of the CO is to act as the focal point within an II 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 II's AML/CFT Systems, including any group-wide AML/CFT Systems in the case of a Hong Kong-incorporated II, to ensure they remain up-to-date, meet current statutory and regulatory requirements, and are effective in managing ML/TF risks arising from the II's business; (b) overseeing all aspects of the II's AML/CFT Systems which include monitoring effectiveness and enhancing the controls and procedures where necessary; (c) communicating key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies; and (d) ensuring AML/CFT staff training is adequate, appropriate and effective.
	3.10	An II should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the Joint Financial Intelligence Unit (JFIU) and law enforcement agencies. The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions of the MLRO should include having oversight of: (a) review of internal disclosures and exception reports and, in light of all available relevant information, determining whether or not it is necessary to make a report to the JFIU; (b) maintenance of all records related to such internal reviews; and (c) provision of guidance on how to avoid tipping off.
Independent audit function		
	3.11	An II should establish an independent audit function which should have a direct line of communication to the senior management of the II. The function should have sufficient expertise and resources to enable it to carry out its responsibilities, including independent reviews of the II's AML/CFT Systems.

	3.12	The audit function should regularly review the AML/CFT Systems to ensure effectiveness. The review should include, but not be limited to: (a) adequacy of the II's AML/CFT Systems, ML/TF risk assessment framework and application of RBA; (b) effectiveness of suspicious transaction reporting systems; (c) effectiveness of the compliance function; and (d) level of awareness of staff having AML/CFT responsibilities.
	3.13	The frequency and extent of the review should be commensurate with the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses. Where appropriate, the II should also seek a review from external parties.
Employee screening		
	3.14	An II should have adequate and appropriate screening procedures in order to ensure high standards when hiring employees.
Group-wide AML/CFT Systems		
	3.15	Subject to paragraphs 3.18 and 3.19, a Hong Kong-incorporated II with overseas branches or subsidiary undertakings that carry on the same business as a financial institution (FI) as defined in the AMLO should implement group-wide AML/CFT Systems to apply the requirements set out in this Guideline[14] to all of its overseas branches and subsidiary undertakings in its financial group, wherever the requirements in this Guideline are relevant and applicable to the overseas branches and subsidiary undertakings concerned.
s.22(1), Sch. 2	3.16	In particular, a Hong Kong-incorporated II 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.

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

	3.17	To the extent permitted by the laws and regulations of the jurisdictions involved and subject to adequate safeguards on the protection of confidentiality and use of information being shared, including safeguards to prevent tipping off, a Hong Kong-incorporated II 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 II'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[15].
	3.18	If the AML/CFT requirements in the jurisdiction where the overseas branch or subsidiary undertaking of a Hong Kong-incorporated II is located (host jurisdiction) differ from those relevant requirements referred to in paragraph 3.15, the II should require that branch or subsidiary undertaking to apply the higher of the two sets of requirements, to the extent that host jurisdiction's laws and regulations permit.
s.22(2), Sch. 2	3.19	If the host jurisdiction's laws and regulations do not permit the branch or subsidiary undertaking of a Hong Kong-incorporated II to apply the higher AML/CFT requirements, particularly the CDD and record-keeping requirements imposed under Parts 2 and 3 of Schedule 2, the II should: (a) inform the IA of such failure; and (b) take additional measures to effectively mitigate ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the requirements.

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

Chapter 4 – CUSTOMER DUE DILIGENCE		
4.1 What CDD measures are		
s.19(3), Sch. 2	4.1.1	The AMLO defines what CDD measures are (see paragraph 4.1.3) and also prescribes the circumstances in which an II should carry out CDD (see paragraph 4.2). This Chapter provides guidance in this regard. Wherever possible, this Guideline gives IIs a degree of discretion in how they comply with the AMLO and put in place procedures for this purpose. In addition, an II should, in respect of each kind of customer, business relationship, product and transaction, establish and maintain effective AML/CFT Systems for complying with the CDD requirements set out in this Chapter.
	4.1.2	An II should apply an RBA when conducting CDD measures and the extent of CDD measures should be commensurate with the ML/TF risks associated with a business relationship. Where the ML/TF risks are high, the II should conduct enhanced due diligence (EDD) measures (see paragraph 4.11). In low risk situations, the II may apply simplified due diligence (SDD) measures (see paragraph 4.10).
s.2(1), Sch. 2	4.1.3	The following are CDD measures applicable to an II: (a) identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source (see paragraph 4.3); (b) where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity so that the II is satisfied that it knows who the beneficial owner is, including, in the case of a legal person or trust[16], measures to enable the II to understand the ownership and control structure of the legal person or trust (see paragraph 4.4); (c) obtain information on the purpose and intended nature of the business relationship (if any) established with the II unless the purpose and intended nature are obvious (see paragraph 4.8); and (d) if a person purports to act on behalf of the customer: (i) identify the person and take reasonable measures to verify the person's identity using documents, data or information provided by a reliable and independent source; and (ii) verify the person's authority to act on behalf of the customer (see paragraph 4.5).

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

	4.1.4	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. For the insurance industry, the term "customer" refers to policy holder.
4.2 When CDD measures should be carried out		
s.3(1) & (1A), Sch. 2	4.2.1	An FI should 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[17]: (i) involving an amount equal to or above $120,000 or an equivalent amount in any other currency; (ii) that is a wire transfer involving an amount equal to or above $8,000 or an equivalent amount in any other currency; or (iii) that is a virtual asset transfer[18] 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; (c) when the FI suspects that the customer or the customer's account is involved in ML/TF[19]; 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	4.2.2	"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	4.2.3	"Occasional transaction" is defined in the AMLO as a transaction between an FI and a customer who does not have a business relationship with the FI.[20]
	4.2.4	An FI should be vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD thresholds of $8,000 (for wire transfers or virtual asset transfers) and $120,000

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

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

[19] This criterion applies irrespective of the $120,000 or $8,000 threshold applicable to occasional transactions set out in paragraph 4.2.1(b).

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

		(for other types of transactions). Where the FI becomes aware that these thresholds are met or exceeded, CDD measures should be carried out.
	4.2.5	The factors linking occasional transactions are inherent in the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over a short period, where a customer regularly transfers funds to one or more destinations. In determining whether the transactions are in fact linked, an FI should consider these factors against the timeframe within which the transactions are conducted.
4.3 Identification and verification of the customer's identity		
s.2(1)(a), Sch. 2	4.3.1	An II should identify the customer and verify the customer's identity by reference to documents, data or information provided by: (a) a governmental body; (b) the IA or any other relevant authority (RA); (c) an authority in a place outside Hong Kong that performs functions similar to those of the IA or any other RA; (d) a digital identification system that is a reliable and independent source that is recognized by the IA[21]; or (e) any other reliable and independent source that is recognized by the IA.
Customer that is a natural person[22]		
s.2(1)(a), Sch. 2	4.3.2	For a customer that is a natural person, an II should identify the customer by obtaining at least the following identification information: (a) full name; (b) date of birth; (c) nationality; and (d) unique identification number (e.g. identity card number or passport number) and document type.
s.2(1)(a), Sch. 2	4.3.3	In verifying the identity of a customer that is a natural person, an II should verify the name, date of birth, unique identification number and document type of the customer by reference to documents, data or information provided by a reliable and independent source, examples of which include: (a) Hong Kong identity card or other national identity card;

[21] The IA recognizes 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 IA may in future recognize other similar digital identification systems developed and operated by governments in other jurisdictions having regard to market developments and specific circumstances.

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

		(b) valid travel document[23] (e.g. unexpired passport); or (c) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).
	4.3.4	The identification document obtained by an II should contain a photograph of the customer.
	4.3.5	An II should obtain the residential address information of a customer that is a natural person[24].
Customer that is a legal person[25]		
s.2(1)(a), Sch. 2	4.3.6	For a customer that is a legal person, an II should identify the customer by obtaining at least the following identification information: (a) full name; (b) date of incorporation, establishment or registration; (c) place of incorporation, establishment or registration (including address of registered office); (d) unique identification number (e.g. incorporation number or business registration number) and document type; and (e) principal place of business (if different from the address of registered office).
s.2(1)(a), Sch. 2	4.3.7	In verifying the identity of a customer that is a legal person, an II should normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the legal person by reference to documents, data or information provided by a reliable and independent source, examples of which include[26]: (a) certificate of incorporation; (b) record in an independent company registry;

[23] The following documents also constitute travel documents for the purpose of identity verification:
(a) Permanent Resident Identity Card of Macau Special Administrative Region;
(b) Mainland Travel Permit for Taiwan Residents;
(c) Seaman's Identity Document (issued under and in accordance with the International Labour Organization Convention/Seafarers' Identity Documents Convention, 1958);
(d) Taiwan Travel Permit for Mainland Residents;
(e) Permit for residents of Macau issued by Director of Immigration;
(f) Exit-entry Permit for Travelling to and from Hong Kong and Macau for Official Purposes; and
(g) Exit-entry Permit for Travelling to and from Hong Kong and Macau.

[24] For the avoidance of doubt, an II may, under certain circumstances, require verification (on top of collection) of residential address from a customer for other purposes (e.g. group requirements, other local or overseas legal and regulatory requirements). In such circumstances, the II should communicate clearly to the customer the reasons of requiring verification of address.

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

[26] In some instances, an II 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) constitutional document; or (h) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).
	4.3.8	For a customer that is a partnership or an unincorporated body, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to verify the identity of the customer as required in paragraph 4.3.7 provided that: (a) the customer is a well-known, reputable organization; (b) the customer has a long history in its industry; and (c) there is substantial public information about the customer, its partners and controllers.
	4.3.9	In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, an II should satisfy itself as to the legitimate purpose of the organization, e.g. by requesting sight of the constitution.
Customer that is a trust or other similar legal arrangement[27]		
s.2(1)(a), Sch. 2	4.3.10	In respect of trusts, an II should identify and verify the trust as a customer in accordance with the requirements set out in paragraphs 4.3.11 and 4.3.12. The II should also regard the trustee[28] as its customer if the trustee enters into a business relationship or carries out occasional transactions on behalf of the trust, which is generally the case if the trust does not possess a separate legal personality. In such a case, the II should identify and verify the identity of the trustee in line with the identification and verification requirements for a customer that is a natural person or a legal person, where applicable.
s.2(1)(a), Sch. 2	4.3.11	For a customer that is a trust or other similar legal arrangement, an II should identify the customer by obtaining at least the following identification information: (a) name of the trust or legal arrangement; (b) date of establishment or settlement;

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

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

		(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 organization number); and (e) address of registered office (if applicable).
s.2(1)(a), Sch. 2	4.3.12	In verifying the identity of a customer that is a trust or other similar legal arrangement, an II should normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the trust or other similar legal arrangement by reference to documents, data or information provided by a reliable and independent source, examples of which include: (a) trust deed or similar instrument[29]; (b) record of an appropriate register[30] in the relevant country of establishment; (c) written confirmation from a trustee acting in a professional capacity[31]; (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 II, if the trust concerned is managed by that trust company.
<u>Reliability of documents, data or information</u>		
	4.3.13	In verifying the identity of a customer, an II needs not establish accuracy of every piece of identification information collected in paragraphs 4.3.2, 4.3.6 and 4.3.11.
	4.3.14	An II should ensure that documents, data or information obtained for the purpose of verifying the identity of a customer as required in paragraphs 4.3.3, 4.3.7 and 4.3.12 is current at the time they are provided to or obtained by the II.
	4.3.15	When using documents for verification, an II should be aware that some types of documents are more easily forged than others, or can be reported as lost or stolen. Therefore, the II should consider applying anti-fraud procedures that are commensurate with the risk profile of the person being verified.

[29] Under exceptional circumstance, the II may choose to retain a redacted copy.

[30] In determining whether a register is appropriate, the II 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.

[31] "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).

	4.3.16	If a natural person customer or a person representing a legal person, a trust or other similar legal arrangement to establish a business relationship with an II is physically present during the CDD process, the II 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 II should take appropriate measures to ensure the reliability of identification documents obtained.[32]
	4.3.17	Where the documents, data or information being used for the purposes of identification are in a foreign language, appropriate steps should be taken by the II to be reasonably satisfied that the documents, data or information in fact provide evidence of the customer's identity.
Connected parties		
	4.3.18	Where a customer is a legal person, a trust or other similar legal arrangement, an II should identify all the connected parties[33] of the customer by obtaining their names.
	4.3.19	A connected party of a customer that is a legal person, a trust or other similar legal arrangement: (a) in relation to a corporation, means a director of the customer; (b) in relation to a partnership, means a partner of the customer; (c) in relation to a trust or other similar legal arrangement, means a trustee (or equivalent) of the customer; and (d) in other cases not falling within subsection (a), (b) or (c), means a natural person holding a senior management position or having executive authority in the customer.
4.4 Identification and verification of a beneficial owner		
s.2(1)(b), Sch. 2	4.4.1	A beneficial owner is normally a natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. An II should identify any beneficial owner in relation to a customer, and take reasonable measures to verify the beneficial owner's identity so that the II is satisfied that it knows who the beneficial owner is.
	4.4.2	While an II usually can identify who the beneficial owner of a

[32] An example is electronic company incorporation (e-Registry) of Companies Registry in Hong Kong, and the original Certificate of Incorporation will only be issued in electronic form. When obtaining a print copy of that Certificate of Incorporation, an II should take appropriate measures such as corroborating with other identification document or information from the Companies Registry record to ensure the reliability of that print copy obtained.

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

		customer is in the course of understanding the ownership and control structure of the customer, the II may obtain an undertaking or declaration[34] from the customer on the identity of, and the information relating to, its beneficial owner. When identifying a beneficial owner, the II should endeavour to obtain the same identification information as set out in paragraph 4.3.2 as far as possible.
	4.4.3	The verification requirements for a customer and a beneficial owner are different under the AMLO. In determining what constitutes reasonable measures to verify the identity of a beneficial owner of a customer, an II should consider and give due regard to the ML/TF risks posed by the customer and the business relationship. It is therefore for the II to consider whether it is appropriate to, for example, (i) make use of the records of a beneficial owner available in the public domain[35]; (ii) request its customer to provide documents or information in relation to the beneficial owner's identity that is obtained from a reliable and independent source; or (iii) where an undertaking or declaration is obtained from the customer (see paragraph 4.4.2), corroborate the customer's undertaking or declaration with publicly available information.
	4.4.4	If the ownership structure of a customer involves different types of legal persons or legal arrangements[36], in determining who the beneficial owner is, an II should identify 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>		
	4.4.5	In respect of a customer that is a natural person, the customer is the beneficial owner, unless the characteristics of the transactions or other circumstances indicate otherwise. Therefore, there is no requirement on an II to make proactive searches for beneficial owners of the customer in such a case, but the II should make appropriate enquiries where there are indications that the customer is not acting on his own behalf.
<u>Beneficial owner in relation to a legal person</u>		
s.1, Sch. 2	4.4.6	The AMLO defines beneficial owner in relation to a corporation as: (a) an individual who (i) owns or controls, directly or indirectly, including through

[34] For example, an II may obtain from a corporate customer its register of beneficial owners (e.g the significant controller register maintained in accordance with the Companies Ordinance of Hong Kong).

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

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

		a trust or bearer share holding, more than 25% of the issued share capital of the corporation; (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or (iii) exercises ultimate control over the management of the corporation; or (b) if the corporation is acting on behalf of another person, means the other person.
s.1, Sch. 2	4.4.7	The AMLO defines beneficial owner, in relation to a partnership as: (a) an individual who (i) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership; (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or (iii) exercises ultimate control over the management of the partnership; or (b) if the partnership is acting on behalf of another person, means the other person.
s.1, Sch. 2	4.4.8	In relation to an unincorporated body other than a partnership, beneficial owner: (a) means an individual who ultimately owns or controls the unincorporated body; or (b) if the unincorporated body is acting on behalf of another person, means the other person.
s.2(1)(b), Sch. 2	4.4.9	For a customer that is a legal person, an II should identify any natural person who ultimately has a controlling ownership interest (i.e. more than 25%) in the legal person and any natural person exercising control of the legal person or its management, and take reasonable measures to verify their identities. If there is no such natural person (i.e. no natural person falls within the definition of beneficial owners set out in paragraphs 4.4.6 to 4.4.8), the II should identify the relevant natural persons who hold the position of senior managing official, 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	4.4.10	The AMLO defines the beneficial owner, in relation to a trust as: (a) a beneficiary or a class of beneficiaries of the trust entitled to a vested interest in the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not;

		(b) the settlor of the trust; (c) the trustee of the trust; (d) a protector or enforcer of the trust; or (e) an individual who has ultimate control over the trust.
s.2(1)(b), Sch. 2	4.4.11	For a customer that is a trust, an II should identify the settlor, the trustee, the protector (if any), the enforcer (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate control over the trust (including through a chain of control or ownership), and take reasonable measures to verify their identities. For a customer that is other similar legal arrangement, an II should identify any natural person in equivalent or similar positions to a beneficial owner of a trust as stated above and take reasonable measures to verify the identity of such person.
	4.4.12	For a beneficiary of a trust designated by characteristics or by class, an II should obtain sufficient information [37] concerning the beneficiary to satisfy the II that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights.
Ownership and control structure		
s.2(1)(b), Sch. 2	4.4.13	Where a customer is not a natural person, an II should understand its ownership and control structure, including identification of any intermediate layers (e.g. by reviewing an ownership chart of the customer). The objective is to follow the chain of ownerships to the beneficial owners of the customer.
	4.4.14	Where a customer has a complex ownership or control structure, an II should obtain sufficient information for the II to satisfy itself that there is a legitimate reason behind the particular structure employed.
Bearer shares[38]		
	4.4.15	Bearer shares refer to negotiable instruments that accord ownership in a legal person to the person who possesses the physical bearer share certificate, and any other similar instruments without traceability. Therefore it is more difficult to establish the beneficial ownership of a company with bearer shares. An II should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the II is notified whenever there is a change of beneficial owner of such shares.

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

[38] For the avoidance of doubt, paragraph 4.4.15 to 4.4.17 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 warrant" respectively.

	4.4.16	Where bearer shares have been deposited with an authorized/registered custodian, an II should seek independent evidence of this, for example confirmation from the registered agent that an authorized/registered custodian holds the bearer shares, together with the identities of the authorized/registered custodian and the person who has the right to those entitlements carried by the share. As part of the II's ongoing periodic review, it should obtain evidence to confirm the authorized/registered custodian of the bearer shares.
	4.4.17	Where the shares are not deposited with an authorized/registered custodian, an II should obtain declarations before establishing a business relationship and annually thereafter from each beneficial owner of such shares. The II should also require the customer to notify it immediately of any changes in the ownership of the shares.
Nominee shareholders		
	4.4.18	For a customer identified to have nominee shareholders in its ownership structure, an II should obtain satisfactory evidence of the identities of the nominees, and the persons on whose behalf they are acting, as well as the details of arrangements in place, in order to determine who the beneficial owner is.
4.5 Identification and verification of a person purporting to act on behalf of the customer		
	4.5.1	A person may be appointed to act on behalf of a customer to establish business relationships, or may be authorized to give instructions to an II to conduct various activities through the account or the business relationship established. Whether the person is considered to be a person purporting to act on behalf of the customer (PPTA) should be determined based on the nature of that person's roles and the activities which the person is authorized to conduct, as well as the ML/TF risks associated with these roles and activities. An II should implement clear policies and procedures for determining who is considered to be a PPTA.
s.2(1)(d), Sch. 2	4.5.2	If a person is a PPTA, an II should: (a) identify the person and take reasonable measures to verify the person's identity on the basis of documents, data or information provided by- (i) a governmental body; (ii) the IA or any other RA; (iii) an authority in a place outside Hong Kong that performs functions similar to those of the IA or any other RA; or (iv) any other reliable and independent source that is recognized by the IA; and (b) verify the person's authority to act on behalf of the customer.

s.2(1)(d)(i), Sch. 2	4.5.3	An II should identify and verify the identity of the PPTA in line with the identification and verification requirements for a customer that is a natural person or a legal person, where applicable.
s.2(1)(d)(ii), Sch. 2	4.5.4	An II should verify the authority of each PPTA by appropriate documentary evidence (e.g. board resolution or similar written authorization).
4.6 Identification and verification of a beneficiary		
s.11(1), Sch. 2	4.6.1	An II should, whenever a beneficiary or a new beneficiary is identified or designated by the policy holder of an insurance policy: (a) if the beneficiary is identified by name, record the name of the beneficiary; (b) if the beneficiary is designated by description (e.g. by characteristics or by class) or other means (e.g. under a will), obtain sufficient information about the beneficiary to satisfy itself that it will be able to establish the identity of the beneficiary: (i) at the time the beneficiary exercises a right vested in the beneficiary under the insurance policy; or (ii) at the time of payout or, if there is more than one payout, the time of the first payout to the beneficiary in accordance with the terms of the insurance policy, whichever is the earlier.
s.11(2), Sch. 2	4.6.2	An II should carry out the measures specified in paragraphs 4.6.3, 4.6.4 and 4.6.7: (a) at the time a beneficiary exercises a right vested in the beneficiary under an insurance policy; or (b) at the time of payout or, if there is more than one payout, the time of the first payout to a beneficiary in accordance with the terms of an insurance policy, whichever is the earlier.
s.11(3)(a), Sch. 2	4.6.3	An II should verify the beneficiary's identity by reference to documents, data or information provided by a reliable and independent source: (a) a governmental body; (b) the IA or any other RA; (c) an authority in a place outside Hong Kong that performs functions similar to those of the IA or any other RA; or (d) any other reliable and independent source that is recognized by the IA.
s.11(3)(b), Sch. 2	4.6.4	Where the beneficiary is a legal person or trust or other similar legal arrangement, an II should:

		(a) identify its beneficial owners; and (b) if there is a high risk of ML or TF having regard to the particular circumstances of the beneficial owners, take reasonable measures to verify the beneficial owners' identities so that the II knows who the beneficial owners are.
	4.6.5	An II should be required to take reasonable measures to determine whether a beneficiary or a beneficial owner of a beneficiary for an insurance policy is a politically exposed person (PEP) as described in paragraphs 4.11.7, 4.11.13, 4.11.15 and 4.11.16. This should occur, at the latest, at the time of the payout. Where higher risks[39] are identified, an II should be required to:- (a) inform senior management before the payout of the policy proceeds; (b) conduct enhanced scrutiny on the whole business relationship with the policy holder; and (c) consider making a suspicious transaction report.
	4.6.6	Where an II is unable to comply with paragraphs 4.6.1 to 4.6.4 above, it should consider making a suspicious transaction report.
	4.6.7	An II should obtain the residential address information of a beneficiary that is a natural person.
	4.6.8	An II should include the beneficiary as a relevant risk factor in determining whether enhanced due diligence measures are applicable[40].
	4.6.9	If payments made under the terms of the policy are to be paid to persons or companies other than the customers or beneficiaries, then the proposed recipients of these moneys should also be the subjects of identification and verification. An II should carry out the same measures of identification and verification of the beneficiaries as set out in paragraphs 4.6.1 to 4.6.8 on the proposed recipients.
4.7 Requirements for reinsurance		
	4.7.1	Reinsurers are subject to the CDD and record-keeping requirements set out in Schedule 2. The customers in relation to whom the reinsurers should carry out the CDD measures are the ceding insurers.

[39] If the identified PEP is a former non-Hong Kong/Hong Kong/international organization PEP, an II should take into account the risk factors specified in paragraphs 4.11.14 and 4.11.20 in determining the risk.

[40] Examples of what might constitute suspicious transactions in relation to beneficiary are provided in Annex I – Indicators of suspicious transactions.

4.8 Purpose and intended nature of business relationship		
s.2(1)(c), Sch. 2	4.8.1	An II should understand the purpose and intended nature of the business relationship. In some instances, this will be self-evident, but in many cases, the II may have to obtain information in this regard. The information obtained by the II to understand the purpose and intended nature should be commensurate with the risk profile of the customer and the nature of the business relationship. In addition, where a customer is not a natural person, an II should also understand the nature of the customer's business.
4.9 Timing of verification		
s.3(2) & (3), Sch. 2	4.9.1	An II should verify the identity of a customer and any beneficial owner of the customer before or during the course of establishing a business relationship or conducting transactions for occasional customers. However, an II may, exceptionally, verify the identity of a customer and any beneficial owner of the customer after establishing the business relationship, provided that: (a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed; (b) it is necessary not to interrupt the normal conduct of business with the customer; and (c) verification is completed as soon as reasonably practicable.
	4.9.2	Examples of situations where it may be necessary not to interrupt the normal conduct of business include: (a) securities transactions – in the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed; and (b) life insurance business – in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policy holder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.
	4.9.3	Having considered the difficulty for an II to obtain copies of the identification documents of individual customers when the sales process occurs outside the office, it may obtain and keep copies of the identification documents after having established the business relationship provided that the ML/TF risks are effectively managed. In all such circumstances, copies of identification documents of individual customers should be obtained and copied

		for retention in the reasonable timeframe or at or before the time of payout, whichever is the earlier.
	4.9.4	If an II allows verification of the identity of a customer and any beneficial owner of the customer after establishing the business relationship, it should adopt appropriate risk management policies and procedures concerning the conditions under which the customer may utilise the business relationship prior to verification. These policies and procedures should include: (a) establishing a reasonable timeframe for the completion of the identity verification measures and the follow-up actions if exceeding the timeframe (e.g. to suspend or terminate the business relationship concerned); (b) placing appropriate limits on the number, types and/or amount of transactions that can be performed; (c) monitoring of large and complex transactions being carried out outside the expected norms for that type of relationship; (d) keeping senior management periodically informed of any pending completion cases; and (e) ensuring that funds are not paid out to any third party. Exceptions may be made to allow payments to third parties subject to the following conditions: (i) there is no suspicion of ML/TF; (ii) the risk of ML/TF is assessed to be low; (iii) the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction; and (iv) the names of recipients do not match with watch lists such as those for terrorist suspects and PEPs.
s.3(3) & (4)(b), Sch. 2	4.9.5	Verification of identity should be completed by an II within a reasonable timeframe, which generally refers to the following: (a) the II completing such verification no later than 30 working days after the establishment of business relationship; (b) the II 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 II 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	4.9.6	If verification cannot be completed within the reasonable timeframe set in the II's risk management policies and procedures, the II 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 II 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.
4.10 Simplified due diligence (SDD)		
General		
	4.10.1	In general, an II should carry out all four CDD measures set out in paragraph 4.1.3 before establishing any business relationship, before carrying out a specified occasional transaction, and continuously monitor its business relationship (i.e. ongoing CDD and transaction monitoring). As stated in Chapter 2, the extent of four CDD measures and ongoing monitoring should be determined using an RBA.
	4.10.2	An II may apply SDD measures in relation to a business relationship or transaction if it determines that, taking into account its risk assessment, the business relationship or transaction presents a low ML/TF risk.
	4.10.3	SDD measures should not be applied or continue to be applied, where: (a) the II's risk assessment changes and it no longer considers that there is a low degree of ML/TF risk; (b) where the II suspects ML or TF; or (c) where there are doubts about the veracity or accuracy of documents or information previously obtained for the purposes of identification or verification.
	4.10.4	The assessment of low risks should be supported by an adequate analysis of ML/TF risks by the II.
	4.10.5	The SDD measures applied should be commensurate with the nature and level of ML/TF risk, based on the lower ML/TF risk factors identified by the II.
s.5(1), Sch. 2	4.10.6	When an II applies SDD measures, it is still required to continuously monitor its business relationship (i.e. ongoing CDD and transaction monitoring) in accordance with section 5 of Schedule 2 and Chapter 5.
	4.10.7	Examples of potentially lower risk factors[41] include: (a) customer risk factors:

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

		(i) a government entity or a public body[42] in Hong Kong or in an equivalent jurisdiction; (ii) a corporation listed on a stock exchange and subject to disclosure requirements (e.g. either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership; (iii) an FI as defined in the AMLO, or other FI incorporated or established in an equivalent jurisdiction and is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; or (iv) a collective investment scheme authorized for offering to the public in Hong Kong or in an equivalent jurisdiction. (b) product/service/transaction or delivery/distribution channel risk factors: (i) a provident, pension, retirement or superannuation scheme (however described) that provides retirement benefits to employees, where contributions to the scheme are made by way of deduction from income from employment and the scheme rules do not permit the assignment of a member's interest under the scheme; (ii) an insurance policy for the purposes of a provident, pension, retirement or superannuation scheme (however described) that does not contain a surrender clause and cannot be used as a collateral; or (iii) a life insurance policy in respect of which: (A) an annual premium of no more than $8,000 or an equivalent amount in any other currency is payable; or (B) a single premium of no more than $20,000 or an equivalent amount in any other currency is payable. (c) country risk factors: (i) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems; or (ii) countries or jurisdictions identified by credible sources as having a lower level of corruption or other criminal activity.
	4.10.8	Examples of possible SDD measures include: (a) accepting other documents, data or information (e.g. proof of

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

		FI's licence, listed status or authorization status etc.), other than examples provided in paragraphs 4.3.7 and 4.3.12, for a customer falling within any category specified in paragraph 4.10.7(a); (b) adopting simplified customer due diligence in relation to beneficial owners as specified in paragraphs 4.10.9 to 4.10.20; (c) reducing the frequency of updates of customer identification information; (d) reducing the degree of ongoing monitoring and scrutiny of transactions based on a reasonable monetary threshold; or (e) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and intended nature from the type of transactions or business relationship established.
Simplified customer due diligence in relation to beneficial owners		
General		
s.4, Sch. 2	4.10.9	An II may choose not to identify and take reasonable measures to verify the beneficial owner in relation to: (a) a customer that is listed in paragraph 4.10.10; (b) a transaction conducted to a customer relates to a product listed in paragraph 4.10.17; or (c) a customer who is a solicitor or a firm of solicitors, and meeting the criteria set out in paragraph 4.10.19.
Specific customers		
s.4(3), Sch. 2	4.10.10	An II may choose not to identify and take reasonable measures to verify the beneficial owner of a customer, if the customer is – (a) an FI as defined in the AMLO; (b) an institution that- (i) is incorporated or established in an equivalent jurisdiction; (ii) carries on a business similar to that carried on by an FI as defined in the AMLO; (iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and (iv) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs; (c) a corporation listed on any stock exchange; (d) an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is- (i) an FI as defined in the AMLO; (ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that-

		(A) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and (B) is supervised for compliance with those requirements; (e) the Government or any public body in Hong Kong; or (f) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.
s.4(2), Sch. 2	4.10.11	If a customer not falling within paragraph 4.10.10 has in its ownership chain an entity that falls within that paragraph, the II is not required to identify or verify the beneficial owners of that entity in that chain when establishing a business relationship with or carrying out an occasional transaction for the customer. However, the II should still identify and take reasonable measures to verify the identity of beneficial owners in the ownership chain that are not connected with that entity.
s.4(3)(c), Sch. 2	4.10.12	Where a customer is a corporation listed on any stock exchange, an II may choose not to identify and take reasonable measures to verify its beneficial owners. For this purpose, the II should assess whether the customer is subject to any disclosure requirements (either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership of the customer.
s.4(3)(a) & (b), Sch. 2	4.10.13	An II may choose not to identify and take reasonable measures to verify the beneficial owner of a customer, if a customer is an FI as defined in the AMLO that opens an account: (a) in the name of a nominee company for holding fund units on behalf of the FI or its underlying customers; or (b) in the name of an investment vehicle in the capacity of a service provider (such as manager or custodian) to the investment vehicle and the underlying investors have no control over the management of the investment vehicle's assets; provided that the FI: (i) has conducted CDD: (A) in the case where the nominee company holds fund units on behalf of the FI or the FI's underlying customers, on its underlying customers; or (B) in the case where the FI acts in the capacity of a service provider (such as manager or custodian) to the investment vehicle, on the investment vehicle pursuant to the provisions of the AMLO; and

		(ii) is authorized to operate the account as evidenced by contractual document or agreement.
s.4(3)(d), Sch. 2	4.10.14	Where a customer is an investment vehicle[43], an II may choose not to identify and take reasonable measures to verify its beneficial owners (i.e. the investors), provided that the II 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.
	4.10.15	An investment vehicle whether or not responsible for carrying out CDD measures on the underlying investors under governing law of the jurisdiction in which the investment vehicle is established may, where permitted by law, appoint another institution ("appointed institution"), such as a manager, a trustee, an administrator, a transfer agent, a registrar or a custodian, to perform the CDD. Where the person responsible for carrying out the CDD measures (the investment vehicle[44] or the appointed institution) falls within any of the categories of institution set out in section 4(3)(d) of Schedule 2, an II may choose not to identify and take reasonable measures to verify the beneficial owners of the investment vehicle provided that it is satisfied that the investment vehicle has ensured that there are reliable systems and controls in place to conduct the 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.
	4.10.16	If neither the investment vehicle nor appointed institution falls within any of the categories of institution set out in section 4(3)(d) of Schedule 2, an II should identify and take reasonable measures to verify the identity of any investor of the investment vehicle in accordance with the requirements on identification and verification of a beneficial owner of a specific type of customer (see paragraph 4.4). The II 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 II accepts such a

[43] 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.

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

		representation, this should be documented, retained, and subject to periodic review.
Specific products		
s.4(4) & (5), Sch. 2	4.10.17	An II may choose not to identify and take reasonable measures to verify the beneficial owners in relation to a customer if the II 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.
	4.10.18	For the purpose of item (a) of paragraph 4.10.17, an II may generally treat the employer as the customer and may choose not to identify and take reasonable measures to verify the beneficial owners of the scheme (i.e. the employees). Where the II has a separate business relationship with the employees, it should apply CDD measures in accordance with relevant requirements set out in this Chapter.
Solicitors' client accounts		
s.4(6), Sch. 2	4.10.19	If a customer of an II is a solicitor or a firm of solicitors, the II may choose not to identify and take reasonable measures to verify the beneficial owners of the client account opened by the customer, provided that the following criteria are satisfied: (a) the client account is kept in the name of the customer; (b) moneys or securities of the customer's clients in the client account are mingled; and (c) the client account is managed by the customer as those clients' agent.
	4.10.20	When opening a client account for a solicitor or a firm of solicitors, an II should establish the proposed use of the account, i.e. whether to hold co-mingled client funds or the funds of a specific client. If a client account is opened on behalf of a single client or there are sub-accounts for each individual client where funds are not co-

		mingled at the II, the II should establish the identity of the underlying client(s) in addition to that of the solicitor opening the account.
4.11 Enhanced due diligence (EDD)		
Situations presenting a high ML/TF risk		
s.15, Sch. 2	4.11.1	An II should apply EDD measures in relation to a business relationship to mitigate and manage the high ML/TF risks in: (a) a situation that by its nature may present a high ML/TF risk taking into account the potentially higher risk factors set out in paragraph 4.11.5; or (b) a situation specified by the IA in a notice in writing given to the II.
s.15, Sch. 2	4.11.2	The EDD measures applied should be commensurate with the nature and level of ML/TF risks, based on the higher ML/TF risk factors identified by the II. The extent of EDD measures should be proportionate, appropriate and discriminating, and be able to be justified to the IA.
s.15, Sch. 2	4.11.3	An II should obtain approval from its senior management to establish a business relationship that presents a high ML/TF risk, or continue an existing business relationship where the relationship subsequently presents a high ML/TF risk.
s.5(3)(c), Sch. 2	4.11.4	An II should conduct enhanced ongoing monitoring of a business relationship that presents a high ML/TF risk, for example, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination. Reference should be made to Chapter 5.
	4.11.5	In addition to those examples of attributes under paragraph 1.14, further examples of potentially higher risk factors[45] include: (a) customer risk factor: (i) business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic difference between the II and the customer); (ii) legal persons or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose; (iii) companies that have nominee shareholders, nominee directors, bearer shares or bearer share warrants; (iv) cash intensive business; or (v) the ownership structure of the legal person or legal arrangement appears unusual or excessively complex

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

		given the nature of the legal person's or legal arrangement's business; (b) product/service/transaction or delivery/distribution channel risk factors: (i) anonymous transactions (which may involve cash); or (ii) frequent payments received from unknown or un-associated third parties; (c) country risk factors: (i) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems; (ii) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity; (iii) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or (iv) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operation.
	4.11.6	Examples of possible EDD measures[46] include: (a) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner; (b) obtaining additional information on the intended nature of the business relationship; (c) obtaining information on the source of wealth of the customer (see paragraph 4.11.26); (d) obtaining information on the source of funds of the customer (see paragraph 4.11.27); (e) obtaining information on the reasons for intended or performed transactions; or (f) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.
<u>Politically exposed persons (PEPs)</u>		
Non-Hong Kong PEPs		
Definition		
s.1, Sch. 2	4.11.7	A non-Hong Kong PEP is defined as:

[46] For the avoidance of doubt, there is no expectation for an II to conduct all the examples of possible EDD measures for each business relationship that presents a high ML/TF risk. IIs are reminded of the requirements set out in paragraph 4.11.2.

		(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 and EDD measures for non-Hong Kong PEPs		
s.19(1), Sch. 2	4.11.9	An II should establish and maintain effective procedures (e.g. by making reference to publicly available information and/or screening against commercially available databases) for determining whether a customer or a beneficial owner of a customer is a non-Hong Kong PEP.
	4.11.10	An II may use publicly available information or refer to relevant reports and databases on corruption risk published by specialized national, international, non-governmental and commercial organizations 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). An II should be vigilant where either the country to which the customer has business connections or the business/industrial sector is more vulnerable to corruption.
s.10(1) & (2), Sch. 2	4.11.11	When an II knows that a customer or a 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 EDD measures[47]: (a) obtaining approval from its senior management for establishing or continuing such business relationship; and (b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds.
s.5(3)(b), Sch.2	4.11.12	An II should conduct enhanced ongoing monitoring[48] of a business relationship with a customer if the customer or the beneficial owner of the customer is a non-Hong Kong PEP. Reference should be made to Chapter 5.
Treatment of former non-Hong Kong PEPs		
s.1, Sch. 2	4.11.13	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).
s5(5) & s.10(3), Sch. 2	4.11.14	Following an RBA[49], an II may decide not to apply, or not to continue to apply, the measures set out in paragraphs 4.11.11 and 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 II should conduct an appropriate assessment on 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 PEP; and (c) whether the individual's previous and current functions are linked in any way (e.g. formally by appointment of the PEP's successor, or informally by the fact that the PEP continues to deal with the same substantive matters).
Hong Kong PEPs & international organization PEPs		

[47] See paragraph 4.11.2.
[48] See paragraph 4.11.4.
[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.

Definition		
	4.11.15	A Hong Kong PEP is defined as: (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).
	4.11.16	An international organization PEP is defined as: (a) an individual who is or has been entrusted with a prominent function by an international organization, 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 organization; (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).
	4.11.17	International organizations referred to in paragraph 4.11.16 are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognized 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 organizations include the United Nations and affiliated international organizations such as the International Maritime Organization; regional international organizations 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 organizations such as the North Atlantic Treaty Organization, and economic organizations such as the World Trade Organization or the Association of Southeast Asian Nations, etc.
Identification of and EDD measures for Hong Kong PEPs & international organization PEPs		

	4.11.18	An II should take reasonable measures to determine whether a customer or a beneficial owner of a customer is a Hong Kong PEP or an international organization PEP.
s5(3)(c) & s.15, Sch. 2	4.11.19	An II should apply the measures set out in paragraphs 4.11.11 and 4.11.12 in any of the following situations[50]: (a) before establishing a high risk business relationship[51] with a customer who is or whose beneficial owner is a Hong Kong PEP or an international organization 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 organization PEP where the relationship subsequently becomes high risk; or (c) when continuing an existing high risk business relationship where the II subsequently knows that the customer or the beneficial owner of the customer is a Hong Kong PEP or an international organization PEP.
Treatment of former Hong Kong or international organization PEPs		
	4.11.20	Following an RBA[52], in the situations described in paragraph 4.11.19, an II may decide not to apply, or not to continue to apply, the measures set out in paragraphs 4.11.11 and 4.11.12 to a former Hong Kong or international organization PEP[53] who no longer presents a high risk of ML/TF after stepping down. To determine whether a former Hong Kong or international organization PEP no longer presents a high risk of ML/TF, the II should conduct an appropriate assessment on 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 PEP; and (c) whether the individual's previous and current functions are linked in any way (e.g. formally by appointment of the PEP's successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

[50] For the avoidance of doubt, an II should consider whether the application of measures in paragraphs 4.11.11 and 4.11.12 could mitigate the ML/TF risk arising from the high risk business relationship with a Hong Kong PEP or an international organization PEP. Where applicable, an II should also apply measures to mitigate such risk in accordance with the guidance provided in paragraphs 4.11.1 to 4.11.6.

[51] In determining whether a business relationship presents a high ML/TF risk, an II should take into account all risk factors (including those in paragraph 4.11.5) that are relevant to the business relationship.

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

[53] 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 or international organization PEP.

Further guidance applied to all types of PEPs		
Scope of PEPs		
	4.11.21	An II should implement appropriate risk management systems to identify PEPs.
	4.11.22	The definitions of PEPs set out above provide some non-exhaustive examples of the types of prominent (public) functions that an individual may be or may have been entrusted with by a government, or by an international organization. An II 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, the II 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 organizational framework of the relevant government or international organization; and any other specific concerns connected to the jurisdiction where the public function is/has been entrusted.
	4.11.23	While an II may refer to commercially available databases to identify PEPs, the use of these databases should never replace traditional CDD processes (e.g. understanding the occupation and employer of a customer). When using commercially available databases, the II should be aware of their limitations, for example, the databases are not necessarily comprehensive or reliable as they generally draw solely from information that is publicly available; the definition of PEPs used by the database providers may or may not align with the definition of PEPs applied by the II; and any technical incapability of such databases that may hinder the II's effectiveness of PEP identification. Therefore, the II should only use such databases as a support tool and ensure they are fit for purpose.
	4.11.24	Although the EDD requirements also apply to family members and close associates of the PEP, the risks associated with them may vary depending to some extent on the social-economic and cultural structure of the jurisdiction of the PEP.
EDD measures for PEPs		
	4.11.25	Since not all PEPs pose the same level of ML risks, an II should adopt an RBA in determining the extent of EDD measures in paragraph 4.11.11 and enhanced ongoing monitoring in paragraph 4.11.12 taking into account relevant factors, such as: (a) the nature of the prominent (public) functions that a PEP holds; (b) the geographical risk associated with the jurisdiction where a PEP holds prominent (public) functions; (c) the nature of the business relationship (e.g. the

		delivery/distribution channel used; or the product or service offered); and (d) in relation to a former PEP, the risk factors specified in paragraphs 4.11.14 and 4.11.20.
	4.11.26	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 II may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources.
	4.11.27	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 II (e.g. the amounts being invested, deposited, or wired as part of the business relationship). Source of funds information should not simply be limited to knowing from which the funds may have been transferred, but also the activity that generates the funds. The information obtained should be substantive and establish a provenance or reason for the funds having been acquired.
	4.11.28	It is for an II to decide which measures it deems appropriate, in accordance with its assessment of the risks, to establish the source of funds and source of wealth. In practical terms, this will often amount to obtaining information from the PEP and verifying it against publicly available information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests[54]. The II should however note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. The II 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.
4.12 Customer not physically present for identification purposes		
s.9(1), Sch. 2	4.12.1	The AMLO permits IIs to establish business relationships through various channels, both face-to-face (e.g. branch) and non-face-to-face (e.g. internet). However, an II should take additional measures to mitigate the risk (e.g. impersonation risk) associated with customers not physically present for identification purposes. Except for the situation specified in paragraph 4.12.2, if a customer

[54] Further examples of information useful for verifying the PEP customer's source of wealth and source of funds include publicly available property registers, land registers, asset disclosure registers, company registers, and other sources of information about legal and beneficial ownership, where available.

		has not been physically present for identification purposes, the II should carry out at least one of the following additional measures to mitigate the risks posed: (a) further verifying the customer's identity on the basis of documents, data or information referred to in section 2(1)(a) of Schedule 2 but not previously used for the purposes of verification of the customer's identity under that section; (b) taking supplementary measures to verify information relating to the customer that has been obtained by the II; 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 ("AI"), 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 AI; (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 Hong Kong Monetary Authority.
s.9(2), Sch. 2	4.12.2	If an II has verified the identity of the customer on the basis of data or information provided by a digital identification system that is a reliable and independent source that is recognized by the IA (see paragraph 4.3.1), the II is not required to carry out any additional measures set out in paragraph 4.12.1.
	4.12.3	The extent of additional measures set out in paragraph 4.12.1 will depend on the nature and characteristics of the product or service requested and the assessed ML/TF risks presented by the customer.
	4.12.4	Paragraph 4.12.1(b) allows an II to utilise different methods to mitigate the risk. These may include measures such as (i) use of an independent and appropriate person to certify identification documents; (ii) checking relevant data against reliable databases or registries; or (iii) using appropriate technology etc. Whether a particular measure or a combination of measures is acceptable should be assessed on a case by case basis. The II should ensure and be able to demonstrate to the IA that the supplementary measure(s) taken can adequately guard against impersonation risk.
	4.12.5	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 II 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 for identification purposes. In such a case, the II should mitigate the increased risk (e.g. applying additional due diligence measures set out in paragraph 4.12.1 to such natural person, except where the II has verified the identity of the natural person on the basis of data or information provided by a digital identification system (see paragraph 4.3.1(d))). In addition, where an II is provided with copies of documents for identifying and verifying a legal person customer's identity, an II should also mitigate any increased risk (e.g. applying additional due diligence measures set out in paragraph 4.12.1).
4.13 Reliance on CDD performed by intermediaries		
General		
s.18, Sch. 2	4.13.1	An II may rely upon an intermediary to perform any part of the CDD measures[55] 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 II. 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 II, and would apply its own procedures to perform the CDD measures.
	4.13.2	Authorized insurers, reinsurers, licensed individual insurance agents, licensed insurance agencies and licensed insurance broker companies all have the responsibility to comply with the requirements relating to CDD as set out in Schedule 2. However, licensed individual insurance agents, licensed insurance agencies and licensed insurance broker companies are usually the first line of contacts with the customer, before the customer is known, introduced or referred to an authorized insurer. An authorized insurer may carry out a CDD measure through its licensed individual insurance agents or licensed insurance agencies, although such insurer remains liable for a failure to carry out that CDD measure. The insurer should be satisfied that its appointed licensed individual insurance agents or licensed insurance agencies have adequate procedures in place to prevent ML and TF, namely: (a) the CDD procedures of the agent/agency should be as rigorous as those which the insurer would have conducted itself for the

[55] For the avoidance of doubt, an II 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.

		customer; and (b) the insurer is satisfied as to the reliability of the systems put in place by the agent/agency to comply with the CDD requirements of Schedule 2. If a customer is introduced to an authorized insurer through a licensed insurance broker company, the insurer may rely on the broker company to carry out any CDD measures pursuant to s. 18(1) of Schedule 2. In this case, paragraphs 4.13.4 to 4.13.8 are to be observed.
	4.13.3	For the avoidance of doubt, reliance on intermediaries does not apply to outsourcing or agency relationships, in which the outsourced entity or agent applies the CDD measures on behalf of the II, in accordance with the II's procedures, and subject to the II's control of effective implementation of these procedures by the outsourced entity or agent.
s.18(1), Sch. 2	4.13.4	When relying on an intermediary, an II should: (a) obtain written confirmation from the intermediary that the intermediary agrees to act as the II'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	4.13.5	An II that carries out a CDD measure by means of an intermediary should immediately after the intermediary has carried out that measure, obtain from the intermediary the data or information that the intermediary has obtained in the course of carrying out that measure, but nothing in this paragraph requires the II 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	4.13.6	Where these documents and records are kept by the intermediary, an II should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the II'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 II ends or until such time as may be specified by the IA. The II should ensure that the intermediary will, if requested by the II within the period specified in the record-keeping requirements of the AMLO, provide to the II 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 II 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 II anymore.
	4.13.7	An II 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.
	4.13.8	Whenever an II 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 II intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the II has any doubts regarding the CDD measures carried out by the intermediary previously, the II should perform the required CDD as soon as reasonably practicable.
<u>Domestic intermediaries</u>		
s.18(3)(a), (3)(b) & (7), Sch. 2	4.13.9	An II may rely upon any one of the following domestic intermediaries, to perform any part of the CDD measures set out in section 2 of Schedule 2: (a) an FI that is an AI, a licensed corporation, an authorized insurer, 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, or a certified public accountant (practising) as defined by section 2(1) of the Accounting and Financial Reporting Council Ordinance; (ii) a corporate practice as defined by section 2(1) of the Accounting and Financial Reporting Council Ordinance; or (iii) a CPA firm as defined by section 2(1) of the Accounting and Financial Reporting Council Ordinance; (c) an estate agent meaning: (i) a licensed estate agent as defined by section 2(1) of the Estate Agents Ordinance; or (ii) a licensed salesperson as defined by section 2(1) of the Estate Agents Ordinance; (d) a legal professional meaning: (i) a solicitor as defined by section 2(1) of the Legal Practitioners Ordinance; or (ii) a foreign lawyer as defined by section 2(1) of the Legal Practitioners Ordinance; or (e) a trust or company service provider (TCSP) licensee meaning:

		(i) a person who holds a licence granted under section 53G or renewed under section 53K of the AMLO; or (ii) a deemed licensee as defined by section 53ZQ(5) of the AMLO, provided that in the case of an accounting professional, an estate agent, a legal professional or a TCSP licensee, the II 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[56].
s.18(3)(a) & (3)(b), Sch. 2	4.13.10	An II should take appropriate measures to ascertain if the domestic intermediary satisfies the criteria set out in paragraph 4.13.9, 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	4.13.11	An II may rely upon an overseas intermediary[57] carrying on business or practising in an equivalent jurisdiction[58] 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; (iv) a TCSP; (v) a trust company carrying on trust business; and (vi) a person who carries on a business similar to that carried on by an estate agent; (b) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that

[56] 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.

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

[58] Guidance on jurisdictional equivalence is provided in paragraph 4.18.

		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).
	4.13.12	An II should take appropriate measures to ascertain if the overseas intermediary satisfies the criteria set out in paragraph 4.13.11. Appropriate measures that should be taken to ascertain if the criterion set out in paragraph 4.13.11(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	4.13.13	An II 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 II; (ii) if the II is incorporated in Hong Kong, it is a branch of the II; (iii) if the II is incorporated outside Hong Kong: (A) it is the head office of the II; or (B) it is a branch of the head office of the II; (b) is required under group policy: (i) to have measures in place to ensure compliance with requirements similar to the requirements imposed under Schedule 2; and (ii) to implement programmes against ML/TF; and (c) is supervised for compliance with the requirements mentioned in paragraph (b) at a group level: (i) by an RA; or (ii) by an authority in an equivalent jurisdiction that performs, in relation to the holding company or the head office of the II, functions similar to those of an RA under the AMLO.
s.18(3A) & (4)(c), Sch. 2	4.13.14	The group policy set out in paragraph 4.13.13(b) refers to a policy of the group of companies to which the II belongs and the policy applies to the II and the related foreign FI. The group policy should include CDD and record-keeping requirements similar to the

		requirements imposed under Schedule 2 and the group-wide AML/CFT Systems[59] (e.g. compliance and audit functions). The group policy should also be able to mitigate adequately any higher country risk in relation to the jurisdiction where the related foreign FI is located. The II should be satisfied that the related foreign FI is subject to regular and independent reviews over its ongoing compliance with the group policy conducted by any group-level compliance, audit or other similar AML/CFT functions.
s.18(3A), Sch. 2	4.13.15	The II 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.
4.14 Pre-existing customers		
s.6, Sch. 2	4.14.1	An II should perform the CDD measures prescribed in Schedule 2 and this Guideline in respect of pre-existing customers (with whom the business relationship was established before the AMLO came into effect on 1 April 2012), when: (a) a transaction takes place with regard to the customer, which is, by virtue of the amount or nature of the transaction, unusual or suspicious; or is not consistent with the II'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 II suspects that the customer or the customer's account is involved in ML/TF; or (d) the II 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.
	4.14.2	Trigger events may include the re-activation of a dormant relationship or a change in the beneficial ownership or control of the account but the II will need to consider other trigger events specific to its own customers and business.
	4.14.3	Examples of trigger events after establishment of an insurance contract are provided in paragraph 5.3.
s.5, Sch. 2	4.14.4	An II should note that requirements for ongoing monitoring under section 5 of Schedule 2 also apply to pre-existing customers (see Chapter 5).
4.15 Failure to satisfactorily complete customer due diligence		

[59] Reference should be made to Chapter 3.

s.3(1) & (4), Sch. 2	4.15.1	Where the II is unable to comply with relevant CDD requirements set out in this Chapter and the ongoing due diligence requirements set out in Chapter 5, it should not establish a business relationship or carry out any occasional transaction with that customer, or should terminate business relationship as soon as reasonably practicable (where applicable), and where there is relevant knowledge or suspicion, should make an STR to the JFIU.
4.16 Prohibition on anonymous accounts		
s.16, Sch. 2	4.16.1	An II should not open, or maintain any anonymous account or account in a fictitious name for any customer. Confidential numbered accounts[60] should not function as anonymous accounts, rather they should be subject to exactly the same CDD and control measures[61] 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 II 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 record should be available to the IA, other competent authorities, the CO, auditors, and other staff with appropriate authority.
4.17 Jurisdictions subject to a call by the FATF		
s.15, Sch. 2	4.17.1	An II should apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including FIs) from jurisdictions for which this is called for by the FATF in accordance with the guidance provided in paragraph 4.11.
s.15, Sch. 2	4.17.2	Where mandatory EDD or countermeasures[62] are called for by the FATF, or in other circumstances independent of any call by the FATF but also considered to be higher risk, the IA may also, through a notice in writing: (a) impose a general obligation on IIs to comply with the requirements set out in section 15 of Schedule 2; or (b) require IIs to undertake specific countermeasures described in the notice. The type of measures in paragraph (a) and (b) would be proportionate to the nature of the risks and/or deficiencies.
4.18 Jurisdictional equivalence		

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

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

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

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	4.18.1	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		
	4.18.2	An II 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 II should document its assessment of the jurisdiction, and may include consideration of the following factors: (a) whether the jurisdiction concerned is a member of FATF-style regional bodies and recent mutual evaluation report published by the FATF-style regional bodies; (b) whether the jurisdiction concerned is identified by the FATF as having strategic AML/CFT deficiencies and the recent progress of improving its AML/CFT regime; (c) any advisory circular issued by the IA from time to time alerting IIs to jurisdictions with poor AML/CFT controls; (d) any other AML/CFT-related publications published by specialized national, international, non-governmental or commercial organizations.
	4.18.3	As the AML/CFT regime of a jurisdiction will change over time, an II should review the jurisdictional equivalence assessment on a regular basis and/or upon trigger events.

Chapter 5 – ONGOING MONITORING		
General		
s.5(1), Sch. 2	5.1	Ongoing monitoring is an essential component of effective AML/CFT Systems. An II should continuously monitor its business relationship with a customer in two aspects: (a) **ongoing CDD**: reviewing from time to time documents, data and information relating to the customer that have been obtained by the II for the purpose of complying with the requirements imposed under Part 2 of Schedule 2 to ensure that they are up-to-date and relevant; and (b) **transaction monitoring**: (i) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the II's knowledge of the customer, the customer's business, risk profile and source of funds; and (ii) identifying transactions that (i) are complex, unusually large in amount or of an unusual pattern; and (ii) have no apparent economic or lawful purpose, and examining the background and purposes of those transactions and setting out the findings in writing.
Ongoing CDD		
s.5(1)(a), Sch. 2	5.2	To ensure documents, data and information of a customer obtained are up-to-date and relevant[63], an II should undertake reviews of existing CDD records of customers on a regular basis and/or upon trigger events [64] . Clear policies and procedures should be developed, especially on the frequency of periodic review or what constitutes a trigger event. Trigger events may include the following circumstances: (a) when a significant transaction[65] is to take place; (b) when a material change occurs in the way the customer's account is operated; (c) when the II's customer documentation standards change substantially; or (d) when the II is aware that it lacks sufficient information about the customer concerned.

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

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

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

	5.3	Examples of trigger events after establishment of an insurance contract may include: (a) there is change in beneficiaries (for instance, to include non-family members, request for payments to persons other than beneficiaries); (b) there is significant increase in the amount of sum insured or premium payment that appears unusual in the light of the income of the policy holder; (c) there is use of cash and/or payment of large single premiums; (d) there is payment/surrender by a wire transfer from/to foreign parties; (e) there is payment by banking instruments which allow anonymity of the transaction; (f) there is change of address and/or place of residence of the policy holder and/or beneficial owner; (g) there are lump sum top-ups to an existing life insurance contract; (h) there are lump sum contributions to personal pension contracts; (i) there are requests for prepayment of benefits; (j) there is use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution); (k) there is change of the type of benefit (for instance, change of type of payment from an annuity into a lump sum payment); (l) there is early surrender of the policy or change of the duration (where this causes penalties or loss of tax relief); (m) there is request for payment of benefits at the maturity date if suspicious circumstances are present; (n) the II is aware that it lacks sufficient information about the customer and/or beneficial owner; (o) there is a suspicion of ML and TF; or (p) benefits from one insurance policy are used to fund the premium payments of the insurance policy of another unrelated person.
s.5(1)(a), Sch. 2	5.4	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 II, to ensure the CDD information retained remains up-to-date and relevant.
Transaction monitoring		
Transaction monitoring systems and processes		
s.19(3), Sch. 2	5.5	An II should establish and maintain adequate systems and processes to monitor transactions. The design, degree of automation and sophistication of transaction monitoring systems and processes should be developed appropriately having regard to the following factors:

		(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). There are various methods by which these objectives can be met including exception reports (e.g. large transactions exception report or manual spreadsheets).
	5.6	An II 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.
	5.7	An II should ensure that the transaction monitoring systems and processes can support the ongoing monitoring of a business relationship in a holistic approach[66].
	5.8	In designing transaction monitoring systems and processes, including setting of parameters and thresholds, an II 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.
	5.9	An II should regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including parameters and thresholds adopted. The parameters and thresholds should be properly documented and independently validated to ensure that they are appropriate to its operations and context.
Risk-based approach to transaction monitoring and review of transactions		

[66] An example is to monitor transactions on a per person basis and on a per insurance intermediary basis. Monitoring of both financial transactions (e.g. large accumulated cash deposit, financial outflow shortly after change of policy ownership, frequent policy cancellation within cooling-off period, termination soon after large deposit/lump sum top-up) and non-financial transactions (e.g. frequent change of policy ownership, frequent change of beneficiary, frequent change of address) should be adequately covered in the transaction monitoring systems.

s.5(3), (4) & (5), Sch. 2	5.10	An II should conduct transaction monitoring in relation to all business relationships following the RBA. The extent of monitoring (e.g. frequency and intensity of monitoring) should be commensurate with the ML/TF risk profile of a customer. Where the ML/TF risks are high[67], the II should conduct enhanced transaction monitoring. In low risk situations, the II may reduce the extent of monitoring.
s.5(1)(b) & (c), Sch. 2	5.11	An II 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 II's knowledge of the customer, the customer's business, risk profile or source of funds; or (b) the II identifies transactions that (i) are complex, unusually large in amount or of an unusual pattern, and (ii) have no apparent economic or lawful purpose[68].
	5.12	Where an II conducts enquiries and obtains what it considers to be a satisfactory explanation of the transaction or activity, it may conclude that there are no grounds for suspicion, and therefore take no further action. Even if no suspicion is identified, the II should consider updating the customer risk profile based on any relevant information obtained.
	5.13	However, where the II 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.
	5.14	An II should be aware that making enquiries to customers, when conducted properly and in good faith, will not constitute tipping off. However, if the II reasonably believes that performing the CDD process will tip off the customer, it may stop pursuing the process. The II should document the basis for its assessment and file an STR to the JFIU.
s.5(1)(a), Sch. 2	5.15	The findings and outcomes of steps taken by the II in paragraph 5.11, as well as the rationale of any decision made after taking these steps, should be properly documented in writing and be available to the IA, other competent authorities and auditors.

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

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

	5.16	Where cash transactions (including deposits and withdrawals) and transfers to third parties are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, an II should approach such situations with caution and make relevant further enquiries. Where the II has been unable to satisfy itself that any cash transaction or third party transfer is reasonable, and therefore considers it suspicious, it should make a suspicious transaction report (STR) to the JFIU.
	5.17	When a customer uses a third party to pay for or receive the proceeds of an insurance policy, there is a risk that the arrangement may be used to disguise the true beneficial owner or the source of funds. An II should take reasonable measures to mitigate the ML/TF risks associated with transactions involving third-party deposits and payments. Using an RBA, an II should, for example, identify and/or verify the third-party payor/payee, validate the relationship between a customer and the payor/payee, and ascertain the reason behind another person receiving payment/paying on behalf of the customer.

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 organizations. It generally refers to the carrying out of transactions involving property owned by terrorists or terrorist organizations, 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 organizations in relation to involvement with Al-Qa'ida, ISIL (Da'esh) and the Taliban under relevant UNSCRs (e.g. UNSCR 1267 (1999), 1988 (2011), 1989 (2011), 2253 (2015), 2368 (2017) and their successor resolutions). All UN member states are required to freeze any funds, or other financial assets, or economic resources of any person(s) named in these lists and to report any suspected name matches to the relevant authorities.
	6.3	UNATMO is an ordinance to further implement a decision under UNSCR 1373 (2001) relating to measures for prevention of terrorist acts and a decision under UNSCR 2178 (2014) relating to the prevention of travel for the purpose of terrorist acts or terrorist training; as well as to implement certain terrorism-related multilateral conventions and certain FATF Recommendations.
s.4 & 5, UNATMO	6.4	Where a person or property is designated by a Committee of the UNSC established pursuant to the relevant UNSCRs as stated in paragraph 6.2 as a terrorist/terrorist associate or terrorist property[69] respectively, the Chief Executive may publish a notice in the Gazette specifying the name of the person or the property under section 4 of the UNATMO. Besides, section 5 of the UNATMO provides that the Chief Executive may make an application to the Court of First Instance for an order to specify a person or property as a terrorist/terrorist associate or terrorist property respectively, and if the order is made, it will also be published in the Gazette.
s.6, 7, 8, 8A & 11L, UNATMO	6.5	A number of provisions in the UNATMO are of particular relevance to IIs, and are listed below:

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

		(a) section 6 empowers the Secretary for Security (S for S) to freeze suspected terrorist property; (b) section 7 prohibits the provision or collection of property for use to commit terrorist acts; (c) section 8 prohibits any person from making available or collecting or soliciting property or financial (or related) services for terrorists and terrorist associates; (d) section 8A prohibits any person from dealing with any property knowing that, or being reckless as to whether, the property is specified terrorist property or property of a specified terrorist or terrorist associate; and (e) section 11L prohibits any person from providing or collecting any property to finance the travel of a person between states with the intention or knowing that the travel will be for a specified purpose, i.e. the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs); or the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs as a result of the training).
s.6(1), 8 & 8A(1), UNATMO	6.6	The S for S can licence exceptions to the prohibitions to enable frozen property to be unfrozen and to allow payments to be made to or for the benefit of a designated party under the UNATMO (e.g. reasonable living/legal expenses and payments liable to be made under the Employment Ordinance). An II seeking such a licence should write to the Security Bureau.
Financial sanctions & proliferation financing		
	6.7	The UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the UNSC, including targeted financial sanctions[70] 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 Development 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

[70] 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).

		assets or economic resources belonging to, or owned or controlled by, such persons 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 II seeking such 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.
Sanctions imposed by other jurisdictions		
	6.11	While IIs do not normally have any obligation under Hong Kong laws to have regard to unilateral sanctions imposed by other organizations or authorities in other jurisdictions, an II operating internationally will need to be aware of the scope and focus of relevant sanctions regimes in those jurisdictions. Where these sanctions regimes may affect its operations, the II should consider what implications exist and take appropriate measures.
Database maintenance, screening and enhanced checking		
	6.12	An II 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 IIs 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 II should be able to identify terrorist suspects and possible designated parties, and detect prohibited transactions. To this end, an II 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 II. Alternatively, an II may subscribe to such a database maintained by a third party service provider and take appropriate measures (e.g. conduct sample testing periodically) to ensure the completeness and accuracy of the database.
	6.14	Whether or not a UNSCR or sanctions list has been implemented through Hong Kong legislation, there are offences under existing legislation relating to ML, TF and PF that are relevant. Inclusion of a country, individual, entity or activity in the UNSCR or sanctions list may constitute grounds for knowledge or suspicion for the purposes of relevant ML, TF and PF laws, thereby triggering statutory (including reporting) obligations as well as offence provisions. The IA draws to the attention to IIs from time to time whenever there are any updates to UNSCRs or sanctions lists relating to terrorism, TF and PF promulgated by the UNSC. IIs 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 II should include in its database: (i) the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau; and (ii) the lists that the IA draws to the attention of IIs from time to time. The database should also be subject to timely update whenever there are changes, and should be made easily accessible by relevant staff.
	6.16	To avoid establishing business relationship or conducting transactions with any terrorist suspects and possible persons or entities falling within paragraph 6.7(a), an II should implement an effective screening mechanism[71], which should include: (a) screening its customers and any beneficial owners of the customers against current database at the establishment of the relationship; and (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.
	6.17	The screening requirements set out in paragraph 6.16(a) and (b) should extend to connected parties as defined in paragraph 4.3.19 and PPTAs of a customer using an RBA.

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

	6.18	When possible name matches are identified during screening, an II should conduct enhanced checks to determine whether the possible matches are genuine hits. In case of any suspicions of TF, PF or sanctions violations, the II 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 II may rely on its overseas office to maintain the database or to undertake the screening process. However, the II is reminded that the ultimate responsibility for ensuring compliance with the relevant regulations and legislation on TF, financial sanctions and PF remains with the II.
	6.20	An II should screen its payees, including policy beneficiaries, to ensure that proposed payments to terrorist suspects and possible sanctioned parties are not made at the time of the payout.

Chapter 7 – SUSPICIOUS TRANSACTION REPORTS, LAW ENFORCEMENT REQUESTS AND CRIME-RELATED INTELLIGENCE		
Suspicious transaction reporting regime in Hong Kong		
General issues		
s.25A(1)&(7), DTROP & OSCO, s.12(1)&14(5), UNATMO	7.1	It is a statutory obligation under sections 25A(1) of the DTROP and the OSCO, as well as section 12(1) of the UNATMO, that where a person knows or suspects that any property: (a) in whole or in part directly or indirectly represents any person's proceeds of, (b) was used in connection with, or (c) is intended to be used in connection with drug trafficking or an indictable offence; or that any property is terrorist property, the person shall as soon as it is reasonable for him to do so, file an STR with the JFIU. The STR should be made together with any matter on which the knowledge or suspicion is based. Under the DTROP, the OSCO and the UNATMO, failure to report knowledge or suspicion carries a maximum penalty of imprisonment for three months and a fine of $50,000.
Knowledge vs. suspicion		
	7.2	Generally speaking, knowledge is likely to include: (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 II is concerned, when a transaction or a series of transactions of a customer is not consistent with the II's knowledge of the customer, or is unusual (e.g. in a pattern that has no apparent economic or lawful purpose), the II should take appropriate steps to further examine the transactions and identify if there is any suspicion (see paragraphs 5.11 to 5.17).
	7.4	The following is a (non-exhaustive) list of examples of situations that might give rise to suspicion in certain circumstances: (a) transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale; (b) transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business; (c) where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular

		customer; (d) where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged; (e) where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process; (f) where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation; (g) the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services; (h) transfers to and from jurisdictions subject to a call by the FATF without reasonable explanation, which are not consistent with the customer's declared business dealings or interests; and (i) unnecessary routing of funds or other property from/to third parties or through third party accounts. Further examples of what might constitute suspicious transactions are provided in Annexes I and II. These are not intended to be exhaustive and only provide examples of the most basic ways in which money may be laundered. However, identification of any of the types of transactions listed above or in Annexes I and II should prompt further investigations and be a catalyst towards making at least initial enquiries about the source of funds. An II should also be aware of elements of individual transactions and situations that might give rise to suspicion of terrorist financing in certain circumstances. The FATF publishes studies of methods and trends of terrorist financing from time to time, and IIs may refer to the FATF website for additional information and guidance.
	7.5	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.
	7.6	Once knowledge or suspicion has been formed, (a) an II should file an STR even where no transaction has been conducted by or through the II[72]; and (b) the STR should be made as soon as reasonably practical after the suspicion was first identified.

[72] 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.

Tipping off		
s.25A(5), DTROP & OSCO, s.12(5), UNATMO	7.7	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 II, but has not yet been reported to the JFIU.
AML/CFT Systems in relation to suspicious transaction reporting		
	7.8	An II should implement appropriate AML/CFT Systems in order to fulfil its statutory reporting obligations, and properly manage and mitigate the risks associated with any customer or transaction involved in an STR. The AML/CFT Systems should include: (a) appointment of an MLRO (see Chapter 3); (b) implementing clear policies and procedures over internal reporting, reporting to the JFIU, post-reporting risk mitigation and prevention of tipping off; and (c) keeping proper records of internal reports and STRs.
	7.9	An II should have measures in place to check, on an ongoing basis, that its AML/CFT Systems in relation to suspicious transaction reporting comply with relevant legal and regulatory requirements and operate effectively. The type and extent of the measures to be taken should be appropriate having regard to the risk of ML/TF as well as the nature and size of its business.
Money laundering reporting officer		
	7.10	An II 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.
Identifying suspicious transactions and internal reporting		
	7.11	An II should provide sufficient guidance to its staff to enable them to form suspicion or to recognize 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.

	7.12	An II 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 (http://www.jfiu.gov.hk).
	7.13	An II should establish and maintain clear policies and procedures to ensure that: (a) all staff are made aware of the identity of the MLRO and of the procedures to follow when making an internal report; and (b) all internal reports should reach the MLRO without undue delay.
	7.14	While an II 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 of an II has reported suspicion to the MLRO in accordance with the policies and procedures established by the II for the making of such reports, the statutory obligation of the staff 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 upon internal reporting.
	7.18	When evaluating an internal report, an MLRO should take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the II concerning the customer to which the report relates. This may include: (a) making a review of other transaction patterns and volumes through connected accounts, preferably adopting a

		relationship-based approach rather than on a transaction-by-transaction basis; (b) making reference to any previous patterns of instructions, the length of the business relationship, and CDD and ongoing monitoring information and documentation; and (c) appropriate questioning of the customer per the systematic approach to identify suspicious transactions recommended by the JFIU[73].
	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.
Reporting to the JFIU		
	7.20	If after completing the review of the internal report, an MLRO decides that there are grounds for knowledge or suspicion, he should disclose the information to the JFIU as soon as it is reasonable to do so after his evaluation is complete together with the information on which that knowledge or suspicion is based. Dependent on when knowledge or suspicion arises, an STR may be made either before a suspicious transaction or activity occurs (whether the intended transaction ultimately takes place or not), or after a transaction or activity has been completed.
	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 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 II to move funds or other property, close the account, make cash available for collection, or carry out significant changes to the business relationship etc.), particularly when the account is part of an ongoing investigation by law enforcement agency, an II should indicate this in the STR. Where exceptional circumstances exist in relation to an urgent reporting, an initial notification by telephone to the JFIU should be considered.
	7.23	An II is recommended to indicate any intention to terminate a business relationship in its initial STR to the JFIU.

[73] For details, please see JFIU's website (http://www.jfiu.gov.hk).

	7.24	An II should ensure STRs filed to the JFIU are of high quality taking into account feedback and guidance provided by the JFIU in its quarterly report[74] and the IA from time to time.
Post STR reporting		
s.25A(2)(a), DTROP & OSCO, s.12(2B)(a), UNATMO	7.25	The JFIU will acknowledge receipt of an STR made by an II under section 25A of both the DTROP and the OSCO, and section 12 of the UNATMO. If there is no need for imminent action, e.g. the issue of a restraint order on an account, consent will usually be given for the II to operate the account under the provisions of section 25A(2)(a) of both the DTROP and the OSCO, and section 12(2B)(a) of the UNATMO. Otherwise, the II should take appropriate action and seek legal advice where necessary.
s.25A(2), DTROP & OSCO, s.12(2), UNATMO	7.26	Filing an STR to the JFIU provides an II 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 II 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 II has performed the disclosed acts (transaction(s)) and the report is made on the II's own initiative and as soon as it is reasonable for the II to do so.
	7.27	However, the statutory defence stated in paragraph 7.26 does not absolve an II from the legal, reputational or regulatory risks associated with the account's continued operation. An II 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 II.
	7.28	An II 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 II'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 II's business objectives, and its capacity to mitigate the

[74] 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 http://www.jfiu.gov.hk. IIs 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.

		risks identified.
	7.29	An II should be aware that the reporting of a suspicion in respect of a transaction or event does not remove the need to report further suspicious transactions or events in respect of the same customer. Further suspicious transactions or events, whether of the same nature or different to the previous suspicion, should continue to be reported to the MLRO who should make further reports to the JFIU if appropriate.
Record-keeping		
	7.30	An II should establish and maintain a record of all ML/TF reports made to the MLRO. The record should include details of the date the report was made, the staff members subsequently handling the report, the results of the assessment, whether the internal report resulted in an STR to the JFIU, and information to allow the papers relevant to the report to be located. An II should also maintain a register of internal reports summarising the records of all ML/TF reports made to the MLRO.
	7.31	An II should establish and maintain a record of all STRs made to the JFIU. The record should include details of the date of the STR, the person who made the STR, and information to allow the papers relevant to the STR to be located. An II should also maintain a register summarising the records of all STRs made to the JFIU. This register may be combined with the register of internal reports, if considered appropriate.
Requests from law enforcement agencies and crime related intelligence		
	7.32	An II may receive various requests from law enforcement agencies, e.g. search warrants, production orders, restraint orders or confiscation orders, pursuant to relevant legislations in Hong Kong. These requests are crucial to aid law enforcement agencies to carry out investigations as well as restrain and confiscate illicit proceeds. Therefore, an II should establish clear policies and procedures to handle these requests in an effective and timely manner, including allocation of sufficient resources and appointing a staff as the main point of contact with law enforcement agencies.
	7.33	An II 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 II encounters difficulty in complying with the timeframes stipulated, the II should at the earliest opportunity contact the officer-in-charge of the investigation for further guidance.
s.10 & 11, DTROP, s.15 & 16, OSCO, s.6, UNATMO	7.34	During a law enforcement investigation, an II may be served with a restraint order which prohibits the dealing with particular funds or property pending the outcome of an investigation. The II should

		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 the II 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	7.35	Upon the conviction of a defendant, a court may order the confiscation of his criminal proceeds and an II may be served with a confiscation order in the event that it holds funds or other property belonging to that defendant that are deemed by the court to represent his benefit from the crime. A court may also order the forfeiture of property where it is satisfied that the property is terrorist property.
	7.36	When an II receives a requirement (e.g. search warrant or production order) or other types of crime-related intelligence requests including those from a law enforcement agency (e.g. notification letter) in relation to a particular customer or business relationship, the II should timely assess the risks involved and the need to conduct an appropriate review on the customer or the business relationship to determine whether there is any suspicion and should also be aware that the customer subject to the request can be a victim of crime.

Chapter 8 – RECORD-KEEPING		
General		
	8.1	Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps the investigating authorities to establish a financial profile of a suspect, trace the criminal or terrorist property or funds and assists the Court to examine all relevant past transactions to assess whether the property or funds are the proceeds of or relate to criminal or terrorist offences. Record-keeping also enables an II to demonstrate compliance with the requirements set out in the AMLO, this Guideline and other relevant guidance promulgated by the IA from time to time.
	8.2	An II 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 II should ensure that: (a) the audit trail for funds moving through the II that relate to any customer and, where appropriate, the beneficial owner of the customer, account or transaction is clear and complete; (b) all CDD information and transaction records are available swiftly to the IA, 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 IA.
Retention of records relating to CDD and transactions		
s.20(1)(b)(i), Sch. 2 s.20(1)(b)(ii), Sch. 2	8.3	An II should keep: (a) the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and, where applicable, verifying the identity of the customer and/or beneficial owner of the customer and/or beneficiary and/or persons who purport to act on behalf of the customer and/or other connected parties to the customer; (b) other documents and records obtained throughout the CDD and ongoing monitoring process, including SDD and EDD; (c) where applicable, the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship; (d) the original or a copy of the records and documents relating to the customer's account (e.g. account opening form, insurance application form or risk assessment form) and business

		correspondence[75] with the customer and any beneficial owner of the customer (which at a minimum should include business correspondence material to CDD measures or significant changes to the operation of the account); and (e) the results of any analysis undertaken (e.g. inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose).
s.20(2), (3) & (3A), Sch. 2	8.4	All documents and records mentioned in paragraph 8.3 should be kept throughout the continuance of the business relationship with the customer and for a period of at least five years after the end of the business relationship. Similarly, for occasional transaction equal to or exceeding the CDD threshold (i.e. $8,000 for wire transfers and virtual asset transfers, and $120,000 for other types of transactions), an II should keep all documents and records mentioned in paragraph 8.3 for a period of at least five years after the date of the occasional transaction.
s.20(1)(a), Sch. 2	8.5	An II 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 II 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.
	8.7	Documents and records that IIs may keep include: (a) initial proposal documentation such as the customer financial assessment, analysis of needs, details of the payment method, illustration of benefits, and copy of documentation in support of verification by the IIs; (b) records associated with the maintenance of the contract post sale, up to and including maturity of the contract; and (c) "Discharge documentation" with details of the maturity processing and/or claim settlement.
s.21, Sch. 2	8.8	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

[75] An II 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.

		consists of data or information, such record should be kept either on microfilm or in the database of a computer.
s.20(4), Sch. 2	8.9	The IA may, by notice in writing to an II, require it to keep the records relating to a specified transaction or customer for a period specified by the IA 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 IA, or to any other purposes as specified in the notice.
Part 3, Sch. 2	8.10	Irrespective of where CDD and transaction records are held, an II is required to comply with all legal and regulatory requirements in Hong Kong, especially Part 3 of Schedule 2.
Records kept by intermediaries		
s.18(4)(a)&(b), Sch. 2	8.11	Where customer identification and verification documents are held by an intermediary on which an II is relying to carry out CDD measures, the II concerned remains responsible for compliance with all record-keeping requirements. The II 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 8.10), and that documents and records will be provided by the intermediary as soon as reasonably practicable after the intermediary receives the request from the II.
s.18(4)(a), Sch. 2	8.12	For the avoidance of doubt, an II 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.
	8.13	An II should ensure that an intermediary will pass the documents and records to the II, upon termination of the services provided by the intermediary.
Record-keeping obligations by licensed individual insurance agents		
	8.14	Licensed individual insurance agents who are appointed agents of an authorized insurer are usually required to provide all customer and transaction related documentation to the insurer directly, and they do not have the capacity to maintain such documents. Under this arrangement, and from the perspective of meeting the record-keeping requirements set out in Part 3 of Schedule 2, these individual insurance agents are considered to have deposited the required records and documents at the premises of the insurer. As the individual insurance agents remain responsible for compliance with all record-keeping requirements, they should ensure that:

		(a) the insurer to which they provide the records and documents has systems in place to comply with all the record-keeping requirements under the AMLO; and (b) such records and documents are accessible from the insurer without delay upon request by the IA. For the avoidance of doubt, the requirements under this paragraph 8.14 apply to licensed individual insurance agents only and do not apply to licensed insurance agencies.

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

		(b) members of staff who are dealing directly with the public (e.g. front-line personnel, licensed individual insurance agents, licensed technical representatives (agent) appointed by licensed insurance agencies, and licensed technical representatives (broker) appointed by licensed insurance broker companies): (i) the importance of their roles in the II's ML/TF strategy, as the first point of contact with potential money launderers; (ii) the II'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 recognize 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 II'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 II 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 II may consider including available FATF papers and typologies as part of the training materials. The II should be able to demonstrate to the IA that all materials are up-to-date and in line with current requirements and standards.
	9.7	No matter which training approach is adopted, an II 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 II should monitor the effectiveness of the training. This may be achieved by: (a) testing staff's understanding of the II's policies and procedures to combat ML/TF, the understanding of their statutory and regulatory obligations, and also their ability to recognize suspicious transactions; (b) monitoring the compliance of staff with the II'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[76] 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)[77].
s.12(2), Sch. 2	10.4	Section 12 of Schedule 2 and this Chapter do not apply to the following wire transfers: (a) a wire transfer between 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[78] 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

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

[77] 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 Hong Kong Monetary Authority in February 2010.

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

		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 should ensure that a wire transfer of amount equal to or above $8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information: (a) the originator's name; (b) the number of the originator's account maintained with the ordering institution and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned by the ordering institution; (c) the originator's address or, the originator's customer identification number[79] or identification document number or, if the originator is an individual, the originator's date and place of birth; (d) the recipient's name; and (e) the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution.
s.12(3), (3A) & (5), Sch. 2	10.6	An ordering institution should ensure that a wire transfer of amount below $8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information : (a) the originator's name; (b) the number of the originator's account maintained with the ordering institution and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned by the ordering institution; (c) the recipient's name; and (d) the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution.

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

	10.7	The unique reference number assigned by the ordering institution or beneficiary institution referred to in paragraphs 10.5 and 10.6 should permit traceability of the wire transfer.
	10.8	For a wire transfer of amount equal to or above $8,000 (or an equivalent amount in any other currency), an ordering institution should ensure that the required originator information accompanying the wire transfer is accurate.
s.3(1)(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 should verify the identity of the originator. For an occasional wire transfer below $8,000 (or an equivalent amount in any other currency), the ordering institution is in general not required to verify the originator's identity, except when several transactions are carried out which appear to the ordering institution to be linked and are equal to or above $8,000 (or an equivalent amount in any other currency), or when there is a suspicion of ML/TF.
s.12(7), Sch. 2	10.10	An ordering institution may bundle a number of wire transfers from a single originator into a batch file for transmission to a recipient or recipients in a place outside Hong Kong. In such cases, the ordering institution may only include the originator's account number or, in the absence of such an account, a unique reference number in the wire transfer but the batch file should contain required and accurate originator information, and required recipient information, that is fully traceable within the recipient country.
s.12(6), Sch. 2	10.11	For a domestic wire transfer[80], an ordering institution may choose not to include the complete required originator information in the wire transfer but only include the originator's account number or, in the absence of an account, a unique reference number, provided that the number permits traceability of the wire transfer.
s.12(6), Sch. 2	10.12	If an ordering institution chooses not to include complete required originator information as stated in paragraph 10.11, it should, on the request of the institution to which it passes on the transfer instruction or the 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

[80] 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.

		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 should ensure that all originator and recipient information which accompanies the wire transfer is retained with the transfer and is transmitted to the institution to which it passes on the transfer instruction.
	10.15	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 should establish and maintain effective procedures for identifying and handling incoming wire transfers that do not comply with the relevant originator or recipient information requirements, which include: (a) taking reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required recipient information; and (b) having risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator information or required recipient information; and (ii) the appropriate follow-up action.
s.12(10)(a), Sch. 2	10.17	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 should as soon as

		reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, the intermediary institution should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved.
s.12(10)(b), Sch. 2	10.18	If the intermediary institution is aware that the accompanying information that purports to be the required originator information or required recipient information is incomplete or meaningless, it should as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
Beneficiary institutions		
s.19(2), Sch. 2	10.19	A beneficiary institution should establish and maintain effective procedures for identifying and handling incoming wire transfers that do not comply with the relevant originator or recipient information requirements, which include: (a) taking reasonable measures (e.g. post-event monitoring) to identify domestic or cross-border wire transfers that lack required originator information or required recipient information; and (b) having risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator information or required recipient information; and (ii) the appropriate follow-up action.
s.12(9)(a) & s.12(10)(a), Sch.2	10.20	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 should as soon as reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, the beneficiary institution should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved.
s.12(9)(b) & s.12(10)(b), Sch.2	10.21	If the beneficiary institution is aware that the accompanying information that purports to be the required originator information or required recipient information is incomplete or meaningless, it should as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
s.3(1)(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.

Annex I - Indicators of suspicious transactions		
		1. A request by a customer to enter into an insurance contract(s) where the source of the funds is unclear or not consistent with the customer's apparent standing. 2. A sudden request for a significant purchase of a lump sum contract with an existing client whose current contracts are small and of regular payments only. 3. A proposal which has no discernible purpose and a reluctance to divulge a "need" for making the investment. 4. A proposal to purchase and settle by cash. 5. A proposal to purchase by utilizing a cheque drawn from an account other than the personal account of the proposer. 6. The prospective client who does not wish to know about investment performance but does enquire on the early cancellation/surrender of the particular contract. 7. A customer establishes a large insurance policy and within a short period of time cancels the policy, requests the return of the cash value payable to a third party. 8. Early termination of a product, especially in a loss. 9. A customer applies for an insurance policy relating to business outside the customer's normal pattern of business. 10. A customer requests for a purchase of insurance policy in an amount considered to be beyond his apparent need. 11. A customer attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments. 12. A customer refuses, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue. 13. A customer is reluctant to provide normal information when applying for an insurance policy, provides minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify. 14. Delay in the provision of information to enable verification to be completed.

		15. Opening accounts with the customer's address outside the local service area. 16. Opening accounts with names similar to other established business entities. 17. Attempting to open or operating accounts under a false name. 18. Any transaction involving an undisclosed party. 19. A transfer of the benefit of a product to an apparently unrelated third party. 20. A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy). 21. Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policy holder. 22. The customer accepts very unfavourable conditions unrelated to his health or age. 23. An atypical incidence of pre-payment of insurance premiums. 24. Insurance premiums have been paid in one currency and requests for claims to be paid in another currency. 25. Activity is incommensurate with that expected from the customer considering the information already known about the customer and the customer's previous financial activity. (For individual customers, consider customer's age, occupation, residential address, general appearance, type and level of previous financial activity. For corporate customers, consider type and level of activity.) 26. Any unusual employment of an intermediary in the course of some usual transaction or financial activity e.g. payment of claims or high commission to an unusual intermediary. 27. A customer appears to have policies with several institutions. 28. A customer wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.

		29. The customer who is based in jurisdictions subject to a call by the FATF or in countries where the production of drugs or drug trafficking may be prevalent. 30. The customer who is introduced by an overseas agent, affiliator or other company that is based in jurisdictions subject to a call by the FATF or in countries where corruption or the production of drugs or drug trafficking may be prevalent. 31. A customer who is based in Hong Kong and is seeking a lump sum investment and offers to pay by a wire transaction or foreign currency. 32. Unexpected changes in employee characteristics, e.g. lavish lifestyle or avoiding taking holidays. 33. Unexpected change in employee or agent performance, e.g. the sales person selling products has a remarkable or unexpected increase in performance. 34. Consistently high activity levels of single premium business far in excess of any average company expectation. 35. The use of an address which is not the client's residential address, e.g. utilization of the salesman's office or home address for the despatch of customer documentation. 36. Any unusual or disadvantageous early redemption of an insurance policy. 37. Transfer of policy ownership to a person without any apparent connection with the original policy holder. 38. Payment to/from a third party without justifiable explanation by considering, for example, relationship between the customer and the third party, identity of the third party and the reason for paying to or receiving the payments from the third party. 39. Cross-border payment to Hong Kong from a jurisdiction with less stringent anti-money laundering controls and where there are no apparent customer activities in that jurisdiction.
Important Note		
		The International Association of Insurance Supervisors (IAIS) has published relevant examples and indicators involving insurance in a document called "Guidance Paper on Anti-money Laundering and Combating the Financing of Terrorism". The document can be downloaded from IAIS website at http://www.iaisweb.org. IIs are

		advised to browse the IAIS website regularly for the latest examples of suspicious transaction indicators.

Annex II - Examples of money laundering and terrorist financing cases[81]		
Money Laundering		
		Case study 1. Early cancellation, insider collusion Mrs. T (teacher) from country A, entered into a life insurance policy with a small initial premium being paid. The transaction was arranged by Mr. B who was the agent of insurance company C and a cousin of Mrs. T. Two days later, company C made a payment of an additional premium, in excess of €540,000, on behalf of Mrs. T. After one month, Mrs. T cancelled her policy and transferred the refund of contributions to three different accounts: a) Mr. MD (Managing Director of Company C) – €240,000; b) Mrs. N (niece of Mr. MD) – €150,000; and c) Mr. U – €150,000. All of them subsequently transferred the money onwards to other accounts in different banks. Following an investigation it appeared that the money being laundered was linked to fuel smuggling. The Financial Intelligence Unit (FIU) ordered the accounts to be blocked and the case was forwarded to the public prosecutor. **Case study 2. High premium, early cancellation** A single premium on a life policy, totalling more than €500,000 was paid on behalf of Mr. A by Mr. A's employer, who was a related person. Half of the amount was withdrawn by Mr. A within a month of paying the premium. A request for withdrawing the balance of the amount was filed at the same time. Following a report to the FIU subsequent checks revealed that Mr. A had a criminal record and was involved in pending legal proceedings. It also appeared that Mr. A was allegedly involved in drug dealing and assassinations. Following further investigation and collection of information, including tax records, and movements of funds on Mr. A's accounts the relevant information was forwarded to law enforcement agencies. **Case study 3. High premium, false pretences for structured withdrawals** A life insurance policy with a very high single premium included a clause for partial redemption, at the customer's request, at the end of each year. The customer claimed that the purpose of the clause was to repay the interest on a loan with a duration of 10 years,

[81] The examples of money laundering and terrorist financing cases in this annex are extracted from the IAIS document "Application Paper on Combating Money Laundering and Terrorist Financing". The document can be downloaded at http://www.iaisweb.org/.

		intended to facilitate the building of a warehouse. The insurer reported a suspicion to the local FIU because of the high premium and because the customer refused to name the bank where he had taken up the loan. After careful examination by the FIU, it turned out that the customer was known to the police as he had committed financial fraud. It appears that the customer had tried to launder money by means of a life insurance product. **Case study 4. Foreign policy holders, source of wealth** An insurance company filed a report of suspicion concerning two foreign individuals each of whom bought a single premium life insurance contract. The premiums were very high. The investigation by the FIU showed that the premiums for these insurance policies were paid through the current accounts of the two customers, while payments to the accounts consisted of cash deposits the origin of which was unknown. Moreover, the accounts were only used for payment for the insurance policy and the account holders had already been the subject of a report on illegal drug trafficking. According to the police reports, the individuals were members of a network responsible for trafficking drugs from Latin America to Western Europe. The insurance company reported suspicion of potential ML on the basis of several factors, namely that the policy holders did not have an official address in the country where they wanted to buy the policy, they were not exercising any professional activity in that country, and they could not explain the origin of the money. This case is currently subject to legal proceedings. **Case study 5. Source of wealth** Mr. A, who claimed to be a 25 year old garage owner, bought a life insurance policy with a high single premium in relation to his age. The policy was issued for a duration of 10 years with Mr. A being the beneficiary if alive and Mrs. B being the beneficiary in the case of the death of Mr. A during the 10 year duration of the policy (Mrs. B being the grandmother of Mr. A). The insurance company reported the case to the FIU. Research by the FIU showed that Mr. A did not own a garage but had been involved in drug trafficking. The FIU forwarded its report to the department of justice, which dealt with cases of drug trafficking. **Case study 6. Early cancellation** A couple in their twenties purchased several single premium life insurance contracts with the same insurance company. A little later they requested an early repayment of these policies in cash. This, combined with the young age of the insured, attracted the attention of the insurance company. The FIU found that both policy holders

		had convictions and were the subjects of a drug investigation. The file was referred to the criminal court. **Case study 7. Early cancellation, payout to third party** A policy holder living abroad bought a life insurance policy and, soon afterwards, requested early surrender of the policy. This early surrender resulted in high costs for the policy holder. Afterwards, the policy holder made a request by fax to transfer the money to an account of another person living abroad. The insurer contacted the FIU, which, in light of the urgency of the situation, requested that the transaction should be postponed for 24 hours. This gave the FIU time to collect data, which indicated that the policy holder had been convicted for illegal public attraction of savings. The case has been transferred to the justice department for further investigation. **Case study 8. Source of wealth** Two life insurance policies were bought for a large amount in the names of Mr. X and Mr. Y. The payments were made by cheque, originating from the account of a European investment company. Both policies were used as security for a mortgage loan with a company that specialized in leasing. As the beneficiaries were not the policy holders and in light of the unusual financing being provided by a leasing company, the insurer contacted the investment company in order to understand the origin of the money that had been deposited in the account. It appeared that the money was deposited with the company in cash by random customers. Following the disclosure of suspicion by the insurance company it became evident that Mr. X and Mr. Y were known by the customs authorities for the illegal importation and exportation of cars. **Case study 9. Early cancellation, source of wealth** A 34 year old car dealer received a loan through a broker of a life insurance company to purchase a house. He invested around 25% of the loan in a single-premium life insurance policy. He later surrendered the policy early to pay back the loan (capital and interest), making up the shortfall through other funds. The use of a substantial proportion of the loan to purchase a policy combined with the unexpectedly early repayment of the loan led to the FIU being contacted. The FIU's investigation revealed that the policy holder was known for stealing and receiving stolen cars. Moreover, he had used false documents to prove the sources of his income and wealth.

		Case study 10. Adverse media for existing customer A life insurance company was contacted by a financial adviser calling on behalf of a customer who had taken out a policy. The customer had recently been convicted of fraud and wished to ascertain whether such a conviction would compromise the policy's terms and conditions. The conviction did not pose a problem for the continuation of the policy. However the disclosure of fraud prompted an internal review. Active investment policies were identified and a media article was found, which stated that the customer had been part of a gang involved in a €6 million tax fraud and subsequent ML offences. A suspicious activity report was submitted to the FIU. Following dissemination of the intelligence by the FIU, the tax authority advised the insurance company that its report provided useful information, allowing a case for confiscation of assets to be made. **Case study 11. Source of funds** A life insurance company received a payment of €25,000 for an existing customer via an "over the counter" transaction. When the money was received, enquiries were made by the company as to where the money had come from. It transpired that the money had been deposited in cash at a bank in order to pay premiums to the insurance company. The receiving bank had not asked questions when the cash was received. However, the life insurance company considered the transaction to be suspicious in light of the amount, the fact that it had not received such a payment from the customer before and that it contradicted confirmations provided by the customer as to how payments would be made, and the absence of reasonable responses by the customer to questions by the insurance company. Consequently, a suspicious activity report was made to the FIU. **Case study 12. PEP** A financial adviser approached a life insurance company in order to make a pre-application enquiry on behalf of a potential customer to PEP classifications and other issues. The potential applicant was married to a former president of a developing country who was in self-imposed exile due to outstanding criminal matters. The spouse was seeking a whole life product in order to protect her tax liabilities. However, the husband was implicated in a multi-million dollar theft of public state money. The business was rejected and a report made to the FIU. **Case study 13. Source of funds, complex scheme** A company director from Company W, Mr. H set up a ML scheme involving two companies, each one established under different

		legal systems. Both of the entities were to provide financial services and providing financial guarantees for which he would act as director. These companies wired the sum of US$1.1 million to the accounts of Mr. H in Country S. It is likely that the funds originated in some sort of criminal activity and had already been introduced in some way into the financial system. Mr. H also received transfers from Country C. Funds were transferred from one account to another (several types of accounts were involved, including both current and savings accounts). Through one of these transfers the funds were transferred to Country U from a current account in order to make payments on life insurance policies. The investment in these policies was the main mechanism in the scheme for laundering the funds. The premiums paid for the life insurance policies in Country U amounted to some US$1.2 million and represented the last step in the laundering operation. **Case study 14. Source of funds** A husband and wife took out a life insurance policy each in their own name with annual premiums. In the event of the death of one of the spouses, the other spouse would become the beneficiary of the insurance. The holder of the account through which the premiums had been paid was found not to be the policy holders but a company abroad of which they were directors. However, this was a life insurance policy taken out privately by the couple and not by the company. Investigation revealed that the scenario set up had been intended to conceal the illicit origin of the funds which originated from serious and organized tax fraud for which the couple involved was known. **Case study 15. Inappropriate beneficiary** A mayor concluded an investment-linked life insurance contract as the representative of the municipality. He was named as the insured person and the insurance fee was taken directly from the budget of the municipality. In case of expiry of the contract, the municipality would have been the beneficiary. However, a notification was submitted to the insurance company after the expiry of the contract, assigning the mayor as the new beneficiary of the insurance policy, and requested the payment to be fulfilled on his private bank account following the expiry of the contract. The insurance company submitted a STR to inform the FIU. **Case study 16. Employee / Agent fraud, source of funds** Misled by an agent of an insurance company, customers deposited large cash payments to the bank account of an insurance company in favour of the insurance policy of the daughter of the agent. The source of these cash payments was a large amount of winning derived from foreign gambling. Certainly, the customers believed

		that they deposited the cash in favour of their own insurance policies. Then, after numerous claims of partial redemptions sent to the insurance company, the agent finally repurchased the investment-linked insurance policy of her daughter. **Case study 17. Source of funds** The deputy mayor of a medium-sized town was in charge of social care of the elderly. He received, in three months, €1 million transferred from the account of an advisor society and €0.6 million from the account of a real estate society (of which he later became a shareholder) to build a retirement home. After having justified the inflows of funds by producing invoices, the elected representative used part of the funds to build a life insurance portfolio and invest in a private real estate purchase. The case was reported to the FIU. **Case study 18. Source of funds** After an investigation, the chairman of a private elementary school was sued by the prosecutor and was judged guilty because he had misused the miscellaneous fees (for tutor classes, comprehensive activities, bilingual classes, etc.) the school received from students. Such fees were not precisely recorded in the school's financial report or the income statement required by the authorities. Having realized that the fees paid by students were deposited in a bank account that belonged to school, the chairman instructed the school's accountant to withdraw the cash in order to hand over to him. A part of the illegal income was used to pay for the premium fee of 15 insurance policies held by him, his wife, and son. Another portion of the illegal income was spent on purchasing properties, stocks, vehicles, trust funds, and long-term deposits. The rest amount of the illegal income was hidden in a safe-deposit box. **Case study 19. Intermediary collusion** A person (later arrested for drug trafficking) made a financial investment (life insurance) of US$250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of US$250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raised no suspicion at the bank since the insurance broker was known to them as being connected to the insurance branch. The insurance broker delivered, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling US$250,000, thus avoiding raising suspicions with the insurance company.

		Case study 20. Intermediary collusion, payout to third party Customers in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the customer by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks. The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the customer stating that there was now a change in circumstances, and the customer would have to surrender the policy, suffering losses but coming away with a clean cheque from the institution. On other occasions the policy would be left to run for a couple of years before being surrendered with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution. **Case study 21. Employe/Agent collusion, multiple withdrawals** A drug trafficker, whose wife was a part-time insurance agent, used the proceeds of his illegal activities to purchase insurance policies from his wife and invest in several businesses including a restaurant business. Substantial increase in monthly premium for one of the insurance policies, multiple withdrawals, where the proceeds were subsequently used to pay premiums of other existing insurance policies and advance premium of one year for most of the insurance policies are some of the risk indicators revealed by the investigation of which he, his mother and his wife were subjected. **Case study 22. Employee/Agent collusion, source of wealth, early cancellation** A drug trafficker purchased a life insurance policy with a value of US$80,000. The policy was purchased through an agent of a large life insurance company using a cashier's cheque. The investigation showed that the customer had made it known that the funds used to finance the policy were the proceeds of drug trafficking. In light of this fact, the agent charged significantly higher commission. Three months following this transaction, the investigation showed that the drug dealer cashed in his policy. **Case study 23. Unusually high premium**

		An insurer in Country A sought reinsurance with a reputable reinsurance company in Country B for its directors and officers cover of an investment firm in Country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer which contacted law enforcement agencies. Investigation made clear that the investment firm was bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that – although drug money would be laundered by a payment received from the reinsurer – the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsurer. By offering to pay above market rate the insurer probably intended to assure continuation of the reinsurance arrangement.
Terrorist Financing		
		Case study 1. Fraudulent claim A leader of a terrorist organization instructed Mr. X, who was trained in Afghanistan and fought U.S. forces in the country for several years, to set aside his initial intention to volunteer as a suicide bomber and sent him to Country A to support the organization from there. In September 2004, Mr. X attempted to acquire large sums of money from life insurance companies fraudulently, intending to direct a great part of this money to the terrorist organization in order to fund its terrorist activities. To this end, Mr. X recruited Mr. Y and Mr. Z, Mr Y's brother. Life insurance policies of 4 million euro were taken out for Mr. Y with his brother, Mr. Z, as the designated beneficiary. Mr. Y was to fake a fatal traffic accident during his stay in Country B. By obtaining a death certificate, if necessary through bribery, the life insurance benefits were to be collected by Mr. Z who would transfer the proceeds abroad via foreign bank accounts to fund terrorist activities. Mr. X was primarily responsible for paying the insurance premiums for these life contracts. The plan was thwarted when Mr. X and Mr. Y were arrested in January 2005. *Subsequent action* Mr. X and Mr. Y were convicted of membership in a terrorist organization and multiple counts of fraud. Mr. X was sentenced to seven years in prison and Mr. Y to six. Mr. Z was also convicted of the lesser charge of supporting a terrorist organization and fraud. He was sentenced to three and a half years in prison. **Case study 2. Early cancellation** Setting up the return of a foreign fighter from a conflict zone required several thousand euros. Accordingly, the close associates of the individual wishing to come back to France had to mobilize funds. Transactions were observed on the accounts of members of

		the family and a circle of sympathizers of individuals present in the combat zone. These operations took various forms. The most frequent were cash withdrawals arising from the proceeds of car or house sales, or from early surrender of a life insurance policy. The insurer submitted a STR to the FIU.
Important Note		
		Apart from the above examples of money laundering and terrorist financing cases, the IAIS has also published specific cases and examples of money laundering in a document called "Guidance Paper on Anti-money Laundering and Combating the Financing of Terrorism". The document can be downloaded from the IAIS website at http://www.iaisweb.org/. IIs are advised to regularly browse the website for latest information.

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)
EDD	Enhanced due diligence
FATF	Financial Action Task Force
FI(s)	Financial institution(s) (Note: unless specified otherwise (e.g. an FI as defined in the AMLO), the term "financial institutions (FIs)" has the same definition as set out in the FATF Recommendations.)
IA	Insurance Authority
IAIS	International Association of Insurance Supervisors
II(s)	Insurance institution(s), referring to authorized insurers and reinsurers carrying on long term business, and licensed individual insurance agents, licensed insurance agencies and licensed insurance broker companies carrying on regulated activities in respect of long term business.
IO	Insurance Ordinance (Cap. 41)
JFIU	Joint Financial Intelligence Unit
MLRO	Money laundering reporting officer
ML/TF	Money laundering and terrorist financing
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)
PEP(s)	Politically exposed person(s)

Proliferation financing or PF	Financing of proliferation of weapons of mass destruction
RA(s)	Relevant authority (authorities)
RBA	Risk-based approach
Schedule 2	Schedule 2 to the AMLO
SDD	Simplified due diligence
Senior management	Senior management means directors (or board) and senior managers (or equivalent) of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business. This may include a firm's Chief Executive Officer, Managing Director, or other senior operating management personnel (as the case may be).
STR(s)	Suspicious transaction report(s)
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
UNSO	United Nations Sanctions Ordinance (Cap. 537)
WMD(CPS)O	Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526)